

Commutative Algebra

About this document

This is a revision of class notes taken during a commutative algebra course taught by Professors L. Barbieri-Viale (lectures) and F. Andreatta (exercise class) at the University of Milan during the academic year 10-11 for the Erasmus Mundus master ALGANT (Algebra, Geometry and Number Theory). Notes taken and typed by F. Binda.

Please report corrections, suggestions, complaints and criticisms.

PRELIMINARY VERSION: 21 March 2011.

Contents

General Introduction	1
Chapter 1. A brief review	3
1. Nakayama's lemma	3
2. Tensor products	4
3. Exact sequences and exactness of the tensor product	6
4. Localization	10
5. Local properties	12
6. Limits	13
Chapter 2. Rings and Algebras: a first view	15
1. Functoriality	16
2. Algebraic sets: a new point of view	19
3. Finiteness	21
4. Field extensions	21
Chapter 3. Hilbert's Nullstellensatz and consequences	27
1. Hilbert's theorem	27
2. Radical ideals	32
3. Geometric points	35
4. Rational Points	37
5. Polynomial mappings	38
Chapter 4. The spectrum of a ring	41
1. The Zariski's topology over $\text{Spec}(A)$	41
2. Nullstellensatz revisited	42
3. Noetherian spaces	46
Chapter 5. Primary decomposition	49
1. Minimal primes and primary ideals	49
2. Primary decomposition in Noetherian rings	52
Chapter 6. A first step in dimension theory	55
1. Basic definitions	55
2. Rings of dimension 0	57
Chapter 7. Valuations, normal rings and integral extensions	63
1. Normal rings and integral extensions	63
2. Further properties of integral extensions	66
3. The going-up theorem	68

4. Dimension and Codimension 1	71
5. Discrete valuations	73
6. Noether's normalization lemma	75
Chapter 8. Zariski's tangent space	79
1. Derivations and differentials	79
2. Zariski tangent space	85
3. Tangent space and dual numbers	87
Bibliography	89

General Introduction

The main task is to give an introduction to modern commutative algebra with a special regard to commutative ring theory, arithmetic, homological methods and algebraic geometry.

Commutative Algebra studies commutative rings (with identity), their ideals, and modules based on such rings. Both *algebraic geometry* and *algebraic number theory* are based on commutative algebra. Algebraic geometry combines commutative algebra with geometry. For example, solutions of systems of polynomial equations, the so called *algebraic sets*, are combined with related algebraic structures which are ideals in the polynomial ring.

Throughout this course, we will assume as known the basic notions: ideals, polynomial rings, localizations, tensor products of modules, Noetherian rings and modules: in section 1, we will review some definitions, theorems and propositions that we will use in the following chapters. Anyway, the reader that is not familiar with this topics can find (a lot of) material in a good textbook, such as [9] or [2].

CHAPTER 1

A brief review

Convention: by *ring* we will always mean (unless expressly specified) a commutative ring with $1 \neq 0$. If A is a ring, we will denote with \mathbf{Mod}_A the category of A -modules.

1. Nakayama's lemma

Remember that an ideal $\mathfrak{p} \neq (1)$ of a ring A is said to be *prime* if $xy \in \mathfrak{p}$ implies $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. An ideal \mathfrak{m} is said to be *maximal* if $\mathfrak{m} \neq (1)$ and if there is no ideal I such that $\mathfrak{m} \subsetneq I \subsetneq (1)$. It's well known that \mathfrak{p} is prime iff A/\mathfrak{p} is integral domain and that \mathfrak{m} is maximal iff A/\mathfrak{m} is a field.

Prime and maximal ideals play a fundamental role in commutative algebra, so let's state the following basic theorem:

1.1. Theorem. *Let A be a ring. Then there exist at least one maximal ideal \mathfrak{m} of A .*

As a corollary we have that an ideal I , $I \neq (1)$, is always contained in a maximal ideal \mathfrak{m} .

1.2. Definition. A ring A with exactly one maximal ideal \mathfrak{m} is called a *local ring*.

1.3. Definition. Let $M \in \mathbf{Mod}_A$:

- (1) We say that M is *finitely generated* if there exists positive integer n and a surjective homomorphism of A -modules $A^n \rightarrow M$.
- (2) We say that M is *finitely presented as A -module* if there exist positive integers m, n and two surjective homomorphism of A -modules: $\varphi: A^n \rightarrow M$ and $A^m \rightarrow \text{Ker } \varphi$. Each generator of the kernel is called a *relation*. Thus a finitely presented module can be described using finitely many generators and relations.

1.4. Lemma (Nakayama). *Let A be a local ring with maximal ideal \mathfrak{m} and M a finitely generated \mathbf{Mod}_A . If the quotient $M/\mathfrak{m}M = 0$, then $M = 0$.*

PROOF. Let's restate the thesis: we have $M/\mathfrak{m}M = 0$ iff $M = \mathfrak{m}M$ and we want to prove that this implies $M = 0$. Suppose $M \neq 0$ and search for a contradiction: let x_1, \dots, x_n be the generators of $M = \mathfrak{m}M$. So we can write $x_1 = a_1x_1 + \dots + a_nx_n$ with $a_i \in \mathfrak{m}$, that is $(1 - a_1)x_1 = a_2x_2 + \dots + a_nx_n$. We claim that $1 - a_1$ is a unit. If it's not, it must belong to \mathfrak{m} (that is the unique maximal ideal of A) and so we would have $1 - a_1 = m \in \mathfrak{m}$, that is $1 \in \mathfrak{m}$ and so $\mathfrak{m} = A$, a contradiction. Then let $u = (1 - a_1)^{-1}$ and write again $x_1 = ua_2x_2 + \dots + ua_nx_n$: in this way we have proved that M can be generated by less than n generators. By descending induction we obtain that there are no generators for M , which is absurd. \square

We have the following corollary:

1.5. Corollary. *Let A be a local ring and let $\mathfrak{m} \subset A$ be the maximal ideal. Let $M, N \in \mathbf{Mod}_A$ and consider a homomorphism of A -modules $\varphi: M \rightarrow N$. Suppose that N is finitely generated. If the map induced by φ , $\bar{\varphi}: M/\mathfrak{m}M \rightarrow N/\mathfrak{m}N$, is surjective, then φ itself is surjective.*

PROOF. To prove that φ is surjective, we prove that $\text{Coker}(\varphi) := N/\varphi(M) = 0$. So we have $\bar{\varphi}$ surjective if and only if $0 = \text{Coker}(\bar{\varphi})$. But

$$(1.1) \quad \text{Coker}(\bar{\varphi}) = \frac{N/\mathfrak{m}N}{\bar{\varphi}(\frac{M}{\mathfrak{m}M})} \simeq \frac{N}{\varphi(M) + \mathfrak{m}N} \simeq \frac{\text{Coker}(\varphi)}{\mathfrak{m} \text{Coker}(\varphi)}.$$

To explain the isomorphisms, observe that $\bar{\varphi}(\frac{M}{\mathfrak{m}M}) = (\varphi(M))/\mathfrak{m}N = (\varphi(M) + \mathfrak{m}N)/\mathfrak{m}N$. The first equality is given by the definition of the induced map $\bar{\varphi}$. Now note that $\varphi(M) + \mathfrak{m}N$ contains $\mathfrak{m}N$, so we can apply the so-called third isomorphism theorem for A -modules¹ and thus obtain the first isomorphism in 1.1. To prove the second isomorphism, note that $\varphi(M) + \mathfrak{m}N \supset \mathfrak{m}N$: by applying again the third isomorphism theorem we have:

$$\frac{N}{\varphi(M) + \mathfrak{m}N} \simeq \frac{\frac{N}{\varphi(M)}}{\frac{\varphi(M) + \mathfrak{m}N}{\varphi(M)}} \simeq \frac{\text{Coker}(\varphi)}{\mathfrak{m} \text{Coker}(\varphi)}$$

Hence we have $0 = \text{Coker}(\bar{\varphi}) \simeq \frac{\text{Coker}(\varphi)}{\mathfrak{m} \text{Coker}(\varphi)}$. But $\text{Coker}(\varphi)$ is a quotient of N , which is finitely generated. Thus must be finitely generated itself. We can apply Nakayama's lemma and obtain the thesis. \square

1.6. Example. Let A, \mathfrak{m} as above. Let N be a finitely generated A -module. Then we have that the quotient $N/\mathfrak{m}N$ is a finitely generated A/\mathfrak{m} vector space²: fix a set e_1, \dots, e_n of N , such that their classes $\bar{e}_1, \dots, \bar{e}_n$ form a basis of $N/\mathfrak{m}N$ as A/\mathfrak{m} vector space. Consider the map $\varphi: A^n \rightarrow N$ defined by $(a_1, \dots, a_n) \mapsto \sum_{i=1}^n a_i e_i$. Then φ is surjective by corollary 1.5. To see this, consider the quotient map

$$\bar{\varphi}: A^n/(\mathfrak{m}A^n) = (A/\mathfrak{m})^n \rightarrow N/\mathfrak{m}N$$

this is clearly an isomorphism of vector spaces, thus is surjective.

Note that φ is not, generally, injective: take $N = A/\mathfrak{m}$ as A -module, then φ is the projection $\varphi: A \rightarrow A/\mathfrak{m}$ which is certainly not injective.

2. Tensor products

Tensor product of modules is another fundamental construction in commutative algebra. We wish to introduce it from the most natural point of view.

2.1. Definition. Let $M, N, P \in \mathbf{Mod}_A$. We say that a map $\varphi: M \times N \rightarrow P$ is *A -bilinear* if it is A -linear in both arguments. Define $\mathcal{L}(M, N)(P)$ as the set of all A -bilinear maps from $M \times N$ to P .

¹Let $A, B, C \in \mathbf{Mod}_A$ such that $A \subseteq B \subseteq C$. Then we have $\frac{C/A}{B/A} \simeq C/B$.

²This can be seen directly or using the isomorphism with a suitable tensor product.

It's easy to show that $\mathcal{L}(M, N)(-)$ is a covariant functor from \mathbf{Mod}_A to \mathbf{Set} . Indeed

$$\begin{array}{ccccc} P & \longrightarrow & \mathcal{L}(M, N)(P) & \ni & \varphi \\ \downarrow g & & \downarrow & & \downarrow \\ P' & \longrightarrow & \mathcal{L}(M, N)(P') & \ni & g \circ \varphi \end{array}$$

2.2. Remark. For all $M, N, P \in \mathbf{Mod}_A$, we have a bijection

$$\Gamma: \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P)) \simeq \mathcal{L}(M, N)(P)$$

$$(\Phi: M \rightarrow \mathrm{Hom}_A(N, P)) \mapsto \Gamma(\Phi)$$

such that, if $\Phi: x \mapsto \Phi_x \in \mathrm{Hom}_A(N, P)$, $\Gamma(\Phi): (x, y) \mapsto \Phi_x(y) \in P$. Note that this isomorphism is natural in P .

So we can ask the following question: is the functor $\mathcal{L}(M, N)(-)$ representable, which is to say that exists an A -module T such that $\mathcal{L}(M, N)(-)$ is naturally isomorphic to $\mathrm{Hom}_A(T, -)$? The answer is positive and is given by the module $T := M \otimes_A N$ that is called the *tensor product of M and N over A* .

We must show that such a module exists, but we first state the following properties, true for all $M, N, P \in \mathbf{Mod}_A$:

- (1) $M \otimes_A N \simeq N \otimes_A M$.
- (2) $M \otimes_A A \simeq M \simeq A \otimes_A M$.
- (3) $(M \otimes_A N) \otimes_A P \simeq M \otimes_A (N \otimes_A P)$.

Properties 1 and 3 can be proved using the universal property of the tensor product that we will state shortly. To show that 2 holds, consider the following isomorphisms: let $T = M \otimes_A A$, so we have

$$\mathrm{Hom}_A(T, P) \simeq \mathcal{L}(M, A)(P) = \mathrm{Hom}_A(M, \mathrm{Hom}_A(A, P)) \simeq \mathrm{Hom}_A(M, P)$$

for all $P \in \mathbf{Mod}_A$. Hence $M \simeq T = M \otimes_A A$.

Suppose again that exists $T \in \mathbf{Mod}_A$ and a natural isomorphism η between the functors $\mathcal{L}(M, N)(-)$ and $\mathrm{Hom}_A(T, -)$. Denote with η_P the bijection $\mathcal{L}(M, N)(P) \xrightarrow{\cong} \mathrm{Hom}_A(T, P)$ for any module P .

In particular, we have $\mathcal{L}(M, N)(T) \xrightarrow{\eta_T} \mathrm{Hom}_A(T, T)$. Let's write π for the unique map $\pi: M \times N \rightarrow T$ such that $\eta_T(\pi) = id_T$.

We show now that T has the following universal property:

2.3. Lemma. *Given any A -module P and any A -bilinear mapping $\varphi: M \times N \rightarrow P$, there exists a unique A -linear mapping $T \rightarrow P$ such that the diagram*

$$\begin{array}{ccc} M \times N & \xrightarrow{\pi} & T \\ & \searrow \varphi & \vdots \\ & & P \end{array}$$

commutes. In other words, every bilinear map on $M \times N$ factors through T .

PROOF. Let $p: T \rightarrow P$, $p \in \text{Hom}_A(T, P)$ be the map that is the image of φ through the isomorphism η_P , that is $p = \eta_P(\varphi)$: note that such p is unique. Now consider the following commutative square:

$$\begin{array}{ccc} \mathcal{L}(M, N)(T) & \xrightarrow{\eta_T} & \text{Hom}_A(T, T) & \xrightarrow{\pi} & \eta_T(\pi) \\ p \circ \downarrow & & p \circ \downarrow & & \downarrow \\ \mathcal{L}(M, N)(P) & \xrightarrow{\eta_P} & \text{Hom}_A(T, P) & \xrightarrow{p \circ \pi} & \eta_P(p \circ \pi) = p \circ \eta_T(\pi). \end{array}$$

We have that $p \circ \eta_T(\pi) = p \circ id_T = p = \eta_P(\varphi)$. The map η_P is a bijection, so it must be $p \circ \pi = \varphi$. \square

We still have to prove that such a module exists. Let C be the free A -module $A^{M \times N}$ generated by the elements of $M \times N$, so that $A^{M \times N} = \{\sum_{finite} a_i(x_i, y_i) : x_i \in M, y_i \in N, a_i \in A\}$. Let D be the submodule of C generated by all elements in the following forms:

- i) $(x + x', y) - (x, y) - (x', y)$
- ii) $(x, y + y') - (x, y) - (x, y')$
- iii) $(ax, y) - a(x, y)$
- iv) $(x, ay) - a(x, y)$

We can now *define* the module T as the quotient $T = C/D$. Given a generator (x, y) of C , we will denote its class with $x \otimes y$. In this way, if $t \in T$ then $t = \sum_{i=1}^n a_i(x_i \otimes y_i)$ with $a_i \in A$. So we have a canonical mapping $M \times N \rightarrow T$ given by $(x, y) \rightarrow x \otimes y$.

Further, any bilinear map $\varphi: M \times N \rightarrow P$, can be extended by A -linearity to a map $\bar{\varphi}: C \rightarrow P$. Obviously $\bar{\varphi}$ vanishes on all the generators of D , so we can define a new map $\hat{\varphi}: T = C/D \rightarrow P$ such that $\hat{\varphi}(x \otimes y) = \varphi(x, y)$. The map is clearly unique, so T satisfies the universal property for the tensor product and we can say $T \simeq M \otimes_A N$.

3. Exact sequences and exactness of the tensor product

3.1. Definition. A sequence of A -modules

$$\dots \rightarrow M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} M_{i+2} \rightarrow \dots$$

is called an *exact sequence* if, for every i , we have $\text{Im}(f_i) = \text{Ker}(f_{i+1})$. An exact sequence of the type

$$0 \rightarrow M \rightarrow N \rightarrow P \rightarrow 0$$

is called a *short exact sequence*.

3.2. Remark. Any exact sequence can be split into the union of short exact sequences by restricting to kernels and images. This is the reason why we will (almost always) reduce to short sequences.

We now give a proof of the so called *snake lemma*, a statement valid in every abelian category, that is a crucial tool used to construct long exact sequences.

3.3. Proposition. *Let*

$$\begin{array}{ccccccc} M & \xrightarrow{f} & N & \xrightarrow{g} & P & \longrightarrow & 0 \\ & & \downarrow a & & \downarrow b & & \downarrow c \\ 0 & \longrightarrow & M' & \xrightarrow{f'} & N' & \xrightarrow{g'} & P' \end{array}$$

be a commutative diagram of A -modules with exact rows. Then there is an exact sequence relating the kernels and cokernels of a , b , and c :

$$\mathrm{Ker}(a) \rightarrow \mathrm{Ker}(b) \rightarrow \mathrm{Ker}(c) \xrightarrow{\delta} \mathrm{Coker}(a) \rightarrow \mathrm{Coker}(b) \rightarrow \mathrm{Coker}(c)$$

where δ is called the “snake” or the “boundary” homomorphism $\delta: \mathrm{Ker}(c) \rightarrow \mathrm{Coker}(a)$.

PROOF. We can define the map δ as follows: given $x \in \mathrm{Ker}(c)$ we can view it as an element of P . Since g is onto, there exists an element $y \in N$ such that $g(y) = x$. Because of the commutativity of the diagram, we have $g'(b(y)) = c(g(y)) = c(x) = 0$, therefore $b(y) \in \mathrm{Ker}(g') = \mathrm{Im}(f')$, by the exactness of the bottom row. So we find an element $z \in M'$ such that $f'(z) = b(y)$: z is unique since f' is injective. We then define $\delta(x) = z + \mathrm{Im}(a)$. Now one has to check that δ is well-defined (i.e. $\delta(x)$ only depends on x and not on the choice of y), that it is a homomorphism, and that the resulting long sequence is indeed exact. We leave the verification to the reader. \square

3.4. Definition. Let $F: \mathbf{Mod}_A \rightarrow \mathbf{Mod}_A$ be a functor. F is called *exact* if, given an exact sequence of A -modules

$$\cdots \rightarrow M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} M_{i+2} \rightarrow \cdots$$

the sequence

$$\cdots \rightarrow F(M_i) \xrightarrow{F(f_i)} F(M_{i+1}) \xrightarrow{F(f_{i+1})} F(M_{i+2}) \rightarrow \cdots$$

is exact.

3.5. Proposition. *Let $M, N, P \in \mathbf{Mod}_A$.*

(1) *The sequence of A -modules.*

$$(3.1) \quad M \xrightarrow{f} N \xrightarrow{g} P \rightarrow 0$$

is exact iff for all A -module Q the sequence

$$(3.2) \quad 0 \rightarrow \mathrm{Hom}_A(P, Q) \xrightarrow{\hat{g}} \mathrm{Hom}_A(N, Q) \xrightarrow{\hat{f}} \mathrm{Hom}_A(M, Q)$$

is an exact sequence.

(2) *The sequence of A -modules.*

$$(3.3) \quad 0 \rightarrow M \xrightarrow{f} N \xrightarrow{g} P$$

is exact iff for all A -module Q the sequence

$$(3.4) \quad 0 \rightarrow \mathrm{Hom}_A(Q, M) \xrightarrow{\bar{f}} \mathrm{Hom}_A(Q, N) \xrightarrow{\bar{g}} \mathrm{Hom}_A(Q, P)$$

is an exact sequence.

PROOF. Let's prove one arrow in the first statement and leave the other parts of this proposition as an exercise³. Suppose that the sequence (3.1) is exact: we wish to show that (3.2) is exact. First we prove that \hat{g} is injective, that is $\text{Ker } \hat{g} = 0$. Let $\alpha: P \rightarrow Q$ be a homomorphism of A -module such that $\alpha \circ g = 0$. Being g surjective, we have that for all $p \in P$, there exists $n \in N$ such that $p = g(n)$. Hence, $\alpha(p) = \alpha(g(n)) = 0$ for all $p \in P$, that is $\alpha = 0$.

Now we want to prove that $\text{Im}(\hat{g}) = \text{Ker}(\hat{f})$. Given $\varphi \in \text{Hom}(N, Q)$ such that $\varphi \circ f = 0$. We need to show that there is a unique map $\bar{\varphi} \in \text{Hom}(P, Q)$ such that the diagram

$$\begin{array}{ccccc} M & \xrightarrow{f} & N & \xrightarrow{g} & P \\ & \searrow 0 & \downarrow \varphi & \swarrow \bar{\varphi} & \\ & & Q & & \end{array}$$

commutes. To do this, observe again that, being g onto, for all $p \in P$ we can find $n \in N$ such that $p = g(n)$. Define $\bar{\varphi}(p) = \varphi(n)$ for such n . The map $\bar{\varphi}$ is well defined, since if $m, n \in N$ are such that $p = g(n) = g(m)$, we have $n - m \in \text{Ker}(g) = \text{Im}(f)$, so $n - m = f(t)$ for a suitable $t \in M$. Thus, $0 = \varphi(f(t)) = \varphi(n) - \varphi(m)$, that proves $\varphi(n) = \varphi(m)$ and the definition of $\bar{\varphi}(p)$ does not depend on the choice of the lifting element $n \in N$. $\bar{\varphi}$ is also a homomorphism of A -modules (easy check), so $\bar{\varphi} \in \text{Hom}(P, Q)$ and it's such that $\bar{\varphi} \circ g = \varphi$, which is to say that $\bar{\varphi} \in \text{Im}(\hat{g})$: in this way we have proved that $\text{Im}(\hat{g}) \supset \text{Ker}(\hat{f})$.

Let now be $\psi \in \text{Im}(\hat{g})$, which is to say that there is $\beta \in \text{Hom}(P, Q)$ such that $\beta \circ g = \varphi$. In this case we have $\alpha \circ f = \beta \circ (g \circ f)$ but $\text{Im}(f) = \text{Ker}(g)$, so we have, for all $m \in M$, $\beta(g(f(m))) = 0$, hence $\psi \in \text{Ker}(\hat{f})$. \square

We have the following proposition that tell us something about the exactness of the tensor product:

3.6. Proposition. *Let*

$$(3.5) \quad M \xrightarrow{f} N \xrightarrow{g} P \rightarrow 0$$

be an exact sequence of A -modules. Let Q be any A -module. Then the sequence

$$(3.6) \quad M \otimes_A Q \xrightarrow{f \otimes 1} N \otimes_A Q \xrightarrow{g \otimes 1} P \otimes_A Q \rightarrow 0$$

is exact (where $1 = id_Q$ denotes the identity map on Q).

3.7. Remark. In this case we say that the functor $- \otimes_A Q$ is *right-exact*. The tensor product is *not*, generally, an exact functor. If Q is an A -module such that, for every short exact sequence of modules

$$0 \rightarrow M \rightarrow N \rightarrow P \rightarrow 0$$

we have

$$0 \rightarrow M \otimes_A Q \rightarrow N \otimes_A Q \rightarrow P \otimes_A Q \rightarrow 0$$

exact, then Q is called a *flat module over A* and we say that Q is *A -flat*.

³You can find the proof of the converse implication on [2], proposition 2.9.

PROOF. We just need to apply the proposition 3.5. From the exactness of (3.5) we deduce that the sequence

$$(3.7) \quad 0 \rightarrow \text{Hom}(P, \text{Hom}(Q, F)) \rightarrow \text{Hom}(N, \text{Hom}(Q, F)) \rightarrow \text{Hom}(M, \text{Hom}(Q, F))$$

for any A -module F . But we have a natural isomorphism that allow us to restate the sequence (3.7) in the following way

$$0 \rightarrow \text{Hom}(P \otimes Q, F) \rightarrow \text{Hom}(N \otimes Q, F) \rightarrow \text{Hom}(M \otimes Q, F)$$

which is again an exact sequence for any A -module F . Apply again proposition 3.5 and obtain the thesis. \square

3.8. Example. Let $A = K[x, y]$ with K field. Let Q be the ideal (x, y) and consider it as A -module. Is it A -flat?

We claim that it is not: by the previous proposition, we just need to show that the tensor product with Q does not preserve injective maps. Consider the exact sequence $0 \rightarrow Q \hookrightarrow A$ given by the inclusion of Q into A . If we tensor with Q we obtain

$$\begin{array}{ccccc} Q \otimes_A Q & \xrightarrow{g} & A \otimes_A Q & \xrightarrow{\simeq} & Q \\ & & 1 \otimes q & \longleftarrow & q \\ m \otimes n & \longrightarrow & m \otimes n = 1 \otimes mn & \longrightarrow & mn. \end{array}$$

The map g brings a generator $m \otimes n$ to itself but seen as an element of $A \otimes_A Q$. By A -linearity we can write $m \otimes n = 1 \otimes mn$ and then apply the isomorphism to Q (which is simply given by multiplication). To show that g is not injective we have to find a non-trivial element in $\text{Ker}(g)$. Notice that $x \otimes y - y \otimes x \mapsto 0$: if it's not zero we have done.

To prove this, consider the quotient $B = Q/Q^2 = (x, y)/(x, y)^2 = (x, y)/(x^2, y^2, xy)$. If (x, y) is formed by all polynomials $f(x, y)$ whose value in $(0, 0)$ is equal to zero, the quotient classes B are given by linear polynomials in the variables x, y without constant terms, that⁴ is $B \simeq K\bar{x} \oplus K\bar{y}$.

Now consider the tensor product:

$$Q/Q^2 \otimes_K Q/Q^2 \simeq (K\bar{x} \otimes \bar{y}) \oplus (K\bar{y} \otimes \bar{x}) \oplus (K\bar{x} \otimes \bar{x}) \oplus (K\bar{y} \otimes \bar{y}) \simeq K^4$$

where we used that the tensor product commutes with direct sums. If $\pi: Q \rightarrow Q/Q^2$ denotes the projection on the quotient, there is an induced map

$$\pi \otimes \pi: Q \otimes_A Q \rightarrow Q/Q^2 \otimes_K Q/Q^2$$

and $x \otimes y - y \otimes x \mapsto \bar{x} \otimes \bar{y} - \bar{y} \otimes \bar{x} \mapsto (1, -1, 0, 0) \neq 0$ in K^4 , that is $(x \otimes y - y \otimes x) \neq 0$.

We give another proof of the previous fact using the *snake lemma*: consider the map $\varphi: A \times A \rightarrow Q$ with $(a, b) \mapsto ax + by$. φ is clearly onto and if $(a, b) \in \text{Ker}(\varphi)$ then $ax + by = 0$, that is $ax = -by$. Hence $a = cy$, $b = -cx$ for $c \in A$; thus $\text{Ker}(\varphi) \simeq A$ and we have the short exact sequence

$$0 \rightarrow \text{Ker}(\varphi) \simeq A \xrightarrow{\Phi} A \times A \xrightarrow{\varphi} Q \rightarrow 0$$

⁴We denote with \bar{x} and \bar{y} the classes in the quotient: for example, we have $\bar{x} = x + (x^2, y^2, xy)$.

with $\Phi(c) = (cy, -cx)$. If we compute the tensor product with Q , we obtain the following commutative diagram

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & \text{Ker } g \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & Q & \longrightarrow & Q \times Q & \longrightarrow & Q \otimes_A Q \longrightarrow 0 \\
 & & \downarrow \iota & & \downarrow & & \downarrow g \\
 0 & \longrightarrow & A & \longrightarrow & A \times A & \xrightarrow{\varphi} & Q \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & K \simeq A/Q & \longrightarrow & K \times K & \longrightarrow & Q/Q^2
 \end{array}$$

By the snake lemma, we obtain the exact sequence $0 \rightarrow \text{Ker}(g) \rightarrow K \simeq A/Q = \text{Coker}(\iota) \rightarrow K \times K$. Notice that the map $A/Q \rightarrow K \times K$ is the null map, since, for every $\bar{c} \in A/Q$ we have $\bar{c} \mapsto (\bar{c}y, -\bar{c}x) = 0$. Since the sequence is exact, we have $\text{Im}(\text{Ker}(g) \rightarrow K) = \text{Ker}(A/Q \rightarrow K \times K) = A/Q = K$, hence we have an isomorphism $\text{Ker}(g) \simeq K \neq 0$ which prove our statement.

4. Localization

4.1. Definition. Let A be any ring. A *multiplicatively closed* subset of A is a subset S of A such that $1 \in S$ and S is closed under multiplication. Define a relation \sim on $A \times S$ as follows:

$$(a, s) \sim (b, t) \text{ iff there exists } u \in S \text{ such that } u(ta - sb) = 0$$

The quotient set $S^{-1}A = A \times S / \sim$ given by $\{\overline{(a, s)} := a/s\}$ has a natural ring structure by defining addition and multiplication of these fractions a/s in the same way as in elementary algebra:

$$\begin{aligned}
 \frac{a}{s} \cdot \frac{b}{t} &= \frac{ab}{st} \\
 \frac{a}{s} + \frac{b}{t} &= \frac{at + bs}{st}
 \end{aligned}$$

The ring $S^{-1}A$ is called the *localization of A to S* or the *ring of fractions of A* with respect to S . We also have a ring homomorphism $A \xrightarrow{f} S^{-1}A$ defined by $f(x) = x/1$. Note that this map needs not to be injective.

The ring of fractions $S^{-1}A$ has the following universal property:

4.2. Proposition. Let A be a ring and S a multiplicative set in A . If $g: A \rightarrow B$ is a homomorphism of ring such that $g(x)$ is a unit in B for all $x \in S \subset A$, then there exists a unique homomorphism $h: S^{-1}A \rightarrow B$ such that the diagram

$$\begin{array}{ccc}
 A & \xrightarrow{f} & S^{-1}A \\
 & \searrow g & \downarrow \text{\scriptsize } h \\
 & & B
 \end{array}$$

commutes.

PROOF. See [2], proposition 3.1. \square

4.3. Remark. Let $\mathfrak{p} \subset A$ be a prime ideal. Then the set $S = A \setminus \mathfrak{p}$ is a multiplicative set. We denote the localized ring $S^{-1}A$ with $A_{\mathfrak{p}}$.

4.4. Remark. Let D be an integral domain, then $\mathfrak{p} = (0)$ is a prime ideal and $D_{\mathfrak{p}} \simeq \text{Frac}(D)$, the field of fractions of D .

We can imitate the construction of the ring of fractions with an A -module M instead of the ring A . Define a relation \sim on $M \times S$ as follows:

$$(m, s) \sim (n, t) \text{ iff there exists } u \in S \text{ such that } u(tm - sm) = 0$$

As before, the relation \sim is an equivalence and we can consider the set $S^{-1}M = M \times S / \sim$. We can denote with m/s the equivalence class of the pair (m, s) . With the sum defined as above and the obvious scalar multiplication, the set $S^{-1}M$ becomes an $S^{-1}A$ -module.

Let $f: M \rightarrow N$ be a homomorphism of A -modules. Then we can define an induced $S^{-1}A$ -modules homomorphism $S^{-1}(f): S^{-1}M \rightarrow S^{-1}N$ such that $m/s \mapsto f(m)/s$. Notice that $S^{-1}(f \circ g) = S^{-1}(f) \circ S^{-1}(g)$.

4.5. Remark. Fixed A and S , we have thus defined a covariant functor $S^{-1}(-): \mathbf{Mod}_A \rightarrow S^{-1}A\text{-Mod}$.

4.6. Proposition. Let A, S as above. The functor $S^{-1}(-)$ is exact.

PROOF. Let $M, N, P \in \mathbf{Mod}_A$ and let $M \xrightarrow{f} N \xrightarrow{g} P$ be an exact sequence. Thus we have to show that $S^{-1}M \xrightarrow{S^{-1}f} S^{-1}N \xrightarrow{S^{-1}g} S^{-1}P$ is exact: being $S^{-1}(-)$ a functor, it preserves compositions. Hence, since $g \circ f = 0$, we have $S^{-1}g \circ S^{-1}f = 0$, that is $\text{Im}(S^{-1}f) \subseteq \text{Ker}(S^{-1}g)$. To show the reverse inclusion, let $n/s \in \text{Ker}(S^{-1}g)$, that is $g(n)/s = 0 := 0/1$. By definition, there exists $t \in S$ such that $tg(n) = 0$, that is $g(tn) = 0$. Thus $tn \in \text{Ker}(g) = \text{Im}(f)$ and we can find $m \in M$ such that $f(m) = tn$. Hence, in $S^{-1}N$ we have $n/s = nt/st = f(m)/st \in \text{Im}(S^{-1}f)$ and we have done. \square

4.7. Proposition. Let A, S as above and let M be an A -module. Then we have an isomorphism of $S^{-1}A$ -modules: $S^{-1}M \simeq M \otimes_A S^{-1}A$.

PROOF. It's easy to show that the map $a/s \otimes m \mapsto am/s$ it's a homomorphism of $S^{-1}A$ -modules with inverse $x/s \mapsto 1/s \otimes x$. \square

4.8. Remark. Using the universal property of the tensor product and of the localization, it can be shown (see [2], proposition 3.5) that there exists a *unique* isomorphism $f: M \otimes_A S^{-1}A \rightarrow S^{-1}M$ for which $f((a/s) \otimes m) = am/s$ for all $a \in A, s \in S, m \in M$.

4.9. Remark. As a consequence of the propositions 4.6 and 4.7, we have that $S^{-1}A$ is flat as A -module.

4.10. Proposition. Let $M \in \mathbf{Mod}_A, \mathfrak{p} \subset A$ a prime ideal. Then there exists a canonical isomorphism of $A_{\mathfrak{p}}$ -modules

$$(M/\mathfrak{p}M)_{\mathfrak{p}} \simeq M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}}.$$

PROOF. First notice that $\mathfrak{p}M_{\mathfrak{p}} \simeq (\mathfrak{p}M)_{\mathfrak{p}}$. We have the exact sequence

$$0 \rightarrow \mathfrak{p}M \rightarrow M \rightarrow M/\mathfrak{p}M \rightarrow 0$$

and by the exactness of the localization we obtain that

$$0 \rightarrow (\mathfrak{p}M)_{\mathfrak{p}} \rightarrow M_{\mathfrak{p}} \rightarrow (M/\mathfrak{p}M)_{\mathfrak{p}} \rightarrow 0$$

is exact. Hence $(M/\mathfrak{p}M)_{\mathfrak{p}} \simeq M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}}$. \square

4.11. Remark. If we consider $A = M$ as an A -module, we notice that $(A/\mathfrak{p}A)_{\mathfrak{p}}$ is the localization of $A/\mathfrak{p}A$ with respect to the image of $(A - \mathfrak{p}) \rightarrow A/\mathfrak{p}A$, that is the multiplicative set $A/\mathfrak{p}A \setminus \{0\}$. Indeed, the quotient ring is integral, since \mathfrak{p} is prime. Hence, by the universal property of the localization, we have the following isomorphisms:

$$A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \simeq (A/\mathfrak{p}A)_{\mathfrak{p}} \simeq \text{Frac}(A/\mathfrak{p}A).$$

5. Local properties

5.1. Definition. We say that a property \mathcal{P} for rings, A -modules or homomorphisms of A -modules is *local* if the following is true: \mathcal{P} is true \Leftrightarrow for all \mathfrak{p} prime ideal, $\mathfrak{p} \subset A$, property \mathcal{P} holds true for $A_{\mathfrak{p}}$, $A_{\mathfrak{p}}$ -modules, homomorphisms of $A_{\mathfrak{p}}$ -modules.

As an example of local property

5.2. Proposition. *Let $M \in \mathbf{Mod}_A$. Then $M = 0$ iff for all \mathfrak{p} prime ideal, $\mathfrak{p} \subset A$, $M_{\mathfrak{p}} = 0$.*

PROOF. We just need to prove one implication, since if $M = 0$ then $M_{\mathfrak{p}} = 0$ for all \mathfrak{p} prime. Suppose $M \neq 0$ and take $0 \neq x \in M$. We define the *annihilator of x* , $\text{Ann}(x) = \{a \in A : ax = 0\}$. $\text{Ann}(x)$ is a proper ideal of A (since $1 \notin \text{Ann}(x)$), so there exists a maximal ideal \mathfrak{m} such that $\text{Ann}(x) \subseteq \mathfrak{m} \subset A$. Then, by assumption, we have $M_{\mathfrak{m}} = 0$, that is there exists $c \in A \setminus \mathfrak{m}$ such that $cx = 0$. Hence $c \in \text{Ann}(x) \subseteq \mathfrak{m}$, which is absurd. \square

From this proposition, we obtain the following corollaries:

5.3. Corollary. *Consider $M \xrightarrow{\varphi} N$ a homomorphism of A -modules. Then:*

- (1) φ is surjective iff for all \mathfrak{p} prime ideal, the map $\varphi_{\mathfrak{p}}: M_{\mathfrak{p}} \rightarrow N_{\mathfrak{p}}$ is surjective,
- (2) φ is injective iff for all \mathfrak{p} prime ideal, the map $\varphi_{\mathfrak{p}}: M_{\mathfrak{p}} \rightarrow N_{\mathfrak{p}}$ is injective.

5.4. Remark. Assume that M is finitely generated. Then we have $M = 0 \Leftrightarrow$ for all \mathfrak{m} maximal ideal, $\mathfrak{m} \subset A$, $M_{\mathfrak{m}} = 0$ (equivalent to the previous proposition) \Leftrightarrow (Nakayama's lemma) $M_{\mathfrak{m}}/\mathfrak{m}M_{\mathfrak{m}} = 0$. This is a simple fact: in order to show it, notice that, since \mathfrak{m} is maximal, $(A/\mathfrak{m})_{\mathfrak{m}} \simeq A/\mathfrak{m}$, so we have $M_{\mathfrak{m}}/\mathfrak{m}M_{\mathfrak{m}} \simeq (M/\mathfrak{m}M)_{\mathfrak{m}}$.

