Algebraic Geometry I
Fall 2013

Eduard Looijenga

Rings are always supposed to possess a unit element 1 and a ring homomorphism will always take unit to unit. We allow that $1 = 0$, but in that case we get of course the zero ring $\{0\}$. We assume a ring to be commutative unless the contrary is stated. If R is a ring, then we denote the multiplicative group of invertible elements (units) of R by $R^\times$. We say that R is a *domain* if R has no zero divisors, equivalently, if (0) is a prime ideal. An *R-algebra* is a ring A endowed with a ring homomorphism $\phi : R \to A$, but if ϕ is understood, then for every $r \in R$ and $a \in A$, the product $\phi(r)a$ is often denoted by ra. We say that A is *finitely generated as an R-algebra* if we can find $a_1, \ldots, a_n$ in A such that every element of A can be written as a polynomial in these elements with coefficients in R; in other words, the R-algebra homomorphism $R[x_1, \ldots, x_n] \to A$ which sends the variable x_i to a_i is onto. This is not to be confused with the notion of finite generation for an R-module M resp. which merely means the existence of a surjective homomorphism of R-modules $R^n \to M$. Similarly, a field K is said to be finitely generated as a field over a subfield k if we can find elements $b_1, \ldots, b_n$ in K such that every element of K can be written as a fraction of two polynomials in these elements with coefficients in k.

CHAPTER 1

Affine varieties

Throughout this chapter we fix an algebraically closed field k. Recall that this means that every polynomial $f \in k[x]$ of positive degree has a root $x_1 \in k$: $f(x_1) = 0$. This implies that we can split off the factor $x - x_1$ from f with quotient a polynomial of degree one less than f. Continuing in this manner we find that f decomposes simply as $f(x) = c(x - x_1) \cdots (x - x_d)$ with $c \in k - \{0\}$, $d = \deg(f)$ and $x_1, \ldots, x_d \in k$. Since an algebraic extension of k is obtained by adjoining to k roots of polynomials in $k[x]$, this also shows that the property in question is equivalent to: every algebraic extension of k is equal to k.

A first example you may think of is the field of complex numbers $\mathbb{C}$, but as we proceed you should be increasingly be aware of the fact that there are many others: it is shown in a standard algebra course that for any field F an algebraic closure $\bar{F}$ is obtained by adjoining to F the roots of every polynomial $f \in F[x]$ (this can not always be done in one step, and might involve an infinite process). So we could take for k an algebraic closure of the field of rational numbers $\mathbb{Q}$, of the finite field $\mathbb{F}_q$, where q is a prime power[1] or even of the quotient field of any domain such as $\mathbb{C}[x_1, \ldots, x_r]$.

1. The Zariski topology

Any $f \in k[x_1, \ldots, x_n]$ determines in an evident manner a function $k^n \to k$. In such cases we prefer to think of k^n not as vector space—its origin and vector addition will be irrelevant to us—but as a set with a weaker structure. We shall make this precise later, but it basically amounts to only remembering that elements of $k[x_1, \ldots, x_n]$ can be understood as k-valued functions on it. For that reason it is convenient to denote this set differently, namely as $\mathbb{A}^n$ (or as $\mathbb{A}^n_k$, if we feel that we should not forget about the field k). We refer to $\mathbb{A}^n$ as the *affine n-space over k*. A k-valued function on $\mathbb{A}^n$ is then said to be *regular* if it is defined by some $f \in k[x_1, \ldots, x_n]$. We denote the zero set of such a function by $Z(f)$ and the complement (the nonzero set) by $U(f) \subset \mathbb{A}^n$. If f is not a constant polynomial (that is, $f \notin k$), then we call $Z(f)$ a *hypersurface* of $\mathbb{A}^n$.

EXERCISE 1. Prove that $f \in k[x_1, \ldots, x_n]$ is completely determined by the regular function it defines. (Hint: do first the case $n = 1$.) So the ring $k[x_1, \ldots, x_n]$ can be regarded as a ring of functions on $\mathbb{A}^n$ under pointwise addition and multiplication. (This would fail to be so had we not assumed that k is algebraically closed: for instance the function on the finite field $\mathbb{F}_q$ defined by $x^q - x$ is identically zero.)

EXERCISE 2. Prove that a hypersurface is nonempty.

[1] Since the elements of any algebraic extension of $\mathbb{F}_q$ of degree $n \geq 2$ are roots of $x^{(q^n)} - x$, we only need to adjoin roots of such polynomials.

It is perhaps somewhat surprising that in this rather algebraic context, the language of topology proves to be quite effective: algebraic subsets of $\mathbb{A}^n$ shall appear as the closed sets of a topology, albeit a rather peculiar one.

LEMMA-DEFINITION 1.1. *The collection $\{U(f) : f \in k[x_1, \ldots, x_n]\}$ is a basis of a topology on $\mathbb{A}^n$, called the* Zariski topology[2]*. A subset of $\mathbb{A}^n$ is closed for this topology if and only if it is an intersection of zero sets of regular functions.*

PROOF. We recall that a collection $\{U_\alpha\}_\alpha$ of subsets of a set X is a basis for a topology if and only if its union is all of X and any intersection $U_{\alpha_1} \cap U_{\alpha_2}$ is a union of members of $\{U_\alpha\}_\alpha$. This is here certainly the case, for we have $U(0) = X$ and $U(f_1) \cap U(f_2) = U(f_1 f_2)$. Since an open subset of $\mathbb{A}^n$ is by definition a union of subsets of the form $U(f)$, a closed subset must be an intersection of subsets of the form $Z(f)$. □

EXAMPLE 1.2. The Zariski topology on $\mathbb{A}^1$ is the cofinite topology: its closed subsets $\neq \mathbb{A}^1$ are the finite subsets.

EXERCISE 3. Show that the diagonal in $\mathbb{A}^2$ is closed for the Zariski topology, but not for the product topology (where each factor $\mathbb{A}^1$ is equipped with the Zariski topology). So $\mathbb{A}^2$ does not have the product topology.

We will explore the mutual relationship between the following two basic maps:

$$\begin{array}{ccc} \{\text{subsets of } \mathbb{A}^n\} & \xrightarrow{\ I\ } & \{\text{ideals of } k[x_1, \ldots, x_n]\} \\ \cup & & \cap \\ \{\text{closed subsets of } \mathbb{A}^n\} & \xleftarrow{\ Z\ } & \{\text{subsets of } k[x_1, \ldots, x_n]\}. \end{array}$$

where for a subset $X \subset \mathbb{A}^n$, $I(X)$ is the ideal of $f \in k[x_1, \ldots, x_n]$ with $f|X = 0$ and for a subset $J \subset k[x_1, \ldots, x_n]$, $Z(J)$ is the closed subset of $\mathbb{A}^n$ defined by $\cap_{f \in J} Z(f)$. Observe that

$$I(X_1 \cup X_2) = I(X_1) \cap I(X_2) \quad \text{and} \quad Z(J_1 \cup J_2) = Z(J_1) \cap Z(J_2).$$

In particular, both I and Z are inclusion reversing. Furthermore, I defines a section of Z: if $Y \subset \mathbb{A}^n$ is closed, then $Z(I(Y)) = Y$. We also note that by Exercise 1 $I(\mathbb{A}^n) = (0)$, and that any singleton $\{p = (p_1, \ldots, p_n)\} \subset \mathbb{A}^n$ is closed, as it is the common zero set of the degree one polynomials $x_1 - p_1, \ldots, x_n - p_n$.

EXERCISE 4. Prove that $I(\{p\})$ is equal to the ideal generated by these degree one polynomials and that this ideal is maximal.

EXERCISE 5. Prove that the (Zariski) closure of a subset Y of $\mathbb{A}^n$ is equal to $Z(I(Y))$.

Given $Y \subset \mathbb{A}^n$, then $f, g \in k[x_1, \ldots, x_n]$ have the same restriction to Y if and only if $f - g \in I(Y)$. So the quotient ring $k[x_1, \ldots, x_n]/I(Y)$ (a k-algebra) can be regarded as a ring of k-valued functions on Y. Notice that this k-algebra does not change if we replace Y by its Zariski closure.

DEFINITION 1.3. Let $Y \subset \mathbb{A}^n$ be closed. The k-algebra $k[x_1, \ldots, x_n]/I(Y)$ is called the *coordinate ring* of Y and we denote it by $A(Y)$. A k-valued function on Y is said to be *regular* if it lies in this ring.

[2]We shall later modify the definition of both $\mathbb{A}^n$ and the Zariski topology.

Given a closed subset $Y \subset \mathbb{A}^n$, then for every subset $X \subset \mathbb{A}^n$ we have $X \subset Y$ if and only if $I(X) \supset I(Y)$, and in that case $I_Y(X) := I(X)/I(Y)$ is an ideal of $A(Y)$: it is the ideal of regular functions on Y that vanish on X. Conversely, an ideal of $A(Y)$ is of the form $J/I(Y)$, with J an ideal of $k[x_1, \dots, x_n]$ that contains $I(Y)$, and such an ideal defines a closed subset $Z(J)$ contained in Y. So the two basic maps above give rise to such a pair on Y:

$$\begin{array}{ccc} \{\text{subsets of } Y\} & \xrightarrow{I_Y} & \{\text{ideals of } A(Y)\} \\ \cup & & \cap \\ \{\text{closed subsets of } Y\} & \xleftarrow{Z_Y} & \{\text{subsets of } A(Y)\}. \end{array}$$

We ask: which ideals of $k[x_1, \dots, x_n]$ are of the form $I(Y)$ for some Y? Clearly, if $f \in k[x_1, \dots, x_n]$ is such that some positive power vanishes on Y, then f vanishes on Y. In other words: if $f^m \in I(Y)$ for some $m > 0$, then $f \in I(Y)$. This suggests:

PROPOSITION-DEFINITION 1.4. *Let R be a ring (as always commutative and with 1) and let $J \subset R$ be an ideal. Then the set of $a \in R$ with the property that $a^m \in J$ for some $m > 0$ is an ideal of R, called the* radical *of J and denoted $\sqrt{J}$.*

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

We say that the ring R is reduced *if the zero ideal (0) is a radical ideal (in other words, R has no nonzero nilpotents: if $a \in R$ is such that $a^m = 0$, then $a = 0$).*

PROOF. We show that $\sqrt{J}$ is an ideal. Let $a, b \in \sqrt{J}$ so that $a^m, b^n \in J$ for certain positive integers m, n. Then for every $r \in R$, $ra \in \sqrt{J}$, since $(ra)^m = r^m a^m \in J$. Similarly $a - b \in \sqrt{J}$, for $(a-b)^{m+n}$ is a linear combination of monomials that are multiples of a^m or b^n and hence lie in J. □

EXERCISE 6. Show that a prime ideal is a radical ideal.

Notice that J is a radical ideal if and only if R/J is reduced. The preceding shows that for every $Y \subset \mathbb{A}^n$, $I(Y)$ is a radical ideal, so that $A(Y)$ is reduced. The dictionary between algebra and geometry begins in a more substantial manner with

THEOREM 1.5 (Hilbert's Nullstellensatz). *For every ideal $J \subset k[x_1, \dots, x_n]$ we have $I(Z(J)) = \sqrt{J}$.*

We inclusion $\supset$ is clear; the hard part is the opposite inclusion (which says that if $f \in k[x_1, \dots, x_n]$ vanishes on $Z(J)$, then $f^m \in J$ for some positive integer m). We postpone its proof, but we discuss some of the consequences.

COROLLARY 1.6. *Let $Y \subset \mathbb{A}^n$ be closed. Then the maps I_Y and Z_Y restrict to bijections:*

$$\{\textit{closed subsets of } Y\} \leftrightarrow \{\textit{radical ideals of } A(Y)\}.$$

These bijections are inclusion reversing and each others inverse.

PROOF. We first prove this for $Y = \mathbb{A}^n$. We already observed that for every closed subset X of $\mathbb{A}^n$ we have $Z(I(X)) = X$. The Nullstellensatz says that for a radical ideal $J \subset k[x_1, \dots, x_n]$, we have $I(Z(J)) = J$.

An ideal of $A(Y)$ is of the form $J/I(Y)$. This is a radical ideal if and only if J is one. So the property also follows for an arbitrary closed Y. □

Let $\mathfrak{m}$ be a maximal ideal of $k[x_1, \ldots, x_n]$. Such an ideal is certainly radical as it is a prime ideal and so it is also maximal among the radical ideals that are distinct from $k[x_1, \ldots, x_n]$. Hence it is of the form $I(Y)$ for a closed subset Y. Since the empty subset of $\mathbb{A}^n$ is defined by the radical ideal $k[x_1, \ldots, x_n]$, Corollary 1.6 implies that Y will be nonempty and minimal for this property. In other words, Y is a singleton $\{y\}$ (and if $y = (a_1, \ldots, a_n)$, then $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$, by Exercise 4). Thus the above correspondence provides a bijection between the points of $\mathbb{A}^n$ and the maximal ideals of $\mathbb{A}^n$. If we are given a closed subset $Y \subset \mathbb{A}^n$ and a point $y \in \mathbb{A}^n$, then $y \in Y$ if and only if the maximal ideal defined by y contains $I(Y)$. But a maximal ideal containing $I(Y)$ is the preimage of a maximal ideal in $A(Y) = k[x_1, \ldots, x_n]/I(Y)$. We conclude that points of Y correspond to maximal ideals of $A(Y)$. Via this (or a very similar) correspondence, algebraic geometry seeks to express geometric properties of Y in terms of algebraic properties of $A(Y)$ and vice versa. In the end we want to forget about the ambient $\mathbb{A}^n$ completely.

2. Irreducibility and decomposition

We introduce a property which for most topological spaces is of little interest, but as we will see, is useful and natural for the Zariski topology.

DEFINITION 2.1. Let Y be a topological space. We say that Y is *irreducible* if it is nonempty and cannot be written as the union of two closed subsets $\neq Y$. An *irreducible component* of Y is a maximal irreducible subset of Y.

EXERCISE 7. Prove that an irreducible Hausdorff space must consist of a single point. Prove also that an infinite set with the cofinite topology is irreducible.

EXERCISE 8. Let $G_1, \ldots, G_s$ be closed subsets of a topological space Y. Prove that any irreducible subset of $G_1 \cup \cdots \cup G_s$ is contained in some G_i.

EXERCISE 9. This exercise has been scrapped.

LEMMA 2.2. *Let Y be a topological space.*

(i) *If Y is irreducible, then every nonempty open subset of Y is dense in Y and irreducible.*
(ii) *Conversely, if $C \subset Y$ is an irreducible subspace, then $\bar{C}$ is also irreducible. In particular, an irreducible component of Y is always closed in Y.*

PROOF. (i) Suppose Y is irreducible and let $U \subset Y$ be open and nonempty. Then Y is the union of the two closed subspaces $Y - U$ and $\bar{U}$. Since Y is irreducible, and $Y - U \neq Y$, we must have $\bar{U} = Y$. So U is dense in Y. To see that U is irreducible, suppose that U is the union of two subsets that are both closed in U. These subsets will be of the form $G_i \cap U$ with G_i closed in Y. Then $G_1 \cup G_2$ is a closed subset of Y which contains U. Since $\bar{U} = Y$, it follows that $G_1 \cup G_2 = Y$. The irreducibility of Y implies that one of the G_i (say G_1) equals Y and then $U = G_1 \cap U$.

(ii) Let $C \subset Y$ be irreducible (and hence nonempty). If $\bar{C}$ is written as a union of two closed subsets G_1, G_2 of Y, then C is the union of the two subsets $G_1 \cap C$ and $G_2 \cap C$ that are both closed in C, and so one of these, say $G_1 \cap C$, equals C. This means that $G_1 \supset C$ and hence $G_1 \supset \bar{C}$. So $\bar{C}$ is irreducible. □

The following proposition tells us what irreducibility amounts to in the Zariski topology.

PROPOSITION 2.3. *A closed subset $Y \subset \mathbb{A}^n$ is irreducible if and only if $I(Y)$ is a prime ideal (which, we recall, is equivalent to: $A(Y) = k[x_1, \ldots, x_n]/I(Y)$ is a domain).*

PROOF. Suppose Y is irreducible and $f, g \in k[x_1, \ldots, x_n]$ are such that $fg \in I(Y)$. Then $Y \subset Z(fg) = Z(f) \cup Z(g)$. Since Y is irreducible, Y is contained in $Z(f)$ or in $Z(g)$. So $f \in I(Y)$ or $g \in I(Y)$, proving that $I(Y)$ is a prime ideal.

Suppose $I(Y)$ is a prime ideal, but that Y is the union of two closed subsets Y_1 and Y_2 that are both $\neq Y$. Since $Y_i \neq Y$, there exists a $f_i \in I(Y_i) - I(Y)$. Then $f_1 f_2$ vanishes on $Y_1 \cup Y_2 = Y$, so that $f_1 f_2 \in I(Y)$. The fact $I(Y)$ is a prime ideal implies that one of f_1 and f_2 is in $I(Y)$. Whence a contradiction. □

One of our first aims is to prove that the irreducible components of any closed subset $Y \subset \mathbb{A}^n$ are finite in number and have Y as their union. This may not sound very surprising, but we will see that this reflects some nonobvious algebraic properties. Let us first consider the case of a hypersurface. Since we are going to use the fact that $k[x_1, \ldots, x_n]$ is a unique factorization domain, we begin with recalling that notion:

DEFINITION 2.4. We say that R is a *unique factorization domain* if R has no zero divisors and every principal ideal $(a) := Ra$ in R which is neither the zero ideal nor all of R is in unique manner a product of principal prime ideals: $(a) = (p_1)(p_2)\cdots(p_s)$ (so the ideals $(p_1), \ldots, (p_s)$ are unique up to order).

Observe that the principal ideal generated by $p \in R$ is prime if and only if for any factoring of p, $p = p'p''$, one of the factors must be a unit and that the identity $(a) = (p_1)(p_2)\cdots(p_s)$ amounts to the statement that a is a unit times $p_1 p_2 \cdots p_s$. The factors are then unique up to order and multiplication by a unit.

For a field (which has no proper principal ideals distinct from (0)) the imposed condition is empty and hence a field is automatically unique factorization domain. A more substantial example (that motivated this notion in the first place) is $\mathbb{Z}$: a principal prime ideal of $\mathbb{Z}$ is of the form (p), with p a prime number. Every integer $n \geq 2$ has a unique prime decomposition and so $\mathbb{Z}$ is a unique factorization domain.

A basic theorem in the theory of rings asserts that if R is a unique factorization domain, then so is its polynomial ring $R[x]$. This implies for instance (with induction on n) that $R[x_1, \ldots, x_n]$ is one. Indeed, in the case when R is a field (think of our k), then a nonzero principal ideal of this ring is prime precisely when it is generated by an irreducible polynomial of positive degree and every $f \in R[x_1, \ldots, x_n]$ of positive degree then can be written as a product of irreducible polynomials: $f = f_1 f_2 \cdots f_s$, a factorization that is unique up to order and multiplication of each f_i by a nonzero element of R.

The following proposition connects two notions of irreducibility.

PROPOSITION 2.5. *If $f \in k[x_1, \ldots, x_n]$ is irreducible, then the hypersurface $Z(f)$ it defines is irreducible. If $f \in k[x_1, \ldots, x_n]$ is of positive degree and $f = f_1 f_2 \cdots f_s$ is a factoring into irreducible polynomials, then $Z(f_1), \ldots, Z(f_s)$ are the irreducible components of $Z(f)$ and their union equals $Z(f)$ (but we are not claiming that the $Z(f_i)$'s are pairwise distinct). In particular, a hypersurface is the union of its irreducible components; these irreducible components are hypersurfaces and finite in number.*

PROOF. If $f \in k[x_1, \ldots, x_n]$ is irreducible, then f generates a prime ideal and so $Z(f)$ is an irreducible hypersurface by Proposition 2.3.

If $f \in k[x_1, \ldots, x_n]$ is of positive degree and $f = f_1 f_2 \cdots f_s$ is as in the proposition, then it is clear that $Z(f) = Z(f_1) \cup \cdots \cup Z(f_s)$ with each $Z(f_i)$ irreducible. To see that $Z(f_i)$ is an irreducible component of $Z(f)$, suppose that $C \subset Z(f)$ is irreducible. By Exercise 8, C is contained in some $Z(f_i)$. Since C is a maximal irreducible subset of $Z(f)$, it follows that we then must have equality: $C = Z(f_i)$. It remains to observe that if any inclusion relation $Z(f_i) \subset Z(f_j)$ is necessarily an identity (prove this yourself) so that each $Z(f_i)$ is already maximal and hence in irreducible component. □

The discussion of the general case begins with the rather formal

LEMMA 2.6. *For a partially ordered set $(A, \leq)$ the following are equivalent:*

(i) *$(A, \leq)$ satisfies the* ascending chain condition*: every ascending chain $a_1 \leq a_2 \leq a_3 \leq \cdots$ becomes stationary: $a_n = a_{n+1} = \cdots$ for n sufficiently large.*

(ii) *Every nonempty subset $B \subset A$ has a maximal element, that is, an element $b_0 \in B$ such that there is* no *$b \in B$ with $b > b_0$.*

PROOF. (i)⇒(ii). Suppose $(A, \leq)$ satisfies the ascending chain condition and let $B \subset A$ be nonempty. Choose $b_1 \in B$. If b_1 is maximal, we are done. If not, then there exists a $b_2 \in B$ with $b_2 > b_1$. We repeat the same argument for b_2. We cannot indefinitely continue in this manner because of the ascending chain condition.

(ii)⇒(i). If $(A, \leq)$ satisfies (ii), then the set of members of any ascending chain has a maximal element, in other words, the chain becomes stationary. □

If we replace $\leq$ by $\geq$, then we obtain the notion of the *descending chain condition* and we find that this property is equivalent to: every nonempty subset $B \subset A$ has a minimal element. These properties appear in the following pair of definitions.

DEFINITIONS 2.7. We say that a ring R is *noetherian* if its collection of ideals satisfies the ascending chain condition.

We say that a topological space Y is *noetherian* if its collection of closed subsets satisfies the descending chain condition.

EXERCISE 10. Prove that a subspace of a noetherian space is noetherian. Prove also that a ring quotient of a noetherian ring is noetherian.

EXERCISE 11. Prove that a noetherian space is compact: every covering of such a space by open subsets contains a finite subcovering.

The interest of the noetherian property is that it is one which is possessed by almost all the rings we encounter and that it implies many finiteness properties without which we are often unable to go very far. Let us give a nonexample first: the ring R of holomorphic functions on $\mathbb{C}$ is not noetherian: if I_k denotes the ideal of $f \in R$ vanishing on all the integers $\geq k$, then $I_1 \subset I_2 \subset \cdots$ is a strictly ascending chain of ideals in R.

Obviously a field is noetherian. The ring $\mathbb{Z}$ is noetherian: if $I_1 \subset I_2 \subset \cdots$ is an ascending chain of ideals in $\mathbb{Z}$, then $\cup_{s=1}^{\infty} I_s$ is an ideal of $\mathbb{Z}$, hence of the form (n) for some $n \in \mathbb{Z}$. But if s is such that $n \in I_s$, then clearly the chain is stationary as of index s. (This argument only used the fact that any ideal in $\mathbb{Z}$ is generated by a single element, i.e., that $\mathbb{Z}$ is a principal ideal domain.) That most rings we know are noetherian is a consequence of

THEOREM 2.8 (Hilbert's basis theorem). *If R is a noetherian ring, then so is $R[x]$.*

As with the Nullstellensatz, we postpone the proof and discuss some of its consequences first.

COROLLARY 2.9. *If R is a noetherian ring (for example, a field) then so is every finitely generated R-algebra. Also, the space $\mathbb{A}^n$ (and hence any closed subset of $\mathbb{A}^n$) is noetherian.*

PROOF. The Hilbert basis theorem implies (with induction on n) that the ring $R[x_1, \ldots, x_n]$ is noetherian. By Exercise 10, every quotient ring $R[x_1, \ldots, x_n]/I$ is then also noetherian. But a finitely generated R-algebra is (by definition actually) isomorphic to some such quotient and so the first statement follows.

Suppose $\mathbb{A}^n \supset Y_1 \supset Y_2 \supset \cdots$ is a descending chain of closed subsets. Then $(0) \subset I(Y_1) \subset I(Y_2) \subset \cdots$ is an ascending chain of ideals. As the latter becomes stationary, so will become the former. □

PROPOSITION 2.10. *If Y is noetherian space, then its irreducible components are finite in number and their union equals Y.*

PROOF. Suppose Y is a noetherian space. We first show that every closed subset can be written as a finite union of closed irreducible subsets. First note that the empty set has this property, for a union with empty index set is empty. Let B be the collection of closed subspaces of Y for which this is not possible, i.e., that *cannot* be written as a finite union of closed irreducible subsets. Suppose that B is nonempty. According to 2.6 this collection has a minimal element, Z, say. This Z must be nonempty and cannot be irreducible. So Z is the union of two proper closed subsets Z' and Z''. The minimality of Z implies that neither Z' nor Z'' is in B and so both Z' and Z'' can be written as a finite union of closed irreducible subsets. But then so can Z and we get a contradiction.

In particular, there exist closed irreducible subsets $Y_1, \ldots, Y_k$ of Y such that $Y = Y_1 \cup \cdots \cup Y_k$ (if $Y = \emptyset$, take $k = 0$). We may of course assume that no Y_i is contained in some Y_j with $j \neq i$ (otherwise, omit Y_i). It now remains to prove that the Y_i's are the irreducible components of Y, that is, we must show that every irreducible subset C of Y is contained in some Y_i. But this follows from an application of Exercise 8. □

If we apply this to $\mathbb{A}^n$, then we find that every subset $Y \subset \mathbb{A}^n$ has a finite number of irreducible components, the union of which is all of Y. If Y is closed in $\mathbb{A}^n$, then so is every irreducible component of Y and according to Proposition 2.3 any such irreducible component is defined by a prime ideal. This allows us to recover the irreducible components of a closed subset $Y \subset \mathbb{A}^n$ from its coordinate ring:

COROLLARY 2.11. *Let $Y \subset \mathbb{A}^n$ be a closed subset. If C is an irreducible component of Y, then the image $I_Y(C)$ of $I(C)$ in $A(Y)$ is a minimal prime ideal of $A(Y)$ and any minimal prime ideal of $A(Y)$ is so obtained: we thus get a bijective correspondence between the irreducible components of Y and the minimal prime ideals of $A(Y)$.*

PROOF. Let C be a closed subset of Y and let $I_Y(C)$ be the corresponding ideal of $A(Y)$. Now C is irreducible if and only if $I(C)$ is a prime ideal of $k[x_1, \ldots, x_n]$, or what amounts to the same, if and only if $I_Y(C)$ is a prime ideal of $A(Y)$. It is

an irreducible component if C is maximal for this property, or what amounts to the same, if $I_Y(C)$ is minimal for the property of being a prime ideal of $A(Y)$. □

EXAMPLE 2.12. First consider the set $C := \{(t, t^2, t^3) \in \mathbb{A}^3 \mid t \in k\}$. This is a closed subset of $\mathbb{A}^3$: if we use (x, y, z) instead of (x_1, x_2, x_3), then C is the common zero set of $y - x^2$ and $z - x^3$. Now the inclusion $k[x] \subset k[x, y, z]$ composed with the ring quotient $k[x, y, z] \to k[x, y, z]/(y - x^2, z - x^3)$ is easily seen to be an isomorphism. Since $k[x]$ has no zero divisors, $(y - x^2, z - x^3)$ must be a prime ideal. So C is irreducible and $I(C) = (y - x^2, z - x^3)$.

We now turn to the closed subset $Y \subset \mathbb{A}^3$ defined by $xy - z = 0$ and $y^3 - z^2 = 0$. Let $p = (x, y, z) \in Y$. If $y \neq 0$, then we put $t := z/y$; from $y^3 = x^2$, it follows that $y = t^2$ and $z = t^3$ and $xy = z$ implies that $x = t$. In other words, $p \in C$ in that case. If $y = 0$, then $z = 0$, in other words p lies on the x-axis. Conversely, any point on the x-axis lies in Y. So Y is the union of C and the x-axis and these are the irreducible components of Y.

We briefly discuss the corresponding issue in commutative algebra. We begin with recalling the notion of localization and we do this in the generality that is needed later.

2.13. LOCALIZATION. Let R be a ring and let S be a *multiplicative subset* of R: $1 \in S$, $0 \notin S$ and S closed under multiplication. Then a ring $S^{-1}R$, together with a ring homomorphism $R \to S^{-1}R$ is defined as follows: an element of $S^{-1}R$ is written as a formal fraction r/s, with $r \in R$ and $s \in S$, with the understanding that $r/s = r'/s'$ if and only if $s''(s'r - sr') = 0$ for some $s'' \in S$. This is a ring indeed: multiplication and subtraction is defined as for ordinary fractions: $r/s.r'/s' = (rr')/(ss')$ and $r/s - r'/s' = (s'r - sr')/(ss')$; it has $0/1$ as zero and $1/1$ as unit element. Since $0 \notin S$, we have $0/1 \neq 1/1$. The homomorphism $R \to S^{-1}R$ is simply $r \mapsto r/1$. Notice that it maps any $s \in S$ to an invertible element of $S^{-1}R$: the inverse of $s/1$ is $1/s$. In a sense (made precise in part (b) of Exercise 12 below) the ring homomorphism $R \to S^{-1}R$ is universal for that property. This construction is called the *localization away from* S.[3]

It is clear that if S does not contain zero divisors, then $r/s = r'/s'$ if and only if $s'r - sr' = 0$; in particular, $r/1 = r'/1$ if and only if $r = r'$, so that $R \to S^{-1}R$ is then injective. If we take S maximal for this property, namely take it to be the set of nonzero divisors of R (which is indeed multiplicative), then $S^{-1}R$ is called the *fraction ring* $\mathrm{Frac}(R)$ of R. In case R is a domain, $S = R - \{0\}$ and so $\mathrm{Frac}(R)$ is a field, the *fraction field* of R. This gives the following corollary, which hints to the importance of prime ideals in the subject.

