# A geometric introduction to commutative algebra

by Enrique Arrondo(*)

Version of September 18th, 2023



These notes correspond to the course of Commutative Algebra that I started teaching the academic year 2003/2004 at the Universidad Complutense de Madrid. Since I am still teaching the course for a third year, the notes (which were incomplete) are suffering continuous changes. I thank my students of each year for their patience and suggestions (I have to thank very particularly to Pepe Higes for many corrections). In the unlikely event that I will succeed in writing something sensible, my goal was to present a self-contained basic introduction to the main topics of commutative algebra, regarded from a geometric point of view.

(*) Departamento de Álgebra, Facultad de Ciencias Matemáticas, Universidad Complutense de Madrid, 28040 Madrid, Spain, Enrique_Arrondo@mat.ucm.es

# 0. Introduction and preliminaries

Our starting point will be the study of subsets of the affine space $\mathbb{A}^n_{\mathbb{K}}$ defined by polynomial equations. More precisely:

**Definition.** Let $S$ be an arbitrary subset of the polynomial ring $\mathbb{K}[X_1, \ldots, X_n]$. Then the set $V(S) = \{(a_1, \ldots, a_n) \in \mathbb{A}^n_{\mathbb{K}} \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in S\}$ is called an *affine set*.

For instance, it is a classical subject the study of plane curves, i.e. subsets in $\mathbb{A}^2_{\mathbb{K}}$ defined as the zero locus of a polynomial in two indeterminates (e.g if the polynomial has degree two the curve is called a conic). We can find however several pathologies:

**Example 0.1.** The zero locus of a polynomial could be smaller than expected, or even empty. For example, the polynomial $X^2 + Y^2$ defines only the point $(0, 0)$ rather than a curve if our ground field is $\mathbb{R}$, while the polynomial $X^2 + Y^2 + 1$ does not have any zero locus at all.

**Example 0.2.** On the opposite side we have that sometimes a nonzero polynomial can define the whole plane. This is the case for instance of the polynomial $X^p + Y^p - X - Y$ if the ground field is $\mathbb{Z}_p$, the finite field of $p$ elements.

**Example 0.3.** The same curve can be defined by different polynomials. For instance, the polynomials $X$ and $X^2$ define the same line, and if the ground field is $\mathbb{R}$ we can also consider other polynomials like $X(X^2 + Y^2)$.

Any text or course on plane curves (see for instance [Fi]) will show that the situation of Example 0.2 is only possible for finite fields, and that the one of Example 0.1 only occurs if the ground field is not algebraically closed. About the situation of Example 0.3, again assuming that the ground field is algebraically closed we can find a satisfactory answer: there is a so-called minimal polynomial defining the curve, with the property that any other polynomial vanishing on the curve is a multiple of this minimal equation (this result or a variant of it is usually known as Study's lemma). And because of this property, such a minimal polynomial is unique up to multiplication by a nonzero constant. Moreover, this minimal polynomial can be found from any other equation of the curve by just removing the exponents of any possible multiple factor of it.

If we try to generalize plane curves to affine sets we immediately see that the situation changes a lot. For example, it looks clear that the line $X + Y = Z - Y = 0$ cannot be defined by only one equation (unless we want to face some of the above pathologies, for instance working on $\mathbb{R}$ and considering only the equation $(X + Y)^2 + (Z - Y)^2 = 0$). We can therefore wonder whether $X + Y$ and $Z - Y$ can be considered as a kind of minimal equations of the line. But why those two and not $X + Y$ and $X + Z$? You could argue

that both pairs are essentially the same, since you can pass from one to another by taking linear combinations, or written in a matricial way

$$\begin{pmatrix} X+Y \\ X+Z \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} X+Y \\ Z-Y \end{pmatrix}$$

and hence they are the same up to multiplication by an invertible matrix of constants (the analogue to the multiplication by a nonzero constant in our case). But I could still propose $X+Y$ and $X+Z-X^2-XY$ as another pair of minimal equations, since the second equation of the original pair can be expressed in terms of the new one as $X+Z = X(X+Y)+(X+Z-X^2-XY)$. And now there is no way of passing from one pair to another by just multiplying by an invertible matrix of constants, since we need to use polynomials in the linear combinations.

This shows that the set of equations of an arbitrary affine set is not as easy as the one for curves, although at least we see readily that any linear combination (with coefficients arbitrary polynomials) of equations of an affine set is still an equation of the set. This motivates the following:

**Definition.** Given any subset $Z \subset \mathbb{A}^n_{\mathbb{K}}$, the set $I(Z) = \{f \in \mathbb{K}[X_1, \ldots, X_n] \mid f(p) = 0 \text{ for any } p \in Z\}$ is an ideal of $\mathbb{K}[X_1, \ldots, X_n]$ called the *ideal of the set* $Z$.

From this point of view, Study's lemma is saying that the ideal of a plane curve is principal (i.e. it is generated by one element), while in our previous example we were just finding different sets of generators of the ideal of the line, which is now the natural generalization of Study's lemma (and the generalization of how to find the minimal equation for plane curves will be the so-called Hilbert's Nullstellensatz, see Theorem 1.19).

Observe that if an affine set of $\mathbb{A}^n_{\mathbb{K}}$ is defined by a set $S \subset \mathbb{K}[X_1, \ldots, X_n]$, then it is also defined by the ideal generated by $S$. Hence any affine set $Z \subset \mathbb{A}^n_{\mathbb{K}}$ can be written as $V(I)$, for some ideal $I \subset \mathbb{K}[X_1, \ldots, X_n]$; this is a very useful remark, since the Hilbert's basis theorem (see Theorem 2.2) will show that $I$ is finitely generated, and hence any affine set can be described with a finite number of equations. In this context, the ideal $I(Z)$ we just defined is the biggest ideal defining $Z$. It is clear that, if $f^m$ vanishes on $Z$, then also $f$ vanishing on $Z$.

**Definition.** The *radical of an ideal* $I$ of a ring $A$ is the set $\sqrt{I}$ defined as the set of all the elements $f \in A$ for which there exists some $m \in \mathbb{N}$ such that $f^m$ is in $I$ (it is an easy exercise to see that $\sqrt{I}$ is an ideal). A *radical ideal* is an ideal such that $\sqrt{I} = I$ (it is also an easy exercise to see that the radical of an ideal is a radical ideal, i.e. that $\sqrt{\sqrt{I}} = \sqrt{I}$ for any ideal $I$).

After these definitions, our last remark can be interpreted by saying that $I(Z)$ is a radical ideal, and that for any ideal $I$, the sets $V(I)$ and $V(\sqrt{I})$ are the same. The

Nullstellensatz (Theorem 1.19) will say that, when $\mathbb{K}$ is algebraically closed, the ideal of $V(I)$ is precisely $\sqrt{I}$.

We now show how the situation of Example 0.2 is not possible for general affine sets when $\mathbb{K}$ is infinite.

**Proposition 0.4.** *If $\mathbb{K}$ is an infinite field, then $I(\mathbb{A}^n_{\mathbb{K}}) = \{0\}$, i.e. the polynomial vanishing at all the points of $\mathbb{A}^n_{\mathbb{K}}$ is zero.*

*Proof:* We will use induction on $n$. For $n = 1$, the statement says that if a polynomial in one indeterminate vanishes at all the points of $\mathbb{A}^1_{\mathbb{K}} = \mathbb{K}$, then it is the zero polynomial, which is trivial if $\mathbb{K}$ is infinite (since the number of roots of a polynomial is bounded by its degree).

If $n > 1$, we have to prove that any non-zero polynomial $f \in \mathbb{K}[X_1, \ldots, X_n]$ does not vanish at all the points of $\mathbb{A}^n_{\mathbb{K}}$. To show this, we write the polynomial as a polynomial (of degree say $d$) in the indeterminate $X_n$, i.e. $f = f_0 + f_1 X_n + \ldots + f_d X_n^d$, where $f_0, f_1, \ldots, f_d \in \mathbb{K}[X_1, \ldots, X_{n-1}]$ and $f_d \neq 0$. By induction hypothesis, there exists $(a_1, \ldots, a_{n-1}) \in \mathbb{A}^{n-1}_{\mathbb{K}}$ such that $f_d(a_1, \ldots, a_{n-1}) \neq 0$. We have now the nonzero polynomial $f_0(a_1, \ldots, a_{n-1}) + f_1(a_1, \ldots, a_{n-1})X_n + \ldots + f_d(a_1, \ldots, a_{n-1})X_n^d \in \mathbb{K}[X_n]$, which as before cannot vanish for all the elements of $\mathbb{K}$. Therefore there exists $a_n \in \mathbb{K}$ not vanishing at it, which means that $f(a_1, \ldots, a_n)$ is not zero, as wanted. □

Since operators $V$ and $I$ reverse the inclusions, it seems natural to guess that the smallest non-empty affine subsets correspond to the biggest proper ideals of $\mathbb{K}[X_1, \ldots, X_n]$. We recall the precise algebraic definition:

**Definition.** A *maximal ideal* of a ring $A$ is a proper ideal $\mathfrak{m}$ such that any other ideal containing $\mathfrak{m}$ is necessarily $A$. Equivalently (this is an easy exercise), the ideal $\mathfrak{m} \subset A$ is maximal if and only if the quotient ring $A/\mathfrak{m}$ is a field.

**Example 0.5.** Let us consider the point $O = (0, \ldots, 0) \in \mathbb{A}^n_{\mathbb{K}}$. It is clear that a polynomial $f$ vanishing at $O$ is characterized by the fact of not having independent term, which is in turn equivalent to belonging to the ideal $(X_1, \ldots, X_n)$ (i.e. the ideal generated by $X_1, \ldots, X_n$). Hence $I(O) = (X_1, \ldots, X_n)$. By performing a translation, this implies that, given any point $p = (a_1, \ldots, a_n)$, $I(p) = (X_1 - a_1, \ldots, X_n - a_n)$. This is in fact a maximal ideal, since the composition map $\mathbb{K} \hookrightarrow \mathbb{K}[X_1, \ldots, X_n] \to \mathbb{K}[X_1, \ldots, X_n]/I(p)$ is an isomorphism: it is immediate to see that it is injective, and for the surjectivity we just write any $f \in \mathbb{K}[X_1, \ldots, X_n]$ as $f = (f - f(p)) + f(p)$ and observe that $f - f(p)$ belongs to $I(p)$; hence the class of $f$ modulo $I(p)$ is the image of $f(p)$. An equivalent statement of Hilbert's Nullstellensatz will be that, if $\mathbb{K}$ is algebraically closed, then all the maximal ideals of $\mathbb{K}[X_1, \ldots, X_n]$ are of this type (see Corollary 1.17).

**Example 0.6.** If $\mathbb{K}$ is not algebraically closed we can find other maximal ideals in $\mathbb{K}[X_1, \ldots, X_n]$. For example, in $\mathbb{R}[X]$, a maximal ideal is generated by an irreducible polynomial, hence of the type $(X-a)$ or $((X-a)^2+b^2)$ (with $b \neq 0$). In the first case we have $(X-a) = I(a)$, but in the second case we get a different situation, since $((X-a)^2+b^2)$ is the set of real polynomials vanishing at the imaginary conjugate points $a \pm bi$. In general, if we have two imaginary conjugate points in $\mathbb{A}^n_{\mathbb{R}}$, after a (real) change of coordinates we can assume that the two points are $(\pm i, 0, \ldots, 0)$ (check this!). It is then clear that the set of real polynomials vanishing at those points is $(X_1^2+1, X_2, \ldots, X_n)$, which is a maximal ideal since $\mathbb{R}[X_1, \ldots, X_n]/(X_1^2+1, X_2, \ldots, X_n)$ is isomorphic to $\mathbb{R}[X_1]/(X_1^2+1)$, which in turn is isomorphic to the field $\mathbb{C}$. Hence we have found in $\mathbb{R}[X_1, \ldots, X_n]$ two kinds of maximal ideals: those corresponding to real points in $\mathbb{A}^n_{\mathbb{R}}$ and those corresponding to pairs of conjugate imaginary points. Again, Hilbert's Nullstellensatz (but its more general version of Theorem 5.14) will imply that these are the only maximal ideals (see Remark 5.16).

**Example 0.7.** For arbitrary ground fields the situation becomes more complicated. Already in one variable, a maximal ideal of $\mathbb{Q}[X]$ is generated by an irreducible polynomial $f$ (which can have arbitrarily large degree). Hence this maximal ideal is the set of rational polynomials vanishing at all the roots of $f$. To put it in a way that recalls Example 0.6, if $\alpha$ is a root of $f$, we can say that the maximal ideal is the set of rational polynomials vanishing at $\alpha$ and any other conjugate element of $\alpha$ (in the sense of Galois theory). This illustrates how to proceed for an arbitrary number of variables. Just to give a sample, consider the point $(\sqrt[4]{2}+\sqrt{2}, \sqrt[4]{8})$. Its coordinates are in the degree four algebraic extension $\mathbb{Q}(\sqrt[4]{2})$ of $\mathbb{Q}$. The conjugates of $\sqrt[4]{2}$ are $\pm\sqrt[4]{2}$ and $\pm\sqrt[4]{2}i$. Hence we should consider the ideal of all the rational polynomials vanishing at the points

$$P_1 = (\sqrt[4]{2}+\sqrt{2}, \sqrt[4]{8})$$

$$P_2 = (-\sqrt[4]{2}+\sqrt{2}, -\sqrt[4]{8})$$

$$P_3 = (\sqrt[4]{2}i-\sqrt{2}, -\sqrt[4]{8}i)$$

$$P_4 = (-\sqrt[4]{2}i-\sqrt{2}, \sqrt[4]{8}i).$$

Since four points define a pencil of conics, we start by considering the simplest elements of this pencil, namely the union of the lines $P_1P_2$ and $P_3P_4$, of equation

$$(2-\sqrt{2}X+Y)(2+\sqrt{2}X+Y) = 4+4Y-2X^2+Y^2,$$

the union of the lines $P_1P_3$ and $P_2P_4$, of equation (we skip the tedious computations)

$$-16+8\sqrt{2}i-16X+8\sqrt{2}iY-4\sqrt{2}iX^2+8XY+8Y^2+2\sqrt{2}iY^2$$

and the union of the lines $P_1P_4$ and $P_2P_3$, of equation

$$-16 - 8\sqrt{2}i - 16X - 8\sqrt{2}iY + 4\sqrt{2}iX^2 + 8XY + 8Y^2 - 2\sqrt{2}iY^2.$$

Only the first of the three equations is rational, but the two others are conjugate, and there sum is (after dividing by a constant)

$$-2 - 2X + XY + Y^2$$

(observe that the imaginary part of the two conjugate equations was, up to multiplication by a constant, the first rational equation we got). Hence our ideal contains the elements

$$f = 4 + 4Y - 2X^2 + Y^2, g = -2 - 2X + XY + Y^2.$$

Since both equations generate the pencil of conics through $P_1, P_2, P_3, P_4$, it seems natural to suspect that these two equations generate the ideal we are looking for. We will check it in an indirect way that shows another technique to deal with this kind of problems. First of all, observe that the second coordinates of the points $P_1, P_2, P_3, P_4$ are the roots of $Y^4 - 8$ (a more complicated path is to start observing that the first coordinates are the roots of $X^4 - 4X^2 - 8X + 2$). And secondly, observe also that the first coordinate can be written in terms of the second one by the formula $X = 4Y^3 + 2Y^2$. We thus consider the ideal $\mathfrak{m} = (Y^4 - 8, X - 4Y^3 - 2Y^2)$ (the reader is invited to check that this ideal coincides with the ideal generated by $f$ and $g$). This is a maximal ideal, because $\mathbb{Q}[X, Y]/\mathfrak{m} \cong \mathbb{Q}[Y]/(Y^4 - 8)$ (where the isomorphism is defined by assigning to the class of $h(X, Y)$ the class of $h(4Y^3 + 2Y^2, Y)$), and the latter is a field because $Y^4 - 8$ is an irreducible polynomial (observe that this field is canonically isomorphic to $\mathbb{Q}(\sqrt[4]{8})$, which coincides with $\mathbb{Q}(\sqrt[4]{2})$). Since the ideal of all the polynomials vanishing at $P_1, P_2, P_3, P_4$ is not the whole $\mathbb{Q}[X, Y]$ and contains the maximal ideal $\mathfrak{m}$, it follows that it coincides with $\mathfrak{m}$. As in the previous example, we will see in Theorem 5.14 Remark 5.16 that this is the way of getting all the maximal ideals.

**Remark 0.8.** Observe that Example 0.5 provides an algebraic way of defining the map $\mathbb{A}^n_{\mathbb{K}} \to \mathbb{K}$ determined by a polynomial $f \in \mathbb{K}[X_1, \ldots, X_n]$. Indeed, given a point $p = (a_1, \ldots, a_n)$, we got a natural isomorphism between $\mathbb{K}[X_1, \ldots, X_n]/I(p)$ and $\mathbb{K}$ defined by assigning to the class of $f$ modulo $I(p)$ the value $f(p)$. Hence we can identify $f(p)$ with the class of $f$ modulo $I(p)$. As we have seen in the previous examples, when $\mathbb{K}$ is not algebraically closed, we have more maximal ideals than the ones corresponding to points. The same construction can be done there, since in those cases we had an isomorphism among $\mathbb{K}[X_1, \ldots, X_n]/\mathfrak{m}$ and a finite extension of $\mathbb{K}$ (to which the coordinates of the points corresponding to $\mathfrak{m}$ belong to). For instance, when $\mathbb{K} = \mathbb{R}$ we can interpret any

$f \in \mathbb{R}[X_1, \ldots, X_n]$ as two different maps: one is the polynomial map $\mathbb{A}^n_{\mathbb{R}} \to \mathbb{R}$ corresponding to the points with real coefficients, and another one that assigns to any maximal ideal corresponding to two conjugate imaginary points the evaluation of $f$ at any of these two points (thus giving a complex number). Observe that if we replace $\mathbb{R}$ with $\mathbb{Q}$ then we would get as many quotient fields as finite extensions of $\mathbb{Q}$. Hence a polynomial in $\mathbb{Q}[X_1, \ldots, X_n]$ can be regarded as infinitely many maps with different targets.

**Remark 0.9.** We can repeat the same construction in rings not related with polynomial rings and hence apparently far from any possible geometry. For instance, consider the set of maximal ideals of $\mathbb{Z}$, i.e. the ideals generated by a prime number $p$. In this case, an element $n \in \mathbb{Z}$ can be regarded as the assignment to any prime number $p$ the class of $n$ in the field $\mathbb{Z}_p$. Hence in this case the target field changes for any maximal ideal in $\mathbb{Z}$. This could look quite unreasonable (and maybe it is so), but we will see that, from this point of view, the set of prime numbers behave much as a geometric line (from the point of view of rings $\mathbb{Z}$ and $\mathbb{K}[X]$ are P.I.D., so that they should share a lot of properties).

We have so far justified the study of $\mathbb{K}[X_1, \ldots, X_n]$ and its ideals. But is this enough to justify the interest of studying more arbitrary rings? We end this section by showing how it is interesting to study other rings (although for the time being our examples will be closely related to polynomial rings).

**Definition.** A *regular function* on an affine set $Z \subset \mathbb{A}^n$ is a function $\varphi : Z \to \mathbb{A}^n$ defined globally by a polynomial $f \in \mathbb{K}[X_1, \ldots, X_n]$. The set of all the regular functions on $Z$ will be denoted by $\mathcal{O}(Z)$.

By definition, there is a surjective map $\mathbb{K}[X_1, \ldots, X_n] \to \mathcal{O}(Z)$ assigning to any polynomial $f$ the function it defines. This is clearly a homomorphism of rings, and its kernel is precisely $I(Z)$. We have therefore a natural isomorphism between $\mathcal{O}(Z)$ and $\mathbb{K}[X_1, \ldots, X_n]/I(Z)$. We will see in these notes that the study of this ring will give most of the geometric properties of the affine set $Z$ (as a first example, we can mention that from Exercise 1.4(vi) there is a bijection between the maximal ideals of $\mathcal{O}(Z)$ and the maximal ideals of $\mathbb{K}[X_1, \ldots, X_n]$ containing $I(Z)$; if $\mathbb{K}$ is algebraically closed, this means that $Z$ can be identified with the set of maximal ideals of $\mathcal{O}(Z)$). Examples 0.6 and 0.7 suggest that, if we replace $I(Z)$ with other ideal defining the empty set, then the set of maximal ideals of this new quotient should represent the set of "imaginary" points defined by the ideal. Hence it look natural to study the set of maximal ideals of any ring (in fact the natural think will be to consider the set of prime ideals). For instance, when considering rings related with $\mathbb{Z}$, this would allow to give geometrical meaning to notions of number theory. Our scope in these notes will be thus to study arbitrary rings and ideals, having in mind the previous geometric interpretation.

# 1. Rings and ideals; the Nullstellensatz

We start by recalling some basic facts about ring and ideals. Throughout these notes, all the rings will be assumed to be commutative and will have a unity element 1 for the product.

**Definition.** A *prime ideal* of a ring $A$ is an ideal $\mathfrak{p}$ such that whenever $fg \in \mathfrak{p}$ for two elements $f, g \in A$, then necessarily $f \in \mathfrak{p}$ or $g \in \mathfrak{p}$. Obviously, we can replace the product of two elements by the product of a finite number of elements of $A$.

The property defining prime ideals can be translated into ideals rather than elements. We recall first the definition of product of ideals.

**Definition.** The *product of the ideals* $I_1, \ldots, I_n$ is defined to be the ideal $I_1 \ldots I_r$ generated by the set of products $f_1 \ldots f_r$, with $f_i \in I_i$ for $i = 1, \ldots, r$. In particular, the *$r$-th power of an ideal* $I$ is defined to be the ideal $I^r$ generated by the products of $r$ elements of $I$ (be careful! because $I^r$ is NOT the ideal generated by the elements $f^r$ with $f \in I$).

**Lemma 1.1.** *An ideal $\mathfrak{p}$ of a ring $A$ is prime if and only if whenever $\mathfrak{p} \supset I_1 \ldots I_r$ (with $I_1, \ldots, I_r$ ideals of $A$) it necessarily holds that $\mathfrak{p}$ contains some $I_i$, $i = 1, \ldots, r$. In particular, if $\mathfrak{p}$ is a prime ideal containing the intersection of a finite number of ideals $\mathfrak{p} \supset I_1 \cap \ldots \cap I_r$, then $\mathfrak{p}$ contains some $I_i$.*

*Proof:* The "if" part of the statement is almost trivial. Given $f, g \in A$ such that $fg \in \mathfrak{p}$, we can re-write this last condition as saying that $\mathfrak{p}$ contains $(f)(g)$, the product of the ideals $(f)$ and $(g)$. By hypotheses, $\mathfrak{p}$ contains then either $(f)$ or $(g)$, hence it contains either $f$ or $g$, which proves that $\mathfrak{p}$ is prime.

For the "only if" part, assume $\mathfrak{p} \supset I_1 \ldots I_r$. Suppose for contradiction that for each $i = 1, \ldots, r$ the ideal $I_i$ is not contained in $\mathfrak{p}$ we could find an element $f_i$ in $I_i$ but not in $\mathfrak{p}$. But then the element $f_1 \ldots f_r$ would be in $I_1 \ldots I_r$, but on the other hand it cannot be in $\mathfrak{p}$ because $\mathfrak{p}$ is prime, which is absurd.

The last part of the statement is immediate by observing that there is an inclusion $I_1 \ldots I_r \subset I_1 \cap \ldots \cap I_r$. □

**Remark 1.2.** Observe that in the above characterization of prime ideals we cannot replace $I_1 \ldots I_r$ with $I_1 \cap \ldots \cap I_r$. For instance, it is easy to see that the ideal $(X^2) \subset \mathbb{K}[X]$ satisfies that whenever $(X^2) \supset I_1 \cap \ldots \cap I_r$ then it contains some $I_i$ (do it as an exercise, by using that $\mathbb{K}[X]$ is a P.I.D.). In fact any $(p^s)$ with $s \geq 2$, where $p$ is an irreducible element of a P.I.D. gives a counterexample. It is not by chance that we need to use powers for a

counterexample; this is in fact the underlying idea of primary ideal that we will study in the next section.

We give now a simple result giving a sufficient condition for the intersection of two ideal two coincide with their product. This is especially useful when one tries to find generators of the intersection of ideals.

**Lemma 1.3.** *Let $I, J \subset A$ be two ideals such that $I + J = A$. Then $IJ = I \cap J$.*

*Proof:* We always have $IJ = I \subset J$, so that it is enough to prove the other inclusion. Since $I + J = A$, we have an equality $1 = f + g$, with $f \in I$ and $g \in J$. Take now any $h \in I \cap J$. We can thus write $h = h1 = h(f+g) = hf + hg$. Since $h \in J$, we have $hf \in IJ$, and since $h \in I$ we also have $hg \in IJ$. Therefore $h \in IJ$, as wanted. □

We give now as an exercise a series of easy properties of ideals that we will use often in the notes.

**Exercise 1.4.** Prove the following properties.

(i) Any maximal ideal is prime.

(ii) Any prime ideal is radical.

(iii) If $I_1, \ldots, I_n$ are ideals, then $\sqrt{I_1 \cap \ldots \cap I_n} = \sqrt{I_1} \cap \ldots \cap \sqrt{I_n}$.

(iv) The inverse image of a prime ideal by a homomorphism of rings is also a prime ideal.

(v) If $I_1 \subset I_2 \subset \ldots$ is an infinite chain of ideals, then $\bigcup_{n\in\mathbb{N}} I_n$ is also an ideal.

(vi) If $I$ is an ideal of $A$, then the projection $\pi : A \to A/I$ induces a bijection between the ideals of $A/I$ and the ideals of $A$ containing $I$. Moreover, this bijection restricts to a bijection between prime ideals of $A/I$ and prime ideals of $A$ containing $I$; a further restriction gives a bijection between maximal ideals of $A/I$ and maximal ideals of $A$ containing $I$.

(vii) Prove that, for any ideal $I$ such that $\sqrt{I}$ is finitely generated, there exists some $m \in \mathbb{N}$ such that $\left(\sqrt{I}\right)^m \subset I$.

We recall now Zorn's Lemma, which we will need to prove a pair of results about ideals.

**Theorem 1.5** (Zorn's Lemma)**.** *Let $\Sigma$ be an ordered set, and assume that any completely ordered set of elements $x_1 \leq x_2 \leq \ldots$ of $\Sigma$ has an upper bound (i.e. there exists $x \in \Sigma$ such that $x_x \leq x$ for each $n \in \mathbb{N}$). Then $\Sigma$ possesses maximal elements (i.e. elements $x$ for which there is no $y \in \Sigma$ such that $x \leq y$).*

**Proposition 1.6.** *For any proper ideal $I$ of a ring $A$, there exists a maximal ideal containing $I$.*

*Proof:* This is an easy application of Zorn's Lemma. Just consider the set $\Sigma$ consisting of all the proper ideals of $A$ containing $I$ and order it by saying that $I_1$ is smaller than $I_2$ if and only if $I_1 \subset I_2$. Then Exercise 1.4(v) implies that $\Sigma$ is in the hypothesis of Zorn's lemma, and clearly a maximal element of $\Sigma$ is a maximal ideal containing $I$. $\square$

**Proposition 1.7.** *If $I$ is a proper ideal of $A$, then $\sqrt{I}$ is the intersection of the prime ideals containing $I$.*

*Proof:* It is clear that $\sqrt{I}$ is contained in any prime ideal containing $I$. Reciprocally, assume that we have $f \notin \sqrt{I}$ and let us prove that then $f$ is not contained in some prime ideal containing $I$. We consider the set $\Sigma$ consisting of all the proper ideals $J \supset I$ such that $f \notin \sqrt{J}$ and order it by the inclusion relation. Exercise 1.4(v) implies that for any chain $I_1 \subset I_2 \subset \ldots$ of ideals in $\Sigma$, the ideal $\bigcup_{n\in\mathbb{N}} I_n$ is an upper bound of $I_1, I_2, \ldots,$. Then Zorn's Lemma implies that $\Sigma$ possesses a maximal element $\mathfrak{p}$. We will finish the proof by showing that $\mathfrak{p}$ is a prime ideal (it is already proper, since it belongs to $\Sigma$).

The first remark is that saying that an element $g \in A$ is not in $\mathfrak{p}$ is equivalent, by the maximality of $\mathfrak{p}$, to say that $f$ belongs to $\sqrt{\mathfrak{p} + (g)}$. We take now two elements $g_1, g_2 \in A$ not in $\mathfrak{p}$, and we need to prove that $g_1 g_2$ is not in $\mathfrak{p}$. By the above remark, we have expressions

$$f^{n_1} = p_1 + h_1 g_1$$

$$f^{n_2} = p_2 + h_2 g_2$$

for some $n_1, n_2 \in \mathbb{N}$ and $h_1, h_2 \in A$. The multiplication of both equalities yields

$$f^{n1+n_2} = (p_1 p_2 + p_1 h_2 g_2 + p_2 h_1 g_1) + h_1 h_2 g_1 g_2 \in \mathfrak{p} + (g_1 g_2)$$

and this implies that $g_1 g_2$ is not in $\mathfrak{p}$, as wanted. $\square$

**Definition.** An element $f \in A$ of a ring is called *nilpotent* if there is some $n \in \mathbb{N}$ such that $f^n = 0$. The *nilradical* of the ring $A$ is $\mathfrak{n} = \sqrt{(0)}$, i.e. the set of all the nilpotent elements of $A$. By the above proposition, the nilradical is the intersection of all the prime ideals of $A$.

We now want to give a geometric interpretation to any ring. For this purpose, we will follow the suggestions of the introduction. The only difference (we will hopefully able to explain why later on) is that, instead of considering just maximal ideals we are going to deal in general with prime ideals.

**Definition.** The *spectrum of a ring* $A$ is the set $\mathrm{Spec}(A)$ consisting of all the prime ideals of $A$.

The idea is to regard any element $f \in A$ as a kind of map defined on $\mathrm{Spec}(A)$. Imitating what we did in Remarks 0.8 and 0.9, given $f \in A$, we assign to each prime ideal $\mathfrak{p}$ the class of $f$ in $A/\mathfrak{p}$ (this is only an integral domain and not a field, if $\mathfrak{p}$ is not maximal; you can take its quotient field, if you prefer). Hence the image of $f$ is zero if and only if $f$ belongs to $\mathfrak{p}$. This motivates the following definitions, which will have the same properties as the corresponding ones in the geometric case.

**Definition.** Given a subset $S \subset A$ we define $V(S)$ as the subset of $\mathrm{Spec}(A)$ consisting of those prime ideals $\mathfrak{p}$ containing $S$ (in terms of the "map" defined by $f$, these are exactly the prime ideals at which $f$ "vanishes"). Similarly, given a subset $X \subset \mathrm{Spec}(A)$, we define $I(X) = \bigcap_{\mathfrak{p} \in X} \mathfrak{p}$, i.e. the set of elements $f \in A$ "vanishing" at all the elements of $X$.

**Example 1.8.** Let us see that our definitions make some sense. If we consider the polynomials $f = X^2 + Y^2 + 1, g = X^2 + 1 \in \mathbb{R}[X, Y]$, we know that they both define the empty set in $\mathbb{A}^2_{\mathbb{R}}$. However, we know that somehow there zero loci cannot be considered to be the same, because $V(f)$ is an imaginary ellipse, while $V(g)$ is a pair of imaginary lines. In fact, we can distinguish both if we regard $V(f), V(g)$ as subsets of $\mathrm{Spec}(\mathbb{R}[X, Y])$ instead of $\mathbb{A}^2_{\mathbb{R}}$ (hence we use the last definition for $V$). Indeed, now $V(f), V(g)$ are not empty and they are different. For instance, the maximal ideal $(X, Y^2 + 1)$ (which represents the imaginary conjugate points $(0, \pm i)$), belongs to $V(f)$ but not to $V(g)$, while the maximal ideal $(X^2 + 1, Y - 1)$ belongs to $V(g)$ but not to $V(f)$. We even have that $V(f) \cap V(g)$ consists (as the geometry says) in just one point, precisely the maximal ideal $(X^2 + 1, Y)$ (which corresponds to the points $(\pm i, 0)$).

We check now the first properties of the operator $V$ defined in the two different contexts of affine sets and spectra of a ring. The first remark is that $V(S)$ coincides (in both contexts) with $V(I)$, where $I$ is the ideal generated by $S$. So if necessary we can always assume that $S$ is an ideal.

**Lemma 1.9.** *The operator $V$ defined on the set of subsets of $\mathbb{K}[X_1, \ldots, X_n]$ (resp. an arbitrary ring $A$) to the set of subsets of $\mathbb{A}^n_{\mathbb{K}}$ (resp. $\mathrm{Spec}(A)$). Then:*

*(i)* $V(1) = \emptyset$ *and* $V(0) = \mathbb{A}^n_{\mathbb{K}}$ *(resp.* $\mathrm{Spec}(A)$*).*

*(ii) If $\{S_j\}_{j \in J}$ is a collection of subsets of $\mathbb{K}[X_1, \ldots, X_n]$ (resp. $A$), then $\bigcap_{j \in J} V(S_j) = V(\bigcup_{j \in J} S_j)$. In particular, if $\{I_j\}_{j \in J}$ is a collection of ideals of $\mathbb{K}[X_1, \ldots, X_n]$ (resp. $A$), then $\bigcap_{j \in J} V(I_j) = V(\sum_{j \in J} I_j)$.*

*(iii) If $I, I'$ are two ideals of $\mathbb{K}[X_1, \ldots, X_n]$ (resp. $A$), then $V(I) \cup V(I') = V(II') = V(I \cap I')$.*

*Proof:* Parts (i) and (ii) are straightforward and are left as an exercise. Part (iii) in the context of $\mathrm{Spec}(A)$ is an immediate consequence of Lemma 1.1. In the context of affine

sets, it is immediate that we have inclusions $V(I) \cup V(I') \subset V(I \cap I') \subset V(II')$, so that it is enough to prove the inclusion $V(II') \subset V(I) \cup V(I')$. Thus assume that we have $p \in V(II')$ but $p \notin V(I)$ and let us prove that then $p \in V(I')$, i.e that $f'(p) = 0$ for any $f' \in I'$. The assumption $p \notin V(I)$ means that there exists $f \in I$ such that $f(p) \neq 0$. We now take any $f' \in I'$. Hence $ff' \in II'$ and since $p \in V(II')$ it follows that $f(p)f'(p) = 0$. Since $f(p) \neq 0$, we conclude $f'(p) = 0$, as wanted. □

Observe that the above lemma is saying that the sets of the form $V(S)$ satisfy the axioms of the closed sets of a topology. We thus make the following:

**Definition.** The *Zariski topology* on the affine space $\mathbb{A}^n$ (resp. $\mathrm{Spec}(A)$) is the one for which the closed sets are precisely the sets of the form $V(S)$ with $S \subset \mathbb{K}[X_1, \ldots, X_n]$ (resp. $S \subset A$).