5.5. Corollary. *Let $M \xrightarrow{\varphi} N$ a homomorphism of A -modules. Suppose that M is finitely generated as A -modules. Then φ is onto iff for all \mathfrak{p} prime (or maximal) the map $\bar{\varphi}_{\mathfrak{p}}: N/\mathfrak{p}N \rightarrow M/\mathfrak{p}M$ is onto.*

PROOF. Apply the remark to $\text{Coker}(\varphi)$ and use that $\text{Coker}(\varphi)_{\mathfrak{p}}/\mathfrak{p}\text{Coker}(\varphi)_{\mathfrak{p}} \simeq \text{Coker}(\bar{\varphi}_{\mathfrak{p}})$. \square

6. Limits

6.1. Definition. A nonempty set I is called a *direct set* if (I, \leq) is a partially ordered set such that for every $\alpha, \beta \in I$, there exists $\gamma \in I$ such that $\alpha \leq \gamma$ and $\beta \leq \gamma$.

6.2. Definition. A family of objects $(X_\alpha)_{\alpha \in I}$ is a *direct system indexed by a direct set I* if for every $\alpha, \beta \in I$ with $\alpha \leq \beta$ there exists a morphism $\varphi_{\alpha\beta}: X_\alpha \rightarrow X_\beta$ such that:

- i) $\varphi_{\alpha\alpha} = id_{X_\alpha}$ for all $\alpha \in I$.
- ii) For any $\alpha, \beta, \gamma \in I$ where $\alpha \leq \beta \leq \gamma$, the following diagram commutes:

$$\begin{array}{ccc} X_\alpha & \xrightarrow{\varphi_{\alpha\beta}} & X_\beta \\ & \searrow \varphi_{\alpha\gamma} & \swarrow \varphi_{\beta\gamma} \\ & & X_\gamma \end{array}$$

6.3. Definition. A *direct limit* of a direct system $(X_\alpha)_{\alpha \in I}$ is an object, denoted by $\varinjlim(X_\alpha)$, with a family of morphisms $\varphi_\alpha: X_\alpha \rightarrow \varinjlim(X_\alpha)$ such that for every $\alpha, \beta \in I$ with $\alpha \leq \beta$ we have $\varphi_\beta \circ \varphi_{\alpha\beta} = \varphi_\alpha$. Further, a direct limit satisfies the following universal property: for every object Y with morphisms $\psi_\alpha: X_\alpha \rightarrow Y$ such that $\psi_\beta \circ \varphi_{\alpha\beta} = \psi_\alpha$, there exists a unique morphism φ making the following diagram commutative for all $\alpha \leq \beta$:

$$\begin{array}{ccccc} & & & & Y \\ & & & & \uparrow \\ & & & & \psi_\beta \\ X_\alpha & \xrightarrow{\varphi_{\alpha\beta}} & X_\beta & \xrightarrow{\psi_\beta} & \\ & \searrow \varphi_\alpha & \swarrow \varphi_\beta & & \vdots \\ & & & & \varinjlim(X_\alpha) \\ & & & & \downarrow \varphi \end{array}$$

6.4. Example. If we consider the category **Set** where morphisms are set inclusions, then given $X_0 \subseteq X_1 \subseteq X_2 \subseteq \dots \subseteq X_n \subseteq \dots$ we have that

$$\varinjlim(X_i) = \bigcup_{i=0}^{\infty} X_i.$$

6.5. Example. If X_α are Abelian groups, then $\varinjlim(X_\alpha) = \bigoplus X_\alpha / D$ where D is the Abelian group generated by $x'_\alpha - \varphi_{\alpha\beta}(x_\alpha)'$ where $x_\alpha \in X_\alpha$ and x'_α and $\varphi_{\alpha\beta}(x_\alpha)'$ are the images of x_α and $\varphi_{\alpha\beta}(x_\alpha)$ in $\bigoplus X_\alpha$.

6.6. Exercise. Show that the Direct limit is an exact functor from the category of direct systems of modules over a fixed directed set to the category of modules. In other words, let $(A_\alpha)_{\alpha \in I}$, $(B_\alpha)_{\alpha \in I}$ and $(C_\alpha)_{\alpha \in I}$ be direct systems of R -modules over the directed set I and consider maps $\varphi_\alpha: A_\alpha \rightarrow B_\alpha$ and $\psi_\alpha: B_\alpha \rightarrow C_\alpha$ such that, for every $\alpha \in I$, the sequence

$$0 \rightarrow A_\alpha \xrightarrow{\varphi_\alpha} B_\alpha \xrightarrow{\psi_\alpha} C_\alpha \rightarrow 0$$

is exact. Then the sequence

$$0 \rightarrow \varinjlim(A_\alpha) \xrightarrow{\varinjlim \varphi_\alpha} \varinjlim(B_\alpha) \xrightarrow{\varinjlim \psi_\alpha} \varinjlim(C_\alpha) \rightarrow 0$$

is exact.

6.7. Exercise. Let A be a ring, $S \subset A$ be a multiplicatively closed set and $M \in \mathbf{Mod}_A$. For every $s \in S$, we denote by M_s the localization of M with respect to the multiplicative set $\{1, s, s^2, \dots\}$. Then we have a family of modules indexed by S . Notice that this is a direct system. In fact for every $s, s' \in S$, we have inclusions $M_s \hookrightarrow M_{ss'}$ and $M_{s'} \hookrightarrow M_{ss'}$. Show that $S^{-1}M = \varinjlim(M_s)$.

CHAPTER 2

Rings and Algebras: a first view

The goal of the first part of the course is *Hilbert's Nullstellensatz*, the fundamental theorem that connects algebraic objects (ring of polynomials) to geometric objects (algebraic sets or varieties). In order to state the theorem, in the following section, we need to recall some important facts about rings and algebras over a fixed ring.

Let $A \xrightarrow{f} B$ be a ring homomorphism. We begin by stating the so-called *substitution principle*:

0.8. Proposition. *Let A, B, f as above. Given $b \in B$, there exist a unique homomorphism $f_b: A[x] \rightarrow B$ such that $f_b|_A = f$ and sending x to b .*

PROOF. For the existence, let us define a ring homomorphism satisfying the two conditions. If $p(x) \in A[x]$, we have $p(x) = \sum_{k=0}^n a_k x^k$. So we can define $f_b(p(x)) = \sum_{k=0}^n f(a_k) b^k$. Obviously f_b is such that $f_b(a) = f(a)$ for all $a \in A$ and that $f_b(x) = b$. It is actually unique: if $\varphi: A[x] \rightarrow B$ is such that $\varphi|_A = f$ and such that $\varphi(x) = b$, then $\varphi(x^k) = b^k$ and φ must act as f_b . \square

0.9. Corollary. *Given $b_1, \dots, b_n \in B$, there exist a unique homomorphism $A[x_1, \dots, x_n] \rightarrow B$ such that $x_i \mapsto b_i$ and such that, as before, the triangle*

$$\begin{array}{ccc} A[x_1, \dots, x_n] & \longrightarrow & B \\ \uparrow & \nearrow f & \\ A & & \end{array}$$

commutes.

Let's take a closer look: if we denote by $\text{Hom}_A(A[x], B)$ the set of A -linear ring homomorphisms, which is to say homomorphisms that extend f to $A[x]$ in the way we explained above, we have proved that there is a bijection

$$\begin{aligned} B &\longrightarrow \text{Hom}_A(A[x], B) \\ b &\longmapsto f_b \end{aligned}$$

0.10. Definition. A ring B along with a ring homomorphism $A \xrightarrow{f} B$ is called an *A -algebra*.

For example, let A be a ring. There exist a unique map $\mathbb{Z} \rightarrow A$, sending $1 \mapsto 1_A$. This map is called the *characteristic homomorphism* and allows us to think any ring as a \mathbb{Z} -algebra. Further, if k is a field and A a ring such that $k \hookrightarrow A$, then A is a k -algebra.

¹Remember that an homomorphism between a field k and a ring A is always injective.

0.11. Definition. An *homomorphism of A -algebras* between $A \xrightarrow{f} B$ and $A \xrightarrow{g} C$ is a ring homomorphism such that is A -linear. In other words, we have that $B \xrightarrow{\varphi} C$ is an homomorphism of A -algebras iff φ is a ring homomorphism and $g = \varphi \circ f$:

$$\begin{array}{ccc} B & \xrightarrow{\varphi} & C \\ \uparrow f & \nearrow g & \\ A & & \end{array}$$

For example, let $A = \mathbb{Z}$. Any ring homomorphism $B \xrightarrow{\varphi} C$ is a \mathbb{Z} -algebras homomorphism: the reason is the uniqueness of the characteristic map, that makes the diagram

$$\begin{array}{ccc} B & \xrightarrow{\varphi} & C \\ \uparrow & \nearrow & \\ \mathbb{Z} & & \end{array}$$

always commutative.

Now that we have defined maps between A -algebras, we can define the category of A -algebras: it will be denoted by \mathbf{Alg}_A .

1. Functoriality

Consider now a more specific case, useful for our purpose. Let $A = k$ be a field, fixed, and let B be the ring of polynomials over k in the variables x_1, \dots, x_n , i.e. $B = k[x_1, \dots, x_n]$. Let C be any k -algebra, e.g. a field extension K of the *base field* k (so we have $k \subset K$).

The set of k -algebras homomorphism from $k[x_1, \dots, x_n]$ to K , $\text{Hom}_k(k[x_1, \dots, x_n], K)$, is actually a k -algebra. It's easy to see, by the corollary of the proposition 0.8, that it is isomorphic to K^n .

Let's see this from a functorial point of view: let² $A \xrightarrow{f} B \in \mathbf{Alg}_A$.

We have the (covariant) Hom functor $G = \text{Hom}_A(A[x], -)$

$$\begin{array}{ccc} B & \xrightarrow{G} & G(B) = \text{Hom}_A(A[x], B) \\ \downarrow \varphi & & \downarrow \varphi \circ \\ B' & \xrightarrow{G} & G(B') = \text{Hom}_A(A[x], B') \end{array}$$

that acts on maps, as usual, by composition: keep in mind this functor for a while.

Fix an integer $n > 1$ and consider now the functor F defined as follows:

$$\begin{array}{ccc} A & \xrightarrow{F} & F(A) = A^n \\ \downarrow f & & \downarrow f^n \\ A' & \xrightarrow{F} & F(B') = (B')^n. \end{array}$$

²We will use this abuse of notation, saying that the map $A \xrightarrow{f} B$ is the A -algebra: in this way we will consider as one the map f and the ring B , when we see it as an A -algebra.

where A, A' are rings and where $f^n(a_1, \dots, a_n) = (f(a_1), \dots, f(a_n))$. We have the following lemma:

1.1. Lemma. *There is a natural isomorphism of functors between the functor F (defined as above) and the Hom functor $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}[x_1, \dots, x_n], -)$*

PROOF. The Hom functor of the lemma acts on maps exactly like the functor $-$ defined above $-\text{Hom}_A(A[x], -)$ (when we consider $A = \mathbb{Z}$ and we take more than one variable). We wish to define a natural transformation of functors and show that is actually an isomorphism. Let's begin by defining the transformation: for all $A \in \mathbf{Rng}$ (the category of the rings), define the map

$$A^n \xrightarrow{\tau_A} \text{Hom}_{\mathbb{Z}}(\mathbb{Z}[x_1, \dots, x_n], A)$$

that sends

$$P = (a_1, \dots, a_n) \mapsto v_P := (p(x) \mapsto p(a_1, \dots, a_n)) \in \text{Hom}_{\mathbb{Z}}(\mathbb{Z}[x_1, \dots, x_n], A).$$

The map v_P is the *evaluation map* of the *point* $P \in A^n$. τ_A is clearly injective, since if $v_P = v_Q$, then $a_i = v_P(x_i) = v_Q(x_i) = b_i$ (if $Q = (b_1, \dots, b_n)$) and so $P = Q$. It is also onto, since for $\psi \in \text{Hom}_{\mathbb{Z}}(\mathbb{Z}[x_1, \dots, x_n], A)$ we can define $P_\psi = (\psi(x_i))_{i=1, \dots, n} \in A^n$. To show that τ is a natural transformation (and hence a natural isomorphism, for what we have just seen), we simply need to prove that the following diagram

$$\begin{array}{ccc} A & A^n \xrightarrow{\tau_A} & \text{Hom}_{\mathbb{Z}}(\mathbb{Z}[x_1, \dots, x_n], A) \\ f \downarrow & f^n \downarrow & \downarrow \\ A' & (A')^n \xrightarrow{\tau_{A'}} & \text{Hom}_{\mathbb{Z}}(\mathbb{Z}[x_1, \dots, x_n], A') \end{array}$$

commutes. But this is an easy check. □

This simple lemma contains the point of view we wish to use in this course: with the following definition, we will introduce the first geometric object, seen in a completely new way.

1.2. Definition. We define the *affine space* $\mathbb{A}_{\mathbb{Z}}^n$ to be the functor $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}[x_1, \dots, x_n], -)$. Let k be a field. We can define in a similar way the *affine space over k* as a functor of k -algebras: $\mathbb{A}_k^n = \text{Hom}_k(k[x_1, \dots, x_n], -)$.

1.3. Remark. If K is a field extension of k (so we have $K \in \mathbf{Alg}_k$) we have that $\mathbb{A}_k^n(K) \cong K^n$ (and that the isomorphism is actually natural in K): it's a simple application of lemma 1.1.

We begin our investigation of the properties of the affine space from this example: consider the space $\mathbb{A}_k^n(k) = \text{Hom}_k(k[x_1, \dots, x_n], k)$ and take a "point" $\varphi \in \text{Hom}_k(k[x_1, \dots, x_n], k)$. So we have the following commutative diagram:

$$\begin{array}{ccc} k[x_1, \dots, x_n] & \xrightarrow{\varphi} & k \\ \uparrow \iota & \searrow id & \\ k & & \end{array}$$

The inclusion ι and the identity map id allow us to consider both k and $k[x_1, \dots, x_n]$ as k -algebras. So φ is such that $id = \varphi \circ \iota$ which means that φ must be onto. For this reason, $I = \text{Ker } \varphi$ is a maximal ideal in the ring $k[x_1, \dots, x_n]$. In order to describe explicitly the ideal I , we note that there exist elements $a_1, \dots, a_n \in k$ s.t.

$$\varphi(x_i) = a_i,$$

so that $\varphi = v_P$ where $P = (a_1, \dots, a_n) \in k^n$. For this reason we have that $I \supset J$, where J is the ideal generated by the monic polynomials $p_i(x_1, \dots, x_n) = x_i - a_i \in k[x_1, \dots, x_n]$ for $i = 1, \dots, n$. Moreover, since $k[x_1, \dots, x_n]/J \cong k$, J is a maximal ideal and we conclude that $I = \text{Ker } \varphi = (p_1, \dots, p_n)$.

Thanks to the last remark, we can define a one-to-one correspondence:

$$\begin{aligned} \mathbb{A}_k^n(k) = \text{Hom}_k(k[x_1, \dots, x_n], k) &\rightarrow \{\text{max. ideals } \mathfrak{m} \text{ of } k[x_1, \dots, x_n] \\ &\text{of the form } (x_1 - a_1, \dots, x_n - a_n)\} = M, \end{aligned}$$

which is also onto.

Question: does M coincide with the set of *all* maximal ideals of $k[x_1, \dots, x_n]$? In other words, if \mathfrak{m} is a maximal ideal of $k[x_1, \dots, x_n]$, is it possible to find elements a_1, \dots, a_n such that $\mathfrak{m} = (x_1 - a_1, \dots, x_n - a_n)$? See the following two examples:

1.4. Example. Let's k the field \mathbb{C} of complex numbers and $n = 1$. It's well known that $\mathbb{C}[x]$ is a PID: if \mathfrak{m} is a maximal ideal, there must exist an irreducible polynomial $f(x)$ such that $\mathfrak{m} = (f(x))$.

We also know that \mathbb{C} is algebraically closed, which is to say that every polynomial of degree greater than one must split in $\mathbb{C}[x]$ or that irreducible non-constant polynomials must have degree one. Hence $f(x)$ must be equal to $x - a$, for a suitable $a \in \mathbb{C}$. In this case we have a positive answer.

1.5. Example. Let's k the field \mathbb{R} of real numbers and again $n = 1$. It's easy to check that there are maximal ideals that are not in M : simply take $I = (x^2 + 1)$. I is maximal (since $x^2 + 1$ is irreducible on $\mathbb{R}[x]$) and does not belong to M .

Here there is another interesting question. Let \mathfrak{m} be a maximal ideal in $\mathbb{R}[x]$. Since \mathbb{R} is a PID, there is an irreducible polynomial $f(x)$ such that $\mathfrak{m} = (f(x))$. So we have the following commutative diagram:

$$\begin{array}{ccc} \mathbb{R}[x] & \twoheadrightarrow & \mathbb{R}[x]/\mathfrak{m} = K \\ \uparrow \iota & \nearrow & \\ \mathbb{R} & & \end{array}$$

In other words: if we take a maximal ideal \mathfrak{m} , how can we *extend* the affine space $\mathbb{A}_{\mathbb{R}}^n(\mathbb{R})$ in order to define a "point" that correspond to such ideal? Here we see that in the space

$$\mathbb{A}_{\mathbb{R}}^n(K) = \text{Hom}_{\mathbb{R}}(\mathbb{R}[x], \mathbb{R}[x]/\mathfrak{m})$$

the quotient map $\pi: \mathbb{R}[x] \rightarrow \mathbb{R}[x]/\mathfrak{m}$ is an \mathbb{R} -algebras homomorphism (so a point in $\mathbb{A}_{\mathbb{R}}^n(K)$) that satisfies $\text{Ker } \pi = \mathfrak{m}$.

This example will be clear later.

2. Algebraic sets: a new point of view

We usually define an algebraic set to be, roughly speaking, the “zero set” of a suitable family of polynomials. We will take again the functorial point of view.

Let k be a field as above. Consider $I \subset k[x_1, \dots, x_n]$ an ideal. Thanks to Hilbert’s basis theorem³, we have that $I = (f_1, \dots, f_r)$. Let K be a field extension of k (so that $K \in \mathbf{Alg}_k$). Consider a K -point:

$$P \in \mathbb{A}_k^n(K) = K^n \quad \text{that is equivalent to} \quad v_P: k[x_1, \dots, x_n] \rightarrow K$$

We have that $P \in V(I) = V((f_1, \dots, f_r)) = \{P \in \mathbb{A}_k^n(K) = K^n \text{ s. t. } f(P) = 0 \text{ for all } f \in I\}$ if and only if $v_P(f_i) = 0$ for $i = 1, \dots, r$. Let’s see this condition in terms of maps between polynomial rings:

2.1. Lemma. *We have that $v_P(f_i) = 0$ for $i = 1, \dots, r$ iff there exists a unique map $k[x_1, \dots, x_n]/I \rightarrow K$ such that the diagram*

$$\begin{array}{ccc} k[x_1, \dots, x_n] & \xrightarrow{v_P} & K \\ \downarrow & \nearrow & \\ R = k[x_1, \dots, x_n]/I & & \end{array}$$

commutes.

PROOF. Suppose first that such map exists. Then we have, for $i = 1, \dots, r$, $f_i \rightarrow 0_R \rightarrow 0$ (where we have applied first the canonical projection and after the map $R \rightarrow K$). From the hypothesis of commutativity of the diagram it follows that $v_P(f_i) = 0$. Suppose now that $v_P(f_i) = 0$ for $i = 1, \dots, r$. Then, for every class $g(x) + I$ in R we can define a map $g(x) + I \mapsto g(P)$: it’s well defined thanks to the hypothesis that $v_P(f_i) = 0$ for every i and obviously commutes with v_P . \square

2.2. Definition. We can define the *zero set of I* as a functor $V_k(I)(-): \mathbf{Alg}_k \rightarrow \mathbf{Set}$ as follows:

$$K \rightarrow V_k(I)(K) := \{P \in \mathbb{A}_k^n(K) = K^n \text{ s.t. } f_i(P) = 0 \text{ for } i = 1, \dots, r\} \subset \mathbb{A}_k^n(K).$$

Notice that, thanks to the previous lemma, we have the following commutative diagram:

$$(2.1) \quad \begin{array}{ccc} \mathbb{A}_k^n(K) & \xrightarrow{\simeq} & \text{Hom}_k(k[x_1, \dots, x_n], K) \\ \cup & & \uparrow \circ \pi \\ V_k(I)(K) & \xrightarrow{\simeq} & \text{Hom}_k(k[x_1, \dots, x_n]/I, K) \end{array}$$

where the map $\text{Hom}_k(k[x_1, \dots, x_n]/I, K) \rightarrow \text{Hom}_k(k[x_1, \dots, x_n], K)$ is defined by composition with the canonical projection $\pi: k[x_1, \dots, x_n] \rightarrow k[x_1, \dots, x_n]/I$.

³Recall Hilbert’s basis theorem: if R is a Noetherian ring, then also $R[x]$ is Noetherian

2.3. Remark. Summarize what we have seen so far: let k be a field and fix $n \in \mathbb{N}$. The functor $\mathbb{A}_k^n: \mathbf{Alg}_k \rightarrow \mathbf{Set}$ is representable by the k -algebra $k[X_1, \dots, X_n]$ (ring of polynomials) in the sense that for any k -algebra K , we have a bijection

$$\begin{aligned} \mathrm{Hom}_k(k[X_1, \dots, X_n], K) &\longrightarrow \mathbb{A}_k^n(K) = K^n \\ (\alpha: k[X_1, \dots, X_n] \rightarrow K) &\longmapsto (\alpha(X_1), \dots, \alpha(X_n)) \\ v_P &\longleftarrow \longmapsto P \end{aligned}$$

which is functorial (or, in other words, natural) in K (thanks to the substitution principle). Then we can define in a natural manner two sub-functors of \mathbb{A}_k^n , which are both representable:

- (1) Let now be $S \subseteq k[X_1, \dots, X_n]$. We can define the sub-functor $V(S) \subseteq \mathbb{A}_k^n$ on \mathbf{Alg}_k defined by:

$$V(S)(K) = \{P = (a_1, \dots, a_n) \in \mathbb{A}_k^n(K) \text{ such that for all } f \in S, v_P(f) = 0\}$$

Thank's to lemma 2.1, we have that it is representable by the k -algebra $k[X_1, \dots, X_n]/I$, where $I = I(S)$ is the ideal generated by S .

- (2) Let S be a multiplicative set in $k[X_1, \dots, X_n]$. Define the sub-functor $D(S) \subseteq \mathbb{A}_k^n$ on \mathbf{Alg}_k defined by:

$$D(S)(K) = \{P = (a_1, \dots, a_n) \in \mathbb{A}_k^n(K) \text{ such that for all } f \in S, v_P(f) \in K^\times\}$$

for any k -algebra K (notice that K is not necessarily a field!). Because of the universal property of the localization, we can show that $D(S)(-)$ is representable by the k -algebra $S^{-1}k[X_1, \dots, X_n]$. Indeed, for any $g: k[X_1, \dots, X_n] \rightarrow K$ homomorphism of k -algebras such that $g(S) \subset K^\times$, it exists a unique homomorphism $\bar{g}: S^{-1}k[X_1, \dots, X_n] \rightarrow K$ that extends g . Thus we have a bijection

$$\mathrm{Hom}_k(S^{-1}k[X_1, \dots, X_n], K) \longrightarrow D(S)(K) \subset \mathbb{A}_k^n(K)$$

2.4. Example. Let $f \in k[X_1, \dots, X_n]$, $f \neq 0$, and consider the multiplicative set $S = \{f^n \mid n \in \mathbb{N}\}$. Then, for any k -algebra K which is a field, the following relation holds:

$$\mathbb{A}_k^n(K) = V(S)(K) \sqcup D(S)(K)$$

where \sqcup means “disjoint union”. To see this, simply notice that

$$V(S)(K) = \{P \in \mathbb{A}_k^n(K) \text{ such that } v_P(f) = 0\}$$

while we have

$$D(S)(K) = \{P \in \mathbb{A}_k^n(K) \text{ such that } v_P(f) \in K^\times = K \setminus \{0\}\}$$

that is $D(S)(K)$ is the set of $P \in \mathbb{A}_k^n(K)$ such that $v_P(f) \neq 0$, hence the conclusion follows.

More generally, assume $f_1, \dots, f_n \in k[X_1, \dots, X_n]$, $f_i \neq 0$, and define the multiplicative set $S_i = \{f_i^n \mid n \in \mathbb{N}\}$. Let S be the multiplicative set defined by f_1, \dots, f_n . In this case, for any k -algebra K which is a field, we have the decomposition

$$\mathbb{A}_k^n(K) = V(S)(K) \sqcup \bigcup_{i=1}^n D(S_i)(K)$$

where $\bigcup_{i=1}^n D(S_i)(K)$ is the set of P such that it exists at least one polynomial f_i such that $v_P(f_i) \neq 0$.

3. Finiteness

3.1. Definition. Let $f: A \rightarrow B$ an \mathbf{Alg}_A .

- (1) we say that f is *finite* (or that B is a *finite* A -algebra) if B is a finitely generated as an A -module;
- (2) we say that f is *of finite type* (or that B is a *finitely generated* A -algebra) if exist elements $x_1, \dots, x_n \in B$ such that every element of B is a polynomial in these elements, that is $A[x_1, \dots, x_n] \rightarrow B$ onto.

3.2. Example. $k[x]$ is not finite as k -algebra: $1, x, x^2, \dots$ is a basis.

$\pi: A \rightarrow A/I = B$ is finite as A -algebra: is generated by $\bar{1}$ as A -module.

From the last definition we have that A -algebras of finite type are quotient of polynomial rings in the variables x_1, \dots, x_n by some ideal (which is finitely generated if A is Noetherian).

3.3. Example. Let k be a field. Consider the ring of polynomials in one variable $k[t]$ and the two polynomials t^2, t^3 . By the substitution principle, we have a ring homomorphism $k[x, y] \rightarrow k[t]$ such that $f(x, y) \mapsto f(t^2, t^3)$. The kernel of this map is the ideal $I = (x^3 - y^2)$ and the image is $k[t^2, t^3]$. By definition, we have then that $k[t^2, t^3]$ is a k -algebra of finite type, since every element can be written as a polynomial in t^2, t^3 (equivalently, we have that $k[t^2, t^3] \simeq k[x, y]/I$). We also have that $k[t]$ is a finite $k[t^2, t^3]$ module: in fact, given $f(t) \in k[t]$, $f(t) = a_0 + a_1t + \dots + a_nt^n = a_1t + 1 \cdot g(t)$ with $g(t) \in k[t^2, t^3]$.

4. Field extensions

We begin with a technical result ([2], prop. 7.8)

4.1. Proposition. *Let $A \subseteq B \subseteq C$ be rings. Suppose that A is a Noetherian ring, that C is a finitely generated A -algebra and a finitely generate B -module. Then B is a finite generated A -algebra.*

PROOF. Let x_1, \dots, x_m be generators of C as A -algebra, and let y_1, \dots, y_n generate C as a B -module, i.e. $C = A[x_1, \dots, x_m]$ and $C = By_1 + \dots + By_n$. Then there exist expression of the form

$$(4.1) \quad x_i = \sum_j b_{ij}y_j \quad \text{with } b_{ij} \in B \text{ for } i=1, \dots, m$$

$$(4.2) \quad y_i y_j = \sum_k b_{ijk}y_k \quad \text{with } b_{ijk} \in B$$

Let B_0 denote the algebra generated over A by the elements b_{ij} and b_{ijk} . A is a Noetherian ring, hence B_0 is Noetherian, since B_0 is a quotient of polynomials ring (apply Hilbert's basis theorem). Then we have $A \subset B_0 \subset B$, since b_{ij} and $b_{ijk} \in B$. Now, any element of C is a polynomial in the variables x_i with coefficients in A . Thus, if $f(x_1, \dots, x_m) \in C$, we can write using (4.1) $f(\sum_j b_{1j}y_j, \dots, \sum_j b_{mj}y_j)$. Making a repeated use of (4.2), we can write f as a *linear* combination of the y_i with coefficients in B_0 . Hence we have proved

that C is a finitely generated B_0 -module. Since B_0 is Noetherian and B is a submodule of C , we have that also B is a finitely generated B_0 module, so that $B = B_0b_1 + \dots + B_0b_l$. In conclusion, $B_0 = A[b_{ij}, b_{ijk}]$ implies $B = A[b_{ij}, b_{ijk}, b_1, \dots, b_l]$. \square

4.2. Remark. The fact that A is a Noetherian ring is crucial. To prove proposition 4.1 we have used, without mentioning it, the following lemma:

4.3. Lemma. M is a Noetherian A -module iff every submodule of M is finitely generated.

A proof can be found in [2], prop. 6.2.

Suppose that $k \subset K$ a field extension. If $x_1, \dots, x_n \in K$, we can consider the intersection of all the fields containing x_1, \dots, x_n . This object is again a field and coincides with the field $k(x_1, \dots, x_n) \simeq \text{Frac}(k[x_1, \dots, x_n])$. It is obtained by taking every polynomial $f(x_1, \dots, x_n)$ as well as every fraction f/g where both f and g are polynomials in the variables x_1, \dots, x_n and $g \neq 0$.

4.4. Remark. The isomorphism between $k(x_1, \dots, x_n)$ and $\text{Frac}(k[x_1, \dots, x_n])$ is unique, since we have the following diagram

$$\begin{array}{ccc} k[x_1, \dots, x_n] & \longrightarrow & \text{Frac}(k[x_1, \dots, x_n]) \\ & \searrow & \downarrow \exists! h \\ & & k(x_1, \dots, x_n). \end{array}$$

The map $k[x_1, \dots, x_n] \rightarrow k(x_1, \dots, x_n)$ is such that every element different from zero becomes a unit in $k(x_1, \dots, x_n)$. Hence, by the universal property of the field of fractions, the map h is the unique homomorphism of rings such that the previous diagram commutes. h is clearly injective (it's homomorphism of fields) with inverse the map $f/g \rightarrow \overline{f/g}$ (which denotes the class of (f, g) in $\text{Frac}(k[x_1, \dots, x_n])$), hence it's an isomorphism. By the previous argument we can identify $\text{Frac}(k[x_1, \dots, x_n])$ with the field $k(x_1, \dots, x_n)$.

4.5. Definition. Let $a \in K \supset k$. We say that a is *algebraic over k* if there exists a non zero polynomial $p(x) \in k[x]$ such that $p(a) = 0$. Otherwise we call it *transcendental*.

Note that, in this case we have a surjective homomorphism $v_a: k[x] \rightarrow k[a] \subset K$, that is called evaluation map. We have $\text{Ker}(v_a) = (f(x)) = I$ with $f(x)$ irreducible polynomial (since the quotient ring $k[x]/I \simeq k[a]$, that is a field). f is the polynomial of least degree satisfied by a and is called the *minimal polynomial of a over k* . Thus, a is algebraic if $k[a] = k(a)$. Similarly, if x_1, \dots, x_n are algebraic elements over k , we have that $k[x_1, \dots, x_n] = k(x_1, \dots, x_n)$.

If a is not algebraic over k , the evaluation map has trivial kernel, hence $k[x] \hookrightarrow k[a]$ and $k[a]$ is not a field.

4.6. Definition. We say that a set of elements $x_1, \dots, x_n \in K$ of a field extension $k \subset K$ is *algebraic dependent* (and we say that the elements x_1, \dots, x_n are *algebraically dependent*) if there exists a non zero polynomial $f \in k[X_1, \dots, X_n]$ such that $f(x_1, \dots, x_n) = 0$.

We say that $x_1, \dots, x_n \in K$ are *algebraically independent* if there is no such polynomial.

4.7. Example. Let $x_1 = \sqrt[4]{\pi}$ and $x_2 = \frac{\sqrt{2\pi}}{2}$. Then x_1, x_2 are algebraically dependent over $\mathbb{Q}[\sqrt{2}]$: in fact, $f(x, y) = x^2 - \sqrt{2}y$ is such that $f(x_1, x_2) = 0$.

If $x_1, \dots, x_n \in K$ are algebraically independent, again we have the injective homomorphism given by the evaluation map $k[X_1, \dots, X_n] \hookrightarrow K$, that is $f(X_1, \dots, X_n) \mapsto f(x_1, \dots, x_n)$. The field $k(x_1, \dots, x_n)$ is isomorphic to $k(X_1, \dots, X_n)$ and the field extension $k(x_1, \dots, x_n)$ over k is called *purely transcendental*.

4.8. Definition. A *transcendental basis* for a field extension $k \subset K$ is a set of algebraically independent elements x_1, \dots, x_n such that $K|k(x_1, \dots, x_n)$ is an algebraic extension.

We will prove that two transcendental basis for a field extension K over k have the same number of elements. Thus is well defined the *transcendental degree of K over k* as the cardinality of a transcendental basis of $k \subset K$. We will denote this number with $\text{Trdeg}_k(K)$.

It's clear that we cannot avoid considering the case of infinite (not necessarily countable) algebraically independent elements. So we need to review the above definitions in a slightly different manner. Let K over k be, as usual, a field extension and let $S \subseteq K$. We introduce a set of functions from S to \mathbb{N} in the following way:

$$S^{\mathbb{N}} := \{v: S \rightarrow \mathbb{N} \text{ such that } v^{-1}(\mathbb{N} \setminus \{0\}) \text{ is finite set}\}.$$

For all $v \in S^{\mathbb{N}}$, we write $M_{(v)}(S) = \prod_{s \in S} s^{v(s)}$ for the the generic monomial in the elements of S .

4.9. Definition. The set S is called *algebraically independent* over k if, for any $I \subset S^{\mathbb{N}}$ such that I is finite, we have the equation

$$\sum_{v \in I} a_v M_{(v)}(S) = 0$$

for $a_v \in k$ and for all $v \in I$ if and only if $a_v = 0$ for all $v \in I$.

Let S be a finite subset of K , $S = \{\alpha_1, \dots, \alpha_n\}$. Then $S^{\mathbb{N}}$ can be identified with the set $\{\alpha_1^{n_1} \cdots \alpha_m^{n_m} \mid n_1, \dots, n_m \in \mathbb{N}\}$. This, in turn, is equivalent to the set \mathbb{N}^m . So we can restate the definition of algebraic independence for the set S as follows:

$$(4.3) \quad \text{for any } I \subset \mathbb{N}^m \text{ finite, } \sum_{\underline{n}=(n_1, \dots, n_m) \in I} a_{\underline{n}} \alpha_1^{n_1} \cdots \alpha_m^{n_m} = 0 \Leftrightarrow a_{\underline{n}} = 0 \text{ for all } \underline{n} \in I$$

Actually, this statement is equivalent to the condition that the evaluation map

$$\begin{array}{ccc} v_S: k[X_1, \dots, X_n] & \longrightarrow & K \\ X_i & \longmapsto & \alpha_i \end{array}$$

(given, as usual, by the substitution principle) is injective.

Indeed, $\{X_1^{n_1} \cdots X_m^{n_m} \mid (n_1, \dots, n_m) \in \mathbb{N}^m\}$ is a basis for $k[X_1, \dots, X_m]$ as k -vector space. So v_S is injective iff it has trivial kernel, that is

$$\text{for any } I \subset \mathbb{N}^m \text{ finite, } v_S\left(\sum_{\underline{n}=(n_1, \dots, n_m) \in I} a_{\underline{n}} X_1^{n_1} \cdots X_m^{n_m}\right) = 0 \Leftrightarrow a_{\underline{n}} = 0 \text{ for all } \underline{n} \in I$$

and, by definition of v_S , this is equivalent to the statement 4.3. Hence we have proved that, in the finite case, the two definitions 4.6 and 4.9 are equivalent.

Notation: Let $k \subset K$ be a field extension. We denote with \mathcal{S} the set

$$\mathcal{S} = \{S \subset K \mid S \text{ is alg. independent over } k\}$$

Then \mathcal{S} is ordered by inclusion (i.e. $S_1, S_2 \in \mathcal{S}$, $S_1 \leq S_2 \Leftrightarrow S_1 \subseteq S_2$).

4.10. Definition. An element $S \in \mathcal{S}$ is called a *transcendental basis* of K over k if S is maximal in \mathcal{S} with respect to \leq . We call $\text{card } S = \#S$ the *transcendental degree* of K .

4.11. Lemma. $S \in \mathcal{S}$ is a transcendental basis for K over k iff $k(S)$, the field generated⁴ by S over k , is such that the field extension K over $k(S)$ is algebraic.

PROOF.

(\Leftarrow) Take $\alpha \in K$, $\alpha \notin k(S)$, then $S \subsetneq S \cup \{\alpha\}$. Hence, $S \cup \{\alpha\}$ is not alg. independent, that is it exists $I \subset (S \cup \{\alpha\})^{\mathbb{N}}$ finite and there exist $a_v \in k$, not all equal to zero, for any $v \in I$ such that

$$(4.4) \quad \sum_{v \in I} a_v M_{(v)}(S \cup \{\alpha\}) = 0.$$

Since S is algebraically independent, there exists $v \in I$ such that $v(\alpha) \neq 0$. Otherwise, notice that we can write the generic monomial in elements of $S \cup \{\alpha\}$ in the following way:

$$M_{(v)}(S \cup \{\alpha\}) = \prod_{s \in S} s^{v(s)} \cdot \alpha^{v(\alpha)} = M_{(v)}(S)$$

if $v(\alpha) = 0$ for all $v \in I$. Hence we would have found a non-trivial linear combination of monomials in elements of S which is zero, contradicting the algebraic independence of S .

By collecting the powers of α , the equation (4.5) can be written as follows:

$$b_n \alpha^n + b_{n-1} \alpha^{n-1} + \dots + b_0$$

with $b_j \in k(S)$. Thus, since α must appear at positive power in (4.5), we have that α satisfies the non zero polynomial $f(X) = b_n X^n + b_{n-1} X^{n-1} + \dots + b_0 \in K(S)[X]$. Hence α is algebraic over $k(S)$.