COROLLARY 2.14. *An ideal $\mathfrak{p}$ of a ring R is a prime ideal if and only if it is the kernel of a ring homomorphism from R to a field*

PROOF. It is clear that the kernel of a ring homomorphism from R to a field is always a prime ideal. Conversely, if $\mathfrak{p}$ is a prime ideal, then it is the kernel of the composite $R \to R/\mathfrak{p} \hookrightarrow \mathrm{Frac}(R/\mathfrak{p})$. □

But the case of interest here is when we are given some $a \in R$ which is not nilpotent. Then we can take $S = \{a^n \mid n \geq 0\}$ in which case we usually write $R[1/a]$ for $S^{-1}R$.

EXERCISE 12. Let R be a ring and let S be a multiplicative subset of R.

(a) What is the the kernel of $R \to S^{-1}R$?
(b) Prove that a ring homomorphism $\phi : R \to R'$ with the property that $\phi(s)$ is invertible for every $s \in S$ factors in a unique manner through $S^{-1}R$.

[3] It is sometimes useful to allow $0 \in S$. We then stipulate that $S^{-1}R$ is the zero ring.

(c) Consider the polynomial ring $R[x_s : s \in S]$ and the homomorphism of R-algebras $R[x_s : s \in S] \to S^{-1}R$ that sends x_s to $1/s$. Prove that this homomorphism is surjective and that its kernel consists of the $f \in R[x_s : s \in S]$ which after multiplication by an element of S lie in the ideal generated the degree one polynomials $sx_s - 1$, $s \in S$.

EXERCISE 13. Let R be a ring and let $\mathfrak{p}$ be a prime ideal of R.

(a) Prove that the complement $R - \mathfrak{p}$ is a multiplicative system. The resulting localization $(R - \mathfrak{p})^{-1}R$ is called the *localization at* $\mathfrak{p}$ and is usually denoted $R_{\mathfrak{p}}$.
(b) Prove that $\mathfrak{p}R_{\mathfrak{p}}$ is a maximal ideal of $R_{\mathfrak{p}}$ and that it is the only maximal ideal of $R_{\mathfrak{p}}$. (A ring with a unique maximal ideal is called a *local ring*.)
(c) Prove that the localization map $R \to R_{\mathfrak{p}}$ drops to an isomorphism of fields $\mathrm{Frac}(R/\mathfrak{p}) \to R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$.
(d) Work this out for $R = \mathbb{Z}$ and $\mathfrak{p} = (p)$, where p is a prime number.
(e) Same for $R = k[x, y]$ and $\mathfrak{p} = (x)$.

LEMMA 2.15. *Let R be a ring. Then the intersection of all the prime ideals of R is the ideal of nilpotents $\sqrt{(0)}$ of R. Equivalently, for every nonnilpotent $a \in R$, there exists a ring homomorphism from R to a field that is nonzero on a.*

PROOF. It is easy to see that a nilpotent element lies in every prime ideal. Now for nonnilpotent $a \in R$ consider the homomorphism $R \to R[1/a]$. The ring $R[1/a]$ has a maximal ideal[4] and hence admits a ring homomorphism to some field F: $\phi : R[1/a] \to F$. Then the kernel of the composite $R \to R[1/a] \to F$ is a prime ideal and a is not in this kernel (for its image is invertible with inverse $\phi(1/a)$). □

EXERCISE 14. Let R be a ring. Prove that the intersection of all the maximal ideals of a ring R consists of the $a \in R$ for which $1 + aR \subset R^\times$ (i.e., $1 + ax$ is invertible for every $x \in R$). You may use the fact that every proper ideal of R is contained in a maximal ideal.

We can do better if R is noetherian. The following proposition is the algebraic counterpart of Proposition 2.10. Note the similarity between the proofs.

PROPOSITION 2.16. *Let R be a noetherian ring. Then any radical ideal of R is an intersection of finitely many prime ideals. Also, the minimal prime ideals of R are finite in number and their intersection is equal to the ideal of nilpotents $\sqrt{(0)}$.*

PROOF. Let B be the collection of the radical ideals $I \subsetneq R$ that can *not* be written as an intersection of finitely many prime ideals and suppose that B is nonempty. Since R is noetherian, B contains a maximal member I_0. We derive a contradiction as follows.

Since I_0 cannot be a prime ideal, there exist $a_1, a_2 \in R - I_0$ with $a_1a_2 \in I_0$. Consider the radical ideal $J_i := \sqrt{I_0 + Ra_i}$. We claim that $J_1 \cap J_2 = I_0$. The inclusion $\supset$ is obvious and $\subset$ is seen as follows: if $a \in J_1 \cap J_2$, then for $i = 1, 2$, there exists an $n_i > 0$ such that $a^{n_i} \in I_0 + Ra_i$. Hence $a^{n_1+n_2} \in (I_0 + Ra_1)(I_0 + Ra_2) = I_0$, so that $a \in I_0$. Since J_i strictly contains I_0, it does not belong to B. In other words,

[4] Every ring has a maximal ideal. For noetherian rings, which are our main concern, this is obvious, but in general this follows with transfinite induction, the adoption of which is equivalent to the adoption of the axiom of choice.

J_i is an intersection of finitely many prime ideals. But then so is $J_1 \cap J_2 = I_0$ and we get a contradiction.

We thus find that $\sqrt{(0)} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s$ for certain prime ideals $\mathfrak{p}_i$. We may of course assume that no $\mathfrak{p}_i$ contains some $\mathfrak{p}_j$ with $j \neq i$ (otherwise, omit $\mathfrak{p}_i$). It now remains to prove that every prime ideal $\mathfrak{p}$ of R contains some $\mathfrak{p}_i$. If that is not the case, then for $i = 1, \ldots, s$ there exists a $a_i \in \mathfrak{p}_i - \mathfrak{p}$. But then $a_1 a_2 \cdots a_s \in \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s = \sqrt{(0)} \subset \mathfrak{p}$ and since $\mathfrak{p}$ is a prime ideal, some factor a_i lies in $\mathfrak{p}$. This is clearly a contradiction. □

EXERCISE 15. Let J be an ideal of the ring R. Show that $\sqrt{J}$ is the intersection of all the prime ideals that contain J. Prove that in case R is noetherian, the prime ideals that are minimal for this property are finite in number and that their common intersection is still $\sqrt{J}$. What do we get for $R = \mathbb{Z}$ and $J = \mathbb{Z}n$?

3. Finiteness properties and the Hilbert theorems

The noetherian property in commutative algebra is best discussed in the context of modules, even if one's interest is only in rings. We fix a ring R and first recall the notion of an R-module.

The notion of an R-module is the natural generalization of a K-vector space (where K is some field). Let us observe that if M is an (additively written) abelian group, then the set $\mathrm{End}(M)$ of group homomorphisms $M \to M$ is a ring for which subtraction is pointwise defined and multiplication is composition (so if $f, g \in \mathrm{End}(M)$, then $f - g : m \in M \mapsto f(m) - g(m)$ and $fg : m \mapsto f(g(m))$); clearly the zero element is the zero homomorphism and the unit element is the identity. It only fails to obey our convention in the sense that this ring is usually noncommutative. We only introduced it in order to be able state succinctly:

DEFINITION 3.1. An *R-module* is an abelian group M, equipped with a ring homomorphism $R \to \mathrm{End}(M)$.

So any $r \in R$ defines a homomorphism $M \to M$; we usually denote the image of $m \in M$ simply by rm. If we write out the properties of an R-module structure in these terms, we get: $r(m_1 - m_2) = rm_1 - rm_2$, $(r_1 - r_2)m = r_1 m - r_2 m$, $1.m = m$, $r_1(r_2 m) = (r_1 r_2)m$. If R happens to be field, then we see that an R-module is the same thing as an R-vector space.

The notion of an R-module is quite ubiquitous if you think about it. A simple example is any ideal $I \subset R$. Any abelian group M is in a natural manner a $\mathbb{Z}$-module. A $\mathbb{R}[x]$-module can be understood as an real linear space V (an $\mathbb{R}$-module) endowed with an endomorphism (the image of x in $\mathrm{End}(V)$). A more involved example is the following: if X is a manifold, f is a C^∞-function on X and ω a C^∞ differential p-form on X, then $f\omega$ is also a C^∞ differential p-form on X. Thus the linear space of C^∞-differential forms on X of a fixed degree p is naturally a module over the ring of C^∞-functions on X.

Here are a few companion notions, followed by a brief discussion.

3.2. In what follows is M an R-module. A map $f : M \to N$ from M to an R-module N is called a *R-homomorphism* if it is a group homomorphism with the property that $f(rm) = rf(m)$ for all $r \in R$ and $m \in M$. If f is also bijective, then we call it an *R-isomorphism*; in that case its inverse is also a homomorphism of R-modules.

For instance, given a ring homomorphism $f : R \to R'$, then R' becomes an R-module by $rr' := f(r)r'$ and this makes f a homomorphism of R-modules.

A subset $N \subset M$ is called an *R-submodule* of M if it is a subgroup and $rn \in N$ for all $r \in R$ and $n \in N$. Then the group quotient M/N is in a unique manner a R-module in such a way that the quotient map $M \to M/N$ is a R-homomorphism: we let $r(m+N) := rm+N$

for $r \in R$ and $m \in M$. Notice that a R-submodule of R (here we regard R as a R-module) is the same thing as an ideal of R.

Given a subset $S \subset M$, then the set of elements $m \in M$ that can be written as $r_1 s_1 + \cdots + r_k s_k$ with $r_i \in R$ and $s_i \in S$ is a R-submodule of M. We call it the *R-submodule of M generated by S* and we shall denote it by RS.

If there exists a finite set $S \subset M$ such that $M = RS$, then we say that M is *finitely generated* as an R-module.

DEFINITION 3.3. We say that an R-module M is *noetherian* if the collection of R-submodules of M satisfies the ascending chain condition: any ascending chain of R-submodules $N_1 \subset N_2 \subset \cdots$ becomes stationary.

It is clear that then every quotient module of a noetherian module is also noetherian. The noetherian property of R as a ring (as previously defined) coincides with this property of R as an R-module.

The following two propositions provide the passage from the noetherian property to finite generation:

PROPOSITION 3.4. *An R-module M is noetherian if and only if every R-submodule of M is finitely generated as an R-module.*

PROOF. Suppose that M is a noetherian R-module and let $N \subset M$ be a R-submodule. The collection of finitely generated R-submodules of M contained in N is nonempty. Hence it has a maximal element N_0. If $N_0 = N$, then N is finitely generated. If not, we run into a contradiction: just choose $x \in N - N_0$ and consider $N_0 + Rx$. This is a R-submodule of N. It is finitely generated (for N_0 is), which contradicts the maximal character of N_0.

Suppose now that every R-submodule of M is finitely generated. If $N_1 \subset N_2 \subset \cdots$ is an ascending chain of R-modules, then the union $N := \cup_{i=1}^{\infty} N_i$ is a R-submodule. Let $\{s_1, \ldots, s_k\}$ be a finite set of generators of N. If $s_\kappa \in N_{i_\kappa}$, and $j := \max\{i_1, \ldots, i_k\}$, then it is clear that $N_j = N$. So the chain becomes stationary as of index j. □

PROPOSITION 3.5. *Suppose that R is a noetherian ring. Then every finitely generated R-module M is noetherian.*

PROOF. By assumption $M = RS$ for a finite set $S \subset M$. We prove the proposition by induction on the number of elements of S. If $S = \emptyset$, then $M = \{0\}$ and there is nothing to prove. Suppose now $S \neq \emptyset$ and choose $s \in S$, so that our induction hypothesis applies to $M' := RS'$ with $S' = S - \{s\}$: M' is noetherian. But so is M/M', for it is a quotient of the noetherian ring R via the surjective R-module homomorphism $R \to M/M'$, $r \mapsto rs + M'$.

Let now $N_1 \subset N_2 \subset \cdots$ be an ascending chain of R-submodules of M. Then $N_1 \cap M' \subset N_2 \cap M' \subset \cdots$ becomes stationary, say as of index j_1. Hence we only need to be concerned with the stabilization of the submodules $N_k/(N_k \cap M')$ of M/M'. These stabilize indeed (say as of index j_2), since M/M' is noetherian. So the original chain $N_1 \subset N_2 \subset \cdots$ stabilizes as of index $\max\{j_1, j_2\}$. □

We are now sufficiently prepared for the proofs of the Hilbert theorems. They are jewels of elegance and efficiency.

We will use the notion of initial coefficient of a polynomial, which we recall. Given a ring R, then every nonzero $f \in R[x]$ is uniquely written as $r_d x^d + r_{d-1} x^{d-1} + \cdots + r_0$ with $r_d \neq 0$. We call $r_d \in R$ the *initial coefficient* of f and

denote it by $\mathrm{in}(f)$. For the zero polynomial, we simply define this to be $0 \in R$. Notice that $\mathrm{in}(f)\,\mathrm{in}(g)$ equals $\mathrm{in}(fg)$ when nonzero.

PROOF OF THEOREM 2.8. The assumption is here that R is a noetherian ring. In view of Proposition 3.4 we must show that every ideal I of $R[x]$ is finitely generated. Consider the subset $\mathrm{in}(I) := \{\mathrm{in}(f) : f \in I\}$ of R. We first show that this is an ideal of R. If $r \in R$, $f \in I$, then $r\,\mathrm{in}(f)$ equals $\mathrm{in}(rf)$ when nonzero and since $rf \in I$, it follows that $r\,\mathrm{in}(f) \in I$. If $f, g \in I$ with $d := \deg(f) - \deg(g) \geq 0$, then $\mathrm{in}(f) - \mathrm{in}(g) = \mathrm{in}(f - t^d g)$. So $\mathrm{in}(I)$ is an ideal as asserted.

Since R is noetherian, $\mathrm{in}(I)$ is finitely generated: there exist $f_1, \ldots, f_k \in I$ such that $\mathrm{in}(I) = R\,\mathrm{in}(f_1) + \cdots + R\,\mathrm{in}(f_k)$. Let d_i be the degree of f_i, $d_0 := \max\{d_1, \ldots, d_k\}$ and $R[x]_{<d_0}$ the set of polynomials of degree $< d_0$. So $R[x]_{<d_0}$ is the R-submodule of $R[x]$ generated by $1, x, \ldots, x^{d_0-1}$. We claim that

$$I = R[x]f_1 + \cdots + R[x]f_k + (I \cap R[x]_{<d_0}),$$

in other words, that every $f \in I$ is modulo $R[x]f_1 + \cdots + R[x]f_k$ a polynomial of degree $< d_0$. We prove this with induction on the degree d of f. Since for $d < d_0$ there is nothing to prove, assume that $d \geq d_0$. We have $\mathrm{in}(f) = r_1\,\mathrm{in}(f_1) + \cdots + r_k\,\mathrm{in}(f_k)$ for certain $r_1, \ldots r_k \in R$, where we may of course assume that every term $r_i\,\mathrm{in}(f_i)$ is nonzero and hence equal to $\mathrm{in}(r_i f_i)$. Then $\mathrm{in}(f)$ equals $\sum_i \mathrm{in}(r_i f_i) = \mathrm{in}(\sum_i r_i f_i x^{d-d_i})$. So $f - \sum_i r_i f_i x^{d-d_i}$ is an element of I of degree $< d$ and hence lies in $R[x]f_1 + \cdots + R[x]f_k + (I \cap R[x]_{<d_0})$ by our induction hypothesis. Hence so does f.

Our claim implies the theorem: $R[x]_{<d_0}$ is a finitely generated R-module and so a noetherian R-module by Proposition 3.5. Hence the R-submodule $I \cap R[x]_{<d_0}$ is a finitely generated R-module by Proposition 3.4. If $\{f_{k+1}, \ldots, f_{k+l}\}$ is a set of R-generators of $I \cap R[x]_{<d_0}$, then $\{f_1, \ldots, f_{k+l}\}$ is a set of $R[x]$-generators of I. □

For the Nullstellensatz we need another finiteness result.

PROPOSITION 3.6 (Artin-Tate). *Let R be a noetherian ring, B an R-algebra and $A \subset B$ an R-subalgebra. Assume that B is finitely generated as an A-module. Then A is finitely generated as an R-algebra if and only if B is so.*

PROOF. By assumption there exist $b_1, \ldots, b_m \in B$ such that $B = \sum_{i=1}^m A b_i$.

If there exist $a_1, \ldots, a_n \in A$ which generate A as an R-algebra (which means that $A = R[a_1, \ldots, a_n]$), then $a_1, \ldots, a_n, b_1, \ldots, b_m$ generate B as an R-algebra.

Suppose, conversely, that there exists a finite subset of B which generates B as a R-algebra. By adding this subset to $b_1, \ldots, b_m$, we may assume that $b_1, \ldots, b_m$ also generate B as an R-algebra. Then every product $b_i b_j$ can be written as an A-linear combination of $b_1, \ldots, b_m$:

$$b_i b_j = \sum_{k=1}^m a_{ij}^k b_k, \quad a_{ij}^k \in A.$$

Let $A_0 \subset A$ be the R-subalgebra of A generated by all the (finitely many) coefficients a_{ij}^k. This is a noetherian ring by Corollary 2.9. It is clear that $b_i b_j \in \sum_k A_0 b_k$ and with induction it then follows that $B = R[b_1, \ldots, b_m] \subset \sum_k A_0 b_k$. So B is finitely generated as an A_0-module. Since A is an A_0-submodule of B, A is also finitely generated as an A_0-module by Proposition 3.4. It follows that A is a finitely generated R-algebra. □

This has a consequence for field extensions:

COROLLARY 3.7. *A field extension L/K is finite if and only if L is finitely generated as a K-algebra.*

PROOF. It is clear that if L is a finite dimensional K-vector space, then L is finitely generated as a K-algebra.

Suppose now $b_1, \dots, b_m \in L$ generate L as a K-algebra. We must show that every b_i is algebraic over K. Suppose that this is not the case. After renumbering we can and will assume that (for some $1 \leq r \leq m$) $b_1, \dots, b_r$ are algebraically independent over K and $b_{r+1}, \dots, b_m$ are algebraic over the quotient field $K(b_1, \dots, b_r)$ of $K[b_1, \dots, b_r]$. So L is a finite extension of $K(b_1, \dots, b_r)$. We apply Proposition 3.6 to $R := K$, $A := K(b_1, \dots, b_r)$ and $B := L$ and find that $K(b_1, \dots, b_r)$ is as a K-algebra generated by a finite subset $S \subset K(b_1, \dots, b_r)$. If g is a common denominator for the elements of S, then clearly $K(b_1, \dots, b_r) = K[b_1, \dots, b_r][1/g]$. Since $K(b_1, \dots, b_r)$ strictly contains $K[b_1, \dots, b_r]$, g must have positive degree. In particular, $1 + g \neq 0$, so that $1/(1+g) \in K(b_1, \dots, b_r)$ can be written as f/g^N, with $f \in K[b_1, \dots, b_r]$. Here we may of course assume that f is not divisible by g in $K[b_1, \dots, b_r]$. From the identity $f(1+g) = g^N$ we see that $N \geq 1$ (for g has positive degree). But then $f = g(-f + g^{N-1})$ shows that f is divisible by g. We thus get a contradiction. □

EXERCISE 16. Prove that a field which is finite generated as a ring (that is, isomorphic to a quotient of $\mathbb{Z}[x_1, \dots, x_n]$ for some n) is finite.

We deduce from the preceding corollary the Nullstellensatz.

PROOF OF THE NULLSTELLENSATZ 1.5. Let $J \subset k[x_1, \dots, x_n]$ be an ideal. We must show that $I(Z(J)) \subset \sqrt{J}$. This amounts to: for every $f \in k[x_1, \dots, x_n] - \sqrt{J}$ there exists a $p \in Z(J)$ for which $f(p) \neq 0$. Consider $k[x_1, \dots, x_n]/J$ and denote by $\bar{f} \in k[x_1, \dots, x_n]/J$ the image of f. Since $\bar{f}$ is not nilpotent, we have defined

$$A := (k[x_1, \dots, x_n]/J)[1/\bar{f}].$$

Notice that A is as a k-algebra generated by the images of $x_1, \dots, x_n$ and $1/\bar{f}$ (hence is finitely generated). Choose a maximal ideal $\mathfrak{m} \subset A$. Then the field $A/\mathfrak{m}$ is a finitely generated k-algebra and so by Corollary 3.7 a finite extension of k. But then it must be equal to k, since k is algebraically closed. Denote by $\phi : k[x_1, \dots, x_n] \to A \to A/\mathfrak{m} = k$ the corresponding surjection and put $p_i := \phi(x_i)$ and $p := (p_1, \dots, p_n) \in \mathbb{A}^n$. So if we view x_i as a function on $\mathbb{A}^n$, then $x_i(p) = p_i = \phi(x_i)$. The fact that ϕ is a homomorphism of k-algebras implies that it is given as 'evaluation in p': any $g \in k[x_1, \dots, x_n]$ takes in p the value $\phi(g)$. Since the kernel of ϕ contains J, every $g \in J$ will be zero in p, in other words, $p \in Z(J)$. On the other hand, $f(p) = \phi(f)$ is invertible, for it has the image of $1/\bar{f}$ in $A/\mathfrak{m} = k$ as its inverse. So $f(p) \neq 0$. □

4. The affine category

We begin with specifying the maps between closed subsets of affine spaces that we wish to consider.

DEFINITION 4.1. Let $X \subset \mathbb{A}^m$ and $Y \subset \mathbb{A}^n$ be closed subsets. We say that a map $f : X \to Y$ is *regular* if the components $f_1, \dots, f_n$ of f are regular functions on X (i.e., are given by the restrictions of polynomial functions to X).

Composition of a regular function on Y with f yields a regular function on X (for if we substitute in a polynomial of n variables $g(y_1, \dots, y_n)$ for every variable y_i a polynomial $f_i(x_1, \dots, x_m)$ of m variables, we get a polynomial of m variables). So f then induces a k-algebra homomorphism $f^* : A(Y) \to A(X)$. There is also a converse:

PROPOSITION 4.2. *Let be given closed subsets $X \subset \mathbb{A}^m$ and $Y \subset \mathbb{A}^n$ and a k-algebra homomorphism $\phi : A(Y) \to A(X)$. Then there is a unique regular map $f : X \to Y$ such that $f^* = \phi$.*

PROOF. Let $f_i := \phi(y_i|Y) \in A(X)$ $(i = 1, \dots, n)$ and define $f = (f_1, \dots, f_n) : X \to \mathbb{A}^n$, so that $f^* y_i = f_i = \phi(y_i|Y)$. If $j : Y \subset \mathbb{A}^n$ denotes the inclusion, then we can also write this as $f^* y_i = \phi j^* y_i$. In other words, the k-algebra homomorphisms $f^*, \phi j^* : k[y_1, \dots, y_n] \to A(X)$ coincide on the generators y_i. Hence they must be equal: $f^* = \phi j^*$. It follows that f^* is zero on $I(Y)$, which means that f takes its values in $Z(I(Y)) = Y$, and that the resulting map $A(Y) \to A(X)$ equals ϕ. □

The same argument shows that if $f : X \to Y$ and $g : Y \to Z$ are regular maps, then so is their composite $gf : X \to Z$. So we have a category (with objects the closed subsets and regular maps as defined above). In particular, we have a notion of isomorphism: a regular map $f : X \to Y$ is an *isomorphism* if is has a two-sided inverse $g : Y \to X$ which is also a regular map. This implies that $f^* : A(Y) \to A(X)$ has a two-sided inverse $g^* : A(X) \to A(Y)$ which is also an isomorphism of k-algebras, and hence is an isomorphism of k-algebras. Proposition 4.2 implies that conversely, an isomorphism of k-algebras $A(Y) \to A(X)$ comes from a unique isomorphism $X \to Y$.

We complete the picture by showing that any finitely generated *reduced* k-algebra A is isomorphic to some $A(Y)$; the preceding then shows that Y is unique up to isomorphism. Since A is finitely generated as a k-algebra, there exists a surjective k-algebra homomorphism $\phi : k[x_1, \dots, x_n] \to A$. If we put $I := \mathrm{Ker}(\phi)$, then ϕ induces an isomorphism $k[x_1, \dots, x_n]/I \cong A$. Put $Y := Z(I) \subset \mathbb{A}^n$. Since A is reduced, I is a radical ideal and hence equal to $I(Y)$ by the Nullstellensatz. It follows that ϕ factors through a k-algebra isomorphism $A(Y) \cong A$.

We may sum up this discussion in categorical language as follows.

PROPOSITION 4.3. *The map which assigns to a closed subset of some $\mathbb{A}^n$ its coordinate ring defines an anti-equivalence between the category of closed subsets of affine spaces (and regular maps between them as defined above) and the category of reduced finitely generated k-algebras (and k-algebra homomorphisms).*

EXAMPLE 4.4. Consider the regular map $f : \mathbb{A}^1 \to \mathbb{A}^2$, $f(t) = (t^2, t^3)$. The image of this map is the hypersurface Z defined by $x^3 - y^2 = 0$. This is a homeomorphism on the image for it is a bijection of sets that have both the cofinite topology. The inverse sends $(0, 0)$ to 0 and is on $Z - \{(0, 0)\}$ given by $(x, y) \mapsto y/x$. In order to determine whether the inverse is regular, we consider f^*. We have $A(Z) = k[x, y]/(x^3 - y^2)$, $A(\mathbb{A}^1) = k[t]$ and $f^* : k[x, y]/(x^3 - y^2) \to k[t]$ is given by $x \mapsto t^2, y \mapsto t^3$. This homomorphism is not surjective for its image misses $t \in k[t]$. So f is not an isomorphism.

EXAMPLE 4.5. An *affine-linear transformation* of k^n is of the form $x \in k^n \mapsto g(x) + a$, where $a \in k^n$ and $g \in \mathrm{GL}(n, k)$ is a linear transformation. Its inverse is $y \mapsto g^{-1}(y - a) = g^{-1}(y) - g^{-1}(a)$ and so of the same type. When we regard such an

affine linear transformation as a map from $\mathbb{A}^n$ to itself, then it is regular: its coordinates $(g_1, \ldots, g_n)$ are polynomials of degree one. So an affine-linear transformation is also an isomorphism of $\mathbb{A}^n$ onto itself. But if $n \geq 2$, not every isomorphism of $\mathbb{A}^n$ onto itself need to be of this form. For example, $(x, y) \mapsto (x, y + x^2)$ defines an automorphism of $\mathbb{A}^2$ with inverse $(x, y) \mapsto (x, y - x^2)$ (see also Exercise 18).

EXERCISE 17. Let $C \subset \mathbb{A}^2$ be the 'circle', defined by $x^2 + y^2 = 1$ and let $p_0 := (-1, 0) \in C$. For every $p = (x, y) \in C - \{p_0\}$, the line through p_0 and p has slope $f(p) = y/(x + 1)$. Denote by $\sqrt{-1} \in k$ a root of the equation $t^2 + 1 = 0$.

(a) Prove that when $\mathrm{char}(k) \neq 2$, f defines an isomorphism[5] onto $\mathbb{A}^1 - \{\pm\sqrt{-1}\}$.
(b) Consider the map $g : C \to \mathbb{A}^1$, $g(x, y) := x + \sqrt{-1}y$. Prove that when $\mathrm{char}(k) \neq 2$, g defines an isomorphism of C onto $\mathbb{A}^1 - \{0\}$.
(c) Prove that when $\mathrm{char}(k) = 2$, the defining polynomial $x^2 + y^2 - 1$ for C is the square of a degree one polynomial so that C is a line.

EXERCISE 18. Let $f_1, \ldots, f_n \in k[x_1, \ldots, x_n]$ be such that $f_1 = x_1$ and $f_i - x_i \in k[x_1, \ldots, x_{i-1}]$ for $i = 2, \ldots, x_n$. Prove that f defines an isomorphism $\mathbb{A}^n \to \mathbb{A}^n$.

4.6. QUADRATIC HYPERSURFACES IN CASE $\mathrm{char}(k) \neq 2$. Let $H \subset \mathbb{A}^n$ be a hypersurface defined by a polynomial of degree two:

$$f(x_1, \ldots, x_n) = \sum_{1 \leq i \leq j = n} a_{ij} x_i x_j + \sum_{i=1}^{n} a_i x_i + a_0.$$

By means of a linear transformation (this involves splitting off squares, hence requires the existence of $1/2 \in k$), the quadratic form $\sum_{1 \leq i \leq j = n} a_{ij} x_i x_j$ can be brought in diagonal form. This means that we can make all the coefficients a_{ij} with $i \neq j$ vanish. Another diagonal transformation (which replaces x_i by $\sqrt{a_{ii}} x_i$ when $a_{ii} \neq 0$) takes every nonzero coefficient a_{ii} to 1 and then renumbering the coordinates (which is also a linear transformation) brings f into the form $f(x_1, \ldots, x_n) = \sum_{i=1}^{r} x_i^2 + \sum_{i=1}^{n} a_i x_i + a_0$ for some $r \geq 1$. Splitting off squares once more enables us to get rid of $\sum_{i=1}^{r} a_i x_i$ so that we get

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{r} x_i^2 + \sum_{i=r+1}^{n} a_i x_i + a_0.$$

We now have the following cases.

If the nonsquare part is identically zero, then we end up with the equation $\sum_{i=1}^{r} x_i^2 = 0$ for H.

If the linear part $\sum_{i=r+1}^{n} a_i x_i$ is nonzero (so that we must have $r < n$), then an affine-linear transformation which does not affect $x_1, \ldots, x_r$ and takes $\sum_{i=r+1}^{n} a_i x_i + a_0$ to $-x_n$ yields the equation $x_n = \sum_{i=1}^{r} x_i^2$. This is the graph of the function $\sum_{i=1}^{r} x_i^2$ on $\mathbb{A}^{n-1}$ and so H is then isomorphic to $\mathbb{A}^{n-1}$.