We enumerate now as an (easy) exercise the common properties of $V$ and $I$ in the two contexts:

**Exercise 1.10.** Prove the following properties of the operators $V$ and $I$:

(i) The sets of the form $D(f) = \mathbb{A}^n_{\mathbb{K}} \setminus V(f)$ (resp. $D(f) = \mathrm{Spec}(A) \setminus V(f)$) form a basis of the Zariski topology when $f$ varies in $\mathbb{K}[X_1, \ldots, X_n]$ (resp. $A$).

(ii) If, $I, J$ are two ideals of $\mathbb{K}[X_1, \ldots, X_n]$ (resp. $A$), then $V(I) = V(J)$ if and only if $\sqrt{I} = \sqrt{J}$.

(iii) If $\{Z_j\}_{j \in J}$ is a collection of subsets of $\mathbb{A}^n_{\mathbb{K}}$ (resp. $\mathrm{Spec}(A)$), then $I(\bigcup_{j \in J} X_j) = \bigcap_{j \in J} I(X_j)$.

(iv) For any subset $Z$ of $\mathbb{A}^n_{\mathbb{K}}$ (resp. $\mathrm{Spec}(A)$), $V(I(Z))$ is the topological closure of $Z$ (hence $V(I(Z)) = Z$ if $Z$ is a closed set).

The special properties of the operators $V$ and $I$ in $\mathrm{Spec}(A)$ are collected in this other exercise:

**Exercise 1.11.** If $A$ a is ring, prove the following properties:

(i) $I(\mathrm{Spec}(A)) = \sqrt{(0)}$ (compare with Proposition 0.4)

(ii) The set $\{\mathfrak{p}\}$ is closed in the Zariski topology if and only if $\mathfrak{p}$ is a maximal ideal.

(iii) If $I$ is an ideal of $A$, then $I(V(I)) = \sqrt{I}$ (the analogue in the geometric case is a very hard result, known as Nullstellensatz and valid only if $\mathbb{K}$ is algebraically closed, which we will prove in Theorem 1.19; in the case of a spectrum, it is just an immediate consequence of Proposition 1.7).

(iv) As a consequence, prove that $V$ and $I$ define a bijection between the set of radical ideals of $A$ and the set of closed sets of $\mathrm{Spec}(A)$.

In the previous section we obtained maximal ideals from points, by observing that a point is the smallest possible non-empty affine set; a weaker fact is that it cannot be split into different affine pieces. The precise general definition is the following:

**Definition.** A nonempty closed subset $Z \subset A$ of a topological space $A$ (think of $A$ as an affine space or a spectrum of a ring, with the Zariski topology) is called *irreducible* if it satisfies any of the following (clearly equivalent) properties:

(i) $Z$ cannot be expressed as a union $Z = Z_1 \cup Z_2$, with $Z_1 \subsetneq Z$ and $Z_2 \subsetneq Z$ closed subsets of $A$.

(ii) If $Z \subset Z_1 \cup Z_2$ (with $Z_1$ and $Z_2$ closed sets of $A$) then either $X \subset Z_1$ or $X \subset Z_2$.

(iii) Any two nonempty open sets of $Z$ necessarily meet.

If $A = \mathbb{A}^n$ with the Zariski topology and $Z$ is an irreducible affine set, then $Z$ is also called an *affine variety*.

The algebraic translation of this concept is given by the following (see also Lemma 1.1):

**Lemma 1.12.** *A closed subset $Z$ in $\mathbb{A}^n_{\mathbb{K}}$ (resp.* $\mathrm{Spec}(A)$*) is irreducible if and only if its ideal $I(Z)$ is prime.*

*Proof:* We will do the prove in $\mathbb{A}^n_{\mathbb{K}}$, the proof for $\mathrm{Spec}(A)$ being identical. Observe that $I(Z)$ is the whole polynomial ring $\mathbb{K}[X_1, \ldots, X_n]$ if and only if $Z$ is the empty set. Hence we are dealing with nonempty sets and proper ideals.

Assume first $Z$ is irreducible. Let $f, g$ be polynomials such that $fg \in I(Z)$. Then clearly $Z \subset V(f) \cup V(g)$, so that the irreducibility implies that either $Z \subset V(f)$ or $X \subset V(g)$. But the latter is equivalent to $f \in I(Z)$ or $g \in I(Z)$, which proves that $I(Z)$ is prime.

Assume now that $I(Z)$ is prime and $Z \subset Z_1 \cup Z_2$ with $Z_1, Z_2$ affine sets. Suppose $Z \not\subset Z_1$ and $Z \not\subset Z_2$. Then $I(Z_1) \not\subset I(Z)$ and $I(Z_2) \not\subset I(Z)$. We can therefore find polynomials $f \in I(Z_1)$ and $g \in I(Z_2)$ none of them in $I(Z)$. But $fg \in I(Z_1 \cup Z_2) \subset I(Z)$, which contradicts the fact that $I(Z)$ is prime. This completes the proof of the Lemma. □

Lemma 1.9 and Exercise 1.10(iii) show that the union of closed sets corresponds to the intersection of ideals, while intersection of closed sets corresponds to the sum of ideals. However, this correspondence is not complete. The cute reader probably has already missed that we did not claim that the ideal of the union of closed sets is the sum of their corresponding ideals. In fact, this is not true, as the following example will show.

**Example 1.14.** Consider the affine sets $C = V(Y - X^2)$ and $L = V(Y)$ of $\mathbb{A}^2$. They are respectively a parabola and a line tangent to it. It is not difficult to see that $I(C) = (Y - X^2)$ and $I(L) = (Y)$. We have therefore $I(C) + I(L) = (X^2, Y) \neq (X, Y) = I(\{(0,0\}) = I(C \cap L)$. However this fact should be considered natural, because $C$ and $L$ share not only the point $(0,0)$, but also the horizontal tangent direction, and this is what the ideal $(X^2, Y)$ encodes. Indeed, a polynomial $f$ belongs to $(X, Y)$ if and only if the curve $V(f)$ passes through $(0,0)$, while $f$ belongs to $(X^2, Y)$ if and only if $V(f)$ passes through $(0,0)$ in the horizontal direction (or more properly if the line $Y = 0$ meets the curve at $(0,0)$ with multiplicity at least two). The idea you should have in mind is that non-radical ideals encode some "infinitesimal" information about the affine sets they define.

We end this section by proving the most important result about the relation of ideals and affine sets: Hilbert's Nullstellensatz. We will need a technical result first (the first part of it will be needed for generalizations of the Nullstellensatz).

**Lemma 1.15.** *Let $\mathbb{K}$ be a field and $f \in \mathbb{K}[X_1, \ldots, X_n]$ is a non-constant polynomial. Then:*

*(i) For sufficiently large $m$, the polynomial $f(X_1 + X_n^{m-1}, \ldots, X_{n-1}^m + X_n, X_n)$ is, up to multiplication by a constant, monic in the variable $X_n$.*

*(ii) If $\mathbb{K}$ is an infinite field, it is possible to find $\lambda_1, \ldots, \lambda_{n-1} \in \mathbb{K}$ such that $f(X_1 + \lambda_1 X_n, \ldots, X_{n-1} + \lambda_{n-1} X_n, X_n)$ is, up to multiplication by a constant, monic in the variable $X_n$.*

*Proof:* For (i), let $m$ be larger than any exponent $i_j$ of any monomial $x_1^{i_1} \ldots x_n^{i_n}$ appearing in $f$. An automorphism of $K[x_1, \ldots, x_n]$ leaving invariant $x_n$ and mapping each other $x_i$ to $x_i + x_n^{m^{n-1-i}}$ sends any monomial $x_1^{i_1} \ldots x_n^{i_n}$ to a polynomial whose monomial of highest degree is $x_n^{i_1 m^{n-1} + \ldots + i_{n-1} m + i_n}$. Regarding this degree as a number written in base $m$, it follows that $i_1 m^{n-1} + \ldots + i_{n-1} m + i_n \leq i'_1 m^{n-1} + \ldots + i'_{n-1} m + i'_n$ if and only if $(i_1, \ldots, i_{n-1}, i_n) \leq (i'_1, \ldots, i'_{n-1}, i'_n)$ in the lexicographical order. Therefore, such automorphism maps $f$ to a monic polynomial in $x_n$ of degree $i_1 m^{n-1} + \ldots + i_{n-1} m + i_n$, where $(i_1, \ldots, i_{n-1}, i_n)$ is the maximum of the set of exponents of $f$ when ordered lexicographically.

For (ii), if $f$ has total degree $d$ and $f_d$ is the homogeneous component of $f$ of degree $d$, then the coefficient of $X_n^d$ in $f(X_1 + \lambda_1 X_n, \ldots, X_{n-1} + \lambda_{n-1} X_n, X_n)$ is $f_d(\lambda_1, \ldots, \lambda_{n-1}, 1)$. Since $\mathbb{K}$ is infinite and $f_d(X_1, \ldots, X_{n-1}, 1)$ is a non-zero polynomial in $\mathbb{K}[X_1, \ldots, X_{n-1}]$, it does not vanish at some point $(\lambda_1, \ldots, \lambda_{n-1})$. This proves (ii). □

With just this easy lemma we can prove the following strong theorem (even if we refer

to it as "weak"), which for spectra of rings is nothing but Proposition 1.6.

**Theorem 1.16.** (Weak Hilbert's Nullstellensatz). *Let $I \subsetneq \mathbb{K}[X_1, \ldots, X_n]$ be a proper ideal. If $\mathbb{K}$ is algebraically closed, then $V(I) \neq \emptyset$.*

*Proof:* We will assume $I \neq 0$, since otherwise the result is trivial. We will prove the theorem by induction on $n$. The case $n = 1$ is immediate, because any proper ideal $I \neq 0$ of $\mathbb{K}[X]$ is generated by a non-constant polynomial, which necessarily has some root $a$ since $\mathbb{K}$ is algebraically closed. Therefore, $f(a) = 0$ for any $f \in I$.

We assume now $n > 1$. Lemma 1.15(ii) allows us ($\mathbb{K}$ is infinite because it is algebraically closed) to perform a change of coordinates such that $I$ contains a monic polynomial $g$ in the variable $X_n$. After this choice, we consider the ideal $I' \subset \mathbb{K}[X_1, \ldots, X_{n-1}]$ consisting of those polynomials of $I$ not depending on the variable $X_n$. Since $1 \notin I$, it follows that $I'$ is a proper ideal. Therefore, by induction hypothesis there is a point $(a_1, \ldots, a_{n-1})$ vanishing at all the polynomials of $I'$. We prove now the following:

**Claim.** The set $J = \{f(a_1, \ldots, a_{n-1}, X_n) \mid f \in I\}$ is a proper ideal of $\mathbb{K}[X_n]$.

Assume for contradiction that there exists $f \in I$ such that $f(a_1, \ldots, a_{n-1}, X_n) = 1$. Thus we can write $f = f_0 + f_1 X_n + \ldots f_d X_n^d$, with $f_i \in \mathbb{K}[X_1, \ldots, X_{n-1}]$, $f_1(a_1, \ldots, a_{n-1}) = \ldots = f_d(a_1, \ldots, a_{n-1}) = 0$ and $f_0(a_1, \ldots, a_{n-1}) = 1$. On the other hand, we write the above monic polynomial as $g = g_0 + g_1 X_n + \ldots + g_{e-1} X_n^{e-1} + X_n^e$ with $g_j \in \mathbb{K}[X_1, \ldots, X_{n-1}]$.

Let $R \in \mathbb{K}[X_1, \ldots, X_{n-1}]$ be the resultant of $f$ and $g$ with respect to the variable $X_n$. In other words,

$$R = \left| \begin{array}{cccccccc} f_0 & f_1 & \ldots & f_d & 0 & 0 & \ldots & 0 \\ 0 & f_0 & \ldots & f_{d-1} & f_d & 0 & \ldots & 0 \\ & & \ddots & & & & & \\ 0 & \ldots & 0 & f_0 & f_1 & \ldots & f_{d-1} & f_d \\ g_0 & g_1 & \ldots & g_{e-1} & 1 & 0 & \ldots & 0 \\ 0 & g_0 & \ldots & g_{e-2} & g_{e-1} & 1 & 0\ldots & 0 \\ & & \ddots & & & & \ddots & \\ 0 & \ldots & 0 & g_0 & g_1 & \ldots & g_{e-1} & 1 \end{array} \right| \begin{array}{l} \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} e \text{ rows} \\ \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} d \text{ rows} \end{array}$$

It is then well-known that $R \in I$ (in the above matrix, add to the first column the second one multiplied by $X_n$, plus the third one multiplied by $X_n^2$, and so on until the last one multiplied by $X_n^{d+e-1}$; developing the resulting matrix by the first column you will find that $R$ is a linear combination of $f$ and $g$). Therefore $R \in I'$. But a direct inspection at the above determinant defining the resultant shows that, when evaluating at $(a_1, \ldots, a_{n-1})$, it becomes the determinant of a lower-triangular matrix, whose entries at

the main diagonal are all 1. Hence $R(a_1, \ldots, a_{n-1}) = 1$, which contradicts the fact that $R \in I'$. This proves the claim.

Therefore $J$ is a proper ideal of $\mathbb{K}[X_n]$, and hence it is generated by a polynomial $h(X_n)$ of positive degree (or $h$ is zero). Since $\mathbb{K}$ is algebraically closed, $h$ has at least one root $a_n \in \mathbb{K}$. This means that $(a_1, \ldots, a_{n-1}, a_n) \in V(I)$, which completes the proof. □

**Corollary 1.17.** *If $\mathbb{K}$ is algebraically closed, then any maximal ideal of $\mathbb{K}[X_1, \ldots, X_n]$ is of the form $(X_1 - a_1, \ldots, X_n - a_n)$ for some $a_1, \ldots, a_n \in \mathbb{K}$.*

*Proof:* Any maximal ideal $\mathfrak{m}$ is proper, and hence the weak Nullstellensatz implies that there exists $a = (a_1, \ldots, a_n) \in \mathbb{A}^n_{\mathbb{K}}$ vanishing at all the polynomials of $\mathfrak{m}$. This means that $\mathfrak{m}$ is contained in the maximal ideal $(X_1 - a_1, \ldots, X_n - a_n)$ of the point $a$. But the fact that $\mathfrak{m}$ is maximal implies that both ideals must coincide. □

**Remark 1.18.** The result of the above corollary is in fact equivalent to the weak Nullstellensatz. Indeed, given a proper ideal $I$ of $\mathbb{K}[X_1, \ldots, X_n]$, it is contained in a maximal ideal. But if $\mathbb{K}$ is algebraically closed, the above corollary states that this maximal ideal is the ideal of a point, which necessarily belongs to $V(I)$.

The strong version of the Nullstellensatz is the following:

**Theorem 1.19** (Hilbert's Nullstellensatz)**.** *Let $I \subset \mathbb{K}[X_1, \ldots, X_n]$ be any ideal. If $\mathbb{K}$ is algebraically closed, then $IV(I) = \sqrt{I}$.*

*Proof:* Since clearly $IV(I) \supset \sqrt{I}$, we just need to prove the other inclusion. The proof can be obtained easily from the above weak Nullstellensatz by using the trick of Rabinowitsch. Let $f \in \mathbb{K}[X_1, \ldots, X_n]$ be a polynomial in $IV(I)$, i.e. vanishing at all the points of $V(I)$. We add a new variable $X_{n+1}$ and consider the polynomial ring $\mathbb{K}[X_1, \ldots, X_{n+1}]$. If $\{f_i\}_{i \in J} \subset \mathbb{K}[X_1, \ldots, X_n]$ is a set of generators of $I$ (Corollary 2.3 will imply that $J$ can be taken to be finite), it follows from the hypothesis on $f$ that the ideal of $\mathbb{K}[X_1, \ldots, X_{n+1}]$ generated by the $f_i$'s and $X_{n+1}f - 1$ defines the empty set. Hence the weak Nullstellensatz implies that there exist $i_1, \ldots, i_r \in J$ and $g_1, \ldots, g_{r+1} \in \mathbb{K}[X_1, \ldots, X_{n+1}]$ such that

$$1 = g_1 f_{i_1} + \ldots + g_r f_{i_r} + g_{r+1}(X_{n+1}f - 1)$$

We now make the substitution $X_{n+1} = \frac{1}{f}$ at each of the polynomials $g_1, \ldots, g_r$. If $l$ is the maximum exponent of $f$ in the denominators of those substitutions, we can thus write $g_i(X_1, \ldots, X_n, \frac{1}{f}) = \frac{h_i}{f^l}$, with $h_i \in \mathbb{K}[X_1, \ldots, X_n]$. Therefore, making the substitution $X_{n+1} = \frac{1}{f}$ in the displayed equation and multiplying by $f^l$ we get the equality $f^l =$

$h_1 f_{i_1} + \ldots + h_r f_{i_r}$, just proving that $f$ belongs to $\sqrt{I}$, finishing the proof of the theorem. □

The above theorem can be interpreted in the following way:

**Corollary 1.20.** *If $\mathbb{K}$ is an algebraically closed field, the operators $V$ and $I$ define bijections (inverse to each other) between the set of radical ideals of $\mathbb{K}[X_1, \ldots, X_n]$ and the set of affine sets in $\mathbb{A}^n_{\mathbb{K}}$. Moreover, in this bijection, prime ideals correspond to irreducible sets and maximal ideals correspond to points.* □

# 2. Noetherian rings

We deal now with the problem of finding a finite number of generators for an ideal (which in the geometric case would imply that the corresponding affine set can be described by a finite number of equations).

**Proposition 2.1.** *Let $A$ be a ring. Then the following conditions are equivalent:*

*(i) Any ideal of $A$ admits a finite number of generators.*

*(ii) The ring $A$ does not contain an infinite strictly ascending chain of ideals $I_1 \subsetneq I_2 \subsetneq \ldots$.*

*Proof:* Assume $A$ satisfies property (i) and let $I_1 \subset I_2 \subset \ldots$ be a chain of ideals of $A$. Let us prove that the inclusions cannot be all of them strict. By Exercise 1.4(v) we have that $I := \bigcup_{n\in\mathbb{N}} I_n$ is an ideal of $A$, and hence our assumption implies that it is generated by a finite number of elements $f_1, \ldots, f_r \in I$. Since each $f_i$ belongs $I$, it belongs to some $I_{n_i}$ with $n_i \in \mathbb{N}$. I we take $n_0 = \max\{n_1, \ldots, n_r\}$, it follows that $f_1, \ldots, f_r$ belong to $I_{n_0}$. Hence, any element of $I$, which is a linear combination of $f_1, \ldots, f_r$, belongs to $I_{n_0}$. This implies that $I_n = I_{n_0}$ if $n \geq n_0$, which proves (ii).

Reciprocally, suppose now that $A$ satisfies (ii), and assume for contradiction that $A$ possesses an ideal $I$ that is not finitely generated. We pick any element $f_1$ in $I$. Since $I$ is not finitely generated, $(f_1)$ is strictly contained in $I$, so that we can find an element $f_2 \in I$ not $(f_1)$. Similarly, $I$ cannot be $(f_1, f_2)$, and hence there exists $f_3 \in I$ not in $(f_1, f_2)$. Iterating the process we find a strictly increasing chain $(f_1) \subsetneq (f_1, f_2) \subsetneq (f_1, f_2, f_3) \subsetneq \ldots$, which contradicts the assumption (ii). □

**Definition.** A ring $A$ is called a *Noetherian ring* if it satisfies any of the two equivalent conditions of the above proposition.

**Theorem 2.2.** (Hilbert's basis theorem). *Let $A$ be a Noetherian ring. Then the polynomial ring $A[X]$ is Noetherian.*

*Proof:* Let $I$ be an ideal of $A[X]$. We can assume $I \neq A[X]$, since otherwise 1 would be a generator of $I$. For each $d \in \mathbb{N}$, the set $J_d := \{r \in A \mid r$ is the leading coefficient of some polynomial of degree $d$ in $I\}$ is easily seen to be an ideal of $A$ (if we take the convention that $0 \in J_d$) and $J_1 \subset J_2 \subset \ldots$. Since $A$ is Noetherian, there exists $d_0 \in \mathbb{N}$ such that $J_d = J_{d_0}$ if $d \geq d_0$. On the other hand, we can find polynomials $f_1, \ldots, f_m \in I$ such that each $J_0, \ldots, J_{d_0}$ is generated by the leading coefficients of some (not necessarily all) of these polynomials. Let us see that these polynomials generate $I$.

Take $f \in I$ and let $d$ be its degree. Assume first that $d \geq d_0$. Then the leading coefficient of $f$ is a linear combination (with coefficients in $A$) of the leading coefficients of

$f_1, \ldots, f_m$. Multiplying each $f_i$ by $X^{d-\deg f_i}$ we see that there exist monomials $h_1, \ldots, h_n \in A[X]$ such that $f - h_1 f_1 - \ldots - h_n f_n$ (which is still in $I$) has degree strictly less than $d$. Iterating the process we arrive to $g_1, \ldots, g_n \in A[X]$ such that $f - g_1 f_1 - \ldots - g_n f_n$ has degree strictly less than $d_0$. Hence we can assume $d < d_0$. But since now $J_d$ is generated by some leading coefficients of $f_1, \ldots, f_n$, we can find $r_1, \ldots, r_n \in A$ such that $f - r_1 f_1 - \ldots - r_n f_n$ has degree strictly smaller than $d$. Iterating the process till degree zero we then find that it is possible to write $f$ as a linear combination of $f_1, \ldots, f_n$ , which concludes the proof. □

**Corollary 2.3.** *The polynomial ring $\mathbb{K}[X_1, \ldots, X_n]$ is Noetherian.*

*Proof:* We use induction on $n$. In case $n = 1$ we know that we have a stronger result, namely that any ideal is generated by just one element. If $n > 1$, we regard $\mathbb{K}[X_1, \ldots, X_n]$ as the polynomial ring in the indeterminate $X_n$ with coefficients in $\mathbb{K}[X_1, \ldots, X_{n-1}]$. The ring of coefficients in now Noetherian by induction hypothesis, and the result comes now readily from Hilbert's basis theorem.

**Example 2.4.** Let us see in some practical case how to find a finite set of generators of an ideal. Consider the set $C = \{(t^3, t^4, t^5) \in \mathbb{A}^3_{\mathbb{K}} \mid t \in \mathbb{K}\}$ and let us find a set of generators for $I(C)$. The main idea is to use Euclidean division, and this works properly only when taking monic polynomials (the more general technique generalizing division is the use of the so-called *Gröbner bases*; the interested reader is referred for instance to [CLO]). So we look for a monic polynomial vanishing at all the points of the form $(t^3, t^4, t^5)$, and we would like it to have the minimum possible degree in the variable in which it is monic. The best candidate seems to be $Y^2 - XZ$, which is monic in $Y$ and has degree two in $Y$ (the reader is invited to try another natural solution, namely $Z^2 - X^2 Y$, which is monic in $Z$ and has also degree two in this variable). We thus start by taking any polynomial $f \in I(C)$ and divide it by $Y^2 - XZ$ as polynomials in $Y$. The remainder will have degree at most one in the variable $Y$, so that we can write

$$f = Q(X, Y, Z)(Y^2 - XZ) + R_1(X, Z)Y + R_0(X, Z)$$

for some polynomials $Q \in \mathbb{K}[X, Y, Z]$, $R_0, R_1 \in \mathbb{K}[X, Z]$. We want to continue this division process if possible. Since we have now eliminate somehow the variable $Y$ we need to look for monic polynomials of $I(C)$ but now depending only in the variables $X, Z$. The best possible choice seems now to take $Z^3 - X^5$, which is monic of degree three when regarded as a polynomial in $Z$. We divide now $R_0$ and $R_1$ by $Z^3 - X^5$ as polynomials in $Z$ and get equalities

$$R_1 = Q_1(X, Z)(Z^3 - X^5) + A_1(X)Z^2 + B_1(X)Z + C_1(X)$$

$$R_0 = Q_0(X,Z)(Z^3 - X^5) + A_0(X)Z^2 + B_0(X)Z + C_0(X)$$

for some $Q_0, Q_1 \in \mathbb{K}[X,Z]$ and $A_0, A_1, B_0, B_1, C_0, C_1 \in \mathbb{K}[X]$. At this point we are only left with the variable $X$, and of course we cannot find polynomials depending only on $X$ vanishing at all the points of $C$ (unless $\mathbb{K}$ is finite, so that we will assume $\mathbb{K}$ to be infinite). Thus we stop at this point our division process and put together all the equalities we got:

$$f = Q(Y^2 - XZ) + (Q_1Y + Q_0)(Z^3 - X^5) + A_1YZ^2 + B_1YZ + C_1Y + A_0Z^2 + B_0Z + C_0.$$

This is the right moment to use the hypothesis that $f$ is in $I(C)$, as well as the fact that we chose $Y^2 - XZ$ and $Z^3 - X^5$ in $I(C)$. For any value $t \in \mathbb{K}$ we will have that $f(t^3, t^4, t^5) = 0$, and substituting in the last equality we get

$$0 = A_1(t^3)t^{14} + B_1(t^3)t^9 + C_1(t^3)t^4 + A_0(t^3)t^{10} + B_0(t^3)t^5 + C_0(t^3).$$

Since we are assuming that $\mathbb{K}$ is infinite, this means that the polynomial $A_1(T^3)T^{14} + B_1(T^3)T^9 + C_1(T^3)T^4 + A_0(T^3)T^{10} + B_0(T^3)T^5 + C_0(T^3) \in \mathbb{K}[T]$ is the zero polynomial. Observe that in $A_1(T^3)T^{14} + B_0(T^3)T^5$ all the exponents of $T$ are all congruent with 2 modulo 3, in $B_1(T^3)T^9 + C_0(T^3)$ they are congruent with 0 modulo 3 and in $C_1(T^3)T^4 + A_0(T^3)T^{10}$ they are congruent with 1 modulo 3. Therefore, no monomial of any of these three pieces can cancel with a monomial of a different piece. This implies that any of these three pieces is zero, i.e.

$$A_1(T^3)T^9 + B_0(T^3) = 0$$

$$B_1(T^3)T^9 + C_0(T^3) = 0$$

$$C_1(T^3) + A_0(T^3)T^6 = 0.$$

This immediately implies equalities $B_0(X) = -A_1(X)X^3$, $C_0(X) = -B_1(X)X^3$ and $C_1(X) = -A_0(X)X^2$ (observe that $A_0, A_1, B_0, B_1, C_0, C_1$ were polynomials in $X$, so that from the above equalities you are not allowed to get relations like $A_1(X)YZ + B_0(X) = 0$). Substituting the above values for $B_0$, $C_0$ and $C_1$ in the above expression for $f$ and collecting terms with $A_1$, $B_1$ and $A_0$ we get the equality:

$$f = Q(Y^2 - XZ) + (Q_1Y + Q_0)(Z^3 - X^5) + A_1(YZ^2 - X^3Z) + B_1(YZ - X^3) + A_0(Z^2 - X^2Y)$$

which proves that $f$ is in the ideal generated by $Y^2 - XZ, Z^3 - X^5, YZ^2 - X^3Z, YZ - X^3, Z^2 - X^2Y$. All these polynomials are in $I(C)$, so that we get that they are actually generators of $I(C)$. Since $YZ^2 - X^3Z = Z(YZ - X^3)$, we can remove this polynomial from the set of generators. Similarly, $Z^3 - X^5 = Z(Z^2 - X^2Y) + X^2(YZ - X^3)$, so that this generator can also be removed (observe that, even if this polynomial can be eventually removed, it has been key to find the set of generators; in fact this is why I think it is better

not to know a priori the right set of generators). Summing up, we conclude that $I(C)$ is the ideal generated by $Y^2 - XZ, YZ - X^3, Z^2 - X^2Y$. The reader is invited to check that no other polynomial can be removed from the set of generators, and moreover (this is a little bit harder) that $I(C)$ cannot be generated by only two polynomials (not necessarily among those three).

**Exercise 2.5.** Find a finite number of generators for the following ideals:

(i) The ideal of the linear space $V(X_1, \ldots, X_r)$ in $\mathbb{A}^n_{\mathbb{K}}$; conclude that the ideal of any linear space of $\mathbb{A}^n_{\mathbb{K}}$ of codimension $r$ is generated by $r$ polynomials of degree one.

(ii) The ideal of the union of the lines $V(X, Z)$ and $V(Y, Z - 1)$ of $\mathbb{A}^3_{\mathbb{K}}$; conclude that the ideal of the union of two noncoplanar lines of degree-one equations $l_1 = l_2 = 0$ and $m_1 = m_2 = 0$ is generated by $l_1m_1, l_1m_2, l_2m_1, l_2m_2$.

(iii) The ideal of the points $(0, 0), (1, 0), (0, 1), (1, 1)$ in $\mathbb{A}^2_{\mathbb{K}}$; conclude that the ideal of four point in $\mathbb{A}^2_{\mathbb{K}}$ in general position (i.e. not three of them collinear) is generated by the equations of two conics passing through them.

**Example 2.6.** Consider the curve $C = \mathbb{A}^2_{\mathbb{K}}$ defined by the polynomial $f = Y^2 - X^2(X+1)$. If you look locally at the point $(0, 0)$ you will notice that, despite of the irreducibility of $f$, there are two branches of $C$ passing through it. If you did not learn to see this from the equation, you can convince yourself by checking that $C$ is precisely the set of points of the form $\big(t^2 - 1, t(t^2 - 1)\big)$, with $t \in \mathbb{K}$; with this description, the curve "passes twice" through $(0, 0)$, namely for the values $t = -1$ and $t = 1$. Even if you localize at $\mathfrak{m} = I(\{(0, 0)\}) = (X, Y)$, the ideal generated by $f$ in $\mathbb{K}[X, Y]_{\mathfrak{m}}$ is still prime. The only way of decomposing $f$ would be the aberration of saying that it has two roots, namely $Y = \pm X\sqrt{X + 1}$. At most, this could make sense maybe in case you are thinking that $\mathbb{K}$ is $\mathbb{R}$ or $\mathbb{C}$. A more algebraic way of writing that is to use Taylor expansions at the origin, so that we could say that the roots of $f$, as a polynomial in the variable $Y$, are $Y = \pm X(1 + 1/2X^2 - 1/8X^3 + 1/16X^4 - 5/128X^5 + \ldots)$. If we allow formal series, without worrying about convergence (a notion that even does not make any sense for arbitrary fields), then we have that formally these two are actually roots of $f$. Hence in a ring allowing infinite formal sums the polynomial $f$ becomes reducible, yielding the precise information about the "local reducibility" of the curve at $(0, 0)$. This motivates the following definition.

**Definition.** The *ring of formal power series in the variable $X$ with coefficients in a ring $A$* is the set $A[[X]]$ of expressions of the form $a_0 + a_1X + a_2X^2 + \ldots$, with $a_i \in A$ for any $i \geq 0$. It has a ring structure with the obvious operations. More generally, the *ring of formal power series in the variables $X_1, \ldots, X_n$ with coefficients in a ring $A$* is the set $A[[X_1, \ldots, X_n]]$ consisting of the formal expressions $f_0 + f_1 + f_2 + \ldots$, where for each $i \geq 0$

$f_i$ is a homogeneous polynomial of degree $i$ in $A[X_1, \ldots, X_n]$. Again this is a ring with the obvious operations.

**Exercise 2.7.** Let $A[[X_0, \ldots, X_n]]$ be the ring of formal power series with coefficients in a ring $A$ and let $f = f_0 + f_1 \ldots$ be a series.

(i) Prove that $f$ is a unit $A[[X_0, \ldots, X_n]]$ if and only if $f_0$ is a unit in $A$.

(ii) Show that any series $f \in \mathbb{K}[[X]]$ can be written in a unique way as $f = uX^n$, where $u$ is a unit in $\mathbb{K}[[X]]$. Deduce from this that $\mathbb{K}[[X]]$ is a PID, and more precisely that any ideal of $\mathbb{K}[[X]]$ is generated by a power of $X$.

(iii) Prove that, if $\mathbb{K}$ is algebraically closed, any unit $f \in \mathbb{K}[[X_0, \ldots, X_n]]$ has always $n$-th roots, i.e. series $g \in \mathbb{K}[[X_0, \ldots, X_n]]$ such that $g^n = f$.

**Proposition 2.8.** *If $A$ is a Noetherian ring, then $A[[X]]$ is also Noetherian.*

*Proof:* It is done as in the polynomial case, but using the order of the series instead of the degree of a polynomial. For each $d \in \mathbb{N}$ we consider the set $J_d \subset A$ consisting of those elements $a \in A$ such that $I$ contains a series of the form $aX^d +$ higher order terms. As in the polynomial case, $J_1 \subset J_2 \subset \ldots$ is a chain of ideal of $A$, and by noetherianity it follows that there is $d_0 \in \mathbb{N}$ such that $J_d = J_{d_0}$ if $d \geq d_0$. We can take now $f_1, \ldots, f_r \in I$ such that, for each $d = 0, \ldots, d_0$, some of the leading coefficients of $f_1, \ldots, f_r$ generate $J_d$. We will prove that any $f \in I$ can be expressed as a linear combination of $f_1, \ldots, f_r$.

If $f$ has order at most $d_0$ and $a$ is its leading coefficient, then we can write $a$ as a linear combination, with coefficients $a_1, \ldots, a_r \in A$, of the leading coefficients of $f_1, \ldots, f_r$. Therefore, the order of $f - a_1 f_1 - \ldots - a_r f_r$ is strictly bigger than the one of $f$. Iterating this process, we arrive to a linear combination of $f_1, \ldots, f_r$ whose difference with $f$ has order bigger than $d_0$. In other words, we can assume that the order of $f$ is at least $d_0 + 1$.