(\Rightarrow) Let $S \subsetneq T$ with $T \in \mathcal{S}$: we need to prove that $T = S$. Suppose, by contradiction, that exists $\alpha \in T \setminus S$. Thus α is algebraic over $k(S)$, i.e. there exists $b_0, \dots, b_n \in k(S)$, not all zero, such that $b_n \alpha^n + b_{n-1} \alpha^{n-1} + \dots + b_0 = 0$. But $k(S) = \text{Frac}(k[S])$, hence we can write each b_j as a fraction $\frac{f_j}{g_j}$ with $f_j, g_j \in k[S]$.

By multiplying all denominators, we obtain the following relation:

$$\prod_{i=0}^{n-1} g_i (b_n \alpha^n + b_{n-1} \alpha^{n-1} + \dots + b_0) = \sum_{j=0}^n \prod_{i=0}^{n-1} g_i b_j \alpha^j = 0$$

in $k[S]$. Thus we have found a non-trivial linear combination of elements in $S \cup \{\alpha\}$ which is equal to zero, which contradicts the assumption that $S \cup \{\alpha\} \subseteq T \in \mathcal{S}$ is algebraically independent. □

⁴ $k(S) = \bigcap_{k \subseteq L \subseteq K} L$ with L field extension that contains S .

4.12. Remark. Notice that in the proof we used the fact that the field $k(S)$ is equal to the field of fractions of the k -algebra $k[S]$. Indeed, if $S = \{\alpha_1, \dots, \alpha_m\} \subset K$ is an algebraic independent *finite* set, we have as usual the evaluation map $v_S: k[x_1, \dots, x_m] \rightarrow K$ such that $x_i \mapsto \alpha_i$. The map is injective, thus the image of $k[x_1, \dots, x_m] \setminus \{0\}$ is contained in K^\times . By the universal property of the field of fractions, v_S extends to an injective map $\text{Frac}(k[x_1, \dots, x_m]) \hookrightarrow K$ and the image is exactly $k(S)$. In the general case, $k[S]$ is the k -algebra generated by S and it is a domain. Then, $\text{Frac}(k[S]) \subset K$ is the smallest field containing S and, by definition, it is equal to $\{\frac{f}{g} \mid f, g \in k[S], g \neq 0\}$.

4.13. Theorem. *Let $\{x_1, \dots, x_n\} \subset K$ be a transcendental basis of K over k . Let $\{w_1, \dots, w_s\}$ be a set of algebraically independent elements. Then $s \leq n$.*

PROOF. We will prove that, if $s \geq n$ then $s = n$. We use induction on r to prove that, after renumbering the set x_1, \dots, x_n , the field K is algebraic over $k(w_1, \dots, w_r, x_{r+1}, \dots, x_n)$. Let $r = 1$. The element w_1 is algebraic over the field $k(x_1, \dots, x_n) \subseteq K$ by the previous lemma. Hence, there exists a monic polynomial $f(z) = z^m + b_{m-1}z^{m-1} + \dots + b_0$ such that $f(w_1) = 0$. The polynomial $f(z)$ belongs to $k(x_1, \dots, x_n)[z]$ but, by multiplying the denominators, we can assume (as above) that there exist $g_0, \dots, g_m \in k[x_1, \dots, x_n]$ such that $g_m w_1^m + g_{m-1} w_1^{m-1} + \dots + g_0 = 0$.

Not all the g_i can be constants (i.e. $g_i \in k$), since, by assumption, w_1 is algebraic independent over k . Hence, at least one of the x_i , say x_1 , appears in one of the polynomials. So, by isolating x_1 , we can write a relation satisfied by x_1 that is a linear combination of w_1, x_2, \dots, x_n and this implies x_1 is algebraic over the field $k(w_1, x_2, \dots, x_n)$. Now we make the inductive step: assume that K is algebraic over $k(w_1, \dots, w_r, x_{r+1}, \dots, x_n)$. Then, in particular, w_{r+1} is algebraic over $k(w_1, \dots, w_r, x_{r+1}, \dots, x_n)$, that is there exist g_0, \dots, g_m in $k[w_1, \dots, w_r, x_{r+1}, \dots, x_n]$ such that

$$(4.5) \quad g_m w_{r+1}^m + g_{m-1} w_{r+1}^{m-1} + \dots + g_0 = 0.$$

As above, not all the $g_i \in k[w_1, \dots, w_r]$, because the elements w_1, \dots, w_{r+1} are algebraically independent. Hence, at least one of the variables x_j , say x_{r+1} , appears in one of the polynomials g_i .

Thus we get from (4.5) that x_{r+1} is algebraic over $k(w_1, \dots, w_r, w_{r+1}, x_{r+2}, \dots, x_n)$ and we have proved the induction claim. Now we have that we can substitute each x_i , $i = 1, \dots, n$, with a suitable w_j , hence K is algebraic over $k(w_1, \dots, w_n)$. If we assume that $s > n$, we have that w_{n+1} is algebraic over $k(w_1, \dots, w_n)$, contradicting the fact that the set $\{w_1, \dots, w_s\}$ is algebraically independent over k . \square

4.14. Corollary. *If K admits a finite transcendental basis $\{x_1, \dots, x_n\}$, then any other transcendental basis has cardinality n .*

Then, at least in the finite case, the transcendental degree is well-defined (does not depend on the choice of the basis). Notice that this is true even in the infinite case, but we will not prove this statement.

4.15. Theorem. *Let $k \subset K$ be a field extension. Then there exists a transcendental basis for K over k .*

PROOF. Let \mathcal{S} be as above. If $\mathcal{S} = \emptyset$ then for all $\alpha \in K$ the set $\{\alpha\}$ is not algebraically independent over k , which is to say that the field extension K over k is algebraic. In this

case we have $\text{Trdeg}_k(K) = 0$. Suppose now $\mathcal{S} \neq \emptyset$. In order to apply Zorn's lemma to show the existence of a maximal element in \mathcal{S} , we need to show that if $S_1 \subseteq \dots \subseteq S_n \subseteq \dots$ is a chain of elements in \mathcal{S} , then $S = \bigcup_{i \in I} S_i$ belongs to \mathcal{S} (easy check, prove this by contradiction). S is clearly a maximal element of the chain and this concludes the proof. \square

4.16. Remark. As in the case of finite dimensional vector spaces, we can always complete a set of independent elements to a basis. More precisely, if $T \subseteq K$ is alg. independent over k , we can find a set $S \supseteq T$ such that S is a transcendental basis of K over k . The proof is the same of the above theorem: simply substitute the set \mathcal{S} with the set $\mathcal{S}_T = \{S \in \mathcal{S} \mid T \subseteq S\}$ and note that $\mathcal{S}_T \neq \emptyset$ since at least $T \in \mathcal{S}_T$.

4.17. Theorem. *Let $S \subseteq K$ be a set such that K is algebraic over $k(S)$. Then there exists $T \subseteq S$ which is a transcendental basis for K over k .*

PROOF. Let $\mathcal{D} = \{T \subseteq S \mid T \text{ is algebraically independent over } k\}$. If \mathcal{D} is empty, any α in S is algebraic over k , hence $k(S)$ is algebraic over k and so K is algebraic over k . In this case we can set $T = \emptyset$. If $\mathcal{D} \neq \emptyset$, apply Zorn's lemma: thus we have a set $T \in \mathcal{D}$ which is maximal. Hence, for all $\alpha \in S \setminus T$, $T \cup \{\alpha\} \notin \mathcal{D}$. Since T is algebraically independent, it must be α algebraic over $k(T)$. Hence, we have $k(T) \subseteq k(S) \subseteq K$ and each extension is algebraic. Thus, in particular, K must be algebraic over $k(T)$ and then, by lemma 4.11, T is a transcendental basis. \square

CHAPTER 3

Hilbert's Nullstellensatz and consequences

1. Hilbert's theorem

We can prove the following important lemma:

1.1. Lemma (Zariski). *Let K over k be a field extension. Assume that $K = k[x_1, \dots, x_n]$ is a finitely generated k -algebra. Then K is a finitely generated k -module (i.e. the extension K over k is algebraic).*

PROOF. Note that the case $n = 1$ is well-known from elementary field theory. In fact, we have $K = k[x_1] = k[X]/(f(X))$ with $f(X)$ a monic, irreducible polynomial (the minimal polynomial of x_1 over k). Let n be the degree of f , then, for any $g(X) \in k[X]$ we have $g(X) = f(X)q(X) + r(X)$ for suitable polynomials $q(X)$ and $r(X)$ such that $\deg(r) < n$ or $r = 0$. From the equation $f(x_1) = 0$, we obtain that $\overline{g(X)} = \overline{r(X)}$ in the quotient, that is $1, x_1, \dots, x_1^{n-1}$ is a basis for K as a k -vector space.

Suppose now $n > 1$ and apply induction: we can write the following chain of field inclusions:

$$k \subset k(x_1) \subset K$$

where $K = (k(x_1))[x_2, \dots, x_n]$ is a finitely generated $k(x_1)$ -algebra, hence, by the induction hypothesis, it's a finitely generated $k(x_1)$ -module. By assumption we also have that K is a finitely generated k -algebra. We can then apply proposition 4.1 and obtain that $k(x_1)$ is a finitely generated k -algebra. In order to conclude the proof we need to prove the following

Claim. x_1 is algebraic over k .

PROOF. Suppose x_1 is not algebraic and look for a contradiction: in that case we would have $k(x_1) \simeq k(Y)$, the field of fractions of the polynomial ring $k[Y]$. By the previous point of the proof, we have then that $k(Y)$ is a finitely generated k -algebra, so let $f_1/g_1, \dots, f_r/g_r$ be a set of generators with $f_i, g_i \in k[Y]$ and we can assume that g_i are irreducible. Hence we have $k(Y) = k[f_1/g_1, \dots, f_r/g_r]$ contains the element

$$h^{-1} = \frac{1}{g_1 \cdots g_r + 1}$$

that is $h^{-1} = \sum_{i=1}^r a_i \frac{f_i}{g_i} = \frac{p}{g_1 \cdots g_r}$. But the polynomial h is prime to each of the g_i and hence we obtained a contradiction. \square

This completes the proof \square

As a corollary of the previous theorem, we obtain the so-called "weak" version of Hilbert's Nullstellensatz.

1.2. Corollary. *Let k be a field, A a finitely generated k -algebra. Let \mathfrak{m} be a maximal ideal of A . Then the residue field A/\mathfrak{m} is a finite algebraic extension of k . In particular, if k is algebraically closed, $A/\mathfrak{m} \simeq k$.*

PROOF. Let $A = k[X_1, \dots, X_n]/I$ and $\mathfrak{m} \subset A$. Then the residue field A/\mathfrak{m} is an extension of the field k and, being the quotient of a finitely generated k -algebra, is again finitely generated. By Zariski's lemma we obtain $A/\mathfrak{m}|k$ is algebraic. \square

Let k be again a field and let A be a k -algebra. Since the beginning of this course, we have been interested in the study of "points" in affine spaces. But, in the previous pages, we saw that it is possible to generalize the idea of "a point in a space", coming from the geometric intuition, to the that of a map from a k -algebra A .

Hence, we substituted an n -uple $P = (p_1, \dots, p_n)$ in some finite-dimensional vector space K^n , for K field extension of k , with the evaluation map $v_P: k[X_1, \dots, X_n] \rightarrow K$, thanks to the bijection (natural in K) between $\text{Hom}_k(k[X_1, \dots, X_n], K)$ and $\mathbb{A}_k^n(K)$.

Now, we should be prepared to another big jump. The "points" will be the prime ideals of a ring A (maybe we will still work with k -algebras, but it's not necessary) and then we need to define new kind of "maps" on the set $\text{Spec}(A)$. Before doing this, let's see some consequences of corollary 1.2 in the case $k = \bar{k}$, an algebraically close field.

First of all, we have can add a term in the chain of isomorphisms that we built:

$$(1.1) \quad k^n = \mathbb{A}_k^n(k) \xrightarrow{\simeq} \text{Hom}_k(k[X_1, \dots, X_n], k) \simeq \text{Max}(k[X_1, \dots, X_n]).$$

The new term is $\text{Max}(k[X_1, \dots, X_n])$, the set of maximal ideals of the polynomial ring $k[X_1, \dots, X_n]$. The last bijection follows from 1.2 and from the fact that k is algebraically closed: in fact, we have that any maximal ideal \mathfrak{m} of $k[X_1, \dots, X_n] = B$, defines a homomorphism (that is the projection on the quotient) $B \twoheadrightarrow B/\mathfrak{m}$. The field B/\mathfrak{m} is, by the previous corollary, an algebraic extension of the base field k . Hence, being k algebraically closed, it must be $k = B/\mathfrak{m}$. Thus the map $B \twoheadrightarrow B/\mathfrak{m}$ belongs to $\text{Hom}_k(k[X_1, \dots, X_n], k)$. On the other hand, for any homomorphism $\varphi: k[X_1, \dots, X_n] \rightarrow k$, we have that $\text{Ker}(\varphi)$ is a maximal ideal of the polynomial ring (since φ is onto, being a morphism of k -algebras into k).

Thanks to this new correspondence, we can build another bijection with the vanishing set $V_k(I)(k)$ (remember diagram 2.1):

$$(1.2) \quad \begin{array}{ccccc} \mathbb{A}_k^n(k) & \xrightarrow{\simeq} & \text{Hom}_k(k[X_1, \dots, X_n], k) & \xrightarrow{\simeq} & \text{Max}(k[X_1, \dots, X_n]) \\ \cup & & \uparrow \circ \pi & & \\ V_k(I)(k) & \xrightarrow{\simeq} & \text{Hom}_k(k[X_1, \dots, X_n]/I, k) & \xrightarrow{\simeq} & \text{Max}(k[X_1, \dots, X_n]/I) \end{array}$$

Remember that, thanks to the so-called correspondence theorem, there is a bijection between the set $\text{Max}(k[X_1, \dots, X_n]/I)$ and the set of maximal ideals of $k[X_1, \dots, X_n]$ that contain I . Given a point $P \in \mathbb{A}_k^n(k)$, $P = (x_1, \dots, x_n) \in k^n$, we have the following bijections:

$$\begin{aligned} P &\mapsto v_P \\ v_P &\mapsto \text{Ker}(v_P) \in \text{Max}(k[X_1, \dots, X_n]). \end{aligned}$$

As usual, v_P is the evaluation map of the point P . It is clearly onto, hence $\text{Ker}(v_P)$ is maximal and the map is well defined. Actually, for $A = k[X_1, \dots, X_n]/I$, we have:

$$\begin{array}{ccc} \text{Hom}_k(A, k) & \xrightarrow{\cong} & \text{Max}(A) \\ \varphi & \longmapsto & \text{Ker}(\varphi) \\ (A \rightarrow A/\mathfrak{m}) & \longleftarrow & \mathfrak{m} \end{array}$$

Being k algebraically closed, we have $A/\mathfrak{m} = k$ (we can apply 1.2 because A is a finitely generated k -algebra).

Notice that this map is also functorial, in the sense that $\text{Max}(-)$ is a functor $\mathbf{Alg}_k \rightarrow \mathbf{Set}$.

1.3. Remark. This is not true in general: if we consider the category of rings, we have the (contravariant) functor $\text{Spec}(-): \mathbf{Rng} \rightarrow \mathbf{Set}$

$$\begin{array}{ccccc} A & \longrightarrow & \text{Spec}(A) & f^{-1}(\mathfrak{p}) & \\ \downarrow f & & \uparrow & \uparrow & \\ B & \longrightarrow & \text{Spec}(B) & \mathfrak{p} & \end{array}$$

If $\mathfrak{p} \in \text{Spec}(B)$, then $f^{-1}(\mathfrak{p})$ is a prime ideal in A (since f is a ring homomorphism). So we could be tempted to do the same thing with maximal ideals, defining a map $\text{Max}(B) \rightarrow \text{Max}(A)$. Unfortunately, this attempt fails: if \mathfrak{m} is maximal in B , we can't deduce that $f^{-1}(\mathfrak{m})$ is maximal in A . However, this can be done in our case.

PROOF. Let $A, B \in \mathbf{Alg}_k$ and let $f: A \rightarrow B$ a homomorphism of k -algebras. Then we have:

$$\begin{array}{ccccccc} A & \longrightarrow & \text{Hom}_k(A, k) & \xrightarrow{\cong} & \text{Max}(A) & f^{-1}(\mathfrak{m}) & \\ \downarrow f & & \uparrow \circ f & & \uparrow & \uparrow & \\ B & \longrightarrow & \text{Hom}_k(B, k) & \xrightarrow{\cong} & \text{Max}(B) & \mathfrak{m} & \end{array}$$

We have to show that $f^{-1}(\mathfrak{m})$ is maximal in A . To do this, consider the following diagram:

$$\begin{array}{ccccc} \mathfrak{m} & \subset & B & \twoheadrightarrow & B/\mathfrak{m} = k \\ \downarrow & & \uparrow f & & \uparrow \alpha \\ f^{-1}(\mathfrak{m}) & \subset & A & \twoheadrightarrow & A/(f^{-1}(\mathfrak{m})) \\ & & \uparrow & \nearrow & \\ & & k & & \end{array}$$

Here we have that $B/\mathfrak{m} = k$, being k algebraically closed. Notice that the map α is surjective, since the diagram

$$\begin{array}{ccc} A/(f^{-1}(\mathfrak{m})) & \xrightarrow{\alpha} & k \\ \uparrow & \nearrow & \\ k & & \end{array}$$

is commutative (remember that $A/(f^{-1}(\mathfrak{m}))$ is a k -algebra).

In order to prove the statement, we need to show that α is also injective. In fact, we have that

$$\begin{array}{ccc} B & \longrightarrow & B/\mathfrak{m} \\ \uparrow f & & \uparrow \alpha \\ A & \longrightarrow & A/(f^{-1}(\mathfrak{m})) \\ \uparrow & \nearrow 0 & \uparrow \\ \text{Ker}(f) & \longrightarrow & \text{Ker}(\alpha) = \text{Ker}(f)/f^{-1}(\mathfrak{m}). \end{array}$$

Since $0 \in \mathfrak{m}$, we have that $\text{Ker}(f) \subset f^{-1}(\mathfrak{m})$, hence $\text{Ker}(\alpha) = 0$. Thus α is injective and the $f^{-1}(\mathfrak{m})$ is maximal. \square

Thanks to the previous remark, we can introduce a new point of view. We can view A as an algebra of functions on the set $X := \text{Max}(A)$. Here, a “point” $x \in X$ is a maximal ideal $\mathfrak{m}_x \subset A$. Each element of A defines a function from X to the base field k , so that $f \in A$ yields a map $f: X \rightarrow k$ that is defined by $x \mapsto f(x) := \bar{f}$ in the quotient field A/\mathfrak{m}_x , which is again equal to k , by Zariski’s lemma, if k is algebraically closed.

Let $A = k[X_1, \dots, X_n]/I$ for some ideal I and let $f \in k[X_1, \dots, X_n]$. Denote again with f the class of f in the quotient¹. Now we have that $f(x) = 0$ for all $x \in X$ iff $\bar{f} = 0$ in A/\mathfrak{m}_x for all $\mathfrak{m}_x \in \text{Max}(A)$. Hence

$$f \in \bigcap_{\mathfrak{m} \in \text{Max}(A)} \mathfrak{m}$$

and every $\mathfrak{m} \in \text{Max}(A)$ corresponds to an ideal of $k[X_1, \dots, X_n]$ that contains I . Hence we can build an ideal of $k[X_1, \dots, X_n]$ in the following way:

$$\tilde{I} = \{f \in k[X_1, \dots, X_n] \mid f(x) = 0 \text{ for all } x \in X, \text{ thinking } f \in A\}$$

and we have $\tilde{I} \supset I$ for what we have just seen. So a question arise in a natural way: when does the equality hold? We have considered all the functions $f \in A$ vanishing on the set $\text{Max}(A)$. Is it possible to reconstruct I in this way, in the sense that we can find an ideal I of the polynomial ring $k[X_1, \dots, X_n]$ such that $A \cong k[X_1, \dots, X_n]/I$?

We have built the ideal of functions vanishing on X . But the well-known isomorphism of the set of maximal ideals of the algebra A with the zero set $V_k(I)(k)$ (that we have seen above), allows us to restate the question in an equivalent form.

First, denote with $Z(I)$ the “zero set” of the ideal I , in the sense that $Z(I) = V_k(I)(k)$. Now the question is: can I be recovered from $Z(I)$ by considering all the polynomials $f \in k[X_1, \dots, X_n]$ such that $f(P) = 0$ for all P in $Z(I)$?

The answer of all those questions will be given by the following theorem:

1.4. Theorem (Hilbert’s Nullstellensatz). *Let $k = \bar{k}$ be an algebraically closed field. Let Σ be a set of polynomials, $\Sigma \subset k[X_1, \dots, X_n]$. Then we have:*

- (1) *If $Z(\Sigma) = \emptyset$, then the ideal generated by Σ is not proper (it contains 1).*

¹This can create some confusion: keep on reading and convince yourself that everything really holds.

- (2) If $f \in k[X_1, \dots, X_n]$ is such that f vanishes at every algebraic zero of Σ (i.e. if $S = Z(\Sigma)$, $f(P) = 0$ for all $P \in S$), then a power of f belongs to the ideal I generated by Σ , i.e. there exist $\nu > 0, g_i \in k[X_1, \dots, X_n], h_i \in \Sigma$ such that $f^\nu = \sum g_i h_i$.

PROOF.

- (1) Let I be the ideal generated by Σ . If $1 \notin I$, there exists a maximal ideal \mathfrak{m} containing I , thus $Z(\Sigma) = Z(I)$ is not empty: by the usual isomorphism there is, at least, the point corresponding to the maximal ideal \mathfrak{m} (keep in mind diagram (1.2)).
- (2) Here there is a trick: let f be as in the hypotheses of the theorem.

Consider the ring $k[X_1, \dots, X_n, X_{n+1}]$ and the set $\Sigma \cup \{1 - X_{n+1}f\}$. This set now has no zeros, i.e.

$$Z(\Sigma \cup \{1 - X_{n+1}f\}) = \emptyset \text{ in } k^{n+1},$$

because $f(P) = 0$ for any P in $Z(\Sigma)$ and $Q \in Z(\Sigma \cup \{1 - X_{n+1}f\})$ iff $Q = (P, t) \in k^{n+1}$ with $P \in Z(S) \subset k^n$ and $t \in k$ such that $1 - tf(P) = 0$. But since $f(P) = 0$ the previous equation has no solution.

So, by the first point of the proof, the ideal $I(S') = I(\Sigma \cup \{1 - X_{n+1}f\})$ contains 1 and we can write

$$(1.3) \quad 1 = \sum \varrho_i h_i + q(1 - X_{n+1}f) \text{ where } h_i \in \Sigma, \varrho_i, q \in k[X_1, \dots, X_n, X_{n+1}].$$

Now we have the substitution homomorphism

$$\varphi: k[X_1, \dots, X_n, X_{n+1}] \rightarrow k(X_1, \dots, X_n) = K$$

such that $X_j \mapsto X_j$ for $j = 1, \dots, n$ and $X_{n+1} \mapsto f^{-1} \in K$ (we send the variable X_{n+1} into the root of the polynomial $1 - X_{n+1}f$ in the field of fractions K . Hence we have the diagram

$$\begin{array}{ccc} k[X_1, \dots, X_n, X_{n+1}] & \xrightarrow{\varphi} & k(X_1, \dots, X_n) = K \\ \uparrow & \nearrow & \\ k[X_1, \dots, X_n] & & \end{array}$$

1.5. Remark. In other words, if $A = k[X_1, \dots, X_n]$, $Y = X_{n+1}$ and $\text{Frac}(A) = k(X_1, \dots, X_n)$, we have the diagram

$$\begin{array}{ccc} A[Y] & \xrightarrow{v_{f^{-1}}} & \text{Frac}(A) \\ \uparrow & \nearrow & \\ A & & \end{array}$$

Then, if we apply the homomorphism φ to equation (1.3) we obtain

$$1 = \sum_{\substack{\varrho_i \in k[X_1, \dots, X_n, f^{-1}] \\ h_i \in k[X_1, \dots, X_n]}} \varrho_i(X_1, \dots, X_n, f^{-1}) \overbrace{h_i(X_1, \dots, X_n)}^{\in k[X_1, \dots, X_n]} + \underbrace{q(1 - (f^{-1}f))}_{=0}$$

Thus, by multiplying by a suitable power of f and cleaning all the denominators (that are necessarily powers of f), we obtain that $f^\nu = \sum g_i h_i$ for $g_i \in k[X_1, \dots, X_n]$ and $\nu \geq 1$. □

2. Radical ideals

2.1. Definition. Let $I \subset A$ be an ideal of $A \in \mathbf{Alg}_k$. We denote with $\sqrt{I} := \{a \in A \mid a^n \in I, n > 0\}$ the *radical* of I . \sqrt{I} is an ideal of A that contains I .

Here we summarize some well-known facts about radical ideals:

- (1) $\sqrt{I} = \{a \in A \mid \bar{a} \in \text{Nil}(A/I)\}$.
- (2) $\sqrt{(0)} = \text{Nil}(A) = \bigcap_{\mathfrak{p} \text{ prime}} \mathfrak{p}$, i.e. the nilradical is the intersection of all primes of A .
- (3) $\sqrt{I} = \bigcap_{\mathfrak{p} \supset I} \mathfrak{p}$, \mathfrak{p} primes.
- (4) $I = \sqrt{I}$ (i.e. I is *radical*) iff A/I is a reduced algebra (i.e. $\text{Nil}(A/I) = 0$).
- (5) I prime $\Rightarrow I$ radical.

2.2. Example. Let $\mathfrak{p}, \mathfrak{q}$ be prime ideals of $A \in \mathbf{Rng}$ and suppose $\mathfrak{p} + \mathfrak{q} = 1$. Hence $\mathfrak{p}\mathfrak{q} = \mathfrak{p} \cap \mathfrak{q} = I$ is a radical ideal,² since for $x^n \in I$ we have $x^n \in \mathfrak{p}$ and $x^n \in \mathfrak{q}$, hence $x \in \mathfrak{p} \cap \mathfrak{q}$, being \mathfrak{p} and \mathfrak{q} primes. Note that, in general, the ideal is not prime: from the fact that $1 = \mathfrak{p} + \mathfrak{q}$ we can find $a \in \mathfrak{p}$ and $b \in \mathfrak{q}$ such that $a + b = 1$. Hence we have $ab = b - b^2 = a - a^2 \in I$. If $a \in \mathfrak{p}$ then $b \notin \mathfrak{p}$ and, on the other hand, $b \in \mathfrak{q}$ implies $a \notin \mathfrak{q}$ (the two ideals are proper), so neither a nor b belong to the intersection.

We can see this fact in a more concrete situation: let $A = \mathbb{Z}$, $\mathfrak{p} = (2)$, $\mathfrak{q} = (3)$ but $I = \mathfrak{p} \cap \mathfrak{q} = (6)$ which is clearly not prime (if you want because $A/I = \mathbb{Z}/(2) \times \mathbb{Z}/(3)$ by the Chinese remainder theorem).

2.3. Example. Take the ring of polynomials in two variables $A = k[X, Y]$ and consider the two ideals $\mathfrak{p} = (X)$ and $\mathfrak{q} = (Y)$. They are both prime ideals (not maximal) but we don't have $\mathfrak{p} + \mathfrak{q} = 1$ (in fact $\mathfrak{p} + \mathfrak{q} = (X, Y)$). However, the homomorphism of rings $k[X, Y] \rightarrow k[X] \times k[Y]$ such that $p(X, Y) \mapsto (p(X, 0), p(Y, 0))$ has kernel $(X) \cap (Y)$ which is radical. Notice that $(X) \cap (Y) = (XY)$, because if $p(X, Y) \in (X) \cap (Y)$, then $p(X, Y) = Xf = Yg$ for $f, g \in k[X, Y]$. Because of the unique factorisation, we have $Y \mid f$, hence $p = XYh \in (XY)$.

The ideal (XY) is not prime (the polynomial XY is clearly reducible). Actually we have that $k[X, Y]/(XY) \subset k[X] \times k[Y]$ (is the subring of pairs $(p(X), q(Y))$ such that $p(0) = q(0)$).

In order to state and prove the following result, we need two more results about radicals and radical ideals. The proof of those properties is straightforward and it is left to the reader.

²The product is, in general, contained in the intersection of the ideals. Note that, being \mathfrak{p} and \mathfrak{q} coprime, we have the equality. In fact it holds, for any $\mathfrak{a}, \mathfrak{b}$ ideals, that $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) \subset \mathfrak{a}\mathfrak{b}$, hence, if $\mathfrak{a} + \mathfrak{b} = 1$, we have $(\mathfrak{a} \cap \mathfrak{b}) \subset \mathfrak{a}\mathfrak{b}$. **Warning:** (see example 2.3) we can have the equality even if the two ideals are not coprime.

2.4. Lemma. *Let A be a ring and let $\{\mathfrak{p}_i\}_{i \in I}$ a collection of primes. Let J, I be ideals of A . Then:*

- (1) $\bigcap_{i \in I} \mathfrak{p}_i$ is radical (in other words, arbitrary intersection of primes is radical).
- (2) \sqrt{J} is radical and $\sqrt{\sqrt{J}} = \sqrt{J}$.
- (3) $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

2.5. Theorem. *Let A be a Noetherian Ring and let $I = \sqrt{I}$ be a radical ideal of A . Then I is a finite intersection of primes, i.e. $I = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \dots \cap \mathfrak{p}_n$.*

PROOF. Let $\mathcal{S} = \{\text{proper radical ideals of } A \text{ which are not finite intersection of primes}\}$. If $\mathcal{S} = \emptyset$ we are done. Otherwise, suppose $\mathcal{S} \neq \emptyset$. Being A a Noetherian ring, we can find a maximal element J in \mathcal{S} . Since J is not prime (because $J \in \mathcal{S}$), there exist $a, b \in A$ such that $ab \in J$ but neither a nor b belong to J . Further, we have $J \subsetneq (J, a)$ and $J \subsetneq (J, b)$: observe that the ideals $(J, a) = J + (a)$ and $(J, b) = J + (b)$ are necessarily proper. In fact, if not, $1 = ra + t$, $r \in A$, $t \in J$, and so $b = bra + bt \in J$, contradicting the assumption $b \notin J$.

Consider now the radical ideals $\sqrt{J + (a)}$ and $\sqrt{J + (b)}$. By the maximality of J , they can't be in \mathcal{S} , hence there exist primes ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ and $\mathfrak{q}_1, \dots, \mathfrak{q}_s$ such that

$$\sqrt{J + (a)} = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_n; \quad \sqrt{J + (b)} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_s$$

Let $J' = \sqrt{J + (a)} \cap \sqrt{J + (b)}$. Clearly $J \subset J'$: we want to prove the equality. Suppose then $x \in J'$: by lemma 2.4 we have that exist $n > 0$ such that³ $x^n \in (J, a)(J, b) \subset J$. Hence $x^n \in J$, but J is radical, so $x \in J$. Then we have proved that $J' = J$ and that J is a finite intersection of primes, which contradicts $J \in \mathcal{S}$. \square

2.6. Remark. Notice that the decomposition of \sqrt{I} as finite intersection of primes is not unique. We will see in the following section that we will recover the uniqueness (up to the order) by the introduction of the minimal primes.

We can now state an important corollary to Hilbert's Nullstellensatz:

2.7. Corollary. *Let A be a finitely generated k -algebra, for a field k algebraically closed. Let $I \subset A$ be an ideal. Then $\sqrt{I} = \bigcap_{\mathfrak{m} \supset I} \mathfrak{m}$, for \mathfrak{m} maximal ideals of A .*

PROOF. By the Nullstellensatz, we have that any f that vanishes in $Z(I)$ belongs to \sqrt{I} (there is a positive ν such that $f^\nu \in I$). In particular the radical \sqrt{I} is the ideal of functions vanishing on $Z(I)$: in fact, if $f \in \sqrt{I}$, then we have $f^n \in I$ for some $n > 0$. Hence, for any $P \in Z(I)$ we have $v_{f^n}(P) = 0$ and then $v_f(P) = 0$, that is f vanishes on $Z(I)$. Let $J = \bigcap_{\mathfrak{m} \supset I} \mathfrak{m}$, \mathfrak{m} maximal ideals of A containing I . Then we have that $f \in J$ implies $f \in \mathfrak{m}$ for all maximals $\mathfrak{m} \supset I$. Hence f vanishes on $Z(\mathfrak{m}) \subset Z(I)$ (since the correspondence is inclusion-reversing) and so $f \in \sqrt{I}$. Then we have proved

³Remember that $(J, a)(J, b) = (J^2, bJ, aJ, ab)$. Since $ab \in J$ we have $(J^2, bJ, aJ, ab) \subset J$.

that $J \subset \sqrt{I}$. On the other hand, simply notice that

$$\sqrt{I} = \bigcap_{\mathfrak{p} \supset I} \mathfrak{p} \subset \bigcap_{\mathfrak{m} \supset I} \mathfrak{m} = J$$

for \mathfrak{p} primes. So we have the equality. \square

Let's take a closer look to the result that we have just proved. We still have, indeed, an open question that raised in a quite natural way in the first part of this section: we introduced a new point of view and we saw that, for a finitely generated k -algebra A , it was possible to think the elements of A as functions defined from the "space" $X = \text{Max}(A)$ to the field k . Thanks to the equivalence of X with the zero set $V_k(I)(k)$, for $A = k[X_1, \dots, X_n]/I$, we defined the ideal \tilde{I} of functions vanishing on I and we clearly observed that this ideal contains I .

At that point we posed the following questions: what is the link between \tilde{I} and I ? Is it possible to recover the ideal I starting from the zero set $Z(I)$?

Thanks to the Nullstellensatz and to the previous corollary, we can now answer: \tilde{I} , this mysterious object, is simply the radical ideal of I . Hence, except in the case $I = \sqrt{I}$, we see that we can't reconstruct the ideal I starting from $Z(I)$: what we have is just $I(Z(I)) = \sqrt{I}$, where $I(S)$, as we have seen in the proof of Nullstellensatz, is the ideal of functions vanishing on $S \subset \mathbb{A}_k^n$.

Conversely, we have this result:

2.8. Corollary. *Let A a finitely generated k -algebra, k algebraically closed. Then any radical ideal is the ideal of vanishing functions of an algebraic set, which is the set of maximal ideals containing I .*

We have then the following picture:

$$\begin{array}{ccc} A & \longleftrightarrow & X = \text{Max}(A) \simeq \text{Hom}_k(A, k) \\ \{\text{radical ideals}\} & \longleftrightarrow & \{\text{algebraic sets}\} \\ I & \longleftrightarrow & \{\mathfrak{m} \in X \mid \mathfrak{m} \supset I\} \end{array}$$

From now on, we remove the hypothesis that k is an algebraically closed field. Let $A = k[X_1, \dots, X_n]/I$ the finitely generated k -algebra which represents the zero set $V_k(I)(-)$ as a functor. Then A is unique, up to isomorphism⁴, and so it is the ideal $I \subseteq k[X_1, \dots, X_n]$ in such a fixed polynomial ring. Thus

$$I = I' \iff V_k(I) = V_k(I')$$

as functors on \mathbf{Alg}_k . Now, by Yoneda's lemma, we have:

$$\mathbf{Alg}_k^{op} \xrightarrow{\simeq} \text{Rep}(\mathbf{Alg}_k)$$

where $\text{Rep}(-)$ denotes here the full subcategory of representable functors. In general, we then may seek for a "geometric" description of \mathbf{Alg}_k^{op} and, similarly, of the category \mathbf{Rng}^{op} , the opposite category of all rings.

⁴Remember that two objects representing the same functor are always isomorphic.

2.9. Remark. If we restrict the functor $V_k(I)(-)$ to the subcategory of \mathbf{Alg}_k given by the field extensions of k , the map $I \rightsquigarrow V_k(I)$ is no more injective. So, it is not enough to consider the subcategory $\mathbf{Alg}_k^{\text{red}} \subseteq \mathbf{Alg}_k$ of reduced k -algebras (that contains the field extensions) if we hope to keep the one-to-one correspondence between the “zero sets” and the k -algebras. In fact, consider the following example.

2.10. Example. Let $I = (t)$ and $I' = (t^2)$ in $k[t]$. We clearly have that $V_k(I)(K) = V_k(I')(K)$ for all K reduced k -algebras, i.e. if the equation $X^2 = 0$ has a non zero solution in K then K is not reduced.

3. Geometric points

Let A be *any*⁵ k -algebra. We here consider the “zero set” as a functor on field extensions of a field k . However, a fixed ground field k is not really needed in what follows (see below). In other words, keeping in mind what we have seen in the previous sections, we say that

$$k \subseteq K \mapsto \text{Hom}_k(A, K)$$

is our “zero set”. Remember that when $A = k[X_1, \dots, X_n]/I$ is finitely generated, then $V_k(I)(K) = \text{Hom}_k(A, K)$.

3.1. Definition. We say that a k -homomorphism $A \rightarrow K'$ for a field extension $k \subseteq K'$ is a *geometric point*. We say that two geometric points $v': A \rightarrow K'$ and $v'': A \rightarrow K''$ are *equivalent* if there exists a third point $w: A \rightarrow \mathcal{K}$ for a field extensions $K' \subseteq \mathcal{K}$ and $K'' \subseteq \mathcal{K}$ such that the following diagram commutes

$$(3.1) \quad \begin{array}{ccc} & K' & \\ & \nearrow v' & \\ A & \xrightarrow{w} & \mathcal{K} \\ & \searrow v'' & \\ & K'' & \end{array}$$

Observe that $\mathfrak{p}_{v'} := \text{Ker } A \xrightarrow{v'} K'$ is a prime ideal since $A/\mathfrak{p}_{v'} \subseteq K'$ is a domain (being contained in a field). Conversely, if we have a prime ideal $\mathfrak{p} \in \text{Spec}(A)$, we get a pair $(v_{\mathfrak{p}}, K(\mathfrak{p}))$

$$A \twoheadrightarrow A/\mathfrak{p} \hookrightarrow \text{Frac}(A/\mathfrak{p}) := K(\mathfrak{p})$$

where we denote by $K(\mathfrak{p})$ the *residue field* for the prime ideal \mathfrak{p} and we define the map $v_{\mathfrak{p}}: A \rightarrow K(\mathfrak{p})$ as the composition between the projection on the quotient and the inclusion of A/\mathfrak{p} into its field of fractions. In this way we can define a geometric point. Moreover we have the following result:

3.2. Proposition. *The mappings $v' \mapsto \mathfrak{p}_{v'}$ and $\mathfrak{p} \mapsto v_{\mathfrak{p}}$ provide a bijective correspondence between the set of equivalence classes of geometric points and the spectrum of A .*

⁵We are no more talking about finitely generated k -algebras.