If the linear part $\sum_{i=r+1}^{n} a_i x_i$ is zero, but the constant term a_0 is nonzero, then we can make another diagonal transformation which replaces x_i by $\sqrt{-a_0} x_i$) and divide f by a_0: then H gets the equation $\sum_{i=1}^{r} x_i^2 = 1$.

[5] We have not really defined what is an isomorphism between two nonclosed subsets of an affine space. Interpret this here as: f^* maps $k[x, y][1/(x + 1)]/(x^2 + y^2 - 1)$ (the algebra of regular functions on $C - \{p_0\}$) isomorphically onto $k[t][1/(t^2 + 1)]$ (the algebra of regular functions on $\mathbb{A}^1 - \{\pm\sqrt{-1}\}$). This will be justified by Proposition 4.10.

In particular, there are only a finite number of quadratic hypersurfaces up to isomorphism. This is also true in characteristic two, but the classification is more delicate. (For instance, the hypersurfaces defined by $x_1x_2 = 1$ and $x_1^2 + x_2^2 = 1$ are in this case *not* isomorphic.)

4.7. THE MAXIMAL IDEAL SPECTRUM. The previous discussion (and in particular Proposition 4.3) leads us to associate to an arbitrary ring R a space with a topology so that for $R = A(Y)$ we get a space homeomorphic to Y. Since the points of Y correspond to maximal ideals of $A(Y)$, we choose the underlying set of this space (which we shall denote by $\mathrm{Specm}(R)$) to be the collection of maximal ideals of R. In order to avoid confusion about whether a maximal ideal is to be viewed as a subset of R or as a point of $\mathrm{Specm}(R)$ we agree that if $\mathfrak{m}$ is a maximal ideal of R, then the corresponding element of $\mathrm{Specm}(R)$ is denoted $x_{\mathfrak{m}}$ and if $x \in \mathrm{Specm}(R)$, then the corresponding maximal ideal of R is denoted $\mathfrak{m}_x$. We write $\kappa(x)$ for the residue field $R/\mathfrak{m}_x$ and $\rho_x : R \to \kappa(x)$ for the reduction modulo $\mathfrak{m}_x$. We now have arranged that when $R = A(Y)$, $x \in \mathrm{Specm}(A(Y))$ is the same thing as a point of Y. Since $\kappa(x)$ is a finitely generated as a k-algebra, it is by Corollary 3.7 a finite extension of k and hence equal to k (k is algebraically closed).

Every $r \in R$ defines a 'regular function' f_r on $\mathrm{Specm}(R)$ which takes in $x \in \mathrm{Specm}(R)$ the value $\rho_x(r) \in \kappa(x)$. So in general f_r takes its values in a field that may depend on x, but for R of the form $A(Y)$ we know this field to be constant equal to k, so that $f_r : \mathrm{Specm}(R) \to k$. We denote by $Z(r) \subset \mathrm{Specm}(A)$ (or $Z(f_r)$) the zero set of this function. So $Z(r)$ consists of the $x \in \mathrm{Specm}(R)$ with $\rho_x(r) = 0$, or equivalently, $r \in \mathfrak{m}_x$. We write $U(r)$ or $(U(f_r))$ for its complement, the nonzero set. We have $U(rr') = U(r) \cap U(r')$ and so the collection of $\{U(r)\}_{r\in R}$ is the basis of a topology on $\mathrm{Specm}(R)$. Note that a subset $\mathrm{Specm}(R)$ is closed precisely if it is an intersection of subsets of the form $Z(r)$; this is equal to the common zero set of the set of functions defined by an ideal of R. The space $\mathrm{Specm}(R)$ is called the *maximal ideal spectrum*[6] *of* R (but our notation for it is less standard). Notice that if $R = A(Y)$, then the above discussion shows that $\mathrm{Specm}(R)$ can be identified with Y as a topological space and that under this identification, $A(Y)$ becomes the ring of regular functions on $\mathrm{Specm}(R)$.

A ring homomorphism $\phi : S \to R$ will in general *not* give rise to a map $\mathrm{Specm}(\phi) : \mathrm{Specm}(R) \to \mathrm{Specm}(S)$: if $x \in \mathrm{Specm}(R)$, then the composite homomorphism $S \to R \to \kappa(x)$ need not be onto and its kernel need not be a maximal ideal (it will be a prime ideal, though). However, in case $\phi : S \to R$ is a homomorphism of k-algebras, then $k \subset S$ maps onto $\kappa(x) = k$ as the identity map so that $\phi^{-1}\mathfrak{m}_x$ is a maximal ideal of S with residue field k. We then do get a map

$$\mathrm{Specm}(\phi) : \mathrm{Specm}(R) \to \mathrm{Specm}(S), \quad x_{\mathfrak{m}} \mapsto x_{\phi^{-1}\mathfrak{m}}.$$

For $s \in S$, the preimage of $U(s)$ is $U(\phi(s))$. This shows that $\mathrm{Specm}(\phi)$ is continuous. We call the resulting pair $(\mathrm{Specm}(\phi), \phi)$ a morphism.

EXERCISE 19. Give an example of ring homomorphism $\phi : S \to R$ and a maximal ideal $\mathfrak{m} \subset R$, such that $\phi^{-1}\mathfrak{m}$ is not a maximal ideal of S. (Hint: take a look at Exercise 13.)

[6] I. Gelfand was presumably the first to consider this in the context of functional analysis: he characterized the Banach algebras that appear as the algebras of continuous $\mathbb{C}$-valued functions on compact Hausdorff spaces and so it might be appropriate to call this the Gelfand spectrum.

EXERCISE 20. Prove that if R is a finitely generated k-algebra, then the map $r \in R \mapsto f_r$ is a k-algebra homomorphism from R to the algebra of k-valued functions on $\mathrm{Specm}(R)$ with kernel $\sqrt{(0)}$. Show that for every subset $X \subset \mathrm{Specm}(R)$, the set $I(X)$ of $r \in R$ with $f_r|X = 0$ is a radical ideal of R.

EXERCISE 21. Prove that $\mathrm{Specm}(R)$ is irreducible when R is a finitely generated algebra over a field and nonzero[7].

DEFINITION 4.8 (Preliminary definition). An *affine k-variety*[8] is a topological space Y endowed with a finitely generated k-algebra $A(Y)$ of regular functions on Y which identifies Y with the maximal ideal spectrum of $A(Y)$.

In more elementary terms, there should exist a homeomorphism h of Y onto a closed subset of some $\mathbb{A}^n$ such that $A(Y) = h^*k[x_1, \dots, x_n]$. We shall often denote an affine variety simply by the underlying topological space, e.g., by Y, where it is then understood that $A(Y)$ is part of the data. Likewise a morphism will simply be denoted by $f : X \to Y$; it is then understood that composition with f takes $A(Y)$ to $A(X)$ and defines $f^* : A(Y) \to A(X)$.

With this terminology Proposition 4.3 takes now a rather trivial form:

4.9. *The functor which assigns to an affine k-variety its k-algebra of regular functions identifies the category of affine k-varieties with the dual of the category of reduced finitely generated k-algebras, the inverse being given by the functor* Specm.

From our previous discussion it is clear that if Y is an affine variety, then every closed subset $Y' \subset Y$ determines an affine variety Y' with $A(Y') := A(Y)/I(Y')$. Here $I(Y')$ is of the course the ideal of regular functions on Y that vanish on Y'.

Our next aim is to give any basic open subset U of Y the structure of an affine variety.

PROPOSITION 4.10. *Let Y be an affine variety. Then every basic open subset $U \subset Y$ is in a natural manner an affine variety so that an inclusion $U \subset U'$ of any two such is a morphism and the algebra of regular functions on $U = U(g)$ is $A(Y)[1/g]$ (assuming $U \neq \emptyset$, so that g is not nilpotent).*

PROOF. We observe that $A(Y)[1/g]$ is defined as a k-algebra and as such it is finitely generated (just add to a generating set for $A(Y)$ the generator $1/g$) and is without zero divisors. So we have an affine variety $\mathrm{Specm}(A(Y)[1/g])$. Any maximal ideal of $A(Y)[1/g]$ intersects $A(Y)$ in a maximal ideal of $A(Y)$ which does not contain g. Conversely, if $\mathfrak{m}$ is a maximal ideal of $A(Y)$, then $\mathfrak{m}A(Y)[1/g]$ is a maximal ideal of $A(Y)[1/g]$ unless $g \in \mathfrak{m}$. So the injection $A(Y) \hookrightarrow A(Y)[1/g]$ induces an injection of $\mathrm{Specm}(A(Y)[1/g])$ in Y with image $U(g) = U$. This allows us to regard U as an affine variety whose coordinate ring is $A(Y)[1/g]$.

Assume that we have an inclusion $U(g') \subset U(g)$. Then $Z(g') \supset Z(g)$ and so by the Nullstellensatz, $g' \in \sqrt{(g)}$. This implies that $(g')^n \in (g)$ for some positive integer n. So we have a natural homomorphism $A(Y)[1/g] \to A(Y)[1/(g')^n] = A(Y)[1/g']$. This also shows that $A(Y)[1/g]$ only depends on U, for if $U(g') = U(g)$, we also a homomorphism in the opposite direction which serves as inverse so that $A(Y)[1/g] = A(Y)[1/g']$. □

[7] This corrects an earlier formulation, with thanks to my students.

[8] Since we fixed k, we will often drop k and speak of an affine variety.

Let $f : X \to Y$ be a morphism of affine varieties. Since f is continuous, a fiber $f^{-1}(y)$, or more generally, the preimage $f^{-1}Y'$ of a closed subset $Y' \subset Y$, will be closed in X. It is the zero set of the ideal in $A(X)$ generated by $f^*I(Y')$. But this ideal need not be a radical ideal. Here is a simple example:

EXAMPLE 4.11. Let $f : X = \mathbb{A}^1 \to \mathbb{A}^1 = Y$ be defined by $f(x) = x^2$. Then $f^* : k[y] \to k[x]$ is given by $f^*y = x^2$. If we assume k not to be of characteristic 2, and we take $a \in Y - \{0\}$, then the fiber $f^{-1}(a)$ consists of two distinct points and is define by the ideal generated by $f^*(y - a) = x^2 - a$. This a radical ideal and the fiber has coordinate ring $k[x]/(x^2 - a)$. However, the fiber over $0 \in Y = \mathbb{A}^1$ is the singleton $\{0\} \subset X = \mathbb{A}^1$ and the ideal generated by $f^*y = x^2$ is not a radical ideal. This example indicates that there might good reason to accept nilpotent elements in the coordinate ring of $f^{-1}(0)$ by endowing $f^{-1}(0)$ with the ring of functions $A(f^{-1}(0)) := k[x]/(x^2)$. Since this is a k-vector space of dimension 2, we thus retain the information that two points have come together and the fiber should be thought of as a point with multiplicity 2.

Example 4.4 shows that a homeomorphism of affine varieties need not be an isomorphism. Here is another class of examples.

EXAMPLE 4.12 (THE FROBENIUS MORPHISM). Assume that k has positive characteristic p and consider the morphism $F_p : \mathbb{A}^1 \to \mathbb{A}^1$, $x \mapsto x^p$. If we remember that $\mathbb{A}^1$ can be identified with k, then we observe that under this identification, F_p is a field automorphism: $F_p(a - b) = (a - b)^p = a^p - b^p = F_p(a) - F_p(b)$ and of course $F_p(ab) = (ab)^p = F_p(a)F_p(b)$ and F_p is surjective (every element of k has a pth root since k is algebraically closed) and injective. But the endomorphism F_p^* of $k[x]$ induced by F_p sends x to x^p and has therefore image $k[x^p]$. Clearly, F_p^* is not surjective.

The fixed point set of F_p (so the set of $a \in \mathbb{A}^1$ with $a^p = a$) is via the identification of $\mathbb{A}^1$ with k just the prime subfield $\mathbb{F}_p \subset k$ and we therefore denote it by $\mathbb{A}^1(\mathbb{F}_p) \subset \mathbb{A}^1$. Likewise, the fixed point set $\mathbb{A}^1(\mathbb{F}_{p^r})$ of F_p^r is the subfield of k with p^r elements. Since the algebraic closure $\bar{\mathbb{F}}_p$ of $\mathbb{F}_p$ in k is the union of the finite subfields of k, the affine line over $\bar{\mathbb{F}}_p$ equals $\cup_{r\geq 1}\mathbb{A}^1(\mathbb{F}_{p^r})$. This generalizes in a straightforward manner to higher dimensions: by letting F_p act coordinatewise on $\mathbb{A}^n$, we get a morphism $\mathbb{A}^n \to \mathbb{A}^n$ (which we still denote by F_p) which is also a bijection. The fixed point of F_p^r is $\mathbb{A}^n(\mathbb{F}_{p^r})$ and $\mathbb{A}^n(\bar{\mathbb{F}}_p) = \cup_{r\geq 1}\mathbb{A}^n(\mathbb{F}_{p^r})$.

EXERCISE 22. Assume that k has positive characteristic p. Let $q = p^r$ be a power of p with $r > 0$ and denote by $\mathbb{F}_q \subset k$ the subfield of $a \in k$ satisfying $a^q = a$. We write F for $F_p^r : \mathbb{A}^n \to \mathbb{A}^n$. Suppose $Y \subset \mathbb{A}^n$ is the common zero set of polynomials with coefficients in $\mathbb{F}_q \subset k$.

(a) Prove that $f \in k[x_1, \ldots, x_n]$ has its coefficients in $\mathbb{F}_q$ if and only if $F^*f = f^q$.
(b) Prove that an affine-linear transformation of $\mathbb{A}^n$ with coefficients in $\mathbb{F}_q$ commutes with F.
(c) Prove that F restricts to a bijection $F_Y : Y \to Y$ and that the fixed point set of F_Y^m is $Y(\mathbb{F}_{q^m}) := Y \cap \mathbb{A}^n(\mathbb{F}_{q^m})$.
(d) Suppose that k is an algebraic closure of $\mathbb{F}_p$. Prove that every closed subset of $\mathbb{A}^n$ is defined over a finite subfield of k.

REMARK 4.13. After this exercise we cannot resist to mention the Weil zeta function. This function and its relatives—among them the Riemann zeta function—codify arithmetic properties of algebro-geometric objects in a very intricate manner. In the situation of Exercise 22, we can use the numbers $|Y(\mathbb{F}_{q^m})|$ (= the number of fixed points of F^m in Y) to define a generating series $\sum_{m\geq 1}|Y(\mathbb{F}_{q^m})|t^m$. It appears to be more convenient to work with the *Weil zeta function*:

$$Z_Y(t) := \exp\Big(\sum_{m=1}^{\infty}|Y(\mathbb{F}_{q^m})|\frac{t^m}{m}\Big),$$

which has the property that $t\frac{d}{dt}\log Z_Y$ yields the generating series above. This series has remarkable properties. For instance, a deep theorem due to Bernard Dwork (1960) asserts that it represents a rational function of t. Another deep theorem, due to Pierre Deligne (1974), states that the roots of the numerator and denominator have for absolute value a nonpositive half-integral power of q and that moreover, these powers have an interpretation in terms of an 'algebraic topology for algebraic geometry'. All of this was predicted by André Weil in 1949. (This can be put in a broader context by making the change of variable $t = q^{-s}$. Indeed, now numerator and denominator have their zeroes when the real part of s is a nonnegative half-integer and this makes Deligne's result reminiscent of the famous conjectured property of the Riemann zeta function.)

EXERCISE 23. Compute the Weil zeta function of affine n-space relative to the field of q elements.

5. The product

Let m and n be nonnegative integers. If $f \in k[x_1,\ldots,x_m]$ and $g \in k[y_1,\ldots,y_n]$, then we have a regular function $f*g$ on $\mathbb{A}^{m+n}$ defined by

$$f*g(x_1,\ldots,x_m,y_1,\ldots,y_n) := f(x_1,\ldots,x_m)g(y_1,\ldots,y_n).$$

It is clear that $U(f*g) = U(f)\times U(g)$, which shows that the Zariski topology on $\mathbb{A}^{m+n}$ refines the product topology on $\mathbb{A}^m\times\mathbb{A}^n$. Equivalently, if $X\subset\mathbb{A}^m$ and $Y\subset\mathbb{A}^n$ are closed, then $X\times Y$ is closed in $\mathbb{A}^{m+n}$. We give $X\times Y$ the topology it inherits from $\mathbb{A}^{m+n}$ (which is usually finer than the product topology). For the coordinate rings we have defined a map:

$$A(X)\times A(Y)\to A(X\times Y),\quad (f,g)\mapsto f*g$$

which is evidently k-bilinear (i.e., k-linear in either variable). We want to prove that the ideal $I(X\times Y)$ defining $X\times Y$ in $\mathbb{A}^{m+n}$ is generated by $I(X)$ and $I(Y)$ (viewed as subsets of $k[x_1,\ldots,x_m,y_1,\ldots y_n]$) and that $X\times Y$ is irreducible when X and Y are. This requires that we translate the formation of the product into algebra. This centers around the notion of the tensor product, the definition of which we recall. (Although we here only need tensor products over k, we shall define this notion for modules over a ring, as this is its natural habitat. This is the setting that is needed later anyhow.)

If R is a ring and M and N are R-modules, then we can form their *tensor product over* R, $M\otimes_R N$: as an abelian group $M\otimes_R N$ is generated by the expressions $a\otimes_R b$, $a\in M$, $b\in N$ and subject to the conditions $(ra)\otimes_R b = a\otimes_R(rb)$, $(a+a')\otimes_R b = a\otimes_R b + a'\otimes_R b$ and $a\otimes_R(b+b') = a\otimes_R b + a\otimes_R b'$. So a general element of $M\otimes_R N$ can be written

like this: $\sum_{i=1}^N a_i \otimes_R b_i$, with $a_i \in M$ and $b_i \in N$. We make $M \otimes_R N$ an R-module if we stipulate that $r(a \otimes_R b) := (ra) \otimes_R b$ (which is then also equal to $r \otimes_R (rb)$). Notice that the map

$$\otimes_R : M \times N \to M \otimes_R N, \quad (a, b) \mapsto a \otimes_R b,$$

is R-bilinear (if we fix one of the variables, then it becomes an R-linear map in the other variable).

In case $R = k$ we shall often omit the suffix k in $\otimes_k$.

EXERCISE 24. Prove that $\otimes_R$ is universal for this property in the sense that every R-bilinear map $M \times N \to P$ of R-modules is the composite of $\otimes_R$ and a *unique* R-homomorphism $M \otimes_R N \to P$. In other words, the map

$$\mathrm{Hom}_R(M \otimes_R N, P) \to \mathrm{Bil}_R(M \times N, P)), \quad f \mapsto f \circ \otimes_R$$

is an isomorphism of R-modules.

EXERCISE 25. Let m and n be nonnegative integers. Prove that $\mathbb{Z}/(n) \otimes_{\mathbb{Z}} \mathbb{Z}/(m)$ can be identified with $\mathbb{Z}/(m, n)$.

If A is an R-algebra and N is an R-module, then $A \otimes_R N$ acquires the structure of an A-module which is characterized by

$$a.(a' \otimes_R b) := (aa') \otimes_R b.$$

For instance, if N is an $\mathbb{R}$-vector space, then $\mathbb{C} \otimes_{\mathbb{R}} N$ is a complex vector space, the *complexification* of N. If A and B are R-algebras, then $A \otimes_R B$ acquires the structure of an R-algebra characterized by

$$(a \otimes_R b).(a' \otimes_R b') := (aa') \otimes_R (bb').$$

Notice that $A \to A \otimes_R B$, $a \mapsto a \otimes_R 1$ and $B \to A \otimes_R B$, $b \mapsto 1 \otimes_R b$ are R-algebra homomorphisms. For example, $A \otimes_R R[x] = A[x]$ as A-algebras (and hence $A \otimes_R R[x_1, \ldots, x_n] = A[x_1, \ldots, x_n]$ with induction).

EXERCISE 26. Prove that $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ is as a $\mathbb{C}$-algebra isomorphic to $\mathbb{C} \oplus \mathbb{C}$ with componentwise multiplication.

PROPOSITION 5.1. *For closed subsets $X \subset \mathbb{A}^m$ and $Y \subset \mathbb{A}^n$ the bilinear map $A(X) \times A(Y) \to A(X \times Y)$, $(f, g) \mapsto f * g$ induces an isomorphism $\mu : A(X) \otimes A(Y) \to A(X \times Y)$ of k-algebras (so that in particular $A(X) \otimes A(Y)$ is reduced).*

If X and Y are irreducible, then so is $X \times Y$, or equivalently, if $A(X)$ and $A(Y)$ are domains, then so is $A(X) \otimes A(Y)$.

PROOF. Since the obvious map

$$k[x_1, \ldots, x_m] \otimes k[y_1, \ldots, y_n] \to k[x_1, \ldots, x_m, y_1, \ldots, y_n]$$

is an isomorphism, it follows that μ is onto. In order to prove that μ is injective, let let first observe that every $u \in A(X) \otimes A(Y)$ can be written $u = \sum_{i=1}^N f_i \otimes g_i$ with $g_1, \ldots, g_N$ are k-linearly independent. Given $p \in X$, then the restriction of $\mu(u) = \sum_{i=1}^N f_i * g_i$ to $\{p\} \times Y \cong Y$ is the regular function $u_p := \sum_{i=1}^N f_i(p) g_i \in A(Y)$. Since the g_i's are linearly independent, we have $u_p = 0$ if and only if $f_i(p) = 0$ for all i. In particular, the subset $X(u) \subset X$ of $p \in X$ for which $u_p = 0$, is equal to $\cap_{i=1}^N Z(f_i)$ and hence closed.

If $\mu(u) = 0$, then $u_p = 0$ for all $p \in X$ and hence $f_i = 0$ for all i. So $u = 0$. This proves that μ is injective.

Suppose now X and Y irreducible and suppose that u is zero divisor: $uv = 0$ for some $v \in A(X \times Y)$ with $u, v \neq 0$. Since the restriction of $uv = 0$ to $\{p\} \times Y \cong Y$ is $u_p v_p$ and $A(Y)$ is a domain, it follows that $u_p = 0$ or $v_p = 0$. So $X = X(u) \cup X(v)$.

Since X is irreducible we have $X = X(u)$ or $X(v)$. This means that $u = 0$ or $v = 0$, which contradicts our assumption. □

EXERCISE 27. Let X and Y be closed subsets of affine spaces. Prove that each irreducible component of $X \times Y$ is the product of an irreducible component of X and one of Y.

It is clear that the projections $\pi_X : X \times Y \to X$ and $\pi_Y : X \times Y \to Y$ are regular. We have observed that $X \times Y$ has not a topological product in general. Still it is the 'right' product in the sense of category theory: it has the following universal property, almost seems too obvious to mention: if Z is a closed subset of some affine space, then any pair of regular maps $f : Z \to X$, $g : Z \to Y$ defines a regular map $Z \to X \times Y$ characterized by the property that its composite with π_X resp. π_Y yields f resp. g (this is of course (f, g)).

6. Function fields and rational maps

In this section we interpret the formation of the fraction ring of an algebra of regular functions.

Let Y be an affine variety. Recall that for $f, g \in A(Y)$, a fraction $f/g \in \mathrm{Frac}(A(Y))$ is defined if g not a zerodivisor. We need the following lemma.

LEMMA 6.1. *Let Y be an affine variety and let $g \in A(Y)$. Then g is not a zero divisor if and only if g is nonzero on every irreducible component of Y. This is also equivalent to $U(g)$ being dense in Y.*

PROOF. Suppose g is zero on some irreducible component C of Y and suppose $C \neq Y$. If Y' denotes the union of the irreducible components of Y distinct form C, then either $Y' = \emptyset$ (and so $g = 0$ in $A(Y)$) or $Y' \neq \emptyset$ and so there exists a nonzero $g' \in I_Y(Y')$. Then gg' vanishes on $C \cup Y' = Y$ and so $gg' = 0$. It follows that g is then a zero divisor.

Conversely, assume that g is a zerodivisor of $A(Y)$. So there exists a nonzero $g' \in A(Y)$ with $gg' = 0$. Let C be an irreducible component of Y on which g' is nonzero. Then we must have $g|C = 0$.

The proof of the last clause is left to you. □

This lemma tells us that this means that the affine variety $U(g)$ is open-dense in Y. Clearly, f/g defines a regular function $U(g) \to k$. Another such fraction f'/g' yields a regular function on an open-dense $U(g')$ and their product $f/g.f'/g' = ff'/gg'$ resp. difference $f/g - f'/g' = (fg' - f'g)/gg'$ in $\mathrm{Frac}(A(Y))$ defines a regular function on $U(gg')$ which is there just the product resp. difference of the associated regular functions. In particular, if $f'/g' = f/g$ in $A(Y)$, then the two associated regular functions coincide on $U(gg')$. There is a priori no best way to represent a given element of $\mathrm{Frac}(A(Y))$ as a fraction (as there is in a UFD), and so we must be content with the observation that an element of $\mathrm{Frac}(A(Y))$ defines a regular function on *some* (unspecified) open dense subset of Y, with the understanding that two such functions are regarded as equal if they coincide on an open-dense subset contained in a common domain of definition. When an element of $\mathrm{Frac}(A(Y))$ is thus understood, then we call it a *rational function* on Y. This is the algebro-geometric analogue of a meromorphic function in complex function theory. When Y is irreducible, then $\mathrm{Frac}(A(Y))$ is a field, called the *function field of* Y, and will be denoted $k(Y)$.

We shall now give a geometric interpretation of finitely generated field extensions of k and the k-linear field homomorphisms between them. We begin with a notion that generalizes that of a rational function.

DEFINITION 6.2. Let X and Y be affine varieties. A *rational map* from X to Y is given by a pair (U, F), where U is an affine open-dense subset of X and $F : U \to Y$ is a morphism, with the understanding that a pair (V, G) defines the same rational map if F and G coincide on $U \cap V$. We denote a rational map like this $f : X \dashrightarrow Y$.

We say that the rational map is *dominant* if for a representative pair (U, F), $F(U)$ is dense in Y. (This is then also so for any other representative pair. Why?)

PROPOSITION 6.3. *Any finitely generated field extension of k is k-isomorphic to the function field of an irreducible affine variety. If X and Y are irreducible and affine, then a dominant rational map $f : X \dashrightarrow Y$ determines a k-linear field embedding $f^* : k(Y) \hookrightarrow k(X)$ and every k-linear field embedding $k(Y) \to k(X)$ is of this form (for a unique f).*

PROOF. Let K/k be a finitely generated field extension of k: there exist elements $a_1, \ldots, a_n \in K$ such that every element of K can be written as a fraction of polynomials in $a_1, \ldots, a_n$. So if R denotes the k-subalgebra R of K generated by $a_1, \ldots, a_n$, (a domain since K is a field), then K is the field of fractions of R. Since R is the coordinate ring of a closed irreducible subset $X \subset \mathbb{A}^n$ (defined by the kernel of the obvious ring homomorphism $k[x_1, \ldots, x_n] \to R$), it follows that K can be identified with $k(X)$.

Suppose we are given an open-dense affine subvariety $U \subset X$ and a morphism $F : U \to Y$ with $F(U)$ dense in Y. Now $F^* : A(Y) \to A(U)$ will be injective, for if $g \in A(Y)$ is in the kernel: $F^*(g) = 0$, then $F(U) \subset Z(g')$. Since $F(U)$ is dense in Y, this implies that $Z(g) = Y$, in other words, that $g = 0$. Hence the composite map $A(Y) \to A(U) \to k(U) = k(X)$ is an injective homomorphism from a domain to a field and therefore extends to a field embedding $k(Y) \to k(X)$.

It remains to show that every k-linear field homomorphism $\Phi : k(Y) \to k(X)$ is so obtained. For this, choose generators $b_1, \ldots, b_m$ of $A(Y)$. Then $\Phi(b_1), \ldots, \Phi(b_m)$ are rational functions on X and so are regular on an open-dense affine subset $U \subset X$. Since $b_1, \ldots, b_m$ generate $A(Y)$ as a k-algebra, it follows that Φ maps $A(Y)$ to $A(U) \subset k(X)$. This is a k-algebra homomorphism and so defines a morphism $F : U \to Y$ such that $F^* = \Phi | A(Y)$. The image of F will be dense by the argument above: if the image of F is contained in a closed subset of Y distinct from Y, then its maps to some $Z(g)$ with $g \in A(Y) - \{0\}$. But this implies that $\Phi(g) = F^*(g) = 0$, which cannot happen, since Φ is injective. It is clear that Φ is the extension of F^* to the function fields.

As to the uniqueness: if (V, G) is another solution, then choose a nonempty affine open-dense subset $W \subset U \cap V$ so that F and G both define morphisms $W \to Y$. The maps $A(Y) \to A(W)$ they define are equal, for are given by Φ. Hence F and G coincide on W. Since W is dense in $U \cap V$, they also coincide on $U \cap V$. $\square$

EXERCISE 28. Let $f \in k[x_1, \ldots, x_{n+1}]$ be irreducible of positive degree. Its zero set $X \subset \mathbb{A}^{n+1}$ is then closed and irreducible. Denote by d the degree of f in x_{n+1}.

(a) Prove that the projection $\pi : X \to \mathbb{A}^n$ induces an injective k-algebra homomorphism $\pi^* : k[x_1, \ldots, x_n] \to A(X) = k[x_1, \ldots, x_n]/(f)$ if and only if $d > 0$.

(b) Prove that for $d > 0$, π is dominant and that the resulting field homomorphism $k(x_1, \ldots, x_n) \to k(X)$ is a finite extension of degree d.