At this point, we observe that the coefficient of $X^{d_0+1}$ (even if it is zero!) in $f$ is a linear combination of the leading coefficients of $Xf_1, \ldots, Xf_r$ (instead of just $f_1, \ldots, f_r$). This produces a new series $f - a_{11}Xf_1 - \ldots a_{r1}Xf_r$ having order at least $d_0 + 2$. We write now the coefficient of $X^{d_0+2}$ in this series as a linear combination of the leading coefficients of $X^2 f_1, \ldots, X^2 f_r$. This yields now a series $f - a_{11}Xf_1 - \ldots a_{r1}Xf_r - a_{12}X^2 f_1 - \ldots a_{r2}X^2 f_r$ of order at least $n_0 + 3$. Defining by iteration the terms $a_{ij} \in A$ for $i = 1, \ldots, r$, $j \in \mathbb{N}$ we get series $g_i = a_{i1}X + a_{i2}X^2 + \ldots \in A[[X]]$, for $i = 1, \ldots, r$. By construction $f = g_1 f_1 + \ldots + g_r f_r$, which completes the proof. □

**Corollary 2.9.** *The ring $\mathbb{K}[[X_1, \ldots, X_n]]$ is Noetherian.*

*Proof:* It is done by induction on $n$, as it was done in the polynomial case. The first step in the induction is Exercise 2.7(ii). □

According to Lemma 1.9(iii) and Exercise 1.10(iii), the decomposition of a closed set into the union of closed pieces correspond to intersection of ideals, and irreducible closed pieces correspond to prime ideals (Lemma 1.1). Hence, if we expect to decompose any closed set into a finite union of irreducible pieces, then one could expect that, in the language of rings, any ideal can be written as a finite intersection of prime ideals. We will see now that the situation is not exactly so, but it is quite similar. We start with a very natural definition.

**Definition.** An *irreducible ideal* is a proper ideal $I$ that cannot be expressed as intersection of ideals like $I = I_1 \cap I_2$, with $I \subsetneq I_1$ and $I \subsetneq I_2$.

Lemma 1.12 implies that prime ideals are irreducible, but the viceversa is not true, so that we will need to deal with a wider class of ideals (see also Remark 1.2).

**Lemma 2.10.** *Any proper ideal of a Noetherian ring $A$ can be expressed as a finite intersection of irreducible ideals.*

*Proof:* Assume there exists a proper ideal $I$ of $A$ that is not a finite intersection of irreducible ideals. In particular, $I$ itself is not irreducible, so that it can be expressed as a non-trivial intersection of two ideals $I_1$ and $J_1$. From our hypothesis, it is clear that both $I_1$ and $J_1$ cannot be a finite intersection of irreducible ideals. Assume for instance that $I_1$ is not a finite intersection of irreducible ideals. Putting $I_1$ instead of $I$ in the previous reasoning, we will find $I_2$ strictly containing $I_1$ and such that $I_2$ is not a finite intersection of irreducible ideals. Iterating the process we would get an infinite chain $I \subsetneq I_1 \subsetneq I_2 \subsetneq \ldots$, which contradicts the fact that $A$ is Noetherian. □

However an irreducible ideal is not necessarily prime. Instead we have the following:

**Lemma 2.11.** *If $I$ is an irreducible ideal of a Noetherian ring $A$, and $f, g$ are two elements of $A$ such that their product is in $I$, then either $g$ belongs to $I$ or a power or $f$ belongs to $I$.*

*Proof:* Let $I$ be an irreducible ideal, and assume that we have two elements $f, g \in A$ such that $fg \in I$. For each $n \in \mathbb{N}$ consider the ideal $I_n = \{h \in A \mid hf^n \in I\}$. Since we have a chain $I = I_0 \subset I_1 \subset I_2 \subset \ldots$ and $A$ is Noetherian, there exists an $n \in \mathbb{N}$ such that $I_n = I_{n+1}$. Now I claim that $I = ((f^n) + I) \cap J$, where $J = \{h \in A \mid fh \in I\}$. Assuming for a while that the claim is true, this would imply from the irreducibility of $I$ that either $I = (f^n) + I$ (and hence $f^n \in I$) or $I = J$ (and hence $g \in I$, since by assumption $g \in J$). Therefore the lemma will follow as soon as we will prove the claim.

Take then $h \in ((f^n) + I) \cap J$. Hence $fh \in I$, and also we can write $h = af^n + b$, with $a \in A$ and $b \in I$. Multiplying by $f$ this last equality we get $af^{n+1} = fh - fb \in I$. Thus

$a \in I_{n+1} = I_n$, so that $af^n \in I$, which implies $h \in I$. This proves the non-trivial inclusion of the claim, and hence the lemma. □

**Definition.** A *primary ideal* of a ring $A$ is a proper ideal $\mathfrak{q}$ with the property that if $fg \in \mathfrak{q}$ but $g \notin \mathfrak{q}$ then there exists some $d \in \mathbb{N}$ such that $f^d \in \mathfrak{q}$. It is immediate to see that if $\mathfrak{q}$ is primary, then $\mathfrak{p} := \sqrt{\mathfrak{q}}$ is a prime ideal. The ideal $\mathfrak{q}$ is then said to be $\mathfrak{p}$-*primary*.

**Remark 2.12.** The fact that the radical of a primary ideal is prime means that, in the geometric case, a primary ideal defines the same affine set as a prime ideal. By the Nullstellensatz, this means that, if the ground field is algebraically closed, this affine set is irreducible.

**Exercise 2.13.** Show that the ideal $(X^2, XY) \subset \mathbb{K}[X, Y]$ is not primary. Hence it is not true that an ideal whose radical is prime is necessarily primary.

We have however the following result:

**Proposition 2.14.** *If the radical of an ideal $I$ is maximal, then $I$ is primary.*

*Proof:* Take $f, g \in A$ such that $fg \in I$ and assume that $f$ is not in $\sqrt{I}$, so that we have to prove that $g$ is in $I$. Since $\sqrt{I} \subsetneq \sqrt{I} + (f)$ and $\sqrt{I}$ is maximal it follows that $\sqrt{I} + (f)$ is the total ring. We can thus find an expression $1 = a + bf$, with $a \in \sqrt{I}$ and $b \in A$. If $a^n$ is a power of $a$ in $I$, the $n$-th power of the above expression becomes $1 = a^n + cf$ for some $c \in A$. We finally multiply this last equality by $g$ to get $g = a^n g + cfg$, which is in $I$ since the two right-hand summands belong to $I$. □

**Exercise 2.15.** Prove the following properties of primary ideals

(i) Prove that a finite intersection of $\mathfrak{p}$-primary ideals is $\mathfrak{p}$-primary.

(ii) Prove that, in a UFD, the ideal generated by a power of an irreducible element is primary.

(iii) Prove that the inverse image by a homomorphism of a primary ideal is also primary.

**Exercise 2.16.** Prove that the ideal $I = (X^2, XY, Y^2) \subset \mathbb{K}[X, Y]$ is primary, but it is not irreducible, since it can be written as $I = (X^2, Y) \cap (X, Y^2)$. Prove that $(X^2, Y)$ and $(X, Y^2)$ are irreducible. Is this decomposition into irreducible ideals unique?

Putting together the results we just have proved we obtain the following:

**Theorem 2.17.** *Any proper ideal $I$ of a Noetherian ring $A$ can be written as $I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_s$, where each $\mathfrak{q}_i$ is primary, the radicals $\sqrt{\mathfrak{q}_1}, \ldots, \sqrt{\mathfrak{q}_s}$ are all different and for each $i = 1, \ldots, s$ $\mathfrak{q}_i \not\supset \bigcap_{j \neq i} \mathfrak{q}_j$.*

*Proof:* It is clear from Lemmas 2.10 and 2.11 that $I$ can be written as a finite intersection of primary ideals. From Exercise 2.15(i) we can collect in one all the primary ideals in the decomposition having the same radical ideal. Therefore we can assume that all these radical ideals are different. Finally, the condition $\mathfrak{q}_i \not\supset \bigcap_{j\neq i} \mathfrak{q}_j$ can be easily obtained by just removing from the decomposition any primary ideal containing the intersection of the others. □

**Definition.** A primary decomposition as in the statement of Theorem 2.17 is called *irredundant, reduced* or *minimal*. The primary ideals corresponding to non-minimal prime ideals appearing in an irredundant decomposition are called *embedded components* of $I$. The radical ideals of the primary components of an irredundant decomposition are called *associated primes* of the ideal.

The important geometric consequence of Theorem 2.17 is the following result (regardless Remark 2.12).

**Corollary 2.18.** *Let $Z$ be a nonempty closed subset of $\mathbb{A}^n_{\mathbb{K}}$ or $\mathrm{Spec}(A)$ for some Noetherian ring $A$. Then:*

*(i) There is a decomposition $I(Z) = I_1 \cap \ldots \cap I_s$, where $I_1, \ldots, I_r$ are prime ideals and $I_j \not\subset I_i$ if $i \neq j$.*

*(ii) For any such decomposition, it follows that $Z_i = V(I_i)$ is an irreducible set with $I(Z_i) = I_i$.*

*(iii) $Z = Z_1 \cup \ldots \cup Z_s$, and $Z_i \not\subset Z_j$ if $i \neq j$.*

*(iv) There is only one such irredundant decomposition of $Z$ into a finite union of irreducible components.*

*Proof:* For part (i) we take $I(Z) = I_1 \cap \ldots \cap I_s$ a primary decomposition of $I(Z)$. Since $I(Z)$ is a radical ideal, taking radicals in the above expression allows us to assume that $I_1, \ldots, I_s$ are radical and hence prime. Removing redundant ideals we can assume that $I_j \not\subset I_i$ if $i \neq j$.

Part (ii) is immediate in the case of $\mathrm{Spec}(A)$ (by Exercise 1.11(iii)) or when $\mathbb{K}$ is algebraically closed (by the Nullstellensatz). An alternative proof valid also for an arbitrary $\mathbb{K}$ consists of decomposing $Z = Z_1 \cup \ldots \cup Z_s$, so that we have $I(Z) = I(Z_1) \cap \ldots \cap I(Z_s)$. Hence each $I_i$ contains $I(Z_1) \cap \ldots \cap I(Z_s)$, and thus Lemma 1.1 implies that it contains some $I(Z_j)$, which in turn contains $I_j$. Therefore $i = j$ and $I(Z_i) = I_i$, so that $Z_i$ is irreducible.

Part (iii) is an immediate consequence of parts (i) and (ii). Finally, in order to prove (iv), assume there is another irredundant decomposition $Z = Z'_1 \cup \ldots \cup Z'_t$. Hence each

$Z_i$ is contained in the union $Z'_1 \cup \ldots \cup Z'_t$. By the irreducibility of $Z_i$, it follows that $Z_i$ is contained in some $Z'_j$. Symmetrically, any $Z'_j$ is contained in some $Z_k$, and by the irredundance $Z_i$ and $Z_k$ coincide. So any irreducible subset of each decomposition is in the other decomposition. □

**Definition.** The sets $Z_1, \ldots, Z_r$ in the statement of the above corollary are called the *irreducible components* of $Z$.

The above corollary shows that the minimal prime ideals in a primary decomposition unique. We will see in the next section a stronger uniqueness result for primary decompositions (in the more general framework of primary decomposition of modules). We give now however a striking example showing that we can have some strange embedded primary ideals in a decomposition that are not unique.

**Example 2.19.** Let us consider in $\mathbb{A}^3_{\mathbb{K}}$ the lines $L = V(X, Z)$ and $L_t = V(Y, Z - t)$. We regard them as a family of lines when $t$ varies in $\mathbb{K}$, and we observe that $L$ and $L_t$ are not coplanar if and only if $t \neq 0$. We have $I(L) = (X, Z)$ and $I(L_t) = (Y, Z - t)$, and if $t \neq 0$ we get from Exercise 2.5(ii) that $I(L \cup L_t)$ is the ideal $I_t = \big(XY, X(Z-t), YZ, Z(Z-t)\big)$. It is a natural temptation to consider for $L \cup L_0$ the ideal $I_0 = (XY, XZ, YZ, Z^2)$. It is not true that this is the ideal of $L_0$ (in fact it is not even radical, since $Z \notin I_0$ but $Z^2 \in I_0$). However $V(I_0) = L_0$. It is another exercise to check the equality

$$I_0 = (X, Z) \cap (Y, Z) \cap (X - aZ, Y - bZ, Z^2)$$

for any $a, b \in \mathbb{K}$. This is a primary decomposition for $I_0$, and you cannot remove any of these three primary ideals. Since $a$ and $b$ can be taken arbitrarily, this means that the primary decomposition is not unique. The ideal $(X - aZ, Y - bZ, Z^2)$ represents, like in Example 1.14, the point $(0, 0, 0)$ together with the tangent direction given by the line $X = aZ, Y = bZ$. When varying the values of $a$ and $b$ we obtain all the lines passing through $(0, 0, 0)$ and not contained in the plane $Z = 0$. The geometric interpretation is that the ideal $I_0$ still "remembers" that the intersection point of the lines came from outside the plane $Z = 0$. Or if you prefer, you are trying to put in the same place the point $(0, 0, 0)$ of the line $L$ and another point coming from $L_t$. Since there is no room in $(0, 0, 0)$ for two different points, you get two infinitely close points.

**Exercise 2.20.** Let $I_\lambda = (\overline{X - \lambda})$ be the ideal generated by the class of $X - \lambda$ in $\mathbb{K}[X, Y]/(Y^2 - X)$, with $\lambda \in \mathbb{K}$. Prove that a minimal primary decomposition of $I_\lambda$ is:

(i) $I_\lambda = (\overline{X - \lambda}, \overline{Y - \mu}) \cap (\overline{X - \lambda}, \overline{Y + \mu})$, if $\lambda = \mu^2$ with $\mu \in \mathbb{K} \setminus \{0\}$ (what happens for instance if $\mathbb{K} = \mathbb{C}$ and $\lambda \neq 0$ or if $\mathbb{K} = \mathbb{R}$ and $\lambda > 0$).

(ii) $I_\lambda$ itself is primary but not prime, if $\lambda = 0$.

(iii) $I_\lambda$ itself is maximal and hence primary, if $\lambda$ has not a square root in $\mathbb{K}$ (what happens for instance if $\mathbb{K} = \mathbb{R}$ and $\lambda < 0$).

Of course the above exercise is saying that the intersection of the parabola $Y = X^2$ with the line $Y = \lambda$ consists of two points with multiplicity one in case (i), one point with multiplicity two in case (ii) or two imaginary points in case (iii). The nice thing is that such a geometric interpretation can be translated to an apparently different context like number theory. This is the scope of the next exercise (in which you should think of $\mathbb{Z}[\sqrt{d}]$ as $\mathbb{Z}[Y]/(Y^2 - d)$, and thus $\mathbb{Z}$ is a PID, so it should behave as $\mathbb{K}[X]$).

**Exercise 2.21.** Let $I_p = (p)$ be the ideal generated by the prime number $p$ in $\mathbb{Z}[\sqrt{d}]$ (where $d$ is a square-free integer). Prove that a minimal primary decomposition of $I_p$ is:

(i) $I_p = (\sqrt{d}-a, p) \cap (\sqrt{d}+a, p)$, if $d \equiv a^2 (\mathrm{mod} p)$ for some $a \in \mathbb{Z}$ such that $a \not\equiv -a (\mathrm{mod}\ p)$.

(ii) $I_p$ itself is primary but not prime, if $d \equiv a^2 (\mathrm{mod}\ p)$ for some $a \in \mathbb{Z}$ such that $a \equiv -a (\mathrm{mod}\ p)$.

(iii) $I_p$ itself is maximal and hence primary, if $d \not\equiv a^2 (\mathrm{mod}\ p)$ for any $a \in \mathbb{Z}$.

# 3. Modules; primary decomposition

**Example 3.1.** Let us study more closely the ideal $I(C)$ of Example 2.4. We already know that it can be generated by $Z^2 - X^2Y, X^3 - YZ, Y^2 - XZ$ and this is a minimal set of generators. But in some sense, these equations are dependent. More precisely, we can find relations

$$X(Z^2 - X^2Y) + Y(X^3 - YZ) + Z(Y^2 - XZ) = 0$$

$$Y(Z^2 - X^2Y) + Z(X^3 - YZ) + X^2(Y^2 - XZ) = 0.$$

Are they all the relations among them? Or more precisely, given polynomials $A, B, C \in \mathbb{K}[X, Y, Z]$ such that $A(Z^2-X^2Y)+B(X^3-YZ)+C(Y^2-XZ) = 0$, can we obtain somehow $A, B, C$ from the two given relations? Let us work out a little bit that generic relation. We can write is as $A(Z^2 - X^2Y) = -B(X^3 - YZ) - C(Y^2 - XZ)$, and since the right-hand term belongs to $(X, Y)$, it also holds that $A(Z^2 - X^2Y)$ is in $(X, Y)$. But $(X, Y)$ is a prime ideal and $Z^2 - X^2Y \notin (X, Y)$, so it follows that we can write $Z^2 - X^2Y = PX + QY$, for some $P, Q \in \mathbb{K}[X, Y, Z]$. Coming back to the original relation, we can write it now as

$$PX(Z^2 - X^2Y) + QY(Z^2 - X^2Y) + B(X^3 - YZ) + C(Y^2 - XZ) = 0.$$

But using the two first relations we can write $X(Z^2 - X^2Y)$ and $Y(Z^2 - X^2Y)$ in terms of $X^3 - YZ, Y^2 - XZ$, so that the relation becomes

$$(-PY - QZ + B)(X^3 - YZ) + (-PZ - QX^2 + C)(Y^2 - XZ) = 0.$$

Since $X^3 - YZ$ and $Y^2 - XZ$ are coprime, it follows that we can write $-PY - QZ + B = R(Y^2 - XZ)$ and $-PZ - QX^2 + C = -R(X^3 - YZ)$ for some $R \in \mathbb{K}[X, Y, Z]$. In other words, we can write

$$B = (P + RY)Y + (Q - XR)Z$$

$$C = (P + RY)Z + (Q - XR)X^2$$

and we observe that we also have

$$A = (P + RY)X + (Q - XR)Y.$$

This means that the polynomials $A, B, C$ given a relation can be written

$$(A, B, C) = (P + RY)(Y, Z, X^2) + (Q - XR)(X, Y, Z)$$

i.e. as a combination of the known relations.

One natural (and necessary) question now is, what is the structure of the set of relations and what does it mean that we were able to write all of them in terms of two known relations? The last expression stating that all the relations come from the two first is written in the cartesian product $\mathbb{K}[X,Y,Z] \times \mathbb{K}[X,Y,Z] \times \mathbb{K}[X,Y,Z]$, and hence the set of relations can be viewed as a subset there. The last displayed expression is saying that the set of relations is the set of linear combinations with coefficients in $\mathbb{K}[X,Y,Z]$ of $(Y,Z,X^2)$ and $(X,Y,Z)$. Thus we are allowed to add relations and multiply them by polynomials, and they become still relations. This suggests that the structure of the set of relations is like the one of a vector space, but allowing the set of "scalars" to be a just a ring instead of a field.

**Definition.** A *module over a ring* $A$ is a set $M$ having an inner operation $+ : M \times M \to M$, such that $(M,+)$ is an abelian group and an external operation $A \times M \to M$ satisfying the following properties:

(i) $a(m_1 + m_2) = am_1 + am_2$ for all $a \in A$ and $m_1, m_1 \in M$.

(ii) $(a_1 + a_2)m = a_1m + a_2m$ for all $a_1, a_2 \in A$ and $m \in M$.

(iii) $(ab)m = a(bm)$ for all $a, b \in A$ and $m \in M$.

(iv) $1m = m$ for all $m \in M$.

The notions of set of generators, linearly independent elements, basis, submodules, sum of submodules, quotients by submodules, homomorphisms,... can be defined exactly as in the case of vector spaces. The only main differences are that it is not true that any finitely generated module has a basis and that $am$ can be zero but $a \neq 0$ and $m \neq 0$. In fact this is something the reader implicitly know since the notion of abelian group is equivalent to the notion of module over $\mathbb{Z}$. Observe also that in this language, an ideal of a ring $A$ is just a submodule of $A$.

**Definition.** A *free module* over a ring $A$ is a module $M$ admitting a basis, i.e. a linearly independent set of generators.

**Exercise 3.2.** Prove that the generators $(Y,Z,X^2), (X,Y,Z)$ of the module of Example 3.1 are linearly independent, and hence the set of relations of the generators of $I(C)$ is a free module.

**Exercise 3.3.** Let $M \subset \mathbb{K}[X,Y,Z] \times \mathbb{K}[X,Y,Z] \times \mathbb{K}[X,Y,Z] \times \mathbb{K}[X,Y,Z]$ be the module of elements $(A,B,C,D)$ such that $AXY + BXZ + CYZ + DZ^2 = 0$ (i.e. $M$ is the module of relations of the ideal $I_0$ of Example 2.19). Prove that $M$ is generated by the elements $(Z,-Y,0,0), (0,Y,-X,0), (0,-Z,0,X), (0,0,-Z,Y)$ but they are not linearly independent [The underlying reason is that $I_0$ has a primary component of codimension three, while in the above example $I(C)$ has only one component of codimension two. This means that we

need one more step, in the sense that the module of "relations of the relations" is eventually free, and in fact generated by the relation $0(Z,-Y,0,0)+Z(0,Y,-X,0)+Y(0,-Z,0,X)-X(0,0,-Z,Y)=(0,0,0,0)$].

**Definition.** The *direct product of the modules* $M_l$ (when $l$ varies in an arbitrary set $\Lambda$) is the cartesian product $\Pi_{l\in\Lambda}M_l$, with the natural module structure given by operating at each coordinate. The *direct sum of the modules* $M_l$ is the subset $\bigoplus_{l\in\Lambda} M_l$ of the direct product consisting of those elements for which all but a finite number of coordinates are zero. Of course, the product and the sum coincide if $\Lambda$ is a finite set.

It is clear that, in this language, a free module over a ring $A$ is a module that is isomorphic to a direct sum of copies of the ring $A$. The need of considering also the product comes from the following exercise.

**Exercise 3.4.** For any $A$-module $M$, define the dual of $M$ as the set of all the homomorphisms from $M$ to $A$. Prove that it has a natural structure of $A$-module. If $M=\bigoplus_{l\in\Lambda} M_l$, prove that the dual of $M$ is canonically isomorphic to the direct product of the dual of the $M_l$'s. (This shows for instance that the dual of a vector space of infinite dimension has dimension bigger, in the sense of cardinals, than the original vector space; hence it is not true that the dual of the dual is the original vector spaces).

**Exercise 3.5.** Prove that the sum of the products are characterized, up to isomorphism, by the following universal properties:

(i) There are homomorphisms $p_l : \Pi_{l\in\Lambda}M_l \to M_l$ and for any other module $M$ with homomorphisms $q_l : M \to M_l$ then there exists a unique homomorphism $f : M \to \Pi_{l\in\Lambda}M_l$ such that $q_l = p_l \circ f$.

(ii) There are homomorphisms $i_l : M_l \to \bigoplus_{l\in\Lambda} M_l$ and for any other module $M$ with homomorphisms $j_l : M_l \to M$ then there exists a unique homomorphism $f : \bigoplus_{l\in\Lambda} M_l \to M$ such that $j_l = f \circ i_l$.

**Definition.** A *Noetherian module* is a module $M$ satisfying one of the following equivalent conditions (the equivalence being proved as in Proposition 2.1):

(i) Any submodule of $M$ is finitely generated.

(ii) $M$ does not contain any chain of submodules $M_1 \subsetneq M_2 \subsetneq \dots$

**Proposition 3.6.** *Let $N$ be a submodule of a module $M$. Then $M$ is Noetherian if and only if $N$ and $M/N$ are Noetherian.*

*Proof:* Assume first that $M$ is Noetherian. Then by condition (ii) of the definition, it is clear that any submodule of $M$ is Noetherian. And since there is a 1:1 correspondence

between submodules of $M/N$ and submodules of $M$ containing $N$ it is also clear that $M/N$ is Noetherian.

We assume now that $N$ and $M/N$ are Noetherian and take a chain $M_1 \subset M_2 \subset \dots$ of submodules of $M$. We need to show that this chain is stationary. From this chain we produce chains in $N$ and $M/N$, namely $M_1 \cap N \subset M_2 \cap N \subset \dots$ and $(M_1 + N)/N \subset (M_2 + N)/N \subset \dots$. Since $N$ and $M/N$ are Noetherian, we can find $i_0 \in \mathbb{N}$ such that $M_i \cap N = M_{i_0} \cap N$ and $M_i + N = M_{i_0} + N$ if $i \geq i_0$. Let us prove that in this range it also holds $M_i = M_{i_0}$.

Indeed if we take $m \in M_i$, then $m$ also belongs to $M_i + N$, which coincides with $M_{i_0} + N$. Therefore we can write $m = m_0 + n$, with $m_0 \in M_{i_0}$ and $n \in N$. From this we can write $n = m - m_0$, which shows that $n$ belongs also to $M_i$, because $M_{i_0} \subset M_i$. Since $M_i \cap N = M_{i_0} \cap N$, it follows that $n$ belongs to $M_{i_0}$, and therefore $m$ is in $M_{i_0}$. □

**Exercise 3.7.** An $A$-module is said to be *Artinian* if any chain of submodules $M_1 \supset M_2 \supset \dots$ is stationary, i.e. there exists $n_0 \in \mathbb{N}$ such that $M_n = M_{n_0}$ for any $n \geq n_0$. Prove that, given any submodule $N$ of $M$, then $M$ is Artinian if and only if $N$ and $M/N$ are Artinian.

**Proposition 3.8.** *Let $A$ be a Noetherian ring and let $M$ be an $A$-module. Then $M$ is Noetherian if and only if it is finitely generated.*

*Proof:* By definition, a Noetherian module is finitely generated, so that we just need to prove the converse. If $M$ is finitely generated, then it is a quotient of a finite sum of copies of $A$, so that by Proposition 3.6 it suffices to prove that for each $r$ the sum $A \oplus \overset{r)}{\dots} \oplus A$ is Noetherian. We will prove it by induction on $r$, the case $r = 1$ being trivial.

For $r > 1$ we consider the submodule $N$ of $A \oplus \overset{r)}{\dots} \oplus A$ consisting of those elements whose first coordinate is zero. Clearly $N \cong A$, which is Noetherian, and $(A \oplus \overset{r)}{\dots} \oplus A)/N \cong A \oplus \overset{r-1)}{\dots} \oplus A$, which is Noetherian by induction hypothesis. Hence, again by Proposition 3.6, it follows that $A \oplus \overset{r)}{\dots} \oplus A$ is Noetherian. □

We generalize now to modules the primary decomposition that we got for ideals. The definition comes naturally as the one for ideals. In order to present it in a more coherent way, we start by the definitions instead of trying to justify them first.

**Definition.** A *primary submodule* of an $A$-module $M$ is a proper submodule $N$ such that for any $f \in A$ and $m \in M$ such that $fm \in N$ then either $m \in N$ or there exists $l \in \mathbb{N}$ such that $f^l M \subset N$ (i.e. for any $m' \in M$ then $f^l m' \in N$). The set $\mathfrak{p} := \{f \in A \mid f^l M \subset N$ for some $l \in \mathbb{N}\}$ is thus a prime ideal, and $N$ is said to be $\mathfrak{p}$-*primary*.

Observe that this definition for modules explains the lack of symmetry in the corresponding definition for ideals.

**Theorem 3.9.** *Let $M$ be a Noetherian $A$-module. Then any proper submodule $N$ of $M$ admits a decomposition $N = N_1 \cap \ldots \cap N_r$ such that each $N_i$ is $\mathfrak{p}_i$-primary (with $\mathfrak{p}_i \neq \mathfrak{p}_j$ if $i \neq j$) and $\bigcap_{j \neq i} N_j \not\subset N_i$.*

*Proof:* It follows the same steps as for ideals. First, using the noetherianity of $M$, we observe, as in Lemma 2.10 that $N$ is a finite intersection of irreducible submodules (irreducible meaning proper and not expressible as a non-trivial intersection of two submodules).

Next we imitate the proof of Lemma 2.11 to conclude that any irreducible module $N$ is primary. Indeed if we have $f \in A$ and $m \in M$ such $fm \in N$, then we can write $N = (f^l M + N) \cap \{m' \in M \mid fm' \in N\}$, where $l$ satisfies that $\{m' \in M \mid f^l m' \in N\} = \{m' \in M \mid f^{l+1} m' \in N\}$, and the proof is the same as in Lemma 2.11.

Finally, removing redundant components and gathering primary components with the same prime, we eventually get the wanted decomposition. □

**Definition.** A decomposition as in the statement of Theorem 3.9 will be called an *irredundant primary decomposition* of $N$.

We prove now a uniqueness theorem for irredundant primary decompositions. Example 2.19 shows that it is the best possible result. Observe that we do not assume the module to be Noetherian. This means that we are proving that if a submodule admits a primary decomposition, then the uniqueness result holds.

**Theorem 3.10.** *Let $N = N_1 \cap \ldots \cap N_r$ be an irredundant primary decomposition in which each $N_i$ is $\mathfrak{p}_i$-primary. Then*

*(i) For each $m \in M$, the set $I_m := \{f \in A \mid f^l m \in N \text{ for some } l \in \mathbb{N}\}$ is an ideal and it can be expressed as $I_m = \bigcap_{m \notin N_i} \mathfrak{p}_i$.*

*(ii) The set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ coincides with the set of ideals $I_m$ that are prime. In particular, $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ does not depend on the primary decomposition.*

*(iii) For each $f \in A$, the set $N(f) := \{m \in M \mid f^l m \in N \text{ for some } l \in \mathbb{N}\}$ is a submodule of $M$ and $N(f) = \bigcap_{f \notin \mathfrak{p}_i} N_i$.*

*(iv) If $\mathfrak{p}_i$ is minimal in the set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$, then $N_i$ does not depend on the primary decomposition.*

*Proof:* To prove (i) it is enough to prove the equality $I_m = \bigcap_{m \notin N_i} \mathfrak{p}_i$. So let us prove the double inclusion. The first inclusion is clear: if we have $f \in I_m$, then some $f^l m$ is in $N$, hence in any $N_i$, and if $m \notin N_i$ it follows from the primarity of $N_i$ that $f$ belongs to $\mathfrak{p}_i$.

Reciprocally, if $f$ belongs to $\bigcap_{m \notin N_i} \mathfrak{p}_i$, then for each $i$ such that $m \notin N_i$ we have $f \in \mathfrak{p}_i$, so that there exists some $f^{l_i} m$ in $N_i$. Taking $l$ to be the maximum of these $l_i$'s we obtain that $f^l m$ is in any $N_i$ not containing $m$. Since obviously $f^l m$ is in any $N_i$ containing $m$, we get $f^l m \in N_1 \cap \ldots \cap N_r = N$. Therefore $f$ is in $I_m$, which proves (i).

To prove (ii), we first observe that if some $I_m$ is prime, then it should coincide with some $\mathfrak{p}_i$, by using Lemma 1.1 and the fact we just proved that $I_m$ is a finite intersection of $\mathfrak{p}_i$'s. On the other hand, since the primary decomposition is irredundant, we can find for each $i = 1 \ldots, r$ an element $m_i \in \bigcap_{j \neq i} N_j \setminus N_i$, and therefore (i) implies $I_{m_i} = \mathfrak{p}_i$.

The proof of (iii) is completely analogous to the proof of (i). Finally, the proof of (iv) is like the end of the proof of (ii), with the difference that only if $\mathfrak{p}_i$ is minimal in the set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ it is possible to find $f_i \in \bigcap_{j \neq i} \mathfrak{p}_j \setminus \mathfrak{p}_i$ (again Lemma 1.1 shows that $\bigcap_{j \neq i} \mathfrak{p}_j \subset \mathfrak{p}_i$ if and only if $\mathfrak{p}_i$ is contained in some $\mathfrak{p}_j$ with $j \neq i$). We thus have that $N_i$ coincides with $N(f_i)$, and therefore it does not depend on the primary decomposition. □

**Definition.** The prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of the above theorem are called the *associated primes of the submodule $N$*. The primary components corresponding to non-minimal prime ideals are called *embedded components of the submodule $N$*.

In case we assume noetherianity, we can improve the characterization of the associated primes given in Theorem 3.10(ii) in the following way:

**Theorem 3.11.** *Let $M$ be a finitely generated module over a Noetherian ring $A$, and let $N \subset M$ be a proper submodule. For any $m \in M$ consider the ideal $Ann_{M/N}(m) := \{f \in A \mid fm \in N\}$. Then the set of associated primes of $N$ is exactly the set of ideals $Ann_{M/N}(m)$ that are prime.*

*Proof:* Let $N = N_1 \cap \ldots \cap N_r$ be an irredundant primary decomposition with $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ their respective associated primes. We first prove that each $\mathfrak{p}_i$ can be written as $Ann_{M/N}(m_i)$ for some $m_i \in M$. We know by Theorem 3.10(i) that we can take $m_i' \in \bigcap_{j \neq i} N_j \setminus N_i$ and then $\mathfrak{p}_i = I_{m_i'} = \{f \in A \mid f^l m_i' \in N \text{ for some } l \in \mathbb{N}\} = \sqrt{Ann_{M/N}(m_i')}$. Since $A$ is Noetherian we can use Exercise 1.4(vii) to conclude that there is some power $\mathfrak{p}_i^l$ contained in $Ann_{M/N}(m_i')$. Take $l$ to be minimum with this condition, i.e. such that there exists $g \in \mathfrak{p}_i^{l-1}$ such that $m_i := gm_i' \notin N$. It is then clear that we have an inclusion $\mathfrak{p}_i \subset Ann_{M/N}(m_i)$, since $fg \in \mathfrak{p}_i^l$ for any $f \in \mathfrak{p}_i$. Let us prove the other inclusion. If $fm_i \in N$, then in particular $fm_i \in N_i$. But by construction $m_i \in \bigcap_{j \neq i} N_j$ and $m_i \notin N$, hence $m_i \notin N_i$. Therefore $f \in \mathfrak{p}_i$, as wanted.