PROOF. We have to prove that the maps are well defined (then they are clearly bijections). Indeed, this means that we have to show that two geometric points are equivalent iff they have the same kernel.

By diagram (3.1), if $A \xrightarrow{v'} K'$ and $A \xrightarrow{v''} K''$ are equivalent, we have that

$$\begin{array}{ccc} \text{Ker}(w) = \text{Ker}(A \xrightarrow{v'} K' \hookrightarrow \mathbb{K}) & = & \text{Ker}(A \xrightarrow{v''} K'' \hookrightarrow \mathbb{K}) \\ \parallel & & \parallel \\ \text{Ker}(A \xrightarrow{v'} K') & & \text{Ker}(A \xrightarrow{v''} K''). \end{array}$$

Conversely, if $\mathfrak{p} = \text{Ker}(A \xrightarrow{v'} K') = \text{Ker}(A \xrightarrow{v''} K'')$, we have the following commutative diagram:

$$\begin{array}{ccccc} & & & & K' \\ & & & & \nearrow \\ A & \xrightarrow{v'} & & & K' \\ & \searrow & & & \searrow \\ & & & & K'' \\ & & & & \nearrow \\ & & & & K'K'' \\ & & & & \nearrow \\ & & & & K' \\ & & & & \searrow \\ & & & & K'' \\ & & & & \searrow \\ & & & & K'K'' \end{array}$$

where $K'K''$ denotes the composite field. Hence v' and v'' are equivalent. \square

Now, in a construction which is completely similar to that one we made for maximal ideals, we can think the primes $\mathfrak{p} \in \text{Spec}(A)$ as “points”. Indeed we have just proved that they correspond to the geometric points $v_{\mathfrak{p}}: A \rightarrow K(\mathfrak{p})$.

3.3. Remark. Notice that there is no reason to take A as a k -algebra for some field k in this construction: it's completely general and can be made for any $A \in \mathbf{Rng}$. We will do so in the following section.

3.4. Definition. For an element $f \in A$ and a prime ideal⁶ $\mathfrak{p} \in \text{Spec}(A)$, we define the *value of f at the prime \mathfrak{p}* as the image of f under the canonical projection:

$$f(\mathfrak{p}) := \bar{f} \in A/\mathfrak{p} \subseteq K(\mathfrak{p}).$$

Then, $\mathfrak{p} = \mathfrak{p}_{v'}$ we have $\bar{f} \rightsquigarrow v'(f)$ under the field extension $K(\mathfrak{p}) \subseteq K'$.

Hence, any element $f \in A$ can be regarded as a function on $\text{Spec}(A)$ (indeed, we can choose the codomain to be any field extension $K' \supset K(\mathfrak{p})$). This “function” is zero at \mathfrak{p} if $f \in \mathfrak{p}$. However, if f is zero everywhere (i.e. at every point \mathfrak{p} in $\text{Spec}(A)$), then

$$f \in \bigcap_{\mathfrak{p} \in \text{Spec}(A)} \mathfrak{p} = \text{Nil}(A).$$

So we have found a map that is zero “everywhere”, but it's not the zero map!

3.5. Remark. We may underline a couple of facts:

⁶i.e. an equivalence class of a geometric point $A \xrightarrow{v'} K'$, thanks to prop. 3.2.

- a) Suppose that $A = k[X_1, \dots, X_n]/I$ is finitely generated and reduced k -algebra, which is to say that $I = \sqrt{I}$. Then, for a polynomial $f \notin I$, there exists a prime $\mathfrak{p} \supset I$ such that $f \notin \mathfrak{p}$. In fact, $I = \sqrt{I}$ is equal to the intersection of all primes containing I . Hence, if $f \in \mathfrak{p}$ for all such primes we would have $f \in I$. Thus f cannot be zero on all $\text{Spec}(A)$. In other words, we have proved that I is exactly the ideal of $f \in A$ vanishing on all primes $\mathfrak{p} \supset I$.
- b) If we need to reconstruct the ring A out of the prime spectrum $\text{Spec}(A)$ we have to add, somehow, the information coming from all “functions” on it. As sets, for example, we have $\text{Spec}(k[t]/(t)) = \text{Spec}(k[t]/(t^n))$ for all $n > 1$, but, of course, $k[t]/(t) \not\cong k[t]/(t^n)$.

4. Rational Points

Let $A \in \mathbf{Alg}_k$ and suppose A finitely generated. Consider the set of maximal ideals $\text{Max}(A) \subset \text{Spec}(A)$. Each $\mathfrak{m} \in \text{Max}(A)$ yields a geometric point, since we have a map $A \rightarrow A/\mathfrak{m}$ and A/\mathfrak{m} is an algebraic field extension of k (thanks to Zariski’s lemma). Before moving to the next section, we want to say something more about a particular family of geometric points.

4.1. Definition. A k -homomorphism $v: A \rightarrow k$ of a k -algebra A is called a *rational point*.

We denote provisionally with $X(k)$ the set of rational points. Then for all $x \in X(k)$ we denote with \mathfrak{m}_x the maximal ideal which is given by $\mathfrak{m}_x := \text{Ker}(A \xrightarrow{x} k)$.

Here we close the circle: we saw that - for an algebraically closed field k - it was possible to think maximal ideals of $A = k[X_1, \dots, X_n]/I$ as the points of the zero set $V_k(I)(k)$. Then, removing the hypothesis of algebraic closure for k , we began a generalization in order to include in this setting also the points of the zero set $V_k(I)(K)$ for some field extension K of k . We found the answer with the definition of geometric points and now, through the correspondence between the set of equivalence classes of geometric points and the prime spectrum $\text{Spec}(A)$, we recognize that the rational points are simply the maximal ideals such that $A/\mathfrak{m} \simeq k$.

To fix this point, we make the following definition, even if we have already met all the involved objects:

4.2. Definition. For a finitely generated k -algebra $A = k[X_1, \dots, X_n]/I$ we call *algebraic set* the set of its rational points $Z(I) := V_k(I)(k) = \text{Hom}_k(A, k) = X(k)$. If $k = \bar{k}$ is an algebraically closed field we then have $Z(I) = \text{Max}(A)$.

Remember now that in the case $k = \bar{k}$, by corollary 2.7, we have $I(Z(I)) = \sqrt{I}$. Further, for any subset $S \subseteq \mathbb{A}_k^n(k) = k^n$ we know that we get an ideal

$$I(S) := \{f \in k[X_1, \dots, X_n] \mid f(z) = 0 \text{ for all } z \in S\}$$

Thus

$$\sqrt{I} = \sqrt{I'} \iff Z(I) = Z(I')$$

for every ideal $I, I' \subseteq k[X_1, \dots, X_n]$. Hence the algebraic set $Z(I) \subseteq \mathbb{A}_k^n(k)$ only depends on the reduced k -algebra $k[X_1, \dots, X_n]/\sqrt{I}$. This is the so called “coordinate ring” of the algebraic set $Z(I)$.

5. Polynomial mappings

A k -algebra homomorphism

$$f: k[X_1, \dots, X_n]/I \rightarrow k[Y_1, \dots, Y_m]/J$$

is given by a map between the two polynomial rings $F: k[X_1, \dots, X_n] \rightarrow k[Y_1, \dots, Y_m]$ with

$$X_i \mapsto p_i(Y_1, \dots, Y_m) \in k[Y_1, \dots, Y_m] \text{ for all } i = 1, \dots, n$$

such that if $f \in I$ then $f(p_1, \dots, p_n) \in J$.

5.1. Remark. Notice that if $p_j \cong \tilde{p}_j \pmod{J}$, then we have $f(p_1, \dots, p_n) \cong f(\tilde{p}_1, \dots, \tilde{p}_n) \pmod{J}$. Hence the p_j can be chosen modulo J only.

Such a k -algebra homomorphism induces, by composition, a map between rational points in the following way. First, notice that the map F yields a map between the affine spaces:

$$\begin{array}{ccc} k[X_1, \dots, X_n] & k^n = \mathbb{A}_k^n(k) \xrightarrow{\cong} \text{Hom}_k(k[X_1, \dots, X_n], k) & \\ \downarrow F & \uparrow & \uparrow -\circ F \\ k[Y_1, \dots, Y_m] & k^m = \mathbb{A}_k^m(k) \xrightarrow{\cong} \text{Hom}_k(k[Y_1, \dots, Y_m], k), & \end{array}$$

that is, if $y = (y_1, \dots, y_m) \in \mathbb{A}_k^m(k)$

$$(y_1, \dots, y_m) \rightsquigarrow (p_1(y_1, \dots, y_m), \dots, p_n(y_1, \dots, y_m))$$

obtained from $v_y: k[Y_1, \dots, Y_m] \rightarrow k$ by composition with F . If $y \in Z(J)$ then $g(y) = 0$ for all $g \in J$. Then there exists a (unique) map $k[Y_1, \dots, Y_m]/J \rightarrow k$ such that

$$\begin{array}{ccc} k[Y_1, \dots, Y_m] & \xrightarrow{v_y} & k \\ \downarrow & \nearrow \text{---} & \\ k[Y_1, \dots, Y_m]/J & & \end{array}$$

commutes: in this case we say that v_y factors modulo J . Hence, by composition with the map f defined above, we get a rational point in $Z(I)$.

So we are ready to give the following definition:

5.2. Definition. For a pair of algebraic sets $Z(I) \subseteq k^n$ and $Z(J) \subseteq k^m$, a mapping $p: Z(J) \rightarrow Z(I)$ is called (a *regular mapping* or a *polynomial mapping* or) a *morphism* if there are polynomials $p_1, \dots, p_n \in k[Y_1, \dots, Y_m]$ such that $p(y) = (p_1(y), \dots, p_n(y))$ where $y \in Z(J)$ and $p(y) \in Z(I)$.

Since we have defined the maps between algebraic sets, we get a category, that we denote with \mathbf{AlgSet}_k , that is the category of algebraic sets over k .

Warning. The objects of this category are *pairs* $(Z(I), Z(I) \subset k^n)$, in the sense that, over than the set $Z(I)$, we have to consider the embedding⁷ $Z(I) \subset k^n$.

⁷Notice that if we consider two different embeddings (e.g. the embeddings given by two different reordering of the variables in the polynomial ring $k[X_1, \dots, X_n]$) the algebraic sets are isomorphic.

It is now easy to check that $A \mapsto \text{Hom}_k(A, k)$ just defines a functor

$$(5.1) \quad \begin{aligned} \mathbf{Alg}_k^{op} &\longrightarrow \mathbf{AlgSet}_k \\ k[X_1, \dots, X_n]/I &\longmapsto Z(I) \end{aligned}$$

between the opposite category of finitely generated k -algebras and algebraic sets.

5.3. Proposition. *Let $k = \bar{k}$ be an algebraically closed field. The functor $A \mapsto \text{Hom}_k(A, k) = \text{Max}(A)$ restricts to an anti-equivalence between the opposite category of reduced finitely generated k -algebras and algebraic sets over k .*

$$\mathcal{Z}: (\mathbf{Alg}_k^{\text{red}})^{op} \xrightarrow{\simeq} \mathbf{AlgSet}_k$$

where the quasi-inverse functor is given by

$$\mathcal{J}: Z(I) \subseteq k^n \mapsto k[X_1, \dots, X_n]/\sqrt{I}$$

PROOF. The functor $\mathcal{Z}: (\mathbf{Alg}_k^{\text{red}})^{op} \rightarrow \mathbf{AlgSet}_k$ is essentially surjective⁸ on the objects because, for an algebraic set $Z(I) \in \mathbf{AlgSet}_k$, we can define $A = k[X_1, \dots, X_n]/I(Z(I))$. By the Nullstellensatz, we have $I(Z(I)) = \sqrt{I}$, so A is a reduced finitely generated k -algebra, and we have $\mathcal{Z}(A) = Z(\sqrt{I}) = Z(I)$.

Then we have to show that \mathcal{Z} is fully faithful. Consider $p: Z(J) \rightarrow Z(I)$ a polynomial mapping and suppose $Z(J) \subseteq k^m$, $Z(I) \subseteq k^n$. Then there exist n polynomials $p_1, \dots, p_n \in k[Y_1, \dots, Y_m]$ providing a k -homomorphism

$$\begin{aligned} \pi: k[X_1, \dots, X_n] &\longrightarrow k[Y_1, \dots, Y_m] \\ X_i &\longmapsto p_i(Y_1, \dots, Y_m), \end{aligned}$$

such that, for $f \in k[X_1, \dots, X_n]$, we have $\pi(f) = f(p_1(Y_1, \dots, Y_m), \dots, p_n(Y_1, \dots, Y_m))$. The map p is such that $Z(J) \ni (y_1, \dots, y_m) \mapsto (p_1(y_1, \dots, y_m), \dots, p_n(y_1, \dots, y_m))$ in $Z(I)$. Hence, if $f \in \sqrt{I} = I(Z(I))$ and $y \in Z(J)$, then

$$\pi(f)(y) = v_y(\pi(f)) = f(p_1(y_1, \dots, y_m), \dots, p_n(y_1, \dots, y_m)) = f(p(y)) = 0$$

and so $\pi(f) \in \sqrt{J}$. Thus π factors through the quotient map $\bar{p} := \mathcal{J}(p)$ and we have the following commutative diagram:

$$(5.2) \quad \begin{array}{ccc} \sqrt{I} & \overset{\text{-----}}{\longrightarrow} & \sqrt{J} \\ \downarrow & & \downarrow \\ k[X_1, \dots, X_n] & \xrightarrow{\pi} & k[Y_1, \dots, Y_m] \\ \downarrow & & \downarrow \\ k[X_1, \dots, X_n]/\sqrt{I} & \xrightarrow{\bar{p}} & k[Y_1, \dots, Y_m]/\sqrt{J} \xrightarrow{v_y} k \end{array}$$

Now we have to show that \bar{p} gives back p as a map between algebraic sets. Given \bar{p} , that is a map between reduced, finitely generated k -algebras, we define $\mathcal{Z}(\bar{p}): Z(J) \rightarrow Z(I)$ in the following way.

⁸A functor $F: \mathbf{C} \rightarrow \mathbf{D}$ is *essentially surjective* if for every object y of \mathbf{D} , there exists an object x of \mathbf{C} and an isomorphism $F(x) \cong y$ in \mathbf{D} .

For $y \in Z(J)$, the evaluation map v_y factors through the quotient map

$$h_y: k[Y_1, \dots, Y_m]/\sqrt{J} \rightarrow k.$$

Then we compose with \bar{p} and we get a rational point $h_y \circ \bar{p}: k[X_1, \dots, X_n]/\sqrt{I} \rightarrow k$. Compose again with the canonical projection $\pi_J: k[X_1, \dots, X_n] \rightarrow k[X_1, \dots, X_n]/\sqrt{I}$ in order to obtain a surjective map $v_x: k[X_1, \dots, X_n] \rightarrow k$. Finally, we define the point $x \in k^n$ with components

$$x_i = v_x(X_i) = h_y(\bar{p}(\pi_J(X_i))) = v_y(\pi(X_i)) = v_y(p_i(Y_1, \dots, Y_m)) = p_i(y_1, \dots, y_m)$$

by the commutativity of diagram (5.2). Hence we have proved that the map $\mathcal{Z}(\bar{p}) = p$. Conversely, in a similar way, we can show that, given a map φ between finitely generated reduced k -algebras, we obtain $\mathcal{J}(\mathcal{Z}(\varphi)) = \varphi$, completing the proof. \square

CHAPTER 4

The spectrum of a ring

1. The Zariski's topology over $\text{Spec}(A)$

Let A be a ring. We have already met the prime spectrum $X = \text{Spec}(A)$ that is, first of all, the set of primes. Further, we will regard elements $x \in X = \text{Spec}(A)$ as “points” and elements $f \in A$ as “functions”.

Therefore, according with definition 3.4, for $x \in X$ we denote $\mathfrak{p}_x \subset A$ the corresponding prime and the value of $f \in A$ at x is

$$f \rightsquigarrow f(x) := \bar{f} \in A/\mathfrak{p}_x \subseteq K(\mathfrak{p}_x)$$

In this section we will replace the polynomial ring $k[X_1, \dots, X_n]$ over an algebraically closed field k along with its algebraic sets by any ring A with a new definition of “algebraic sets”.

1.1. Definition. Let $S \subseteq A$ be a subset of A . We define the “zero set” $\mathcal{V}(S) \subseteq X = \text{Spec}(A)$ as follows

$$\begin{aligned} \mathcal{V}(S) &:= \{x \in X \mid f(x) = 0 \text{ for all } f \in S\} \\ &= \{\mathfrak{p}_x \in \text{Spec}(A) \mid f \in \mathfrak{p}_x \text{ for all } f \in S\} \\ &= \{\mathfrak{p}_x \in \text{Spec}(A) \mid \mathfrak{p}_x \supset S\}. \end{aligned}$$

It's clear that $\mathcal{V}(S) = \mathcal{V}(I)$ for $I = I(S) \subseteq A$, the ideal generated by S , since we have $\mathfrak{p}_x \supset S$ iff $\mathfrak{p}_x \supset I$. Let's see some properties of this “new” object:

1.2. Proposition. *We have:*

- i) if $S \subseteq S'$ then $\mathcal{V}(S') \subseteq \mathcal{V}(S)$;
- ii) $\mathcal{V}(\emptyset) = \mathcal{V}(0) = X$;
- iii) $\mathcal{V}(A) = \mathcal{V}(1) = \emptyset$;
- iv) $\mathcal{V}(\cup_{\alpha} S_{\alpha}) = \cap_{\alpha} \mathcal{V}(S_{\alpha})$;
- v) $\mathcal{V}(\sum_{\alpha} I_{\alpha}) = \cap_{\alpha} \mathcal{V}(I_{\alpha})$;
- vi) $\mathcal{V}(I \cap J) = \mathcal{V}(I) \cup \mathcal{V}(J)$;

PROOF. Straightforward for i)-v). For the last one, note that if $\mathfrak{p}_x \supset (I \cap J)$ then, being \mathfrak{p}_x prime, we have $\mathfrak{p}_x \supseteq I$ or $\mathfrak{p}_x \supseteq J$, hence $\mathcal{V}(I \cap J) \subset \mathcal{V}(I) \cup \mathcal{V}(J)$. Conversely $\mathcal{V}(I \cap J) \supseteq \mathcal{V}(I) \cup \mathcal{V}(J)$ by (i). \square

1.3. Remark. In order to stress the use of “functions”, we can also argue to prove 1.2 (vi) as follows: if $x \notin \mathcal{V}(I) \cup \mathcal{V}(J)$ then exist $f \in I$ and $g \in J$ such that $f(x) \neq 0$ and $g(x) \neq 0$, so that $fg \in I \cap J$ and $fg(x) \neq 0$, thus $x \notin \mathcal{V}(I \cap J)$.

Proposition 1.2 shows that every set of the form $\mathcal{V}(S)$ for $S \subseteq A$ is a *closed set* for a topology on X , which is called *Zariski topology* over the prime spectrum $\text{Spec}(A)$. From

this moment on, we will always consider $X = \text{Spec}(A)$ endowed with this topology. Every $U \subseteq X$ such that $U = X \setminus \mathcal{V}(I)$ for some $I \subseteq A$ is an open set.

We will study different properties of this set as a topological space: we begin with the following

1.4. Definition. Let (X, τ) be a topological space. We say that X is *quasi-compact* with respect to the topology τ if, given an open covering of X , i.e. $X = \bigcup_{\lambda \in \Lambda} U_\lambda$, there exist a finite subset $\{U_1, \dots, U_k\} \subset \{U_\lambda \mid \lambda \in \Lambda\}$ such that $X = \bigcup_{i=1}^k U_k$.

1.5. Proposition. *The prime spectrum of a ring is quasi-compact with respect to Zariski's topology.*

PROOF. We will prove that the following condition holds (that is equivalent to definition 1.4): let $\{\mathcal{V}(S_\lambda) \mid \lambda \in \Lambda\}$ be a family of closed subsets of X such that $\bigcap_{\lambda \in \Lambda} \mathcal{V}(S_\lambda) = \emptyset$. Then there exist a finite subset $\{\mathcal{V}(S_1), \dots, \mathcal{V}(S_k)\} \subset \{\mathcal{V}(S_\lambda) \mid \lambda \in \Lambda\}$ such that $\bigcap_{i=1}^k \mathcal{V}(S_k) = \emptyset$.

Since, by the previous proposition, we have

$$\emptyset = \bigcap_{\lambda \in \Lambda} \mathcal{V}(S_\lambda) = \mathcal{V}\left(\bigcup_{\lambda \in \Lambda} S_\lambda\right).$$

Hence, there does not exist a prime \mathfrak{p} such that $\mathfrak{p} \supset \bigcup_{\lambda \in \Lambda} S_\lambda$, which is to say that the ideal generated by S_λ (call it I) is not proper, that is $I = (1)$. Then, by definition of I , we have that there exists a *finite* number of $s_j \in \bigcup_{\lambda \in \Lambda} S_\lambda$ and $p_j \in A$ such that

$$1 = \sum_{j=1}^k p_j s_j.$$

Thus a finite number of elements s_j generates the ideal $I = A$ and hence, being the map \mathcal{V} inclusion-reversing, we have $\mathcal{V}\left(\bigcup_{\lambda \in \Lambda} S_\lambda\right) = \mathcal{V}(I) = \bigcap_{i=1}^k \mathcal{V}(S_k) = \emptyset$ where we choose the subsets S_j such that $s_j \in S_j$. \square

2. Nullstellensatz revisited

As we have seen for algebraic sets, we can go back from the subsets of X to the ideals of A by defining a new map (that will be, in a certain way, the inverse of \mathcal{V}) in the following way:

2.1. Definition. Let $Y \subseteq X = \text{Spec}(A)$ be a subset of the prime spectrum of A . We define the *ideal generated by Y* , $\mathcal{I}(Y) \subseteq A$, as follows

$$\begin{aligned} \mathcal{I}(Y) &:= \{f \in A \mid f(y) = 0 \text{ for all } y \in Y\} \\ &= \{f \in A \mid \bar{f} = 0 \text{ in } A/\mathfrak{p}_y \text{ for all } y \in Y\} \\ &= \{f \in A \mid f \in \mathfrak{p}_y \text{ for all } y \in Y\} = \bigcap_{y \in Y} \mathfrak{p}_y. \end{aligned}$$

2.2. Remark. $\mathcal{I}(Y)$ is clearly an ideal of A . It is not, in general, a prime ideal but, being an intersection of primes, is certainly a radical ideal (remember proposition 2.4).

2.3. Remark. We have $\mathcal{I}(X) = \bigcap_{x \in X} \mathfrak{p}_x = \text{Nil}(A)$.

2.4. Proposition. *Let A be a ring, $X = \text{Spec}(A)$.*

- (1) Let $Y \subseteq Y' \subset X$. Then $\mathcal{I}(Y') \subseteq \mathcal{I}(Y)$.
(2) Let $Y \subset X$, then $Y \subseteq \mathcal{V}(\mathcal{I}(Y))$ and the equality holds iff $Y = \mathcal{V}(I)$ (i.e. Y is closed in the Zariski topology of X).
(3) Let $J \subseteq A$ be an ideal. Then $J \subseteq \mathcal{I}(\mathcal{V}(J))$.

PROOF. 1) is trivial: $f \in \mathcal{I}(I')$ is such that $f(y') = 0$ for all $y' \in Y'$, therefore, in particular, $f(y) = 0$ for all $y \in Y \subseteq Y'$, that is $f \in \mathcal{I}(I)$. For 3), remember that $\mathcal{V}(J) = \{\mathfrak{p} \text{ prime}, \mathfrak{p} \supset J\}$. Hence

$$\mathcal{I}(\mathcal{V}(J)) = \bigcap_{\mathfrak{p} \text{ primes}, \mathfrak{p} \supset J} \mathfrak{p} \supset J.$$

Finally, for 2), we have that:

$$\begin{aligned} \mathcal{V}(\mathcal{I}(Y)) &= \{x \in X \mid \mathfrak{p}_x \supset \mathcal{I}(Y)\} \\ &= \{x \in X \mid \mathfrak{p}_x \supset \bigcap_{y \in Y} \mathfrak{p}_y\} \end{aligned}$$

and, for all $y \in Y$, we have $\mathfrak{p}_y \in \mathcal{V}(\mathcal{I}(Y))$ (since clearly $\mathfrak{p}_y \supset \bigcap_{y \in Y} \mathfrak{p}_y$). Hence we have $Y \subseteq \mathcal{V}(\mathcal{I}(Y))$, proving the first part of the assertion. Moreover, by definitions of $\mathcal{V}(J)$ and $\mathcal{I}(Y)$, we have that

$$\mathcal{I}(\mathcal{V}(J)) = \bigcap_{y \in \mathcal{V}(J)} \mathfrak{p}_y = \bigcap_{\mathfrak{p}_x \supset J} \mathfrak{p}_x \supset J.$$

Thus, if we apply \mathcal{V} we obtain that

$$\mathcal{V}(\mathcal{I}(\mathcal{V}(J))) \subseteq \mathcal{V}(J)$$

by the first part of the proof. Therefore, if $Y = \mathcal{V}(J)$ is a Zariski closed set, we have that $Y \supseteq \mathcal{V}(\mathcal{I}(Y))$ and we have done. \square

2.5. Remark. Let $f \in A$ be an element of the ring A . Notice that $\mathcal{V}(f) = \mathcal{V}(f^n)$ for all $n \geq 1$, since we have $\mathfrak{p} \supset (f^n) \iff \mathfrak{p} \supset (f)$ (being \mathfrak{p} a prime).

2.6. Proposition. Let $Y \subset X = \text{Spec}(A)$ be a non-closed subset. Then the (Zariski) closure of Y is $\bar{Y} = \mathcal{V}(\mathcal{I}(Y))$.

PROOF. In fact, $\bar{Y} \subseteq \mathcal{V}(\mathcal{I}(Y))$, because $\mathcal{V}(\mathcal{I}(Y))$ is a Zariski closed set containing Y . So we have to show that for every closed set $\mathcal{V}(J) \supset Y$, it holds $\mathcal{V}(J) \supset \mathcal{V}(\mathcal{I}(Y))$. To see this, simply notice that if $\mathcal{V}(J) \supset Y$, then $J \subset \mathcal{I}(\mathcal{V}(J)) \subset \mathcal{I}(Y)$. Hence $\mathcal{V}(J) \supset \mathcal{V}(\mathcal{I}(Y))$. \square

2.7. Theorem (Hilbert's Nullstellensatz revisited). Let $J \subset A$ be an ideal and let $X = \text{Spec}(A) \supset \mathcal{V}(J)$ be the corresponding Zariski closed subset. Then

$$\mathcal{I}(\mathcal{V}(J)) = \sqrt{J}$$

PROOF. We have

$$\begin{aligned} \mathcal{I}(\mathcal{V}(J)) &= \{f \in A \mid f(y) = 0, y \in \mathcal{V}(J)\} \\ &= \bigcap_{y \in \mathcal{V}(J)} \mathfrak{p}_y = \bigcap_{\mathfrak{p} \supset J} \mathfrak{p} = \sqrt{J}. \end{aligned}$$

\square

2.8. Corollary. *We have a bijection*

$$\begin{array}{ccc} A & \xrightleftharpoons[\mathcal{I}]{\mathcal{V}} & \text{Spec}(A) \\ \{\text{radical ideals}\} & & \{\text{Zariski closed sets}\} \\ I = \sqrt{I} & & Y = \mathcal{V}(I) \end{array}$$

In the previous section, thank's to Hilbert's Nullstellensatz, we built the correspondence between the set of algebraic sets over k - in the hypothesis of algebraically closed field - and the set of radical ideals of the polynomial ring $k[X_1, \dots, X_n]$. Moreover, we saw that the correspondence could be extended to an anti-equivalence of categories between $(\mathbf{Alg}_k^{\text{red}})^{op}$ and \mathbf{AlgSet}_k , where an algebraic set $Z(I)$ is determined, up to isomorphism, by the reduced k -algebra $k[X_1, \dots, X_n]/\sqrt{I}$. The objects of \mathbf{AlgSet}_k were couples $(Z(I) \subset \mathbb{A}_k^n)$, where $Z(I)$ is the set of rational points of the k -algebra $k[X_1, \dots, X_n]/I$ that is equal, if $k = \bar{k}$, to the set $\text{Max}(A)$. Now we have, in a certain sense, re-built this construction from a totally abstract point of view. We are no longer talking about k -algebras, because we are considering generic rings, and we are concentrating on the space $\text{Spec}(A)$ instead of $\text{Max}(A)$.

From classical algebraic geometry, we know that prime ideals in $k[X_1, \dots, X_n]$ correspond to irreducible algebraic sets. They are the "blocks" that we use to build all the algebraic sets, and this corresponds to the fact that every radical ideal is finite intersection of primes and that primes are radical. So it's quite natural to suppose that prime ideals should have a particular role also in this abstract construction.

Therefore, there is a new question for us: what is $\mathcal{V}(\mathfrak{p})$? The problem, here, is that we have to think primes as "points" in the space (and then we have that, given an ideal I , we can build the set of primes containing I) but also as prime *ideals*, so we can define the set of primes that contain a given prime \mathfrak{p} . To a prime \mathfrak{p} we can associate a point in $\text{Spec}(A)$ but also subset of $\text{Spec}(A)$ (that contains the point \mathfrak{p}). To see how weird is the situation, consider the following examples.

2.9. Example.

- (1) Let $x \in \text{Spec}(A)$ and consider $Y = \{x\} \subset X$. We have that Y is a Zariski closed subset iff \mathfrak{p}_x is maximal. In fact, by proposition 2.6, we have that

$$\overline{Y} = \overline{\{x\}} = \mathcal{V}(\mathcal{I}(Y)) = \{\mathfrak{m} \text{ primes} \mid \mathfrak{m} \supseteq \mathfrak{p}_x\}$$

hence $y \in \overline{\{x\}} \iff \mathfrak{p}_y \supset \mathfrak{p}_x$.

- (2) Let A be a PID (e.g. $\mathbb{Z}, k[X], \dots$). Then, for every non-zero prime \mathfrak{p}_x , we have that $\{x\}$ is closed, which is to say that all points but one are closed in X . Moreover, we have that (0) is a prime and it's contained in every maximal ideal. Hence $\overline{\{(0)\}} = X$ and we say that $\{(0)\}$ is dense.

2.10. Proposition. *Let $f: A \rightarrow B$ be a ring homomorphism and let $f^*: \text{Spec}(B) \rightarrow \text{Spec}(A)$ be the induced map on the prime spectra. Then f^* is continuous for Zariski topology. Further, we have that $\text{Spec}(-): \mathbf{Rng}^{op} \rightarrow \mathbf{Top}$ is a (contravariant) functor.*

PROOF. Let $V = \mathcal{V}(S) \subset \text{Spec}(A)$ be a closed subset. Then

$$\begin{aligned} (f^*)^{-1}(V) &= \{\mathfrak{p} \in \text{Spec}(B) \mid f^*(\mathfrak{p}) = f^{-1}(\mathfrak{p}) \supset S\} \\ &= \{\mathfrak{p} \in \text{Spec}(B) \mid \mathfrak{p} \supset f(S)\} = \mathcal{V}(f(S)) \end{aligned}$$

that is a closed subset in $\text{Spec}(B)$. □

2.11. Corollary. $(f^*)^{-1}(\mathcal{V}(S)) = \mathcal{V}(f(S))$.

2.12. Corollary. Let $\pi: A \twoheadrightarrow A/I$, for $I \subset A$ an ideal. Then the following diagram

$$\begin{array}{ccc} \text{Spec}(A/I) & \xrightarrow{\pi^*} & \text{Spec}(A) \\ \downarrow \simeq & \nearrow & \\ \mathcal{V}(I) & & \end{array}$$

commutes. Moreover, π^* is closed.

PROOF. Straightforward for the first part. To see that π^* is closed, notice that $\pi^*(\mathcal{V}(J/I)) = \mathcal{V}(J)$ that is closed in $\text{Spec}(A)$ for every ideal J that contains I . □

2.13. Remark. We should stress two facts.

- (1) Let $I = \text{Nil}(A)$. Then by the previous corollary we have that $\text{Spec}(A/I) = \text{Spec}(A_{\text{red}}) \cong \text{Spec}(A)$, that is $\text{Spec}(A_{\text{red}})$ and $\text{Spec}(A)$ are homeomorphic as topological spaces.
- (2) Let $I \subset A$ be an ideal and consider the powers of I , i.e. I^k for $k \geq 1$. Then we have the following sequence

$$\dots \rightarrow A/I^3 \rightarrow A/I^2 \rightarrow A/I$$

but $\text{Spec}(A/I^k) \simeq \text{Spec}(A/I)$.

2.14. Proposition. Let X be any topological space. Then the following are equivalent:

- i) any intersection of a finite number of non-empty open subsets is non empty (i.e. $U_0, U_1 \neq \emptyset$ implies $U_0 \cap U_1 \neq \emptyset$).
- ii) X is not a finite union of disjoint distinct proper closed subsets.
- iii) $X = X_0 \cup X_1$ for X_0, X_1 closed subsets, implies $X_0 = X$ or $X_1 = X$.
- iv) Any non-empty open subset is dense (i.e. for $U \neq \emptyset$, open, $\overline{U} = X$).

2.15. Definition. A topological space such that one of the above conditions holds is called *irreducible*.

PROOF. $i) \Rightarrow ii) \Rightarrow iii) \Rightarrow iv)$ it's obvious. Now, $U = X \setminus Z$ is an open dense subset iff $U \cap U' \neq \emptyset$ for all $U' \subset X$. Hence $iii) \Rightarrow iv) \Rightarrow i)$. □

Now we have the following proposition.

2.16. Proposition. $Y = \mathcal{V}(S) \subset \text{Spec}(A)$ is irreducible \iff the ideal $\mathcal{I}(Y)$ is prime.

PROOF.

- (\Leftarrow) Suppose $\mathcal{I}(Y)$ is a prime ideal. If $Y = Y_1 \cup Y_2$, with Y_i closed, then we have $\mathcal{I}(Y) = \mathcal{I}(Y_1) \cap \mathcal{I}(Y_2)$. Hence $\mathcal{I}(Y) \supset \mathcal{I}(Y_1)$ or $\mathcal{I}(Y) \supset \mathcal{I}(Y_2)$: suppose $\mathcal{I}(Y) \supset \mathcal{I}(Y_1)$. Therefore, being $Y_1 \subset Y$, we have also $\mathcal{I}(Y) \subset \mathcal{I}(Y_1)$ and so we have the equality $\mathcal{I}(Y) = \mathcal{I}(Y_1)$. Thus $\mathcal{V}(\mathcal{I}(Y)) = \mathcal{V}(\mathcal{I}(Y_1))$ and then $Y = Y_1$ (we can apply proposition 2.4, part 2, since they are closed).
- (\Rightarrow) Let $ab \in \mathcal{I}(Y)$, then $\mathcal{V}(ab) = \mathcal{V}(a) \cup \mathcal{V}(b) \supset \mathcal{V}(\mathcal{I}(Y)) = Y$ (again, because Y closed). To complete the proof we use the following lemma:

2.17. Lemma. *Let $E \subseteq X$ be a closed irreducible subset of X . Let A, B be closed such that $E \subseteq A \cup B$. Then $E \subseteq A$ or $E \subseteq B$.*

PROOF. In fact we have $E = (A \cap E) \cup (B \cap E)$. A, B, E are closed, hence also $A \cap E$ and $B \cap E$ are closed. Therefore, being E irreducible, we have $E = A \cap E$ or $E = B \cap E$, which is to say $E \subseteq A$ or $E \subseteq B$. \square

In our case, $\mathcal{V}(a)$ and $\mathcal{V}(b)$ are both closed. Hence $Y \subseteq \mathcal{V}(a)$ or $Y \subseteq \mathcal{V}(b)$. Then, $\mathcal{I}(Y) \subset \mathcal{I}(\mathcal{V}(a)) \ni a$ or $\mathcal{I}(Y) \subset \mathcal{I}(\mathcal{V}(b)) \ni b$. \square

2.18. Corollary. *Let $X = \text{Spec}(A)$ and $x \in X$. Then $\mathcal{V}(\mathfrak{p}_x) = \{y \in X \mid \mathfrak{p}_y \supset \mathfrak{p}_x\} = \overline{\{x\}}$ is irreducible.*

PROOF. Simply notice that, thanks to the “revisited Nullstellensatz”, we have $\mathcal{I}(\mathcal{V}(\mathfrak{p}_x)) = \sqrt{\mathfrak{p}_x} = \mathfrak{p}_x$. Then apply the previous proposition. \square

2.19. Remark. In particular, we have that the whole space $X = \text{Spec}(A)$ is irreducible iff $\mathcal{I}(X) = \text{Nil}(A)$ is a prime iff $A/\text{Nil}(A) = A_{\text{red}}$ is a domain. In particular, if A is a domain, we have that $\text{Nil}(A) = (0)$ is a prime. Hence $\text{Spec}(A)$ is irreducible and it's the closure of the point $\{\eta\}$, where $\mathfrak{p}_\eta = (0)$, being (0) contained in every prime of A . η is called the *generic point*.