COROLLARY 6.4. *There is a category with objects the irreducible affine varieties and morphisms the rational dominant maps. Assigning to an irreducible affine variety its function field makes this category anti-equivalent to the category of finitely generated field extensions of the base field k.*

PROPOSITION-DEFINITION 6.5. *A rational map $f : X \dashrightarrow Y$ is an isomorphism in the above category (that is, induces a k-linear isomorphism of function fields) if and only if there exists a representative pair (U, F) of f such that F maps U* isomorphically *onto an open subset of Y. If these two equivalent conditions are satisfied, then f is called a* birational map. *If a birational map $X \dashrightarrow Y$ merely exists (in other words, if there exists a k-linear field isomorphism between $k(X)$ and $k(Y)$), then we say that X and Y are* birationally equivalent.

PROOF. If f identifies a nonempty open subset of X with one of Y, then $f^* : k(Y) \to k(X)$ is clearly a k-algebra isomorphism.

Suppose now we have a k-linear isomorphism $k(Y) \cong k(X)$. Represent this isomorphism and its inverse by (U, F) and (V, G) respectively. Then $F^{-1}V$ is affine and open-dense in U and $GF : F^{-1}V \to X$ is defined. Since GF induces the identity on $k(X)$, GF is the identity on a nonempty open subset of $F^{-1}V$ and hence on all of $F^{-1}V$. This implies that F maps $F^{-1}V$ injectively to $G^{-1}U$. For the same reason, G maps $G^{-1}U$ injectively to $F^{-1}V$. So F defines an isomorphism between the open subsets $F^{-1}V \subset X$ and $G^{-1}U \subset Y$. □

EXERCISE 29. We here assume k not of characteristic 2. Let for $X \subset \mathbb{A}^2$ be defined by $x_1^2 + x_2^2 = 1$. Prove that X is birationally equivalent to the affine line $\mathbb{A}^1$. (Hint: take a look at Exercise 17.) More generally, prove that the quadric in $\mathbb{A}^{n+1}$ defined by $x_1^2 + x_2^2 + \cdots x_{n+1}^2 = 1$ is birationally equivalent to $\mathbb{A}^n$. What about the quadric cone in $\mathbb{A}^{n+1}$ defined by $x_1^2 + x_2^2 + \cdots x_{n+1}^2 = 0$ ($n \geq 2$)?

In case $k(X)/k(Y)$ is a finite extension, one may wonder what the geometric meaning is of the degree d of that extension, perhaps hoping that this is just the number of elements of a general fiber of the associated rational map $X \dashrightarrow Y$. We will see that this often true (namely when the characteristic of k is zero, or more generally, when this characteristic does not divide d), but not always, witness the following example.

EXAMPLE 6.6. Suppose k has characteristic $p > 0$. We take $X = \mathbb{A}^1 = Y$ and let f be the Frobenius map: $f(a) = a^p$. Then f is homeomorphism, but $f^* : A(Y) \to A(X)$ is given by $y \mapsto x^p$ and so induces the field extension $k(y) = k(x^p) \subset k(x)$, which is of degree p. From the perspective of Y, we have enlarged its algebra of regular functions by introducing a formal pth root of its coordinate (which yields another copy of $\mathbb{A}^1$, namely X). From the perspective of X, $A(Y)$ is just $f^*A(X)$.

This is in fact the basic example of a *purely inseparable* field extension, i.e., a field extension L/K with the property that every element of L has a minimal polynomial in $K[T]$ that has at most one root in L. Such a polynomial must be of the form $T^{p^r} - c$, with $c \in K$ not a p-th power of an element of K when $r > 0$, where p is the characteristic of K (for $p = 0$ we necessarily have $L = K$). So if $L \neq K$, then the Frobenius map $F_p : a \in K \mapsto a^p \in K$ is not surjective. Purely inseparable

extensions are not detected by Galois theory, for they have trivial Galois group: after all, there is only one root to move around.

For any algebraic extension L/K, the elements of L that are separable over K make up an intermediate extension L^{sep}/K that is (of course) separable and is such that L/L^{sep} is purely inseparable. When L is an algebraic closure of K, then L^{sep} is called a *separable algebraic closure* of K: it is a separable algebraic extension of K which is maximal for that property. Then L is as an extension of L^{sep} obtained by successive adjunction of p-power roots of elements of L^{sep}: it is an extension minimal for the property of making the Frobenius map $a \in L \mapsto a^p \in L$ surjective. In case L/K is a finite normal extension (i.e., a finite extension with the property that every $f \in K[x]$ that is the minimal polynomial of some element of L has all roots in L), then the fixed point set of the Galois group of L/K is a subextension L^{insep}/L that is purely inseparable, whereas L/L^{insep} separable. In that case the natural map $L^{\text{sep}} \otimes_K L^{\text{insep}} \to L$ is an isomorphism of K-algebras.

EXERCISE 30. Let $f : X \to Y$ be a dominant morphism of irreducible affine varieties which induces a purely inseparable field extension $k(Y)/k(X)$. Prove that there is an open-dense subset $U \subset Y$ such that f restricts to a homeomorphism $f^{-1}U \to U$. (Hint: show first that it suffices to treat the case when $k(X)$ is obtained from $k(Y)$ by adjoining the pth root of an element $f \in k(Y)$. Then observe that if f is regular on the affine open-dense $U \subset Y$, then Y contains as an open dense subset a copy of the locus of $(x,t) \in U \times \mathbb{A}^1$ satisfying $t^p = f$.)

If K/k is a finitely generated field extension and generated by $b_1, \ldots, b_m$, say, then we may after renumbering assume that for some $r \leq m$, $b_1, \ldots, b_r$ are algebraically independent (so that the k-linear field homomorphism $k(x_1, \ldots, x_r) \to K$ which sends x_i to b_i is injective) and $b_{r+1}, \ldots, b_m$ are algebraic over $k(b_1, \ldots, b_r)$. This number r is invariant of K/k, called its *transcendence degree*. So if $K = k(X)$, then this defines a dominant rational map $X \dashrightarrow \mathbb{A}^r$. We now recall the theorem of the primitive element:

THEOREM 6.7. *Every separable field extension L/K of finite degree is generated by a single element (which we then call a* primitive element *for L/K).*

It follows that if $b_{r+1}, \ldots, b_m$ are separable over $k(b_1, \ldots, b_r)$, then we can find a $b \in K$ that is algebraic over $k(b_1, \ldots, b_r)$ such that K is obtained from $k(b_1, \ldots, b_r)$ by adjoining b. This b is a root of an irreducible polynomial $F \in k(b_1, \ldots, b_r)[T]$. If we clear denominators, we may assume that the coefficients of F lie in $k[b_1, \ldots, b_r][T] = k[b_1, \ldots, b_r, T]$. Then we can take for X the hypersurface in $\mathbb{A}^{r+1}$ defined by F, when viewed as an element of $k[x_1, \ldots, x_r, x_{r+1}]$.

In particular, every irreducible affine variety Y is birationally equivalent to a hypersurface in $\mathbb{A}^{r+1}$, where r is the transcendence degree of $k(Y)$. This suggests that this transcendence degree might be a good way to define the dimension of Y. We shall return to this.

Much of the algebraic geometry in the 19th century and early 20th century was of a birational nature: birationally equivalent varieties were regarded as not really different. This sounds rather drastic, but it turns out that many interesting properties of varieties are an invariant of their birational equivalence class.

Here is an observation which not only illustrates how affine varieties over algebraically nonclosed fields can arise when dealing with affine k-varieties, but one that is also a tell-tale sign that we ought to enlarge the maximal ideal spectrum. Let $f : X \to Y$ be a dominant morphism of irreducible affine varieties. This implies that $f^* : A(Y) \to A(X)$ is injective and that $f(X)$ contains an open-dense subset of Y. Then we may ask whether there exists something like a general fiber: is there an open-dense subset $V \subset Y$ such that the fibers $f^{-1}(y)$, $y \in V$ all "look the same"? The question is too vague for a clear answer and for most naive ways of making this precise, the answer will be no. But there is a cheap way out by simply refusing to specify one such V and allowing it to be arbitrarily small: we would like to take a limit over all open-dense subsets of Y. This we cannot do (yet) topologically, but we can do this algebraically by making all the nonzero elements of $A(Y)$ in $A(X)$ invertible: we take

$$(A(Y) - \{0\})^{-1}A(X) = k(Y) \otimes_{A(Y)} A(X)$$

(this equality follows from the fact that $A(X) = A(Y) \otimes_{A(Y)} A(X)$). This is a reduced finitely generated $k(Y)$-algebra and we may regard its maximal ideal spectrum $\mathrm{Specm}(k(Y) \otimes_{A(Y)} A(X))$ as an affine variety over the (algebraically nonclosed) field $k(Y)$: now every regular function on X which comes from Y is treated as a scalar (and will be invertible when nonzero). If we decide to add to $Y \cong \mathrm{Specm}(k(Y))$ a point $\eta(Y)$ with residue field $k(Y)$, then we can simply say that the generic fiber of f is the fiber $X_{\eta(Y)}$ over $\eta(Y)$[9]. But once we decide to do this for Y, we should of course do this for every irreducible affine variety. In particular, we must then add for every irreducible subset Z of Y (or equivalently, for every prime ideal $\mathfrak{p} \subset A(Y)$) a point to $\mathrm{Specm}(k(Y))$ with residue field $k(Z)$ $(= \mathrm{Frac}(A(Y)/\mathfrak{p}))$. We do this below in the same kind of generality as the maximal ideal spectrum, namely for an arbitrary ring.

6.8. THE PRIME IDEAL SPECTRUM. Let R be a ring. Its *spectrum* $\mathrm{Spec}(R)$ is a topological space whose underlying set is the set of its prime ideals, where we employ the following notation: if $\mathfrak{p}$ is a prime ideal of R, then we denote the corresponding element of $\mathrm{Spec}(R)$ by $x_{\mathfrak{p}}$ and if $x \in \mathrm{Spec}(R)$, we denote by $\mathfrak{p}_x \subset R$ the corresponding prime ideal. If $r \in R$, then we write $U(r)$ for the set of $x \in \mathrm{Spec}(R)$ with $r \notin \mathfrak{p}_x$. We have $U(r) \cap U(r') = U(rr')$ and so this collection of subsets is a basis for a to topology on $\mathrm{Spec}(R)$, called (from now on) the *Zariski topology*. It is also characterized by the property that the closed sets are those defined by an ideal of R: if we put $Z(r) := \mathrm{Spec}(R) - U(r)$, then any closed subset of $\mathrm{Spec}(R)$ is of the form $Z(S) = \cap_{r \in S} Z(r)$ for some subset $S \subset R$ (and vice versa). Notice that this just the set of $x \in \mathrm{Spec}(R)$ with $\mathfrak{p}_x \supset S$ and hence only depends on the ideal $I(S)$ generated by S: $Z(S) = Z(I(S))$.

Since the zero ring (for which we have $0 = 1$) has no prime ideals, its spectrum is the empty set.

As the following exercise shows, points of $\mathrm{Spec}(R)$ need not be closed:

[9]It is often preferable to work over an algebraically closed field. We can remedy this simply by choosing an algebraic closure L of $k(Y)$. The maximal ideal spectrum of $L \otimes_{A(Y)} A(X)$ is then an affine L-variety, and yields a notion of a general fiber that is even closer to our geometric intuition.

EXERCISE 31. Let $x, y \in \mathrm{Spec}(R)$. Prove that x lies in the closure of y if and only if $\mathfrak{p}_x \supset \mathfrak{p}_y$. Conclude that x is closed in $\mathrm{Spec}(R)$ if and only if $\mathfrak{p}_x$ is a maximal ideal of R.

We can think (at least for now) of $r \in R$ a defining a 'regular function' on $\mathrm{Spec}(R)$, but its value field varies with the point: to $x \in \mathrm{Spec}(R)$ we associate the field $\kappa(x) := \mathrm{Frac}(R/\mathfrak{p}_x)$, called the *residue field* of x. Then $r \in R$ determines a 'regular function' on $\mathrm{Spec}(R)$: it assigns to x the image of r in $\kappa(x)$ (denoted $r(x)$). (We will come up with something better when we discuss sheaves.)

One immediate advantage of the prime ideal spectrum over the maximal ideal spectrum is that any ring homomorphism $\phi : R' \to R$ determines a map

$$\mathrm{Spec}(\phi) : \mathrm{Spec}(R) \to \mathrm{Spec}(R'), \quad x_{\mathfrak{p}} \mapsto x_{\mathfrak{p}'},$$

where $\mathfrak{p}' := \phi^{-1}\mathfrak{p} = \ker(R' \to R \to R/\mathfrak{p})$. This is a prime ideal of R' indeed, for ϕ now induces an embedding of $R'/\mathfrak{p}'$ in $R/\mathfrak{p}$ and so $R'/\mathfrak{p}'$ has no zero divisors (but if $\mathfrak{p}$ were a maximal ideal, then we would not be able to conclude that $\phi^{-1}\mathfrak{p}$ is maximal). The embedding $R'/\mathfrak{p}' \hookrightarrow R/\mathfrak{p}$ of domains of course extends to an embedding of their fields of fractions, $\kappa(x_{\mathfrak{p}'}) \hookrightarrow \kappa(x_{\mathfrak{p}})$. For $r' \in R'$, the 'regular function' it defines on $\mathrm{Spec}(R')$ as above precomposed with ϕ yields the 'regular function' on $\mathrm{Spec}(R)$ defined by $\phi(r')$ and so $\mathrm{Spec}(\phi)^{-1}(U(r')) = U(\phi(r'))$. Hence $\mathrm{Spec}(\phi)$ is continuous.

A *generic point* of $\mathrm{Spec}(R)$ is a point that does not lie in the closure of another point. In other words, it is associated to a minimal prime ideal of R, or equivalently, to an irreducible component $\mathrm{Spec}(R)$. If R is a domain, there is only one such point, namely $x_{(0)}$ with residue field $\mathrm{Frac}(R)$.

Notice that for ϕ as above, the fiber of $\mathrm{Spec}(\phi)$ over $x' = x_{\mathfrak{p}'} \in \mathrm{Spec}(R')$ is (as a subspace of $\mathrm{Spec}(R)$) the set of $x \in \mathrm{Spec}(R)$ with for which $\mathfrak{p}' = \phi^{-1}\mathfrak{p}_x$, or equivalently, for which $\mathfrak{p} \cap \phi(R') = \phi(\mathfrak{p}')$. In Exercise 33 you will show that such prime ideals correspond bijectively to prime ideals of the $\kappa(x')$-algebra $\kappa(x') \otimes_{R'} R$. Hence it makes sense to regard $\mathrm{Spec}(\kappa(x') \otimes_{R'} R)$ as the fiber over x'. (Here with the given of the $\kappa(x')$-algebra $\kappa(x') \otimes_{R'} R$); we will later employ definitions for which this is automatic.) If R' is a domain, then the fiber over the generic point, $\mathrm{Spec}(\mathrm{Frac}(R') \otimes_{R'} R)$, is called the *generic fiber* of $\mathrm{Spec}(\phi)$.

EXAMPLE 6.9. The spectrum of $\mathbb{Z}$ has a point x_p for every prime number p (with residue field $\kappa(x_p) = \mathbb{F}_p$), and one for the zero ideal, yielding the generic point x_0 (with residue filed $\kappa(x_0) = \mathbb{Q}$). For every ring R we have a natural ring homomorphism $\mathbb{Z} \to R$. This defines a map $\mathrm{Spec}(R) \to \mathrm{Spec}(\mathbb{Z})$. In case R is not the zero ring (so that $\mathrm{Spec}(R)$ is nonempty), the fiber over x_p is $\mathrm{Spec}(\mathbb{F}_p \otimes R) = \mathrm{Spec}(R/pR)$ (which is empty if p is invertible in R) and the fiber over x_0 is $\mathrm{Spec}(\mathbb{Q} \otimes R)$.

EXERCISE 32. Determine the points and their residue fields of $\mathrm{Spec}(k[X])$ and $\mathrm{Spec}(\mathbb{R}[X])$. Also try your hand at $\mathrm{Spec}(\mathbb{Z}[X])$.

EXERCISE 33. Let $\phi : R' \to R$ be a ring homomorphism and $\mathfrak{p}' \subset R'$ a prime ideal. Prove that for every prime ideal $\mathfrak{p} \subset R$ with $\phi^{-1}\mathfrak{p} = \mathfrak{p}'$, the image of $\mathrm{Frac}(R'/\mathfrak{p}') \otimes_{R'} \mathfrak{p}$ in $\mathrm{Frac}(R'/\mathfrak{p}') \otimes_{R'} R$ is a prime ideal of latter. Prove that this defines a bijection between the prime ideals $\mathfrak{p} \subset R$ with $\phi^{-1}\mathfrak{p} = \mathfrak{p}'$ and the prime ideals of $\mathrm{Frac}(R'/\mathfrak{p}') \otimes_{R'} R$.

Now let us return to the case of an affine variety: we take $R = A$, with A a reduced finitely generated k-algebra and we write X for $\mathrm{Specm}(A)$. Any $x \in \mathrm{Spec}(A)$ corresponds to a prime ideal in A. But this in turn corresponds to a closed irreducible subset $Z_x \subset X$ so that $A/\mathfrak{p}_x = A(Z_x)$. The residue field $\kappa(x)$ is then $\mathrm{Frac}(A/\mathfrak{p}_x) = k(Z_x)$. So when x is a closed point (so that $\mathfrak{p}_x$ is a maximal ideal of A), then Z_x is a singleton and we have $\kappa(x) = k$. It is clear how any $f \in A$ will define a function of $\mathrm{Spec}(A)$: for $x \in \mathrm{Spec}(A)$, $f(x)$ is the restriction of f to Z_x (viewed as a rational function on Z_x, which just happens to be regular).

We can now bring the definition of an affine variety in an almost final form.

DEFINITION 6.10 (Almost final form of the definition). An *affine k-variety* is the prime ideal spectrum of a k-algebra of a reduced finitely generated k-algebra.

This definition does not seem to amount to much. The reason for making it is to some extent psychological: we reversed the arrows of our category, so that we can draw on our geometric intuition (and employ associated terminology). The final definition has to wait until we discuss sheaves.

7. Finite morphisms

Let A be a ring and B an A-algebra.

PROPOSITION-DEFINITION 7.1. *We say that $b \in B$ is* integrally dependent *on A if one the following equivalent properties is satisfied.*

(i) *b is a root of a monic polynomial $x^n + a_1 x^{n-1} + \cdots + a_n \in A[x]$,*
(ii) *$A[b]$ is as an A-module finitely generated,*
(iii) *$A[b]$ is contained in a A-subalgebra $C \subset B$ which is finitely generated as an A-module.*

In particular, if B is finite over *A (which is short for: B is a finitely generated A-module), then B is integral over A (which is short for: every element of B is integral over A).*

PROOF. $(i) \Rightarrow (ii)$. If b is a root of $x^n + a_1 x^{n-1} + \cdots + a_n \in A[x]$, then clearly $A[b]$ is generated as a A-module by $1, b, b^2, \ldots, b^{n-1}$.
$(ii) \Rightarrow (iii)$ is obvious.
$(iii) \Rightarrow (i)$. Suppose that C is as in (iii). Choose an epimorphism $\pi : A^n \to C$ of A-modules and denote the standard basis of A^n by $(e_1, \ldots, e_n)$. We may (and will) assume that $\pi(e_1) = 1$. By assumption, $b\pi(e_i) = \sum_{j=1}^n x_{ij}\pi(e_j)$ for certain $x_{ij} \in A$. Put $\sigma := (b\delta_{ij} - x_{ij})_{i,j} \in \mathrm{End}(A[b]^n)$. Then $\pi\sigma = 0$.
If $\sigma' \in \mathrm{End}(A[b]^n)$ is the matrix of cofactors of σ, then $\sigma\sigma' = \det(\sigma)1_n$ by Cramer's rule. We find that $\det(\sigma) = \det(\sigma)\pi(e_1) = \pi(\det(\sigma)e_1) = \pi(\sigma\sigma')(e_1) = (\pi\sigma)\sigma'(e_1) = 0$. Clearly, $\det(\sigma)$ is a monic polynomial in b. □

The *integral closure of A in B* is the set elements of B that are integrally dependent on A and will be denoted $\overline{A}^B$.

COROLLARY 7.2. *The integral closure of A in B is an A-subalgebra of B.*

PROOF. It is enough to prove the following: if $b, b' \in B$ are integrally dependent over A, then every element of $A[b, b']$ is algebraically dependent over A. Since b' is integrally dependent over A, it is so over $A[b]$. Hence $A[b][b'] = A[b, b']$ is a

finitely generated $A[b]$-module. Since $A[b]$ is a finitely generated A-module, it follows that $A[b, b']$ is a finitely generated A-module. Hence by (iii) every element of $A[b, b']$ is integrally dependent over A. □

EXERCISE 34. Prove that 'being integral over' is transitive: if B is an A-algebra integral over A, then any B-algebra that is integral over B is as an A-algebra integral over A.

We say that the ring homomorphism $A \to B$ is an *integral extension* if it is injective (so that A may be regarded as a subring of B) and B is integral over A.

PROPOSITION 7.3. *Let $A \subset B$ be an integral extension and let $\mathfrak{p} \subset A$ be a prime ideal of A. Then the* going up *property holds: $\mathfrak{p}$ is of the form $\mathfrak{q} \cap A$, where $\mathfrak{q}$ is a prime ideal of B. If also is given is a prime ideal $\mathfrak{q}'$ of B with the property that $\mathfrak{q}' \cap A \subset \mathfrak{p}$, then we can take $\mathfrak{q} \supset \mathfrak{q}'$. Moreover the* incomparability *property holds: two distinct prime ideals of B having the same intersection with A cannot obey an inclusion relation (equivalently, if $\mathfrak{q}' \cap A = \mathfrak{p}$, then $\mathfrak{q} = \mathfrak{q}'$ is the only solution).*

If B is a domain, then $\mathrm{Frac}(B)$ is an algebraic field extension of $\mathrm{Frac}(A)$, which is finite whenever B is finite over A.

PROOF. Consider the localizations $A_{\mathfrak{p}}$ resp. $A_{\mathfrak{p}}B$ obtained by making the elements of $A - \mathfrak{p}$ invertible. Then $A_{\mathfrak{p}}$ is a local ring with maximal ideal $\tilde{\mathfrak{p}} := \mathfrak{p}A_{\mathfrak{p}}$ and $A_{\mathfrak{p}}B$ is an integral extension of $A_{\mathfrak{p}}$. If we find a prime ideal $\tilde{\mathfrak{q}}$ of $A_{\mathfrak{p}}B$ with $\tilde{\mathfrak{q}} \cap A_{\mathfrak{p}} = \tilde{\mathfrak{p}}$, then $\mathfrak{q} := \tilde{\mathfrak{q}} \cap B$ is a prime ideal of B the property that $\mathfrak{q} \cap A = \tilde{\mathfrak{q}} \cap A = \tilde{\mathfrak{p}} \cap A = \mathfrak{p}$. Hence there is no loss in generality in assuming that A is a local ring and $\mathfrak{p}$ is its unique maximal ideal $\mathfrak{m}_A$.

We claim that $\mathfrak{m}_A B \neq B$. Otherwise $1 \in B$ can be written as an $\mathfrak{m}_A$-linear combination of a finite set elements of B. Denote by B' the A-algebra generated by this finite set. Then B' is an integral extension of A and finitely generated as an A-algebra. This implies that B' is a finitely generated A-module. Since $1 \in \mathfrak{m}_A B'$ we have $B' = \mathfrak{m}_A B'$, and it then follows from Nakayama's lemma (recalled below) that $B' = 0$. This is clearly a contradiction.

Now that we know that $\mathfrak{m}_A B \neq B$, we can take for $\mathfrak{q}$ any maximal ideal of B which contains the ideal $\mathfrak{m}_A B$: then $\mathfrak{q}B \cap A$ is a maximal ideal of A, hence equals $\mathfrak{m}_A$.

For the refinement and the incomparability property we can, simply by passing to the integral extension $A/(\mathfrak{q}' \cap A) \subset B/\mathfrak{q}'$, assume that $\mathfrak{q}' = 0$. This reduces the refinement to the case already treated, while the incomparability property then amounts showing that $\mathfrak{q} \neq (0)$ implies $\mathfrak{q} \cap A \neq (0)$. If b is a nonzero element of $\mathfrak{q}$, then it is a root of a monic polynomial: $b^n + a_1 b^{n-1} + \cdots + a_{n-1} b + a_n = 0$ ($a_i \in A$), where we can of course assume that $a_n \neq 0$ (otherwise divide by b). We then find that $0 \neq a_n \in Bb \cap A \subset \mathfrak{q} \cap A$.

Since B is a union of finitely generated A-modules, the last clause follows if we prove that $\mathrm{Frac}(B) = \mathrm{Frac}(A)B$. Let $b \in B$. It is a root of a monic polynomial $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ ($a_i \in A$) with $a_n \neq 0$ and so $1/b = -1/a_n.(b^{n-1} + a_1 b^{n-2} + \cdots + a_{n-1}) \in \mathrm{Frac}(A)B$. □

REMARK 7.4. Note that the *going-up property* implies that for any strictly ascending sequence $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ of prime ideals in A is the intersection with A of a (necessarily strictly) ascending sequence of prime ideals $\mathfrak{q}_0 \subset \mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_n$ in B. Conversely, the incomparability property implies that if we intersect a strictly

ascending sequence of prime ideals $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_n$ in B with A, we get a strictly ascending sequence of prime ideals of A.

For completeness we state and prove:

LEMMA 7.5 (Nakayama's lemma). *Let R be a local ring with maximal ideal $\mathfrak{m}$ and M a finitely generated R-module. Then a finite subset $S \subset M$ generates M as a R-module if (and only if) the image of S in $M/\mathfrak{m}M$ generates the latter as a $R/\mathfrak{m}$-vector space. In particular (take $S = \emptyset$), $\mathfrak{m}M = M$ implies $M = 0$.*

PROOF. In fact, we first reduce to the case when $S = \emptyset$ by passing to M/RS. Our assumptions then say that $M = \mathfrak{m}M$. We must show that $M = 0$. Let $\pi : R^n \to M$ be an epimorphism of R-modules and denote the standard basis of R^n by $(e_1, \ldots, e_n)$. By assumption there exist $x_{ij} \in \mathfrak{m}$ such that $\pi(e_i) = \sum_{j=1}^{s} x_{ij}\pi(e_j)$. So if $\sigma := (\delta_{ij} - x_{ij})_{i,j} \in \mathrm{End}(R^n)$, then $\pi\sigma = 0$. Notice that $\det(\sigma) \in 1 + \mathfrak{m}$. Since $1 + \mathfrak{m}$ consists of invertible elements, Cramer's rule shows that σ is invertible. So $\pi = \pi(\sigma\sigma^{-1}) = (\pi\sigma)\sigma^{-1} = 0$ and hence $M = 0$. □

EXERCISE 35. Prove that an integral extension $A \subset B$ defines surjective morphisms $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ and $\mathrm{Specm}(B) \to \mathrm{Specm}(A)$.

DEFINITION 7.6. We say that a morphism of affine varieties $f : X \to Y$ is *finite* if the k-algebra homomorphism $f^* : A(Y) \to A(X)$ is finite, i.e., makes $A(X)$ a finitely generated $A(Y)$-module.

EXERCISE 36. Prove that if Y is an affine variety, then the disjoint union of its irreducible components is finite over Y.

In the corollary below we use our recent definition 6.10 of an affine variety.

COROLLARY 7.7. *Let $f : X \to Y$ be a finite morphism of affine varieties such that $f^* : A(Y) \to A(X)$ is injective. Then f is surjective, in particular, every closed irreducible subset $Y' \subset Y$ is the image of a closed irreducible subset $X' \subset X$. If furthermore is given a closed irreducible subset $X'' \subset X$ with $f(X'') \supset Y'$, then we may choose $X' \subset X''$.*

If in addition X is irreducible, then so is Y and $f^* : k(Y) \to k(X)$ is a finite algebraic extension.

PROOF. Apply Proposition 7.3 to f^*. □

EXERCISE 37. Prove that a finite morphism $f : X \to Y$ of affine varieties is closed and that every fiber $f^{-1}(y)$ is finite (possibly empty).

THEOREM 7.8 (Noether normalization). *Let K be a field. Every finitely generated K-algebra B is a finite extension of a polynomial algebra over K: there exist an integer $r \geq 0$ and an injection $K[x_1, \ldots, x_r] \hookrightarrow B$ such that B is finite over $K[x_1, \ldots, x_r]$. In fact, if we are given an epimorphism $\phi : K[x_1, \ldots, x_m] \to B$ of K-algebras, then ϕ is an isomorphism or we can take in this statement $r < m$.*

The proof will be with induction on m and the induction step is worth recording separately.