Reciprocally, if some $Ann_{M/N}(m)$ is prime, then it is radical, and hence it is coincide with $\sqrt{Ann_{M/N}(m)} = I_m$. It now follows from Theorem 3.10(ii) that $Ann_{M/N}(m)$ is an associated prime. □

**Example 3.12.** Now it is clear why the ideal $I_0 = (XY, XZ, YZ, Z^2) \subset \mathbb{K}[X,Y,Z]$ of Example 2.19 has an embedded component. The ideal $Ann_{\mathbb{K}[X,Y,Z]/I_0}(Z) = \{f \in \mathbb{K}[X,Y,Z] \mid fZ \in I_0\}$ is the maximal ideal $(X,Y,Z)$, and hence there should be an embedded component having $(X,Y,Z)$ as its associated prime.

**Definition.** *A zerodivisor of a module $M$* is an element $f \in A$ for which there exists $m \in M \setminus \{0\}$ such that $fm = 0$.

**Proposition 3.13.** *Let $M$ be a finitely generated module over a Noetherian ring and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the associated primes of a proper submodule $N$. Then $\mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_r$ is the set of zerodivisors of $M/N$, i.e. the elements $f \in S$ for which there exists $m \in M \setminus N$ such that $fm \in N$. In particular, the set of zerodivisors of $M$ is the union of the associated primes of $(0)$.*

*Proof:* Let first $f$ be a zerodivisor of $M/N$. Thus there exists an element $m \in M \setminus N$ such that $fm \in N$. Since $m \notin N$, then there exists $i = 1, \ldots, r$ such that $m \notin N_i$. But on the other hand $fm$ is in $N$, so that it belongs to $N_i$. Now the fact that $N_i$ is $\mathfrak{p}_i$-primary implies that $f$ belongs to $\mathfrak{p}_i$.

Reciprocally, by Theorem 3.11 each $\mathfrak{p}_i$ has the form $Ann_{M/N}(m_i)$ (and obviously $m_i \notin N$), which means that all of its elements are zerodivisors of $M/N$. □

In order to apply this result, we need a lemma about unions of prime ideals.

**Lemma 3.14.** *Let $I$ be an ideal contained in a union $\mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_r$ of prime ideals. Then $I$ is contained in some of the $\mathfrak{p}_i$'s.*

*Proof:* We use induction on $r$, the case $r = 1$ being trivial. Assume now $r > 1$. I claim that there is some $i$ such that $I$ is contained in $\bigcup_{j \neq i} \mathfrak{p}_j$ (and hence by induction hypothesis $I$ is contained in some $\mathfrak{p}_j$, which would finish the prove). Indeed, assume for contradiction that for each $i = 1, \ldots, r$ the ideal $I$ is not contained in $\bigcup_{j \neq i} \mathfrak{p}_j$. Hence we can find $f_i \in I$ that is not in any $\mathfrak{p}_j$ with $j \neq i$. Since $I$ is contained in $\mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_r$, it follows that necessarily $f_i$ is in $\mathfrak{p}_i$. We define now $g_i = \Pi_{j \neq i} f_j$. By construction and the fact that $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are primes, it follows that $g_i$ is in $I$, in any $\mathfrak{p}_j$ with $j \neq i$, and not in $\mathfrak{p}_i$. But then the element $g_1 + \ldots + g_r$ is in $I$ but cannot be in any $\mathfrak{p}_i$, which is a contradiction. □

**Corollary 3.15.** *Let $M$ be a finitely generated module over a Noetherian ring $A$, and let $N \subset M$ be a submodule. For any $m \in M \setminus N$ the ideal $Ann_{M/N}(m) = \{f \in A \mid fm \in N\}$ is contained in some associated ideal of $N$. Hence the maximal elements in the set of associated primes of $N$ is exactly the set of maximal elements in the set of ideals $Ann_{M/N}(m)$ with $m \notin N$.*

*Proof:* It is clear that each $Ann_{M/N}(m)$ is made out of zerodivisors of $M/N$. Therefore Proposition 3.13 implies that $Ann_{M/N}(m)$ is contained in the union of the associated primes of $N$. But now from Lemma 3.14 we conclude that $Ann_{M/N}(m)$ is contained in some associated prime of $N$, which proves the result. □

**Example 3.16.** Let us try to explain with an example what primary decomposition for modules means. Let $A$ be a ring and let $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ be a finite set of primary ideals such that $\sqrt{\mathfrak{q}_i} \neq \sqrt{\mathfrak{q}_j}$ if $i \neq j$. Consider the module $M = A/\mathfrak{q}_1 \oplus \ldots \oplus A/\mathfrak{q}_r$ and let $p_i : M \to A/\mathfrak{q}_i$ be the $i$-th projection, for $i = 1, \ldots, r$. If we write $M_i = \ker p_i$, it is clear that $(0) = M_1 \cap \ldots \cap M_r$. I claim that this is an irredundant primary decomposition of $(0)$.

To see that each $M_i$ is primary can be done by hand, since $f(\bar{f}_1, \ldots, \bar{f}_r) \in M_i$ (the bar meaning taking classes modulo the corresponding $\mathfrak{q}_j$) implies $ff_i \in \mathfrak{q}_i$, and thus either $f_i \in \mathfrak{q}_i$ (hence $(\bar{f}_1, \ldots, \bar{f}_r) \in M_i$) or $f^l \in \mathfrak{q}_i$ for some $l \in \mathbb{N}$ (hence $f^l M \subset M_i$). A more abstract way of proving the primarity would be to observe that, for each $i = 1, \ldots, r$, $(0)$ is a primary submodule (or ideal, if you prefer) of $A/\mathfrak{q}_i$, so its inverse image by $p_i$, i.e. $M_i$ is a primary module. The irredundance of the decomposition is clear.

Observe that we could have some inclusion $\mathfrak{q}_i \subset \mathfrak{q}_j$ and the decomposition is still irredundant. This shows that the primary decomposition of the module is finer than the primary decomposition of the ideal $I = \{f \in A \mid fM = 0\}$ (which clearly decomposes as $I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_r$) even if the proof of the existence of the decomposition could suggest that both decompositions are equivalent. Observe that we could have allowed having several primary ideals with the same radical $\mathfrak{p}$. The $\mathfrak{p}$-primary component would be then the $r$-uples with zeros at the coordinates corresponding to quotients $A/\mathfrak{q}$ for which $\sqrt{\mathfrak{q}} = \mathfrak{p}$. Hence the primary decomposition can be viewed as a way of finding copies of the type $A/\mathfrak{q}$ in $M$.

The situation of the above example occurs for instance when we are dealing with finitely generated abelian groups, in which the structure theorem states that such a group is isomorphic to a unique group of the form $\mathbb{Z} \oplus \ldots \oplus \mathbb{Z} \oplus \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \ldots \oplus \mathbb{Z}_{d_s}$, with $d_1 | d_2 | \ldots | d_s$. Since $\mathbb{Z}_{p_1^{a_1} \ldots p_t^{a_s}}$ is isomorphic to $\mathbb{Z}_{p_1^{a_1}} \oplus \ldots \oplus \mathbb{Z}_{p_s^{a_s}}$ (if $p_1, \ldots, p_s$ are different prime numbers), we can write each finitely generated abelian group as a direct sum of the form $\mathbb{Z} \oplus \ldots \oplus \mathbb{Z} \oplus \mathbb{Z}_{p_1^{a_1}} \oplus \ldots \oplus \mathbb{Z}_{p_s^{a_s}}$ for a finite collection of prime numbers $p_1, \ldots, p_s$ (not necessarily different from each other). The main point in the proof of the structure theorem is that $\mathbb{Z}$ is a PID. In fact, the following is true:

**Theorem 3.17.** *Let $A$ be a PID. Then for any finitely generated $A$-module $M$ there exist a unique integer $r$ and elements $f_1 | f_2 | \ldots | f_s$ of $A$ such that $M$ is isomorphic to*

$A \oplus \overset{r)}{\ldots} \oplus A \oplus A/(f_1) \oplus A/(f_2) \oplus \ldots \oplus A/(f_s)$.

*Proof:* See for instance [Sh], Chapter 10. □

Reasoning as above, we can write $M \cong M_1 \oplus \ldots \oplus M_r$, in which for each $i = 1, \ldots, r$ there exists an irreducible element $f_i \in A$ such that $M_i$ is a direct sum of blocks of the type $A/(f_i^{a_i})$ (observe that one of the $f_i$'s could be zero). Let us see a nice application of this result.

**Example 3.18.** Let $\varphi : V \to V$ be an endomorphism of a $\mathbb{K}$-vector space $V$ of finite dimension $n$. We endow $V$ with a structure of $\mathbb{K}[T]$-module by defining $(a_0 + a_1 T + \ldots + a_d T^d)v = a_0 v + a_1 \varphi(v) + \ldots + a_d \varphi^d(v)$. Since $V$ has finite dimension, $V$ is a finitely generated $\mathbb{K}[T]$-module, so the above structure theorem applies. Observe that $V$ cannot have a summand of the type $\mathbb{K}[T]$, since the latter has infinite dimension as a vector space. A more elegant way of seeing this is that, in our language of $\mathbb{K}[T]$-modules, the Cayley-Hamilton theorem states that, if $P$ is the characteristic polynomial of $\varphi$, then $Pv = 0$ for any $v \in V$, and hence $V$ cannot have a free summand. Let us thus write $V \cong M_1 \oplus \ldots \oplus M_r$, with each $M_i$ being a direct sum of blocks of the type $\mathbb{K}[T]/(f_i^{a_i})$ for some nonzero irreducible polynomial $f_i \in \mathbb{K}[T]$. Let us see the interpretation of this decomposition following a series of observations:

1) As we have observed, the product of any element of $V$ by the characteristic polynomial $P$ is zero. Therefore, the polynomials $f_i$ are necessarily irreducible factors of $P$. Moreover, if we have a summand of the type $\mathbb{K}[T]/(f_i^{a_i})$ then $P$ must be divisible by $f_i^{a_i}$.

2) If $V$ has a summand of the type $W \cong \mathbb{K}[T]/(T-\lambda)$, then $W$ is generated by a vector $w$, image of the class of 1 in $\mathbb{K}[T]/(T-\lambda)$, and it holds $(T-\lambda)w = 0$, i.e. $\varphi(w) = \lambda w$, and hence $W$ is generated by an eigenvector of eigenvalue $\lambda$. Reciprocally, an eigenvector $w$ of eigenvalue $\lambda$ generates a submodule of $V$ isomorphic to $\mathbb{K}[T]/(T-\lambda)$

3) If $P(T)$ has $n$ different roots $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$, then for each $i = 1, \ldots, n$ there is a nonzero eigenvector $w_i$ with eigenvalue $\lambda_i$, and we can thus write, according to 2), $V \cong \mathbb{K}[T]/(T-\lambda_1) \oplus \ldots \oplus \mathbb{K}[T]/(T-\lambda_n)$ as $\mathbb{K}[T]$-modules. Reciprocally, having such a decomposition implies that $\varphi$ has $n$ different eigenvalues and it is therefore diagonalizable.

4) More generally, if $V \cong \mathbb{K}[T]/(T-\lambda_1) \oplus \ldots \oplus \mathbb{K}[T]/(T-\lambda_n)$, not necessarily with $\lambda_i \neq \lambda_j$ if $i \neq j$, it also follows that $V$ has a bases of eigenvectors, and hence $\varphi$ is diagonalizable.

5) If If $V$ has a summand of the type $W \cong \mathbb{K}[T]/((T-\lambda)^a)$, then $W$ has dimension $a$, and if $w_1$ is the image of the class of 1 in $\mathbb{K}[T]/((T-\lambda)^a)$, $W$ has a basis $w_1, w_2 = (T-\lambda)w, \ldots, w_a = (T-\lambda)^{a-1}w$. In other words, $w_i = \varphi(w_{i-1}) - \lambda w_{i-1}$ for $i = 2, \ldots, a$ and observe that $(\varphi - \lambda id_V)(w_a) = (\varphi - \lambda id_V)^a w = 0$, hence $\varphi(w_a) = \lambda w_a$. In particular,

$W$ is invariant by $\varphi$. The matrix of $\varphi_{|W}$ with respect to the basis $w_1, \ldots, w_a$ is then

$$\begin{pmatrix} \lambda & & & & \\ 1 & \lambda & & & \\ & \ddots & \ddots & & \\ & & 1 & \lambda & \\ & & & 1 & \lambda \end{pmatrix}$$

i.e. a Jordan block of order $a$. Reversing the construction, a Jordan block of order $a$ produces a summand $W \cong \mathbb{K}[T]/((T-\lambda)^a)$ in $V$.

6) By the above observation, if $\mathbb{K}$ is algebraically closed, or if $P$ factorizes into linear factors, the decomposition of $V$ in summands of the type $W \cong \mathbb{K}[T]/((T-\lambda)^a)$ coincide with the decomposition of the canonical form of $\varphi$ in Jordan blocks, and the way of finding the basis coincides with the one we are taught in a linear algebra course.

7) This allows to generalize the notion of canonical form to arbitrary fields. Assume for instance that $V$ has a summand $W \cong \mathbb{K}[T]/(f)$, where $f = a_0 + a_1 T + \ldots + a_{d-1}T^{d-1}T^d$ is an irreducible monic polynomial. If $w$ is the image of the class of 1 in $\mathbb{K}[T]/(f)$ then $W$ has a basis $w_1 = w, w_2 = Tw = \varphi(w_1), \ldots, w_d = T^{d-1}w = \varphi(w_{d-1})$. Now we have $\varphi(w_d) = T^d w = -a_0 w_1 - a_1 w_2 - \ldots - a_{d-1} w_d$. Hence $W$ is invariant by $\varphi$ and the matrix of $\varphi_{|W}$ with respect to the basis $w_1, \ldots, w_d$ is

$$\begin{pmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ & \ddots & \ddots & & \\ & & 1 & 0 & -a_{d-2} \\ & & & 1 & -a_{d-1} \end{pmatrix}$$

which can be considered as the diagonal block corresponding to the irreducible polynomial $a_0 + a_1 T + \ldots + a_{d-1}T^{d-1}T^d$.

8) In some particular cases, it is possible to find a nicer ad-hoc expression for the matrix of 7). For example, if $\mathbb{K} = \mathbb{R}$, the irreducible factors of the characteristic polynomial are either linear (in whose case we apply what we said in the observation 5)) or quadratic. We write a monic quadratic polynomial as $(T-a)^2 + b^2$, so that we make explicit its roots $a \pm bi$. If $V$ has a summand of the type $\mathbb{R}[T]/\big((T-a)^2 + b^2\big)$, then we generate $W$ by the respective images $w_1$ and $w_2$ of the classes of $b$ and $T-a$. Hence $f(w_1)$ is the image of the class of $bT$ and $f(w_2)$ is the image of the class of $T(T-a)$, i.e. the class of $aT - a^2 - b^2$. Since $bT = ab + b(T-a)$ and $aT - a^2 - b^2 = -b \cdot b + a(T-a)$ it follows that $\varphi(w_1) = aw_1 + bw_2$ and $\varphi(w_2) = -bw_1 + aw_2$. Therefore $W$ is invariant by $\varphi$ and the matrix of $\varphi_{|W}$ with respect to the basis $w_1, w_2$ is

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

which is the real canonical block of order two corresponding to the imaginary eigenvalues $a \pm bi$.

**Exercise 3.19.** Generalize 7) and 8) finding nice Jordan blocks for summands $\mathbb{K}[T]/(f^a)$ (for the generalization of case 7)) and $\mathbb{R}[T]/\big(((T-a)^2+b^2)^r\big)$ (for the generalization of case 8)).

# 4. Rings and modules of fractions

Now we want to construct new modules from existing modules by allowing denominators. One typical example is the construction of $\mathbb{Q}$ starting from $\mathbb{Z}$. We will show first some geometrical examples to clarify the kind of thing we need.

**Example 4.1.** Consider the set $U = \mathbb{A}^1 \setminus \{0\}$. This is obviously not an affine set of $\mathbb{A}^1$ if $\mathbb{K}$ is infinite (since the affine sets of $\mathbb{A}^1$ are given by zeros of polynomials in $\mathbb{K}[X]$, they are necessarily finite except for the whole $\mathbb{A}^1$). But on the other hand we observe that the assignment $X \mapsto (X, \frac{1}{X})$ defines a bijection between $U$ and $C = V(XY - 1) \subset \mathbb{A}^2$. Since $C$ is an affine set, we could also consider $U$ as an affine set via that bijection. With this point of view, a regular function on $U$ would be an element of the ring $\mathbb{K}[X, Y]/(XY - 1)$. Of course this not satisfactory, since we do not have coordinate $Y$ on $U$. The solution is to use the relation $XY = 1$ to write $Y = \frac{1}{X}$. We could thus write any regular function on $U$ as $g(X, \frac{1}{X})$, with $g \in \mathbb{K}[X, Y]$. In other words, a regular function on $U$ is a quotient of the form $\frac{h}{X^m}$, with $h \in \mathbb{K}[X]$ and $m \in \mathbb{N}$, i.e. a quotient of regular function on $\mathbb{A}^1$ with the condition that the denominator does not vanish on any point of $U$ (in fact, if $\mathbb{K}$ is algebraically closed, the only irreducible factor of a polynomial vanishing only at 0 is necessarily $X$).

**Example 4.2.** The above example can be immediately generalized to the case in which $U$ is the open set of an affine set $Z \subset \mathbb{A}^n$ consisting of those points outside $V(f)$, for some $f \in \mathbb{K}[X_1, \ldots, X_n]$. In this case, we can consider the assignment $(X_1, \ldots, X_n) \mapsto (X_1, \ldots, X_n, \frac{1}{f(X_1, \ldots, X_n)})$, which defines a bijection between $U$ and the affine set $Z' \subset \mathbb{A}^{n+1}$ determined by the equations of $Z$ plus the equation $X_{n+1}f - 1 = 0$. Proceeding as in the above example, we see that it is natural to define a regular function on $U$ as a quotient of a regular function on $Z$ and a power of $f$, hence the quotient of two regular functions on $Z$ such that the denominator does not vanish at any point of $U$ (the fact that any regular function on $Z$ vanishing only at points of $V(f)$ is a power of $f$ is only true if $\mathbb{K}$ is algebraically closed, and it will be a consequence of Hilbert's Nullstellensatz).

**Exercise 4.3.** In the conditions of the above example show that, if $I(Z)$ is generated by $f_1, \ldots, f_r$, then $f_1, \ldots, f_r, X_{n+1}f - 1$ generate $I(Z')$.

**Example 4.4.** Let us see that a naive notion of quotient could cause unexpected problems. For instance, let $Z \subset \mathbb{A}^2$ be the union of the lines $X = 0$ and $Y = 0$. It is easy to see that $I(Z)$ is the ideal $(XY)$, and hence the set of regular functions on $Z$ is $\mathbb{K}[X, Y]/(XY)$. We proceed as in Example 4.2 and consider $U = Z \setminus V(Y)$. Thus the set "presumed" ring of regular functions on $U$ should be the set of quotients of the form $\frac{\bar{g}}{X^m}$, where $m \in N$ and $\bar{g}$ is the class modulo $(XY)$ of a polynomial $g \in \mathbb{K}[X, Y]$. Observe that $U$ is nothing but

the line $X = 0$ minus the point $(0, 0)$ (hence essentially the set of Example 4.1). It is thus clear that $\bar{X}$, or $\frac{\bar{X}}{1}$ if you want to write denominators for all the elements, must be the function zero, or $\frac{0}{1}$. But the equality $\frac{\bar{X}}{1} = \frac{0}{1}$ does not follow from the usual rule for the equality of fractions, since $\bar{X}$ is not zero in $\mathbb{K}[X, Y]/(XY)$. We can however arrive to the right conclusion by using the following chain of natural equalities: $\frac{\bar{X}}{1} = \frac{\bar{X}\bar{Y}}{\bar{Y}} = \frac{0}{\bar{Y}} = \frac{0}{1}$. In other words, the key point for the equality $\frac{\bar{X}}{1} = \frac{0}{1}$ to hold is not the equality $\bar{X} = 0$, but its product by $\bar{Y}$ (which is an allowable denominator.

All this suggests the idea of defining rings with denominators. We will make the construction more general, i.e. for modules. Of course the first thing to do will be to choose the right notion of denominator. We concrete now all this.

**Definition.** Let $A$ be a ring. A *multiplicative set* of $A$ will be a subset $S \subset A$ such that $1 \in S$, $0 \notin S$, and for any $s, s' \in S$ it holds $ss' \in S$.

In the spirit of Example 4.4, given a multiplicative set $S$ of a ring $A$ and an $A$-module $M$, we define the following relation on $M \times S$: $(m_1, s_1) \sim (m_2, s_2)$ if and only if there exists $s \in S$ such that $s(s_2 m_1 - s_1 m_2) = 0$.

**Proposition 4.5.** *The above relation is an equivalent relation. Moreover, if $M = A$, the set of equivalence classes is a ring with the obvious operations (denoted with $S^{-1}A$). And for any $A$-module $M$, the set of equivalence classes is an $S^{-1}A$-module, again with the obvious operations, (denoted $S^{-1}M$).*

*Proof:* The reflexive and symmetric properties are obvious. For the transitive property, assume $(m_1, s_1) \sim (m_2, s_2)$ and $(m_2, s_2) \sim (m_3, s_3)$. By definition, there exists $s, s' \in S$ such that $s(s_2 m_1 - s_1 m_2) = 0$ and $s'(s_3 m_2 - s_2 m_3) = 0$. But then it follows $ss'(s_3 m_1 - s_1 m_3) = 0$, which proves $(m_1, s_1) \sim (m_3, s_3)$. We leave as en easy exercise to prove that $S^{-1}A$ is a ring and that $S^{-1}M$ is an $S^{-1}A$-module. □

**Definition.** The ring $S^{-1}A$ is called the *ring of fractions of $A$ with respect to $S$*. The module $S^{-1}M$ is called the *module of fractions of $M$ with respect to $S$*. There is a natural map $\varphi_S : M \to S^{-1}M$ defined by $\varphi_S(m) = \frac{m}{1}$, which in general is not injective (see Exercise 4.6). We will usually identify an element $f \in A$ with its image in $S^{-1}A$.

**Exercise 4.6.** Prove that the natural map $\varphi_S : M \to S^{-1}M$ defined by $\varphi_S(m) = \frac{m}{1}$ is a homomorphism of $A$-modules. Show also that the kernel of $\varphi_S$ is the ideal $\{m \in M \mid sm = 0 \text{ for some } s \in S\}$. Hence, if $S$ does not contain zerodivisors of $M$, then $\varphi_S$ is injective. Prove also that, under this new condition, two elements $\frac{m}{s}$ and $\frac{m'}{s'}$ are equal if and only if $s'm = sm'$.

**Example 4.7.** We give now some examples, the first two corresponding to the previous geometric examples:

(i) If $\mathfrak{p}$ is a prime ideal of $A$, then $S := A \setminus \mathfrak{p}$ is easily seen to be a multiplicative set of $A$. In this case $S^{-1}M$ is denoted by $M_{\mathfrak{p}}$ and it is called the *localization of $M$ at the prime ideal $\mathfrak{p}$*.

(ii) In case $f \in A$ is a non-nilpotent element of $A$, the set $S$ of non-negative powers of $f$ is a multiplicative set of $A$, and $S^{-1}M$ will be denoted by $M_f$. When $M = A$, this corresponds to Example 4.2.

(iii) If we take $S$ to be the set of nonzerodivisors of a ring $A$, it is clear that $S$ is a multiplicative set of $A$. The ring $S^{-1}A$ is called then the *total quotient ring of $A$*. The map $A \to S^{-1}A$ is injective in this case (see Exercise 4.6). If $A$ is a domain, then $S = A \setminus \{0\}$, and then $S^{-1}A$ is a field called the *quotient field of $A$* (think of this as the generalization of the construction of $\mathbb{Q}$ starting from $\mathbb{Z}$).

**Proposition 4.8.** *Let $A$ be a ring and $M$ an $A$-module. Then:*

*(i) If $N$ is a submodule of $M$, then $S^{-1}N := \{\frac{n}{s} \in S^{-1}M \mid n \in N,\ s \in S\}$ is a submodule of $S^{-1}M$.*

*(ii) For any homomorphism of $A$-modules $\psi : M \to M'$, the map $S^{-1}\psi : S^{-1}M \to S^{-1}M'$ defined by $\frac{m}{s} \mapsto \frac{\psi(m)}{s}$ is a homomorphism of $S^{-1}A$-modules extending $\psi$ (via the corresponding maps $\varphi_S$ for $M$ and $M'$). Moreover, $\ker(S^{-1}\psi) = S^{-1}(\ker\psi)$ and $\mathrm{Im}(S^{-1}\psi) = S^{-1}(\mathrm{Im}\,\psi)$; hence if $\psi$ is injective (resp. surjective) then $S^{-1}\psi$ is also injective (resp. surjective).*

*(iii) The quotient $S^{-1}M/S^{-1}N$ is naturally isomorphic to $S^{-1}(M/N)$.*

*(iv) Assume that there exists an ideal $I \subset A$ such that $fm = 0$ for each $f \in I, m \in M$. Then $M$ has a natural structure of $A/I$-module, and if $S \cap I = \emptyset$, then the set $\bar{S} \subset A/I$ of classes of elements of $S$ is a multiplicative set of $A/I$, and there is a natural isomorphism of $A$-modules between $S^{-1}M$ and $\bar{S}^{-1}M$.*

*Proof:* The proofs of (i) and (ii) are straightforward. As a sample, let us prove the equality $\ker(S^{-1}\psi) = S^{-1}(\ker\psi)$, which is the only one for which some extra work is needed. Since an element of $S^{-1}(\ker\psi)$ can be written as $\frac{m}{s}$ with $m \in \ker\psi$, it is clear that it belongs to $\ker(S^{-1}\psi)$. Reciprocally, if $\frac{m}{s}$ is in $\ker(S^{-1}\psi)$, then $\frac{\psi(m)}{s} = 0$ in $S^{-1}M'$. This means that there exists $s' \in S$ such that $s'\psi(m) = 0$ in $M'$. Therefore, $s'm$ is in $\ker\psi$, and writing $\frac{m}{s} = \frac{s'm}{s's}$ we conclude that $\frac{m}{s}$ is in $S^{-1}(\ker\psi)$.

For (iii), we get from (ii) that the canonical surjection $\pi : M \to M/N$ induces an epimorphism $S^{-1}\pi : S^{-1}M \to S^{-1}(M/N)$. Its kernel is $S^{-1}(\ker\pi) = S^{-1}N$, which proves the wanted isomorphism.

For (iv), everything is clear except the isomorphism (observe that $\bar{S}$ does not contain the zero class since $S \cap I = \emptyset$). We define it by $\frac{m}{s} \mapsto \frac{m}{\bar{s}}$. This is well defined since $\frac{m}{s} = \frac{m'}{s'}$ iff there exists $s'' \in S$ such that $s''s'm = s''sm'$, iff $\bar{s}''\bar{s}'m = \bar{s}''\bar{s}m'$, iff $\frac{m}{\bar{s}} = \frac{m'}{\bar{s}'}$. Hence this is an injective map, which is clearly surjective □

When restricting our attention to rings of fractions we can say more:

**Proposition 4.9.** *Let $A$ be a ring and let $S$ be a multiplicative set of $A$.*

*(i) If $I$ is an ideal of $A$, the set $S^{-1}I := \{\frac{f}{s} \in S^{-1}A \mid f \in I\}$ is an ideal of $S^{-1}A$, which is proper if and only if $S \cap I = \emptyset$.*

*(ii) If $S \cap I = \emptyset$, the quotient $S^{-1}A/S^{-1}I$ is canonically isomorphic (as a ring) to $\bar{S}^{-1}(A/I)$, where $\bar{S} \subset A/I$ is the set of classes modulo $I$ of the elements of $S$.*

*(iii) If $\mathfrak{p}$ is a prime ideal not meeting $S$, then $S^{-1}\mathfrak{p}$ is a prime ideal, and $\frac{f}{s} \in S^{-1}\mathfrak{p}$ if and only if $f \in \mathfrak{p}$.*

*(iv) If $\mathfrak{p}'$ is a prime ideal of $S^{-1}A$, then $\bar{\mathfrak{p}}' := \{f \in A \mid \frac{f}{1} \in \bar{\mathfrak{p}}'\}$ is a prime ideal of $A$.*

*(v) The assignments $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$ and $\mathfrak{p}' \mapsto \bar{\mathfrak{p}}'$ are inverse to each other and induce a bijection between the set of prime ideals of $A$ not meeting $S$ and the set of prime ideals of $S^{-1}A$. In particular, if $\mathfrak{p}$ is a prime ideal of $A$, there is a bijection between the set of prime ideals of $A_{\mathfrak{p}}$ and the set of prime ideals of $A$ contained in $\mathfrak{p}$.*

*Proof:* The first part of (i) is Proposition 4.8(i). For the second part, we remark that $S^{-1}I$ is not proper if and only if $\frac{1}{1}$ is in $S^{-1}I$. Observe that this does not imply a priori that 1 is in $I$ (in (iii) we will get such property only for prime ideals), but just that $\frac{1}{1} = \frac{f}{s}$, for some $f \in I$, $s \in S$. But by definition this equality means that there exists some $t \in S$ such that $st = ft$. The left-hand side in the equality is in $S$, while the right-hand side is in $I$, which proves that $S \cap I$ is not empty. Reciprocally, if there exists $s \in S \cap I$, then $\frac{1}{1} = \frac{s}{s}$, which is in $S^{-1}I$. Hence $S^{-1}I$ is not proper.

For part (ii), we first observe that by Proposition 4.8(iii) we know that $S^{-1}A/S^{-1}I$ is canonically isomorphic to $S^{-1}(A/I)$. But Proposition 4.8(iv) implies that this is in turn canonically isomorphic to $\bar{S}^{-1}(A/I)$ (as $A$-modules, but it is straightforward to check that also as rings).

For part (iii), we first conclude from part (ii) that $S^{-1}A/S^{-1}\mathfrak{p}$ is isomorphic to $S^{-1}(A/\mathfrak{p})$, which is an integral domain (because $A/\mathfrak{p}$ is), and hence $S^{-1}\mathfrak{p}$ is a prime ideal. For the second statement, if $\frac{f}{s}$ is in $S^{-1}\mathfrak{p}$, it means that there exists $f' \in \mathfrak{p}$, $s' \in S$ such that $\frac{f}{s} = \frac{f'}{s'}$. By definition, there exists $t \in S$ such that $fs't = f'st$, which is an element of $\mathfrak{p}$. Since $st$ is in $S$, by hypothesis is not in $\mathfrak{p}$. And since $\mathfrak{p}$ is prime, this implies that $f$ is in $\mathfrak{p}$, as wanted.

Parts (iv) and (v) are straightforward. □

**Exercise 4.10.** Extend the above proposition to primary ideals:

(i) If $S$ is a multiplicative set and $\mathfrak{q}$ is a $\mathfrak{p}$-primary ideal of $A$, prove that $S \cap \mathfrak{p} = \emptyset$ if and only if $S \cap \mathfrak{q} = \emptyset$.

(ii) In the above situation, prove that $\frac{f}{s} \in S^{-1}\mathfrak{q}$ if and only if $f \in \mathfrak{q}$.

(iii) Again under the same conditions, prove that $S^{-1}\mathfrak{q}$ is $S^{-1}\mathfrak{p}$-primary.

(iv) Conclude that there exists a bijection between the primary ideals of $A$ not meeting $S$ and the primary ideals of $S^{-1}A$.

**Remark 4.11.** Observe that Proposition 4.9(v) provides a natural bijection between $\mathrm{Spec}(S^{-1}A)$ and the subset $\Sigma_S \subset \mathrm{Spec}(A)$ consisting of all prime ideals of $A$ not meeting $S$ (this bijection is in fact a homeomorphism with the Zariski topology, as we will see in Lemma 6.3). Hence, at we did in Examples 4.1 and 4.2, it makes sense to speak of regular functions on the subset $\Sigma_S$ and identify them with elements of $S^{-1}A$ (see section 1). Precisely, if $\alpha = \frac{f}{s} \in S^{-1}A$, for any $\mathfrak{p} \in \Sigma_S$, we can consider the class of $\alpha$ in $S^{-1}A/S^{-1}\mathfrak{p}$, which by Proposition 4.9(ii) is isomorphic to $\bar{S}^{-1}(A/\mathfrak{p})$. If $k(\mathfrak{p})$ is the quotient field of $A/\mathfrak{p}$, we have then inclusions $A/\mathfrak{p} \subset S^{-1}(A/\mathfrak{p}) \subset k(\mathfrak{p})$ (see Exercise 4.6), which proves that $A/\mathfrak{p}$ and $S^{-1}A/S^{-1}\mathfrak{p}$ have the same quotient field. Hence the class of $\alpha$ determines a map from $\Sigma_S$ to the disjoint union of all the $k(\mathfrak{p})$. Observe that the denominator $s$ in $\alpha$ is in $S$, hence it is not in any $\mathfrak{p} \in \Sigma_S$, which means that it does not "vanish" at $\mathfrak{p}$.

In particular, when $S$ is the set of powers of a non-nilpotent $f \in A$, then we have a natural homeomorphism between $\mathrm{Spec}(A_f)$ and $D(f)$. Recall from Exercise 1.10(i) that the sets of the form $D(f)$ provide a basis of the Zariski topology of $\mathrm{Spec}(A)$. Hence $A_f$ can be regarded as the set of regular functions defined in the open set $D(f)$. When $S = A \setminus \mathfrak{p}$, then the elements of $A_\mathfrak{p}$ take the form $\alpha = \frac{g}{f}$, with $f, g \in A$ and $\notin \mathfrak{p}$. This means that $\alpha$ is a regular function in the neighborhood $D(f)$ of $\mathfrak{p}$. Hence $A_\mathfrak{p}$ can be regarded as germs of regular functions in a sufficiently small neighborhood of $\mathfrak{p}$. Observe that Proposition 4.9(v) is saying that $A_\mathfrak{p}$ contains only one maximal ideal (precisely the one corresponding to $\mathfrak{p}$), which we will denote with $\mathfrak{p}A_\mathfrak{p}$. This maximal ideal can be naturally identified with the set of germs of regular functions vanishing at $\mathfrak{p}$.