3. Noetherian spaces

We begin with the following

3.1. Definition. We say that a topological space X is *Noetherian* if it satisfies the *descending chain condition* for closed subsets, i.e. every chain of closed subsets

$$X \supset Y_1 \supset \dots \supset Y_n \supset Y_{n+1} \supset \dots$$

is stationary, which is to say that there exists $k \in \mathbb{N}$ such that $Y_k = Y_{k+1}$.

3.2. Proposition. *Let A be a Noetherian ring, then $\text{Spec}(A)$ is Noetherian (as a topological space).*

PROOF. Let $Y_1 \supset \dots \supset Y_n \supset Y_{n+1} \supset \dots$ be a descending chain of Zariski closed subsets. Then $\mathcal{I}(Y_1) \subset \dots \subset \mathcal{I}(Y_n) \subset \mathcal{I}(Y_{n+1}) \subset \dots$ is an ascending chain of ideals. Being A Noetherian, there exists $k \in \mathbb{N}$ such that $\mathcal{I}(Y_k) = \mathcal{I}(Y_{k+1})$ and so we have a stationary chain of (closed) subsets of X given by $\mathcal{V}(\mathcal{I}(Y_1)) \supset \dots \supset \mathcal{V}(\mathcal{I}(Y_k)) = \mathcal{V}(\mathcal{I}(Y_{k+1}))$. But the sets Y_j are closed, then $Y_j = \mathcal{V}(\mathcal{I}(Y_j))$ and we have done. \square

3.3. Proposition. *Let X be a topological space. Then:*

- (1) Any subspace $Y \subset X$ of a Noetherian space X is Noetherian.
 (2) Let $\{X_i\}$ be a finite covering of X such that every X_i is Noetherian. Then X is Noetherian.

PROOF.

- (1) Let $Y \subset X$ and take $\{F_n\}: F_1 \supset \dots \supset F_n \supset \dots$ be a descending chain of closed subsets in Y (with respect to the induced topology): consider its closure in X , call it $\{\overline{F_n}\}$. Then $\{\overline{F_n}\}$ is a descending chain of closed subsets in X , so there exists an index k such that $\overline{F_k} = \overline{F_{k+1}}$. Now we intersect again with Y and we obtain that $F_k = \overline{F_k} \cap Y = \overline{F_{k+1}} \cap Y = F_{k+1}$.
 (2) Let $\{F_n\}: F_1 \supset \dots \supset F_n \supset \dots$ be a descending chain of closed subsets in X and consider the chains $\{F_n \cap X_i\}$ in each of the X_i . They are all Noetherian spaces, hence for each $i = 1, \dots, p$, there exists $n_i \in \mathbb{N}$ such that, for all $n \geq n_i$, $X_i \cap F_{n_i} = X_i \cap F_n$. Let $k = \max\{n_1, \dots, n_p\}$. Then, since it holds $X = \bigcup_{i=1}^p X_i$, for all $n \geq k$ we have

$$F_n = \bigcup_{i=1}^p (X_i \cap F_n) = \bigcup_{i=1}^p (X_i \cap F_k) = F_k.$$

□

3.4. Proposition. *The following are equivalent:*

- i) X is Noetherian,
 ii) any open set of X is quasi-compact.

PROOF.

- i) \Rightarrow ii) It suffices to show that X is quasi compact (in fact, any open set of X is itself Noetherian by the previous proposition). So, consider an open covering of X , $\{U_i\}_{i \in I}$. Since X is a Noetherian space, every non-empty family of open sets has a maximal element¹. So consider the family $\mathcal{S} = \{\text{finite unions of } U_i \text{ for } i \in I\}$ and let U be a maximal element of \mathcal{S} . Hence $U \subset X$: suppose that the inclusion is strict, that is there exists $x \in X \setminus U$. Therefore $x \in U_i$ for some i and $U_i \not\subset U$: from this it follows that $U \cup U_i \supsetneq U$ and clearly $U \cup U_i \in \mathcal{S}$, contradicting the maximality of U .
 ii) \Rightarrow i) We prove that X satisfies the ascending chain condition for the open sets (that is equivalent to the d.c.c. for closed sets). Thus, let $\{U_n\}$ be an ascending chain of open subsets. Then the set $U = \bigcup_n U_n$ is open, hence quasi-compact by assumption. Thus we can extract a finite covering such that $U = \bigcup_{i=1}^N U_i$. Being the family $\{U_n\}$ a chain, there exists an index k such that, for $n \geq k$, $U_n = U_k$.

□

3.5. Proposition. *Let X be a Noetherian space. Then every closed set in X is finite union of irreducible closed subsets of X .*

¹The proof of this fact uses the same argument of the proof of the analogous statement for Noetherian rings.

PROOF. Let $\mathcal{S} = \{U \subset X \text{ closed} \mid U \text{ is not finite union of proper irr. closed subsets}\}$. Being a family of closed sets, it satisfies the dual of the condition for a family of open sets, i.e., if $\mathcal{S} \neq \emptyset$, there exists a *minimal* element in \mathcal{S} , say E . Then E cannot be irreducible and we can write $E = E_1 \cup E_2$ with $E_i \subsetneq E$. By the minimality of E , $E_i \notin \mathcal{S}$, hence $E_i = \bigcup_{j=1}^{N_i} F_{ij}$ for $i = 1, 2$ with F_{ij} proper irreducible closed sets. But then we trivially have that E itself is a finite union of proper irreducible closed sets, contradicting the assumption $E \in \mathcal{S}$. Hence $\mathcal{S} = \emptyset$ and the conclusion follows. \square

Let's now summarize, thanks to the previous propositions, the situation that we have in the case $X = \text{Spec}(A)$. Then there is the following picture:

$$\begin{array}{ccc}
 \mathbf{Rng} & & \mathbf{Top} \\
 \\
 A \text{ (Noetherian)} & \text{Spec}(A) \text{ (Noetherian)} & \\
 I = \sqrt{I} \text{ (radicals)} & \begin{array}{c} \xrightarrow{\mathcal{V}} \\ \xleftarrow{\mathcal{I}} \end{array} & \{\text{Zariski closed}\} \\
 \cup & & \cup \\
 \mathfrak{p} \text{ (primes)} & \begin{array}{c} \xrightarrow{\quad} \\ \xleftarrow{\quad} \end{array} & \{\text{Irred. closed}\} \\
 \cup & & \cup \\
 \mathfrak{m} \text{ (maximals)} & \begin{array}{c} \xrightarrow{\quad} \\ \xleftarrow{\quad} \end{array} & \{\text{Closed points}\}.
 \end{array}$$

Moreover, by proposition 3.5, we have that every closed set $\mathcal{V}(I)$ can be written as a finite union of proper irreducible closed. But we know that irreducible sets in $X = \text{Spec}(A)$ are exactly the sets $\mathcal{V}(\mathfrak{p})$ for \mathfrak{p} prime. Hence we have $\mathcal{V}(I) = \mathcal{V}(\mathfrak{p}_1) \cup \dots \cup \mathcal{V}(\mathfrak{p}_r)$. If we apply the map \mathcal{I} and the Nullstellensatz we obtain the corresponding decomposition of \sqrt{I} as finite intersection of the primes $\mathfrak{p}_1, \dots, \mathfrak{p}_r$. As usual, the decomposition is not unique.

CHAPTER 5

Primary decomposition

1. Minimal primes and primary ideals

1.1. Definition. Let A be a ring and $\mathfrak{p} \subset A$ a prime ideal. We say that \mathfrak{p} is *minimal* if it is minimal in $\text{Spec}(A)$ with respect to the inclusion.

1.2. Proposition. *If $A \neq 0$, then the set of minimal primes of A is not empty.*

PROOF. If $A \neq 0$ then $\text{Spec}(A) \neq \emptyset$. Let $(\mathfrak{p}_i)_{i \in I}$ be a chain of primes in A and set $\mathfrak{p} = \bigcap_{i \in I} \mathfrak{p}_i$. Then \mathfrak{p} is prime, since, for $a, b \in A$ with $ab \in \mathfrak{p}$ and $a \notin \mathfrak{p}$, we can find $j \in I$ such that $a \notin \mathfrak{p}_j$. Hence, for all $k \in I$ such that $\mathfrak{p}_k \subset \mathfrak{p}_j$, we have $a \notin \mathfrak{p}_k$. But \mathfrak{p}_k is prime and $ab \in \mathfrak{p}_k$, so $b \in \mathfrak{p}_k$ and then $b \in \mathfrak{p} = \bigcap_k \mathfrak{p}_k$.

Then we can apply Zorn's lemma to $\text{Spec}(A)$, with the reverse inclusion as partial order, and obtain the thesis. \square

Let $I \subset A$ be an ideal. Then we can define the set of minimal primes *containing* I . If we apply the proposition to the ring A/I we obtain the following

1.3. Corollary. *The set of minimal primes containing I is not empty.*

In consequence, we have that, for an ideal $I \subset A$,

$$\sqrt{I} = \bigcap_{\mathfrak{p} \supset I} \mathfrak{p} = \bigcap_{\substack{\mathfrak{p} \text{ minimal,} \\ \mathfrak{p} \supset I}} \mathfrak{p}.$$

Thanks to theorem 2.5, we know that in a Noetherian ring any radical ideal is a finite intersection of primes. That decomposition is not unique: we can recover uniqueness using minimal primes.

1.4. Proposition. *Let A be a Noetherian ring and $I = \sqrt{I}$ be a radical ideal. Then $\sqrt{I} = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_r$ where \mathfrak{p}_i are the minimal primes over I . This decomposition is unique up to reorder.*

PROOF. The radical \sqrt{I} is a finite intersection of primes and we can certainly assume that the primes that appear in such a decomposition of \sqrt{I} are minimal: in fact, if

$$(1.1) \quad \sqrt{I} = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_n$$

and \mathfrak{p}_k is not minimal over I for some k , there exists a prime \mathfrak{p} such that $I \subseteq \mathfrak{p} \subsetneq \mathfrak{p}_k$. Thus $\mathfrak{p} \supset \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_n$. Remember that, in general, if \mathfrak{p} is a prime such that $\mathfrak{p} \supset I_1 \cap \dots \cap I_n$, then $\mathfrak{p} \supset I_j$ for some j : in fact, if $I_i \not\subseteq \mathfrak{p}$ for all i , there would exist elements $x_i \in I_i \setminus \mathfrak{p}$. But the product $\prod x_i$ always belongs to \mathfrak{p} , absurd.

Hence there is \mathfrak{p}_j in the decomposition (1.1) such that $\mathfrak{p}_j \subseteq \mathfrak{p} \subsetneq \mathfrak{p}_k$. By the minimality of \mathfrak{p} we obtain $\mathfrak{p} = \mathfrak{p}_j$. This implies that we can simply ignore the term \mathfrak{p}_k and suppose

that in (1.1) there appear only minimal primes. Therefore we need to show only the uniqueness of such decomposition. Indeed, if we have

$$\sqrt{I} = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_r = \mathfrak{p}'_1 \cap \dots \cap \mathfrak{p}'_s,$$

by the above argument we obtain that there exists k such that $\mathfrak{p}'_1 \supseteq \mathfrak{p}_k$ and there exists j such that $\mathfrak{p}_k \supseteq \mathfrak{p}'_j$. Hence we have $\mathfrak{p}'_1 \supseteq \mathfrak{p}_k \supseteq \mathfrak{p}'_j$ and, by the minimality assumption, we obtain $\mathfrak{p}'_1 = \mathfrak{p}_k = \mathfrak{p}'_j$. We can iterate this argument to complete the proof. \square

1.5. Example. Let $\mathfrak{p} \in \text{Spec}(A)$. Then we have $\sqrt{\mathfrak{p}^n} = \mathfrak{p}$ and so \mathfrak{p} is the minimal prime containing \mathfrak{p}^n (since every prime ideal that contains \mathfrak{p}^n must contain \mathfrak{p}). If $\mathfrak{p} = \mathfrak{m}$ is a maximal ideal, then \mathfrak{m} is the *only* prime containing \mathfrak{m}^n (by the same argument, if \mathfrak{q} is a prime that contains \mathfrak{m}^n , then $\mathfrak{q} \supseteq \mathfrak{m}$ hence $\mathfrak{q} = \mathfrak{m}$).

We have just said that if I is a power of a prime ideal \mathfrak{p} , then $\sqrt{I} = \mathfrak{p}$ and \mathfrak{p} is the minimal prime containing I . More generally, if I is an ideal such that \sqrt{I} is equal to a prime \mathfrak{p} , then it is the minimal prime over I . We can ask if the converse is true: if $\sqrt{I} = \mathfrak{p}$ is a minimal prime over I , can we deduce that $I = \mathfrak{p}^m$ for some m ? In general, the answer is negative (see an example below).

1.6. Example. This fact is true, for example, in \mathbb{Z} . Let $I = (a)$ such that $\sqrt{(a)} = (p)$ for a rational prime p . Suppose $a \neq 0$, then $a = p^n$. In fact, assume $a \neq p$ (trivial case); then $(p) \not\supseteq (a)$, so $p \nmid a$ and we can write $a = pb$. If $p \nmid b$, there exists a prime $q \neq p$ such that $q \mid b$ and so $q \mid a$, that is $(q) \supseteq (a)$ (notice that b is not a unit in \mathbb{Z} if $(p) \not\supseteq (a)$). Then we have found a maximal ideal $\mathfrak{q} = (q)$ different from $\mathfrak{p} = (p)$ that contains (a) . Hence $\mathfrak{q} \supset \sqrt{(a)} = (p)$ and this is a contradiction. Therefore $p \mid b$ and so on. In conclusion we have $(a) = (p^n)$ for some $n \geq 1$ and this is the form of all non-zero ideals I in \mathbb{Z} such that $\sqrt{I} = (p)$.

Notice that this is equivalent to say that $\mathbb{Z}/(p^n)$ has only nilpotent elements as zero-divisors.

The previous example yields the following definition:

1.7. Definition. An ideal $\mathfrak{q} \subset A$ is called a *primary ideal* if \mathfrak{q} is proper and, for all $x, y \in A$ such that $xy \in \mathfrak{q}$, it holds $x \in \mathfrak{q}$ or $y^n \in \mathfrak{q}$ for some $n \in \mathbb{N}$.

Equivalently, $\mathfrak{q} \subset A$ is primary $\iff A/\mathfrak{q} \neq 0$ and every zero divisor is in $\text{Nil}(A/\mathfrak{q})$. Clearly every prime ideal is primary.

1.8. Remark (Contraction of primary ideal is primary). Given a ring homomorphism $f: A \rightarrow B$ and an ideal $I \subset B$, we can define the *contraction* of I in A as the inverse image of I through f : it's clearly an ideal of A . If $\mathfrak{q} \subset B$ is a primary ideal of B , we can consider its contraction $f^{-1}(\mathfrak{q})$. Suppose $f^{-1}(\mathfrak{q}) \neq A$: hence we have the following (commutative) diagram:

$$\begin{array}{ccccc} f^{-1}(\mathfrak{q}) & \hookrightarrow & A & \twoheadrightarrow & A/f^{-1}(\mathfrak{q}) \\ & & \downarrow f & & \downarrow \\ \mathfrak{q} & \hookrightarrow & B & \twoheadrightarrow & B/\mathfrak{q}. \end{array}$$

The induced map $A/f^{-1}(\mathfrak{q}) \rightarrow B/\mathfrak{q}$ is injective (check this by exercise), so we can embed the quotient ring $A/f^{-1}(\mathfrak{q})$ in a ring where nilpotents are the only zero-divisors. Therefore the same holds for $A/f^{-1}(\mathfrak{q}) \neq 0$, that is to say $f^{-1}(\mathfrak{q})$ is primary.

1.9. Proposition. *If $\mathfrak{q} \subset A$ is a primary ideal, then $\sqrt{\mathfrak{q}}$ is prime (and hence is the minimal prime containing \mathfrak{q}).*

PROOF. Let x, y in A such that $xy \in \sqrt{\mathfrak{q}}$: then $(xy)^m \in \mathfrak{q}$ for some $m \geq 1$. So $x^m \in \mathfrak{q}$ or $(y^m)^n = y^{mn} \in \mathfrak{q}$ for some $n \geq 1$. But this implies, by the definition of the radical ideal, $x \in \sqrt{\mathfrak{q}}$ or $y \in \sqrt{\mathfrak{q}}$. \square

1.10. Definition. If $\mathfrak{p} = \sqrt{\mathfrak{q}}$ for a primary ideal \mathfrak{q} , then \mathfrak{q} is said to be \mathfrak{p} -primary.

Warning. The power of a prime ideal \mathfrak{p} is *not*, in general, primary. Conversely, a primary ideal is not necessarily a prime-power. Consider the following examples:

1.11. Example. Let $A = k[X, Y, Z]/(XY - Z^2) := k[x, y, z]$ be the ring of functions vanishing on the cone with vertex in the origin determined by the equation $XY - Z^2 = 0$. Let $\mathfrak{p} = (x, z)$ be an ideal of A : \mathfrak{p} is prime, since the quotient $A/\mathfrak{p} \simeq k[Y]$ which is a domain. The ideal $\mathfrak{p}^2 = (x^2, z^2, xz) = (x^2, xy, xz)$ is not primary, since $xy \in \mathfrak{p}^2$ but $x \notin \mathfrak{p}^2$ and there is no $n \in \mathbb{N}$ such that $y^n \in \mathfrak{p}^2$.

1.12. Example. Let $A = k[X, Y]$ and consider the ideal $\mathfrak{q} = (X, Y^n)$ for $n \geq 2$. The quotient ring A/\mathfrak{q} is isomorphic to $k[Y]/(Y^n)$ and in this ring zero-divisors are nilpotent, hence \mathfrak{q} is primary. But the radical $\sqrt{\mathfrak{q}} = (X, Y) = \mathfrak{p}$ is maximal, thus it is the unique prime containing (X, Y^n) . Hence $\mathfrak{p} \supsetneq \mathfrak{q} \supsetneq \mathfrak{p}^n$ (strict inclusions) and so \mathfrak{q} is not a power of prime (otherwise it should be a power of \mathfrak{p}).

However, the following proposition holds:

1.13. Proposition. *Let $\mathfrak{q} \subset A$ be an ideal of A . If $\sqrt{\mathfrak{q}} = \mathfrak{m}$ for a maximal ideal \mathfrak{m} , then \mathfrak{q} is primary.*

PROOF. As we have seen before, if $\sqrt{\mathfrak{q}} = \mathfrak{m}$, then \mathfrak{m} is the unique prime containing the ideal \mathfrak{q} . Hence, $\mathfrak{m}/\mathfrak{q}$ is the only prime in the quotient ring A/\mathfrak{q} and so it coincides with the nilradical. Thus every element of A/\mathfrak{q} is either invertible or nilpotent and so \mathfrak{q} is primary. \square

1.14. Remark. In particular, this implies that powers of maximal ideals are always primary. If all primes are maximals in A (e.g. if A is a PID), combining the previous propositions, we have the following inclusion:

$$\{\mathfrak{q}^n \mid \mathfrak{q} \in \text{Spec}(A)\} \subseteq \{\mathfrak{q} \text{ primary ideals}\} \subseteq \{I \subset A \mid \sqrt{I} = \mathfrak{p} \in \text{Spec}(A)\}.$$

The theory of primary decomposition plays a central role in commutative algebra. For Noetherian rings, as we will soon see, it generalizes the known fact that every radical ideal can be written as finite intersection of primes. More generally, given an ideal I which is not necessarily radical, the theory allows us to determine a finite set of primary ideals (that will be connected with the minimal primes appearing in the decomposition of \sqrt{I}) such that I is equal to the intersection of them.

First we need the following definition:

1.15. Definition. We say that an ideal $I \subset A$ has a *primary decomposition* if I is a finite intersection of primary ideals, i.e. $I = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_n$. If, further, we have:

- i) $\sqrt{\mathfrak{q}_i} = \mathfrak{p}_i$, called *associated primes*, are all different;
- ii) $\mathfrak{q}_i \not\supseteq \bigcap_{i \neq j} \mathfrak{q}_j$ for all $1 \leq i \leq n$;

then we say that this decomposition is *minimal* (or *reduced*, or *normal*). We say that I is decomposable if it has a primary decomposition.

We can achieve i) by the following lemma and ii) by omitting all those terms that are superfluous.

1.16. Lemma. *If \mathfrak{q}_i , $1 \leq i \leq r$ are \mathfrak{p} -primary ideal (i.e. $\sqrt{\mathfrak{q}_i} = \mathfrak{p}$), then the intersection $\mathfrak{q} = \bigcap_{i=1}^r \mathfrak{q}_i$ is again \mathfrak{p} -primary.*

PROOF. Clearly $\sqrt{\mathfrak{q}} = \sqrt{\bigcap_{i=1}^r \mathfrak{q}_i} = \bigcap_{i=1}^r \sqrt{\mathfrak{q}_i} = \mathfrak{p}$. Further, if a product xy belongs to \mathfrak{q} and $x \notin \mathfrak{q}$, then there exists i such that $xy \in \mathfrak{q}_i$ and $x \notin \mathfrak{q}_i$. Therefore $y \in \sqrt{\mathfrak{q}_i} = \mathfrak{p}$, since \mathfrak{q}_i is \mathfrak{p} -primary, which is to say $y \in \sqrt{\mathfrak{q}}$. \square

Hence, given a primary decomposition of an ideal I , we can always reduce to i) by taking the intersection of all \mathfrak{p} -primary ideals (for all associated primes \mathfrak{p}). Then we can always reduce to a minimal decomposition.

1.17. Example. Let $I = (X^2, XY)$ in the ring of polynomials $k[X, Y]$ over a field k . We can write the ideal I as an intersection $I = (X) \cap (X, Y)^2 = \mathfrak{q}_1 \cap \mathfrak{q}_2$ that is a primary reduced decomposition. The associated primes are $\mathfrak{p}_1 = \mathfrak{q}_1 = (X)$ and $\mathfrak{p}_2 = \sqrt{\mathfrak{q}_2} = (X, Y)$ (that is maximal). Here we have $\mathfrak{p}_1 \subset \mathfrak{p}_2$ and $\sqrt{I} = \mathfrak{p}_1 \cap \mathfrak{p}_2 = \mathfrak{p}_1$ (and I is not a primary ideal). In general, this example shows that, given a primary reduced decomposition, we cannot say that the decomposition of the radical \sqrt{I} obtained considering the intersection of the associated primes, is minimal.

1.18. Definition. Let I be an ideal and let $I = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_r$ a minimal primary decomposition of I . Let $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ be the associated primes. The minimal elements of the set $\{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ are called the *isolated* primes belonging to I . The others are called *embedded* primes.

1.19. Remark. In the example 1.17, the prime $\mathfrak{p}_2 = (X, Y)$ is embedded and the prime $\mathfrak{p}_1 = (X)$ is isolated. Notice that it is not true that all primary components are independent of the decomposition: in the same example, we can write (X^2, XY) as $(X) \cap (X, Y)^2$ but also as $(X) \cap (X^2, Y)$. However, the isolated primary components (i.e. primary components corresponding to isolated primes) are uniquely determined by I (for a proof of this fact see [2], page 53-54).

2. Primary decomposition in Noetherian rings

In this section we will establish a result about the existence of a primary decomposition for every ideal of a Noetherian ring. This theorem was first established by Emmy Noether in 1921. Before doing this, we state an interesting result that holds for Noetherian rings:

2.1. Proposition. *Let A be a Noetherian ring and let $\mathfrak{q} \subset A$ be an ideal such that $\mathfrak{m} \supset \mathfrak{q}$ for a maximal ideal \mathfrak{m} . Then the following are equivalent:*

- i) \mathfrak{q} is \mathfrak{m} -primary.
- ii) $\sqrt{\mathfrak{q}} = \mathfrak{m}$.
- iii) $\mathfrak{m}^M \subseteq \mathfrak{q} \subseteq \mathfrak{m}$ for some $M > 0$.

PROOF. We have already seen that i) is equivalent to ii). For ii) \Rightarrow iii), we notice that, being A Noetherian, for any ideal $I \subset A$ we have $\sqrt{I} = (x_1, \dots, x_k)$. Now, consider the positive integers $n_i = \min\{n > 0 \mid x_i^n \in I\}$ and take $M \geq \max\{n_i\}$. Thus $(\sqrt{I})^M \subseteq I$: if we take $I = \mathfrak{q}$ such that $\mathfrak{m} = \sqrt{\mathfrak{q}}$ we have done. Finally, to prove iii) \Rightarrow ii), we simply pass to the radicals and obtain $\sqrt{\mathfrak{m}^M} \subseteq \sqrt{\mathfrak{q}} \subseteq \sqrt{\mathfrak{m}}$, that is $\mathfrak{m} \subseteq \sqrt{\mathfrak{q}} \subseteq \mathfrak{m}$. \square

As a consequence, we have the following

2.2. Corollary. *Let A be a Noetherian ring, then the nilradical $\text{Nil}(A)$ is nilpotent (i.e. there exists $n > 0$ such that $(\text{Nil}(A))^n = 0$).*

Now we can begin the proof of the result of Emmy Noether referred to at the beginning of this section.

2.3. Definition. Let $\mathfrak{q} \subset A$ be an ideal. Then \mathfrak{q} is called *irreducible* if from $\mathfrak{q} = \mathfrak{q}_1 \cap \mathfrak{q}_2$ it follows $\mathfrak{q} = \mathfrak{q}_1$ or $\mathfrak{q} = \mathfrak{q}_2$.

2.4. Remark. Every prime ideal \mathfrak{p} is irreducible. In fact from $\mathfrak{p} \supseteq \mathfrak{q}_1 \cap \mathfrak{q}_2$ we have $\mathfrak{p} \supseteq \mathfrak{q}_1$ or $\mathfrak{p} \supseteq \mathfrak{q}_2$ and also $\mathfrak{p} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \subseteq \mathfrak{q}_1, \mathfrak{q}_2$, so one of the two equalities must hold.

2.5. Lemma. *Let A be a Noetherian ring. Then every ideal is a finite intersection of irreducible ideals.*

PROOF. As usual, let \mathcal{S} be the set of ideals of A which are not finite intersection of proper irreducible ideals and take \mathfrak{m} to be maximal in \mathcal{S} . \mathfrak{m} cannot be irreducible, so we can write $\mathfrak{m} = \mathfrak{q}_1 \cap \mathfrak{q}_2$ and neither \mathfrak{q}_1 nor \mathfrak{q}_2 belong to \mathcal{S} , since $\mathfrak{q}_i \supsetneq \mathfrak{m}$. Then both \mathfrak{q}_i are finite intersection of irreducible proper ideals, so the same must hold for \mathfrak{m} , contradiction. Therefore \mathcal{S} must be empty and the result follows. \square

2.6. Lemma. *Let A be a Noetherian ring. Then every irreducible ideal is primary.*

Notice that $\mathfrak{q} \subset A$ is primary and irreducible iff $0 \subset A/\mathfrak{q}$ is primary and irreducible: remember that \mathfrak{q} is primary iff $A/\mathfrak{q} \neq 0$ and every zero divisor is nilpotent, which is to say that 0 is primary in the quotient. The same thing holds for irreducible. So we can reduce to prove the following

Claim. *Let A be a Noetherian ring. If $0 \subset A$ is irreducible then it is primary.*

PROOF. Let $x, y \in A$ such that $xy = 0$ and $y \neq 0$, then $y \in \text{Ann}(x)$. We want to show that $x^n = 0$ for some n . Consider the following ascending chain of ideals:

$$\text{Ann}(x) \subset \text{Ann}(x^2) \subset \dots \subset \text{Ann}(x^n) \subset \dots$$

Since A is Noetherian, the chain must stabilize. Therefore there is $n \geq 1$ such that $\text{Ann}(x^n) = \text{Ann}(x^{n+1})$. Now we claim that $(x^n) \cap (y) = 0$. In fact, if $a \in (x^n) \cap (y)$, then $ax = 0$ since $a \in (y)$ and $yx = 0$. On the other hand, $a = bx^n$; but then, if we multiply by x again, we have $ax = bx^{n+1}$, which is to say $b \in \text{Ann}(x^{n+1}) = \text{Ann}(x^n)$. Thus $0 = bx^n = a$. Hence since 0 is irreducible and $y \neq 0$, we have proved that $0 = x^n$, so 0 is primary. \square

If we combine the two previous lemmas we obtain the following theorem:

2.7. Theorem. *In a Noetherian ring A , every ideal I has a primary decomposition.*

CHAPTER 6

A first step in dimension theory

1. Basic definitions

One of the basic things that we have learnt from classical geometry is the notion of *dimension* of a space. In this section we want to define a concept of dimension that can fit our purpose. This should agree with, and generalize, our geometric intuition.

1.1. Definition. Let X be a topological space, we define the *dimension* of X (denoted $\dim X$) to be the supremum of all integers n such that there exists a chain $Z_0 \subset Z_1 \subset \dots \subset Z_n$ of distinct irreducible closed subsets of X .

1.2. Example. Let k be a field and consider $\mathbb{A}^1 = \mathbb{A}_k^1(k) \cong k$ as a topological space with the Zariski topology, i.e. closed sets are zeros of polynomials in $k[X]$. Then the dimension of \mathbb{A}^1 is 1. Indeed, by the definition of the topology on \mathbb{A}^1 , we have that the only irreducible closed subsets of \mathbb{A}^1 are the whole space and single points.

1.3. Definition. Let A be a ring and let $\mathfrak{p} \in \text{Spec}(A)$ be a prime ideal. We define the *height* of the prime \mathfrak{p} (denoted $\text{ht}(\mathfrak{p})$) to be the supremum of all integers k such that there exists a chain $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \dots \subset \mathfrak{p}_k = \mathfrak{p}$ of distinct prime ideals. We define the *Krull dimension* (or, simply, the *dimension*) of A (denoted $\dim(A)$) to be the supremum of the heights of all prime ideals. Finally, we define the *depth* or *co-height* of a prime \mathfrak{p} (denoted $\text{coht}(\mathfrak{p})$) to be the Krull dimension of the quotient ring A/\mathfrak{p} .

Even if $I \subset A$ is not a prime ideal, we can define the dimension of I , written $\dim(I)$, to be $\dim A/I$. In the case $I = \mathfrak{p}$ prime, it is the given definition of coheight. Notice that, if A is the ring of functions on an algebraic set, then $\dim I$ is the dimension of the (algebraic) subset corresponding to I ; that is, the subset on which the “functions” in I vanish.

Indeed, thanks to the previous section, we see that the Krull dimension of A coincides with the dimension (as a topological space) of $\text{Spec}(A)$.

1.4. Example. Let $A = \mathbb{Z}/(6)$: we have only two prime ideals, i.e. $\mathfrak{p} = (2)$ and $\mathfrak{q} = (3)$ in the quotient, that are maximal. Since (0) is not prime, every chain has just one element $\mathfrak{p}_0 = \mathfrak{p}$ or $\mathfrak{p}_0 = \mathfrak{q}$. Hence the (Krull) dimension of the ring is zero.

1.5. Remark.

- (1) Let X be an irreducible space, $Y \subset X$ a closed subspace and suppose that $\dim X < \infty$. Then, if $\dim X = \dim Y$, we have $X = Y$: indeed, given a chain of irreducible closed subsets in Y , we can extend it with X , which is irreducible by assumption and closed. Since the dimension is finite, this implies that, if $Y \subsetneq X$, the length of the new chain is strictly greater than the length of the given one, contradicting the hypothesis $\dim X = \dim Y$.

- (2) Let X be a Noetherian space and let $X = X_1 \cup \dots \cup X_m$ be a decomposition of X in irreducible closed components. Then $\dim X = \sup_i \dim X_i$. We say that X has *pure dimension* n iff $\dim X_i = n$ for all $i = 1, \dots, m$.

We must pay attention with the notion of dimension for reducible spaces. In particular, if X is the disjoint union of a subset of dimension 2 and of a subset of dimension 1, then it has dimension 2. For this reason we will often consider only irreducible spaces when we will talk about dimension.

1.6. Definition. Let $Y \subset X$ be a closed irreducible subset of a topological space X . We define the *codimension of X and Y* (denoted $\text{codim}(Y, X)$) to be the supremum of the lengths of increasing chains of irreducible closed subsets starting at Y , i.e. $Y \subseteq Z_1 \subset Z_2 \subset \dots \subset Z_n$. If Y is reducible and Z_i are the irreducible components, we set $\text{codim}(Y, X) = \inf_i(\text{codim}(Z_i, X))$.

In particular, we have $\text{codim}(\mathcal{V}(\mathfrak{p}), \text{Spec}(A)) = \text{ht}(\mathfrak{p})$.

1.7. Example.

- (1) Let A be the zero-ring, $A = 0$. In this case A has no prime ideals, hence we set conventionally $\dim(\text{Spec}(A)) = -1$.
- (2) Let A be a ring with only one prime \mathfrak{m} (hence $\mathfrak{m} = \text{Nil}(A)$). Then $\text{Spec}(A) = \{\mathfrak{m}\}$ and $\dim(A) = 0$.
- (3) Let $A = \mathbb{Z}$ or $A = k[X]$ for a field k . They are both PID, hence (0) is prime and every non zero prime is maximal: hence a chain in A has, at most, length 1 and this implies $\dim(A) = 1$. The same argument applies in any principal ideal domain that is not a field. A local ring A which is a PID is actually a local domain. In this case $\text{Spec}(A) = \{\eta, x\}$, where η is the generic point which corresponds to the prime (0) and x is the closed point corresponding to the maximal ideal \mathfrak{m} . Two examples of such rings are \mathbb{Z} localized at a prime p and the ring of formal power series $A = k[[X]]$.

1.8. Exercise. Remember that a topological space is called connected if there do not exist $X_1, X_2 \subset X$ closed subsets such that $X = X_1 \sqcup X_2$, $X_1 \cap X_2 = \emptyset$ and $X_i \neq \emptyset$ for $i = 1, 2$. Otherwise X is called disconnected. Show that the ring A is disconnected iff the ring A is a direct product $A \simeq A_1 \times A_2$ with $A_i \neq \{0\}$ for $i = 1, 2$.

PROOF. First suppose that A is a direct product. Then, for all $\mathfrak{p} \in \text{Spec}(A)$ we have a map $\pi: A_1 \times A_2 \rightarrow A/\mathfrak{p}$ and A/\mathfrak{p} is domain. Now consider the elements $e_1 = (1, 0)$ and $e_2 = (0, 1)$. We have $e_1 + e_2 = 1$, $e_1 e_2 = 0$, $e_1^2 = e_1$ and finally $e_2^2 = e_2$. Since π is a homomorphism of rings, we get the two equations $\pi(e_1) + \pi(e_2) = 1$ and $\pi(e_1)\pi(e_2) = 0$: being A/\mathfrak{p} a domain, this implies that $\pi(e_1) = 0$ or $\pi(e_2) = 0$. In the first case we have $\pi(a_1, 0) = 0$ for all $a_1 \in A_1$ and hence we have that the prime \mathfrak{p} of A is of the form $A_1 \times \mathfrak{p}_2$ for $\mathfrak{p}_2 \in \text{Spec}(A_2)$. Similarly, in the second case we obtain $\mathfrak{p} = \mathfrak{p}_1 \times A_2$ for $\mathfrak{p}_1 \in \text{Spec}(A_1)$. Hence we have $\text{Spec}(A) = \{A_1 \times \mathfrak{p} \text{ (resp. } \mathfrak{p} \times A_2) \mid \mathfrak{p} \subset A_2 \text{ (resp. } \mathfrak{p} \subset A_1) \text{ is prime}\}$, that is $\text{Spec}(A) = \text{Spec}(A_1) \sqcup \text{Spec}(A_2)$. Notice that $A_1 = (A_1 \times A_2)/[(A_1 \times A_2) \cdot (0, 1)]$, hence $\text{Spec}(A_1) = \mathcal{V}((0, 1)) := X_1$ and, in the same way, $\text{Spec}(A_2) = \mathcal{V}((1, 0)) := X_2$. X_1 and X_2 are non empty (since $A_i \neq \{0\}$), closed, disjoint subsets of X , which implies X disconnected.

Vice versa, suppose $X = X_1 \sqcup X_2$ for $X_i \neq \emptyset$, $X_i \subset X$ closed ($i = 1, 2$). Hence $X_i = \mathcal{V}(I_i)$ for a proper ideal $I_i \subset A$. So we have $X = X_1 \cup X_2 = \mathcal{V}(I_1 \cap I_2)$, therefore $\sqrt{I_1 \cap I_2} = \sqrt{0} = \text{Nil}(A)$. Equivalently, for all $a \in I_1 \cap I_2$, there exists $m \in \mathbb{N}$ such that $a^m = 0$. We also know that $\mathcal{V}(I_1 + I_2) = X_1 \cap X_2 = \emptyset$ and so I_1 and I_2 are coprime, i.e. $I_1 + I_2 = A$ (otherwise, by Zorn's lemma, there would be a maximal ideal \mathfrak{m} s.t. $I_1 + I_2 \subseteq \mathfrak{m} \subset A$ that would provide a point in $\mathcal{V}(I_1 + I_2)$).