LEMMA 7.9. *Let $\phi : K[x_1, \ldots, x_m] \to B$ be an epimorphism of K-algebras, which is not an isomorphism. Then there exists a K-algebra homomorphism $\phi' : K[x_1, \ldots, x_{m-1}] \to B$ such that $\phi(x_m)$ is integral over the image of ϕ'.*

PROOF. We define for any positive integer s a K-algebra automorphism σ_s of $K[x_1,\dots,x_m]$ by $\sigma_s(x_m) = x_m$ and $\sigma_s(x_i) := x_i + x_m^{s^{m-i}}$ for $i < m$ (its inverse fixes x_m and sends x_i to $x_i - x_m^{s^{m-i}}$ for $i < m$). So if $I = (i_1,\dots,i_m) \in \mathbb{Z}^m_{\geq 0}$, and $x^I := x_1^{i_1}\cdots x_m^{i_m}$, then

$$\sigma_s(x^I) = (x_1 + x_m^{s^{m-1}})^{i_1}\cdots(x_{m-1} + x_m^s)^{i_{m-1}} x_m^{i_m}.$$

When viewed as an element of $K[x_1,\dots,x_{m-1}][x_m]$, this is a monic polynomial in x_m of degree $p_I(s) := i_1 s^{m-1} + i_2 s^{m-2} + \cdots + i_m$. Now give $\mathbb{Z}^m_{\geq 0}$ the lexicographic ordering: this means that $I > J$ implies $p_I(s) > p_J(s)$ for s large enough. Choose a nonzero $f \in \ker(\phi)$. Then $\sigma_s(f) \in \ker(\phi\sigma_s^{-1})$. If $I \in \mathbb{Z}^m_{\geq 0}$ is the largest multi-exponent of a monomial that appears in f with nonzero coefficient, then for s large enough, $\sigma_s(f)$ is a constant times a monic polynomial in x_m of degree $p_I(s)$ with coefficients in $K[x_1,\dots,x_{m-1}]$ and hence $\phi\sigma_s^{-1}(x_m) = \phi(x_m)$ becomes integral over $\phi\sigma_s^{-1}K[x_1,\dots,x_{m-1}]$. So $\phi' := \phi\sigma_s^{-1}|K[x_1,\dots,x_{m-1}]$ is then as desired. □

PROOF OF NOETHER NORMALIZATION. Let $\phi : K[x_1,\dots,x_m] \to B$ be an epimorphism of K-algebras which is not an isomorphism (otherwise we are done). We prove the refined version of the theorem with induction on m. According to Lemma 7.9, there exists a K-algebra homomorphism $\phi' : K[x_1,\dots,x_{m-1}] \to B$ such that $\phi(x_m)$ is integral over $B' := \phi'(K[x_1,\dots,x_{m-1}])$. By induction, B' is a finite extension of some polynomial algebra $K[x_1,\dots,x_r]$ with $r \leq m-1$. Hence so is B. □

REMARK 7.10. If A is a domain, then according to Proposition 7.3, $\mathrm{Frac}(A)$ will be a finite extension of $K(x_1,\dots,x_r)$ and so r must be the transcendence degree of $\mathrm{Frac}(A)/K$. In particular, r is an invariant of A.

COROLLARY 7.11. *For every affine variety Y there exists an integer $r \geq 0$ and a finite surjective morphism $f : Y \to \mathbb{A}^r$.*

This corollary gives us a better grasp on the geometry of Y, especially when Y is irreducible, for it shows that Y can be spread over $\mathbb{A}^r$ in a finite-to-one manner over affine r-space. The last assertion of Proposition 7.3 has a converse, also due to Noether, which we state without proof.

*THEOREM 7.12 (Emmy Noether). *Let K be a field and A be a finitely generated K-domain. Then for any finite field extension $L/\mathrm{Frac}(A)$, the integral closure $\overline{A}^L$ of A in L is finite over A.*

If we take $L = \mathrm{Frac}(A)$, then $\overline{A}^L$ is called the *normalization* of A and if A equals its normalization, then we say that A is *normal*. We carry this terminology to the geometric setting by saying that an irreducible affine variety X is *normal* when $A(X)$ is. Any nonempty open subset of $\mathbb{A}^n$ is normal. More generally:

LEMMA 7.13. *Any unique factorization domain A is normal.*

PROOF. Suppose $b \in \mathrm{Frac}(A)$ is integral over A: $b^d + a_1 b^d + \cdots + a_d$ with $a_i \in A$. Write $b = r/s$ with r, s relatively prime. Then $r^d + a_1 r s^{d-1} + \cdots + a_d s^d$ and we see that r^d is divisible by s. This can only happen when s is a unit, so that $b \in A$. □

Proposition 7.12 has a remarkable geometric interpretation: let be given an irreducible affine variety Y and a finite field extension $L/k(Y)$. Then Proposition 7.12 asserts that $\overline{A}^L$ is a finitely generated $A(Y)$-module. It is also an domain (because it is contained in a field) and so it defines an irreducible variety $Y_L := \mathrm{Spec}(\overline{A}^L)$. Since $A \subset \overline{A}^L$ is an integral extension, we have a finite surjective morphism $Y_L \to Y$. Notice that this morphism induces the given field extension $L/k(Y)$. This shows that every finite field extension of $k(Y)$ is canonically realized by a finite morphism of irreducible affine varieties!

If L is a separable algebraic closure of $k(Y)$, then this does not apply, for $L/k(Y)$ will not be finite, unless Y is a singleton. But L can be written as a monotone union of finite (separable) field extensions: $L = \cup_{i=1}^{\infty} L_i$ with $L_i \subset L_{i+1}$ and L_{i+1}/L_i finite. This yields a sequence of finite surjective morphisms

$$Y \leftarrow Y_{L_1} \leftarrow Y_{L_2} \leftarrow Y_{L_3} \leftarrow \cdots$$

of which the projective limit can be understood as a "pro-affine variety" (a point of this limit is given by a sequence $(y_i \in Y_{L_i})_{i=1}^{\infty}$ such that y_{i+1} maps to y_i for all i). Its algebra of regular functions is $\cup_{i=1}^{\infty} \overline{A(Y)}^{L_i} = \overline{A(Y)}^L$ (which is usually not a finitely generated k-algebra) and its function field is L.

Of special interest is the case of a finite Galois extension. We begin with the corresponding result from commutative algebra which has also important applications in algebraic number theory:

PROPOSITION 7.14. *Let A be a normal domain and let $L/\mathrm{Frac}(A)$ be a finite normal extension with Galois group G. Then G leaves invariant the integral closure $\overline{A}^L$ of A in L, and for every prime ideal $\mathfrak{p} \subset A$, G acts transitively on the set of prime ideals $\mathfrak{q} \subset \overline{A}^L$ that lie over $\mathfrak{p}$ (i.e., with $\mathfrak{q} \cap A = \mathfrak{p}$).*

PROOF. That any $g \in G$ leaves invariant $\overline{A}^L$ is clear, for g fixes the coefficients of an equation of integral dependence over A.

Let $\mathfrak{q}$ and $\mathfrak{q}'$ lie over $\mathfrak{p}$. We first show that $\mathfrak{q}' \subset \cup_{g \in G} g\mathfrak{q}$. If $b \in \mathfrak{q}'$, then the norm of b over $\mathrm{Frac}(A)$, which is defined as the product $\prod_{g \in G} gb$, lies in $\mathrm{Frac}(A)$, and hence in $\overline{A}^L \cap \mathrm{Frac}(A)$. Since A is assumed to be normal, we have $\overline{A}^L \cap \mathrm{Frac}(A) = A$. Hence $\prod_{g \in G} gb \in A \cap \mathfrak{q}' = \mathfrak{p} \subset \mathfrak{q}$. So we must have $gb \in \mathfrak{q}$ for some $g \in G$, or equivalently, $b \in g^{-1}\mathfrak{q}$.

From $\mathfrak{q}' \subset \cup_{g \in G} g\mathfrak{q}$ and the fact that each $g\mathfrak{q}$ is a prime ideal, it follows from the prime avoidance lemma below that $\mathfrak{q}' \subset g\mathfrak{q}$ for some $g \in G$. Since both $\mathfrak{q}'$ and $g\mathfrak{q}$ lie over $\mathfrak{p}$, the incomparability property implies that $\mathfrak{q}' = g\mathfrak{q}$. □

LEMMA 7.15 (The prime avoidance lemma). *Let R be a ring, $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ prime ideals in R and $I \subset R$ an ideal contained in $\cup_{i=1}^n \mathfrak{q}_i$. Then $I \subset \mathfrak{q}_i$ for some i.*

PROOF. We prove this induction on n. The case $n = 1$ being trivial, we may assume that $n > 1$ and that for every $i = 1, \ldots, n$, I is not contained in $\cup_{j \neq i} \mathfrak{q}_j$. Choose $a_i \in I \setminus \cup_{j \neq i} \mathfrak{q}_j$. So then $a_i \in \mathfrak{q}_i$. Consider $a := a_1 a_2 \cdots a_{n-1} + a_n$. Then $a \in I$ and hence $a \in \mathfrak{q}_i$ for some i. If $i < n$, then $a_n = a - a_1 a_2 \cdots a_{n-1} \in \mathfrak{q}_i$ and we get a contradiction. If $i = n$, then $a_1 a_2 \cdots a_{n-1} = a - a_n \in \mathfrak{q}_n$ and hence $a_j \in \mathfrak{q}_n$ for some $j \leq n-1$. This is also a contradiction. □

We transcribe this to algebraic geometry:

COROLLARY 7.16. *Let Y be a normal variety and $L/k(Y)$ be a normal Galois extension with Galois group G. Then G acts on Y_L in such a manner that it commutes with $f : Y_L \to Y$: for all $g \in G$ we have $fg = f$. If $Y' \subset Y$ is closed an irreducible, then G acts transitively on the irreducible components of $f^{-1}Y'$. In other words, G acts transitively on the fibers of f (including the fibers over nonclosed points).*

This also leads for normal domains to a supplement of the going up property:

COROLLARY 7.17 (Going down property). *Suppose A is a normal domain and $B \supset A$ an integral extension without zero divisors. Given prime ideals $\mathfrak{p}$ in A and $\mathfrak{q}'$ in B such that $\mathfrak{q}' \cap A \supset \mathfrak{p}$, then there exists a prime ideal $\mathfrak{q}$ in B with $\mathfrak{q} \cap A \subset \mathfrak{p}$.*

PROOF. Choose an algebraic closure $\overline{\mathrm{Frac}(B)}$ of $\mathrm{Frac}(B)$ and let L be the subfield of $\overline{\mathrm{Frac}(B)}$ generated by all the $\mathrm{Frac}(A)$-embeddings of $\mathrm{Frac}(B)$ in $\overline{\mathrm{Frac}(B)}$ (so this is obtained by adjoining the roots of the irreducible polynomials in $\mathrm{Frac}(A)[x]$ having a root in $\mathrm{Frac}(B)$). Galois theory tells us that this is a finite normal extension of $\mathrm{Frac}(B)$ (with Galois group G, say), which brings us in the situation of Proposition 7.14 above. Since L contains $\mathrm{Frac}(B)$, $\overline{A}^L$ contains B. Observe that $\overline{A}^L$ is finite over B and (hence) over A.

Put $\mathfrak{p}' := \mathfrak{q}' \cap A$ so that $\mathfrak{p}' \supset \mathfrak{p}$. According to Proposition 7.3 we can find in $\overline{A}^L$ nested prime ideals $\tilde{\mathfrak{p}}' \supset \tilde{\mathfrak{p}}$ which meet A in $\mathfrak{p}' \supset \mathfrak{p}$. Similarly, there exists a prime ideal $\tilde{\mathfrak{q}}'$ in $\overline{A}^L$ which meets B in $\mathfrak{q}'$. Since $\tilde{\mathfrak{q}}'$ and $\mathfrak{p}'$ both meet A in $\mathfrak{p}'$, there exists according to Proposition 7.14 a $g \in G$ which takes $\tilde{\mathfrak{p}}'$ to $\tilde{\mathfrak{q}}'$. Then upon replacing $\tilde{\mathfrak{p}}'$ by $g'\tilde{\mathfrak{p}}'$, we may assume that $\tilde{\mathfrak{p}}' = \tilde{\mathfrak{q}}'$. Then $\mathfrak{q} := \tilde{\mathfrak{p}} \cap B$ is as desired: it meets A in $\mathfrak{p}$ and is contained in $\tilde{\mathfrak{p}}' \cap B = \tilde{\mathfrak{q}}' \cap B = \mathfrak{q}$. □

8. Dimension

One way to define the dimension of a topological space X is as follows: the empty set has dimension -1 and X has dimension $\leq n$ if it admits a basis of open subsets such that the boundary of every basis element has dimension $\leq n-1$. This is close in spirit to the definition that we shall use here (which is however adapted to the Zariski topology; as you will find in Exercise 38, it is useless for Hausdorff spaces).

DEFINITION 8.1. Let X be a nonempty topological space. We say that the *Krull dimension of X* is at least d if there exists an *irreducible chain of length d* in X, that is, a strictly descending chain of closed irreducible subsets $Y^0 \supsetneq Y^1 \supsetneq \cdots \supsetneq Y^d$ of X. The *Krull dimension* of X is the supremum of the d for which an irreducible chain of length d exists and we then write $\dim X = d$. We stipulate that the Krull dimension of the empty set is -1.

LEMMA 8.2. *For a subset Z of a topological space X we have* $\dim Z \leq \dim X$.

PROOF. If $Y \subset Z$ is irreducible, then so is its closure $\bar{Y}$ in X. So if we have an irreducible chain of length d in Z, then the closures of the members of this chain yield an irreducible chain of length d in X. This proves that $\dim Z \leq \dim X$. □

EXERCISE 38. What is the Krull dimension of a nonempty Hausdorff space?

EXERCISE 39. Let U be an open subset of the space X. Prove that for an irreducible chain $Y^\bullet$ in X of length d with $U \cap Y^d \neq \emptyset$, $U \cap Y^\bullet$ is an irreducible

chain of length d in U. Conclude that if $\mathcal{U}$ is an open covering of X, then $\dim X = \sup_{U\in\mathcal{U}} \dim U$.

EXERCISE 40. Suppose that X is a noetherian space. Prove that the dimension of X is the maximum of the dimensions of its irreducible components. Prove also that if all the singletons (= one element subsets) in X are closed, then $\dim(X) = 0$ if and only if X is finite.

It is straightforward to transcribe this notion of dimension into algebra:

DEFINITION 8.3. Let R be a ring. We say that the *Krull dimension of R* is at least d if there exists an *prime chain of length d* in R, that is, a strictly ascending chain $\mathfrak{p}_\bullet$ of prime ideals $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_d$ in R. The *Krull dimension* of R is the supremum of the d for which this is the case and we then write $\dim R = d$. We stipulate that the trivial ring $R = \{0\}$ (which has no prime ideals) has Krull dimension -1.

The prime ideals of a ring R are the preimages of the prime ideals of $R_{\rm red} := R/\sqrt{(o)}$ and so these rings have the same dimension.

It is clear that for a closed subset $X \subset \mathbb{A}^n$, $\dim A(X) = \dim X$. Similarly, we have that for a finitely generated k-algebra A, $\dim A = \dim \mathrm{Spec}(A)$.

Remark 7.4 shows immediately:

LEMMA 8.4. *The Krull dimension is invariant under integral extension: if B is integral over A, then A and B have the same Krull dimension.*

The notion of Krull dimension was easily defined, but can be difficult to use in concrete cases. How can we be certain that given prime chain has maximal possible length? It is not even clear how we can tell whether the Krull dimension of a given ring is finite. We will settle this for a finitely generated k-domain (i.e., of the form $A(Y)$ with Y an irreducible affine variety), by showing that this is just the transcendence degree over k of its field of fractions.

THEOREM 8.5. *Let K be a field. For a finitely generated K-domain A, the Krull dimension of A equals the transcendence degree of $\mathrm{Frac}(A)/K$. Moreover, every maximal prime chain in A (i.e., one that cannot be extended to a longer prime chain) has length $\dim A$.*

PROOF. We prove both assertions with induction on the transcendence degree of $\mathrm{Frac}(A)$. By Noether normalization there exists an integer $r \geq 0$ and a K-linear embedding of $K[x_1, \ldots, x_r]$ in A such that A is finite over $K[x_1, \ldots, x_r]$. Then $\mathrm{Frac}(A)$ is a finite extension of $K(x_1, \ldots, x_r)$ and so the transcendence degree of $\mathrm{Frac}(A)/K$ is r.

Let $(0) = \mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_m$ be a prime chain of A of length m. By the incomparability property, $\mathfrak{p}_\bullet := \mathfrak{q}_\bullet \cap S_r$ is then a prime chain in S_r, also of length m. Choose an irreducible $f \in \mathfrak{p}_1$. After renumbering the coordinates, we may assume that f does not lie in $K[x_1, \ldots, x_{r-1}]$ and so $f = \sum_{i=0}^N a_{N-i} x_r^i$ with $a_i \in K[x_1, \ldots, x_{r-1}]$, $a_0 \neq 0$ and $N > 1$. Then the image of x_r in $\mathrm{Frac}(S_r/(f))$ is a root of the monic polynomial $x_r^N + \sum_{i=0}^{N-1}(a_{N-i}/a_0)x_r^i \in K(x_1, \ldots, x_{r-1})[x_r]$ so that $\mathrm{Frac}(S_r/(f))$ is a finite extension of $K(x_1, \ldots, x_{r-1})$. Hence $\mathrm{Frac}(S_r/(f)$ has transcendence degree $r-1$ over K. By our induction induction hypothesis, the Krull dimension of $S_r/(f)$ equals $r-1$. The image of the subchain $\mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_m$ in $S_d/(f)$ will still be strictly ascending (for it will be so in $S_r/\mathfrak{p}_1$) and so $m-1 \leq r-1$. Hence $m \leq r$.

On the other hand, r is attained as the length of a prime chain in A, for the prime chain of length r in S_r given by $(0) \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq \cdots \subsetneq (x_1, x_2, \ldots, x_r)$, lifts to one in A, by Remark 7.4.

The last assertion relies on the going down theorem. If we assume that $\mathfrak{q}_\bullet$ is a maximal prime chain in A, then the going down property Corollary **??** (which applies here since S_r is normal) implies that $\mathfrak{p}_\bullet$ is one in S_r. Since our irreducible f generates a prime ideal, it must then generate $\mathfrak{p}_1$. The image of $\mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_m$ in $S_r/\mathfrak{p}_1 = S_r/(f)$ is then a maximal prime chain in $S_r/(f)$ and hence of length $r-1$ by induction hypothesis. This shows that $m = r$. □

If $S \subset R$ is a multiplicative system, then the preimage of a prime ideal $\tilde{\mathfrak{q}}$ of $S^{-1}R$ under the ring homomorphism $R \to S^{-1}R$ is a prime ideal $\mathfrak{q}$ of R which does not meet S and we have $\tilde{\mathfrak{q}} = S^{-1}\mathfrak{q}$. This sets up a bijection between the prime ideals of $S^{-1}R$ and those of R not meeting S. If we take $S = R - \mathfrak{p}$, with $\mathfrak{p}$ a prime ideal, then this implies that $\dim R_\mathfrak{p}$ is the supremum of the prime chains in R which end with $\mathfrak{p}$. Since the prime chains in R which start with $\mathfrak{p}$ correspond to prime chains in $R/\mathfrak{p}$, it follows that $\dim R_\mathfrak{p} + \dim R/\mathfrak{p}$ is the supremum of the prime chains in R which contain $\mathfrak{p}$. According to Theorem 8.5, the latter is for a domain R finitely generated over a field always equal to the dimension of R.

COROLLARY 8.6. *Let X be an irreducible affine variety. Then every irreducible chain in X is a subchain of one of length $\dim X$. Moreover, every nonempty open affine $U \subset X$ has the same dimension as X.*

EXERCISE 41. Prove that a hypersurface in $\mathbb{A}^n$ has dimension $n-1$.

EXERCISE 42. Let X be an irreducible affine variety and $Y \subset X$ an irreducible closed subvariety. Prove that $\dim X - \dim Y$ is equal to the Krull dimension of $A(X)_{I(Y)}$.

EXERCISE 43. Prove that when X and Y are irreducible affine varieties, then $\dim(X \times Y) = \dim X + \dim Y$. (Hint: Embed each factor as a closed subset of some affine space. You may also want to use the fact that the equality to be proven holds in case $X = \mathbb{A}^m$ and $Y = \mathbb{A}^n$.)

9. Nonsingular points

In this section we focus on the local properties of an affine variety $X = \mathrm{Spec}(A)$ (so $A = A(X)$ is here a reduced finitely generated k-algebra) at a point o (which most of the time will be a closed point of X) and so a central role will be played by the local algebra $A_{\mathfrak{p}_o} := (A - \mathfrak{p}_o)^{-1}A$ whose maximal ideal is $(A - \mathfrak{p}_o)^{-1}\mathfrak{p}_o$. We will write $\mathcal{O}_{X,o}$ for this local algebra and $\mathfrak{m}_{X,o}$ for its maximal ideal.

If $k = \mathbb{C}$ and $X \subset \mathbb{C}^n$ is a closed subset of dimension d, then we hope that there is a nonempty open subset of X where X is 'smooth', i.e., where X looks like a complex submanifold of complex dimension d. Our goal is to define smoothness in algebraic terms (so that it make sense for our field k) and then to show that the set of smooth points of a variety is open and dense in that variety.

Our point of departure is the implicit function theorem. One version states that if $U \subset \mathbb{R}^n$ is an open neighborhood of $o \in \mathbb{R}^n$ and $f_i : U \to \mathbb{R}$, $i = 1, \ldots n-d$ are such that $f_i(o) = 0$ and the total differentials at o, $df_1(o), \ldots, df_{n-d}(o)$ are linearly independent in o (this is equivalent to: the Jacobian matrix of $(f_1, \ldots, f_{n-d})$ at o is

of rank $n-d$), then the common zero set of $f_1, \ldots, f_{n-d}$ is a submanifold of dimension d at o whose tangent space there is the common zero set of $df_1(o), \ldots, df_{n-d}(o)$. In fact, this solution set is there the graph of a map: we can express $n-d$ of the coordinates as smooth functions in the d remaining ones. Conversely, any submanifold of $\mathbb{R}^n$ at o of dimension d is locally thus obtained.

We begin with the observation that for any ring R partial differentiation of a polynomial $f \in R[x_1, \ldots, x_n]$ is well-defined and produces another polynomial. The same goes for a fraction $\phi = f/g$ in $R[x_1, \ldots, x_n][g^{-1}]$: a partial derivative of ϕ is a rational function (in this case with denominator g^2). We then define the *total differential* of a rational function $\phi \in R[x_1, \ldots, x_n]$ as usual:

$$d\phi := \sum_{i=1}^{n} \frac{\partial \phi}{\partial x_i}(x) dx_i,$$

where for now, we do not worry about interpreting the symbols dx_i: we think of $d\phi$ simply as a regular map from an open subset of $\mathbb{A}^n$ to a k-vector space of dimension n with basis $dx_1, \ldots, dx_n$, leaving its intrinsic characterization for later. However, caution is called for when R is a field of positive characteristic:

EXERCISE 44. Prove that $f \in k[x]$ has zero derivative, if and only if f is constant or (when $\mathrm{char}(k) = p > 0$) a pth power of some $g \in k[x]$.

Generalize this to: given $f \in k[x_1, \ldots, x_n]$, then $df = 0$ if and only if f is constant or (when $\mathrm{char}(k) = p > 0$) a pth power of some $g \in k[x_1, \ldots, x_n]$.

We should also be aware of the failure of the inverse function theorem:

EXAMPLE 9.1. Let $C \subset \mathbb{A}^2$ be the curve defined by $y^2 = x^3 + x$. By any reasonable definition of smoothness we should view the origin $(0,0)$ as a smooth point of C. Indeed, the projection $f : C \to \mathbb{A}^1$, $(x, y) \mapsto y$, would be a local-analytic isomorphism in case $k = \mathbb{C}$. But the map is not locally invertible within our category: the inverse requires us to find a rational function $x = u(y)$ which solves the equation $y^2 = x^3 + x$ and it is easy to verify that none exists. (We can solve for x formally: $x = u(y) = y^2 - y^6 + 3y^{10} + \cdots$, where it is important to note that the coefficients are all integers so that this works for every characteristic.) In fact, the situation is worse: no affine neighborhood U of $(0,0)$ in C is isomorphic to an open subset V of $\mathbb{A}^1$. The reason is that this would imply that $k(C) = k(U)$ is isomorphic to $k(V) = k(x)$ and one can show that this is not so.

Somewhat related to this is an issue illustrated by the following example.

EXAMPLE 9.2. Consider the curve $C' \subset \mathbb{A}^2$ defined by $xy = x^3 + y^3$ and let $o = (0,0)$. The polynomial $x^3 + y^3 - xy$ is irreducible in $k[x, y]$, so that $A(C')$ is without zero divisors. Hence $\mathcal{O}_{C',o} \subset k(C')$ is also without zero divisors. But C' seems to have two branches at o which apparently can only be recognized formally: one such branch is given by $y = u(x) = x^2 + x^5 + 3x^8 + \cdots$ and the other by interchanging the roles of x and y: $x = v(y) = y^2 + y^5 + 3y^8 + \cdots$. If we use $\xi := x - v(y)$ and $\eta := y - u(x)$ as new formal coordinates, then C' is simply given at 0 by the reducible equation $\xi\eta = 0$.

These examples make it clear that for a local understanding of a variety X at o, the local ring $\mathcal{O}_{X,o}$ still carries too much global information, and that one way to get

rid of this overload might be by passing formal power series. This is accomplished by passage to what is known as

9.3. FORMAL COMPLETION. Let R be a ring and $I \subsetneq R$ a proper ideal. We endow every R-module M with a topology, the *I-adic topology* of which a basis is the collection additive translates of the submodules $I^n M$, i.e., the collection of subsets $a + I^n M$, $a \in M$, $n \geq 0$. This is a topology indeed: given two basic subsets $a + I^n M$, $a' + I^{n'} M$, then for any element c in their intersection, the basic subset $c + I^{\max\{n,n'\}} M$ is also in their intersection. The fact that our basis is translation invariant implies that with this topology, M is a topological abelian group ($(a, b) \in M \times M \mapsto a - b \in M$ is continuous). If we endow R also with the I-adic topology and $R \times M$ with the product topology, then the map $(r, a) \in R \times M \to ra \in M$ which gives the action by R is also continuous.

For the topology on M to be Hausdorff, it suffices that the intersection of all neighborhoods of 0 is reduced to $\{0\}$: $\cap_{n\geq 0} I^n M = \{0\}$. It is then even metrizable: if $\phi : \mathbb{Z}_+ \to (0, \infty)$ is any strictly monotonously decreasing function with $\lim_{n\to\infty} \phi(n) = 0$ (one often takes u^{-n}, where $u > 1$), then a metric ρ is defined by

$$\rho(a, a') := \inf\{\phi(n) \,:\, a - a' \in I^n M\}.$$

This metric is *nonarchimedean* in the sense that $\rho(a, a'') \leq \max\{\rho(a, a'), \rho(a', a'')\}$. and a sequence $(a_n \in M)_{n=0}^{\infty}$ is then a Cauchy sequence if and only if for every integer $n \geq 0$ all but finitely many terms lie in the same coset of $I^n M$ in M; in other words, there exists an index $i_n \geq 0$ such that $a_j - a_{i_n} \in I^n M$ for all $j \geq i_n$. This makes it clear that the notion of Cauchy sequence is independent of the choice of ϕ. We also note that the Cauchy sequence defines a sequence of cosets $(\alpha_n \in M/I^n M)_{n\geq 0}$ with the property that α_n is the reduction of $\alpha_{n+1} \in M/I^{n+1}$. Recall that a metric space is said to be *complete* if every Cauchy sequence in that space converges. A standard construction produces a completion of every metric space M: its points are represented by Cauchy sequences in M, with the understanding that two such sequences represent the same point if the distance between the two nth terms goes to zero as $n \to \infty$. In the present situation this yields what is called the *I-adic completion*, $\hat{M}_I$. From the above discussion we see that an element of $\hat{M}_I$ is uniquely given by a sequence $(\alpha_n \in M/I^n M)_{n\geq 0}$ whose terms are compatible in the sense that α_n is the reduction of α_{n+1} for all n. It is an R-module for componentwise addition and multiplication so that the obvious map $M \to \hat{M}_I$, $a \mapsto (a + I^n)_{n\geq 0}$ is a R-module homomorphism. (This makes $\hat{M}_I$ a submodule of the R-module $\prod_{n=0}^{\infty} M/I^n M$.) It is easy to verify that $\hat{M}_I$ is complete for the $\hat{I}$-adic topology and that the homomorphism $M \to \hat{M}_I$ is continuous and has dense image.

Notice that $\hat{R}_I$ is in fact a subring of $\prod_{n=0}^{\infty} R/I^n$ in a way that makes $R \to \hat{R}_I$ a ring homomorphism. Moreover, $\hat{M}_I$ is a $\hat{R}_I$-module (use that $M/I^n M$ is a R/I^n-module for every n) and an R-homomorphism $\phi : M \to N$ of R-modules extends uniquely to an $\hat{R}_I$-homomorphism $\hat{\phi}_I : \hat{M}_I \to \hat{N}_I$ (use that ϕ sends $I^n M$ to $I^n N$ and hence induces a homomorphism $M/I^n \to N/I^n$).

EXAMPLE 9.4. Take the ring $k[x_1, \ldots, x_n]$. Its completion relative the maximal ideal $(x_1, \ldots, x_n)$ is just the ring of formal power series $k[[x_1, \ldots, x_n]]$. We get the same result if we do this for the localization $\mathcal{O}_{\mathbb{A}^n, o}$ of $k[x_1, \ldots, x_n]$ at $(x_1, \ldots, x_n)$.

EXAMPLE 9.5. Take the ring $\mathbb{Z}$. Its completion with respect to the ideal (p), p prime, yields the ring of p-adic integers $\hat{\mathbb{Z}}_{(p)}$: an element of $\hat{\mathbb{Z}}_{(p)}$ is given by a sequence $(a_i \in \mathbb{Z}/(p^i))_{i=1}^{\infty}$ with the property that a_i is the image of a_{i+1} under the reduction $\mathbb{Z}/(p^{i+1}) \to \mathbb{Z}/(p^i)$. We get the same result if we do this for the localization $\mathbb{Z}_{(p)} = \{a/b : a \in \mathbb{Z}, b \in \mathbb{Z} - (p)\}$. If n is an integer ≥ 2, then it follows from the Chinese remainder theorem that $\hat{\mathbb{Z}}_{(n)} = \prod_{p|n} \hat{\mathbb{Z}}_{(p)}$.

EXERCISE 45. Let I and J be ideals of a ring R and m a positive integer with $J^m \subset I$. Prove that the J-adic topology is finer than the I-adic topology and that there is a natural continuous ring homomorphism $\hat{R}_J \to \hat{R}_I$. Conclude that when R is noetherian, $\hat{R}_I$ can be identified with $\hat{R}_{\sqrt{I}}$.