**Proposition 4.12.** *Let $A$ be a ring. Then:*

*(i) The set of the nonunits of $A$ is the union of the maximal ideals of $A$.*

*(ii) The set of nonunits of $A$ is an ideal if and only if $A$ has a unique maximal ideal; in this case, the maximal ideal is precisely the set of nonunits.*

*Proof:* If an element of $A$ is contained in a maximal ideal it is clear that it cannot be a unit (otherwise the maximal ideal would be the total ideal). On the other hand, if $f$ is not

a unit, then the ideal $(f)$ is proper, and hence by Proposition 1.6 it is contained in some maximal ideal. This proves (i).

If the set of non units is an ideal $I$ (which is proper, because $1 \notin I$), then $I$ is the union of the maximal ideals of $A$. Therefore any maximal ideal is contained in $I$, and hence coincides with $I$. This means that $I$ is maximal and is the only one. Reciprocally, if there is only one maximal ideal, by part (i) the set of nonunits is that maximal ideal. This proves (ii). □

**Definition.** A *local ring* is a ring containing just one maximal ideal.

**Example 4.13.** A typical example of local ring is the ring of formal series $\mathbb{K}[[X_1, \ldots, X_n]]$ over a field $\mathbb{K}$. Its set of non units is (Exercise 2.7(i)) is the set of series without constant term, i.e. the series "vanishing" at the origin, which is the ideal $(X_1, \ldots, X_n)$. This fits exactly with our intuition of what local means. For instance, if you think of $\mathbb{K}$ to be $\mathbb{R}$ or $\mathbb{C}$ and you think of analytic functions in a neighborhood of $(0, \ldots, 0)$, then they are uniquely determined by their Taylor series at the point (the only difference is that in $\mathbb{K}[[X_1, \ldots, X_n]]$ we do not care about convergence). As another algebraic evidence, we leave as an easy exercise to show that there is a natural ring homomorphism $\mathbb{K}[X_1, \ldots, X_n]_{(X_1,\ldots,X_n)} \to \mathbb{K}[[X_1, \ldots, X_n]]$, which can be considered as taking the Taylor expansion of the quotient of two polynomial functions (with the condition that the denominator does not vanish at the origin).

The following result can also be interpreted in the framework of germs of regular functions: if a quotient of regular function is locally regular at any (closed) point, then it is globally regular.

**Proposition 4.14.** *Let $A$ be an integral domain with quotient field $K$. Then the intersection in $K$ of all the localizations $A_{\mathfrak{m}}$ in maximal ideals $\mathfrak{m} \subset A$ is $A$. In particular, $A$ is also the intersection in all its localizations in prime ideals.*

*Proof:* Assume that we have an element $\alpha \in K$ that is not in $A$. This means that the ideal $I := \{f \in A \mid f\alpha \in A\}$ (this can be regarded as the set of all possible denominators of $\alpha$) is not the whole $A$ (since $1 \in I$ would imply that $\alpha$ is in $A$). Therefore, by Proposition 1.6 there exists a maximal ideal $\mathfrak{m}$ of $A$ containing $I$. But then $\alpha$ is not in $A_{\mathfrak{m}}$, since otherwise one could write $\alpha = \frac{g}{f}$, with $g \in A$ and $f \notin \mathfrak{m}$, hence $f\alpha = g \in A$, and by definition $f \in I$, contradicting that $I$ is contained in $\mathfrak{m}$. □

Localizing modules at prime ideals has a similar meaning as before: it means that we "restrict" the module to a sufficiently small neighborhood of the prime ideal. This is a little more difficult to justify, so that we will just give the evidence of this with a series of results.

**Lemma 4.15.** *Let $A$ be a ring and let $M$ be an $A$-module. Then the following are equivalent*

*(i)* $M = 0$.

*(ii)* $M_{\mathfrak{p}} = 0$ *for any prime ideal* $\mathfrak{p} \subset A$.

*(iii)* $M_{\mathfrak{m}} = 0$ *for any maximal ideal* $\mathfrak{m} \subset A$.

*Proof:* It is clear that (i) implies (ii) and that (ii) in turn implies (iii). So we are left to prove that (iii) implies (i). Assume that we have a nonzero element $m \in M$. Then the ideal $\{f \in A \mid fm = 0\}$ is not the total ideal, hence it is contained in a maximal ideal $\mathfrak{m}$. Since $\frac{m}{1}$ must be zero in $M_{\mathfrak{m}}$, it follows that there exists $s \notin \mathfrak{m}$ such that $sm = 0$, which is absurd. Hence $M = 0$, as wanted. □

From this lemma we immediately get the following:

**Proposition 4.16.** *Let $\psi : M \to N$ be a homomorphism of $A$-modules. Then:*

*(i)* *$\psi$ is injective if and only if $\psi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is injective for any prime ideal $\mathfrak{p} \subset A$ if and only if $\psi_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective for any maximal ideal $\mathfrak{m} \subset A$.*

*(ii)* *$\psi$ is surjective if and only if $\psi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is surjective for any prime ideal $\mathfrak{p} \subset A$ if and only if $\psi_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is surjective for any maximal ideal $\mathfrak{m} \subset A$.*

*(iii)* *$\psi$ is an isomorphism if and only if $\psi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is an isomorphism for any prime ideal $\mathfrak{p} \subset A$ if and only if $\psi_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is an isomorphism for any maximal ideal $\mathfrak{m} \subset A$.*

*Proof:* Let $K$ be the kernel of $\psi$. We know from Proposition 4.8(ii) that $K_{\mathfrak{p}}$ is the kernel of $\psi_{\mathfrak{p}}$. Then (i) follows immediately from Lemma 4.15. We obtain (ii) with the same reasoning when using the image of $\psi$ instead of its kernel. And finally (iii) is an immediate consequence of (i) and (ii). □

**Exercise 4.17.** Let $S$ be a multiplicative set of a ring $A$.

(i) Prove that $S^{-1}A$ is characterized, up to isomorphism, by the following universal property: there is a homomorphism $\varphi : A \to S^{-1}A$ such that the image by $\varphi$ of any element of $S$ is a unit, and for any ring homomorphism $\psi : A \to B$ such that the image by $\psi$ of any element of $S$ is a unit, then there exists a unique ring homomorphism $\eta : S^{-1}A \to B$ such that $\psi = \eta \circ \varphi$.

(ii) If $M$ is an $A$-module, prove that $S^{-1}M$ is characterized by the following universal property: there is an $A$-bilinear map $\varphi : S^{-1}A \times M \to S^{-1}M$, and for any other $S^{-1}A$-module $N$ such that there is an $A$-bilinear map $\psi : S^{-1}A \times M \to N$ then there exists a unique homomorphism of $S^{-1}A$-modules $\eta : S^{-1}M \to N$ such that $\psi = \eta \circ \varphi$.

**Remark 4.18.** The above universal property for $S^{-1}M$ is saying that it is built by starting with $M$, but extending the multiplication by elements of $A$ to a multiplication by elements of $S^{-1}A$. For instance, consider $M = \mathbb{Z}^n$ as a $\mathbb{Z}$-module and take $S = \mathbb{Z} \setminus \{0\}$. It is clear that, in the same way as $S^{-1}\mathbb{Z} = \mathbb{Q}$, it holds $S^{-1}\mathbb{Z}^n = \mathbb{Q}^n$. The universal property is saying that $\mathbb{Q}^r$ is obtained by letting the elements of $\mathbb{Z}^n$ to be multiplied by elements of $\mathbb{Q}$. Of course, it is possible to generalize this construction when allowing multiplication by elements of $\mathbb{R}$ (thus getting $\mathbb{R}^n$) or by elements of $\mathbb{C}$ (getting $\mathbb{C}^n$). Since this is not obtained as a module of fractions, we will need for this a new definition, based on the universal property for $S^{-1}M$.

**Definition.** The *tensor product of two $A$-modules $M$* and $N$ is a $A$-module, (unique up to isomorphism), $M \otimes_A N$ satisfying the following universal property: there is an $A$-bilinear map $\varphi : M \times N \to M \otimes_A N$ and for any other $A$-module $P$ with an $A$-bilinear map $\psi : M \times N \to P$ there exists a unique homomorphism of $A$-modules $\eta : M \otimes_A N \to P$ such that $\psi = \eta \circ \varphi$. Given $m \in M$ and $n \in N$, $\varphi(m, n)$ is denoted by $m \otimes n$.

We give now a construction showing the existence of the tensor product of any two modules.

**Lemma 4.19.** *Let $M$, $N$ be two $A$-modules. Let $F$ be the free $A$-module having as a formal basis all the elements of the form $(m, n) \in M \times N$. Let $F'$ be the submodule of $F$ generated by all the elements of the form $(fm + f'm', n) - f(m, n) - f'(m', n)$, $(m, fn + f'n') - f(m, n) - f'(m, n')$, with $m, m' \in M$, $n, n' \in N$ and $f, f' \in A$. Then $F/F'$ is the tensor product of $M$ and $N$.*

*Proof:* It is clear from the definition that we have a map $\varphi : M \times N \to F/F'$ associating to each $(m, n)$ the class modulo $P'$ of the generator $(m, n)$ of $F$. It is bilinear because the required relations are precisely obtained when quotienting with $F'$. On the other hand, given another $A$-module $P$ and an $A$-bilinear map $\psi : M \times N \to P$, we can define a homomorphism $\eta' : F \to P$ by the condition $\eta'(m, n) = \psi(m, n)$. The fact the $\psi$ is $A$-bilinear implies that all the generators of $F'$ map to zero. Hence $\eta'$ factors through $\eta : F/F' \to P$ and it clearly holds that $\psi = \eta \circ \varphi$. On the other hand, this equality obviously determine the uniqueness of $\eta$. □

**Exercise 4.20.** If $A$ is a ring and $B$ is another ring that has structure of $A$-module, prove that $A[X_1, \ldots, X_n] \otimes_A B$ is isomorphic to $B[X_1, \ldots, X_n]$ (in particular, $A[X_1, \ldots, X_n] \otimes_A A[Y_1, \ldots, Y_m]$ is isomorphic to $A[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$). In general, for any $A$-module $M$, $M \otimes_A B$ has a natural structure of $B$ module, and can be considered as a way of "changing coefficients" from $A$ to $B$ (think of $A = \mathbb{R}$ and $B = \mathbb{C}$; then the tensor product gives the complexification of any vector space).

# 5. Integral dependence and the generalized Nullstellensatz

In this section we will try to generalize the Nullstellensatz when the ground field is not necessarily algebraically closed. In view of Remark 1.18, an idea will be to understand what the maximal ideals of $\mathbb{K}[X_1, \ldots, X_n]$ are (and see that the situation is as in Examples 0.6 and 0.7). We start with several considerations that will lead us to the right techniques to use.

**Example 5.1.** Consider the first projection map $p : C = V(Y^2 - X) \subset \mathbb{A}^2_{\mathbb{K}} \to \mathbb{A}^1_{\mathbb{K}}$ given by $p(a, b) = a$. If $\mathbb{K}$ is algebraically closed, it is clear that this map is surjective and the the inverse image of any point consists of two points except for $a = 0$. Even if this last case, we can say algebraically that the inverse image of 0 consist of two points, in this case infinitely close. Indeed, for any $a \in \mathbb{A}^1_{\mathbb{K}}$, in order to find the inverse image of $a$ we have to solve the equations $Y^2 - X = 0, X = a$. In other words, the ideal corresponding to $p^{-1}(a)$ is $(Y^2 - Y, X - a)$. In case $a = 0$, as indicated in Example 1.14, this ideal becomes $(Y^2, X)$, which represents the point $(0, 0)$ and a tangent direction, or if you prefer, the point $(0, 0)$ counted with multiplicity two.

We can try to recover this information in a more algebraic way. The map $p$ induces a map $\mathcal{O}(\mathbb{A}^1_{\mathbb{K}}) \to \mathcal{O}(C)$ given by $f \mapsto f \circ p$. In coordinates, this map is nothing but the natural inclusion $\mathbb{K}[X] \hookrightarrow \mathbb{K}[X, Y]/(Y^2 - X)$. Observe that this natural inclusion allows to endow $\mathbb{K}[X, Y]/(Y^2 - X)$ with a natural structure of $\mathbb{K}[X]$-module, namely $f(X)\bar{g}(X, Y) = \overline{fg}$ (a bar denoting the class of a polynomial in $\mathbb{K}[X, Y]$ modulo $(Y^2 - X)$). It is clear that $\mathbb{K}[X, Y]/(X^2 + Y^2 - 1)$ is a $\mathbb{K}[X]$-module generated by the classes of 1 and $Y$. The reason is that, given any $g \in \mathbb{K}[X, Y]$ you can divide it by $Y^2 - X$ as polynomials in $Y$ (since $Y^2 - X$ is monic) and get that the class of $g$ is the class of its remainder, which can be written as $r_1(X)Y + r_2(X)$. On the other hand, it is clear that the class of $r_1(X)Y + r_2(X)$ is zero (i.e. is a multiple of $Y^2 - X$) if and only if $r_1 = r_2 = 0$. Therefore, $\mathbb{K}[X, Y]/(Y^2 - X)$ is a free $\mathbb{K}[X]$-module of rank two. It is not a coincidence that this rank is exactly the number of points in the inverse image of any point of $\mathbb{A}^1_{\mathbb{K}}$.

The above example suggests that a map of rings provides a richer structure. We concrete it in the following:

**Definition.** An *algebra over a ring* $A$ is a ring $B$ that has the structure of module over $A$ in such a way that the addition in both structures coincide, and there is an associativity of the type $a(b_1 b_2) = (ab_1)b_2$. A *homomorphism of* $A$*-algebras* is a map $B_1 \to B_2$ such that it is both a homomorphism of rings and a homomorphism of $A$-modules.

**Remark 5.2.** The notion of $A$-algebra is in fact equivalent to the notion of homomorphism of rings $f : A \to B$. Indeed, given such a homomorphism, we can endow $B$ with a structure

of $A$-module by defining $ab$ as $f(a)b$. Reciprocally, if $B$ is an $A$-algebra, then we can define $f : A \to B$ by $f(a) = a1_B$ which is a homomorphism of rings (here you need the associativity condition). Both processes are clearly inverse from each other. With this equivalence, if $B_1, B_2$ are two $A$-algebras whose respective structures are given by homomorphisms of rings $f_1 : A \to B_1$, $f_2 : A \to B_2$, then $f : B_1 \to B_2$ is a homomorphism of $A$-algebras if and only if it is a homomorphism of rings such that $f_2 = f \circ f_1$.

**Example 5.3.** Let us see that things are not always as nice as suggested by Example 5.1. We consider now $C = V(XY - 1)$ and again consider the first projection $p : C \to \mathbb{A}^1_{\mathbb{K}}$. This time the map is not surjective, but any point of $\mathbb{A}^1_{\mathbb{K}}$ except 0 has exactly one preimage. What does it means in terms of the $\mathbb{K}[X]$-module structure on $\mathbb{K}[X, Y]/(XY - 1)$ induced by $\mathbb{K}[X] \hookrightarrow \mathbb{K}[X, Y]/(XY - 1)$? We observe now that, even if a general point has only one preimage, $\mathbb{K}[X, Y]/(XY - 1)$ is not finitely generated. Indeed, if the classes of $g_1, \ldots, g_r$ generated $\mathbb{K}[X, Y]/(XY - 1)$ as $\mathbb{K}[X]$-module, let $d$ be the maximum of the degrees of $g_1, \ldots, g_r$ in the variable $Y$. Then the class of $Y^{d+1}$ cannot be written as $f_1g_1 + \ldots + f_rg_r$, with $f_1, \ldots, f_r \in \mathbb{K}[X]$, since this would mean that $Y^{d+1} - f_1g_1 - \ldots - f_rg_r$ (which is a monic polynomial in $Y$) must be a multiple of $XY - 1$, and this is impossible.

However this is not a pathology of the curve itself, since a suitable change of coordinates allows us to write the hyperbola like $V(Y^2 - X^2 - 1)$, and in this case the projection onto $\mathbb{A}^1_{\mathbb{K}}$ works exactly as in Example 5.1. In fact the point is to find a good system of coordinates in such a way that we find a monic polynomial in $Y$ (this is exactly what allowed us to work in Example 5.1, since we could perform the Euclidean division). On the other hand, the use such a good system of coordinates to get a monic polynomial (see Lemma 1.15) was also the main idea for the proof of the Nullstellensatz. This motivates the following:

**Definition.** Let $A$ be a subring of a ring $B$. Then an element $b \in B$ is said to be integral over $A$ if it satisfy a monic polynomial with coefficients in $A$, i.e. there is a relation $b^r + a_{r-1}b^{r-1} + \ldots + a_1b + a_0 = 0$, with $a_{r-1}, \ldots, a_1, a_0 \in A$. If all the elements of $B$ are integral over $A$, we say that $B$ *is integral over* $A$.

**Proposition 5.4.** *Let $A$ be a UFD and let $K$ be its quotient field. If $\frac{p}{q}$, with $p$ and $q$ coprime, is a root of the polynomial $a_0 + a_1X + \ldots + a_{n-1}X^{n-1} + a_nX^n \in A[X]$, then $p$ is a divisor of $a_0$ and $q$ is a divisor of $a_n$. Hence, if $a_n = 1$, then $\frac{p}{q} \in A$. In particular, any rational root of a monic polynomial with coefficients in $\mathbb{Z}$ is necessarily an integer.*

*Proof:* Multiplying by $q^n$ the equality $a_0 + a_1(\frac{p}{q}) + \ldots + a_{n-1}(\frac{p}{q})^{n-1} + a_n(\frac{p}{q})^n = 0$, we get the equality $a_0q^n + a_1pq^{n-1} + \ldots + a_{n-1}p^{n-1}q + a_np^n = 0$. From this we obtain that $p$ divides $-(a_1pq^{n-1} + \ldots + a_{n-1}p^{n-1}q + a_np^n) = a_0q^n$, and hence it divides $a_0$. Similarly, $q$ divides $-(a_0q^n + a_1pq^{n-1} + \ldots + a_{n-1}p^{n-1}q) = a_np^n$, and hence divides $a_n$. □

The above examples also suggest the following:

**Definition.** Given an $A$-algebra $B$ and elements $b_1, \ldots, b_r \in B$, the *$A$-algebra generated by $b_1, \ldots, b_r$* is the subalgebra of $B$, denoted by $A[b_1, \ldots, b_r]$, consisting of all the polynomial expressions, with coefficients in $A$, of the elements $b_1, \ldots, b_r$. If $B$ can be written as $A[b_1, \ldots, b_r]$ for a finite set of elements $b_1, \ldots, b_r \in B$, $B$ is called a *finitely generated $A$-algebra*. On the other hand, $B$ is called a *finite algebra* if it is finitely generated as an $A$-module.

Observe that clearly a finite algebra is also finitely generated, but the converse is not true. For instance, in Example 5.3 we have seen that $\mathbb{K}[X,Y]/(XY-1)$ is not a finite $\mathbb{K}[X]$-algebra, while it is obvious a finitely generated $\mathbb{K}[X]$-algebra (generated by the class of $Y$).

**Lemma 5.5.** *If $A \subset B \subset C$ are rings, $B$ is finite over $A$ and $C$ is finite over $B$, then $C$ is finite over $A$.*

*Proof:* Let $\{b_1, \ldots, b_r\}$ be generators of $B$ as an $A$-module, and let $\{c_1, \ldots, c_1\}$ be generators of $C$ as a $B$-module. For any $c \in C$, we can write $c = b'_1 c_1 + \ldots + b'_s c_s$, with $b'_1, \ldots, b'_s \in B$. On the other hand, any $b'_i$ can be written as $b'_i = a_{i1} b_1 + \ldots + a_{ir} b_r$. Therefore, $c$ can be written as the sum $\Sigma_{i,j} a_{ij} b_j c_i$. Hence the finite set $\{b_j c_i\}$ generates $C$ as an $A$-algebra. □

**Proposition 5.6.** *Let $A \subset B$ be rings and $b \in B$. Then the following are equivalent:*

*(i) The element $b$ is integral over $A$.*

*(ii) $A[b]$ is a finite $A$-algebra.*

*(iii) $A[b]$ is contained in a finitely generated $A$-module.*

*Proof: (i)⇒(ii).* Let $f(X) = a_0 + a_1 X + \ldots + a_{r-1} X^{r-1} + X^s \in A[X]$ be a monic polynomial such that $f(b) = 0$ (which exists since $b$ is integral over $A$). By definition of $A[b]$, any element of it has the form $g(b)$, where $g(X)$ is a polynomial with coefficients in $A$. Since $f(X)$ is monic, we can perform the Euclidean division of $g$ between $f$, and obtain an equality $g(X) = q(X) f(X) + r(X)$, where $q, r$ are in $A[X]$ and $r$ has degree at most $sr$, i.e. it can be written as $r(X) = a'_0 + a'_1 X + \ldots + a'_{s-1} X^{s-1}$. We thus have

$$g(b) = r(b) = a'_0 + a'_1 b + \ldots + a'_{s-1} b^{s-1}$$

Since such a relation exists for any $g(b) \in A[b]$, it follows that $A[b]$ is generated, as an $A$-module, by $\{1, b, \ldots, b^{s-1}$. Hence $A[b]$ is a finitely generated $A$-module, i.e. a finite $A$-algebra.

*(ii)⇒(iii).* It is trivial: just take $A[b]$ as the required subalgebra.

*(iii)⇒(i).* Assume now that $A[b]$ is contained in an $A$-module $C$ generated by elements $c_1, \dots c_r$. For each $i = 1, \dots, r$, the element $bc_i$ is still in $C$, so that we can write $bc_i = a_{i1}c_1 + \dots + a_{ir}c_r$, with the $a_{ij}$'s in $A$. We thus find a relation

$$\begin{pmatrix} b - a_{11} & -a_{12} & \dots & -a_{1r} \\ -a_{12} & b - a_{22} & \dots & -a_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{r1} & -a_{r2} & \dots & b - a_{rr} \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_r \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

We observe that the determinant of the left-hand side matrix takes the form $b^r + a_{r-1}b^{r-1} + \dots + a_1 b + a_0$ for some $a_{r-1}, \dots, a_1, a_0 \in A$. Multiplying the above equality with the adjoint matrix of the left-hand side matrix, we obtain that $(b^r + a_{r-1}b^{r-1} + \dots + a_1 b + a_0)c_i = 0$ for $i = 1, \dots, r$. Since 1 is in $A$, it is also in $C$, so that it is generated by $c_1, \dots, c_r$, i.e there exist $a'_1, \dots, a'_r \in A$ such that $1 = a'_1 c_1 + \dots + a'_r c_r$. Multiplying this relation by $b^r + a_{r-1}b^{r-1} + \dots + a_1 b + a_0$, we deduce that $b^r + a_{r-1}b^{r-1} + \dots + a_1 b + a_0 = 0$, which proves that $b$ is integral over $A$. □

**Corollary 5.7.** *Let $A \subset B$ be rings. If $B$ is finite over $A$, then $B$ is integral over $A$. Moreover, if $B$ is finitely generated over $A$, then the converse is true, i.e. if $B$ is integral over $A$ then $B$ is finite over $A$.*

*Proof:* If $B$ is finite over $A$, then for any $b \in B$, we have that $A[b]$ is contained in the finite $A$-algebra $B$, and hence Proposition 5.6 implies that $b$ is integral over $B$. Therefore $B$ is integral over $A$.

Assume now that $B$ is a finitely generated $A$-algebra, i.e. $B = A[b_1, \dots, b_r]$ for some $b_1, \dots, b_r \in B$. Assume also that $B$ is integral over $A$. In particular, $b_1$ is integral over $A$, and by Proposition 5.6 $A[b_1]$ is a finite $A$-algebra. We observe now that, since $b_2$ is integral over $A$, it is trivially integral over $A[b_1]$. Again by Proposition 5.6, $A[b_1, b_2]$ is a finite $A[b_1]$-algebra. By Lemma 5.5, it follows that $A[b_1, b_2]$ is a finite $A$-algebra. Iterating the process, we obtain that $B = A[b_1, \dots, b_r]$ is a finite $A$-algebra, as wanted. □

**Corollary 5.8.** *Let $A \subset B$ be rings. Then the set of elements of $B$ that are integral over $A$ form a ring. As a consequence, a finitely generated extension $A \subset A[b_1, \dots, b_r]$ is integral if and only if $b_1, \dots, b_r$ are integral over $A$.*

*Proof:* If $b_1$ and $b_2$ are integral over $A$, then we repeat the same trick as in the second part of the proof of Corollary 5.7 and obtain that $A[b_1, b_2]$ is finite over $A$. Since $A[b_1 + b_2]$ and $A[b_1 b_2]$ are subalgebras of $A[b_1, b_2]$, then again by Proposition 5.6 we get that $b_1 + b_2$ and $b_1 b_2$ are integral over $A$. □

**Definition.** If $A \subset B$ are rings, the ring $A'$ of elements of $B$ integral over $A$ is called the *integral closure of $A$ in $B$*. If $A' = A$ we say that $A$ is *integrally closed in $B$*. A domain is called *integrally closed* or *normal* if it is integrally closed in its quotient field.

We have seen in Lemma 5.5 that the property of being finite is transitive. Since being finite is equivalent to be integral when dealing with finitely generated algebras, finiteness should also be transitive at least in this case. Since the finiteness of an element depends only on finitely many elements, this allows to prove the transitivity of the integral dependence general:

**Corollary 5.9.** *Let $A \subset B \subset C$ be rings:*

*(i) If $C$ is integral over $B$ and $B$ is integral over $A$, then $C$ is integral over $A$.*

*(ii) If $B$ is the integral closure of $A$ in $C$ then $B$ is integrally closed in $C$.*

*Proof:* To prove (i), take $c \in C$ any element of $C$ and let us prove that it is integral over $A$. Since $c$ is integral over $B$, there is a relation of the type $c^r + b_{r-1}c^{r-1} + \ldots + b_0 = 0$, with $b_0, \ldots, b_{r-1} \in B$. But this relation also shows that $c$ is integral over $A[b_0, \ldots, b_{r-1}]$. By Proposition 5.6, it follows that $A[b_0, \ldots, b_{r-1}][c]$ is a finite $A[b_0, \ldots, b_{r-1}]$-algebra. On the other hand, $A[b_0, \ldots, b_{r-1}]$ is contained in $B$, which is integral over $A$, hence it is also integral over $A$. Since it is a finitely generated $A$-algebra, by Corollary 5.7 we have that $A[b_0, \ldots, b_{r-1}]$ is finite over $A$. It follows from Lemma 5.5 that $A[b_1, \ldots, b_{r-1}][c]$ is finite over $A$. Since $A[c] \subset A[b_1, \ldots, b_{r-1}][c]$, Proposition 5.6 implies that $c$ is integral over $A$.

In order to prove (ii), we take $B'$ to be the integral closure of $B$ in $C$. Thus, $B'$ is integral over $B$ and $B$ is integral over $A$. Hence, by part (i) it follows that $B'$ is integral over $A$. This means that any element of $B'$ is integral over $A$, hence it belongs to $B$. Therefore $B' = B$, which means that $B$ is integrally closed in $C$. □

Let us see now how integral extensions behave under localizations and quotients.

**Lemma 5.10.** *Let $A \subset B$ be an integral extension and let $S$ be a multiplicative set of $A$ (and hence also a multiplicative set of $B$). Then the natural map $S^{-1}A \to S^{-1}B$ is an integral extension. In particular for any prime ideal $\mathfrak{p}$ of $A$, $B_{\mathfrak{p}}$ is integral over $A_{\mathfrak{p}}$.*

*Proof:* We remark first that the inclusion $A \subset B$ indices an inclusion $S^{-1}A \subset S^{-1}B$ by Proposition 4.8(ii). Consider now any element $\frac{b}{s} \in S^{-1}B$ and let us see that it is integral over $S^{-1}A$. Since $B$ is integral over $A$, there is a relation $b^n + a_{n-1}b^{n-1} + \ldots + a_1b_1 + a_0 = 0$, with $a_0, a_1 \ldots, a_{n-1} \in A$. From this we immediately obtain a relation $(\frac{b}{s})^n + \frac{a_{n-1}}{s}(\frac{b}{s})^{n-1} + \ldots + \frac{a_1}{s^{n-1}}\frac{b_1}{s} + \frac{a_0}{s^n} = 0$, which proves that $\frac{b}{s}$ is integral over $S^{-1}A$. □

**Lemma 5.11.** *Let $A$ be an integral domain with quotient field $K$. Then the following are equivalent:*

*(i) $A$ is integrally closed.*

*(ii) For any multiplicative set $S \subset A$, $S^{-1}A$ is integrally closed.*

*(iii) For any prime ideal $\mathfrak{p} \subset A$, $A_{\mathfrak{p}}$ is integrally closed.*

*(iv) For any maximal ideal $\mathfrak{m} \subset A$, $A_{\mathfrak{m}}$ is integrally closed.*

*Proof: (i)⇒(ii).* Take $\alpha \in K$ that is integral over $S^{-1}A$ (observe that the quotient field of $S^{-1}A$ is $K$). Then, taking a common denominator in the coefficients, we have a relation $\alpha^n + \frac{a_{n-1}}{s}\alpha^{n-1} + \ldots + \frac{a_1}{s}\alpha + \frac{a_0}{s} = 0$, with $a_i \in A$ and $s \in S$. Multiplying by $s^n$ we get a new relation $(s\alpha)^n + a_{n-1}(s\alpha)^{n-1} + \ldots + s^{n-2}a_1(s\alpha) + s^{n-1}a_0 = 0$, which shows that $s\alpha$ is integral over $A$. Since $A$ is integrally closed, is follows that $s\alpha$ is in $A$, and hence $\alpha$ is in $S^{-1}A$, as wanted.

*(ii)⇒(iii).* It is immediate, by taking $S = A \setminus \mathfrak{p}$.

*(iii)⇒(iv).* It is obvious.

*(iv)⇒(i).* Let $\alpha \in K$ be an element that is integral over $A$. In particular, $\alpha$ is integral over $A_{\mathfrak{m}}$, for any maximal ideal $\mathfrak{m} \subset A$. Since $A_{\mathfrak{m}}$ is integrally closed, it follows that $\alpha$ is in $A_{\mathfrak{m}}$ for any $\mathfrak{m}$. Hence by Proposition 4.14 $\alpha$ is in $A$. □

**Lemma 5.12.** *Let $A \subset B$ be an integral extension. If $I$ is an ideal of $B$, then $B/I$ is integral over $A/(I \cap A)$.*

*Proof:* First of all, observe that we have a natural inclusion $A/(I \cap A) \subset B/I$. Let $\bar{b} \in B/I$ be the class of $b \in B$ modulo $I$. Since $B$ is integral over $A$, there is a relation $b^r + a_{r-1}b^{r-1} + \ldots b_0 = 0$ in $B$, with $a_0, \ldots, a_{r-1} \in A$. Taking classes modulo $I$ we get that $\bar{b}^r + \bar{a}_{r-1}\bar{b}^{r-1} + \ldots \bar{b}_0 = 0$ is an integral dependence relation for $\bar{b}$ over $A/(I \cap A)$. □

**Lemma 5.13.** *Let $A \subset B$ be two integral domains, and assume that $B$ is integral over $A$. Then $A$ is a field if and only if $B$ is a field.*

*Proof:* Assume first that $A$ is a field and let us prove that $B$ is also a field. We thus take any $b \in B \setminus \{0\}$ and want to see that it has an inverse. Since $B$ is integral over $A$, there exists a relation $b^r + a_{r-1}b^{r-1} + \ldots + a_1 b + a_0 = 0$ for some $a_{r-1}, \ldots, a_1, a_0 \in A$. If we assume $r$ to be the minimum degree of such a relation, we have that $a_0 \neq 0$ (since otherwise $b^{r-1} + a_{r-1}b^{r-2} + \ldots + a_1$ would be zero because $B$ is an integral domain). We thus have that $a_0$ has an inverse and $-a_0^{-1}(b^{r-1} + a_{r-1}b^{r-2} + \ldots + a_1)$ is an inverse of $b$, proving that $B$ is a field (observe that for this implication we did not use strictly that $B$ was integral over $B$, since any algebraic relation, not necessarily monic would be enough to conclude).

Assume now that $B$ is a field. Given a nonzero element $a$ in $A$, we can find an inverse $a^{-1}$ of it at least in $B$, and we need to prove that this inverse is actually in $A$. For this, we write an integral dependence relation for $a^{-1}$ over $A$

$$(a^{-1})^r + a_{r-1}(a^{-1})^{r-1} + \ldots + a_1 a^{-1} + a_0 = 0$$

Multiplying it by $a^{r-1}$ we get a relation $a^{-1} = -a_{r-1} - \ldots - a_1 a^{r-2} - a_0 a^{r-1}$, which proves that $a^{-1}$ is in $A$. □

**Corollary 5.14** (Generalized weak Nullstellensatz)**.** *Let $\mathbb{K}$ be a field. Then for any maximal ideal $\mathfrak{m} \subset \mathbb{K}[X_1, \ldots, X_n]$ it follows that the field $\mathbb{K}[X_1, \ldots, X_n]/\mathfrak{m}$ is a finite extension of $\mathbb{K}$.*

*Proof:* As in the proof of Theorem 1.16, we use induction on $n$, the case $n = 1$ being trivial. Consider now a maximal ideal $\mathfrak{m} \subset \mathbb{K}[X_1, \ldots, X_n]$. It certainly contains a nonconstant polynomial $f$, and renaming the variables we can assume that it depends on the variable $X_1$. By Lemma 1.15(i) we can consider an isomorphism $\varphi : \mathbb{K}[X_1, \ldots, X_n] \cong \mathbb{K}[X_1, \ldots, X_n]$ assigning to any $g(X_1, \ldots, X_n)$ the polynomial $g(X_1 + X_n^m, X_2, \ldots, X_n)$ such that $\varphi(\mathfrak{m})$ is a maximal ideal containing a polynomial that is monic in the variable $X_n$. Since we have an isomorphism $\mathbb{K}[X_1, \ldots, X_n]/\mathfrak{m} \cong \mathbb{K}[X_1, \ldots, X_n]/\varphi(\mathfrak{m})$ preserving $\mathbb{K}$, we can assume $f$ is monic in $X_n$. We consider the intersection $\mathfrak{m}' = \mathfrak{m} \cap \mathbb{K}[X_1, \ldots, X_{n-1}]$. I claim that this is a maximal ideal of $\mathbb{K}[X_1, \ldots, X_{n-1}]$. Indeed, we observe first that the extension $\mathbb{K}[X_1, \ldots, X_{n-1}]/\mathfrak{m}' \subset \mathbb{K}[X_1, \ldots, X_n]/\mathfrak{m}$ is integral (the class of $f$ modulo $\mathfrak{m}$ defines an integral relation for the class of $X_n$). Hence Lemma 5.13 implies that $\mathbb{K}[X_1, \ldots, X_{n-1}]/\mathfrak{m}'$ is a field, i.e. $\mathfrak{m}'$ is a maximal ideal. By induction hypothesis, the field extension $\mathbb{K} \subset \mathbb{K}[X_1, \ldots, X_{n-1}]/\mathfrak{m}'$ is finite. Since the extension $\mathbb{K}[X_1, \ldots, X_{n-1}]/\mathfrak{m}' \subset \mathbb{K}[X_1, \ldots, X_n]/\mathfrak{m}$ is also finite, the result follows. □

**Remark 5.15.** In the above proof (and many others later on), the reader is allowed to assume that $\mathbb{K}$ is infinite and then use the part (ii) of Lemma 1.15 instead of part (i). This is probably more geometric and easy to understand, and in a first reading it should not be a tragedy to avoid finite fields.