Using this fact, we can find two elements, say a_1, a_2 in I_1, I_2 resp. such that $a_1 + a_2 = 1$. Since $a_1 a_2 \in I_1 I_2 \subset I_1 \cap I_2$, there exists $n \in \mathbb{N}$ such that $a_1^n a_2^n = 0$. But now we have $\mathcal{V}(a_1) = \mathcal{V}(a_1^n) \supseteq \mathcal{V}(I_1) = X_1$ and $\mathcal{V}(a_2) = \mathcal{V}(a_2^n) \supseteq \mathcal{V}(I_2) = X_2$. It also holds that $\mathcal{V}(a_1^n) \cap \mathcal{V}(a_2^n) = \mathcal{V}(a_1) \cap \mathcal{V}(a_2) = \mathcal{V}(a_1 + a_2) = \mathcal{V}(1) = \emptyset$ and so, since $X_1 \sqcup X_2 = X$, it follows that $\mathcal{V}(a_1^n) = X_1$ and $\mathcal{V}(a_2^n) = X_2$. In conclusion, we have two coprime ideals (a_1^n) and (a_2^n) with $a_1^n a_2^n = 0$. Thus, by the Chinese Remainder Theorem, we have that the map $A \rightarrow A/(a_1^n) \times A/(a_2^n)$ is an isomorphism. \square

2. Rings of dimension 0

From now on, assume that A is a Noetherian ring and that $\dim(A) = 0$. Thus there is just one prime (=maximal) ideal \mathfrak{m} and $0 \subseteq \mathfrak{m} \subseteq A$. Then we have two possible cases: if (0) is prime we have no more ideals: A must be a field and we don't have much more to say. So let's turn to the interesting case and suppose that (0) is not prime.

Since we are assuming the Noetherian hypothesis, we have a primary decomposition of $(0) = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_n$. By passing to the radicals, we obtain $\sqrt{0} = \text{Nil}(A) = \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_n$ for $\mathfrak{m}_i = \sqrt{\mathfrak{q}_i}$ maximal ideals. Therefore, since $\text{Nil}(A) = \bigcap_{\mathfrak{p} \in \text{Spec}(A)} \mathfrak{p}$, we have established the following result:

2.1. Lemma. *Let A be a Noetherian ring of dimension 0. Then A is a field or it has a finite number of prime (=maximal) ideals.*

Indeed, if \mathfrak{m} is a maximal ideal, then $\mathfrak{m} \supset (0)$, hence $\mathfrak{m} \supseteq \mathfrak{m}_k$ for some k and so, being \mathfrak{m}_k maximal, $\mathfrak{m}_k = \mathfrak{m}$.

Now we apply the corollary to prop. 2.1:

$$(0) = (\text{Nil}(A))^N = \left(\bigcap_{i=1}^n \mathfrak{m}_i \right)^N \supseteq \prod_{i=1}^n \mathfrak{m}_i^N$$

and then we have that $\mathfrak{m}_1^N \mathfrak{m}_2^N \dots \mathfrak{m}_n^N = 0$. This information is crucial, since we can determine explicitly a structure theorem for the ring:

2.2. Lemma. *Let A be as above and let $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ the distinct primes of A . Then*

$$A \simeq \bigoplus_{i=1}^n A/\mathfrak{m}_i^N$$

PROOF. Set $I_i = \mathfrak{m}_i^N$ for $i = 1, \dots, n$. We claim that, for $i \neq j$, $I_i + I_j = A$ (i.e. they are pairwise coprime). Assuming this, we have that

$$(2.1) \quad \bigcap_{i=1}^n I_i = \prod_{i=1}^n I_i = 0$$

and then, by the Chinese Remainder Theorem, we obtain the thesis. Hence we have to prove the claim. Since the primes \mathfrak{m}_j are maximal, it is enough¹ to show that if \mathfrak{p} and \mathfrak{q} are (distinct) maximal ideals in A , then $\mathfrak{p}^a + \mathfrak{q}^b = A$ for all $a, b \geq 1$. We will do induction on a and b . Clearly we have $\mathfrak{p} + \mathfrak{q} = A$. Then $\mathfrak{p}^a = \mathfrak{p}^a A = \mathfrak{p}^a(\mathfrak{p} + \mathfrak{q}) \subset \mathfrak{p}^{a+1} + \mathfrak{q}$, and so $\mathfrak{p}^a + \mathfrak{q} \subset \mathfrak{p}^{a+1} + \mathfrak{q}$. Hence (since $\mathfrak{p}^{a+1} \subset \mathfrak{p}^a$), we have $\mathfrak{p}^a + \mathfrak{q} = \mathfrak{p}^{a+1} + \mathfrak{q}$: by induction on a we obtain $\mathfrak{p}^a + \mathfrak{q} = \mathfrak{p} + \mathfrak{q} = A$. We can argue in a similar way for \mathfrak{q} and b to conclude. \square

2.3. Remark. Notice that each term A/\mathfrak{m}_i^k in the decomposition of A is, at least (it can be a field) a local ring with just one maximal ideal, that is the quotient $\mathfrak{m}_i/\mathfrak{m}_i^k$. Moreover, they are all Noetherian.

We now introduce a new class of rings:

2.4. Definition. Let A be a ring. A is called *Artinian* if it satisfies the *descending chain condition on ideals* (shortly d.c.c.); that is, A is Artinian if every descending chain of ideals is stationary.

We see that a ring is Artinian if it satisfies a condition that is the dual to the Noetherian one. It's easy to show that any quotient of an Artinian ring is artinian. Artinian rings will provide a non-trivial class of examples. In particular, we will show that a local Noetherian ring of dimension zero is Artinian. We first begin with the following proposition:

2.5. Proposition. *An Artinian ring A is such that every prime is maximal.*

Let \mathfrak{p} be a prime ideal, $\mathfrak{p} \subset A$. Then the quotient A/\mathfrak{p} is an artinian domain: the proposition is then equivalent to the following

2.6. Lemma. *Let D be an Artinian domain (i.e. an Artinian ring which is also an integral domain), then D is a field.*

PROOF. Let $x \in D$, $x \neq 0$ and consider the chain of ideals $(x) \supset (x^2) \supset \dots \supset (x^n) \supset \dots$. By the descending chain condition we have $(x^n) = (x^{n+1})$ for some n , therefore there exists $y \in D$ s.t. $x^n = x^{n+1}y$. Being D an integral domain (and $x \neq 0$), it follows that $1 = xy$. Thus we have found an inverse for x in D , which is therefore a field. \square

2.7. Proposition. *Let A be a ring such that the zero ideal is a product of maximal ideals, i.e. $0 = \mathfrak{m}_1 \cdots \mathfrak{m}_n$. Then A is Artinian iff is Noetherian.*

PROOF. See [2], Corollary 6.11. \square

In a Noetherian ring, the a.c.c. implies that every non-empty family of ideals, ordered by inclusion, admits a maximal elements. In a similar way it's possible to prove that in an Artinian ring, every non-empty family of ideals (again ordered by inclusion), admits a minimal element. As a consequence, we have the following results:

2.8. Proposition. *An Artinian ring has finitely many maximal ideals.*

PROOF. Let $\mathcal{S} = \{\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r \mid \mathfrak{m}_i \in \text{Max}(A), r \in \mathbb{N}\}$ be the set of finite intersections of maximal ideals. Hence there is a minimal element, say $\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_n$. This implies that, for all maximal ideal $\mathfrak{m} \subset A$, $\mathfrak{m} \cap (\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_n) = \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_n$ (since $\mathfrak{m} \cap (\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_n) \subseteq \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_n$ that is minimal by assumption). Therefore $\mathfrak{m} \supset \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_n$ and then, by the usual argument, $\mathfrak{m} \supset \mathfrak{m}_i$ for some i . Being \mathfrak{m}_i maximal, it follows that $\mathfrak{m} = \mathfrak{m}_i$. \square

¹Indeed, this is more than what we need to conclude the proof.

2.9. Proposition. *In an Artinian ring, the nilradical $\text{Nil}(A)$ is nilpotent.*

PROOF. Consider the descending chain given by

$$\text{Nil}(A) \supset (\text{Nil}(A))^2 \supset \dots \supset (\text{Nil}(A))^k \supset \dots$$

Being A Artinian, it follows that the chain stabilizes, that is for some $k > 0$ we have $I = (\text{Nil}(A))^k = (\text{Nil}(A))^{k+1} = \dots$. Suppose that $I \neq (0)$ and let \mathcal{S} be the set of all ideals J such that the product $IJ \neq (0)$. Then $\mathcal{S} \neq \emptyset$, since $I \in \mathcal{S}$ (being $I^2 = (\text{Nil}(A))^{2k} = I \neq (0)$ and $2k > k$), and we can find a minimal element H . Then there exists an element $x \in H$ such that $xI \neq (0)$ (hence $x \neq 0$). Being $(x) \subseteq H$ we have that $H = (x)$, by the minimality of H . But then we have that $(xI)I = xI^2 = xI \neq 0$ so $(xI) \in \mathcal{S}$ and, again by the minimality of H , $H = (x) = xI$. Therefore, there exists an element $y \in I$ such that $x = xy$. Thus we have

$$x = xy = xy^2 = \dots = xy^n = \dots$$

Moreover, $y \in I = \text{Nil}(A)^k$, then $y \in \text{Nil}(A)$ and so y is nilpotent. As a consequence, there exists $m > 0$ such that $x = xy^m = 0$, which is then a contradiction. \square

2.10. Proposition. *Let A be a ring. Then A is Artinian if and only if A is Noetherian and $\dim(A) = 0$.*

PROOF.

(\Leftarrow) We have already seen that if A is Noetherian of dimension 0, then A has only finitely many prime= maximal ideals and that the nilradical $\text{Nil}(A)$ is nilpotent. Let $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ be the set of the distinct prime ideals of A . Again we have that

$$(0) = (\text{Nil}(A))^k = \left(\bigcap_{i=1}^n \mathfrak{m}_i\right)^k \supset \prod_{i=1}^n \mathfrak{m}_i^k.$$

Then, by proposition 2.7, we have that A is Artinian.

(\Rightarrow) Since every prime ideal is maximal (by the previous proposition), the dimension of the ring must be 0. Let $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ be the set of the distinct maximal ideals of A . By the same argument of the converse implication, we have that $\prod_{i=1}^n \mathfrak{m}_i^k = (0)$ and, again by proposition 2.7, we have that A is Noetherian. \square

Indeed, we have a stronger result for a Noetherian ring which is local.

2.11. Proposition. *Let A be a local Noetherian ring. Then the following are equivalent:*

- i) $\dim(A) = 0$;
- ii) $\text{Nil}(A) = \mathfrak{m}$ (where \mathfrak{m} is the unique maximal ideal of A);
- iii) There exists $k > 0$ such that $\mathfrak{m}^k = 0$;
- iv) A is an Artinian ring.

PROOF. If A is a local ring, then all the elements of $A \setminus \mathfrak{m}$ are units. If $\dim(A) = 0$, then \mathfrak{m} is the unique prime ideal of A . Being the nilradical $\text{Nil}(A)$ equal to the intersection of all primes, we have then that $\text{Nil}(A) = \mathfrak{m}$. Hence i) \Rightarrow ii). Similarly, if $\text{Nil}(A) = \mathfrak{m}$, we have that \mathfrak{m} is the unique prime ideal of A which has then dimension 0. Thus we have proved i) \Leftrightarrow ii). Being A Noetherian, we have already proved that the nilradical is

nilpotent and, hence, ii) \Rightarrow iii). Now we show that iii) \Rightarrow iv). Suppose then that (A, \mathfrak{m}) is a local Noetherian ring and that $\mathfrak{m}^k = 0$ for some k .

Notice that, for each $r \geq 1$, the module $M = \mathfrak{m}^r$ is a finitely generated A -module (since A is Noetherian). Then² we have that $M/(\mathfrak{m}M)$ is a finite dimensional k -vector space, where $k = A/\mathfrak{m}$ is the residue field. Let now $(I_n)_{n \in \mathbb{N}}$ be a descending chain of ideals. Hence we have an inclusion of k -vector spaces

$$\dots \subseteq (I_n \cap \mathfrak{m}^r)/(\mathfrak{m}^{r+1} \cap I_n) \subseteq \dots \subseteq (I_0 \cap \mathfrak{m}^r)/(\mathfrak{m}^{r+1} \cap I_0) \subseteq \mathfrak{m}^r/\mathfrak{m}^{r+1} = M/\mathfrak{m}M$$

for all n . We have then built a descending chain of finite dimensional k -vector space that is, then, stationary: in fact, if $V' \subsetneq V$, then $\dim(V') < \dim(V)$ and so the chain is bounded by the dimensions. This implies that there exists $N > 0$ such that for every $n \geq N$ and for every $r \leq k$, $I_n \cap \mathfrak{m}^r \subseteq I_{n+1} + I_n \cap \mathfrak{m}^{r+1}$. Hence we have

$$I_n \subseteq I_{n+1} + I_n \cap \mathfrak{m} \subseteq \dots \subseteq I_{n+1} + I_n \cap \mathfrak{m}^k = I_{n+1}$$

since $\mathfrak{m}^k = 0$. But the chain $(I_n)_n$ was descending, then we have also $I_{n+1} \subseteq I_n$ and then we have the equality $I_n = I_{n+1}$. Hence A is Artinian. Finally, by proposition 2.10, we have that iv) \Leftrightarrow i) and this completes the proof. \square

2.12. Remark. Let (A, \mathfrak{m}) be a local Noetherian ring and consider the descending chain of ideals given by $\mathfrak{m}^k \supset \mathfrak{m}^{k+1} \supset \dots$. If this is stationary, then $\mathfrak{m}^n = \mathfrak{m}^{n+1}$ for some n , that is (if we denote with M the A -module \mathfrak{m}^n) $M = \mathfrak{m}M$. This implies, by Nakayama's lemma, that $M = 0$ and then $\dim(A) = 0$ by the previous proposition.

Let's come back to the decomposition given by 2.1 for a Noetherian ring A of dimension 0. We have already observed (see rmk. 2.3) that each term A/\mathfrak{m}_j^k is a local Noetherian ring with maximal ideal $\mathfrak{m}_j/\mathfrak{m}_j^k$. Clearly we have $(\mathfrak{m}_j/\mathfrak{m}_j^k)^k = (0)$ and then, by the previous proposition, this implies that A/\mathfrak{m}_j^k is Artinian. Hence we have proved the following:

2.13. Theorem. *A Noetherian ring of dimension zero is a finite product of local Artinian rings (and conversely).*

2.14. Proposition. *Let (A, \mathfrak{m}) be a Noetherian local ring of dimension 0. Then the following are equivalent:*

- i) *Every ideal is principal.*
- ii) *The maximal ideal \mathfrak{m} is principal.*
- iii) *Let $k = A/\mathfrak{m}$ the residue field. Then $\dim_k(\mathfrak{m}/\mathfrak{m}^2) \leq 1$.*

2.15. Remark. The Noetherian hypothesis implies that \mathfrak{m} is finitely generated, hence we certainly have $\dim_k(\mathfrak{m}/\mathfrak{m}^2) < +\infty$.

PROOF. Clearly i) \Rightarrow ii). If $\mathfrak{m} = (x)$ then the vector space $\mathfrak{m}/\mathfrak{m}^2$ has (at most) one generator: $\dim_k(\mathfrak{m}/\mathfrak{m}^2)$ is then equal to 1 if $\mathfrak{m} \neq 0$ and is equal to zero otherwise (in that case A is a field). To see that iii) \Rightarrow ii) we consider the two different cases $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$ and $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 0$. The latter implies $\mathfrak{m} = \mathfrak{m}^2$ and then, by Nakayama's lemma,

²This is a consequence of the following general fact: let A be a ring, $I \subset A$ an ideal and M an A -module: then we have an isomorphism $A/I \otimes_A M \simeq M/IM$. This can be proved using the right-exactness of the tensor product. Thanks to this isomorphism, we have that M/IM has a natural structure of A/I module.

we have $\mathfrak{m} = 0$ and again A is a field. If $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$ then the module $\mathfrak{m} = M$ is generated by one element, say x (that is such that \bar{x} is a basis for $\mathfrak{m}/\mathfrak{m}^2$ as k -vector space). Therefore $\mathfrak{m} = (x)$ is principal. Actually, we can use this fact to show that every ideal is principal (and so we have iii) \Rightarrow ii) \Rightarrow i)). Take $(0) \neq I \subsetneq A$ a proper ideal of A . Then $I \subset \mathfrak{m}$ and also $\sqrt{I} = \mathfrak{m}$ (since \mathfrak{m} is the only prime ideal of the ring). Moreover, \mathfrak{m} is nilpotent and therefore, since $I \neq (0)$, there exists an integer r such that $I \subseteq \mathfrak{m}^r = (x^r)$ but $I \not\subseteq \mathfrak{m}^{r+1} = (x^{r+1})$; hence there exists $t \in I$ such that $y = ax^r$ (i.e. $y \in (x^r)$) but $y \notin (x^{r+1})$, i.e. $a \notin (x)$. So a is a unit in A and consequently we have $x^r \in I$ that implies $I = (x^r)$. Hence I is principal. \square

2.16. Remark. Actually, we have proved not only that every ideal in A is principal, but also that it is a power of the maximal ideal \mathfrak{m} .

2.17. Example. There are several examples of local Artinian rings (that are, thanks to proposition 2.10, exactly the local Noetherian rings of dimension 0) that satisfy the conditions of the proposition 2.14. For instance, we can consider $\mathbb{Z}/(p^n)$ for p prime. It's clearly an Artinian ring (as is every finite ring!) and the maximal ideal $\mathfrak{m} = (p)/(p^n)$ is principal. Another example is given by $A = k[X]/(f^n)$ for a field k and an irreducible polynomial f : again A is local, Noetherian and it has dimension 0 (it has just one prime ideal, that is $(f)/(f^n)$) and the maximal ideal is principal.

However, this is not always true: there exist local Artinian rings such that the maximal ideal \mathfrak{m} is not generated by 1 element. Consider the ring $A = k[X^2, X^3]/(X^4)$: it's a local ring. In fact all the ideals of A correspond to ideals of $k[X^2, X^3]$ that contain (X^4) , and there exist only one such ideal that is maximal: it's exactly (X^2, X^3) . Hence $\mathfrak{m} = (\bar{X}^2, \bar{X}^3)$ (where we denote by \bar{f} the class of $f \pmod{X^4}$) is the unique maximal ideal of A . A has dimension 0 (since there are no more primes!) but \mathfrak{m} is not principal. Moreover, since $\mathfrak{m}^2 = 0$, we have $\dim(\mathfrak{m}/\mathfrak{m}^2) = 2$.

Valuations, normal rings and integral extensions

1. Normal rings and integral extensions

In this section we will prove some results about integral dependence. In particular we study important results concerning prime ideals in an integral extension. We begin with an important integral criterion, stated in the most general form. Let's start with the following definition.

1.1. Definition. Let A be a ring, and $R \subseteq A$ be a subring of A . An element α of A is said to be *integral over R* if there exists a monic polynomial $f \in R[X]$ such that $f(\alpha) = 0$. We say that A is *integral over R* if every element of A is integral over R .

Let $R \xrightarrow{f} A$ be an R -algebra. We recall that the product between an element $r \in R$ and an element of $a \in A$, denoted by $r \cdot a$, is by definition $f(r)a$ (product in A). Moreover, we say that an element $\alpha \in A$ is *integral over R* if whenever α satisfies an equation

$$(1.1) \quad \alpha^n + a_1\alpha^{n-1} + \dots + a_n = 0,$$

then $a_i \in R$ for all $i = 1, \dots, n$. As usual, we will not mention explicitly the map f .

1.2. Remark. For an element $\alpha \in A$, we gave a definition of being integral over a subring R of A . For an R -algebra A , this is equivalent to the previous one if we consider the subring $f(R)$.

1.3. Theorem. Let $R \xrightarrow{f} A$ be an R -algebra. Let $\alpha \in A$. Then the following are equivalent:

- i) $\alpha \in A$ is integral over R .
- ii) The subalgebra $R[\alpha]$ of A generated by α is a finitely generated R -module.
- iii) There is an $R[\alpha]$ -module M which is faithful (i.e. $\text{Ann } M = 0$)¹ and which is a finitely generated R -module.

PROOF. For i) \Rightarrow ii), we write² the algebra $R[\alpha]$ as $R + R\alpha + R\alpha^2 + \dots$ (generated by the powers of α). Being α integral over R , we may write (using the notation of (1.1)):

$$\alpha^{n+r} = -(a_1\alpha^{n+r-1} + \dots + a_n\alpha^r)$$

for all r . Hence we can use this relation repeatedly to express any power of α as a linear combination of $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$. To see ii) \Rightarrow iii), take $M = R[\alpha]$. M is clearly faithful as $R[\alpha]$ -module (remember that any ring R is faithful as R -module). Finally we show that iii) \Rightarrow i). Let m_1, \dots, m_r be generators of M as R -module (hence as an $R[\alpha]$ -module). Since M is an $R[\alpha]$ -module, we can express αm_i as a linear combination of m_j with

¹Recall that if $M \in \mathbf{Mod}_A$, then $\text{Ann } M = \{a \in A \mid am = 0 \text{ for all } m \in M\}$.

²Notice that this is always true, even if α is not integral over R .

coefficients in the ring R . Set $\alpha m_i = \sum_{j=1}^r a_{ij} m_j$, $\alpha_{ij} \in R$ for $i = 1, \dots, r$. This condition is equivalent to the following linear system:

$$(1.2) \quad (\alpha I - (a_{ij})_{i,j}) \begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} = 0,$$

where I denotes the identity matrix in $M_{r,r}(R[\alpha])$ (square matrices with entries in the ring $R[\alpha]$). We can then define a matrix $(b_{ij}) = (\alpha I - (a_{ij})_{i,j}) \in M_{r,r}(R[\alpha])$ and set $\beta = \det(b_{ij})$. Now let (B_{ij}) be the adjoint matrix of (b_{ij}) (i.e. the square matrix such that $(B_{ij})(b_{ij}) = (b_{ij})(B_{ij}) = \beta I$). If we denote with (m) the column vector of $(m_i)_{i=1,\dots,r}$, we can multiply (1.2) by (B_{ij}) and thus obtain $\beta I(m) = 0$, i.e. $\beta m_i = 0$ for all $i = 1, \dots, r$. Hence β is an element of $R[\alpha]$ such that $\beta \cdot M = 0$, and so $\beta \in \text{Ann } M = (0)$, that is $\beta = 0$. Being $\beta = \det(b_{ij})$, this express the fact that α is a root of the characteristic polynomial of the matrix $(a_{ij}) \in M_{r,r}(R[\alpha])$, which is monic. Hence α is integral over R . \square

This result brings us the following definition

1.4. Definition. A ring homomorphism $A \xrightarrow{f} B$ is called *integral* or we say that B is integral over A if and only if for all $b \in B$, b is integral over A in the sense of the theorem.

1.5. Corollary. *The property of being integral is stable under composition, i.e. if we have maps $R \rightarrow A \rightarrow B$ with A integral over R and B integral over A , then B is integral over R .*

PROOF. For all $\beta \in B$, we have an integral equation for β , i.e. $\beta^n + \alpha_1 \beta^{n-1} + \dots + \alpha_n = 0$ with coefficients $\alpha_i \in A$. Moreover, being A integral over R , the elements α_i satisfy integral equations over R , $\alpha_i^{n_i} + a_{1,i} \alpha_i^{n_i-1} + \dots + a_{n_i,i} = 0$ for all i . Now, we can consider the subalgebra $R[\alpha_1, \dots, \alpha_n, \beta]$ generated over R by the elements α_i and β . This is a finitely generated R -module (by induction on n)³ and it is also a faithful $R[\beta]$ -module (since it contains $R[\beta]$). Therefore, by the theorem, β is integral over R . \square

1.6. Corollary. *Let $R \rightarrow A$ be an R -algebra. The set of elements of A which are integral over R is a subring of A .*

PROOF. Let α and β be elements of A , integral over R . Then the algebra $R[\alpha, \beta]$ is a finitely generated R -module (by the previous remark). Hence $\alpha \pm \beta$ and $\alpha\beta$ are integral over R . \square

Let R be a ring and A be an R -algebra. Then we can consider the ring of all elements of A that are integral over R . This ring, subring of A (as we have just seen), is called the *integral closure*, or *normalization* of R in A . The most important examples occur when R is an integral domain and A is its field of fractions. In this case the sub-algebra of elements of A integral over R is simply called the *normalization of R* . A domain that is equal to its normalization is called a *normal domain*.

1.7. Exercise. Let R be a unique factorization domain. Show that R is normal.

³In general, let $A \subset B$. If $1 \leq \alpha_i \leq n$ are elements of B , integral over A , then the ring $A[\alpha_1, \dots, \alpha_n]$ is a finitely-generated A -module. The proof is by induction on n : the case $n = 1$ is part of theorem 1.3.

PROOF. Indeed, let $k = \text{Frac}(R)$ and let $\alpha = \frac{r}{s}$ be an element of k , integral over R . We can assume that $(r, s) = 1$ (i.e. r, s coprime). Then α satisfies a monic equation

$$\alpha^n + a_1\alpha^{n-1} + \dots + a_n = 0 \quad a_i \in R$$

$$\left(\frac{r}{s}\right)^n + a_1\left(\frac{r}{s}\right)^{n-1} + \dots + a_n = 0 \quad a_i \in R.$$

Suppose by contradiction that $\frac{r}{s} \in k \setminus R$ (hence s is not a unit in R). If we multiply the above equation by s^n , we obtain $r^n + a_1r^{n-1}s + \dots + a_ns^n = 0$, hence $r^n = -(a_1r^{n-1} + \dots + a_ns^{n-1})s$, i.e. $s \mid r$ (by unique factorisation), contradicting $(r, s) = 1$. \square

1.8. Example. Let k and consider the ring $A = k[t^2, t^3] \subset B = k[t]$. Then the rings A and B have the same field of fractions $K = k(t)$. Moreover, \bar{t} is clearly integral over A but $t \notin A$, then A is not normal. Since the normalization \bar{A} of A must contain A and t , we have $B = k[t] \subseteq \bar{A}$. Since B is a UFD, it is normal, and so $\bar{A} = B$ is the integral closure of A in K .

Notice that $A \simeq k[X, Y]/(Y^2 - X^3)$, thus A is the coordinate ring of the algebraic set $\mathcal{C} = Z(I)$, where I is the principal ideal generated by $f(X, Y) = Y^2 - X^3$. The plane curve $Y^2 = X^3$ has a singularity at the origin. The fact that A is not normal is closely related to the existence of that singularity. We will consider again this important example.

1.9. Proposition. *Let A be a normal domain and let $K = \text{Frac}(A)$ be its field of fractions. Let L be an algebraic extension of K . Then an element $\alpha \in L$ is integral over A if and only if its minimal polynomial over K has all its coefficients in A .*

PROOF. See [7], Theorem 9.2. \square

1.10. Example (From [7]). Let A be a UFD in which 2 is a unit. Let $f \in A$ be square-free, (i.e. f is not divisible by the square of any prime of A). Then the ring $A[\sqrt{f}]$ is normal.

PROOF. Let K be the field of fractions of A and let α be a square root of f in the algebraic closure of K . Being A a UFD, by exercise 1.7, it is integrally closed in K . Hence, if $\alpha \in K$, we have $\alpha \in A$, then $A[\alpha] = A$, and the assertion is trivial. Suppose then that $\alpha \notin K$. Then α is algebraic over K and the field of fractions of $A[\alpha]$ is $K(\alpha) = K \oplus K\alpha$. Hence, every element $t \in K(\alpha)$ can be written in a unique way as $t = x + y\alpha$ with $x, y \in K$. It's easy to see that the minimal polynomial of t over K is $X^2 - 2xX + (x^2 - y^2f)$, so that using the previous proposition, if t is integral over A , we get $2x \in A$ and $x^2 - y^2f \in A$. By assumption, $2x \in A$ implies $x \in A$, since 2 is a unit. Hence $y^2f \in A$. Let $y = \frac{a}{b}$ with $a, b \in A$. If some prime p of A divides the denominator b of y , we get that $p^2 \mid f$, contradicting the square-free hypothesis. Therefore $y \in A$ and so $t \in A \oplus A\alpha = A[\alpha]$, so that $A[\alpha]$ is integrally closed in $K(\alpha)$. \square

1.11. Proposition. *Let A be a normal ring in which there is only one non-zero prime ideal, say \mathfrak{m} . Suppose that \mathfrak{m} is finitely generated: then \mathfrak{m} is principal.*

PROOF. Let $a \in \mathfrak{m} \setminus \{0\}$ and consider the ideal (a) generated by a . Then the radical $\sqrt{(a)}$ is equal to \mathfrak{m} (being \mathfrak{m} the unique non-zero prime ideal of A). Since \mathfrak{m} is finitely generated, there exists a positive integer n such that $\mathfrak{m}^n \subset (a)$ but $\mathfrak{m}^{n-1} \not\subset (a)$; therefore, we can find an element $0 \neq b \in \mathfrak{m}^{n-1}$ but $b \notin (a)$. Now, in the field of fractions $k =$

$\text{Frac}(A)$, the element $x = \frac{a}{b} \in k$ is such that $x^{-1} \notin A$ (since $b \notin (a)$), and then it is not integral over A , being A integrally closed. Let $x^{-1}\mathfrak{m}$ be the image of the multiplication by x^{-1} on \mathfrak{m} in the field of fractions k .

Claim. $x^{-1}\mathfrak{m} \not\subseteq \mathfrak{m}$.

PROOF. If it was $x^{-1}\mathfrak{m} \subseteq \mathfrak{m}$, then \mathfrak{m} would be $A[x^{-1}]$ -module, since \mathfrak{m} is closed under multiplication by all powers of x^{-1} (and then under multiplication by all elements of $A[x^{-1}]$, being \mathfrak{m} also an A -module). Moreover, \mathfrak{m} is, by assumption, finitely generated as A -module; it's easy to see that it is faithful as $A[x^{-1}]$ -module, which implies x^{-1} integral over A , which is absurd. \square

Since $\mathfrak{m}^n \subset (a)$ any monomial M of degree $\geq n$ in the generators $\{m_i\}$ of $\mathfrak{m} = (m_1, \dots, m_r)$ is divisible by a . Then b is a polynomial of degree $n-1$ in $\{m_i\}$ and so, for all $i = 1 \dots, r$, we have $m_i \frac{b}{a} \in A$, since $m_i b$ is of degree n , so it is divisible by a . Therefore $mx^{-1} \in A$ for all $m \in \mathfrak{m}$, hence $x^{-1}\mathfrak{m} \subseteq A$. By the claim, $x^{-1}\mathfrak{m} = A$, hence $1 = \overline{m} \frac{b}{a}$ for some $\overline{m} \in \mathfrak{m}$; so we have $x = \frac{a}{b} = \overline{m} \in \mathfrak{m}$, and then $(x) \subseteq \mathfrak{m}$. Moreover, for every element $y \in \mathfrak{m}$, we have $y = (yx^{-1})x$ (and $yx^{-1} \in A$), so $y \in (x)$ and then, finally, $(x) = \mathfrak{m}$. \square

2. Further properties of integral extensions

2.1. Proposition. *Let A be a subring of a ring B and suppose that B is integral over A . Then we have:*

- i) *if $J \subseteq B$ is an ideal of B , then B/J is integral over A/I , where $I = A \cap J$.*
- ii) *Let S be a multiplicative set in A . Then $S^{-1}B$ is integral over $S^{-1}A$.*

PROOF. i) let $\bar{b} \in B/J$ be the class of $b \in B \text{ mod } J$. Then, by assumption, b is integral over A , therefore b satisfies a monic equation $b^n + a_1 b^{n-1} + \dots + a_n = 0$ with $a_i \in A$. Then, if we reduce mod J , we obtain $\bar{b}^n + \bar{a}_1 \bar{b}^{n-1} + \dots + \bar{a}_n = 0$, for $\bar{a}_i \equiv a_i \pmod{J}$. For ii), let $\frac{b}{s} \in S^{-1}B$, for $b \in B$ and $s \in S$. Hence b satisfies $b^n + a_1 b^{n-1} + \dots + a_n = 0$ ($a_i \in A$). If we multiply by s^{-n} we obtain the following equation for $\frac{b}{s}$

$$\left(\frac{b}{s}\right)^n + \frac{a_1}{s} \left(\frac{b}{s}\right)^{n-1} + \dots + \frac{a_n}{s^n} = 0$$

with $\frac{a_i}{s^i} \in S^{-1}A$ and so $\frac{b}{s}$ is integral over $S^{-1}A$. \square

2.2. Proposition. *Let A be a subring of a ring B . Let \overline{A} the integral closure of A in B . Then, for all multiplicative set $S \subset A$, we have that $S^{-1}\overline{A}$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.*

PROOF. By ii) of 2.1, $S^{-1}\overline{A}$ is integral over $S^{-1}A$, hence $S^{-1}\overline{A} \subset \overline{S^{-1}A}$. Conversely, if $\frac{b}{s}$ is integral over $S^{-1}A$, then it satisfies an equation of the form

$$\left(\frac{b}{s}\right)^n + \frac{a_1}{s_1} \left(\frac{b}{s}\right)^{n-1} + \dots + \frac{a_n}{s_n} = 0$$

for $a_i \in A$, $s_i \in S$. Let $t = s_1 \cdots s_n \in S$: then we have

$$(st)^n \left(\frac{b}{s}\right)^n + (st)^n \frac{a_1}{s_1} \left(\frac{b}{s}\right)^{n-1} + \dots + (st)^n \frac{a_n}{s_n} = 0.$$

If we clear denominators, we get $(tb)^n + ss_2 \cdots s_n t^{n-1} b^{n-1} + \dots + (s^n s_1 \cdots s_{n-1} t^{n-1}) a_n = 0$, therefore $tb \in \overline{A}$. Finally, since $\frac{bt}{st} = \frac{b}{s}$, we get $\frac{b}{s} \in S^{-1}\overline{A}$. \square

2.3. Corollary. *Let A be an integrally closed domain. Then $A_{\mathfrak{p}}$ is normal for any prime $\mathfrak{p} \in \text{Spec}(A)$.*

PROOF. Let $S = A \setminus \mathfrak{p}$ be the multiplicative set associated to the prime \mathfrak{p} and let K be the field of fractions $\text{Frac}(A)$. Then $S^{-1}\overline{A} = S^{-1}A = A_{\mathfrak{p}}$ is the integral closure of $A_{\mathfrak{p}}$ in the field of fractions $S^{-1}K = S^{-1}\text{Frac}(A) = K$. \square

Being normal for a ring A is a local property:

2.4. Proposition. *Let A be a domain. Then A is normal iff $A_{\mathfrak{p}}$ is normal for all $\mathfrak{p} \in \text{Spec}(A)$.*

PROOF. The previous corollary shows the “only if” part. Conversely, consider the inclusion $A \hookrightarrow \overline{A}$. For each prime \mathfrak{p} , let $S = A \setminus \mathfrak{p}$ be the corresponding multiplicative set. Then we have $A_{\mathfrak{p}} = S^{-1}A \hookrightarrow S^{-1}\overline{A}$ and, by assumption, $A_{\mathfrak{p}} \simeq \overline{A_{\mathfrak{p}}}$, that is the integral closure of $A_{\mathfrak{p}}$ in its field of fractions, $\text{Frac}(A_{\mathfrak{p}}) = \text{Frac}(A)$. Moreover, by proposition 2.1, we have that $\overline{A_{\mathfrak{p}}} = \overline{A_{\mathfrak{p}}} = S^{-1}\overline{A}$. Hence we have that, for each prime $\mathfrak{p} \in \text{Spec}(A)$, $A_{\mathfrak{p}} \simeq \overline{A_{\mathfrak{p}}}$ and this implies⁴ $A \simeq \overline{A}$. \square

We can refine the previous result in the following sense:

2.5. Proposition. *A is normal iff $A_{\mathfrak{m}}$ is normal for all $\mathfrak{m} \in \text{Max}(A)$*

PROOF. As above, we have already proved the “only if” part. Conversely, let $x \in \text{Frac}(A)$ which is integral over A and let $x^n + a_1 x^{n-1} + \dots + a_n = 0$ be the monic equation satisfied by x , with $a_i \in A \subset A_{\mathfrak{m}} \subset \text{Frac}(A)$ for each maximal ideal $\mathfrak{m} \subset A$. Hence x is also integral over $A_{\mathfrak{m}}$ for all $\mathfrak{m} \in \text{Max} A$. By assumption, $A_{\mathfrak{m}}$ is normal, and so $x \in A_{\mathfrak{m}}$ for all $\mathfrak{m} \in \text{Max} A$, that is $x \in \bigcap_{\mathfrak{m} \in \text{Max} A} A_{\mathfrak{m}}$. To complete the proof, we need the following lemma. \square

2.6. Lemma. *Let A be a domain, then*

$$A = \bigcap_{\mathfrak{p} \in \text{Spec}(A)} A_{\mathfrak{p}} = \bigcap_{\mathfrak{m} \in \text{Max} A} A_{\mathfrak{m}}.$$

PROOF. Since A is a domain, the map $A \rightarrow A_{\mathfrak{p}}$ is injective. Therefore we have $A \subset A_{\mathfrak{p}}$ for all $\mathfrak{p} \in \text{Spec}(A)$. Now, take $x = \frac{a}{b} \in K = \text{Frac}(A)$ and consider the ideal $I(x) := \{b \in A \mid bx \in A\} \subset A$. We have $x \notin A \iff I(x) \subsetneq A$. The ideal $I(x)$ is proper iff there exists a maximal ideal $\mathfrak{m} \subset A$ such that $\mathfrak{m} \supset I(x)$. So we get $x \notin A$ iff there exists a maximal ideal $\mathfrak{m} \in \text{Max}(A)$ such that $x \notin A_{\mathfrak{m}}$. In fact, if $x \in A_{\mathfrak{m}}$, then $x = \frac{a}{b}$ with $b \notin \mathfrak{m}$. But $b \in I(x) \subset \mathfrak{m}$, a contradiction. Hence we have that $A \supseteq \bigcap_{\mathfrak{m} \in \text{Max} A} A_{\mathfrak{m}} \supseteq \bigcap_{\mathfrak{p} \in \text{Spec}(A)} A_{\mathfrak{p}}$ and this completes the proof. \square

In the Noetherian case we can actually refine the result of lemma 2.6 in the following sense:

⁴Being isomorphic is a local property for A -modules.

2.7. Proposition. *Let A be a Noetherian domain, then*

$$A = \bigcap_{\mathfrak{p} \in I} A_{\mathfrak{p}}$$

where I is the set $I = \{\mathfrak{p} \in \text{Spec}(A) \mid \text{there exists } m \in A \text{ such that } \mathfrak{p} \text{ is maximal among the primes associated to } (m)\}$.