*LEMMA 9.6 (Artin-Rees). *Let R be a noetherian ring, $I \subset R$ an ideal, M a finitely generated R-module and $M' \subset M$ a R-submodule. Then there exists an integer $n_0 \geq 0$ such that for all $n \geq 0$:*

$$M' \cap I^{n+n_0} M = I^n (M' \cap I^{n_0} M).$$

The proof (which is ingeneous, but not difficult) can be found in any book on commutative algebra (e.g., Atiyah-Macdonald). The Artin-Rees lemma implies that for every $n \geq 0$ there exists a $n' \geq 0$ such that $M' \cap I^{n'} M \subset I^n M'$ (we can take $n' = n + n_0$). This implies that the inclusion $M' \subset M$ is not merely continuous, but that the I-adic topology on M' is induced by that of M. We will use the Artin-Rees lemma via this property only.

COROLLARY 9.7. *In the situation of Lemma 9.6, the homomorphism $\hat{M}'_I \to \hat{M}_I$ induced by the inclusion $M' \subset M$ is a closed embedding with the property that the preimage of M is M': if the image of $a \in M$ under $M \to \hat{M}_I$ lies in the image of $\hat{M}'_I \to \hat{M}_I$, then $a \in M'$. Moreover, $\hat{M}_I / \hat{M}'_I$ can be identified with the I-adic completion of M/M'.*

One might phrase this by saying that when R is noetherian, I-adic completion is an exact functor on the category of finitely generated R-modules.

PROOF OF COROLLARY 9.7. We first part of the corollary amounts to the following property: if a sequence $(a_i \in M')_{i=0}^{\infty}$ in M' is a Cauchy sequence in M, then it is already one in M' and when its limit lies in the image of M, then this limit lies in fact in the image of M' (an element of the kernel of $\hat{M}'_I \to \hat{M}_I$ is given by a sequence $(a_i \in M')_{i=0}^{\infty}$ in M' which converges in M to 0 and so this implies that $\hat{M}'_I \to \hat{M}_I$ is injective).

Suppose therefore given a sequence $(a_i \in M')_{i=0}^{\infty}$ which is a Cauchy sequence in M. Then for every n there exists an i_n such that $a_i - a_{i_n} \in I^n M$ for $i \geq i_n$. So if we take $i \geq i_{n+n_0}$, then $a_i - a_{i_n} \in M' \cap I^{n+n_0} M = I^n (M' \cap I^{n_0} M) \subset I^n M'$. Hence $(a_i \in M')_{i=0}^{\infty}$ is a Cauchy sequence in M'. If $(a_i \in M')_{i=0}^{\infty}$ converges to the image of $a \in M$, then for every n there exists an i'_n such that $a_i - a \in I^n M$ for $i \geq i'_n$. So if we take $i \geq i'_{n+n_0}$, then by the preceding argument, $a_i - a \in I^n M'$. Hence $a \in a_i + I^n M' \subset M'$ and $(a_i \in M')_{i=0}^{\infty}$ converges to the image of a in M'.

As to the last statement, we observe that $\hat{R}_I$-homomorphism $\hat{M}_I \to \widehat{M/M'}_I$ induced by the surjection $M \to M/M'$ is also surjective: any $\hat{b} \in \widehat{M/M'}_I$ is representable by a Cauchy sequence $(b_i \in M/M')_{i=0}^{\infty}$ with $b_m - b_n \in I^n (M/M')$ for

$m \geq n$. Since $I^n(M/M') \cong I^n M/(I^n M \cap M')$, we can represent $b_{n+1} - b_n$ by some $d_{n+1} \in I^n M$. Let $d_0 \in M$ lift b_0. Then the series $d_0 + d_1 + \cdots + d_n + \cdots$ converges in $\hat{M}$ and maps to $\hat{b}$.

The kernel of $M_I \to \widehat{M/M'}_I$ clearly contains M' and since a kernel is closed, it will also contain its closure $\hat{M'}_I$ in $\hat{M}_I$. In order to see that it is not bigger, let $\hat{a} \in \ker(M_I \to \widehat{M/M'}_I)$ be arbitrary. If we represent $\hat{a}$ by a Cauchy sequence $(a_i \in M)_{i=0}^{\infty}$, then for every n there exists an i_n such that for $i \geq i_n$, $a_i \in M' + I^n M$. Write a_i accordingly: $a_i = a'_i + d_i$ with $a'_i \in M'$ and $d_i \in I^n M$. Since $(d_i \in M)_{i=0}^{\infty}$ converges to $0 \in M$, $(a'_i \in M')_{i=0}^{\infty}$ is also a Cauchy sequence converging to $\hat{a}$. As we saw above, this is then a Cauchy sequence in M' with the same limit and so $\hat{a} \in \hat{M'}_I$. □

Let R be a noetherian local ring with maximal ideal $\mathfrak{m}$ and residue field κ. We use simply $\widehat{\ }$ for completion with respect to $\mathfrak{m}$.

Then $\mathfrak{m}$ is a finitely generated R-module. Since the ring R acts on $\mathfrak{m}/\mathfrak{m}^2$ via $R/\mathfrak{m} = \kappa$, $\mathfrak{m}/\mathfrak{m}^2$ is a finite dimensional vector space over κ.

DEFINITION 9.8. The *Zariski cotangent space* $T^*(R)$ of R is the κ-vector space $\mathfrak{m}/\mathfrak{m}^2$ and its κ-dual, $T(R) := \mathrm{Hom}_\kappa(\mathfrak{m}/\mathfrak{m}^2, \kappa)$ (which is also equal to $\mathrm{Hom}_R(\mathfrak{m}, \kappa)$), is called the *Zariski tangent space* $T(R)$ of R. The *embedding dimension* $\mathrm{embdim}(R)$ is the dimension of $\mathfrak{m}/\mathfrak{m}^2$ as a vector space over κ.

If X is an affine variety and $o \in X$, then the Zariski cotangent space $T^*_o X$ resp. the Zariski tangent space $T_o X$ resp. the embedding dimension $\mathrm{embdim}_o X$ of X at o are by definition that of $\mathcal{O}_{X,o}$.

For instance, the embedding dimension of $\mathbb{A}^n$ at any closed point $o \in \mathbb{A}^n$ is n. This follows from the fact that the map $d_o : f \in \mathfrak{m}_{\mathbb{A}^n,o} \mapsto df(o) \in k^n$ defines an isomorphism of k-vector spaces $\mathfrak{m}_{\mathbb{A}^n,o}/\mathfrak{m}^2_{\mathbb{A}^n,o} \cong k^n$. We note in passing that we here have a way of understanding the total differential at o in more intrinsic terms as the map $d_o : \mathcal{O}_{\mathbb{A}^n,o} \to \mathfrak{m}_{\mathbb{A}^n,o}/\mathfrak{m}^2_{\mathbb{A}^n,o}$ which assigns to $f \in \mathcal{O}_{\mathbb{A}^n,o}$ the image of $f - f(o) \in \mathfrak{m}_{\mathbb{A}^n,o}$ in $\mathfrak{m}_{\mathbb{A}^n,o}/\mathfrak{m}^2_{\mathbb{A}^n,o}$. Thus, a differential of f at o can be understood a k-linear function $df(o) : T_o\mathbb{A}^n \to k$ and $(d_o(x_i) = dx_i(o))_{i=1}^n$ is a basis of $\mathfrak{m}_{\mathbb{A}^n,o}/\mathfrak{m}^2_{\mathbb{A}^n,o}$.

Notice that the embedding dimension and the Zariski tangent space of a local ring only depend on its formal completion.

EXERCISE 46. Let $(R', \mathfrak{m})$ and $(R, \mathfrak{m}')$ be local rings with the same residue field[10] κ. Prove that a nonzero ring homomorphism $\phi : R' \to R$ induces an κ-linear map of Zariski tangent spaces $T(\phi) : T(R) \to T(R')$

An application of Nakayama's lemma to $M = \mathfrak{m}$ yields:

COROLLARY 9.9. *The embedding dimension of a noetherian local ring R is the smallest number of generators of its maximal ideal. The embedding dimension is zero if and only if R is a field.*

DEFINITION 9.10. A local ring R with maximal ideal $\mathfrak{m}$ is said to be *regular* if it is noetherian and its Krull dimension equals its embedding dimension.

[10]By this we mean that ϕ induces an isomorphism $R'/\mathfrak{m}' \cong R/\mathfrak{m}$ and that we identify the two residue fields via this isomorphism.

A point o of an affine variety X is called *regular* if its local ring $\mathcal{O}_{X,o}$ is and *singular* when it is not. (We write X_{reg} resp. X_{sing} for the subsets of X defined by this property.) An affine variety without singular points is said to be *nonsingular*.

We will show that for a closed point $o \in X$ this is indeed an intrinsic characterization of 'being like a submanifold'.

We mention without proof that an arbitrary point of X is a regular point of X precisely when its closure contains a closed point with that property. In other words, if that point is given by the closed irreducible subset $Z \subset X$, then it is regular if and only if Z contains a closed point that is also a regular point of X.

We begin with a formal version of the implicit function theorem.

LEMMA 9.11. *Let $o \in \mathbb{A}^n$ be a closed point and let $f_1, \ldots, f_{n-d} \in \mathfrak{m}_{\mathbb{A}^n,o}$ be such that their images in $\mathfrak{m}_{\mathbb{A}^n,o}/\mathfrak{m}^2_{\mathbb{A}^n,o}$ are linearly independent. Then $f_1, \ldots, f_{n-d}$ generate a prime ideal $\mathfrak{p}$ in the local ring $\mathcal{O}_{\mathbb{A}^n,o}$ and the formal completion of $\mathcal{O}_{\mathbb{A}^n,o}/\mathfrak{p}$ with respect to its maximal ideal is isomorphic to $k[[x_1, \ldots, x_d]]$ as a complete local k-algebra. Moreover, there exists an affine neighborhood U of o in $\mathbb{A}^n$ on which $f_1, \ldots, f_{n-d}$ are regular and generate a prime ideal in $A(U)$ with the property that the corresponding irreducible affine variety $X \subset U$ has o as a regular point.*

PROOF. Let us abbreviate $\mathcal{O}_{\mathbb{A}^n,o}$ by $\mathcal{O}$ and its maximal ideal by $\mathfrak{m}$. Extend $f_1, \ldots, f_{n-d}$ to a system of regular functions $f_1, \ldots, f_n \in \mathfrak{m}$ such that their images in $\mathfrak{m}/\mathfrak{m}^2$ are linearly independent. (After an affine linear transformation, we may then just as well assume that o is the origin of $\mathbb{A}^n$ and that $f_i \equiv x_i \pmod{\mathfrak{m}^2}$.) Hence the monomials of degree N in $f_1, \cdots, f_n$ map to a k-basis of $\mathfrak{m}^N/\mathfrak{m}^{N+1}$. This implies that the monomials of degree $\leq N$ in $f_1, \cdots, f_n$ make up a k-basis of $\mathcal{O}/\mathfrak{m}^{N+1}$. It follows that the map

$$y_i \in k[[y_1, \ldots, y_n]] \mapsto f_i \in \hat{\mathcal{O}}$$

determines an isomorphism $k[[y_1, \ldots, y_n]] \cong \hat{\mathcal{O}}$ of complete local rings (a ring isomorphism that is also a homeomorphism). Its inverse defines a topological embedding of $\mathcal{O}$ in $k[[y_1, \ldots, y_n]]$ (sending f_i to y_i). The ideal generated by $(y_1, \ldots, y_{n-d})$ in $k[[y_1, \ldots, y_n]]$ is the closure of the image of $\mathfrak{p}$. It is clearly a prime ideal. According to Corollary 9.7 the preimage of that prime ideal in $\mathcal{O}$ is $\mathfrak{p}$ (hence $\mathfrak{p}$ is a prime ideal) and the embedding

$$\mathcal{O}/\mathfrak{p} \hookrightarrow k[[y_1, \ldots, y_n]]/(y_1, \ldots, y_{n-d}) = k[[y_{n-d+1}, \ldots, y_n]]$$

realizes the $\mathfrak{m}$-adic completion of $\mathcal{O}/\mathfrak{p}$.

Let $U \subset \mathbb{A}^n$ be an affine neighborhood of o on which the $f_1, \ldots, f_{n-d}$ are regular and denote by $P \subset A(U)$ the preimage of $\mathfrak{p}$ under the localization homormorphism $A(U) \to \mathcal{O}$. This is a prime ideal which contains $f_1, \ldots, f_{n-d}$ and has the property that it generates the same ideal in $\mathcal{O}$ as $(f_1, \ldots, f_{n-d})$. Choose a finite set of generators $\phi_1, \ldots, \phi_r$ of P and write $\phi_i = \sum_{j=1}^{n-d} u_{ij} f_j$ with $u_{ij} \in \mathcal{O}$. By passing to a smaller U, we may then assume that each u_{ij} is regular on U so that P is in fact equal to the ideal $(f_1, \ldots, f_{n-d})$ in $A(U)$ generated by $f_1, \ldots, f_{n-d}$. Hence $(f_1, \ldots, f_{n-d})$ defines an irreducible affine variety $X \subset U$ which has o is a regular point of dimension d. □

THEOREM 9.12. *Let $X \subset \mathbb{A}^n$ be closed and let $o \in X$ be a closed point of X. Then the local ring $\mathcal{O}_{X,o}$ is regular of dimension d if and only there exist regular functions $f_1, \dots, f_{n-d}$ on an affine neighborhood U of o in $\mathbb{A}^n$ such that these functions generate $I_U(X \cap U)$ and $df_1, \dots, df_{n-d}$ are linearly independent in every point of U. In that case, $X \cap U$ is regular and for every closed point $q \in X \cap U$ the Zariski tangent space T_qX is the kernel of the linear map $(df_1(q), \dots, df_{n-d}(q)) : T_q\mathbb{A}^n \to k^{n-d}$.*

PROOF. Suppose that $\mathcal{O}_{X,o}$ is regular of dimension d. Let $\mathcal{I}_{X,o} \subset \mathcal{O}_{\mathbb{A}^n,o}$ be the ideal of regular functions at o vanishing on a neighborhood of o in X, in other words, the kernel of $\mathcal{O}_{\mathbb{A}^n,o} \to \mathcal{O}_{X,o}$. The latter is a surjective homomorphism of local rings and so the preimage of $\mathfrak{m}_{X,o}$ resp. $\mathfrak{m}_{X,o}^2$ is $\mathcal{I}_{X,o} + \mathfrak{m}_{\mathbb{A}^n,o} = \mathfrak{m}_{\mathbb{A}^n,o}$ resp. $\mathcal{I}_{X,o} + \mathfrak{m}_{\mathbb{A}^n,o}^2$. It follows that the quotient $\mathfrak{m}_{\mathbb{A}^n,o}/(\mathcal{I}_{X,o} + \mathfrak{m}_{\mathbb{A}^n,o}^2) \cong \mathfrak{m}_{X,o}/\mathfrak{m}_{X,o}^2$ has dimension d. So the image $(\mathcal{I}_{X,o}+\mathfrak{m}_{\mathbb{A}^n,o}^2)/\mathfrak{m}_{\mathbb{A}^n,o}^2$ of $\mathcal{I}_{X,o}$ in the n-dimensional vector space $\mathfrak{m}_{\mathbb{A}^n,o}/\mathfrak{m}_{\mathbb{A}^n,o}^2$ must have dimension $n-d$. Choose $f_1, \dots, f_{n-d} \in \mathcal{I}_{X,o}$ such that $df_1(o), \dots, df_{n-d}(o)$ are linearly independent. We show among other things that these functions generate $\mathcal{I}_{X,o}$ (this will in fact be the key step).

According to Lemma 9.11, the ideal $\mathfrak{p}_i \subset \mathcal{O}_{\mathbb{A}^n,o}$ generated by $f_1, \dots, f_i$ is prime and so we have a prime chain

$$(0) \subseteq \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{n-d} \subseteq \mathcal{I}_{X,o}.$$

As $\mathcal{O}_{X,o}$ is of dimension d, there also exists a prime chain of length d containing $\mathcal{I}_{X,o}$:

$$\mathcal{I}_{X,o} \subseteq \mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_d \subseteq \mathcal{O}_{\mathbb{A}^n,o}.$$

Since $\mathcal{O}_{\mathbb{A}^n,o}$ has dimension n, these two prime chains cannot make up a prime sequence of length $n+1$ and so $\mathfrak{p}_{n-d} = \mathcal{I}_{X,o} = \mathfrak{q}_0$.

In particular, $f_1, \dots, f_{n-d}$ generate $\mathcal{I}_{X,o}$. Let U' be an affine neighborhood of o in $\mathbb{A}^n$ on which the f_i's are regular and has the property that $X \cap U'$ is the common zero set of $f_1, \dots, f_{n-d}$. Since the differentials $df_1(o), \dots, df_{n-d}(o)$ are linearly independent, there exist $n-d$ indices $1 \le \nu_1 < \nu_2 < \cdots < \nu_{n-d} \le n$ such that $\delta := \det((\partial f_i/\partial x_{\nu_j})_{i,j}) \in A(U')$ is nonzero in o. Then $U := U(\delta) \subset U'$ has all the asserted properties (with the last property following from Lemma 9.11).

The converse says that if U, o and $f_1, \dots, f_{n-d}$ are as in the theorem, then the functions $f_1, \dots, f_{n-d}$ generate a prime ideal $\mathcal{I}_o$ in $\mathcal{O}_{\mathbb{A}^n,o}$ such that $\mathcal{O}_{\mathbb{A}^n,o}/\mathcal{I}_o$ is regular. This follows Lemma 9.11.

The last assertion is clear from the preceding. □

PROPOSITION 9.13. *The regular closed points of an affine variety X form an open-dense subset X_{reg} of the set of closed points of X.*

For the proof we will assume Proposition 9.14 below, which we will leave unproved for now. (Note that it tells us only something new in case k has positive characteristic.)

*PROPOSITION 9.14. *Every finitely generated field extension L/k (so with k as in these notes, i.e., algebraically closed) is* separably generated *by which we mean that there exists an intermediate extension $k \subset K \subset L$ such that K/k is purely transcendental (i.e., of the form $k(x_1, \dots, x_r)$) and L/K is a finite* separable *extension.*

According to 6.7 and the subsequent discussion, this implies that every irreducible affine variety is birationally equivalent to a hypersurface.

PROOF OF PROPOSITION 9.13. Without loss of generality we may assume that X is irreducible. Since we already know that $X_{\rm reg}$ is open, it remains to see that it is nonempty. It thus becomes an issue which only depends on $k(X)$. Hence it suffices to treat the case of a hypersurface in $\mathbb{A}^n$ so that $I(X)$ is generated by an irreducible polynomial $f \in k[x_1, \dots, n]$. In view of Lemma Lemma 9.11 it then suffices to show that df is not identically zero on X. Suppose otherwise, i.e., that each partial derivative $\partial f/\partial x_i$ vanishes on X. Then each $\partial f/\partial x_i$ must be multiple of f and since the degree of $\partial f/\partial x_i$ is less than that of f, this implies that it is identically zero. But then we know from Exercise 44 that the characteristic p of k is positive and that f is of the form g^p. This contradicts the fact that f is irreducible. □

EXERCISE 47. Let X be a nonsingular variety. Prove that X is connected if and only if it is irreducible.

REMARK 9.15. This enables us to find for an affine variety X of dimension d a descending chain of closed subsets $X = X^d \supset X^{d-1} \supset \cdots \supset X^0$ such that $\dim X^i \leq i$ and all the (finitely many) connected components of $X^i - X^{i-1}$ are nonsingular subvarieties of dimension i (such a chain is called a *stratification* of X). We let X^{d-1} be the union of $X_{\rm sing}$ and the irreducible components of dimension $< d$ and if (with downward induction) X^i has been defined, then we take for X^{i-1} the union of the singular locus $X^i_{\rm reg}$ and the irreducible components of dimension $\leq i-1$. Then $\dim X^{i-1} \leq i-1$ and every connected component of $X^i - X^{i-1}$ is an nonempty open subset of some $X^i_{\rm reg}$ and hence a nonsingular subvariety of dimension i.

9.16. DIFFERENTIALS AND DERIVATIONS. The differential that we defined earlier has an intrinsic, coordinate free description that turns out to be quite useful. Let us begin with the observation that the formation of the total differential of a polynomial, $\phi \in k[x_1, \dots, x_n] \mapsto d\phi := \sum_{i=1}^n \frac{\partial \phi}{\partial x_i}(x) dx_i$ is a k-linear map which satisfies the Leibniz rule: $d(\phi\psi) = \phi d\psi + \psi d\phi$. This property is formalized with the following definition. Let us fix a ring R (the *base ring*) and an R-algebra A.

DEFINITION 9.17. Let M be a A-module. An *R-derivation of A with values in M* is a map $D : A \to M$ is an R-module homomorphism which satisfies the Leibniz rule: $D(a_1 a_2) = a_1 D(a_2) + a_2 D(a_2)$ for all $a_1, a_2 \in A$.

The last condition usually prevents D from being an A-module homomorphism. Let us note that (by taking $a_1 = a_2 = 1$) that we must have $D(1) = 0$. Then it also follows that for every $r \in R$, $D(r) = rD(1) = 0$. Note also that if a happens to be invertible in A, then $0 = D(1) = D(a/a) = 1/aD(a) + aD(1/a)$ so that $D(1/a) = -D(a)/a^2$.

Given $a_1, \dots, a_n \in A$, then the values of D on $a_1, \dots, a_n$ determine its values on the subalgebra A' by the a_i's, for if $\phi : R[x_1, \dots, x_n] \to A$ denotes the corresponding R-homomorphism and $f \in R[x_1, \dots, x_n]$, then

$$D\phi(f) = \sum_{i=1}^n \phi\Big(\frac{\partial f}{\partial x_i}\Big) Da_i.$$

If we combine this with the formula for $D(1/a)$, we see that this even determines D on the largest subalgebra A' of A generated by the a_i's and the invertible elements in A'. In particular, if we are given a field extension L/K, then a K-derivation of L with values in some L-vector space is determined by its values on a set of generators of L as a field extension of K.

Observe that the set of R-derivations of A in M form an R-module: if D_1 and D_2 are R-derivations of A with values in M, and $a_1, a_2 \in A$, then $a_1 D_1 + a_2 D_2$ is also one. We denote this module by $\mathrm{Der}_R(A, M)$.

EXERCISE 48. Prove that if $D_1, D_2 \in \mathrm{Der}_R(A,A)$, then $[D_1,D_2] := D_1D_2 - D_2D_1 \in \mathrm{Der}_R(A,A)$. What do we get for $R = k$ and $A = k[x_1,\dots,x_n]$?

It is immediate from the definition that for every homomorphism of A-modules $\phi : M \to N$, the composition of a D as above with ϕ is an R-derivation of A with values in N. We can now construct a universal R-derivation of A, $d : A \to \Omega_{A/R}$ (where $\Omega_{A/R}$ must of course be an R-module) with the property that every D as above is obtained by composing d with a unique homomorphism of A-modules $\bar{D} : \Omega_{A/R} \to N$. The construction that is forced upon us starts with the free A-module $A^{(A)}$ which has A itself as a generating set—let us denote the generator associated to $a \in A$ by $\tilde{d}(a)$—which we then divide out by the A-submodule of $A^{(A)}$ generated by the expressions $\tilde{d}(ra) - r\tilde{d}(a)$, $\tilde{d}(a_1+a_2) - \tilde{d}(a_1) - \tilde{d}(a_2)$ and $\tilde{d}(a_1a_2) - a_1\tilde{d}(a_2) - a_2\tilde{d}(a_2)$, with $r \in R$ and $a, a_1, a_2 \in A$. The quotient A-module is denoted $\Omega_{A/R}$ and the composite of $\tilde{d}$ with the quotient map by $d : A \to \Omega_{A/R}$. The latter is an R-derivation of A by construction. Given an R-derivation $D : A \to M$, then the map which assigns to $\tilde{d}(a)$ the value Da extends (obviously) as a A-module homomorphism $A^{(A)} \to M$. It has the above submodule in its kernel and hence determines an A-module homomorphism of $\bar{D} : \Omega_{A/R} \to M$. This has clearly the property that $D = \bar{D}d$. We call $\Omega_{A/R}$ the module of *Kähler differentials*. We will see that the map $d : A \to \Omega_{A/R}$ can be thought of as an algebraic version of the formation of the (total) differential.

The universal derivation of a finitely generated R-algebra is obtained as follows. First we do the case of a polynomial algebra $P := R[x_1,\dots,x_n]$. Assigning to $f \in P$ the row vector $(\partial f/\partial x_1,\dots,\partial f/\partial x_n)$ is an R-derivation on P with values in P^n. By the universal property of $\Omega_{P/R}$ this must be given by a unique P-homomorphism $\Omega_{P/R} \to P^n$. For any R-derivation $D : P \to M$ we have $Df = \sum_{i=1}^n (\partial f/\partial x_i)Dx_i$ and the Dx_i can be prescribed arbitrarily. So if we take $M = P^n$ as above, we see that $\Omega_{P/R} \to P^n$ is an isomorphism. Thus the universal R-derivation $d : P \to \Omega_{P/R}$ may be regarded as the intrinsic way of forming the total differential.

Next consider a quotient $A := P/I$ of P, where $I \subset P$ is an ideal. If M is an A-module and $D' : A \to M$ is an R-derivation, then its composite with the projection $\pi : P \to A$, $D = D'\pi : P \to M$, is an R-derivation of P with the property that $Df = 0$ for every $f \in I$. Conversely, every R-derivation $D : P \to M$ in an A-module M with this property factors through an an R-derivation $D' : A \to M$. We observe here that the map $f \in I \mapsto D(f)$ factors through I/I^2, for if $f, g \in I$, then $D(fg) = fDg + gDf \in IM = \{0\}$. Since I/I^2 is an A-module, we thus obtain a short exact sequence of A-modules

$$I/I^2 \to \Omega_{P/R}/I\Omega_{P/R} \to \Omega_{A/R} \to 0.$$

If we are given a generating set $f_1,\dots,f_m$ for I, then $\Omega_{A/R}$ can be identified with the quotient of A^n by the A-submodule generated by the row vectors $(\partial f_i/\partial x_1,\dots,\partial f_i/\partial x_n)$, $i = 1,\dots,m$. Note that if R is a noetherian ring, then, as we know, so is A and it also follows that $\Omega_{A/R}$ is a noetherian R-module.

This applies to the case when $R = k$ and $A = A(X)$ for some affine variety X. We then write $\Omega(X)$ for $\Omega_{A(X)/k}$.

EXERCISE 49. Prove that $\Omega_{A/R}$ behaves well with localization: if $S \subset A$ is a multiplicative subset, then every R-derivation with values is some A-module M extends naturally to R-derivation of $S^{-1}A$-with values in $S^{-1}M$. Prove that we have a natural map $S^{-1}\Omega_{A/R} \to \Omega_{S^{-1}A/R}$ and that this map is a A-homomorphism.

For an affine variety X and $x \in X$, we write $\Omega_{X,x}$ for $\Omega_{\mathcal{O}_{X,x}/k}$. The preceding exercise implies that $\Omega_{X,x}$ is the localization of $\Omega(X)$ at x: $\Omega_{X,x} = (A(X) - \mathfrak{p}_x)^{-1}\Omega(X)$.

EXERCISE 50. Let X be an affine variety and let $o \in X$ be a closed point. Show that the Zariski tangent space of X at o can be understood (and indeed, be defined) as the space of k-derivations of $\mathcal{O}_{X,o}$ with values in k, where we regard k as a $\mathcal{O}_{X,o}$-module via $\mathcal{O}_{X,o}/\mathfrak{m}_{X,o} \cong k$. Prove that this identifies its dual, the Zariski cotangent space, with $\Omega_{X,o}/\mathfrak{m}_{X,o}\Omega_{X,o}$.

EXERCISE 51. Show (perhaps with the help of the preceding exercises) that if $o \in \mathbb{A}^n$ is a closed point, then $\Omega_{\mathcal{O}_{\mathbb{A}^n,o}/k}$ is the free $\mathcal{O}_{\mathbb{A}^n,o}$-module generated by $dx_1, \ldots, dx_n$ and that if X is an affine variety in $\mathbb{A}^n$ that has o a regular point, then $\Omega_{X,o}$ is a free $\mathcal{O}_{X,o}$-module of rank $\dim \mathcal{O}_{X,x}$.

We must be careful with this construction when dealing with formal power series rings. For instance, as we have seen, the completion of the local k-algebra $\mathcal{O}_{\mathbb{A}^1,0}$ with respect to its maximal ideal is $k[[x]]$ and the embedding of $\mathcal{O}_{\mathbb{A}^1,0} \hookrightarrow k[[x]]$ is given by Taylor expansion. A k-derivation D of $k[[x]]$ with values in some $k[[x]]$-module is not determined by Dx. All it determines are the values on the k-subalgebra $\mathcal{O}_{\mathbb{A}^1,0}$. This issue disappears however if we require that D commutes with infinite summation when the series converges relative to the (x)-adic metric, for then $D(\sum_{r=0}^{\infty} c_r x^r)$ will be equal to $\sum_{r=0}^{\infty} c_r r x^{r-1} Dx$.

EXERCISE 52. Prove that the composite $d : A \to \Omega_{A/R} \to (\hat{\Omega}_{A/R})_I$ factors through a derivation $\hat{d}_I : \hat{A}_I \to (\hat{\Omega}_{A/R})_I$ and prove that it is universal among all the R-derivations of A in R-modules that are complete for the I-adic topology (i.e., for which $M = \hat{M}_I$).

So if o is a regular closed point of an affine variety X, then $\hat{\Omega}_{X,o}$ is a free $\hat{\mathcal{O}}_{X,o}$-module of rank $\dim \mathcal{O}_{X,x}$.