**Remark 5.16.** Corollary 5.14 is just saying that maximal ideals in a polynomial ring behave as we have seen in Examples 0.6 and 0.7. Since the only finite extension of an algebraically closed field is the field itself, Corollary 5.14 implies that, for each $\mathfrak{m} \subset \mathbb{K}[X_1, \ldots, X_n]$, there is an isomorphism of $\mathbb{K}$-algebras $\mathbb{K}[X_1, \ldots, X_m]/\mathfrak{m} \cong \mathbb{K}$. If for $i = 1, \ldots, n$ we call $a_i$ to the image of the class of $X_i$ we have that the class of $X_i - a_i$ maps to zero, so that $X_i - a_i$ is in $\mathfrak{m}$. This implies that $\mathfrak{m}$ must be the ideal generated by

$(X_1 - a_1, \ldots, X_n - a_n)$, and we thus recover the weak Nullstellensatz (see Remark 1.18). In case $\mathbb{K}$ is not algebraically closed, Corollary 5.14 is saying something similar. Assume for a while that $\mathbb{K}$ is $\mathbb{R}$. Then it has only two finite extensions, namely $\mathbb{R}$ and $\mathbb{C}$. In case we have a maximal ideal $\mathfrak{m} \subset \mathbb{R}[X_1, \ldots, X_n]$ such that $\mathbb{R}[X_1, \ldots, X_m]/\mathfrak{m} \cong \mathbb{R}$, the above argument shows that $\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n)$ for some point $(a_1, \ldots, a_n) \in \mathbb{A}^n_{\mathbb{R}}$. If instead $\mathbb{R}[X_1, \ldots, X_m]/\mathfrak{m} \cong \mathbb{C}$, for each $j = 1, \ldots, n$ let $a_j + b_j i$ be the image by this isomorphism of the class of $X_j$. Then $\mathfrak{m}$ is an ideal whose zero locus in $\mathbb{A}^n_{\mathbb{R}}$ is empty, but vanishing in the two conjugate points $(a_1 \pm b_1 i, \ldots, a_n \pm b_n i)$. Similarly, for an arbitrary field $\mathbb{K}$, a maximal ideal $\mathfrak{m} \subset \mathbb{K}[X_1, \ldots, X_n]$ corresponds to a set of "conjugate" points whose coordinates are in a finite extension of $\mathbb{K}$. For instance, in characteristic zero (for which the primitive theorem holds) such a finite extension can be written as $\mathbb{K}[T]/(P)$, where $P$ is an irreducible polynomial of degree say $d$. Then $\mathfrak{m}$ represents $d$ points whose coordinates depend on the roots of $P$ and are somehow conjugate (in order to explain this better one should use Galois theory; in fact, the above description works completely well only for Galois extensions, which is the case for extensions of degree two).

# 6. Geometry on the spectrum of a ring

We come back here to our task of studying geometrical properties of the spectrum of a ring defined in section §1.

**Remark 6.1.** Observe that our definition of spectrum does not allow to distinguish for instance between the point $(0,0)$ of $\mathbb{A}^2_{\mathbb{K}}$ (given by the ring $\mathbb{K}[X,Y]/(X,Y) \cong \mathbb{K}$) and the same point with a tangent direction of Example 1.14 (given by the ring $\mathbb{K}[X,Y]/(X^2,Y) \cong \mathbb{K}[X]/(X^2)$). In fact, the spectra of both rings consist just of one point. The underlying reason is that the primes of $A/I$ are in bijection with the primes of $A$ containing $I$, these are exactly the primes containing $\sqrt{I}$ and hence they are in bijection with the set of primes of $A/\sqrt{I}$. Hence it is important to keep track of the ring rather than just the set of primes of it. A way of doing so is to define a morphism of spectra as a homomorphism of rings. For instance, a homomorphism of $\mathbb{K}$-algebras $\mathbb{K}[X_1,\ldots,X_n] \to \mathbb{K}$ is determined by the images $a_i$ of $X_i$ for $i = 1,\ldots,n$; this is the same as giving a point $(a_1,\ldots,a_n) \in \mathbb{A}^n_{\mathbb{K}}$. However, a homomorphism of $\mathbb{K}$-algebras $\mathbb{K}[X_1,\ldots,X_n] \to \mathbb{K}[X]/(X^2)$ is determined by the images $a_i + b_iX$ of $X_i$ for $i = 1,\ldots,n$; this is now equivalent to give a point $(a_1,\ldots,a_n) \in \mathbb{A}^n_{\mathbb{K}}$ and a tangent vector $(b_1,\ldots,b_n) \in \mathbb{K}^n$ (in fact, since we can get an automorphism of $\mathbb{K}[X]/(X^2)$ by multiplying the class of $X$ with a nonzero constant, we see that the vector is determined up to multiplication by a nonzero constant, hence we only have a direction rather than a vector, as suggested by Example 1.14).

This example shows that we need to take care of the ring $A$ defining $\mathrm{Spec}(A)$ and not just of the topological space. In fact, recall that we are considering the elements of $A$ as regular functions on $\mathrm{Spec}(A)$. The idea will be, as in differential geometry, to define a morphism in such a way that it sends regular functions to regular functions (under composition). More precisely:

**Definition.** A *morphism of spectra* is a pair $(\varphi,\varphi^*)$, where $\varphi : A \to B$ is a homomorphism of rings and $\varphi^* : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is defined by $\varphi^*(\mathfrak{q}) = \varphi^{-1}(\mathfrak{q})$.

**Lemma 6.2.** *Let $\varphi : A \to B$ be a ring homomorphism. Then for any ideal $I \subset A$, ${\varphi^*}^{-1}(V(I)) = V(<\varphi(I)>)$ (where $<\varphi(I)>$ is the ideal generated by $\varphi(I)$). In particular, $\varphi^*$ is a continuous map with the Zariski topology.*

*Proof:* To see that $\varphi^*$ is continuous it is enough to see that the inverse image of any closed set is a closed set. Hence we just need to prove the first part of the statement. The inverse image of $V(I)$ will consist of all prime ideals $\mathfrak{q} \subset B$ such that $\varphi^{-1}(\mathfrak{q}) \in V(I)$, i.e. $\varphi(I) \subset \mathfrak{q}$, or $<\varphi(I)> \subset \mathfrak{q}$. □

We see next that we can endow closed sets and basic open sets with a spectrum structure.

**Lemma 6.3.** *Let $A$ be a ring. Then:*

*(i) If $I$ is any ideal of $A$, the natural projection $\pi : A \to A/I$ induces a homeomorphism $\pi^* : \mathrm{Spec}(A/I) \to \mathrm{Spec}(A)$ onto its image $V(I)$.*

*(ii) If $S$ is a multiplicative set of $A$, then the natural map $\varphi_S : A \to S^{-1}A$ induces a homeomorphism $\varphi_S^* : \mathrm{Spec}(S^{-1}A) \to \mathrm{Spec}(A)$ onto its image $\Sigma_S = \{\mathfrak{p} \in \mathrm{Spec}(A) \mid \mathfrak{p} \cap S = \emptyset\}$ (with the induced topology). In particular:*

*a) If $\mathfrak{p}$ is a prime ideal of $A$, the natural map $\varphi_{\mathfrak{p}} : A \to A_{\mathfrak{p}}$ induces a homeomorphism $\varphi_{\mathfrak{p}}^* : \mathrm{Spec}(A_{\mathfrak{p}}) \to \mathrm{Spec}(A)$ onto its image $\Sigma_{\mathfrak{p}} := \{\mathfrak{p}' \in \mathrm{Spec}(A) \mid \mathfrak{p}' \subset \mathfrak{p}\}$.*

*b) If $f \in A$, the natural map $\varphi_f : A \to A_f$ induces a homeomorphism $\varphi_f^* : \mathrm{Spec}(A_f) \to \mathrm{Spec}(A)$ onto its image $D(f) = \{\mathfrak{p} \in \mathrm{Spec}(A) \mid f \notin \mathfrak{p}\}$.*

*(iii) If $\mathfrak{p}$ is a prime ideal of $A$, the inclusion $\{\mathfrak{p}\} \subset \mathrm{Spec}(A)$ is canonically represented by the natural homomorphism $A \to \mathbb{A}_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$.*

*Proof:* Properties (i) and (ii) are just the respective reinterpretations in terms of spectra of Exercise 1.4(v) and Proposition 4.9(v). For (iii), we observe that $\{\mathfrak{p}\} = V(\mathfrak{p}) \cap \Sigma_{\mathfrak{p}}$. By (ii), $\Sigma_{\mathfrak{p}}$ can be identified with $\mathrm{Spec}(A_{\mathfrak{p}})$ via $\varphi_{\mathfrak{p}}^*$. Hence $\{\mathfrak{p}\}$ is naturally identified with ${\varphi_{\mathfrak{p}}^*}^{-1}(V(\mathfrak{p}))$, and this is, by Lemma 6.2, $V(\mathfrak{p}A_{\mathfrak{p}}) \subset \mathrm{Spec}(A_{\mathfrak{p}})$. Now, (i) identifies this with $\mathrm{Spec}(A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}})$, as wanted. □

**Proposition 6.4.** *Let $i : A \to B$ an inclusion of rings and let $\mathfrak{p} \subset A$ be a prime ideal.*

*(i) If $i : A \to B$ is an inclusion of rings and $\mathfrak{p} \subset A$ is a prime ideal, then the restriction of $i^*$ to ${i^*}^{-1}(\Sigma_{\mathfrak{p}})$ is canonically identified with the map $\mathrm{Spec}(B_{\mathfrak{p}}) \to \mathrm{Spec}(A_{\mathfrak{p}})$ induced by the natural homomorphism $i_{\mathfrak{p}} : A_{\mathfrak{p}} \to B_{\mathfrak{p}}$ (regarding $S = A \setminus \mathfrak{p}$ as a multiplicative set of both $A$ and $B$).*

*(ii) If $i : A \to B$ is an inclusion of rings and $\mathfrak{p} \subset A$ is a prime ideal, then ${i^*}^{-1}(\mathfrak{p})$ is canonically identified with $\mathrm{Spec}(B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}})$.*

*Proof:* For (i), the image by $i^*$ of a prime $\mathfrak{q} \subset B$ lies in $\Sigma_{\mathfrak{p}}$ if and only if $\mathfrak{q} \cap A \subset \mathfrak{p}$, i.e. if and only if $\mathfrak{q} \cap (A \setminus \mathfrak{p}) = \emptyset$. By Lemma 6.3(ii) the set of those $\mathfrak{p}$ is canonically identified with $\mathrm{Spec}(B_{\mathfrak{p}})$, and hence (i) follows.

For (ii) it is enough to observe, as in the corresponding proof of Lemma 6.3, that $\{\mathfrak{p}\}$ is the intersection of $V(\mathfrak{p})$ and $\Sigma_{\mathfrak{p}}$, so that ${i^*}^{-1}(\mathfrak{p})$ can be identified with ${i^*}^{-1}(V(\mathfrak{p})) \cap {i^*}^{-1}(\Sigma_{\mathfrak{p}})$. By (i), ${i^*}^{-1}(\Sigma_{\mathfrak{p}})$ is identified with $\mathrm{Spec}(B_{\mathfrak{p}})$, and inside it, ${i^*}^{-1}(V(\mathfrak{p}))$ corresponds to ${i_{\mathfrak{p}}^*}^{-1}(V(\mathfrak{p}A_{\mathfrak{p}}))$. By Lemma 6.2, this is $V(\mathfrak{p}B_{\mathfrak{p}}) \subset \mathrm{Spec}(B_{\mathfrak{p}})$, and by Lemma 6.3(i) it is identified with $\mathrm{Spec}(B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}})$. □

**Example 6.5.** Consider the inclusion $i : \mathbb{K}[X] \subset \mathbb{K}[X,Y]/(Y^2 - X)$, as in Example 5.1. The map $i^* : \mathrm{Spec}(\mathbb{K}[X,Y]/(Y^2 - X)) \to \mathrm{Spec}(\mathbb{K}[X])$ corresponds to the projection

of the parabola $Y^2 = X$ onto the $X$-axis. For each $\lambda \in \mathbb{K}$, consider the ideal $\mathfrak{p}_\lambda = (X - \lambda)$ of $\mathbb{K}[X]$. According to Proposition 6.4(ii), the fiber of $\mathfrak{p}_\lambda$ by $i^*$ is identified with $\mathrm{Spec}((\frac{\mathbb{K}[X,Y]/(Y^2-X)}{(\overline{X-\lambda})})_{\mathfrak{p}_\lambda})$. In case $\mathbb{K}$ is algebraically closed, we have seen in Exercise 2.20 that the ideal $(\overline{X-\lambda})$ is either $(\overline{X-\lambda}, \overline{Y-\mu}) \cap (\overline{X-\lambda}, \overline{Y+\mu})$ (with $\lambda = \mu^2$) if $\lambda \neq 0$ or is $(\bar{X}, \bar{Y})$-primary if $\lambda = 0$. This shows that $\mathrm{Spec}(\frac{\mathbb{K}[X,Y]/(Y^2-X)}{(\overline{X-\lambda})})$ consists of two maximal ideals (corresponding to the points $(\lambda, \pm\mu)$) if $\lambda \neq 0$ or one maximal ideal (corresponding to the point $(0,0)$) if $\lambda = 0$. Since in neither case none of those ideal meet $\mathbb{K}[X] \setminus \mathfrak{p}_\lambda$, it follows that $\mathrm{Spec}((\frac{\mathbb{K}[X,Y]/(Y^2-X)}{(\overline{X-\lambda})})_{\mathfrak{p}_\lambda})$ coincides with $\mathrm{Spec}(\frac{\mathbb{K}[X,Y]/(Y^2-X)}{(\overline{X-\lambda})})$. If $\lambda \neq 0$ we get that the fiber consists of two points with multiplicity one. However, if $\lambda = 0$, the fiber is identified with $\mathrm{Spec}(\frac{\mathbb{K}[X,Y]/(Y^2-X)}{(\bar{X})}) \cong \mathrm{Spec}(\mathbb{K}[X,Y]/(X^2, Y))$, thus representing the point $(0,0)$ with multiplicity two.

The reason why we could avoid localizing at $\mathfrak{p}_\lambda$ in order to describe the fiber was that we were dealing with maximal ideals. In general we actually need to localize. If we take $\mathfrak{p} = (0)$ in $\mathrm{Spec}(\mathbb{K}[X])$, then clearly ${i^*}^{-1}(\{\mathfrak{p}\}) = (0)$. On the other hand, $\mathrm{Spec}((\mathbb{K}[X,Y]/(Y^2 - X))_{\mathfrak{p}})$, and this is identified with the set of prime ideals of $\mathbb{K}[X,Y]/(Y^2 - X)$ not meeting $\mathbb{K}[X] \setminus \{0\}$. It is precisely this last condition (which come from the fact that we are localizing at $\mathfrak{p}$) which implies that only $(0)$ satisfies that condition. Indeed, let $\mathfrak{q}$ be a nonzero prime ideal of $\mathbb{K}[X,Y]/(Y^2 - X)$. Then $\mathfrak{q}$ contains the class of some polynomial $g \in \mathbb{K}[X,Y]$. By performing the Euclidean division of $g$ between $Y^2 - X$ as polynomials in the variable $Y$, we can assume $g$ takes the form $g = f_0(X) + f_1(X)Y$. Multiplying $g$ by $f_0(X) - f_1(X)Y$, we get that $f_0(X)^2 - f_1(X)^2Y^2$ is in $\mathfrak{q}$, and hence also $f_0(X)^2 - f_1(X)^2X$ is in $\mathfrak{q}$. Since clearly $f_0(X)^2 - f_1(X)^2X$ cannot be the zero polynomial, we see that then $\mathfrak{q}$ meets necessarily $\mathbb{K}[X] \setminus \{0\}$.

We will see now how the result of Proposition 6.4(ii) can be improved for a general homomorphism of rings. We will need first some previous results.

**Exercise 6.6.** Let $B_1, B_2$ be two $A$-algebras. Prove that $B_1 \otimes_A B_2$ is an $A$-algebra (with the obvious internal product) satisfying the following universal property: There are homomorphisms $j_i : B_i \to B_1 \otimes_A B_2$ such that for any homomorphisms $\alpha_i : B_i \to C$ (where $C$ is another $A$-algebra) there exists a unique homomorphism $\varphi : B_1 \otimes_A B_2 \to C$ such that $\varphi \circ j_i = \alpha_i$ for $i = 1, 2$.

Considering spectra and recalling that the structure of $A$-algebra is equivalent to a homomorphism of rings $A \to B$ (see Remark 5.2), we get that the above exercise says that $\mathrm{Spec}(B_1 \otimes_A B_2)$ is the fibered product over $\mathrm{Spec}(A)$ of $\mathrm{Spec}(B_1)$ and $\mathrm{Spec}(B_2)$, according to the following definition:

**Definition.** Let $X_1, X_2, Y$ be objects in a category, with morphisms $f_1 : X_1 \to Y$ and $f_2 : X_2 \to Y$. The *fibered product* of $X_1$ and $X_2$ over $Y$ is another object $X$ having maps

$p_1 : X \to X_1$ and $p_2 : X \to X_2$ satisfying $f_1 \circ p_1 = f_2 \circ p_2$ with the following universal property: For any other object $Z$ in the same category with morphisms $q_1 : Z \to X_1$ and $q_2 : Z \to X_2$ such that $f_1 \circ q_1 = f_2 \circ q_2$ then there exists a unique morphism $g : Z \to X$ such that $q_i = p_1 \circ g$ for $i = 1, 2$.

The typical example is, when the category is the one of sets (and hence a morphism is just a map). In this case, the fibered product is the set of pairs $(x_1, x_2) \subset X_1 \times X_2$ having the same image in $Y$ under $f_1$ and $f_2$. If $Y$ consists of just one point, then the fibered product is nothing but the Cartesian product $X_1 \times X_2$.

**Remark 6.7.** We can now generalize Proposition 6.4(ii) for a general homomorphism $\varphi : A \to B$. Given $\mathfrak{p} \in \mathrm{Spec}(A)$, we have that the inclusion $\{\mathfrak{p}\} = V(\mathfrak{p}) \cap \Sigma_{\mathfrak{p}} \subset \mathrm{Spec}(A)$ can be identified, using (i) and (ii) with the map induced by the natural homomorphism $A \to A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} =$ quotient field of $A/\mathfrak{p}$. Since the fiber ${\varphi^*}^{-1}(\mathfrak{p})$ should be the fibered product of $\mathrm{Spec}(B)$ and $\{\mathfrak{p}\}$ over $\mathrm{Spec}(A)$, this is canonically identified with $\mathrm{Spec}\left(B \otimes_A (A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}})\right)$.

**Theorem 6.8.** *Let $A \subset B$ be an integral extension. Then the intersection map $i^* : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is surjective and moreover $i^*(\mathfrak{q})$ is a maximal ideal if and only if $\mathfrak{q}$ is a maximal ideal.*

*Proof:* Let us check first the last statement. If $\mathfrak{q}$ is a prime ideal of $B$, by Lemma 5.12 we have that $B/\mathfrak{q}$ is integral over $A/(\mathfrak{q} \cap A)$. Now Lemma 5.13 implies, since $B/\mathfrak{q}$ is a field if and only if $A/(\mathfrak{q} \cap A)$ is a field, i.e. that $\mathfrak{q}$ is a maximal ideal if and only if $i^*(\mathfrak{q})$ is a maximal ideal.

Take now any $\mathfrak{p} \in \mathrm{Spec}(A)$, and let us see that it is in the image of $i^*$. By Proposition 6.4(i) it is enough to see that the maximal ideal of $A_{\mathfrak{p}}$ is in the image of the map $j^* : \mathrm{Spec}(B_{\mathfrak{p}}) \to \mathrm{Spec}(A_{\mathfrak{p}})$ induced by $j : A_{\mathfrak{p}} \to B_{\mathfrak{p}}$. By Lemma 5.10, $j : A_{\mathfrak{p}} \to B_{\mathfrak{p}}$ is an integral extension, and hence from what we just proved $j^*$ takes maximal ideals into maximal ideals. Since $\mathrm{Spec}(A_{\mathfrak{p}})$ has only one maximal ideal, it is necessarily the image of any maximal ideal of $B_{\mathfrak{p}}$. □

**Theorem 6.9** (Going-up)**.** *Let $A \subset B$ be an integral extension, let $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1$ be prime ideals of $A$ and let $\mathfrak{q}_0$ be a prime ideal of $B$ such that $\mathfrak{q}_0 \cap A = \mathfrak{p}_0$. Then there exists a prime ideal $\mathfrak{q}_1 \supset \mathfrak{q}_0$ of $B$ such that $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$.*

*Proof:* By Lemma 5.12 $A/\mathfrak{p}_0 \subset B/\mathfrak{q}_0$ is an integral extension, and after the identifications of Lemma 6.3(i) we just need to check that $\mathfrak{p}_1/\mathfrak{p}_0$ in in the image of $\mathrm{Spec}(B/\mathfrak{q}_0) \to \mathrm{Spec}(A/\mathfrak{p}_0)$. But this is true by Theorem 6.8. □

The above theorem is saying that strict chains of primes in $A$ can be lifted to $B$. We can rephrase that in a more geometrical way, for which we need a previous definition.

**Definition.** The *Krull dimension of a ring* $A$ is the maximum length $r$ of a chain $\mathfrak{p}_0 \subsetneq / \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_r$ of prime ideals in $A$ (since we will not use any other definition of dimension we will just refer to this notios as the dimension of the ring).

**Corollary 6.10.** *If $A \subset B$ is an integral extension, then* $\dim A = \dim B$.

*Proof:* By Theorems 6.8 and 6.9, any chain $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_r$ of prime ideals in $A$ lifts to a chain $\mathfrak{q}_0 \subset \mathfrak{q}_1 \subset \ldots \subset \mathfrak{q}_r$ of prime ideals in $B$ such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for $i = 0, \ldots, r$. It is clear that this chain in $B$ is also strict, since $\mathfrak{p}_i \subsetneq \mathfrak{p}_{i+1}$ implies $\mathfrak{q}_i \subsetneq \mathfrak{q}_{i+1}$. This proves $\dim A \leq \dim B$.

For the other inequality, we consider now a chain $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \ldots \subsetneq \mathfrak{q}_r$ of prime ideals in $B$ and consider $\mathfrak{p}_i = \mathfrak{q}_i \cap A$ for $i = 0, \ldots, r$. We clearly have that $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_r$ is a chain of prime ideals in $A$, and it is enough to see that it is strict. For each $i = 1, \ldots, r$ we consider the natural map $A_{\mathfrak{p}_i} \to B_{\mathfrak{p}_i}$, which is an integral extension by Lemma 5.10. Thus by Theorem 6.8 the inverse image by $\mathrm{Spec}(B_{\mathfrak{p}_i}) \to \mathrm{Spec}(A_{\mathfrak{p}_i})$ of the maximal ideal consists only of maximal ideals. Therefore, since $\mathfrak{q}_{i-1}B_{\mathfrak{p}_i} \subsetneq \mathfrak{q}_i B_{\mathfrak{p}_i}$, it follows that the image of $\mathfrak{q}_{i-1}B_{\mathfrak{p}_i}$ is not $\mathfrak{p}_i A_{\mathfrak{p}_i}$. With the identification of Proposition 6.4(i), $\mathfrak{q}_{i-1} \cap A \neq \mathfrak{p}_i$, i.e. $\mathfrak{p}_{i-1} \subsetneq \mathfrak{p}_i$, as wanted. □

**Exercise 6.11.** Let $A$ be a ring.

(i) Prove that an integral domain is a field if and only if it has dimension zero.

(ii) Prove that, if $A$ is a PID, then $\dim A = 1$.

(iii) Prove that, if $\mathbb{K}$ is any field, then $\mathbb{K}[[X]]$ has dimension one.

(iv) Prove that $\dim(A[X]) \geq \dim A + 1$. If you feel self-confident, prove also that equality holds if $A$ is a P.I.D.

**Definition.** The *dimension of the spectrum* $\mathrm{Spec}(A)$ is the dimension of $A$; in other words (see Lemma 1.12), it is the maximum lenght of a strict chain of irreducible closed subsets of $\mathrm{Spec}(A)$. The *dimension of a closed set* $V(I) \subset \mathrm{Spec}(A)$ is the dimension of $\mathrm{Spec}(A/I)$ (see Lemma 6.3(i)), i.e. the dimension of $A/I$. The *dimension of an affine set* $X \subset \mathbb{A}^n$ is the dimension of $\mathrm{Spec}(\mathbb{K}[X_1, \ldots, X_n]/I(X))$, i.e. the dimension of $\mathbb{K}[X_1, \ldots, X_n]/I(X)$.

**Remark 6.12.** Observe that the dimension of $A/I$ is the maximum length of a chain $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_r$ of prime ideals containing $I$. Since a prime ideal contains an ideal $I$ if and only if it contains its radical $\sqrt{I}$, if follows that $\dim V(I) = \dim V(\sqrt{I})$, i.e. the dimension of a closed set is well defined, independently on the ideal defining it.

**Exercise 6.13.** Let $A$ be a ring and let $Z \subset \mathrm{Spec}(A)$ be an irreducible closed subset. Prove that the following are equivalent:

(i) $X$ has dimension zero .

(ii) $X$ consists of just one point.

(iii) $X = V(\mathfrak{m})$ for some maximal ideal $\mathfrak{m} \subset A$.

As we have seen in Corollary 6.10, the dimension of a subring is related with the dimension of the ambient ring only in the case of an integral extension. It is not even true that the dimension of a subring is at most the dimension of the ambient ring (think of any integral domain of arbitrary dimension inside its quotient field). In fact, the right notion of "smaller" ring is not subring, but quotient ring, as the following result shows.

**Lemma 6.14.** *Let $A$ be a ring.*

*(i) For any ideal $I \subset A$, $\dim V(I) \leq \dim A$.*

*(ii) If there is an epimorphism $\varphi : A \to B$, then $\dim A \geq \dim B$.*

*(iii) For any two ideals $I \subset J$ of $A$ it holds $\dim V(J) \leq \dim V(I)$.*

*(iv) If $I \subsetneq J$ are two ideal and $I$ is prime, then $\dim V(J) < \dim V(I)$.*

*Proof:* Property (i) follows immediately from the bijection between the set of prime ideals of $A/I$ and the prime ideals of $A$ containing $I$. Property (ii) comes from (i), since $B$ is isomorphic to $A/\ker\varphi$. Property (iii) follows from (ii), using the natural epimorphism $A/I \to A/J$. Finally, property (iv) is a consequence of the fact that any chain of primes $\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_r$ containing $J$ can be extended to the chain of primes $I \subsetneq \mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_r$ containing $I$. □

**Proposition 6.15.** *Let $A$ be a ring and let $I \subset A$ be an ideal having a primary decomposition $I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_r$. Then the dimension of $V(I)$ is the maximum of the dimensions of $V(\mathfrak{q}_1), \ldots, V(\mathfrak{q}_r)$ (i.e. it is the maximum of the dimensions of its irreducible components).*

*Proof:* From Lemma 6.14 we get $\dim V(I) \geq \dim V(\mathfrak{q}_i)$ for all $i = 1, \ldots, r$. We thus need to show that we have equality for some $i$. If we set $s = \dim A$, we have some chain $\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_s$ of prime ideals of $A$ containing $I$. Hence $\mathfrak{p}_0 \supset (0) = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_r$, and by Lemma 1.1, $\mathfrak{p}_0$ must contain some $\mathfrak{q}_i$. We thus get a chain $\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_s$ of prime ideals containing $\mathfrak{q}_i$, which proves that $\dim V(\mathfrak{q}_i) \geq s$. Since we already proved the converse inequality, we get in fact an equality, which finishes the proof. □

Let $\mathfrak{p}$ be a prime ideal of a ring $A$. Since the dimension of $V(\mathfrak{p})$ is the maximum length of a strict chain of irreducible closed sets of $\mathrm{Spec}(A)$ contained in $V(\mathfrak{p})$, it looks natural to define the codimension of $V(\mathfrak{p})$ as the maximum length of a strict chain of irreducible closed sets of $\mathrm{Spec}(A)$ containing $V(P)$. In algebraic terms, the corresponding definition is:

**Definition.** If $A$ is a ring, the *height of a prime ideal* $\mathfrak{p}$ (denoted by $\operatorname{ht}\mathfrak{p}$) is the maximal length $r$ of a chain $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_r$ of prime ideals contained in $\mathfrak{p}$. By Proposition 4.9(v), it holds $\operatorname{ht}\mathfrak{p} = \dim(A_{\mathfrak{p}})$.

The height of a prime ideal does not always coincide with the codimension of the corresponding irreducible set, as the second part of the following exercise shows:

**Exercise 6.16.** Let $A$ be a ring.

(i) For any prime ideal $\mathfrak{p}$, prove the inequality $\operatorname{ht}\mathfrak{p} \leq \dim A - \dim V(\mathfrak{p})$.

(ii) Prove that, if $A = \mathbb{K}[[X]][Y]$ and $\mathfrak{p} = (XY - 1)$, the above inequality is strict.

(iii) If $A$ is a U.F.D., prove that the prime ideals of height one are precisely the ideals generated by an irreducible element.

**Definition.** A ring is called *catenary* if $\dim A = \dim V(\mathfrak{p}) + \operatorname{ht}\mathfrak{p}$ for any prime ideal $\mathfrak{p} \subset A$.

In the geometric case, everything works fine:

**Theorem 6.17.** *If $A$ is an integral finitely generated $\mathbb{K}$-algebra, then $A$ is catenary.*

*Proof:* We write $A = \mathbb{K}[X_1, \ldots, X_n]/I$ and prove the result by induction on $n$, the case $n = 0$ being trivial. We thus assume $n > 0$ and take a prime ideal $\mathfrak{p}/I$ of $A$. If it is zero there is nothing to prove, so we assume $I \subsetneq \mathfrak{p}$, so that we can take $f \in \mathfrak{p}$ not in $I$. By Lemma 1.15 (see Remark 5.15), we can assume $f$ is monic in the indeterminate $X_n$. Set $\dim A/I = m + 1$, so that there exists a chain of prime ideals

$$\{0\} \subsetneq \mathfrak{p}_0/I \subsetneq \mathfrak{p}_1/I \subsetneq \ldots \subsetneq \mathfrak{p}_m/I.$$

If we call $\mathfrak{p}_0' = \mathfrak{p}_0 \cap \mathbb{K}[X_1, \ldots, X_{n-1}]$, the fact that $\mathfrak{p}_0$ contains a monic polynomial in $X_n$ implies that the extension $\mathbb{K}[X_1, \ldots, X_{n-1}]/\mathfrak{p}_0' \subset \mathbb{K}[X_1, \ldots, X_n]/\mathfrak{p}_0$ is integral, and hence both rings have the same dimension, which is clearly $m$. By induction hypothesis $\mathbb{K}[X_1, \ldots, X_{n-1}]/\mathfrak{p}_0'$ is catenary, so that if we define $\mathfrak{p}' = \mathfrak{p} \cap \mathbb{K}[X_1, \ldots, X_n]$ (and thus clearly $\mathfrak{p}_0' \subset \mathfrak{p}'$) we have that

$$m = \dim\big((\mathbb{K}[X_1, \ldots, X_{n-1}]/\mathfrak{p}_0')/(\mathfrak{p}'/\mathfrak{p}_0')\big) + \operatorname{ht}(\mathfrak{p}'/\mathfrak{p}_0').$$

Observe first that $(\mathbb{K}[X_1, \ldots, X_{n-1}]/\mathfrak{p}_0')/(\mathfrak{p}'/\mathfrak{p}_0')$ is isomorphic to $\mathbb{K}[X_1, \ldots, X_{n-1}]/\mathfrak{p}'$ and that the extension $\mathbb{K}[X_1, \ldots, X_{n-1}]/\mathfrak{p}' \subset \mathbb{K}[X_1, \ldots, X_n]/\mathfrak{p}$ is integral (again because $\mathfrak{p}$ contains $f$), so that $(\mathbb{K}[X_1, \ldots, X_{n-1}]/\mathfrak{p}_0')/(\mathfrak{p}'/\mathfrak{p}_0')$ has the same dimension as $\mathbb{K}[X_1, \ldots, X_n]/\mathfrak{p}$, say $r$, which is also the dimension of $(\mathbb{K}[X_1, \ldots, X_n]/I)/(\mathfrak{p}/I)$. Hence $\operatorname{ht}(\mathfrak{p}'/\mathfrak{p}_0') = m - r$, and therefore we have a chain of prime ideals

$$\mathfrak{p}_0'/\mathfrak{p}_0' \subsetneq \mathfrak{p}_1'/\mathfrak{p}_0' \subsetneq \ldots \subsetneq \mathfrak{p}_{m-r}'/\mathfrak{p}_0' = \mathfrak{p}'/\mathfrak{p}_0'$$

in $\mathbb{K}[X_1, \ldots, X_{n-1}]/\mathfrak{p}_0'$, which by the going-up theorem lifts to a chain of prime ideals

$$\mathfrak{p}_0/\mathfrak{p}_0 \subsetneq \mathfrak{p}_1/\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_{m-r}/\mathfrak{p}_0 = \mathfrak{p}/\mathfrak{p}_0$$

in $\mathbb{K}[X_1, \ldots, X_n]/\mathfrak{p}_0$. Recalling that $\mathfrak{p}_0/I$ had height one, this yields a chain of prime ideals

$$\{0\} \subsetneq \mathfrak{p}_0/I \subsetneq \mathfrak{p}_1/I \subsetneq \ldots \subsetneq \mathfrak{p}_{m-r}/I = \mathfrak{p}/I$$

in $A$, proving that $\mathfrak{p}/I$ has height at least $m+1-r = \dim A - \dim(A/(\mathfrak{p}/I))$. By Exercise 6.16(i), this completes the proof. □

From this we immediately deduce the following (we will give a second proof, in case the reader decided to skip the above result):

**Proposition 6.18.** *If $\mathbb{K}$ is a field, the Krull dimension of $\mathbb{K}[X_1, \ldots, X_n]$ is $n$. Hence $\mathbb{A}^n_{\mathbb{K}}$ has dimension $n$.*

*Proof 1:* We prove it by induction on $n$, the cases $n = 0, 1$ being a consequence of Exercise 6.11(i),(ii). We consider the prime ideal $\mathfrak{p} = (X_n)$, which has height one (Exercise 6.16(iii)). Since $\mathbb{K}[X_1, \ldots, X_n]$ is catenary by Theorem 6.17, it follows that $\dim \mathbb{K}[X_1, \ldots, X_n] = \dim \mathbb{K}[X_1, \ldots, X_n]/(X_n) + 1$. Since $\mathbb{K}[X_1, \ldots, X_n]/(X_n) \cong \mathbb{K}[X_1, \ldots, X_{n-1}]$, it has dimension $n-1$ by induction hypothesis. This implies the result.