PROOF. Each localization clearly contains A , hence we need to show that A contains the intersection of $A_{\mathfrak{p}}$ where $\mathfrak{p} \in I$. Let $K := \text{Frac}(A)$ and let $b \in K$, $b = \frac{a}{u}$ for $a, u \in A$, $u \neq 0$. Suppose that $b \notin A$, i.e. $a \notin (u) \Leftrightarrow 0 \neq \bar{a} \in A/(u)$. Remember that there is a one to one correspondence between the primes of A associated to (u) and the primes of the quotient $A/(u)$ associated to (0) (if $\mathfrak{q} \subset A/(u)$ is an associated prime, then we get a prime of A associated to (u) by taking the inverse image of \mathfrak{q} via the projection $A \rightarrow A/(u)$). This correspondence preserves maximality. Consider now the ideal $\text{Ann}(\bar{a}) \subset A/(u)$. Being the quotient $A/(u)$ a Noetherian ring, there exists an ideal \mathfrak{q} of the form $\mathfrak{q} = \text{Ann}(\bar{m})$ which is maximal between the ideals containing $\text{Ann}(\bar{a})$. Then such \mathfrak{q} is maximal among the primes associated to (0) (show this as an exercise). Then we can localize at \mathfrak{q} the quotient $A/(u)$ and we can consider the image of \bar{a} via the natural map $\varphi: A/(u) \rightarrow (A/(u))_{\mathfrak{q}}$. Then $\varphi(\bar{a}) \neq 0$, since $\text{Ann}(\bar{a}) \subseteq \mathfrak{q}$. Let \mathfrak{p} be the ideal of A corresponding to \mathfrak{q} . We have that $\mathfrak{p} \in I$, since the correspondence preserves maximality. Moreover, we have that $\bar{a} \neq 0$ in $A_{\mathfrak{p}}/uA_{\mathfrak{p}} = (A/(u))_{\mathfrak{q}}$. Hence $a \notin uA_{\mathfrak{p}}$, i.e. $b = \frac{a}{u} \notin A_{\mathfrak{p}}$. In other words, we have shown that $b \in K$, $b \notin A$, then $b \notin A_{\mathfrak{p}}$ and this proves the other inclusion. \square

2.8. Exercise. Let A be a normal local domain with maximal ideal \mathfrak{p} such that there exists $u \in A$ such that \mathfrak{p} is maximal among the primes associated to (u) . Then A is a PID.

PROOF. The assumption is equivalent to the fact that there exists $m \in A$ such that $\bar{\mathfrak{p}}$ (=image of \mathfrak{p} in the quotient $A/(u)$) is the annihilator of \bar{m} , where $m \equiv \bar{m} \pmod{(u)}$. We set \mathfrak{p}^{-1} to be the A -module $\mathfrak{p}^{-1} := \{r \in k = \text{Frac}(A) \mid r\mathfrak{p} \subseteq A\}$: clearly $\mathfrak{p}^{-1} \supset A$. Moreover, we have $\mathfrak{p}^{-1}\mathfrak{p} \subseteq A$ and $\mathfrak{p}\mathfrak{p}^{-1} \supseteq \mathfrak{p}$. So $\mathfrak{p}^{-1}\mathfrak{p}$ is an ideal of A containing \mathfrak{p} . Since \mathfrak{p} is maximal, we have either $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$ or $\mathfrak{p}^{-1}\mathfrak{p} = A$. In the first case, for all $\alpha \in \mathfrak{p}^{-1}$, we can consider the multiplication map $k \xrightarrow{\cdot\alpha} k$. Notice that $\cdot\alpha$ sends \mathfrak{p} to itself, so \mathfrak{p} is also an $A[\alpha]$ -module. \mathfrak{p} is a finitely generated A module which is faithful as $A[\alpha]$ -module. Hence α is integral over A . Since A is normal, $\alpha \in A$ and so $\mathfrak{p}^{-1} = A$. But we know that there exist $u, m \in A$ such that $\mathfrak{p} = \{s \in A \mid sm \subseteq (u)\}$, hence $\frac{m}{u} \in \mathfrak{p}^{-1} = A$. Therefore $m \in (u)$ and so $\mathfrak{p} = A$, contradicting the assumption that \mathfrak{p} is the unique maximal ideal of A . Then we must have $\mathfrak{p}^{-1}\mathfrak{p} = A$, i.e. there exists $\alpha \in \mathfrak{p}^{-1}, \beta \in \mathfrak{p}$ such that $\alpha\beta = 1$. So $A \subseteq A\mathfrak{p} \subseteq A$, i.e. $A = \alpha\mathfrak{p}$. Hence $\mathfrak{p} = \beta A$ and so \mathfrak{p} is principal. \square

3. The going-up theorem

3.1. Proposition. *Let $A \subseteq B$ be integral domains and suppose that B is integral over A . Then B is a field iff A is a field.*

PROOF. First suppose that B is a field. If $0 \neq a \in A$, then $a^{-1} \in B$, so that a^{-1} is integral over A , i.e. there is a relation $a^{-n} + c_1 a^{-n+1} + \dots + c_n = 0$ with $c_i \in A$. Then we have $a^{-1} = -(c_1 + c_2 a + \dots + c_n a^{n-1}) \in A$. Conversely, suppose that A is a field and let

$0 \neq b \in B$. Then we have that b is integral over A and so there is a relation of the form $b^n + a_1 b^{n-1} + \dots + a_n = 0$ with $a_i \in A$. Since A is an integral domain, we can assume that $a_n \neq 0$. Therefore we have $b^{-1} = -a_n^{-1}(b^{n-1} + \dots + a_{n-1}) \in B$. \square

3.2. Corollary. *Let A be a subring of a ring B and suppose that B is integral over A . Let \mathfrak{q} be a prime ideal of B and let $\mathfrak{p} = \mathfrak{q} \cap A$. Then \mathfrak{q} is maximal iff \mathfrak{p} is maximal.*

PROOF. Notice that \mathfrak{p} is certainly prime, since \mathfrak{p} is $\iota^{-1}(\mathfrak{q})$ where ι is the inclusion $\iota: A \hookrightarrow B$ (so \mathfrak{p} is the contraction of \mathfrak{q} via the inclusion ι). Moreover, B/\mathfrak{q} is integral over A/\mathfrak{p} and they are both domains. Then, by 3.1, we have that B/\mathfrak{q} is a field iff A/\mathfrak{p} is a field, i.e. \mathfrak{q} is maximal iff \mathfrak{p} is maximal. \square

3.3. Proposition (Going-up theorem - first form). *Let A be a subring of a ring B and suppose that B is integral over A . Let \mathfrak{p} be a prime ideal of A . Then there exists a prime ideal \mathfrak{q} of B such that $\mathfrak{q} \cap A = \mathfrak{p}$, i.e. the map $\text{Spec}(B) \rightarrow \text{Spec}(A)$ is surjective.*

PROOF. Let $S = A \setminus \mathfrak{p}$ be the multiplicative set associated to the prime \mathfrak{p} . We have the following commutative diagram:

$$\begin{array}{ccc} A & \xrightarrow{\iota} & B \\ f \downarrow & & \downarrow g \\ A_{\mathfrak{p}} & \xrightarrow{\beta} & S^{-1}B \end{array}$$

where f and g are the canonical maps and the horizontal maps ι and β are injections. So $S^{-1}B \neq 0$ and we can take a maximal ideal $\mathfrak{m} \subset S^{-1}B$. Let now $\mathfrak{n} := \beta^{-1}(\mathfrak{m})$ be a prime ideal of $A_{\mathfrak{p}}$. Then, by 2.1, $S^{-1}B$ is integral over the local ring $A_{\mathfrak{p}}$. Therefore, by the previous corollary, \mathfrak{n} is maximal and so it is the unique maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$ of $A_{\mathfrak{p}}$. The diagram

$$\begin{array}{ccc} \text{Spec}(B) & \xrightarrow{\iota^*} & \text{Spec}(A) \\ g^* \uparrow & & \uparrow f^* \\ \text{Spec}(S^{-1}B) & \xrightarrow{\beta^*} & \text{Spec}(A_{\mathfrak{p}}) \end{array}$$

is commutative, since $\text{Spec}(-)$ is functorial, and so, if $\mathfrak{q} := g^*(\mathfrak{m})$, we have that $\mathfrak{p} = f^*(\mathfrak{p}A_{\mathfrak{p}}) = f^*(\mathfrak{n}) = f^*(\beta^*(\mathfrak{m})) = \iota^*(\mathfrak{q}) = \mathfrak{q} \cap A$. \square

From the going-up theorem we obtain the following important result of dimension theory.

3.4. Proposition. *Let $A \xrightarrow{\varphi} B$ be an A -algebra and let B integral over A . Let $\mathfrak{q} \in \text{Spec}(B)$ and $\mathfrak{p} = \varphi^{-1}(\mathfrak{q}) \in \text{Spec}(A)$. Then:*

- i) $\text{ht}(\mathfrak{q}) \leq \text{ht}(\mathfrak{p})$. In particular, $\dim B \leq \dim A$.
- ii) If φ is injective, then $\dim A_{\mathfrak{p}} = \dim B_{\mathfrak{q}}$ and $\dim A = \dim B$.

PROOF. i) We will show that for each chain $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \dots \subsetneq \mathfrak{q}_n = \mathfrak{q}$ of length n in B , we have a corresponding chain of length n in A given by $\varphi^{-1}(\mathfrak{q}_0) \subsetneq \dots \subsetneq \varphi^{-1}(\mathfrak{q}_n) = \mathfrak{p}$. This will imply that $\text{ht}(\mathfrak{q}) \leq \text{ht}(\mathfrak{p})$. Actually, it's enough to show that if $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1$ are distinct prime ideals of B , then $\varphi^{-1}(\mathfrak{q}_0) \subsetneq \varphi^{-1}(\mathfrak{q}_1)$. By replacing B by B/\mathfrak{q}_0 and A by $A/\varphi^{-1}(\mathfrak{q}_0)$, we may assume that A and B are domains, that $\mathfrak{q}_0 = (0)$ and that $\varphi^{-1}(\mathfrak{q}_0) = (0)$, i.e. that

φ is injective. Hence we have $\mathfrak{q}_1 \supsetneq (0)$ and we must show that $\varphi^{-1}(\mathfrak{q}_1) \neq (0)$. Let $0 \neq b \in \mathfrak{q}_1$. Then b is integral over A and we can consider the equation of integral dependence for b of smallest possible degree, say $b^n + a_1b^{n-1} + \dots + a_n = 0$. Then $a_n \neq 0$, since B is a domain (as in the proof of Proposition 3.1), and so $a_n = -b(b^{n-1} + \dots + a_{n-1}) \in (b) \subseteq \mathfrak{q}_1$. Hence $a_n \in \varphi^{-1}(\mathfrak{q}_1) \setminus \{0\}$.

For ii), recall that $\dim A_{\mathfrak{p}} = \text{ht}(\mathfrak{p}) = \text{codim}(\mathcal{V}(\mathfrak{p}), \text{Spec}(A))$. Hence, by i), it is enough to show the first equality. Let $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1$ be prime ideals of A . Let $\mathfrak{q}_0 \in \text{Spec}(B)$ be such that $\varphi^{-1}(\mathfrak{q}_0) = \mathfrak{p}_0$. By considering the injective integral homomorphism $A/\mathfrak{p}_0 \rightarrow B/\mathfrak{q}_0$, we obtain a prime ideal \mathfrak{q}_1 of B such that $\varphi^{-1}(\mathfrak{q}_1) = \mathfrak{p}_1$ and $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1$. By repeatedly applying this result to a chain of prime ideals of A containing \mathfrak{p} , we get $\dim A_{\mathfrak{p}} \leq \dim B_{\mathfrak{q}}$, and hence the equality since $A_{\mathfrak{p}} \rightarrow B_{\mathfrak{q}}$ is integral. Moreover, since $\dim A = \sup_{\mathfrak{p}}(\dim A_{\mathfrak{p}})$ for $\mathfrak{p} \in \text{Spec}(A)$, we can also deduce that $\dim A = \dim B$. \square

3.5. Exercise (Going-up theorem - second form). Let $A \subseteq B$ and suppose that B is integral over A . Show that if $\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \dots \subset \mathfrak{p}_n$ is a chain of prime ideals of A , and $\mathfrak{q}_1 \subset \mathfrak{q}_2 \subset \dots \subset \mathfrak{q}_m$ ($m < n$) is a chain of prime ideals of B such that \mathfrak{q}_i “lies over” \mathfrak{p}_i (i.e. $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for $1 \leq i \leq m$), then the second chain can be extended to $\mathfrak{q}_1 \subset \mathfrak{q}_2 \subset \dots \subset \mathfrak{q}_n$ so that this remains true, i.e. $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for $1 \leq i \leq n$.

To understand the geometric nature of integral extensions we should combine the going-up theorem with the following result:

3.6. Proposition. *Let $A \xrightarrow{f} B$ be a finitely generated A -algebra and let B be integral over A . Then the map $\text{Spec}(B) \rightarrow \text{Spec}(A)$ is finite-to-one.*

PROOF. Let $\mathfrak{p} \in \text{Spec}(A)$. The proposition tells us that the fibre $\{\mathfrak{p}_i\}_{i \in I}$ of \mathfrak{p} via the induced map $f^*: \text{Spec}(B) \rightarrow \text{Spec}(A)$ is a finite set. By definition, for all $i \in I$ we have $f^*(\mathfrak{p}_i) = f^{-1}(\mathfrak{p}_i) = \mathfrak{p}$. Let $S = A \setminus \mathfrak{p}$ be the multiplicative set associated to the prime \mathfrak{p} . Then, for all $s \in S$, $f(s) \notin \mathfrak{p}_i$ (otherwise $s \in f^{-1}(\mathfrak{p}_i) = \mathfrak{p}$) and we have the following commutative diagrams:

$$\begin{array}{ccc} B & \xrightarrow{\alpha} & S^{-1}B \\ f \uparrow & & \uparrow \\ A & \xrightarrow{e} & A_{\mathfrak{p}} \end{array} \quad \begin{array}{ccc} \text{Spec}(S^{-1}B) & \xrightarrow{\alpha^*} & \text{Spec}(B) \\ \downarrow & & \downarrow f^* \\ \text{Spec}(A_{\mathfrak{p}}) & \xrightarrow{e^*} & \text{Spec}(A) \end{array}$$

where, as usual, we denote by $S^{-1}B$ the localization of B with respect to the multiplicative set $f(S)$. As we noticed above, the primes of the fibre of \mathfrak{p} do not meet $f(S)$, hence they generate distinct prime ideals (say $\{S^{-1}\mathfrak{p}_i\}_{i \in I}$) in $S^{-1}B$. Moreover, if we consider the map $\text{Spec}(S^{-1}B) \rightarrow \text{Spec}(A_{\mathfrak{p}})$, we see (since $\text{Spec}(-)$ is functorial) that they lie over the maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$ of $A_{\mathfrak{p}}$. Thus it suffices to treat the case A local and $\mathfrak{p} = \mathfrak{m}$ its maximal ideal. Now, for any prime \mathfrak{q} of B such that $f^{-1}(\mathfrak{q}) = \mathfrak{m}$, we have $\mathfrak{m}B \subset \mathfrak{q}$ (where $\mathfrak{m}B$ denotes the ideal generated by $f(\mathfrak{m})$ in B). Hence \mathfrak{q} corresponds to a prime ideal of the quotient ring $B/\mathfrak{m}B$, which is a finite dimensional A/\mathfrak{m} -vector space and thus has only finitely many prime ideals. \square

4. Dimension and Codimension 1

In general, the normalization of a ring which is the coordinate ring of an algebraic set \mathcal{V} has the effect of sorting out certain irregularities of the varieties. This is a step toward a process of resolution of the singularities of \mathcal{V} . First, we need to give a definition of *regularity*.

4.1. Definition. Suppose that (A, \mathfrak{m}) is a local ring of dimension d . We say that A is *regular* if \mathfrak{m} can be generated by exactly d elements.

By Nakayama's lemma, a set of elements generates \mathfrak{m} iff the images of these elements generates $\mathfrak{m}/\mathfrak{m}^2$ as a A/\mathfrak{m} -vector space. So this vector space has dimension d iff A is regular.

Regular local rings play a fundamental role in algebraic geometry, since — as we will see — they correspond to non singular points on algebraic varieties.

A first step in this direction is to study the case of “codimension one”. Geometrically, this is the study of points in curves, curves in surfaces and so on. Hence we begin with the description of one-dimensional normal local rings. In this case, a ring (A, \mathfrak{m}) is regular iff its maximal ideal can be generated by one element. A generator for \mathfrak{m} is called a *regular* (or *uniformizing*) *parameter* for A .

To study the structure such rings, we need to introduce the so-called *discrete valuation rings* (DVR). We will show that a normal one-dimensional local Noetherian ring is regular and that regular one-dimensional rings are DVRs. In particular, a normal one-dimensional variety is already non-singular: normalization is then a canonical process for resolution of singularities in dimension one. Since normalization commutes with localization, this fact implies that the localizations of normal rings at primes with codimension one⁵ are regular, i.e. they are DVR. This fact is called *regularity in codimension 1*. Geometrically, this means that the “singular locus” of a normal variety is of codimension greater or equal than 2.

Before defining discrete valuation rings, we introduce a larger class of domains.

4.2. Definition. Let A be an integral domain and let $k = \text{Frac}(A)$ be its field of fractions. We say that A is a *valuation ring* if for every $\alpha \in k^\times = k \setminus \{0\}$ such that $\alpha \notin A$, then $\alpha^{-1} \in A$.

Clearly any field is a valuation ring (and this is the trivial situation). From this definition we have immediately an important property of valuation rings, that is for any two ideals I and J of A , $I \neq J$, either $I \subset J$ or $J \subset I$: in fact, let $x \in I$, $x \notin J$. Then, for any $y \in J$, $y \neq 0$, we have $xy^{-1} \notin A$ (otherwise if $xy^{-1} = a \in A$ then $x = ya \in J$). Thus, by definition of valuation ring, it holds $yx^{-1} \in A$ and $y = x(yx^{-1}) \in I$, therefore $J \subset I$. Thus the ideals of A form a totally ordered set.

Hence there exist exactly one maximal ideal \mathfrak{m} and we have then that A is a local domain. We can easily see that $k \setminus A = \{\alpha \in k^\times \mid \alpha^{-1} \in \mathfrak{m}\}$, since $\alpha \in A \setminus \mathfrak{m} \iff \alpha \in A^\times$. Thus the ring A is completely determined by its field of fractions and by the ideal \mathfrak{m} .

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

⁵Recall that $\text{codim}(\mathcal{V}(\mathfrak{p}), \text{Spec}(A)) = \text{ht } \mathfrak{p}$. Hence the primes with codimension one are exactly the primes of A such that $\dim A_{\mathfrak{p}} = 1$.

PROOF. Let $x \in k = \text{Frac}(A)$ be integral over A , $x \neq 0$, so that $x^n + a_1x^{n-1} + \dots + a_n = 0$ with $a_i \in A$. If $x \notin A$ then $x^{-1} \in \mathfrak{m}$ where \mathfrak{m} is the unique maximal ideal of A . So we have $1 + a_1x^{-1} + \dots + a_nx^{-n} = 0$ and we get $1 \in \mathfrak{m}$ which is a contradiction. \square

If U denotes the set of units of a valuation ring A and $k = \text{Frac}(A)$, we can consider the group $\Gamma = k^\times/U$, written additively. Then Γ is an *ordered group*, in the sense that we can define a suitable total order relation \leq in Γ such that

$$(4.1) \quad \alpha \leq \beta \iff \text{for all } \gamma \in \Gamma, \alpha + \gamma \leq \beta + \gamma.$$

In particular, if we denote with $[x]$ the class of x in Γ , we say that $[x] \leq [y]$ iff $yx^{-1} \in A$. The group Γ together with the relation \leq , as we will see with the following lemma, is an ordered group.

4.4. Lemma. *Let (Γ, \leq) be as above. Then*

- i) \leq is a total order:*
- ii) (Γ, \leq) satisfies the condition (4.1).*

PROOF. We begin with the proof that \leq is a total order. Indeed \leq is transitive, since $[x] \leq [y] \leq [z]$ iff $yx^{-1} \in A$ and $zy^{-1} \in A$. Then $zx^{-1} = (zy^{-1})(yx^{-1}) \in A$ and hence $[x] \leq [z]$. Moreover, $[x] \leq [y] \leq [x]$ iff $yx^{-1} \in A$ and $xy^{-1} \in A$. Thus $A \ni yx^{-1} = (xy^{-1})^{-1}$, and then $yx^{-1} \in U$, which is to say $y = xu$, and hence $[x] = [y]$. Further, for all $x, y \in k^\times$, it holds either $xy^{-1} \in A$ or $yx^{-1} \in A$, by the definition of valuation ring. Therefore \leq is a total order over the group Γ . The condition (4.1) is clearly satisfied. \square

Now we can consider the natural projection $v: k^\times \rightarrow \Gamma = k^\times/U$: such a map satisfies the conditions

- (a) $v(xy) = v(x) + v(y)$;
- (b) $v(x + y) \geq \min\{v(x), v(y)\}$.

The projection v is a homomorphism of groups, then (a) clearly holds. To see the second, take $x, y \in k^\times$. Since \leq is a total order, we can assume $v(x) \geq v(y)$. This is equivalent to say $xy^{-1} \in A$. Notice⁶ that for all $\alpha \in A$, $v(\alpha) \geq 0 = [1]$, since $[1] \leq [\alpha] \Leftrightarrow \alpha 1 = \alpha \in A$. Hence $v(1 + xy^{-1}) \geq 0 = v(1)$. Therefore

$$v(x + y) \geq v(y(1 + xy^{-1})) = v(y) + v(1 + xy^{-1}) \geq v(y).$$

More generally, we have the following

4.5. Definition. let K be a field and H an ordered group. A map $v: K^\times \rightarrow H$ is called an *additive valuation* or simply a *valuation* of the field K if it satisfies the conditions (a) and (b) stated above.

4.6. Remark. Many authors (see, for instance, [7]), given an ordered group H , define an ordered set $H \cup \{\infty\}$ by adding to H an element ∞ which is, by definition, bigger than all the elements of H , and fix the conventions $\infty + \alpha = \infty$ for all $\alpha \in H$ and $\infty + \infty = \infty$. Then a valuation map is defined as a function $v: K \rightarrow H \cup \{\infty\}$ that satisfies the conditions (a), (b) and the additional request

$$(c) \quad v(x) = \infty \Leftrightarrow x = 0.$$

⁶Pay attention to the additive notation.

However, this does not change in a substantial way what follows, hence we will not adopt this convention.

A valuation map v of a field K defines by (a) a homomorphism of groups between K^\times and H . The image is a subgroup of H , called the *value group* of v . We can also set

$$A_v := \{x \in K \mid v(x) \geq 0\} \cup \{0\} \quad \text{and} \quad \mathfrak{m}_v := \{x \in K \mid v(x) \geq 0\} \cup \{0\}$$

and we have the following

4.7. Lemma. *The subset A_v of K is a valuation ring with \mathfrak{m}_v as its maximal ideal. A_v is called the valuation ring of v and \mathfrak{m}_v the valuation ideal of v .*

PROOF. We prove that A_v is a ring. By definition $0 \in A_v$. Then we have $v(1) = v(1 \cdot 1) = v(1) + v(1)$ and hence $v(1) = 0$, so $1 \in A_v$. Moreover, for $x, y \in A_v$, $v(xy) = v(x) + v(y) \geq 0$ and, if $x + y \neq 0$, $v(x + y) \geq \min\{v(x), v(y)\} \geq 0$. So $xy \in A_v$ and $x + y \in A_v$. Finally, if $x \in A_v$, then $v(-x) = v(-1) + v(x)$: thus we just need to prove that $v(-1) \geq 0$. If it is not, notice that $v(-1) + v(-1) = v(1) = 0$ and then, if $v(-1) < 0$, we have $0 = v(-1) + v(-1) < 0$, which is a contradiction.

Hence A_v is a ring. Further, consider the field of fractions $\text{Frac}(A_v) = k \subseteq K$. We claim that $K = k$. In fact, for all $\alpha \in K$, $\alpha \notin A_v$, we have $v(\alpha) < 0$. Moreover, $v(\alpha) + v(\alpha^{-1}) = v(\alpha \cdot \alpha^{-1}) = v(1) = 0$ and so it holds $v(\alpha) = -v(\alpha^{-1})$ that implies $v(\alpha^{-1}) > 0$. Therefore $\alpha^{-1} \in \mathfrak{m}_v$ and then $\alpha^{-1} \in A_v$. As a consequence, $\alpha = (\alpha^{-1})^{-1} \in k = \text{Frac}(A_v)$.

By this argument, we have also proved that A_v is a valuation ring, since whenever $k \ni \alpha \notin A_v$ we have that $\alpha^{-1} \in A_v$. Finally, the ideal \mathfrak{m}_v is clearly the maximal ideal of the valuation ring A_v , since we have $v(x) = 0$ iff x is a unit⁷. \square

Conversely, if A is a valuation ring with field of fractions k , we have shown that the projection $v: k^\times \rightarrow \Gamma$ is a valuation map with value group Γ .

4.8. Remark. The valuation corresponding to a valuation ring A is not unique, in the sense that it is possible to have different valuations of the field K having the same valuation ring A . However, if v and v' are valuations of K with value groups H and H' (both having the valuation ring A) then there exists an order-preserving isomorphism $\varphi: H \rightarrow H'$ such that $v' = \varphi \circ v$.

5. Discrete valuations

5.1. Definition. A valuation ring whose value group is isomorphic to \mathbb{Z} is called a *discrete valuation ring* (DVR).

For a domain A to be a discrete valuation ring is a very strong condition, as we will prove with the following theorem.

5.2. Theorem. *Let A be a valuation ring. The following are equivalent:*

- i) A is a DVR.
- ii) A is a PID.
- iii) A is a Noetherian ring.

⁷The reason should be clear: convince yourself.

PROOF. Let $k = \text{Frac}(A)$ be the field of fractions of A and \mathfrak{m} be its maximal ideal. We have already seen that $\mathfrak{m} = \{0\} \cup \{x \in k^\times \mid v(x) > 0\}$.

i) \Rightarrow ii). Let $v: k^\times \rightarrow \mathbb{Z}$ be the valuation of A having value group \mathbb{Z} ; being v surjective on \mathbb{Z} , there exists an element t such that $v(t) = 1$. For all $x \in \mathfrak{m}$, $x \neq 0$, the valuation $v(x) = n$ is a strictly positive integer. We recall that for all $a \in A \setminus \mathfrak{m} = A^\times$ it holds $v(a) = 0$. Moreover, if $v(a) = v(b)$ then $v(ab^{-1}) = 0$, hence $ab^{-1} \in A^\times$. Further, we also have $n = v(x) = v(t^n) = nv(t)$ and then $v(xt^{-n}) = 0$, so that we can write $x = ut^n$ with u a unit of A . In particular, this implies $x \in (t)$. Since this holds for all $x \in \mathfrak{m}$ (and since \mathfrak{m} is maximal), we have proved that $\mathfrak{m} = (t)$. Let now $I \neq (0)$ be a non zero ideal of A . The set $\{v(a) \mid a \in I, a \neq 0\}$ is a set of non-negative integers, and so has a smallest element, say n_I . If $n_I = 0$ then I contains a unit of A , so that $I = A$. Otherwise, if $n_I > 0$, we can consider the element $x \in I$ such that $v(x) = n_I$. If we apply the above argument, then we obtain that $I = (x) = (t^{n_I})$ (use the minimality of $v(x)$). Therefore A is a principal ideal domain, and moreover every non-zero ideal of R is a power of \mathfrak{m} .

ii) \Rightarrow iii) it's obvious. For iii) \Rightarrow ii), notice that we have already proved that given the set of all ideals in a valuation ring A is totally ordered. Hence, if $I = (a_1, \dots, a_n)$ is an ideal of A (finitely generated by the Noetherian assumption), then it must be equal to one of the ideals (a_i) , and therefore principal. Finally we have to prove that ii) \Rightarrow i). Notice that (A, \mathfrak{m}) is a local PID, hence we can write $\mathfrak{m} = (t)$ for some $t \in A$. Then the ideal $I = \bigcap_{k=1}^{\infty} (t^k)$ is principal, say $I = (y)$. Clearly $\mathfrak{m} \supset I$, hence $y = tz$, and also $y \in (t^\nu)$ for all $\nu > 0$, therefore we get $z \in (t^{\nu-1})$ which holds for all ν . Hence $z \in I$, so we get $z = ya$ and then $y = tya$, $y(1 - ta) = 0$. Since t is not a unit ($t \in \mathfrak{m}$), we must have $y = 0$, and so $I = (0)$. By this argument, we can say that for all non-zero element $a \in A$, there exists a non-negative integer ν such that $a \in (t^\nu)$ and $a \notin (t^{\nu+1})$: then its well defined the map $\tau: A \setminus \{0\} \rightarrow \mathbb{N}$ such that $a \mapsto \tau(a) := \nu$. We can extend τ to a map v from field of fractions $k \setminus \{0\}$ to \mathbb{Z} by defining $v(a/b) = \tau(a) - \tau(b)$. It can easily be seen that v is a valuation of k and that $A_v = A$, $\mathfrak{m}_v = \mathfrak{m}$. Therefore A is a DVR. \square

Thanks to this theorem, the definition that we have seen at the beginning of the previous section makes sense:

5.3. Definition. If A is a DVR with maximal ideal \mathfrak{m} , an element t such that $(t) = \mathfrak{m}$ is called a *uniformizing parameter* of A .

Consider again a local regular Noetherian ring of dimension 1. We have seen that the maximal ideal \mathfrak{m} is principal, generated by an element t . Further, every ideal I is a power of the maximal ideal \mathfrak{m} : clearly there exists r such that $I \subseteq \mathfrak{m}^r$ since $\sqrt{I} = \mathfrak{m}$. If the inclusion is strict, apply 2.11 to the ring A/\mathfrak{m}^r .

Moreover, if we apply the same argument of the proof of the previous theorem, we can define a valuation map from $k^\times = \text{Frac}(A)^\times$ to \mathbb{Z} . Therefore we have proved the following result:

5.4. Proposition. *Let (A, \mathfrak{m}) be a regular local Noetherian ring of dimension 1. Then A is a DVR (and hence it's normal).*

More generally, it can be proved the following.

5.5. Theorem. *Let A be a ring; then the following are equivalent:*

- i) A is a DVR;*
- ii) A is a local principal ideal domain, and not a field;*
- iii) A is a Noetherian local ring, $\dim A > 0$ and the maximal ideal \mathfrak{m} is principal;*
- iv) A is a one-dimensional normal Noetherian local ring.*

PROOF. We have already seen that $i) \Rightarrow ii) \Rightarrow iii)$. For $i) \Rightarrow iv)$, notice that in a DVR the only ideals are (0) the powers of the maximal ideal. Therefore the only prime ideals of A are (0) (being a domain) and \mathfrak{m} . Hence $\dim A = 1$. By the previous theorem, A is Noetherian, and it is normal (because it is a valuation ring). For a proof of $iii) \Rightarrow i)$ and $iv) \Rightarrow iii)$, see [7], Theorem 11.2. \square

Notice that the assumption of Proposition 1.11 is satisfied by any local Noetherian normal ring of dimension 1. If we combine this remark with the previous results, we have then the following important result for such rings:

$$A \text{ is regular} \Leftrightarrow A \text{ is a DVR} \Leftrightarrow A \text{ is normal.}$$

6. Noether's normalization lemma

The Noether Normalization Theorem provides a refinement of a choice of transcendence base so that certain ring extensions are integral extensions, not just algebraic extensions. In this section we will restrict again to the case of finitely generated algebras over a field k . Recall that if A is a Noetherian ring, subring of a ring B such that B is integral over A and $B = A[x_1, \dots, x_n]$ (i.e. B is finitely generated A -algebra), then B is a finitely generated A -module (i.e. $A \hookrightarrow B$ is finite).

Now consider a finitely generated k -algebra, i.e. $k[x_1, \dots, x_n] = k[X_1, \dots, X_n]/I$ which we may assume to be a domain (i.e. $I = \mathfrak{p}$ prime) with field of fractions $K = k(x_1, \dots, x_n)$. As we have seen in Chapter 2, we can extract from $\{x_1, \dots, x_n\}$ a transcendental basis for K over k , hence $\text{Trdeg}_k(K) \leq n$.

6.1. Proposition. *Let $A = k[x_1, \dots, x_n]$ be a finitely generated k -algebra. Let $\mathfrak{p} \subset \mathfrak{q} \subset A$ be prime ideals of A . Then $\text{Trdeg}_k(\text{Frac}(A/\mathfrak{q})) \leq \text{Trdeg}_k(\text{Frac}(A/\mathfrak{p}))$.*

PROOF. By replacing A with A/\mathfrak{p} , we can assume that A is a domain and that \mathfrak{q} is a non-zero prime of A . Let $\{y_1, \dots, y_r\}$ be a transcendental basis for $\text{Frac}(A/\mathfrak{q})$ over k : if we consider the projection $A \rightarrow A/\mathfrak{q}$, we can lift the set $\{y_1, \dots, y_r\}$ to A choosing a set of representatives $\{x'_1, \dots, x'_r\} \subset A$. This set is clearly algebraically independent over k , otherwise we can reduce modulo \mathfrak{q} any relation of integral dependence between the x'_i 's, obtaining a relation of integral dependence between the y_i 's. Therefore we have that $\text{Trdeg}_k(\text{Frac}(A/\mathfrak{q})) \leq \text{Trdeg}_k(\text{Frac}(A))$. Suppose now by contradiction that the equality holds with $\mathfrak{q} \neq 0$. Let $p \in \mathfrak{q}$: this element is algebraic over $k(x'_1, \dots, x'_r)$. So there exist $p_0, \dots, p_m \in k[X_1, \dots, X_r]$ such that $p_0(x'_1, \dots, x'_r) + p_1(x'_1, \dots, x'_r)p + \dots + p_m(x'_1, \dots, x'_r)p^m = 0$ with m minimal. Hence $p_0 \neq 0$ and reducing the relation modulo \mathfrak{q} we obtain $\bar{p}_0(y_1, \dots, y_r) = 0$, contradicting the fact that $\{y_1, \dots, y_r\}$ is a transcendental basis for $\text{Frac}(A/\mathfrak{q})$ over k . \square

6.2. Corollary. *Let A be a finitely generated integral domain over a field k . Then $\dim(A) \leq \text{Trdeg}_k(\text{Frac}(A))$.*

PROOF. In fact, consider a chain of primes $(0) \subset \mathfrak{p}_1 \subset \dots \subset \mathfrak{p}_n \subset A$ in A . Then $A \twoheadrightarrow A/\mathfrak{p}_1 \twoheadrightarrow \dots \twoheadrightarrow A/\mathfrak{p}_n$ and so $\text{Trdeg}_k(\text{Frac}(A)) \geq \text{Trdeg}_k(\text{Frac}(A/\mathfrak{p}_1)) \geq \text{Trdeg}_k(\text{Frac}(A/\mathfrak{p}_n))$, hence the claim follows. \square

As a consequence, we get an important result about the dimension of the polynomial ring in n variables over a field k . In fact, let $A = k[X_1, \dots, X_n]$. For each $i = 1, \dots, n$, we have the prime ideal $\mathfrak{p}_i := (X_1, \dots, X_i)$. Hence we have the chain of primes $(0) \subset \mathfrak{p}_1 \subset \dots \subset \mathfrak{p}_n$, and so $\dim(A) \geq n$. Moreover, by the previous corollary, we get $n \leq \dim(A) \leq \text{Trdeg}_k(\text{Frac}(A)) = \text{Trdeg}_k(k(X_1, \dots, X_n)) = n$. Hence $\dim(A) = n$.

6.3. Theorem (Noether's lemma). *Let A be a finitely generated integral domain over a field k . Let $K = \text{Frac}(A)$ be the field of fractions of A and suppose that the transcendental degree of K over k is $\text{Trdeg}_k(K) = s$. Then there exists a set of elements $\{y_1, \dots, y_s\}$, algebraically independent over k , such that A is an integral extension of $k[y_1, \dots, y_s]$.*

PROOF (NAGATA). By assumption, A is a finitely generated k -algebra which is a domain, hence we can write A as $k[X_1, \dots, X_n]/\mathfrak{p}$ for a prime ideal $\mathfrak{p} \subset k[X_1, \dots, X_n]$. Let x_1, \dots, x_n be the images of X_1, \dots, X_n through the projection $k[X_1, \dots, X_n] \twoheadrightarrow A$. We can certainly choose a set $\{y_1, \dots, y_r\}$ so that $k[x_1, \dots, x_n]$ is integral over $k[y_1, \dots, y_r]$ (for example, take $y_i = x_i$ and $n = r$). But we will show that if we choose such y_i with r minimal, then the set $\{y_i\}$ is algebraically independent over k , hence $\{y_i\}$ is a transcendental basis for K over k .

Notice that if the elements x_1, \dots, x_n are algebraically independent (i.e. $s = n$), then $\mathfrak{p} = 0$ and the assert follows for $y_i = x_i$. Suppose now that $n \geq s$: we prove the claim by induction on the number of generators n . It will be enough to find a subring $A' \subset A$ generated by $n - 1$ elements such that $A' \subset A$ is an integral extension. In fact, by induction, A' has the claimed property and $k[y_1, \dots, y_s] \subset A' \subset A$. Since A is integral over A' and A' is integral over $k[y_1, \dots, y_s]$, by transitivity we have $k[y_1, \dots, y_s] \subset A$ integral.