10. Local nature of a regular function and the notion of a variety

In any topology or analysis course you learn that the notion of continuity is *local*: there exists a notion of continuity at a point so that a function is continuous if it is so at every point of its domain. We shall see that in algebraic geometry the notion of a regular function also has a local nature.

DEFINITION 10.1. Let X be an affine variety, $U \subset X$ an open subset and $\phi : U \to k$ a function. We say that ϕ is *regular* at $x \in U$ if it is so on an affine neighborhood of x in X. In other words: there should exist $g_x \in A(X) - \mathfrak{p}_x$ and $f_x \in A(X)$ such that $\phi|U(g_x) \cap U$ is representable as the fraction f_x/g_x. We say that ϕ is *locally regular* if it is so in every point of U and we denote the k-algebra of such functions by $\mathcal{O}(U)$.

We will see that for U affine, locally regular implies regular. After that, we will abandon the adjective *locally* and just speak of regular functions, whether the domain is affine or not. Both the notion of 'locally regular' and the proof that for affine varieties this is the same notion as regular have a counterpart in the context of ring spectra and we will in fact prove an intermediate result in that setting.

PROPOSITION 10.2. *The natural map $A(X) \to \mathcal{O}(X)$ is an isomorphism of k-algebras. A map $\phi : X \to Y$ between affine varieties is a morphism if and only if ϕ is continuous and for any $f \in \mathcal{O}(V)$ (with $V \subset Y$ open) we have $f^*\phi = \phi f \in \mathcal{O}(f^{-1}V)$.*

REMARK 10.3. Before we begin the proof we make the following observation. Suppose $(r_i \in R)_{i \in I}$ is a collection of elements such that $\mathrm{Spec}(R) = \cup_{i \in I} U(r_i)$. This means that the ideal generated by the r_i is not contained in any maximal ideal and hence must be all of R. In particular, this ideal contains 1 so that $1 = a_1 r_{i_1} + \cdots + a_n r_{i_n}$ for certain $i_1, \ldots, i_n \in I$ and $a_1, \ldots, a_n \in R$. It follows that $\mathrm{Spec}(R) = \cup_{\nu=1}^{n} U(r_{i_\nu})$. This shows that $\mathrm{Spec}(R)$ is quasi-compact: any open

covering of $\mathrm{Spec}(R)$ admits a finite subcovering. In particular, any affine variety has this property.

PROOF OF PROPOSITION 10.2. It is clear that the map is injective: if $f \in A(X)$ is in the kernel, then f must be identically zero as a function and hence $f = 0$.

For surjectivity, let $\phi : X \to k$ be regular in every point of X. We must show that ϕ is representable by some $f \in A(X)$. By definition there exists for every $x \in X$, $g_x \in A(X) - \mathfrak{p}_x$ and $f_x \in A(X)$ such that $\phi|U(g_x)$ is representable as the fraction f_x/g_x. Since X is quasicompact, the covering $\{U(g_x)\}_{x\in X}$ of X possesses a finite subcovering $\{U(g_{x_i})\}_{i=1}^N$. Let us now write f_i for f_{x_i} and g_i for g_{x_i}. Then f_i/g_i and f_j/g_j define the same regular function on $U(g_i) \cap U(g_j) = U(g_ig_j)$ and so $g_if_j - g_jf_i$ is annihilated by $(g_ig_j)^{m_{ij}}$ for some $m_{ij} \geq 0$. Let $m := \max\{m_{ij}\}$ so that $g_i^{m+1}g_j^m f_j = g_i^m g_j^{m+1} f_i$ for all i, j. Since $\phi|U(g_i)$ is also represented by $(f_ig_i^m)/g_i^{m+1}$ we may then without loss of generality assume that $m = 0$, so that $g_if_j = g_jf_i$ for all i, j.

Since the $U(g_i)$ cover X, the ideal generated by $g_1, \ldots, g_N$ must be all of $A(X)$ and hence contain 1. So $1 = \sum_{i=1}^N a_ig_i$ for certain $a_i \in A(X)$. Now consider $f := \sum_{i=1}^N a_if_i \in A(X)$. We have for every j,

$$fg_j = \sum_{i=1}^N a_if_ig_j = \sum_{i=1}^N a_ig_if_j = f_j$$

and so f represents ϕ on U_j. It follows that ϕ is represented by f.

The last statement is left as an exercise. □

Let us denote by $\mathcal{O}_X$ the collection of the k-algebras $\mathcal{O}(U)$, where U runs over all open subsets of X. The preceding proposition says that $\mathcal{O}_X$ is a *sheaf* of k-valued functions on X, by which we mean the following:

DEFINITION 10.4. Let X be a topological space and K a ring. A *sheaf $\mathcal{O}$ of K-valued functions*[11] on X assigns to every open subset U of X a K-subalgebra $\mathcal{O}(U)$ of the K-algebra of K-valued functions on the *set of closed points in* U with the property that

(i) for every inclusion $U \subset U'$ of open subsets of X, 'restriction to U' maps $\mathcal{O}(U')$ in $\mathcal{O}(U)$ and
(ii) given a collection $(U_i)_{i\in I}$ of open subsets of X and $f : \cup_{i\in I}U_i \to K$, then $f \in \mathcal{O}(\cup_i U_i)$ if and only if $f|U_i \in \mathcal{O}(U_i)$ for all i.

If $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ are topological spaces endowed with a sheaf of K-valued functions, then a continuous map $f : X \to Y$ is called a *morphism* if for every open $V \subset Y$, composition with f takes $\mathcal{O}_Y(V)$ to $\mathcal{O}_X(f^{-1}V)$.

With the notion of a morphism, we have a category of topological spaces endowed with a sheaf of K-valued functions. In particular, we have the notion of isomorphism: this is a homeomorphism $f : X \to Y$ which for every open $V \subset Y$ maps $\mathcal{O}_Y(V)$ onto $\mathcal{O}_X(f^{-1}V)$.

Note that a sheaf $\mathcal{O}$ of K-valued functions on X restricts to a sheaf $\mathcal{O}|U$ for every open $U \subset X$.

[11] We give the general definition of a sheaf later. This will do for now. A defect of this definition is that a sheaf of K-valued functions on X need not restrict to one on an arbitrary subspace of X. Another is the special role attributed to the closed points.

The definition above is a way of expressing that we are dealing with a local property—just as we have a sheaf of continuous $\mathbb{R}$-valued functions on a topological space, a sheaf of differentiable $\mathbb{R}$-valued functions on a manifold and a sheaf of holomorphic $\mathbb{C}$-valued functions on a complex manifold. In fact for the following definition, which includes our final definition of an affine variety, we take our cue from the definition of a manifold.

DEFINITION 10.5. An *affine k-variety* is a topological space X endowed with a sheaf $\mathcal{O}_X$ of k-valued functions which is isomorphic to a pair as above[12].

A *k-prevariety* is a topological space X endowed with a sheaf $\mathcal{O}_X$ of k-valued functions such that X can be covered by *finitely many* open subsets U such that $(U, \mathcal{O}_X|U)$ is an affine k-variety.

A *quasi-affine k-variety* is a k-prevariety which is isomorphic to an open subset of an affine variety.

Given k-prevarieties $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$, then a morphism $f : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ is simply a morphism in the category of spaces endowed with a sheaf $\mathcal{O}_X$ of k-valued functions, so f is continuous and for every open $V \subset Y$, composition with f takes $\mathcal{O}_Y(V)$ to $\mathcal{O}_X(f^{-1}V)$.

We often designate a prevariety and its underlying topological space by the same symbol, a habit which rarely leads to confusion. The composite of two morphisms is evidently a morphism so that we are dealing here with a category. The prefix 'pre' in prevariety refers to the fact that we have not imposed a separation requirement which takes the place of the Hausdorff property that one normally imposes on a manifold (see Example 10.8 below).

Let X be a prevariety. By assumption X is covered by finitely many affine open subvarieties $U_1, \ldots, U_N$. Suppose κ_i is an isomorphism of U_i onto an affine variety X_i that sits as a closed subset in some affine space. Then $X_{i,j} := \kappa_i(U_i \cap U_j)$ is an open subset of X_i and $\kappa_{i,j} := \kappa_j \kappa_i^{-1}$ is an isomorphism of $X_{i,j}$ onto $X_{j,i} \subset X_j$. We can recover X from the disjoint union of the $X_1, \ldots, X_N$ by means of a gluing process: if we use $\kappa_{i,j}$ to identify $X_{i,j}$ with $X_{j,i}$ for all i, j we get back X. The collection $\{(U_i, \kappa_i)\}_{i=1}^N$ is called an *affine atlas* for X.

EXERCISE 53. Let $(X, \mathcal{O}_X)$ be a prevariety.

(i) Prove that X is a noetherian space.
(ii) Prove that X contains an open-dense subset which is affine.
(iii) Let $Y \subset X$ be *locally closed* (i.e., the intersection of a closed subset with an open subset). Prove that Y is in natural manner a prevariety in such a manner that the inclusion $Y \subset X$ is a morphism of prevarieties.

Much of what we did for affine varieties extends in a straightforward manner to this more general context. For instance, a *rational function* $f : X \dashrightarrow k$ is defined as before: it is represented by a regular function on a subset of X that is open-dense in its set of closed points and two such represent the same rational function if they coincide on a nonempty open-dense subset in their common domain of definition.

If X is irreducible, then the rational functions on X form a field $k(X)$, the *function field of* X. If $U \subset X$ is an open nonempty affine subset, then $k(X) = k(U) = \mathrm{Frac}(\mathcal{O}(U))$ (but we will see that it is not true in general that $k(X) =$

[12]Note that X can then be identified with the spectrum of $\mathcal{O}_X(X)$

$\mathrm{Frac}(\mathcal{O}(X))$). In particular, $U_1, \ldots, U_N$ all have the same dimension $\mathrm{trdeg}_k\, k(X)$. According to Exercise 39, this is then also the (Krull) dimension of X.

Similarly, if X and Y are prevarieties, then a *rational map* $f : X \dashrightarrow Y$ is represented by morphism from a nonempty open-dense subset of X to Y with the understanding that two such defined the same map if they coincide on a nonempty open-dense subset. If some representative morphism has dense image in Y, then f is said to be *dominant* and then f induces a field extension $f^* : k(Y) \hookrightarrow k(X)$. Conversely, an embedding of fields $k(Y) \hookrightarrow k(X)$ determines a dominant rational map $X \dashrightarrow Y$. If $U \subset X$ is open and nonempty, then $k(U) = k(X)$ and the inclusion is a birational equivalence.

The notion of a regular point is local and so automatically carries over to this general setting. It is then also clear that the regular points of a prevariety X define an open-dense subset X_{reg} of X.

10.6. THE PRODUCT OF TWO PREVARIETIES. Our discussion of the product of closed subsets of affine spaces dictates how we should define the product of two prevarieties X and Y: if $(p, q) \in X \times Y$, then let $p \in U \subset X$ and $q \in V \subset Y$ be affine open neighborhoods of the components. We require that the topology on $U \times V$ be the Zariski topology so that a basis of neighborhoods of (p, q) consists of the loci $(U \times V)(h)$ where a $h \in \mathcal{O}(U) \otimes \mathcal{O}(V)$ with $h(p, q) \neq 0$ is nonzero. We also require that ring of sections of $\mathcal{O}_{X\times Y}$ over such a basic neighborhood $(U \times V)(h)$ be $\mathcal{O}(U) \otimes \mathcal{O}(V)[1/h]$.

EXERCISE 54. Prove that this product has the usual categorical characterization: the two projections $X \times Y \to X$ and $X \times Y \to Y$ are morphisms and if Z is a prevariety, then a pair of maps $(f : Z \to X, g : Z \to Y)$ defines a morphism $(f, g) : Z \to X \times Y$ if and only both f and g are morphisms.

The Hausdorff property is not of a local nature: a non-Hausdorff space can very well be locally Hausdorff. The standard example is the space X obtained from two copies of $\mathbb{R}$ by identifying the complement of $\{0\}$ in either copy by means of the identity map. Then X is locally like $\mathbb{R}$, but the images of the two origins cannot be separated. A topological space X is Hausdorff precisely when the diagonal of $X \times X$ is a closed subset relative to the product topology. As we know, the Zariski topology is almost never Hausdorff. But on the other hand, the selfproduct of the underlying space has not the product topology either and so requiring that the diagonal is closed is not totally unreasonable a priori. In fact, imposing this condition turns out to be the appropriate way of avoiding the pathologies that can result from an unfortunate choice of gluing data.

DEFINITION 10.7. A k-prevariety X is called a *k-variety* if the diagonal is closed in $X \times X$ (where the latter has the Zariski topology as defined above).

The diagonal in $\mathbb{A}^n \subset \mathbb{A}^n \times \mathbb{A}^n$ is closed, so $\mathbb{A}^n$ is a variety. This implies that the same is true for any quasi-affine subset of $\mathbb{A}^n$. Hence a quasi-affine prevariety is in fact a variety.

EXAMPLE 10.8. The simplest example of a prevariety that is not a variety is the obvious generalization of the space described above: let X be obtained from two copies $\mathbb{A}^1_+$ and $\mathbb{A}^1_-$ of $\mathbb{A}^1$ by identifying $\mathbb{A}^1_+ - \{0\}$ with $\mathbb{A}^1_- - \{0\}$ by means of the identity map. If $o_\pm \in X$ denotes the image of origin of $\mathbb{A}^1_\pm$, then $(o_+, o_-) \in X \times X$ lies in the closure of the diagonal, but is not contained in the diagonal.

A subset of a variety X is called a *subvariety* if it is open in a closed subset of X. The proof of the following assertion is left as an exercise (see also Exercise 53).

PROPOSITION 10.9. *A subvariety is in a natural manner a variety such that the inclusion becomes a morphism. The product of two varieties is a variety.*

EXAMPLE 10.10. We can take this further: if $U \subset \mathbb{A}^m$ is open and $f : U \to \mathbb{A}^n$ is a morphism, then consider the graph of f, $\tilde{U} := \{(x, y) \in \mathbb{A}^{m+n} : x \in U, y = f(x)\}$. It is easy to see that $\tilde{U}$ is a subvariety of $\mathbb{A}^{m+n}$. The map $x \in U \mapsto (x, f(x)) \in \tilde{U}$ and the projection $\tilde{U} \to U$ are regular and each others inverse. So they define an isomorphism $\tilde{U} \to U$. Notice that via this isomorphism f appears as a projection mapping: $(x, y) \in \tilde{U} \mapsto y \in V$.

EXERCISE 55. The goal of this exercise is to show that $U := \mathbb{A}^2 - \{(0, 0)\}$ is not affine. Let $U_x \subset U$ resp. $U_y \subset U$ be the complement of the x-axis resp. y-axis so that $U = U_x \cup U_y$.

(a) Prove that U_x is affine and that $\mathcal{O}(U_x) = k[x, y][1/x]$.
(b) Prove that every regular function on U extends to $\mathbb{A}^2$ so that $\mathcal{O}(U) = k[x, y]$.
(c) Show that U is not affine.

CHAPTER 2

Projective varieties

1. Projective spaces

Two distinct lines in the plane intersect in a single point or are parallel. In the last case one would like to say that the lines intersect at infinity so that the statement becomes simply: two distinct lines in a plane meet in a single point. There are many more examples of geometric configurations for which the special cases disappear by the simple remedy of adding points at infinity. A satisfactory approach to this which makes no a priori distinction between ordinary points and points at infinity involves the notion of a projective space. The following notion, perhaps a bit abstract, is quite useful. It will soon become more concrete.

DEFINITION 1.1. A *projective space of dimension n over k* is a set P endowed with an extra structure that can be given by a pair (V, ℓ), where V is k-vector space of dimension $n+1$ and ℓ is a bijection between P and the collection of 1-dimensional linear subspaces of V: $p \in P \mapsto \ell_p \subset V$. It is here understood that another such pair (V', ℓ') defines the same structure if and only if there exists a k-linear isomorphism $\phi : V \to V'$ such that for every $p \in P$, ϕ sends ℓ_p to ℓ'_p. (We are in fact saying that thus is defined an equivalence relation on the collection of such pairs and that a projective structure is given by an equivalence class.)

In particular, if V is a finite dimensional k-vector space, then the collection of its 1-dimensional linear subspaces is in a natural manner a projective space; we denote it by $\mathbb{P}(V)$. We often write $\mathbb{P}^n$ or $\mathbb{P}^n_k$ for $\mathbb{P}(k^{n+1})$ and call it simply *projective n-space (over k)*.

EXERCISE 56. Prove that the linear isomorphism ϕ in Definition 1.1 is unique up to scalar multiplication.

DEFINITION 1.2. Given a projective space P of dimension n over k, then a subset L of P is said to be *linear subspace of dimension d* if, for some (or any) pair (V, ℓ) as above, there exists a linear subspace $V_L \subset V$ of dimension $d+1$ such that $\ell(L)$ is the collection of 1-dimensional linear subspaces of V_L.

A map $f : P \to P'$ between two projective spaces over k is said to be *linear morphism* if for corresponding structural data (V, ℓ) and (V', ℓ') for P resp. P' there exists a linear *injection* $F : V \to V'$ such that F sends ℓ_p to $\ell'_{f(p)}$ for all $p \in P$.

So a linear subspace has itself the structure of a projective space and its inclusion in the ambient projective space is a linear morphism. Conversely, the image of a linear morphism is linear subspace.

A linear subspace of dimension one resp. two is often called a *line* resp. a *plane*. A linear subspace of codimension one (of dimension one less than the ambient projective space) is called a *hyperplane*. It is now clear that two distinct lines in a

plane intersect in a single point: this simply translates the fact that the intersection of two distinct linear subspaces of dimension two in a three dimensional vector space is of dimension one.

Let P be a projective space of dimension n. We can of course describe its structure by a pair (V, ℓ) for which $V = k^{n+1}$. This gives rise to a 'coordinate system on P' as follows: if we denote the coordinates of k^{n+1} by $(X_0, \ldots, X_n)$, then every point $p \in \mathbb{P}(V)$ is representable as a ratio $[p_0 : \cdots : p_n]$ of $n+1$ elements of k that are not all zero: choose a generator $\tilde{p} \in \ell_p$ and let $p_i = X_i(\tilde{p})$. Any other generator is of the form $\lambda\tilde{p}$ with $\lambda \in k - \{0\}$ and indeed, $[\lambda p_0 : \cdots : \lambda p_n] = [p_0 : \cdots : p_n]$. This is why $[X_0 : \cdots : X_n]$ is called a *homogeneous coordinate system on* $\mathbb{P}(V)$ even though an individual X_i is not a function on $\mathbb{P}(V)$ (but the ratios X_i/X_j are, albeit that for $i \neq j$ they are not everywhere defined).

1.3. LINEAR CHARTS AND STANDARD ATLAS. Let $U \subset P$ be a *hyperplane complement* in P, i.e., the complement of a hyperplane $H \subset P$. We show that U is in a natural manner an affine space. To see this, let the structure on P be given by the pair (V, ℓ). Then the hyperplane H corresponds to a hyperplane $V_H \subset V$. A coset A of V_H in V is an affine hyperplane in the classical sense of the word. Given a coset A of V_H distinct from V_H, then assigning to $v \in A$ the 1-dimensional linear subspace spanned by v defines a bijection $A \cong P - H$ whose inverse were denote by $\kappa_A : P - H \cong A$. This puts on U a structure of an affine space. This is independent of the choice of A: any another choice A' is obtained from A by multiplication by some nonzero scalar $u \in k$ and hence $\kappa_{A'}$ is the composite of κ_A and the map $u\cdot : A \cong A'$; since the latter is an isomorphism of affine spaces, $\kappa_{A'}$ defines the same affine structure on $P - H$ as κ_A. For a linear subspace $L \subset P$ the bijection $U \cong A$ restricts to one between $L \cap U$ and the affine-linear subspace $V_L \cap A$. So if $L \cap U \neq \emptyset$, then $L \cap U$ is an affine subspace of U. Concretely, if we choose a homogeneous coordinate system $(X_0, \ldots, X_n)$ such that H is given by $X_0 = 0$, then $(x_1 := X_1/X_0, \ldots, x_n := X_n/X_0)$ maps A bijectively onto $\mathbb{A}^n$ and any other choice will differ from this one by an affine-linear transformation of $\mathbb{A}^n$. We call such an isomorphism from a hyperplane complement in P onto $\mathbb{A}^n$ a *linear chart* for P.

Thus the homogeneous coordinate system $[X_0, \ldots, X_n]$ defines a chart for every $i = 0, \ldots, n$: if $U_i \subset P$ is the hyperplane complement defined by $X_i \neq 0$, then

$$\kappa_i : U_i \cong \mathbb{A}^n, \quad [X_0 : \cdots : X_n] \mapsto (X_0/X_i, \ldots, \widehat{X_i/X_i}, \ldots, X_n/X_i),$$

is a chart with inverse $(x_1, \ldots, x_n) \mapsto [x_1 : \cdots : x_i : 1 : x_{i+1} : \cdots : x_n]$. Notice that the U_i's cover P. We call a collection of linear charts $(U_i, \kappa_i)_{i=0}^n$ thus obtained from a homogeneous coordinate system a *standard atlas* for P. Let us determine the coordinate change for a pair of charts, say for $\kappa_n\kappa_0^{-1}$. The image of $U_0 \cap U_n$ under κ_0 resp. κ_n is the open subset $U(x_n)$ resp. $U(x_1)$ of $\mathbb{A}^n$ and

$$\kappa_n\kappa_0^{-1} : U(x_n) \to U(x_1), \quad (x_1, x_2, \ldots, x_n) \mapsto (1/x_n, x_1/x_n, \ldots, x_{n-1}/x_n).$$

Notice that this defines an isomorphism of affine varieties (the inverse is $\kappa_0\kappa_n^{-1}$).

Thus P becomes the set of closed points of a prevariety. In particular, P acquires a (Zariski) topology for which $U \subset P$ is open if and only if $\kappa(U \cap U_i)$ is open in the set of closed points of $\mathbb{A}^n$. We now change the interpretation of P a bit as to by adding a point for every subset of P that is closed and irreducible for this topology (and was not already in P). Then we have a prevariety $(P, \mathcal{O}_P)$ with the

property that $U \subset P$ is open if and only if $\kappa(U \cap U_i)$ is open in $\mathbb{A}^n$ and $f \in \mathcal{O}_P(U)$ if and only if $f\kappa_i^{-1} \in \mathcal{O}_{\kappa_i(U)}$ for all i. We shall see shortly that this structure is independent of the coordinate system $(X_0, \dots, X_n)$ and that P is in fact a k-variety.

We could also proceed in the opposite direction and start with an affine space and realize it as the hyperplane complement of a projective space. Changing our point of view accordingly, we might say that a projective space arises as a 'completion with points at infinity' of a given affine space. For instance, $\mathbb{A}^n$ embeds in $\mathbb{P}^n$ by $(x_1, \dots, x_n) \mapsto [1 : x_1 : \cdots : x_n]$ with image the hyperplane complement defined by $X_0 \neq 0$.

2. The Zariski topology on a projective space

We begin with giving a simpler, more classical characterization of the Zariski topology on a projective space.

Let P be a projective space of dimension n over k and let $[X_0 : \cdots : X_n]$ be a homogeneous coordinate system for P. Suppose $F \in k[X_0, \dots, X_n]$ is homogeneous of degree d so that $F(tX_0, \dots, tX_n) = t^d F(X_0, \dots, X_n)$ for $\lambda \in k$. The property of this being zero only depends on $[X_0 : \cdots : X_n]$ and hence the zero set of F defines a subset $Z_F \subset P$ (even though F is not a function on P). We denote its nonzero set by $U_F := P - Z_F$.

PROPOSITION 2.1. *The collection U_F, where F runs over the homogeneous polynomials in $k[X_0, \dots, X_n]$, is a basis for the Zariski topology on P. This topology is independent of the choice of our homogeneous coordinate system $[X_0, \dots, X_n]$ and every linear chart is a homeomorphism that identifies the sheaf of regular functions on its domain with $\mathcal{O}_{\mathbb{A}^n}$.*

PROOF. That the collection $\{U_F\}_F$ is a basis of a topology follows from the obvious equality $U_F \cap U_{F'} = U_{FF'}$. The independence of the coordinate choice results from the observation that under a linear substitution a homogeneous polynomial transforms into a homogeneous polynomial (of the same degree).

Let now $U = P - H$ be a hyperplane complement. Choose a homogeneous coordinate system $[Y_0, \dots, Y_n]$ such that U is defined by $Y_0 \neq 0$ and denote by $j : \mathbb{A}^n \cong U$, $(y_1, \dots, y_n) \mapsto [1 : y_1 : \cdots : y_n]$ the inverse. If $F \in k[Y_0, \dots, Y_n]$ is homogeneous, then $j^{-1}U_F = U(f)$, where $f(y_1, \dots, y_n) := F(1, y_1, \dots, y_n)$. So the inclusion j is continuous. Conversely, if $f \in k[y_1, \dots, y_n]$ is nonzero of degree d, then its 'homogenization' $F(Y_0, \dots, Y_n) := Y_0^d f(Y_1/Y_0, \dots, Y_n/Y_0)$ is homogeneous of degree d and $U(f) = j^{-1}U_F$. So j is also open.

By letting (U, j^{-1}) run over the charts (U_ν, κ_ν), we see that have thus recovered the Zariski topology. The last statement follows from the fact that each $\kappa_\nu j$ is an isomorphism between two open subsets of $\mathbb{A}^n$. □

EXERCISE 57. Let $0 \neq F \in k[X_0, \dots, X_n]$ be homogeneous of degree d.

(a) Prove that every function $U_F \to k$ of the form G/F^r with $r \geq 0$ and G homogeneous of the same degree as F^r is regular.
(b) Prove that conversely every regular function on U_F is of this form.

We now discuss the projective analogue of the (affine) $I \leftrightarrow Z$ correspondence and at the same time clarify what a nonclosed point is. Let us denote for an integer $d \geq 0$ by $k[X_0, \dots, X_n]_d$ the set of $F \in k[X_0, \dots, X_n]$ that are homogeneous of degree d. It is clear that $k[X_0, \dots, X_n]$ is the direct sum of the $k[X_0, \dots, X_n]_d$,

$d = 0, 1, \dots$ and that $k[X_0, \dots, X_n]_d \cdot k[X_0, \dots, X_n]_e = k[X_0, \dots, X_n]_{d+e}$. A good way to understand the decomposition of $k[X_0, \dots, X_n]$ into its homogeneous summands is in terms of the action in $\mathbb{A}^{n+1}$ defined by scalar multiplication: if $F \in k[X_0, \dots, X_n]_d$, then for every $t \in k$, we have $F(tX_0, \dots, tX_n) = t^d F(X_0, \dots, X_n)$. So this decomposition is in fact the eigenspace decomposition for this action of the multiplicative group $k^\times$ on $k[X_0, \dots, X_n]$. (Indeed, this simple decomposition should be understood as the algebraic expression of that action.) This implies among other things that for any $F \in k[X_0, \dots, X_n]_d$ the zero set $Z(F) \subset \mathbb{A}^{n+1} = k^{n+1}$ is invariant under scalar multiplication. This is still true for an intersection of such zero sets, in other words, if $I \subset k[X_0, \dots, X_n]$ is an ideal generated by homogeneous polynomials of positive degree, then $Z(I) \subset \mathbb{A}^{n+1}$ is invariant under scalar multiplication. Such a closed subset is called an *affine cone*; the origin is called the *vertex* of that cone. Observe that since we insisted that the degrees of the homogeneous generators of I be positive, we have $I \subset (X_0, \dots, X_n)$, and so $Z(I)$ will always contain the vertex 0.

If $Y \subset \mathbb{P}^n$ is closed, Y can be written as an intersection $\cap_\alpha Z_{F_\alpha}$, where each F_α is homogeneous. The common zero set of the F_α in $\mathbb{A}^{n+1}$, $\cap_\alpha Z(F_\alpha)$, is the cone that as a set is just the union of the 1-dimensional linear subspaces of k^{n+1} parameterized by Y. We denote this affine cone by $\mathrm{Cone}(Y)$.

Given a subset $Y \subset \mathbb{P}^n$, then for $d \geq 1$, we denote by $I_{Y,d}$ the set of $F \in k[X_0, \dots, X_n]_d$ with $Y \subset Z_F$ (we put $I_{Y,0} = 0$). This is a vector space and we have $I_{Y,d} \cdot k[X_0, \dots, X_n]_e \subset I_{Y,d+e}$. So the direct sum of the $I_{Y,d}$, $d = 1, 2, \dots$, denoted by $I_Y \subset k[X_0, \dots, X_n]$, is an ideal of $k[X_0, \dots, X_n]$. Notice that with this definition, $I_\emptyset$ is the ideal generated by $X_0, \dots, X_n$.

The k-algebra $k[X_0, \dots, X_n]$ is graded and the ideal I_Y is homogeneous in the sense below.

DEFINITION 2.2. A *(nonnegatively) graded ring* is a ring R whose underlying additive group comes with a direct sum decomposition $R_\bullet = \oplus_{k=0}^\infty R_d$ such that the ring product maps $R_d \times R_e$ in R_{d+e}, or equivalently, is such that $\sum_{d=0}^\infty R_d t^d$ is a subring of $R[t]$. An ideal I of such a ring is said to be *homogeneous* if it is the direct sum of its homogeneous parts $I_d := I \cap R_d$.

If $R_\bullet$ is a graded ring, then clearly R_0 is a subring of R. If $I_\bullet$ is a homogeneous ideal, then $R/I = \oplus_{d=0}^\infty R_d/I_d$ is again a graded ring. Of special interest is the homogeneous ideal $R_+ := \oplus_{k=1}^\infty R_d$, for which we have $R/R_+ = R_0$. We will be mostly concerned with the case when $R_0 = k$, so that R_+ is then a maximal ideal (and the only one that is homogeneous).