*Proof 2:* Since there is a chain $(0) \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq \ldots \subsetneq (X_1, X_2, \ldots, X_n)$, it follows that the Krull dimension of $\mathbb{K}[X_1, \ldots, X_n]$ is at least $n$. We thus need to prove that any other chain of prime ideals has length at most $n$. We will prove it by induction on $n$. If $n = 1$ the result is trivial.

Assume that $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_r$ is a chain of prime ideals. We can also assume that it is saturated, i.e. that it is impossible to add new primes to the chain. In particular, $\mathfrak{p}_0$ must be the zero ideal. Let $f$ be a nonzero element of $\mathfrak{p}_1$. Since $\mathfrak{p}_1$ is prime, some of the irreducible factors of $f$ must be in $\mathfrak{p}_1$. In other words, we can assume that $f$ is irreducible. We thus have inclusions $0 = \mathfrak{p}_0 \subsetneq (f) \subset \mathfrak{p}_1$. Since $(f)$ is a prime ideal and the above chain was saturated, it follows that $\mathfrak{p}_1 = (f)$. By Lemma 1.15 (see Remark 5.15) we can also assume that $f$ is monic in the variable $X_n$. This means that $\mathbb{K}[X_1, \ldots, X_n]/(f)$ in integral over $\mathbb{K}[X_1, \ldots, X_{n-1}]$, and by Corollary 6.10 and the induction hypothesis it follows that $\dim \mathbb{K}[X_1, \ldots, X_n]/(f) = n-1$. But $0 = \mathfrak{p}_1/(f) \subsetneq \mathfrak{p}_2/(f) \subsetneq \ldots \subsetneq \mathfrak{p}_r/(f)$ is a chain of prime ideals in $\mathbb{K}[X_1, \ldots, X_n]/(f)$ of length $r-1$, and therefore $r-1 \leq n-1$, as wanted. □

**Theorem 6.19** (Noether's normalization lemma)**.** *Let $A$ be a finitely generated algebra over a field $\mathbb{K}$. Then there exist $\alpha_1, \ldots, \alpha_r \in A$ algebraically independent over $\mathbb{K}$ such that the extension $\mathbb{K}[\alpha_1, \ldots, \alpha_r] \subset A$ is integral.*

*Proof:* We will use induction on the number of generators of $A$ as a $\mathbb{K}$-algebra. If $A$ is generated by only one element $a$, then either $a$ is algebraically independent over $\mathbb{K}$ (and hence there is nothing to prove) or it vanishes at a non-trivial polynomial $f \in \mathbb{K}[T]$. In this last case we can assume that $f$ is monic (by just multiplying by the inverse of its leading coefficient), and hence $A$ is integral over $\mathbb{K}$.

Assume now that $A$ is generated by $a_1, \ldots, a_n$, and $n > 1$. As before, if $a_1, \ldots, a_n$ are algebraically independent over $\mathbb{K}$, there is nothing to prove. Otherwise, there would be a non-trivial polynomial $f \in \mathbb{K}[X_1, \ldots, X_n]$ such that $f(a_1, \ldots, a_n) = 0$. In this case, Lemma 1.15 (see Remark 5.15) allows us (after maybe reordering $a_1, \ldots, a_n$) to choose new generators $a_1' = a_1 + a_n^m, a_2' = a_2 \ldots, , a_n' = a_n$ (with $\lambda_1, \ldots, \lambda_{n-1} \in \mathbb{K}$) such that $a_n'$ (and hence $A$) is integral over $\mathbb{K}[a_1', \ldots, a_{n-1}']$. By induction hypothesis, we can find $\alpha_1, \ldots, \alpha_r \in \mathbb{K}[a_1', \ldots, a_{n-1}']$ algebraically independent over $\mathbb{K}$ and such that $\mathbb{K}[a_1', \ldots, a_{n-1}']$ is integral over $\mathbb{K}[\alpha_1, \ldots, \alpha_r]$. By the transitivity of the integral dependence (Lemma 5.9), it follows that $A$ is integral over $\mathbb{K}[\alpha_1, \ldots, \alpha_r]$, as wanted. □

**Exercise 6.20.** Use Noether's normalization lemma and Lemma 5.13 to give another proof of the generalized Nullstellensatz (Corollary 5.14).

**Corollary 6.21.** *If $\mathbb{K}$ is a field, the Krull dimension of a finitely generated $\mathbb{K}$-algebra $A$ that is a domain is the transcendence degree of its quotient field over $\mathbb{K}$.*

*Proof:* By Theorem 6.19, $A$ is an integral extension of a polynomial ring $\mathbb{K}[X_1, \ldots, X_r]$. By Corollary 6.10, the Krull dimension of $A$ is the one of $\mathbb{K}[X_1, \ldots, X_r]$, which is $r$ (by Proposition 6.18). On the other hand, by taking quotient fields (since $A$ is an integral domain), it follows that the quotient field of $A$ is a finite extension of the quotient field of $\mathbb{K}[X_1, \ldots, X_r]$. Hence both fields have the same transcendence degree over $\mathbb{K}$, which is $r$. This proves the result. □

**Remark 6.22.** The ideas in the last proofs suggests a geometric interpretation of ring homomorphisms. Any ring homomorphism $f : A \to B$ can be factored canonically as $A \to A/\ker f \cong \operatorname{Im} f \hookrightarrow B$. As we have seen in Lemma 6.3(i), the epimorphism $A \to A/\ker f$ corresponds to the inclusion $V(\ker f) \subset \operatorname{Spec}(A)$, so that we have factorized our map $f^* : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ through $V(\ker f) \subset \operatorname{Im} f^*$. We just need to interpret what the map between spectra means for a monomorphism of rings. We have already seen that if $f$ is injective it does not imply that $f^* \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is surjective (see for instance Example 5.3). The idea is that instead we have that the image is a dense subset. The reader can think that this is a crazy idea, since we can consider the inclusion of $\mathbb{K}[X_1, \ldots, X_n]$ in its quotient field $\mathbb{K}(X_1, \ldots, X_n)$ and the image of

$\mathrm{Spec}\left(\mathbb{K}(X_1,\ldots,X_n)\right) \to \mathrm{Spec}(\mathbb{K}[X_1,\ldots,X_n])$ is just the ideal (0). However, in the Zariski topology, the closure of (0) is the whole $\mathrm{Spec}(\mathbb{K}[X_1,\ldots,X_n])$. But let us check our claim about density in a more geometric context.

Assume we have an inclusion $A = \mathbb{K}[X_1,\ldots,X_n]/I \to \mathbb{K}[Y_1,\ldots,Y_m]/J = B$ of $\mathbb{K}$-algebras. For simplicity, we will assume that $I$ and $J$ are prime ideals (i.e. we are dealing with irreducible sets), and we can also assume (by including the classes of $X_1,\ldots,X_n$ among the generators of $B$) that $B$ has the form $\mathbb{K}[X_1,\ldots,X_m]/J$ with $m \geq n$. On the other hand, we can assume that the variables $X_{n+1},\ldots,X_m$ are ordered in such a way that the classes of the first ones $X_{n+1},\ldots,X_p$ are algebraically independent over $A$ and the rest are algebraic. We now consider the factorization $\mathrm{Spec}(B) \to \mathrm{Spec}(A[X_{n+1},\ldots,X_p]) \to \mathrm{Spec}(A)$. Since the map $\mathrm{Spec}\, A[X_{n+1},\ldots,X_p] \to \mathrm{Spec}\, A$ is clearly surjective (in fact for any ring $A$), we can assume that $X_{n+1},\ldots,X_m$ are algebraic over $A$.

Let $f_{n+1},\ldots,f_m \in A[T]$ be nonzero polynomials vanishing respectively on $X_{n+1},\ldots,X_m$. Let $g_{n+1},\ldots,g_m \in A$ be respectively the leading coefficients of $f_{n+1},\ldots,f_m$. Then the localization $B_{f_{n+1}\ldots f_m}$ is integral over $A_{f_{n+1}\ldots f_m}$. Therefore the map $\mathrm{Spec}(B_{f_{n+1}\ldots f_m}) \to \mathrm{Spec}(A_{f_{n+1}\ldots f_m})$ is surjective. In other words, the open set $\mathrm{Spec}(A) \setminus V(f_{n+1}\ldots f_m)$ is in the image of $f^*$.

We compute now the dimension of the ring of formal series. The main idea is to treat series as polynomials, and the main tool in this direction is the following:

**Theorem 6.23** (Weierstrass preparation theorem)**.** *Let $f \in \mathbb{K}[[X_1,\ldots,X_n]]$ of order $d$ and assume that its homogeneous part of degree $d$ is monic in the variable $X_n$. Then there exist unique factorization $f = uP$ such that $u \in \mathbb{K}[[X_1,\ldots,X_n]]$ is a unit and $P = X_n^d + a_{d-1}X_n^{d-1} + \ldots + a_1X^n + a_0$ with $a_0,\ldots,a_{d-1} \in \mathbb{K}[[X_1,\ldots,X_{n-1}]]$.*

*Proof:* Write $f = f_d + f_{d+1} + f_{d+2} + \ldots$ for the decomposition of $f$ into its homogeneous summands, and the same for the wanted $u$ and $P$. It is clear that it should be $u = 1 + u_1 + u_2 + \ldots$ and $P = f_d + P_{d+1} + P_{d+2} + \ldots$, and for $i = 1, 2, \ldots$ each $P_{d+i}$ has degree at most $d-1$ in $X_n$. From the required equality $f_{d+1} = u_1 f_d + P_{d+1}$ it is clear that $u_1$ and $P_{d+1}$ have to be necessarily the quotient and remainder respectively of the Euclidean division of $f_{d+1}$ between $f_d$, viewed as a monic polynomial in $X_n$ of degree $d$. Similarly, from the equality $f_{d+2} - u_1 P_{d+1} = u_2 f_d + P_{d+2}$ we see that this is again the division of $f_{d+2} - u_1 P_{d+1}$ between $f_d$. Iterating this process, we can (and should) construct inductively the pairs $(u_i, P_{d+i})$ as quotients and remainders of suitable Euclidean divisions between $f_d$, proving the statement. □

**Corollary 6.24.** *If $\mathbb{K}$ is a field, $\mathbb{K}[[X_1,\ldots,X_n]]$ is a UFD.*

*Proof:* We do it by induction on $n$, the case $n = 0$ being trivial. Assume we have two different factorizations $f_1 \dots f_r = g_1 \dots g_s$ into irreducible series. Applying simultaneously Lemma 1.15 (see Remark 5.15) to the initial form of $f_1 \dots f_r = g_1 \dots g_s$, we can assume that $f_1, \dots, f_r, g_1, \dots, g_s$ have initial forms monic in $X_n$, and by Theorem 6.23 we can thus assume that $f_1, \dots, f_r, g_1, \dots, g_s$ are polynomials in the variable $X_n$. By induction hypothesis, we know that $\mathbb{K}[[X_1, \dots, X_{n-1}]]$ is a UFD, and hence so is $\mathbb{K}[[X_1, \dots, X_{n-1}]][X_n]$. On the other hand, it is obvious that $f_1, \dots, f_r, g_1, \dots, g_s$ are still irreducible as elements in $\mathbb{K}[[X_1, \dots, X_{n-1}]][X_n]$. Hence $f_1, \dots, f_r$ and $g_1, \dots, g_s$ are the same up to a permutation and multiplication by a unit of $\mathbb{K}[[X_1, \dots, X_{n-1}]][X_n]$ (which is obviously a unit as a series in $\mathbb{K}[[X_1, \dots, X_{n-1}, X_n]]$). This proves the corollary. □

**Proposition 6.25.** *If $\mathbb{K}$ is a field, the Krull dimension of $\mathbb{K}[[X_1, \dots, X_n]]$ is $n$.*

*Proof:* We have the chain $(0) \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq \dots \subsetneq (X_1, X_2, \dots, X_n)$, which implies that the Krull dimension of $\mathbb{K}[X_1, \dots, X_n]$ is at least $n$. We prove by induction on $n$ that it cannot exceed $n$. If $n = 0$ this is trivial the case $n = 1$ follows also immediately from Exercise 2.7(ii)). Assume now $n \geq 1$ and suppose we have a chain $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_r$ of primes in $\mathbb{K}[[X_1, \dots, X_n]]$. We need to prove $r \leq n$. We can assume the chain is maximal. This implies that $\mathfrak{p}_0$ is zero. Let us see that $\mathfrak{p}_1$ is principal. Take a nonzero element $f$ of $\mathfrak{p}_1$. Since one of its irreducible components must be in $\mathfrak{p}_1$, we can assume $f$ is irreducible, and therefore $\mathfrak{p}_1 = (f)$ by the maximality of the chain (observe that all this makes sense only because $\mathbb{K}[[X_1, \dots, X_n]]$ is a UFD after Corollary 6.24). We have thus a chain of primes $0 = \mathfrak{p}_1/(f) \subsetneq \mathfrak{p}_2/(f) \subsetneq \dots \subsetneq \mathfrak{p}_r/(f)$ in $\mathbb{K}[[X_1, \dots, X_n]]/(f)$, so it is enough to prove that $\mathbb{K}[[X_1, \dots, X_n]]/(f)$ has dimension $n - 1$. For this, we first use Lemma 1.15 (see Remark 5.15) to assume that the initial form of $f$ is monic in $X_n$, and then Theorem 6.23 to assume that $f$ is a monic polynomial in the variable $X_n$. Then, the fact that $\mathbb{K}[[X_1, \dots, X_n]]/(f)$ has dimension $n-1$ is immediate from Corollary 6.10, since $\mathbb{K}[[X_1, \dots, X_n]]/(f)$ is integral over $\mathbb{K}[[X_1, \dots, X_{n-1}]]$, which has dimension $n - 1$ by induction hypothesis.

# 7. Local rings

**Example 7.1.** It is well-known from the theory of plane curves that a plane curve defined by a (reduced) polynomial $f \in \mathbb{K}[X,Y]$ is nonsingular at $(0,0)$ if and only if the degree-one part of $f$ is nonzero (and of course the degree-zero part must be zero); moreover, this degree-one part is precisely the equation for the tangent line at $(0,0)$. We want to describe these properties in a purely algebraic way. To give a concrete example, take $f = X - 2Y + X^2 - XY + Y^3$. Then $C = V(f)$ is nonsingular at $(0,0)$ and its tangent line is $X - 2Y = 0$. Let us consider $\mathfrak{m} = (X,Y)$ i.e. the maximal ideal corresponding to $(0,0)$. The fact that $(0,0)$ belongs to $C$ is given by the fact that $f$ is in $\mathfrak{m}$. A way of getting the equation of the tangent line is to remove from $f$ all the terms of degree at least two, i.e. in $\mathfrak{m}^2$. Hence we can represent this tangent equation as the class of $f$ in $\mathfrak{m}/\mathfrak{m}^2$.

On the other hand, the smoothness of $C$ at $(0,0)$ is interpreted, in terms of analysis, by the fact that one of the variables $X, Y$ can be expressed locally as a function of the other. This can be interpreted in an algebraic way as follows. First, we work on the ring of polynomial functions on $C$, which is $\mathbb{K}[X,Y]/(f)$. In our concrete example, we have the equality $\bar{X}(\overline{1+X-Y}) = \bar{Y}(\overline{2-Y^2})$ (where as usual a bar means class modulo the ideal $(f)$). In order to express, for instance, to express $\bar{X}$ in terms of $\bar{Y}$ we would need $\overline{1+X-Y}$ to be a unit. Since $1+X-Y$ does not vanish at zero, it would suffice to localize $\mathbb{K}[X,Y]/(f)$ in the maximal ideal $\bar{\mathfrak{m}} = (\bar{X}, \bar{Y})$. Eventually, we get that the maximal ideal of $\big(\mathbb{K}[X,Y]/(f)\big)_{\bar{\mathfrak{m}}}$ is generated by just one element, for instance $\bar{Y}$.

In this way, any element of $\big(\mathbb{K}[X,Y]/(f)\big)_{\bar{\mathfrak{m}}}$ (which can be interpreted as a local function on $C$ around $(0,0)$), should be expressible in terms of $X$, and the order of vanishing at $(0,0)$ will be the number of times it is divisible by $Y$. To continue with a concrete example, take the local function $\frac{X-2Y}{1+X-Y}$. The first observation is that $\frac{1}{1+X-Y}$ does not vanish at $(0,0)$, so that its order of vanishing is zero. Hence we just need to find the order of vanishing of the numerator $X - 2Y$. Making the substitution $\bar{X} = \bar{Y}\frac{\overline{2-Y^2}}{\overline{1+X-Y}}$ we get the equality $\overline{X-2Y} = \frac{\overline{-Y^3-2XY+2Y^2}}{\overline{1+X-Y}}$. We thus need to compute the order of vanishing of $\overline{-Y^3-2XY+2Y^2}$, which in turn equals (performing again the same substitution) $\bar{Y}^2\frac{\overline{-2+2X-3Y-XY+3Y^2}}{\overline{1+X-Y}}$. Since the function on the right does not vanish at $(0,0)$, it eventually follows that the order of vanishing is exactly two.

Our goal in this section will be to translate all these ideas to a general algebraic context.

**Definition.** Let $X \subset \mathbb{A}^n_{\mathbb{K}}$ be an affine set containing $a = (a_1, \ldots, a_n)$. Then the tangent space of $X$ at $a$ is defined as the linear space $T_aX \subset \mathbb{A}^n_{\mathbb{K}}$ defined by the equations $\frac{\partial f}{\partial X_1}(a)(X_1 - a_1) + \ldots + \frac{\partial f}{\partial X_n}(a)(X_1 - a_n) = 0$, when $f$ varies in $I(X)$. It is a simple exercise

to see that it is enough to let $f$ vary in a set of generators (which of course we can take to be finite).

Observe that, if $a = (0, \ldots, 0)$ (which can always be obtained with just a translation), the linear equation for $T_a X$ produced by an element $f \in I(X)$ is nothing but the linear part of $f$ (observe that $f$ has not constant term, since it vanishes at the origin). Taking that linear part is the same as taking the class of $f$ modulo $(X_1, \ldots, X_n)^2$. This is the underlying idea of the following result.

**Proposition 7.2.** *Let $X \subset \mathbb{A}^n_{\mathbb{K}}$ be an affine set containing $O = (0, \ldots, 0)$, let $\mathcal{O}_{X,O}$ be the local ring of $X$ at the point $O$ and let $\mathfrak{m}$ be the maximal ideal of $\mathcal{O}_{X,O}$. Then the dimension of the Zariski tangent space of $X$ at $O$ is the dimension of $\mathfrak{m}/\mathfrak{m}^2$ as a $\mathbb{K}$-vector space.*

*Proof:* The vector space $\mathfrak{m}/\mathfrak{m}^2$ is generated by the classes modulo $\mathfrak{m}^2$ of $\bar{X}_1 \ldots, \bar{X}_n$ (where a bar indicates the class of a polynomial modulo $I(X)$. If its dimension is $r$, we can assume, after reordering the variables, that the classes of $\bar{X}_1 \ldots, \bar{X}_r$ modulo $\mathfrak{m}^2$ form a basis of $\mathfrak{m}/\mathfrak{m}^2$. In particular, for each $i = r+1, \ldots, n$, the class of $\bar{X}_i$ can be written as

$$\bar{X}_i = a_{i1}\bar{X}_1 + \ldots + a_{ir}\bar{X}_r + \bar{q}_i$$

with $a_{ij} \in \mathbb{K}$ and $\bar{q}_i \in \mathfrak{m}^2 \subset \big(\mathbb{K}[X_1, \ldots, X_n]/I(X)\big)_{(\bar{X}_1 \ldots, \bar{X}_n)}$. In order to eliminate denominators, we write each $\bar{q}_i$ as $\bar{q}_i = \frac{\bar{g}_i}{\bar{s}_i}$, with $g_i \in (\bar{X}_1 \ldots, \bar{X}_n)^2$ and $s_i \notin (X_1 \ldots, X_n)$ (i.e. $s_i(0, \ldots, 0) \neq 0$). Therefore, the above equality implies that, for $i = r+1, \ldots, n$, there exists $f_i \in I(X)$ of the form

$$f_i = a_{i1}s_iX_i + \ldots + a_{ir}s_iX_r - s_iX_i + g_i$$

Since $s_i(0, \ldots, 0) \neq 0$, this means that the linear part of $f_i$ takes the form $b_{i1}X_1 + \ldots b_{ir}X_r + c_iX_i$, with $c_i \neq 0$. Hence we find $n - r$ linearly independent linear forms in the tangent space of $X$ at $O$, which shows that this has dimension at most $r$.

Finally, assume for contradiction that the dimension of this tangent space were strictly smaller than $r$. Hence we could find another linear equation of it that is linearly independent with the above $n - r$ equations. Since the coefficients $c_{r+1}, \ldots, c_n$ are not zero, we can assume that the coefficients of $X_{r+1}, \ldots, X_n$ of this new equation are zero. Hence, there would be an element $f \in I(X)$ taking the form $f = \lambda_1 X_1 + \ldots + \lambda_r X_r + g$, with $\lambda_1, \ldots, \lambda_r \in \mathbb{K}$ (not all of them zero) and $g \in (X_1, \ldots, X_n)^2$. But this would imply that the classes of $\bar{X}_1, \ldots, \bar{X}_r$ modulo $\mathfrak{m}^2$ are linearly dependent, which is a contradiction. $\square$

The above result shows that we need to work over $\mathfrak{m}$ module $\mathfrak{m} \cdot \mathfrak{m}$. We will prove now a crucial result for local rings showing that the behavior of any module over a local ring is essentially the same when quotienting by the submodule generated by the multiplication by the maximal ideal.

**Proposition 7.3** (Nakayama's lemma)**.** *Let $M$ be a finitely generated module over a local ring $A$ with maximal ideal $\mathfrak{m}$. If $N$ is a submodule of $M$ such that $M = N + \mathfrak{m}M$, then $N = M$.*

*Proof:* Let $m_1, \ldots, m_n$ a set of generators of $M$. By assumption, we have congruences modulo $N$ of the type:

$$\begin{array}{rcl} m_1 & \equiv & a_{11}m_1 + \ldots + a_{1n}m_r \\ & \vdots & \\ m_r & \equiv & a_{r1}m_1 + \ldots + a_{rr}m_r \end{array}$$

where the $a_{ij}$'s are in $\mathfrak{m}$. In matricial form, we have

$$\begin{pmatrix} a_{11}-1 & a_{12} & \ldots & a_{1r} \\ a_{21} & a_{22}-1 & \ldots & a_{r2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{r1} & a_{r2} & \ldots & a_{rr}-1 \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_r \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

The determinant $u$ of the left-hand side matrix is not in $\mathfrak{m}$, and hence it is a matrix. Multiplying the above expression by the adjoint of that matrix we get $um_i \equiv 0$ for $i = 1, \ldots, r$. Since $u$ is a unit we thus get that $m_1, \ldots, m_r$ are in $N$, as wanted. □

**Corollary 7.4.** *Let $A$ be a local ring with maximal ideal $\mathfrak{m}$. If the $A/\mathfrak{m}$-vector space $\mathfrak{m}/\mathfrak{m}^2$ is generated by the classes of $f_1, \ldots, f_r$, then $\mathfrak{m}$ is generated by $f_1, \ldots, f_r$.*

*Proof:* Apply Nakayama's lemma with $M = \mathfrak{m}$ and $N = (f_1, \ldots, f_r)$. □

The main example to have in mind for the next results is the following:

**Example 7.5.** Consider the ring $\mathbb{K}[[X]]$ of formal series and let $\mathbb{K}((X))$ be its quotient field. By Exercise 2.7(ii), any element of $\mathbb{K}[[X]]$ can be written in a unique way as the product of a unit (i.e. a series with nonzero constant term) and a power of $X$. This means (by collecting the units of numerator and denominator) that any element of $\mathbb{K}((X))$ is the product of a unit in $\mathbb{K}[[X]]$ and a (maybe negative) power of $X$, i.e. a Laurent formal series. We can thus define the order $\nu(f)$ of any $f \in \mathbb{K}((X)) \setminus \{0\}$ by $\nu(f) = n$ iff $f = uX^n$, with $u$ a unit of $\mathbb{K}[[X]]$. It clearly follows that $\nu(fg) = \nu(f) + \nu(g)$ and $\nu(f+g) \geq \min\{\nu(f), \nu(g)\}$ (with strict inequality only if $\nu(f) \neq \nu(g)$). Observe that $\mathbb{K}[[X]]$ is a local ring whose maximal ideal is $(X)$, hence $\nu(f)$ is measuring "how many times $f$ is contained in $(X)$". The precise way of saying that when $f \in \mathbb{K}[[X]]$ is that $\nu(f)$ is the maximum power of the maximal ideal containing $f$.

**Proposition 7.6.** *Let $A$ be a local ring whose maximal ideal $\mathfrak{m}$ is generated by one element $f$. Then:*

*(i) If $A$ is Noetherian, then it contains no nonzero prime ideals different from $\mathfrak{m}$. In particular, $A$ has dimension at most one, and if it has dimension one, then it is a domain.*

*(ii) If $A$ is a domain of dimension one, then for any nonzero element $g$ of the quotient field of $A$ there exist a unique $n \in \mathbb{Z}$ and a unique unit $u \in A$ such that $g = uf^n$. In particular $A$ is a PID and hence Noetherian.*

*Proof:* For (i), assume for that there is a prime $\mathfrak{p} \subsetneq \mathfrak{m}$ of $A$ and let us check that it is zero. Since $\mathfrak{p} \subsetneq \mathfrak{m}$, $f$ cannot be in $\mathfrak{p}$. Take any element $g \in \mathfrak{p}$ and let us see that it is necessarily zero. For each $n \in \mathbb{N}$ we consider the ideal $I_n = \{h \in A \mid hf^n \in (g)\}$. Since we have a chain $I_1 \subset I_2 \subset \ldots$ and $A$ is Noetherian, there is some $n$ for which $I_n = I_{n+1}$. On the other hand, $g$ is in $\mathfrak{m} = (f)$, so that there exists $g_1 \in A$ such that $g = g_1 f$. Since $g \in \mathfrak{p}$ and $f \notin \mathfrak{p}$, it follows that $g_1$ is also in $\mathfrak{p}$, hence in $\mathfrak{m} = (f)$. We can thus write $g_1 = g_2 f$ (so that $g = g_2 f^2$) for some $g_2 \in A$, and by the same reason as above $g_2$ must be in $\mathfrak{p} \subset (f)$. Iterating this process we can write $g = g_{n+1} f^{n+1}$ for some $g_{n+1} \in A$. This means that $g_{n+1}$ is in $I_{n+1}$, which was equal to $I_n$. Therefore we can write $g_{n+1} f^n = ag$ for some $a \in A$. We thus get the equalities $g = g_{n+1} f^{n+1} = afg$, i.e. $(1 - af)g = 0$. Since $1 - af$ is not in $\mathfrak{m}$, it is a unit, hence $g = 0$, which proves the first statement of (i). The second one follows now immediately, since the only prime ideals of $A$ are $\mathfrak{m}$ and maybe $(0)$, and $(0)$ is a prime ideal if and only if $A$ is a domain.

For (ii), we start by taking $g \in A$ not a unit. Observe that by assumption $\mathfrak{m}$ and $(0)$ are the only prime ideals of $A$, hence $\mathfrak{m}$ is the only prime ideal containing $(g)$. Therefore, Proposition 1.7 implies that $\sqrt{(g)} = \mathfrak{m} = (f)$, from which there exists $n \in \mathbb{N}$ such that $f^n$ is in $(g)$. Take $n$ to be minimum with this property and write $f^n = ag$ (with $a \in A$). It is enough to prove that $a$ is not in $\mathfrak{m}$, since this would imply that $a$ is a unit, and hence $g = a^{-1} f^n$. Assume for contradiction that $a$ is in $\mathfrak{m} = (f)$. We can thus write $a = bf$ for some $b \in A$. Hence we have the equality $f^n = bfg$, but since $A$ is a domain and $f \neq 0$ we get $f^{n-1} = bg$, contradicting the minimality of $n$. For the last statement of (ii), it is easy to prove that any ideal $I \subset A$ is generated by $f^n$, where $n \in \mathbb{N}$ is the minimum integer such that $f^n \in I$. □

**Definition.** Let $K$ be a field. A *discrete valuation* over $K$ is a surjective map $\nu : K \setminus \{0\} \to \mathbb{Z}$ such that for all $f, g \in K \setminus \{0\}$ the following holds:

(i) $\nu(fg) = \nu(f) + \nu(g)$ .

(ii) $\nu(f + g) \geq \min\{\nu(f), \nu(g)\}$

(in order to avoid problems when $f = -g$ in (ii) it is convenient to extend the definition of $\nu$ to 0 by assigning $\nu(0) = +\infty$ ). The set of elements $f \in K$ for which $\nu(f) \geq 0$ (this includes $f = 0$) is a ring called a *discrete valuation ring (DVR).*

**Lemma 7.7.** *Let $A$ be a local Noetherian domain that is integrally closed, and let $\varphi$ be an element of the quotient field of $A$ that is not in $A$. If $\varphi\mathfrak{m} \subset A$, then $\mathfrak{m}$ is a principal ideal, generated by $\frac{1}{\varphi}$.*

*Proof:* Clearly, $\varphi\mathfrak{m}$ is an ideal of $A$. Assume we know that this ideal is the whole $A$. In particular we could write $1 = \varphi m_0$ for some $m_0 \in \mathfrak{m}$, so that $\frac{1}{\varphi} = m_0 \in \mathfrak{m}$. On the other hand, for any $m \in \mathfrak{m}$ we would have $m = (\varphi m)\frac{1}{\varphi}$, and by assumption $\varphi m \in A$. Therefore $\mathfrak{m}$ would be generated by $\frac{1}{\varphi}$.

Hence it is enough to prove that $\varphi\mathfrak{m}$ is the whole ring $A$. Since $A$ is a local ring, $\varphi\mathfrak{m}$ is the whole ring if and only if it is not contained in $\mathfrak{m}$. Assume for contradiction that $\varphi\mathfrak{m} \subset \mathfrak{m}$, and take a set of generators $m_1, \ldots, m_r$ of $\mathfrak{m}$. This would yield relations

$$\begin{aligned} \varphi m_1 &= a_{11}m_1 + \ldots + a_{1r}m_r \\ &\vdots \\ \varphi m_r &= a_{r1}m_1 + \ldots + a_{rr}m_r \end{aligned}$$

with the $a_{ij}$'s in $A$. As usual, this provides equalities

$$\begin{vmatrix} \varphi - a_{11} & \ldots & -a_{1r} \\ \vdots & \ddots & \vdots \\ -a_{r1} & \ldots & \varphi - a_{rr} \end{vmatrix} m_i = 0, \qquad i = 1, \ldots, r$$

Since $\mathfrak{m}$ is not zero (otherwise $A$ would coincide with its quotient field, contrary to the existence of $\varphi$) and $A$ is a domain, it follows that the left-hand side determinant is zero. Therefore $\varphi$ is integral over $A$. Since $\varphi$ is not in $A$, this contradicts that $A$ is integrally closed. □

It is clear that a DVR is a domain (it is contained in a field $K$, which in fact is its quotient field), and that any ideal is generated by any element whose image by $\nu$ is minimum. Then it is Noetherian of dimension one. In fact, we have the following characterization:

**Theorem 7.8.** *Let $A$ be a Noetherian local domain of dimension one. Let $\mathfrak{m}$ be its maximal ideal and let $K$ be its quotient field. Then the following are equivalent:*

*(i) $A$ is a DVR.*

*(ii) For any nonzero element $f \in K$, either $f \in A$ or $f^{-1} \in A$.*

*(iii) $A$ is integrally closed.*

*(iv) $\mathfrak{m}$ is a principal ideal.*

*(v) The dimension of $\mathfrak{m}/\mathfrak{m}^2$ as a vector space over $A/\mathfrak{m}$ is one.*

*Moreover, in this situation, $\mathfrak{m}$ is generated by any element $f \in K$ such that $\nu(f) = 1$, and $\nu(g)$ is defined as the unique integer such that $g/f^{\nu(g)}$ is a unit in $A$.*

*Proof:* It is enough to prove the equivalence of the different points (the last part of the statement being a consequence of the given proofs).