Since we are assuming that $n \geq \text{Trdeg}_k(K) = s$, the elements x_1, \dots, x_n cannot be algebraically independent. Hence there is a non-trivial relation among them, i.e. there exists a polynomial $f \in k[X_1, \dots, X_n]$, $f \neq 0$, such that $f(x_1, \dots, x_n) = 0$.

$$0 = f(x_1, \dots, x_n) = \sum_{j_i} a_{j_1, \dots, j_n} x_1^{j_1} \cdots x_n^{j_n} = \sum_{(j)} a_{(j)} x^{(j)}$$

where (j) is the multi-index (j_1, \dots, j_n) and $x^{(j)} = x_1^{j_1} \cdots x_n^{j_n}$. We now claim that there exist integers $r_i \geq 1$ such that the elements $z_i := x_i - x_1^{r_i}$ $i = 2, \dots, n$ are such that the ring $A' := k[z_2, \dots, z_n]$ is, as above, generated by $n - 1$ elements and such that $A' \subset A$ is an integral extension. To see this, consider the following chain of equalities:

$$\begin{aligned} 0 &= f(x_1, \dots, x_n) = f(x_1, z_2 + x_1^{r_2}, \dots, z_n + x_1^{r_n}) = \\ &= \sum_{(j)} a_{(j)} x_1^{j_1} \prod_{i=2}^n (z_i + x_1^{r_i})^{j_i} = \sum_{(j)} a_{(j)} x_1^{j_1} \prod_{i=2}^n \left(\sum_{k_i=0}^{j_i} \binom{j_i}{k_i} z_i^{j_i - k_i} x_1^{r_i k_i} \right) = \\ &= \sum_{(j)} a_{(j)} \sum_{k_2=0}^{j_2} \cdots \sum_{k_n=0}^{j_n} \prod_{i=2}^n \binom{j_i}{k_i} x_1^{j_1 + \sum_{i=2}^n k_i r_i} \prod_{i=2}^n z_i^{j_i - k_i}. \end{aligned}$$

Let N be an integer strictly bigger than the degree of f in each of the variables x_i and set $r_i := N^i$. Hence we have $r_2 < r_3 < \dots < r_n$ and the terms $L_{k_i} := j_1 + \sum_{i=2}^n k_i r_i$ are all different (remember that k_i is varying here). Set $M = \max_{k_i} \{L_{k_i}\} = \max_{j_i} \{L_{j_i}\}$. Hence we have

$$0 = f(x_1, z_2 + x_1^{r_2}, \dots, z_n + x_1^{r_n}) = bx_1^M + [\text{terms of degree lower than } M],$$

with $b \in k$, $b \neq 0$. This is an equation of integral dependence for x_1 over $k[z_2, \dots, z_n]$. Since the terms x_i ($i = 2, \dots, n$) are integral too, since $x_i = z_i + x_1^{r_i}$, the whole ring is integrally dependent over the subring A' . By induction, we have done. \square

CHAPTER 8

Zariski's tangent space

1. Derivations and differentials

We first consider a purely algebraic characterisation of the partial derivatives of a polynomial. The main themes are derivations and modules of differentials.

1.1. Definition. Let A be a ring and M be an A -module. A *derivation* from A to M is a homomorphism of abelian groups $D: A \rightarrow M$ such that the Leibniz rule

$$D(fg) = fD(g) + gD(f)$$

holds for all $f, g \in A$; the set of all these is written $\text{Der}(A, M)$.

The set $\text{Der}(A, M)$ becomes an A -module in a natural way, with $D + D'$ and aD defined by $(D + D')a = D(a) + D'(a)$ and $(aD)(b) = a(D(b))$. If A is a k -algebra, with the action of k into A defined by a ring homomorphism $f: k \rightarrow A$, we say that a derivation D is a k -derivation if $D \circ f = 0$. The set of all k -derivation of A into M is denoted by $\text{Der}_k(A, M)$.

1.2. Remark. Notice that, since $1 \cdot 1 = 1$, for any $D \in \text{Der}(A, M)$ we have $D(1) = D(1) + D(1)$, so that $D(1) = 0$. Viewing A as a \mathbb{Z} -algebra, from this we have $\text{Der}(A, M) = \text{Der}_{\mathbb{Z}}(A, M)$. Moreover, a derivation D is k -linear (i.e. $D(rx) = rD(x)$ for all $r \in k, x \in A$) if and only if $D(r) = 0$ for all $r \in k$.

The given definition of the module $\text{Der}_k(A, M)$ allow us to define a covariant functor $\text{Der}_k(A, -): \mathbf{Mod}_A \rightarrow \mathbf{Set}$:

$$\begin{array}{ccc} M & \longrightarrow & \text{Der}_k(A, M) \\ \downarrow f & & \downarrow \\ N & \longrightarrow & \text{Der}_k(A, N); \end{array}$$

if $f: M \rightarrow N$ is a map of A -modules, then we have an induced map $\text{Der}_k(A, M) \rightarrow \text{Der}_k(A, N)$ such that $D \mapsto f \circ D$.

1.3. Proposition. *The functor $M \mapsto \text{Der}_k(A, M)$ is representable, i.e. we have $A \xrightarrow{d} \Omega_{A/k}$ a universal derivation such that*

$$\text{Der}_k(A, M) \cong \text{Hom}_A(\Omega_{A/k}, M)$$

The so called *A-module of differentials* (or *Kähler differentials of A over k*) $\Omega_{A/k}$ is obtained by taking the free A -module generated by symbols $d(f)$ (also written df) for any $f \in A$ modulo the relations $d(af + bg) - ad(f) - bd(g)$ and $d(fg) - fd(g) - gd(f)$ for all $a, b \in k, f, g \in A$. Then we can define a map (that is clearly a derivation) $d: A \rightarrow \Omega_{A/k}$ such that $b \mapsto db$. This map is called the universal k -linear derivation.

The module of Kähler differential, together with the derivation $d: A \rightarrow \Omega_{A/k}$ has the following universal property: for any A -module M and any $D \in \text{Der}_k(A, M)$, there exists a unique A -linear map $f: \Omega_{A/k} \rightarrow M$ such that $D = f \circ d$. The map f can be defined on generators db of $\Omega_{A/k}$ as $f(db) := D(b)$: this clearly implies the uniqueness. Since D is a derivation, the relations between the elements db are satisfied and this makes the map f a homomorphism of abelian groups: we can simply extend by A -linearity to conclude.

1.4. Remark. In the particular case $M = A$, we write $\text{Der}_k(A)$ for $\text{Der}_k(A, A)$. If $D, D' \in \text{Der}_k(A)$, we can compose D and D' as maps from A to A . Note that $\text{Der}_k(A, A) \cong \text{Hom}_A(\Omega_{A/k}, A) \cong (\Omega_{A/k})^\vee$ the dual A -module is a Lie algebra with the bracket $[D, D'] := D \circ D' - D' \circ D$.

There is another construction of Kähler differentials. In order to introduce this different approach, we need to recall some general facts about extensions and splitting exact sequences (for reference see [7], chapter 9).

The general setting can be described as follow: given $M, N \in \mathbf{Mod}_A$, we want to describe the A -modules E that can be written in an exact sequence like

$$0 \rightarrow M \rightarrow E \rightarrow N \rightarrow 0.$$

In this situation we say that E is an extension of N by M . The first example of extension is given by the direct sum of modules: if M and N are A -modules, we have the exact sequence

$$0 \rightarrow M \rightarrow M \oplus N \xrightarrow{p} N \rightarrow 0.$$

where p denotes the projection on the second component of the sum. Notice that we can reverse all arrows, i.e. we have two maps $N \xrightarrow{i} M \oplus N$ and $N \oplus M \rightarrow M$ such that

$$0 \rightarrow N \xrightarrow{i} M \oplus N \rightarrow M \rightarrow 0.$$

is exact and such that $p \circ i = id_N$. Clearly it is not always possible to reverse the arrows. For example, consider the following exact sequence of \mathbb{Z} -modules:

$$0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Q} \xrightarrow{p} \mathbb{Q}/\mathbb{Z} \rightarrow 0$$

where p denotes the projection to the quotient. In this case there does not exist any \mathbb{Z} -module homomorphism $i: \mathbb{Q}/\mathbb{Z} \rightarrow \mathbb{Q}$ such that $p \circ i = id_{\mathbb{Q}/\mathbb{Z}}$. In fact, any element of \mathbb{Q}/\mathbb{Z} has \mathbb{Z} -torsion, while \mathbb{Q} is torsion-free. Hence $\text{Hom}(\mathbb{Q}/\mathbb{Z}, \mathbb{Q}) = 0$. Another example is given by the exact sequence $0 \rightarrow \mathbb{Z} \xrightarrow{m} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/m\mathbb{Z} \rightarrow 0$: again $\text{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}) = 0$ and so there is no \mathbb{Z} -module homomorphism $i: \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}$ such that $\pi \circ i = id_{\mathbb{Z}/m\mathbb{Z}}$.

1.5. Definition. Let M, N, E be A -modules. We say that the exact sequence

$$(1.1) \quad 0 \rightarrow M \xrightarrow{f} E \xrightarrow{g} N \rightarrow 0$$

is *split* or that E is the *trivial extension* if there exists an isomorphism $j: E \cong M \oplus N$ such that the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & M & \longrightarrow & E & \longrightarrow & N \longrightarrow 0 \\ & & & \searrow & \downarrow & \nearrow & \\ & & & i & j & \pi & \\ & & & & M \oplus N & & \end{array}$$

commutes.

1.6. Proposition. *The exact sequence (1.1) is split \iff there exists $h: E \rightarrow M$ such that $h \circ f = id_E$.*

PROOF. First assume that the sequence (1.1) is split, i.e. there exists an isomorphism $j: E \rightarrow M \oplus N$. Then we have $M \xrightarrow{f} E \cong M \oplus N$ and the maps $i: M \hookrightarrow M \oplus N$ and $p: M \oplus N \rightarrow M$. Set $h := p \circ j$: then $h \circ f = p \circ j \circ f = p \circ i$, since (by assumption) $j \circ f = i$. Moreover $\pi \circ j = id_M$ and we have done. Conversely, given the short exact sequence (1.1) together with the map $h: E \rightarrow M$ such that $h \circ f = id_M$, we can consider the following diagram

$$(1.2) \quad \begin{array}{ccccccc} 0 & \longrightarrow & M & \xleftarrow{h} & E & \xrightarrow{g} & N \longrightarrow 0 \\ & & \searrow f & & \downarrow j & \nearrow \pi & \\ & & & & M \oplus N & & \end{array}$$

where π and i are, as usual, the canonical projection and injection and j is the A -module homomorphism such that $x \mapsto j(x) = (h(x), g(x))$. Then $j \circ f(m) = j(f(m)) = (h(f(m)), g(f(m))) = (h(f(m)), g(f(m))) = (m, g(f(m))) = (m, 0) = i(m)$. Similarly, $\pi \circ j(e) = g(e)$. Hence the diagram (1.2) commutes and we can write the following commutative diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & M & \longrightarrow & E & \longrightarrow & N \longrightarrow 0 \\ & & \parallel & & \downarrow j & & \parallel \\ 0 & \longrightarrow & M & \longrightarrow & M \oplus N & \longrightarrow & N \longrightarrow 0. \end{array}$$

Finally, j is an isomorphism as a consequence of the 5-lemma. □

More generally, we have the following proposition:

1.7. Proposition. *Let M, N, E be A -modules and let the sequence*

$$(1.3) \quad 0 \rightarrow M \xrightarrow{f} E \xrightarrow{g} N \rightarrow 0$$

be exact. The following are equivalent:

- i) The sequence (1.3) is split;*
- ii) there exists $h: E \rightarrow M$ such that $h \circ f = id_M$;*
- iii) there exists $k: N \rightarrow E$ such that $g \circ k = id_N$;*
- iv) there exists $h: E \rightarrow M$ and $k: N \rightarrow E$ such that $f \circ h + k \circ g = id_E$.*

PROOF. This is simply an application of the 5-lemma. □

1.8. Exercise. Let $0 \rightarrow M \rightarrow N \rightarrow P \rightarrow 0$ be an exact sequence of A -module with P free. Show that the sequence is split.

Now let k be a ring (not necessarily a field) and B a k -algebra. Let I be an ideal of B such that $I^2 = 0$ and set $A := B/I$. The B -module I can be viewed as an A -module: in this situation we have that B is an extension of the k -algebra A by the A -module I . As usual, we can write this extension in form of exact sequence

$$0 \rightarrow I \xrightarrow{i} B \xrightarrow{f} A = B/I \rightarrow 0.$$

We say that this extension is split if one of the (equivalent) conditions of proposition 1.7 is satisfied, with the additional requirement that the involved maps are k -algebra homomorphisms. Hence, the above extension is split if there exists a k -algebra homomorphism $k: A \rightarrow B$ such that $f \circ k = id_A$. Conversely, given any k -algebra A together with an A -module I , we can make the direct sum $A \oplus I$ of k -modules into a split extension of A by I .

In general, let $A, B, C \in \mathbf{Alg}_k$ and consider a commutative diagram

$$\begin{array}{ccc} B & \xrightarrow{f} & A \\ & \searrow h & \uparrow g \\ & & C \end{array}$$

Suppose that f is fixed. In this case we say that any map $h: C \rightarrow B$ that makes the above diagram commutative is a lifting of g to B . Let $I = \text{Ker}(f) \subset B$. If $h': C \rightarrow B$ is another lifting of g , then $h - h' \in \text{Hom}(C, I)$. If $I^2 = 0$ then I is an $f(B)$ -module; in fact $f(B) \cong B/I$ and we can define the action $(b + I) \cdot m = bm + mI = bm$ since $mI \subseteq I^2 = 0$, so that $f(b) \cdot m = (b + N)m = bm$. Moreover, using $g: C \rightarrow f(B) \subset A$, we can consider I as a C -module. In fact, $g(c) \cdot m = f(h(c)) \cdot m = h(c)m$; then it is easy to see that $h - h': C \rightarrow I$ is a k -derivation of C to the C -module I . Indeed, for all $a, b \in C$, $(h - h')(ab) = h(a)a(b) - h'(a)h'(b) = h(a)a(b) - h'(a)h'(b) + h(a)h'(b) - h(a)h'(b) = a \cdot (h - h')(b) + b \cdot (h - h')(a)$. Conversely, given any $D \in \text{Der}_k(C, I)$, then $h + D$ is another lifting of g to B .

Now we can come back to the original setting on derivations and differentials. Let k be a field and A a k -algebra. As we noticed at the beginning of this chapter, we have a covariant functor $M \mapsto \text{Der}_k(A, M)$ from \mathbf{Mod}_A to itself. Define the multiplication map $\mu: A \otimes_k A \rightarrow A$ by

$$\mu(x \otimes y) = xy.$$

Let $I = \text{Ker}(\mu)$. We have that I/I^2 is a $(A \otimes_k A)/I \cong A$ module.¹ Set $\Omega_{A/k} = I/I^2$ and $B = (A \otimes_k A)/I^2$. Then μ induces $\mu': B \rightarrow A$, and we have an exact sequence

$$0 \rightarrow \Omega_{A/k} \rightarrow B \xrightarrow{\mu'} A \rightarrow 0$$

that is an extension of the k -algebra A by $\Omega_{A/k}$; this extension splits. In particular we can define two maps $\lambda_i: A \rightarrow B$ for $i = 1, 2$:

$$\lambda_1(a) = a \otimes 1 \pmod{I^2}, \quad \lambda_2(a) = 1 \otimes a \pmod{I^2}.$$

Clearly we have that $\mu' \circ \lambda_i = id_A$. Using the above notation, we have (for $i = 1, 2$) a commutative diagram

$$\begin{array}{ccc} B & \xrightarrow{\mu'} & A \\ & \searrow \lambda_i & \parallel id_A \\ & & A \end{array}$$

¹ I is a $A \otimes_k A$ -module and $I/I^2 \simeq I \otimes_{A \otimes_k A} (A \otimes_k A)/I$.

hence λ_1 and λ_2 are two liftings of $id_A: A \rightarrow A$. Hence the map $d := \lambda_2 - \lambda_1: A \rightarrow I/I^2$, $d: b \mapsto 1 \otimes b - b \otimes 1 \pmod{I^2}$ is a derivation. We claim that I/I^2 together with the derivation d represents the functor $\text{Der}_k(A, -)$.

PROOF. Let Δ be the direct sum of k -modules $A \oplus M$ with the product $(a, x)(a', x') = (aa', ax' + a'x)$. Δ is then a k -algebra and the extension $0 \rightarrow M \rightarrow \Delta \rightarrow A \rightarrow 0$ splits. Let $D \in \text{Der}_k(A, M)$ and define the homomorphism of k -algebras $\varphi: A \otimes_k A \rightarrow \Delta$ by $\varphi(x \otimes y) = (xy, xDy)$. Notice that if $\sum x_i \otimes y_i \in I$, i.e. $\mu(\sum x_i \otimes y_i) = \sum x_i y_i = 0$, then $\varphi(\sum x_i \otimes y_i) = (0, \sum x_i Dy_i) \mapsto \sum x_i Dy_i$, hence φ maps I into M . Moreover, it's easy to check that $I^2 \subset \text{Ker } \varphi$, hence φ factors through the quotient I/I^2 and we get a map $f: I/I^2 = \Omega_{A/k} \rightarrow M$. By definition, we have $f(da) = f(1 \otimes a - a \otimes 1 \pmod{I^2}) = \varphi(1 \otimes a) - \varphi(a \otimes 1) = D(a) - aD(1) = D(a)$, so that $D = f \circ d$. In order to show that I/I^2 has the claimed universal property, we need to prove the uniqueness of the map f such that $D = f \circ d$ and that f is A -linear. Notice that the multiplication by $a \otimes 1$ in $A \otimes A$ induces the A -module structure on I/I^2 , so that if $I/I^2 \ni \alpha = \sum x_i \otimes y_i \pmod{I^2}$ then $a\alpha = \sum ax_i \otimes y_i \pmod{I^2}$ and $f(a\alpha) = \sum ax_i Dy_i = af(\alpha)$, proving that f is also A -linear; thus we made from a derivation D a map $f \in \text{Hom}_A(I/I^2, M)$.

Since $a \otimes b \pmod{I^2} = (a \otimes 1)(1 \otimes b - b \otimes 1) + ab \otimes 1 \pmod{I^2} = (a \otimes 1)db + ab \otimes 1 \pmod{I^2}$, we have $I/I^2 \ni \alpha = \sum x_i \otimes y_i \pmod{I^2} = \sum x_i dy_i$, proving that $I/I^2 = \Omega_{A/k}$ is generated as A -modules by $\{da \mid a \in A\}$. This clearly implies the uniqueness of f (since we defined the action on generators) and completes the proof: we have that $\text{Der}_k(A, M) \cong \text{Hom}_A(I/I^2, M) = \text{Hom}_A(\Omega_{A/k}, M)$. \square

1.9. Example. Let $A = k[X_1, \dots, X_n]$ be a polynomial ring in n -variables. Denote $D_i: A \rightarrow A$ the usual partial derivative $\partial/\partial X_i$ with respect to X_i . We get $D_i \in \text{Der}_k(A, A)$. Note that any $D \in \text{Der}_k(A, M)$ is determined by its values on X_i and if we just set $D(X_i) := m_i \in M$ for $1 \leq i \leq n$ we get

$$(1.4) \quad D(f) = \sum_{i=1}^n \frac{\partial f}{\partial X_i} m_i$$

for all polynomials $f \in k[X_1, \dots, X_n]$. Thus $\text{Der}_k(A, A)$ is a free A -module on D_1, \dots, D_n , e.g. this also follows from the universal property of the dual $\Omega_{A/k}$ which is a free A -module on $d(X_1), \dots, d(X_n)$.

Note that for a given ideal $I \subseteq k[X_1, \dots, X_n]$ any such derivation D factors through $k[X_1, \dots, X_n]/I$ if $D(f) = 0$ for all $f \in I$.

1.10. Definition. Let $A = k[X_1, \dots, X_n]/I$ be a finitely generated k -algebra. Let M be an A -module. The *tangent module* is the A -module

$$T_M(A) := \{(m_1, \dots, m_n) \in M^n \mid \sum_{i=1}^n D_i(f)m_i = 0 \text{ for all } f \in I\}$$

where $D_i(f)$ is the class of $\partial f/\partial X_i$ modulo I .

For $(m_1, \dots, m_n) \in T_M(A)$ we then get a derivation $D_{(m_1, \dots, m_n)} \in \text{Der}_k(A, M)$ as follows. Let $f \in k[X_1, \dots, X_n]$ and $\bar{f} \in A$ its class modulo I then

$$D_{(m_1, \dots, m_n)}(\bar{f}) := \sum_{i=1}^n D_i(f)m_i$$

is a derivation. It is well defined since $D_{(m_1, \dots, m_n)}(\bar{f}) = 0$ for all $f \in I$ by the definition of $T_M(A)$ and clearly satisfies the Leibniz rule. We then get a mapping

$$(1.5) \quad \tau : T_M(A) \rightarrow \text{Der}_k(A, M)$$

1.11. Proposition. *The map τ in (1.5) is an isomorphism of A -modules.*

PROOF. The injectivity is clear since $D_{(m_1, \dots, m_n)}(\bar{X}_i) = m_i$ for $1 \leq i \leq n$ so we are left to check the surjectivity. Let $D \in \text{Der}_k(A, M)$ and regard D as a derivation from $k[X_1, \dots, X_n]$ into M by composition. We then just set $m_i := D(X_i)$ for $1 \leq i \leq n$ and we get $D(f)$ as in (1.4) above for all polynomials $f \in k[X_1, \dots, X_n]$. Since this derivation factors through $A = k[X_1, \dots, X_n]/I$ we have $D(f) = 0$ for all $f \in I$ thus $(m_1, \dots, m_n) \in T_M(A)$. Finally note that $D_{(m_1, \dots, m_n)}(\bar{X}_i) = D(X_i)$ thus $D_{(m_1, \dots, m_n)} = D$ as claimed. \square

1.12. Remark. Fix a maximal ideal $\mathfrak{m} \subset k[X_1, \dots, X_n]$ containing a radical ideal I such that $A/\mathfrak{m} = k$ is an A -module, i.e. an element x of the algebraic set $X := \mathcal{Z}(I) \subseteq \text{Max}(A)$, $A = k[X_1, \dots, X_n]/I$. We get back the usual tangent space at the rational point x by taking values of derivations at x via $A \rightarrow k$ as usual. In fact, for $I = (f_1, \dots, f_r)$ we have

$$T_k(A) = \{(m_1, \dots, m_n) \in k^n \mid \sum_{i=1}^n \frac{\partial f_j}{\partial X_i}(x)m_i = 0 \text{ for all } j = 1, \dots, r\}$$

Note that

$$D_{(m_1, \dots, m_n)}(f) := \sum_{i=1}^n \frac{\partial f}{\partial X_i}(x)m_i$$

is a derivation on all $k[X_1, \dots, X_n]$ and if $f = \sum_j g_j f_j$ then

$$\sum_{i=1}^n \frac{\partial f}{\partial X_i}(x)m_i = \sum_j g_j(x) \sum_{i=1}^n \frac{\partial f_j}{\partial X_i}(x)m_i + \sum_j f_j(x) \sum_{i=1}^n \frac{\partial g_j}{\partial X_i}(x)m_i = 0$$

and therefore $D_{(m_1, \dots, m_n)}(f) = 0$ for all $f \in I$, i.e. $D_{(m_1, \dots, m_n)} \in \text{Der}_k(A, k)$.

1.13. Corollary. *For an algebraic set $X := \mathcal{Z}(I)$ and a point $x \in X$ denote $T_x(X) := T_k(A)$ and $\text{Der}_x(X) := \text{Der}_k(A, k)$ the corresponding k -vector spaces. Then*

$$\tau : T_x(X) \xrightarrow{\simeq} \text{Der}_x(X)$$

is an isomorphism of k -vector spaces.

2. Zariski tangent space

We now look at the local nature of the tangent space at a rational point. Let $X = \text{Spec}(A)$ where A is a (finitely generated) k -algebra and let $x \in X(k)$ be a rational point. We denote the corresponding maximal ideal by $\mathfrak{m}_x \subset A$.

For $D \in \text{Der}_k(A, k)$ consider the restriction of $D : A \rightarrow k$ to the maximal ideal \mathfrak{m}_x and get

$$D(fg) = f(x)D(g) + g(x)D(f) = 0$$

for all $f, g \in \mathfrak{m}_x$ (recall that $f(x) := \bar{f} \in A/\mathfrak{m}_x = k$). Since $D(\mathfrak{m}_x^2) = 0$ we get a k -linear mapping $\mathfrak{m}_x/\mathfrak{m}_x^2 \rightarrow k$. Let

$$(\mathfrak{m}_x/\mathfrak{m}_x^2)^\vee := \text{Hom}_k(\mathfrak{m}_x/\mathfrak{m}_x^2, k)$$

be the dual k -vector space. Recall that we always have

$$\mathfrak{m}_x/\mathfrak{m}_x^2 \xrightarrow{\cong} \mathfrak{m}_x A_{\mathfrak{m}_x} / \mathfrak{m}_x^2 A_{\mathfrak{m}_x}$$

where $A_{\mathfrak{m}_x}$ is the local ring and $A_{\mathfrak{m}_x} \twoheadrightarrow A_{\mathfrak{m}_x}/\mathfrak{m}_x A_{\mathfrak{m}_x} = k$ so that we can regard it just locally. By restricting derivations to \mathfrak{m}_x we thus obtain

$$(2.1) \quad \delta : \text{Der}_k(A, k) \rightarrow (\mathfrak{m}_x/\mathfrak{m}_x^2)^\vee$$

2.1. Proposition. *The map δ in (2.1) is an isomorphism of k -vector spaces.*

PROOF. It is clear that δ is k -linear and injective since $D(\mathfrak{m}_x) = 0$ implies $D = 0$. Let $\ell : \mathfrak{m}_x/\mathfrak{m}_x^2 \rightarrow k$ be a k -linear mapping. Note that, for any $f \in A$, $f(x) \in k \subset A$ and $f - f(x) \in \mathfrak{m}_x$. Considering $f - f(x)$ modulo \mathfrak{m}_x^2 we set

$$D_\ell(f) := \ell(f - f(x))$$

and we get a derivation. In fact, for $f, g \in A$ we have $(f - f(x))(g - g(x)) \in \mathfrak{m}_x^2$ so that

$$fg - f(x)g(x) = f(x)(g - g(x)) + g(x)(f - f(x))$$

modulo \mathfrak{m}_x^2 and applying ℓ we get $D_\ell(fg) = f(x)D_\ell(g) + g(x)D_\ell(f)$. Note that if $f \in k$ is a constant $f(x) = f$, i.e. $D_\ell(f) = 0$, and if $f \in \mathfrak{m}_x$ clearly $D_\ell(f) = \ell(f)$ so that the restriction of D_ℓ to \mathfrak{m}_x yields back the linear mapping ℓ . This is showing that δ is surjective. \square

Since² $\text{Der}_k(A, k) = \text{Hom}_A(\Omega_{A/k}, k) = \text{Hom}_k(\Omega_{A/k} \otimes_A k, k)$ from (2.1) we get, in the finitely generated case, the following.

2.2. Corollary. *We have an isomorphism*

$$\mathfrak{m}_x/\mathfrak{m}_x^2 \xrightarrow{\cong} \Omega_{A/k} \otimes_A k$$

Notice that this is true in general (but in that case it does not follow from the previous proposition).

²This is a standard application of the following property of the tensor product: if $f : A \rightarrow B$ is an A -algebra, M is an A -module and N is a B -module, then we have an isomorphism $\text{Hom}_A(M, N) \cong \text{Hom}_B(M \otimes_A B, N)$.

2.3. Remarks. (a) Let $A = k[X_1, \dots, X_n]/I$ be a finitely generated k -algebra. Let $X := \mathcal{Z}(I)$ be the algebraic set and consider the maximal ideal $\mathfrak{m}_x \subset k[X_1, \dots, X_n]$ containing I . We then have

$$T_x(X) \cong \text{Der}_x(X) \cong (\mathfrak{m}_x/\mathfrak{m}_x^2)^\vee$$

Actually we can describe the inverse mapping

$$(\mathfrak{m}_x/\mathfrak{m}_x^2)^\vee \rightarrow T_x(X)$$

of the composition of (1.5) and (2.1) as follows. Suppose given $\ell \in \text{Hom}_k(\mathfrak{m}_x/\mathfrak{m}_x^2, k)$ and $\mathfrak{m}_x = (X_1 - x_1, \dots, X_n - x_n)$. Considering D_ℓ above as a derivation on $k[X_1, \dots, X_n]$ we obtain D_ℓ as in (1.4), i.e. for $f \in k[X_1, \dots, X_n]$

$$\ell(f - f(x)) = \sum_{i=1}^n \frac{\partial f}{\partial X_i}(x) \ell(X_i - x_i)$$

We get $m_i := \ell(X_i - x_i)$ and clearly $(m_1, \dots, m_n) \in T_x(X)$ since $D_\ell \in \text{Der}_k(A, k)$. If you like to assume a Taylor expansion

$$f = f(x) + \sum_{i=1}^n \frac{\partial f}{\partial X_i}(x)(X_i - x_i) + \text{terms of degree } \geq 2$$

you can see it applying ℓ after cutting off the non-linear terms.

(b) Similarly, for a derivation $D \in \text{Der}_k(A_{\mathfrak{m}_x}, k)$ we can restrict it to the extended maximal ideal $\mathfrak{m}_x A_{\mathfrak{m}_x}$ of the local ring and similar arguments as above apply. We thus obtain

$$\text{Der}_x(X) \cong \text{Der}_k(A_{\mathfrak{m}_x}, k)$$

2.4. Exercise. Let A be a k -algebra, $X = \text{Spec}((A))$, $x \in X(k)$. For a derivation $D : A \rightarrow k$ there exists a unique extension to a derivation $D : A_{\mathfrak{m}_x} \rightarrow k$, i.e. we have $\text{Der}_k(A, k) \cong \text{Der}_k(A_{\mathfrak{m}_x}, k)$. Given $D \in \text{Der}_k(A, k)$ and $f/g \in A_{\mathfrak{m}_x}$ we just set

$$D(f/g) := \frac{1}{g^2(x)}(g(x)D(f) - f(x)D(g))$$

and we obtain $D \in \text{Der}_k(A_{\mathfrak{m}_x}, k)$.

2.5. Example. (a) Let $X = \mathcal{Z}(I)$, $A = k[X_1, \dots, X_n]/I$ where $I = (f_1, \dots, f_r)$ are linear homogeneous polynomials. Then $T_x(X) = X$ for any $x \in X$.

(b) Let $X = \mathcal{Z}(f)$, $A = k[X, Y]/(f)$ where $f = X^3 - Y^2$. Let $x = (t^2, t^3) \in X$ for $t \in k$, $\partial f/\partial X = 3X^2$, $\partial f/\partial Y = -2Y$ and $\dim_k T_x(X) = 1$ for $t \neq 0$ and $\dim_k T_x(X) = 2$ for $t = 0$.

2.6. Definition. Let $x \in X = \text{Spec}(A)$ we say that X is *regular* at x if $A_{\mathfrak{p}_x}$ is regular. Otherwise we say that x is a *singular* point.

For $x \in X = \mathcal{Z}(I)$ and $A = k[X_1, \dots, X_n]/I$ finitely generated saying that X is regular at x means that we have $\dim A_{\mathfrak{m}_x} = \dim_k T_x(X)$.

2.7. Corollary. (Jacobian criterion). For $x \in X = \mathcal{Z}(I)$, $A = k[X_1, \dots, X_n]/I$ and $I = (f_1, \dots, f_r)$ a radical ideal consider the $r \times n$ matrix

$$\text{Jac}_x := \left(\frac{\partial f_i}{\partial X_j}(x) \right)$$

We have that X is regular at x if and only if

$$\text{rank}(\text{Jac}_x) = n - \dim A_{\mathfrak{m}_x}$$

Since this characterisation due to Zariski of the tangent space is purely algebraic we may even define it in general.

2.8. Definition. (Zariski tangent space). For $X = \text{Spec}(A)$ of any k -algebra A let $x \in X(k) \subset \text{Max}(A)$ be a rational point, i.e. a maximal ideal $\mathfrak{m}_x \subset A$ such that $A/\mathfrak{m}_x = k$. We set

$$T_x(X) := (\mathfrak{m}_x/\mathfrak{m}_x^2)^\vee$$

3. Tangent space and dual numbers

Consider the so-called *ring of dual numbers* given by $k[\varepsilon] := k[t]/(t^2)$. A dual number is written as $a + b\varepsilon$ with $a, b \in k$ and $\varepsilon^2 = 0$ and it is a unit if and only if $a \neq 0$ (the inverse is $a^{-1} - a^{-2}b\varepsilon$). As a consequence, we see that the dual numbers over any field k form a Artin local ring with nilpotent maximal ideal (ε) . We then have $k[\varepsilon] \rightarrow k$ by sending ε to zero. Since $(\varepsilon) \cong k$ we can regard $k[\varepsilon] = k \oplus k$ with the ring structure given by $\varepsilon^2 = 0$.

For a k -algebra A let $x \in X(k) \subset \text{Max}(A)$ be a maximal ideal $\mathfrak{m}_x \subset A$ such that $A/\mathfrak{m}_x = k$. For any k -linear $\ell : \mathfrak{m}_x/\mathfrak{m}_x^2 \rightarrow k$ we get a push-out diagram

$$(3.1) \quad \begin{array}{ccccccc} 0 & \longrightarrow & \mathfrak{m}_x/\mathfrak{m}_x^2 & \longrightarrow & A/\mathfrak{m}_x^2 & \longrightarrow & k \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \parallel \\ 0 & \longrightarrow & (\varepsilon) & \longrightarrow & k[\varepsilon] & \longrightarrow & k \longrightarrow 0 \end{array}$$

inducing by composition with the projection a k -algebra homomorphism $f_\ell : A \rightarrow k[\varepsilon]$. We therefore obtain a map sending $x \in X(k)$ together with $\ell \in T_x(X)$ to $f_\ell \in \text{Hom}_k(A, k[\varepsilon])$ which we denote

$$(3.2) \quad \varphi : \{(x, \ell) / x \in X(k) \text{ and } \ell \in T_x(X)\} \rightarrow \text{Hom}_k(A, k[\varepsilon])$$

3.1. Proposition. *The map φ in (3.2) is an isomorphism.*

PROOF. A k -algebra homomorphism from A to $k[\varepsilon]$ say $f \in \text{Hom}_k(A, k[\varepsilon])$ is provided with a maximal ideal $\mathfrak{m}_x \subset A$ given by the kernel of the composition into k . By restriction of f to $\mathfrak{m}_x \subset A$ we get $\mathfrak{m}_x \rightarrow (\varepsilon)$ thus a k -linear mapping $\ell : \mathfrak{m}_x/\mathfrak{m}_x^2 \rightarrow (\varepsilon) \cong k$ since $\varepsilon^2 = 0$. This is showing that φ is invertible (note that the push-out diagram in 3.1 grants it). \square

3.2. Remark. (a) Note that the previous constructions are local. This means that the push-out diagram in 3.1 can be provided for $A_{\mathfrak{m}_x}$ without changes and $\text{Hom}_k(A, k[\varepsilon])$ can be nicely described by the collection of pairs $\{(x, f_x)\}$ where $x \in X(k)$ and f_x is a local k -homomorphism $f_x : A_{\mathfrak{m}_x} \rightarrow k[\varepsilon]$. In fact, in the proof of 3.1 since $k[\varepsilon]$ is local, \mathfrak{m}_x

is mapped to (ε) and $f(A - \mathfrak{m}_x)$ is invertible in $k[\varepsilon]$ we get $f_x \in \text{Hom}_k(A_{\mathfrak{m}_x}, k[\varepsilon])$ by the universal property of $A_{\mathfrak{m}_x}$. By restriction of f_x to $\mathfrak{m}_x A_{\mathfrak{m}_x}$ we get the same k -linear mapping as in the proof of 3.1.

(b) The result in 3.1 can be translated in the functorial language as follows. Consider the covariant representable functor $F = \text{Hom}_k(A, -)$ on the category of k -algebras and the induced mapping $F(k[\varepsilon]) \rightarrow F(k)$. Let $x \in F(k)$ and let $T_x(X)$ denote the subset of $F(k[\varepsilon])$ of those elements mapping to x . Then $T_x(X)$ is actually the Zariski tangent space. This translation suggests that one can define the tangent space to a functor F even if it is not representable.

(c) Notably, the interpretation of the tangent space given in 3.1 is suggesting that in order to develop differential geometry techniques catching infinitesimal phenomena in algebraic geometry we have to handle the functor $\text{Hom}_k(A, -)$ on *non* reduced rings. Roughly, its value on fields is concerned with points and its value on local Artinian rings provides infinitesimal neighbourhoods of points.

Bibliography

- [1] M. Artin (1966), *Commutative rings*, Mimeographed lecture notes (18.732), MIT, Boston, Mass.
- [2] M. F. Atiyah and I. Macdonald (1969), *Introduction to commutative algebra*, Addison-Wesley, Reading, Mass.
- [3] L. Barbieri-Viale (2009), *Lecture Notes on Algebraic Geometry*.
- [4] D. Eisenbud (2004), *Commutative algebra with a view toward algebraic geometry*, Springer, NY.
- [5] A. Grothendieck and J. Dieudonné (1960), *Éléments de Géométrie Algébrique I, Le Langage des Schémas*, Publications Mathématiques, IHES, Paris.
- [6] R. Hartshorne (1997), *Algebraic Geometry*, GTM, Springer-Verlag, NY.
- [7] H. Matsumura (1986), *Commutative ring theory*, Cambridge Univ. Press, Cambridge.
- [8] Q. Liu (2006), *Algebraic Geometry and Arithmetic Curves*, Oxford Univ. Press Inc., NY
- [9] M. Reid (1995), *Undergraduate commutative algebra*, London Mathematical Society, London.