*(i)⇒(ii).* If $A$ is a DVR with valuation $\nu$, it is then clear that for any $f \neq 0$ in $K$ either $\nu(f) \geq 0$ or $\nu(f^{-1}) \geq 0$, since $\nu(f) + \nu(f^{-1}) = \nu(ff^{-1}) = 0$.

*(ii)⇒(iii).* Let $f \in K$ be an element integral over $A$. We consider an integral dependence equation $f^n + a_{n-1}f^{n-1} + \ldots + a_1 f + a_0 = 0$, with $a_0, \ldots, a_{n-1} \in A$. Since either $f \in A$ or $f^{-1} \in A$, we can assume $f^{-1} \in A$. But in this case, multiplying by $f^{-n+1}$ the integral dependence equation we get $f = -a_{n-1} - \ldots - a_1(f^{-1})^{n-2} - a_0(f^{-1})^{n-1}$, which proves that $f$ is in $A$.

*(iii)⇒(iv).* Take any nonzero element $g$ of $\mathfrak{m}$. Since $A$ has dimension one and (0) is a prime ideal (because $A$ is a domain), it follows that $\mathfrak{m}$ is the only prime ideal containing $(g)$, and therefore $\sqrt{(g)} = \mathfrak{m}$ by Proposition 1.7. Take $n$ to be the minimum integer such that $\mathfrak{m}^n \subset (g)$. We can thus pick $h \in \mathfrak{m}^{n-1} \setminus (g)$. Hence $\frac{h}{g} \notin A$ and $\frac{h}{g}\mathfrak{m} \subset A$. Lemma 7.7 implies that $\mathfrak{m}$ is a principal ideal, as wanted.

*(iv)⇔(v).* This is Nakayama's lemma, or more precisely Corollary 7.4.

*(iv)⇒(i).* This is just what we have seen in Proposition 7.6. □

**Example 7.9.** Let us find all the valuations of the quotient field $\mathbb{K}(X)$ of $\mathbb{K}[X]$, when $\mathbb{K}$ is an algebraically closed field. So fix a valuation $\nu$ on $\mathbb{K}(X)$, and let $f$ be a generator of the maximal ideal $\mathfrak{m}$ of the corresponding valuation ring. The first observation is that any $\lambda \in \mathbb{K} \setminus \{0\}$ is a unit in $A$. Indeed, if $|\nu(\lambda)| = n > 0$, take an $(n+1)$th-root $\mu$ of $\lambda$; we have $\nu(\lambda) = \nu(\mu^{n+1}))(n+1)\nu(\mu)$, which is a contradiction. On the other hand, since $f$ is, up to a constant, a product of elements of the form $X - a$ and $\frac{1}{X-b}$, then one element of that type is in $\mathfrak{m}$. We will distinguish those two cases:

*Case 1)* If $\mathfrak{m}$ contains an element of the form $X - a$, since any nonzero constant $\lambda \in \mathbb{K}$ is a unit in $A$, it follows that $X - a + \lambda$ is also a unit. Hence any $X - b$ with $b \neq a$ is a unit, and therefore any nonzero element of $\mathbb{K}(X)$ is written in a unique way as $u(X-a)^n$, for some unit $u$ of $A$ and some integer $n \in \mathbb{Z}$. Hence the valuation is given by $\nu(f) = n$, and $A$ is the localization of $\mathbb{K}[X]$ in the maximal ideal $(X - a)$.

*Case 2)* If $\mathfrak{m}$ contains an element of the form $\frac{1}{X-b}$, then as before, for any $\lambda \in \mathbb{K} \setminus \{0\}$ it follows that $\frac{1}{X-b} + \lambda = \frac{\lambda X - \lambda b + 1}{X-b}$ is a unit of $A$. Therefore $\frac{1}{X-b+\frac{1}{\lambda}} = \lambda \frac{X-b}{\lambda X - \lambda b + 1} \frac{1}{X-b}$ is also in $\mathfrak{m}$. This means that any $\frac{1}{X-a}$ is in $\mathfrak{m}$. Making the substitution $X = \frac{1}{Y}$, we just have that $\frac{Y}{Y-c}$ is in $\mathfrak{m}$ for any $c \in \mathbb{K} \setminus \{0\}$. Since $\mathbb{K}(X) = \mathbb{K}(Y)$, we are in fact in case 1), and the valuation is given by $\nu(uY^n) = n$, where $u$ is a quotient of products none of their factors being $Y$. This corresponds to the valuation at the infinity point of $\mathbb{A}^1_{\mathbb{K}}$.

**Example 7.10.** As a consequence of Example 7.9, we can find all the valuations of the quotient field of the ring of regular functions of parametrizable curves. For instance, we consider the curve $C = V(X^2 - Y^2 + X^3 - 2X^2Y) \subset \mathbb{A}^2_k$. It is an easy exercise (just write $Y = tX$) to get a parametrization of $C$ of the type $X = \frac{1-t^2}{2t-1}, Y = \frac{t(1-t^2)}{2t-1}$. We can thus define a map from the quotient field of $\mathbb{K}[X,Y]/I(C)$ to $\mathbb{K}(T)$ by assigning $\bar{X} \mapsto \frac{1-T^2}{2T-1}$, $\bar{Y} \mapsto \frac{T(1-T^2)}{2T-1}$. This map is an isomorphism ($T$ is the image of $\frac{\bar{Y}}{\bar{X}}$). Hence the valuations of the quotient field of $\mathbb{K}[X,Y]/I(C)$ correspond to the valuations of $\mathbb{K}[T]$. The valuation corresponding to the point at infinity in $\mathbb{A}^1_{\mathbb{K}}$ corresponds in $C$ to the point of infinity of $C$ in the vertical direction $(0,1)$. The valuation corresponding to the point $\frac{1}{2} \in \mathbb{K}$ corresponds to the other infinity point of $C$, in the direction of the vector $(2,1)$. For any $t \in \mathbb{A}^1_{\mathbb{K}} \setminus \{\frac{1}{2}\}$, the associated valuation corresponds to the point $(\frac{1-t^2}{2t-1}, \frac{t(1-t^2)}{2t-1})$ of $C$. Observe that there are two different valuations for the point $(0,0)$ of $C$, namely the ones of $\mathbb{K}(T)$ corresponding to the points $1, -1$. Hence the set of all the valuations of the quotient field of $\mathbb{K}[X,Y]/I(C)$ is a kind of desingularization of the projective closure of $C$.

**Proposition 7.11.** *Let $A$ be an integrally closed Noetherian domain, and let $f \in A \setminus \{0\}$ be a nonunit. Then any associated prime of $(f)$ (i.e. the radical of any primary component of $(f)$) is a minimal nonzero prime ideal of $A$, i.e. it has height one.*

*Proof:* Let $\mathfrak{p}$ be an associated prime of $(f)$. By Theorem 3.11, it follows that there exists $g \in A$ such that $\mathfrak{p} = \{h \in A \mid hg \in (f)\}$. Localizing $A$ at $\mathfrak{p}$ we immediately see that $\mathfrak{p}A_{\mathfrak{p}} = \{h \in A_{\mathfrak{p}} \mid hg \in (f)\}$. Since $\mathfrak{p}A_{\mathfrak{p}}$ is the maximal ideal of $A_{\mathfrak{p}}$, in particular it is not the whole $A_{\mathfrak{p}}$, and hence $\frac{g}{f}$ is not in $A_{\mathfrak{p}}$. On the other hand $\frac{g}{f}\mathfrak{p}A_{\mathfrak{p}}$ is clearly contained in $A_{\mathfrak{p}}$. By Lemma 7.7 we get that $\mathfrak{p}A_{\mathfrak{p}}$ is a principal ideal. Hence by Proposition 7.6(i), $A_{\mathfrak{p}}$ has dimension one, which implies that $\mathfrak{p}$ has height one. □

**Exercise 7.12.** Let $I$ be the kernel of the map $\varphi : k[W,X,Y,Z] \to k[U,V]$ defined by $\varphi(P(W,X,Y,Z) = P(U^4, U^3V, UV^3, V^4)$.

(i) Prove $I$ is generated by $WZ - XY$, $X^3 - W^2Y$, $Y^3 - XZ^2$ and $X^2Z - WY^2$.

(ii) Prove that $\mathbb{K}[W,X,Y,Z]/I$ has dimension two.

(iii) Prove that an irredundant primary decomposition of $I + (X - Y)$ is given by $(W, X, Y) \cap (X, Y, Z) \cap (W - X, X - Y, Y - Z) \cap (W + X, X - Y, Y + Z) \cap (X - Y, Z - \lambda Y, Y - \lambda W, W^3)$, for any $\lambda \neq 0, 1, -1$.

**Theorem 7.13.** *Let $A$ be a noetherian domain. Then $A$ is normal if and only if the following two conditions hold:*

*(i) For any prime ideal $\mathfrak{p} \subset A$ of height one, the localization $A_{\mathfrak{p}}$ is normal (i.e. a DVR).*

*(ii) For any nonunit element $f \in A \setminus \{0\}$, the ideal $(f)$ has no embedded components.*

*Proof:* Assume $A$ is normal. Then (i) holds by Lemma 5.11, while (ii) holds by Proposition 7.11. Hence we just need to prove that (i) and (ii) imply that $A$ is normal. Thus, take $\frac{g}{f}$ in the quotient field of $A$ and assume it is integral over $A$, and we need to prove $\frac{g}{f} \in A$, or equivalenty $g \in (f)$. If $f$ is a unit, there is nothing to prove, so we assume $f$ is not a unit. Hence, by (ii) we have a primary decomposition $(f) = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_r$ such that $\sqrt{\mathfrak{q}_1}, \ldots, \sqrt{\mathfrak{q}_r}$ have all height one. Hence by (i) each localization of $A$ at $\sqrt{\mathfrak{q}_i}$ is normal. Since $\frac{g}{f}$ is integral over this localization, it follows that $\frac{g}{f} \in A_{\sqrt{\mathfrak{q}_i}}$. Therefore $\frac{g}{f} = \frac{h}{s}$, with $h \in A$ and $s \in A \setminus \sqrt{\mathfrak{q}_i}$. Equivalently, $sg \in (f)$, and in particular $sg \in \mathfrak{q}_i$. Since $\mathfrak{q}_i$ is primary and $s \notin \sqrt{\mathfrak{q}_i}$, it follows $g \in \mathfrak{q}_i$. This is true for any $i = 1, \ldots, r$, and therefore $g \in \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_r = (f)$, as wanted. □

**Example 7.14.** In the situation of Exercise 7.12, it should happen, after Proposition 7.11, that the quotient field of $k[W, X, Y, Z]/I$ is not integrally closed. In fact, we can take the element $\alpha = \frac{\bar{X}^2}{\bar{W}}$ (i.e. the element corresponding to the "missing monomial $U^2V^2$). It clearly satisfies the relation $\alpha^2 - \bar{W}\bar{Z} = 0$, hence it is integral over $k[W, X, Y, Z]/I$. However, it is easy to see that $\alpha$ does not belong to $k[W, X, Y, Z]/I$. Indeed, if $\alpha$ were the class of a polynomial $f \in \mathbb{K}[W, X, Y, Z]$, then $WY - Xf$ would be an element of $I$, i.e. by definition $U^5V^3 - U^3Vf(U^4, U^3V, UV^3, V^4) = 0$. Hence $f(U^4, U^3V, UV^3, V^4) = U^2V^2$, which is clearly impossible.

Regarding $\alpha$ as a rational function defined over $V(I)$, we see from the equalities $\alpha = \frac{\bar{X}^2}{\bar{W}} = \frac{\bar{W}\bar{Y}}{\bar{X}} = \frac{\bar{X}\bar{Z}}{\bar{Y}} = \frac{\bar{Y}^2}{\bar{Z}}$ that $\alpha$ is defined in all the surface except maybe at $(0, 0, 0, 0)$ (in fact only the first and last of the above equalities are needed to see this). This means that $\alpha$ is in the localization of all the maximal ideals of $k[W, X, Y, Z]/I$ except maybe in the one corresponding to $(0, 0, 0, 0)$ (we are now assuming that $\mathbb{K}$ is algebraically closed and use Corollary 1.17). By Proposition 4.14, it follows that $\alpha$ cannot be in the localization of the maximal ideal corresponding to $(0, 0, 0, 0)$, i.e. it cannot be extended to the origin. The next result is saying that, when the ring is normal, rational functions can be extended as long as their indeterminacy locus has codimension at least two.

**Theorem 7.15.** *Let $A$ be an integrally closed Noetherian ring with quotient field $K$. Then $A$ is the intersection in $K$ of all the localizations of $A$ in its prime ideals of height one.*

*Proof:* Let $\frac{f}{g} \in K$ be an element that is not in $A$ and we will show that there is a prime of height one such that $\frac{f}{g} \in K$ is not in the localization of $A$ at it. Since $\frac{f}{g}$ is not in $A$, it follows that $f$ is not in $(g)$, and hence by Corollary 3.15 the ideal $\{h \in A \mid fh \in (g)\}$ is contained in some associated prime $\mathfrak{p}$ of $(g)$. By Proposition 7.11, $\mathfrak{p}$ has height one, and it is clear that $\frac{f}{g}$ is not in $A_{\mathfrak{p}}$ (otherwise, there would exist $s \in A \setminus \mathfrak{p}$ such that $fs \in (g)$, which is absurd). □

We will prove a result saying that the intersection of something of dimension $r$ with a hypersurface has all its components of dimension $r-1$ (the height of a prime ideal should be regarded as the codimension of the variety it defines): Exercise 7.12 shows that it could actually happen that some (necessarily embedded) associated primes have bigger height.

**Theorem 7.16.** *Let $A$ be a Noetherian domain. If $f$ is a nonunit element of $A \setminus \{0\}$, then any nonembedded associated prime of $(f)$ has height one.*

*Proof:* Assume for contradiction that $(f) = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_r$ is an irredundant primary decomposition and that $\mathfrak{p}_1 = \sqrt{\mathfrak{q}_1}$ is a nonembedded prime ideal of length at least two. The fact that $\mathfrak{p}_1$ is not embedded implies that we can find an element of $\mathfrak{p}_2 \cap \ldots \cap \mathfrak{p}_r$ that is not in $\mathfrak{p}_1$. Taking a suitable power of this element, we find $s \in \mathfrak{q}_2 \cap \ldots \cap \mathfrak{q}_r$ that is not in $\mathfrak{p}_1$. On the other hand, the fact that $\mathfrak{p}_1$ has length at least two means that there exists a chain $(0) \subsetneq \mathfrak{p} \subsetneq \mathfrak{p}_1$. If we localize at $\mathfrak{p}_1$, we have that this chain still remains in $A_{\mathfrak{p}_1}$, and that for any $\frac{g}{t} \in \mathfrak{p}_1 A_{\mathfrak{p}_1}$ we have that some $g^l$ is in $\mathfrak{q}_1$, hence we can write $(\frac{g}{t})^l = \frac{g^l s}{t^l s}$, which is in the ideal generated by $\frac{f}{1}$. In other words, we can assume that $A$ is a local ring with maximal ideal $\mathfrak{m} = \mathfrak{p}_1$ and that $\sqrt{(f)}$ is $\mathfrak{m}$ (the latter implies from Exercise 1.4(vii), since $A$ is noetherian, that there exists some $l \in \mathbb{N}$ for which $\mathfrak{m}^l \subset (f)$). Let us see that under these conditions we cannot have a chain $(0) \subsetneq \mathfrak{p} \subsetneq \mathfrak{m}$.

We first define for each $n \in \mathbb{N}$ the ideal $\mathfrak{q}_n = \{g \in A \mid \text{ there exists } s \notin \mathfrak{p} \text{ such that } gs \in \mathfrak{p}^n\}$. It is not difficult to see that each $\mathfrak{q}_n$ is a $\mathfrak{p}$-primary ideal and that there are inclusions $\mathfrak{q}_{n+1} \subset \mathfrak{q}_n$. I claim that there is some $n$ for which $\mathfrak{q}_{n+1} + (f) = \mathfrak{q}_n + (f)$.

Indeed it is enough to prove the claim when quotienting by $\mathfrak{m}^l$, and for this it suffices to prove that $A/\mathfrak{m}^l$ is an Artinian $A$-module (see Exercise 3.7). But considering the submodule $\mathfrak{m}^{l-1}/\mathfrak{m}^l$, this is equivalent to prove that $\mathfrak{m}^{l-1}/\mathfrak{m}^l$ and $A/\mathfrak{m}^{l-1}$ are Artinian. Iterating the process, we need to prover that $\mathfrak{m}^{i-1}/\mathfrak{m}^i$ are Artinian for $i = 1, \ldots, l$. We observe that each $\mathfrak{m}^{i-1}/\mathfrak{m}^i$ is in fact a finitely generated $A/\mathfrak{m}$-module, hence a vector space of finite dimension, and this is obviously Artinian, which proves the claim.

Take now any element $g \in \mathfrak{q}_n$. As we have just proved, it is also in $\mathfrak{q}_{n+1} + (f)$, so that we can write $g = h + af$, with $h \in \mathfrak{q}_{n+1}$ and $a \in A$. Since $\mathfrak{q}_{n+1} \subset \mathfrak{q}_n$, we have that $af$ belongs to $\mathfrak{q}_n$. We cannot have $f \in \mathfrak{p}$, because that would imply $\mathfrak{m} = \sqrt{(f)} \subset \mathfrak{p}$ and thus $\mathfrak{m} = \mathfrak{p}$, contrary to our assumption. Therefore, since $\mathfrak{q}_n$ is $\mathfrak{p}$-primary, it follows that $a$ must be in $\mathfrak{q}_n$. This shows that $g$ is in $\mathfrak{q}_{n+1} + f\mathfrak{q}_n$, hence in $\mathfrak{q}_{n+1} + \mathfrak{m}\mathfrak{q}_n$, i.e. we have an inclusion $\mathfrak{q}_n \subset \mathfrak{q}_{n+1} + \mathfrak{m}\mathfrak{q}_n$. By Nakayama's lemma, it follows that we have an equality $\mathfrak{q}_{n+1} = \mathfrak{q}_n$.

We localize now in $\mathfrak{p}$, and consider in $A_\mathfrak{p}$ its maximal ideal $\mathfrak{m}' = \mathfrak{p}A_\mathfrak{p}$. It is clear that, for each $l \in \mathbb{N}$, the power $\mathfrak{m}'^l$ is the set of quotients whose numerator is in $\mathfrak{q}_l$. Therefore, $\mathfrak{m}'^n = \mathfrak{m}'^{n+1}$. This implies, using again Nakayama's lemma that $\mathfrak{m}'^n$ is zero. Take finally any $p \in \mathfrak{p}$. The element $\frac{p^n}{1}$ of $A_\mathfrak{p}$ is in $\mathfrak{m}'^n$, so it is zero. This means that there exists $s \notin \mathfrak{p}$ such that $p^n s = 0$. Since $A$ is a domain, it follows that $p$ is zero. Therefore $\mathfrak{p}$ is the zero ideal, which is a contradiction. This completes the proof of the theorem. □

**Exercise 7.17.** Let $\mathfrak{p}$ be a prime ideal of a ring $A$. Prove that $\mathfrak{q}_n = \{g \in A \mid gs \in \mathfrak{p}^n \text{ for some } s \notin \mathfrak{p}\}$ is the smallest $\mathfrak{p}$-primary ideal containing $\mathfrak{p}^n$. Show that in $A_\mathfrak{p}$ an element $\frac{g}{s}$ belongs to $(\mathfrak{p}A_\mathfrak{p})^n$ if and only if $g \in \mathfrak{q}_n$.

We generalize Theorem 7.16 to the intersection with an arbitrary number of generators.

**Theorem 7.18.** *Let $A$ be a Noetherian ring and let $I$ be a proper ideal of $A$ generated by $r$ elements. Then any nonembedded associated prime of $I$ has height at most $r$.*

*Proof:* We will prove the theorem by induction on $r$, the case $r = 1$ being Theorem 7.16. Assume now $r \geq 2$ and let $I = (f_1, \ldots, f_r)$ be a proper ideal of $A$ and let $\mathfrak{p}$ be a nonembedded associated prime of $I$. By localizing at $\mathfrak{p}$ we can assume that $A$ is a local ring. Let $\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_s$ be a chain of maximal length of prime ideals. We need to prove $s \leq r$. Necessarily $\mathfrak{p}_s = \mathfrak{p}$, and in particular $f_r \in \mathfrak{p}_s$. If we had $f_r \in \mathfrak{p}_1$ then we could consider $A/\mathfrak{p}_1$, in which we have the chain $\mathfrak{p}_1/\mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_s/\mathfrak{p}_1$ of length $s-1$; in this ring, the maximal ideal $\mathfrak{p}_s/\mathfrak{p}_1$ is a nonembedded associated prime of the ideal $I/\mathfrak{p}_1$, generated by the classes of $f_1, \ldots, f_{r-1}$, and by induction hypothesis we would obtain $s - 1 \leq r - 1$. Our trick will be to reduce ourselves to such a situation by substituting the prime ideals in the chain.

Consider first the biggest $i \in \{1, \ldots, s-1\}$ such that $f_r \notin \mathfrak{p}_i$. We have then a (maximal) chain $(0) \subsetneq \bar{\mathfrak{p}}_i \subsetneq \bar{\mathfrak{p}}_{i+1}$ of prime ideals in $A/\mathfrak{p}_{i-1}$ (the bars meaning classes modulo $\mathfrak{p}_{i-1}$), hence $\bar{\mathfrak{p}}_{i+1}$ has height two. By assumption, the class $\bar{f}_r$ is in $\bar{\mathfrak{p}}_{i+1}$ but not in $\bar{\mathfrak{p}}_i$, and in particular is neither zero nor a unit. We can therefore apply Theorem 7.16 and conclude that any nonembedded associated prime of $(\bar{f}_r)$ has height one (and it is

hence different from $\bar{\mathfrak{p}}_{i+1}$). Since $\sqrt{(\bar{f}_r)}$ is contained in $\bar{\mathfrak{p}}_{i+1}$ and is the intersection of the nonembedded associated prime of $(\bar{f}_r)$, it follows from Lemma 1.1 that $\bar{\mathfrak{p}}_{i+1}$ contains one of these nonembedded associated primes. Such a prime corresponds to a prime ideal $\mathfrak{p}'_i$ that contains strictly $\mathfrak{p}_{i-1}$, is strictly contained in $\mathfrak{p}_{i+1}$ and contains the element $f_r$. We can thus replace $\mathfrak{p}_i$ with this other prime $\mathfrak{p}'_i$ in the above chain. Iterating the process, we arrive to a chain of prime ideals in which $\mathfrak{p}_1$ contains $f_r$, and we can use the above induction argument to conclude. □

**Corollary 7.19.** *Let $A$ be a local ring with maximal ideal $\mathfrak{m}$. Then the dimension of $A$ is at most the dimension of the $A/\mathfrak{m}$-vector space $\mathfrak{m}/\mathfrak{m}^2$.*

*Proof:* If $\mathfrak{m}/\mathfrak{m}^2$ has dimension $r$, by Corollary 7.4 we know that $\mathfrak{m}$ can be generated by $r$ elements. The result follows now from Theorem 7.18. □

**Definition.** A *local regular ring* is a local ring $A$ whose dimension coincides with the dimension of $\mathfrak{m}/\mathfrak{m}^2$ as a vector space over $A/\mathfrak{m}$ (where $\mathfrak{m}$ is the maximal ideal of $A$). Equivalently, $A$ is regular if and only if its maximal ideal can be generated by as many elements as $\dim A$.

**Definition.** A *smooth point of an affine set $X \subset \mathbb{A}^n_{\mathbb{K}}$* is a point such that its tangent space has dimension equal to the dimension of $\mathcal{O}_{X,a}$. Equivalently, $\mathcal{O}_{X,a}$ is a local regular ring. A set of generators of the maximal ideal $\mathfrak{m}$ of $\mathcal{O}_{X,a}$ such that their classes modulo $\mathfrak{m}^2$ form a basis of $\mathfrak{m}/\mathfrak{m}^2$ is called a *system of local parameters of $X$* at $a$.

**Proposition 7.20.** *Let $X \subset \mathbb{A}^n_{\mathbb{K}}$ be an affine set containing $O = (0, \ldots, 0)$ as a smooth point, and assume that $\mathbb{K}$ is infinite. Then for any set of local parameters $\alpha_1, \ldots, \alpha_r$ of $\mathfrak{m}$ of $X$ at $O$ there exists a (unique) homomorphism $i_O : \mathcal{O}_{X,O} \hookrightarrow \mathbb{K}[[Y_1, \ldots, Y_r]]$ such that $i_O(f_i) = Y_i$.*

*Proof:* Take any $f \in \mathcal{O}_{X,O}$ and let $a = f(O)$. Clearly, $f - a$ is in $\mathfrak{m}$, and hence it is possible to write $f = a + f_1\alpha_1 + \ldots f_r\alpha_r$, with $f_1, \ldots, f_r \in \mathcal{O}_{X,O}$. For each $i = 1, \ldots, r$, we write $a_i = f_i(O)$ and using again that $f_i - a_i \in \mathfrak{m}$, and hence $f - a - a_1\alpha_1 - \ldots - a_r\alpha_r$ is in $\mathfrak{m}^2$. We can thus write $f = a + a_1\alpha_1 + \ldots + a_r\alpha_r + f_{11}\alpha_1^2 + f_{12}\alpha_1\alpha_2 + \ldots + f_{rr}\alpha_r^2$. We can go on and consider the values $a_{ij} = f_{ij}(O)$ and iterate the process. In this way, we can write, for any $l \in \mathbb{N}$, $f = F_0 + F_1 + \ldots + F_l + G_{l+1}$, with $F_i$ a homogeneous expression of degree $i$ in $\alpha_1, \ldots, \alpha_r$ and $G_{l+1} \in \mathfrak{m}^{l+1}$. It is clear that the result will follow if we prove that $F_0, F_1, \ldots$ are uniquely determined by $f$. This is the same as proving that, when $f = 0$, it follows $F_0 = F_1 = \ldots = 0$.

Assume for contradiction that there exists $l \in \mathbb{N}$ such that $F_l \neq 0$. If we take $l$ minimum with that condition, then it follows that $F_l$ is in $\mathfrak{m}^{l+1}$. Using that $\mathbb{K}$ is infinite, we can assume, after Lemma 1.15(ii), that $F_l$ is monic in $\alpha_r$, i.e. that it takes the form

$$F_l = \alpha_r^l + G_1\alpha_r^{l-1} + \ldots + G_{l-1}\alpha_r + G_l$$

where for each $i = 1\ldots, l$, the coefficient $G_i$ is a homogeneous expression of degree $i$ in $\alpha_1, \ldots, \alpha_{r-1}$. On the other hand, the fact that $F_l$ is in $\mathfrak{m}^{l+1}$ allows to write

$$F_l = h_0\alpha_r^l + h_1\alpha_r^{l-1} + \ldots + h_{l-1}\alpha_r + h_l$$

with $h_0 \in \mathfrak{m}$ and $h_1, \ldots, h_l \in (\alpha_1, \ldots, \alpha_{r-1})$. Comparing the two expressions of $F_l$, we get that $(1 - h_0)\alpha_r^l$ is in $(\alpha_1, \ldots, \alpha_{r-1})$. Since $1 - h_0 \notin \mathfrak{m}$, it is a unit and hence $\alpha_r^l$ is in $(\alpha_1, \ldots, \alpha_{r-1})$. This means that $\sqrt{(\alpha_1, \ldots, \alpha_{r-1})} = \mathfrak{m}$, and hence (see Proposition 2.14) $(\alpha_1, \ldots, \alpha_{r-1})$ is an $\mathfrak{m}$-primary ideal. This means that its only associated prime is $\mathfrak{m}$. By Theorem 7.18, $\mathfrak{m}$ should have height at most $r - 1$, which is absurd, since its height is the dimension of $\mathcal{O}_{X,O}$, which is $r$. □

**Definition.** Given a smooth point $a$ of an affine set, local parameters $\alpha_1, \ldots, \alpha_r$ of $X$ at $a$, and given $f \in \mathcal{O}_{X,a}$, we call the *Taylor expansion* of $f$ at $a$ with respect to the local parameters to the formal series described in Proposition 7.20 (after making a translation to the origin).

Observe that in fact the above proof shows that we can assign a Taylor expansion with respect to any system of generators of $\mathfrak{m}$, even if the point is singular. When the point is smooth and the system of generators form a system of local parameters, then this series is unique. We could also ask whether any element of $\mathcal{O}_{X,a}$ is uniquely determined by its Taylor expansion with respect to a system of parameters. The answer will be yes (Corollary 7.23), but we need some results first.

**Theorem 7.21** (Artin-Rees Lemma)**.** *Let $A$ be a Noetherian ring with an ideal $\mathfrak{m}$. Then for any ideal $I \subset A$, there exists $k \in \mathbb{N}$ such that $\mathfrak{m}^n \cap I = \mathfrak{m}^{n-k}(\mathfrak{m}^k \cap I)$ for each $n \geq k$.*

*Proof:* We first consider the set $\tilde{A}_\mathfrak{m} := A \oplus \mathfrak{m} \oplus \mathfrak{m}^2 \oplus \ldots$. We can endow $\tilde{A}_\mathfrak{m}$ with a ring structure with the obvious sum and such that the product of an element in a summand $\mathfrak{m}^n$ and an element in the summand $\mathfrak{m}^m$ is its product (inside the ring $A$) in the summand $\mathfrak{m}^{n+m}$. If $f_1, \ldots, f_r$ is a set of generators of $\mathfrak{m}$, there is a natural epimorphism $A[X_1, \ldots, X_r] \to \tilde{A}_\mathfrak{m}$ that assigns to any monomial $X_1^{i_1} \ldots X_r^{i_r}$ the element $f_1^{i_1} \ldots f_r^{i_r}$ in the summand $\mathfrak{m}^{i_1+\ldots+i_r}$. Hence $\tilde{A}_\mathfrak{m}$ is isomorphic to a quotient of $A[X_1, \ldots, X_n]$ (which is a Noetherian ring by Hilbert's basis theorem, see Theorem 2.2). Then Proposition 3.6 implies that $\tilde{A}_\mathfrak{m}$ is a Noetherian ring.

For each $k \in \mathbb{N}$, we consider the subset $I_k \subset \tilde{A}_{\mathfrak{m}}$ consisting of the elements such that, for $n \geq k$, its component in $\mathfrak{m}^n$ belongs to $\mathfrak{m}^{n-k}(\mathfrak{m}^k \cap I)$. It is easy to see that $I_k$ is an ideal and that we have a chain $I_0 \subset I_1 \subset I_2 \subset \ldots$. Since $\tilde{A}_{\mathfrak{m}}$ is Noetherian, it follows that there exists $k \in \mathbb{N}$ such that $I_k = I_{k+1} = I_{k+2} = \ldots$. For each $n \geq k$, looking at the component $\mathfrak{m}^n$ of $I_k$ and $I_n$ we get $\mathfrak{m}^n \cap I = \mathfrak{m}^{n-k}(\mathfrak{m}^k \cap I)$, as wanted. □

**Theorem 7.22** (Krull)**.** *Let $A$ be a Noetherian local ring with maximal ideal $\mathfrak{m}$. Then:*

*(i)* $\bigcap_{n\in\mathbb{N}} \mathfrak{m}^n = 0$.

*(ii) For any ideal $I \subset A$, it follows* $\bigcap_{n\in\mathbb{N}}(I + \mathfrak{m}^n) = I$.

*Proof:* For (i), consider the ideal $I = \bigcap_{n\in\mathbb{N}} \mathfrak{m}^n$. By Artin-Rees Lemma, there exists $k \in \mathbb{N}$ such that $\mathfrak{m}^n \cap I = \mathfrak{m}^{n-k}(\mathfrak{m}^k \cap I)$ for each $n \geq k$. Using the definition of $I$ and taking $n = k + 1$, we get $I = \mathfrak{m}I$. Using Nakayama's Lemma (see Proposition 7.3) we obtain $I = 0$, as wanted.

For (ii) we just need to apply (i) to $A/I$, having in mind that the $n$-th power of its maximal ideal $\mathfrak{m}/I$ is $I + \mathfrak{m}^n/I$. □

**Corollary 7.23.** *In the situation of Proposition 7.20, the map $i_O$ is injective.*

*Proof:* By definition of $i_O$, we have that $i_O(f) = 0$ when $f \in \bigcap_{l\in\mathbb{N}} \mathfrak{m}^l$, and this is zero by Theorem 7.22(i). □

**Corollary 7.24.** *Let $X \subset \mathbb{A}^n_{\mathbb{K}}$ be an affine set and let $x \in X$ be a smooth point. Then there is only an irreducible component of $X$ passing through $x$.*

*Proof:* By Corollary 7.23, we know that $\mathcal{O}_{X,x}$ is contained in some $\mathbb{K}[[X_1, \ldots, X_r]]$, and hence it is an integral domain. Identifying $\mathcal{O}_{X,x}$ with the quotient of $\mathbb{K}[X_1, \ldots, X_n]_{I(x)}$ over the localization $I(X)_{I(x)}$ of $I(X)$, we get that $I(X)_{I(x)}$ is a prime ideal. This means that, in the prime decomposition of $I(X)$, only one prime ideal is contained in $I(x)$, which is precisely our claim. □

# References


[A] M.F. Atiyah, I.G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., 1969.

[CLO] D. Cox, J. Little, D. O'Shea, *Ideals, Varieties and Algorithms*, Springer-Verlag 1992.

[Fi] G. Fischer, *Plane algebraic curves*, AMS 2001.

[H] J. Harris, *Algebraic Geometry: a first course*, Springer-Verlag 1992.

[Ha] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag 1977.

[Ma] H. Matsumura, *Commutative algebra*, Benjamin/Cumming co., 1981.

[Mu] D. Mumford, *Algebraic Geometry I: Complex Projective Varieties*, Springer 1991 (reprinted ed.).

[Re] M. Reid, *Undergraduate Commutative Algebra*, Cambridge University Press 1995.

[Sh] R.Y. Sharp, *Steps in Commutative Algebra*, London Math. Soc. Student Texts 19 1990.

[ZS] O. Zariski, P. Samuel, *Commutative Algebra*, Vols. I and II, van Nostrand 1965.