LEMMA 2.3. *If I, J are homogeneous ideals of a graded ring $R_\bullet$, then so are $I \cap J$, IJ, $I + J$ and $\sqrt{I}$. Moreover, a minimal prime ideal of $R_\bullet$ is a graded ideal.*

PROOF. The proofs of the first statement are not difficult. We omit them.

As to the last, it suffices to show that if $\mathfrak{p} \subset R_\bullet$ is a prime ideal, then the direct sum of its homogeneous parts, $\mathfrak{p}_\bullet := \oplus_n(\mathfrak{p} \cap R_n)$ is also a prime ideal. Indeed, suppose $r, s \in R$ are such that $rs \in \mathfrak{p}_\bullet$ and neither r nor s lies in $\mathfrak{p}_\bullet$. Write r and s as a sum of its homogenous parts and let $r_k \in R_k$ resp. $s_l \in R_l$ be the lowest degree part or r resp. s that is not in $\mathfrak{p}$. Then it is easily seen that $r_k s_l \in \mathfrak{p}$ and so $r_k \in \mathfrak{p}$ or $s_l \in \mathfrak{p}$ and we get a contradiction. □

LEMMA 2.4. *If $X \subset \mathbb{A}^{n+1}$ is an affine cone (with vertex 0), then $I(X)$ is a homogeneous ideal.*

PROOF. Let $F \in I(X)$. We must show that each homogeneous component of F lies in $I(X)$. As X is invariant under scalar multiplication, the polynomial $F(tX_0, \ldots, tX_n) = \sum_{d \geq 1} t^d F_d(X_0, \ldots, X_n)$ (as an element of $k[x_1, \ldots, x_n][t]$) vanishes on $X \times \mathbb{A}^1$ in $\mathbb{A}^{n+1} \times \mathbb{A}^1$. Clearly the zero set of $I(X)[t]$ is $X \times \mathbb{A}^1 \subset \mathbb{A}^{n+1} \times \mathbb{A}^1$ and since the quotient is $k[x_1, \ldots, x_n][t]/I(X)[t] = A(X)[t]$ is reduced, we have $I(X \times \mathbb{A}^1) = I(X)[t]$. It follows that $F_d \in I(X)$ for all d. □

The ideal $I(X)$ is of course a radical ideal and so we find:

COROLLARY 2.5. *The maps $Y \mapsto \mathrm{Cone}(Y)$ and $Y \mapsto I_Y$ set up bijections between (i) the collection of closed subsets of $\mathbb{P}^n$, (ii) the collection of affine cones in $\mathbb{A}^{n+1}$ and (iii) the collection of homogeneous radical ideals of $k[X_0, \ldots, X_n]$ contained in $(X_0, \ldots, X_n)$.*

Note that here $Y = \emptyset \leftrightarrow \{0\} \subset \mathbb{A}^{n+1} \leftrightarrow$ the homogeneous ideal $(X_0, \ldots, X_n)$. The bijections above restrict to bijections between (i) the collection of irreducible subsets of $\mathbb{P}^n$ (which we can also think of as $\mathbb{P}^n$, its nonclosed points included), (ii) the collection of irreducible affine cones in $\mathbb{A}^{n+1}$ strictly containing the vertex 0 and (iii) the collection of homogeneous prime ideals of $k[X_0, \ldots, X_n]$ strictly contained in $(X_0, \ldots, X_n)$.

DEFINITION 2.6. The *homogeneous coordinate ring* of a closed subset Y of $\mathbb{P}^n$ is the graded ring $S(Y)_\bullet := k[X_0, \ldots, X_n]/I_Y$, $S(Y)_d = k[X_0, \ldots, X_n]_d/I_{Y,d}$.

Notice that if we ignore the grading of $S(Y)_\bullet$, then we just get the coordinate ring of the affine cone over Y, $A(\mathrm{Cone}(Y))$.

EXERCISE 58. Let $R_\bullet$ be a graded ring.

(b) Prove that if I is a prime ideal in the homogeneous sense: if $rs \in I$ for some $r \in R_k, s \in R_l$ implies $r \in I$ or $s \in I$, then I is a prime ideal.
(c) Prove that the intersection of all homogeneous prime ideals of $R_\bullet$ is its ideal of nilpotents.

EXERCISE 59. Prove that a closed subset $Y \subset \mathbb{P}^n$ is irreducible if and only if I_Y is a prime ideal.

Since $k[X_0, \ldots, X_n]$ is a noetherian ring, any ascending chain of homogeneous ideals in this ring stabilizes. This implies that any projective space is noetherian (and according to Exercise 53 $\mathbb{P}^b$, as any prevariety, is noetherian). In particular, every subset of a projective space has a finite number of irreducible components whose union is all of that subset.

EXERCISE 60. Let $S_\bullet$ be a graded k-algebra that is reduced, finitely generated and has $S_0 = k$.

(a) Prove that $S_\bullet$ is as a graded k-algebra isomorphic to the homogeneous coordinate ring of a closed subset Y.
(b) Prove that under such an isomorphism, the homogeneous radical ideals contained in the maximal ideal $S_+ := \oplus_{d \geq 1} S_d$ correspond to closed subsets of Y under an inclusion reversing bijection: homogeneous ideals strictly contained in S_+ and maximal for that property correspond to points of Y.
(c) Suppose $S_\bullet$ a domain. Show that a fraction F/G that is homogeneous of degree zero ($F \in S_d$ and $0 \neq G \in S_d$ for some d) defines a function on U_g.

EXERCISE 61. Let Y be an affine variety.

(a) Show that a homogeneous element of the graded ring $A(Y)[X_0, \dots, X_n]$ defines a closed subset of $Y \times \mathbb{P}^n$ as its zero set.
(b) Prove that every closed subset of $Y \times \mathbb{P}^n$ is an intersection of finitely many zero set of homogeneous elements of $A(Y)[X_0, \dots, X_n]$.
(c) Prove that we have a bijective correspondence between closed subsets of $Y \times \mathbb{P}^n$ and homogeneous radical ideals in $A(Y)[X_0, \dots, X_n]$.

3. The Segre embeddings

First we show how a product of projective spaces can be realized as a closed subset of a projective space. This will imply among other things that a projective space is a variety. Consider the projective spaces $\mathbb{P}^m$ and $\mathbb{P}^n$ with their homogeneous coordinate systems $[X_0 : \cdots : X_m]$ and $[Y_0 : \cdots : Y_n]$. We also consider a projective space whose homogeneous coordinate system is the set of matrix coefficients of an $(m+1) \times (n+1)$-matrix $[Z_{00} : \cdots Z_{ij} : \cdots : Z_{mn}]$; this is just $\mathbb{P}^{mn+m+n}$ with an unusual indexing of its homogeneous coordinates.

PROPOSITION 3.1 (The Segre embedding). *The map $f : \mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^{mn+m+n}$ defined by $Z_{ij} = X_i Y_j$, $i = 0, \dots, m; j = 0, \dots, n$ is an isomorphism onto a closed subset of $\mathbb{P}^{mn+m+n}$. If $m = n$, then the diagonal of $\mathbb{P}^m \times \mathbb{P}^m$ is the preimage of the linear subspace of $\mathbb{P}^{m^2+2m}$ defined by $Z_{ij} = Z_{ji}$ and hence is closed in $\mathbb{P}^m \times \mathbb{P}^m$.*

PROOF. In order to prove that f defines an isomorphism onto a closed subset of $\mathbb{P}^{mn+m+n}$, it is enough to show that for every chart domain U_{ij} of the standard atlas of $\mathbb{P}^{mn+m+n}$, $f^{-1}U_{ij}$ is open in $\mathbb{P}^m \times \mathbb{P}^n$ and is mapped by f isomorphically onto a closed subset of U_{ij}. For this purpose we may (simply by renumbering) assume that $i = j = 0$. So then $U_{00} \subset \mathbb{P}^{mn+m+n}$ is defined by $Z_{00} \neq 0$ and is parametrized by the coordinates $z_{ij} := Z_{ij}/Z_{00}$, $(i,j) \neq (0,0)$. It is clear that $f^{-1}U_{00}$ is defined by $X_0 Y_0 \neq 0$. This is just $U_{X_0} \times U_{Y_0}$ and hence parametrized by $x_1 := X_1/X_0, \dots, x_m := X_m/X_0$ and $y_1 := Y_1/Y_0, \dots, y_n := Y_n/Y_0$. In terms of these coordinates, $f : f^{-1}U_{00} \to U_{00}$ is given by $z_{ij} = x_i y_j$, where $(i,j) \neq (0,0)$ and where we should read 1 for x_0 and y_0 (so that $z_{i0} = x_i$ and $z_{0j} = y_j$). It is now clear that the image is in fact the graph of the morphism $\mathbb{A}^m \times \mathbb{A}^n \to \mathbb{A}^{mn}$ with coordinates $x_i y_j$, $1 \leq i \leq m$, $1 \leq j \leq n$. This graph is closed in $\mathbb{A}^m \times \mathbb{A}^n \times \mathbb{A}^{mn}$ and isomorphic to $\mathbb{A}^m \times \mathbb{A}^n$. So f indeed restricts to an isomorphism of $f^{-1}U_{00}$ onto a closed subset of U_{00}.

In case $m = n$, we must also show that the condition $X_i Y_j = X_j Y_i$ for $0 \leq i < j \leq m$ implies that $[X_0 : \cdots : X_m] = [Y_0 : \cdots : Y_m]$, assuming that not all X_i resp. Y_j are zero. Suppose $X_i \neq 0$ and put $t := Y_i/X_i \in k^\times$. Then $X_i Y_j = X_j Y_i$ implies $Y_j = t X_j$ for all j. So $t \neq 0$ and $[Y_0 : \cdots : Y_m] = [X_0 : \cdots : X_m]$. □

COROLLARY 3.2. *A projective space over k is a variety.*

PROOF. Proposition 3.1 shows that the diagonal of $\mathbb{P}^m \times \mathbb{P}^m$ is closed. □

DEFINITION 3.3. A variety is said to be *projective* if it is isomorphic to a closed irreducible subset of some projective space. A variety is called *quasi-projective* if is isomorphic to an open subset of some projective variety.

COROLLARY 3.4. *Every irreducible closed (resp. locally closed) subset of $\mathbb{P}^n$ is a projective (resp. quasi-projective) variety. The collection of projective (resp. quasi-projective) varieties is closed under a product.*

PROOF. The first statement follows from 10.9 and the second from Proposition 3.1. □

EXERCISE 62. (a) Prove that the image of the Segre embedding is the common zero set of the homogenenous polynomials $Z_{ij}Z_{kl} - Z_{il}Z_{kj}$.

(b) Show that for every $(p, q) \in \mathbb{P}^m \times \mathbb{P}^n$ the image of $\{p\} \times \mathbb{P}^n$ and $\mathbb{P}^m \times \{q\}$ in $\mathbb{P}^{mn+m+n}$ is a linear subspace.

(c) Prove that the map $\mathbb{P}^n \to \mathbb{P}^{(n^2+3n)/2}$ defined by $Z_{ij} = X_iX_j$, $0 \leq i \leq j \leq n$ is an isomorphism on a closed subset defined by quadratic equations. Find these equations for $n = 2$.

(d) As a special case we find that the quadric hypersurface in $\mathbb{P}^3$ defined by $Z_0Z_1 - Z_2Z_3 = 0$ is isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$. Identify in this case the two systems of lines on this quadric.

EXERCISE 63 (Intrinsic Segre embedding). Let V and W be finite dimensional k-vector spaces. Describe the Segre embedding for $\mathbb{P}(V) \times \mathbb{P}(W)$ intrinsically as a morphism $\mathbb{P}(V) \times \mathbb{P}(W) \to \mathbb{P}(V \otimes W)$.

4. Projections

Let V be a finite dimensional k-vector space. If $W \subset V$ is a linear subspace, then we can form the quotient vector space V/W and we have linear surjection $\pi : V \to V/W$. We cannot projectivize this as a morphism from $\mathbb{P}(V)$ to $\mathbb{P}(V/W)$, but we shall see that it defines at least a morphism $\mathbb{P}\pi : \mathbb{P}(V) - \mathbb{P}(W) \to \mathbb{P}(V/W)$ (which then determines a rational map $\mathbb{P}(V) \dashrightarrow \mathbb{P}(V/W)$ in case $W \neq V$). As a map, $\mathbb{P}\pi$ is defined as follows: for $p \in \mathbb{P}(V) - \mathbb{P}(W)$, ℓ_p is a one dimensional subspace of V not contained in W so that $\pi(\ell_p)$ is a one dimensional subspace of V/W; we then put $\mathbb{P}\pi(p) := [\pi(\ell_p)]$. To see that this is morphism, let $n := \dim \mathbb{P}(V)$, $m := \dim \mathbb{P}(V/W)$ (so that $\dim V = n + 1$ and $\dim W = n - m$) and choose a coordinate system $(X_0, \ldots, X_n)$ for V such that W is given by $X_0 = \cdots = X_m = 0$. Then $(X_0, \ldots, X_m)$ serves as a coordinate system for V/W and $\pi : V \to V/W$ is simply given by $(X_0, \ldots, X_n) \to (X_0, \ldots, X_m)$. In projective coordinates this is of course given by $[X_0 : \cdots : X_n] \to [X_0 : \cdots : X_m]$ and so is indeed a morphism where it makes sense, namely where $X_0, \ldots, X_m$ not all vanish, that is, on the complement of $\mathbb{P}(W)$.

DEFINITION-LEMMA 4.1. *The* blowup of $\mathbb{P}(V)$ along $\mathbb{P}(W)$, *denoted* $\mathrm{Bl}_{\mathbb{P}(W)}\mathbb{P}(V)$, *is the closure of the graph of* $\mathbb{P}\pi$ *in* $\mathbb{P}(V) \times \mathbb{P}(V/W)$ *(hence is a projective variety). It enjoys the following properties:*

The projection on the first factor, $p_1 : \mathrm{Bl}_{\mathbb{P}(W)}\mathbb{P}(V) \to \mathbb{P}(V)$ *is an isomorphism over* $\mathbb{P}(V) - \mathbb{P}(W)$ *whereas the preimage over* $\mathbb{P}(W)$ *is* $\mathbb{P}(W) \times \mathbb{P}(V/W)$.

The projection to the second factor $p_2 : \mathrm{Bl}_{\mathbb{P}(W)}\mathbb{P}(V) \to \mathbb{P}(V/W)$ *is a* locally trivial bundle *of projective spaces of dimension* $\dim W$, *to be precise, if* $U \subset \mathbb{P}(V/W)$ *is a hyperplane complement (hence an affine space), then there exists an isomorphism* $p_2^{-1}U \cong \mathbb{P}^{n-m} \times U$ *whose second component is given by* p_2.

PROOF. We use a homogeneous coordinate system $[X_0 : \cdots : X_n]$ for $\mathbb{P}(V)$ as above (so that $\mathbb{P}(W)$ is given by $X_0 = \cdots = X_m = 0$). If we denote the corresponding coordinate system for $\mathbb{P}(V/W)$ by $[Y_0 : \cdots : Y_m]$, then the graph of $\mathbb{P}\pi$ in $\mathbb{P}(V) \times \mathbb{P}(V/W)$ is given by the pairs $([X_0 : \cdots : X_n], [Y_0 : \cdots : Y_m])$ with $[X_0 : \cdots : X_m]$ proportional to $[Y_0 : \cdots : Y_m]$ and $(X_0, \ldots, X_m) \neq (0, \ldots, 0)$. The

proportionality property is equivalent to: $X_iY_j = X_jY_i$ for all $0 \leq i < j \leq m$. Let Z be the subset of $\subset \mathbb{P}(V) \times \mathbb{P}(V/W)$ defined by these equations: $X_iY_j = X_jY_i$, $0 \leq i < j \leq m$. In terms of the Segre embedding of $\mathbb{P}^n \times \mathbb{P}^m \hookrightarrow \mathbb{P}^{nm+n+m}$ this amounts to $Z_{ij} = Z_{ji}$ in this range and so Z is a closed subset of $\mathbb{P}(V) \times \mathbb{P}(V/W)$. The equations defining Z are trivially satisfied when $(X_0, \ldots, X_m) = (0, \ldots, 0)$ and so Z contains $\mathbb{P}(W) \times \mathbb{P}(V/W)$. We have just shown that the graph of $\mathbb{P}\pi$ equals the complement of $\mathbb{P}(W) \times \mathbb{P}(V/W)$ in Z.

Let us now see what the projection $Z \to \mathbb{P}(V/W)$ is like over the open subset U_{Y_0} of $\mathbb{P}(V/W)$ defined by $Y_0 \neq 0$. We parametrize U_{Y_0} by $\mathbb{A}^m$ via $(y_1, \ldots, y_m) \in \mathbb{A}^m \mapsto [1 : y_1 : \cdots : y_m]$. Then its preimage $Z_{U_{Y_0}} := Z \cap (\mathbb{P}(V) \times U_{Y_0})$ in Z is parametrized by $\mathbb{P}^{n-m} \times U_{Y_0}$ by means of the morphism

$$([X_0 : X_{m+1} : \cdots : X_n], [1 : y_1 : \cdots : y_n]) \in \mathbb{P}^{n-m} \times U_{Y_0} \mapsto$$
$$([X_0 : X_0y_1 : \cdots : X_0y_m : X_{m+1} : \cdots : X_n], [1 : y_1 : \cdots : y_n]) \in Z_{U_{Y_0}}.$$

This is an isomorphism (the inverse is obvious) which commutes with the projection on U_{Y_0}. Notice that it makes $Z_{U_{Y_0}} \cap (\mathbb{P}(V) \times \mathbb{P}(V/W))$ correspond to the locus where $X_0 = 0$, which is the product of a hyperplane in $\mathbb{P}^{n-m}$ times U_{Y_0}. In particular, $Z_{U_{Y_0}} \cap (\mathbb{P}(V) \times \mathbb{P}(V/W))$ lies in the closure of the graph of $\mathbb{P}\pi$. This remains true, of course, if we replace U_{Y_0} by U_{Y_i}, $i = 1, \ldots, m$, or by any other hyperplane complement in $\mathbb{P}(V/W)$. It follows that Z is the closure of the graph of $\mathbb{P}\pi$ and that Z enjoys the stated properties. □

It is worthwhile to describe this map in purely projective terms. This starts with the observation that the π-preimage of a one-dimensional linear subspace of V/W is a linear subspace of V which contains W as a hyperplane and that every such subspace so arises. So we can think of $\mathbb{P}(V/W)$ as parameterizing the projective linear subspaces of $\mathbb{P}(V)$ that contain $\mathbb{P}(W)$ as a projective hyperplane.

EXERCISE 64. Prove that the projective structure on this collection of linear subspaces is intrinsic: prove that if P is a projective space and $Q \subset P$ is a projective linear subspace of codimension $m > 0$, then the collection of projective linear subspaces $\tilde{Q} \subset P$ which contain Q as a projective hyperplane is in a natural manner a projective space (denoted here by P_Q) of dimension $m-1$. Show that the blowup $\mathrm{Bl}_Q P$ of P along Q can be identified with the set of pairs $(p, [\tilde{Q}]) \in P \times P_Q$ with $p \in \tilde{Q}$.

5. Elimination theory and closed projections

Within a category of reasonable topological spaces (say, the locally compact Hausdorff spaces), the compact ones can be characterized as follows: K is compact if and only if the projection $K \times X \to X$ is closed for every space X in that category. In this sense the following theorem states a kind of compactness property for projective varieties.

THEOREM 5.1. *If U is a variety, then the projection $\pi_U : \mathbb{P}^n \times U \to U$ is closed. Moreover, if $Z \subset \mathbb{P}^n \times U$ is closed and irreducible, then there exists an open-dense subset $Y' \subset \pi_U(Z)$ such that for every closed point $y \in Y'$ we have $\dim Z = \dim \pi_U(Z) + \dim Z_y$, where $Z_y \subset \mathbb{P}^n$ denotes the fiber $\pi_U|Z$ over y.*

We derive this theorem from the main theorem of elimination theory, which we will state and prove first.

Given an integer $d \geq 0$, let us write V_d for $k[X_0, X_1]_d$, the k-vector space of homogeneous polynomials in $k[X_0, X_1]$ of degree d. The monomials $(X_0^{d-i}X_1^i)_{i=0}^d$ form a basis, in particular, $\dim V_d = d+1$. Given $F \in V_m$ and $G \in V_n$, then

$$u_{F,G} : V_{n-1} \oplus V_{m-1} \to V_{n+m-1}, \quad (A, B) \mapsto AF + BG$$

is a linear map between two k-vector spaces of the same dimension $m+n$. The *resultant* $R(F, G)$ of F and G is defined as the determinant of this linear map with respect to the monomial bases of the summands of $V_{n-1} \oplus V_{m-1}$ and of V_{n+m-1}. So $R(F, G) = 0$ if and only if $u_{F,G}$ fails to be injective.

Notice that $R(F, G)$ is a polynomial in the coefficients of F and G: if $F = \sum_{i=0}^m a_i X_0^{m-i} X_1^i$ and $G = \sum_{j=0}^n b_i X_0^{n-i} X_1^i$, then

$$R(F,G) = \det \begin{pmatrix} a_0 & a_1 & \cdots & a_m & 0 & \cdots & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_m & \cdots & \cdots & 0 \\ 0 & 0 & a_0 & & & & \cdots & 0 \\ & & & \cdots & & & & \\ 0 & 0 & \cdots & 0 & a_0 & a_1 & \cdots & a_m \\ b_0 & b_1 & \cdots & \cdots & b_n & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & \cdots & b_n & 0 \cdots & 0 \\ 0 & 0 & b_0 & & & & \cdots & 0 \\ & & & \cdots & & & & \\ 0 & \cdots & 0 & b_0 & b_1 & \cdots & \cdots & b_n \end{pmatrix}$$

So the resultant defines an element of $A(V_m \times V_n) = A(V_m) \otimes A(V_n)$.

LEMMA 5.2. *$R(F, G) = 0$ if and only if F and G have a common zero in $\mathbb{P}^1$.*

PROOF. If $R(F, G) = 0$, then $u_{F,G}$ is not injective, so that there exist a nonzero $(A, B) \in V_{n-1} \oplus V_{m-1}$ with $AF + BG = 0$. Suppose that $B \neq 0$. It is clear that F divides BG. Since $\deg(B) = m - 1 < m = \deg F$, it follows that F and G must have a common factor.

If conversely F and G have a common zero in $\mathbb{P}^1$, then they must have a common linear factor L, say: $F = LF_1$, $G = LG_1$ and we see that $(G_1, -F_1) \in V_{n-1} \oplus V_{m-1}$ is nonzero and in the kernel of $u_{F,G}$. □

PROOF OF THEOREM 5.1. Let $Z \subset \mathbb{P}^n \times U$. It is clear that $\pi_U(Z)$ is closed in U if for every open affine subset $U' \subset U$, $\pi_U(Z) \cap U'$ is closed in U'. Since $\pi_U(Z) \cap U' = \pi_{U'}(Z \cap (\mathbb{P}^n \times U'))$ we may (and will) assume that is U affine.

We first treat the case $n = 1$ and then proceed with induction on n.

Let $Z \subset \mathbb{P}^1 \times U$ be closed. Denote by $I_{Z,\bullet}$ the homogeneous ideal in the graded algebra $A(U)[X_0, X_1]$ of functions vanishing on Z. Then Z is the common zero set of the members of $I_{Z,\bullet}$ (see Exercise 61). For every homogeneous pair $F, G \in \cup_m A(U)[X_0, X_1]_m$, we can form the resultant $R(F, G) \in A(U)$. We claim that $\pi_U(Z)$ is the common zero set $Z(\mathcal{R}) \subset U$ of the set of resultants $R(F, G)$ of pairs of homogeneous forms F, G taken in $\cup_m I_{Z,m}$, hence is closed in U.

Suppose that $y \in \pi_U(Z)$ so that $(y, p) \in Z$ for some $p \in \mathbb{P}^1$. Then p is a common zero of each pair F_y, G_y, where $F, G \in \cup_m I_{Z,m}$ and the subscript y refers to substituting y for the first argument. So $R(F, G)$ vanishes in y. It follows that $y \in Z(\mathcal{R})$.

Next we show that if $y \notin \pi_U(Z)$, then $y \notin Z(\mathcal{R})$. Since $\{y\} \times \mathbb{P}^1$ is not contained in Z, there exists an integer $m > 0$ and a $F \in I_{Z,m}$ with $F_y \neq 0$. Denote by

$p_1, \ldots, p_r \in \mathbb{P}^1$ the distinct zeroes of F_y. We show that there exists a $G \in I_{Z,n}$ for some n such that G_y does not vanish in any p_i. This suffices, for this means that $R(F_y, G_y) \neq 0$ and so $y \notin Z(\mathcal{R})$. To this end, we note that for any given $1 \leq i \leq r$, $Z \bigcup \cup_{j \neq i}\{(y, p_j)\}$ is closed in $U \times \mathbb{P}^1$, so that there will exist a $G^{(i)} \in \cup_m I_{Z,m}$ with $G^{(i)}_y$ zero in all the p_j with $j \neq i$, but nonzero in p_i. Upon replacing each $G^{(i)}$ by some positive power of it , we may assume that $G^{(1)}, \ldots, G^{(r)}$ all have the same degree n, say. Then $G := G^{(1)} + \cdots + G^{(r)} \in I_{Z,n}$ and $G_y(p_i) = G^{(i)}(p_i) \neq 0$.

In order to prove the dimension assertion, we assume Z irreducible so that $Y := \pi_U(Z)$ is irreducible and closed. We show that either $Z = \mathbb{P}^1 \times Y$ (so that $\dim Z = \dim Y + 1$) or that there exists an open-dense $Y' \subset Y$ such that $Z_{Y'} := Z \cap (\mathbb{P}^1 \times Y') \to Y'$ is a finite morphism (so that $\dim Y = \dim Y' = \dim Z_{Y'} = \dim Z$).

Consider the ideal in $A(U)$ generated by the coefficients of all the members of $I_Z \subset A(U)[X_0, X_1]$ and denote by $Y_1 \subset U$ its zero set. This is closed subset of Y consisting of the $y \in U$ with the property that $\mathbb{P}^1 \times \{y\} \subset Z$. If $Z_1 = Y$, then $Z = \mathbb{P}^1 \times Y$. Assume therefore that Z_1 is a proper closed subset of Y. Choose $p \in \mathbb{P}^1$ such that $\{p\} \times Y$ is not contained in Z. By adapting the coordinates in $\mathbb{P}^1$, we may assume that $p = \infty$. Let $Y_2 := \pi_U(\{\infty\} \times U \cap Z)$. This is also a proper closed subset of Y and so Y contains an an affine open-dense subset $Y' \subset Y - Y_1 - Y_2$ such that $Z_{Y'}$ is contained in $\mathbb{A}^1 \times Y'$ and has finite fibers over Y'. Then $Z_{Y'}$ can be given as a subset of $\mathbb{A}^1 \times Y'$ by a polynomial in $A(Y')[t]$. After possible shrinking Y', we can assume that the top coefficient of this polynomial is a unit in $A(Y')$. Then $Z_{Y'}$ will be given by a monic polynomial and hence $Z_{Y'} \to Y'$ is a finite morphism.

Now assume $n \geq 2$. Let $q = [0 : \cdots : 0 : 1]$ and consider the blowup $\tilde{\mathbb{P}}^n := \mathrm{Bl}_{\{q\}} \mathbb{P}^n \to \mathbb{P}^n$. Recall that an element of $\tilde{\mathbb{P}}^n$ is the set of pairs in $([X_0 : \cdots : X_n], [Y_0 : \cdots : Y_{n-1}])$ in $\mathbb{P}^n \times \mathbb{P}^{n-1}$ with $[X_0 : \cdots : X_{n-1}] = [Y_0 : \cdots : Y_{n-1}]$. We have seen that over the open subset $U_{Y_i} \subset \mathbb{P}^{n-1}$ defined by $Y_i \neq 0$, the projection $\tilde{\mathbb{P}}^n \to \mathbb{P}^{n-1}$ is isomorphic to the projection $\mathbb{P}^1 \times U_{Y_i} \to U_{Y_i}$. Hence the projection $\pi_1 : \tilde{\mathbb{P}}^n \times U \to \mathbb{P}^{n-1} \times U$ is over $U_{Y_i} \times U$ like $\mathbb{P}^1 \times U_{Y_i} \times U \to U_{Y_i} \times U$. So this projection is closed over $U_{Y_i} \times U$. It follows that the projection π_1 is closed. The preimage $\tilde{Z}$ of Z under the projection $\tilde{\mathbb{P}}^n \times U \to \mathbb{P}^n \times U$ is closed and by what we just proved, $\pi_1(\tilde{Z})$ is closed in $\mathbb{P}^{n-1} \times U$. By induction, the image of the latter under the projection $\pi_2 : \mathbb{P}^{n-1} \times U \to U$ is closed. But this is just $\pi_U(Z)$.

For the dimension assertion, we may without loss of generality assume that Z is not contained in $\{q\} \times U$ (otherwise choose a different q) and that $\pi_U(Z) = U$ (otherwise replace U by $\pi(Z)$). We then replace $\tilde{Z}$ by the closure of $Z \cap (\mathbb{P}^n - \{q\}) \times U$ in $\tilde{\mathbb{P}}^n \times U$ so that $\tilde{Z}$ is irreducible, is of the same dimension as Z and maps also onto U. It therefore suffices to prove the dimension assertion for the projection $\tilde{\pi} : \tilde{Z} \to U$. We put $W := \pi_1(\tilde{Z}) \subset \mathbb{P}^{n-1} \times U$.

The case $n = 1$ treated above shows that for the projection $\pi_1 : \tilde{\mathbb{P}}^n \to \mathbb{P}^{n-1} \times U$ either $\tilde{Z} = \pi_1^{-1} W$ (so that $\tilde{Z}$ is a $\mathbb{P}^1$-bundle over W and $\dim \tilde{Z} = \dim W + 1$), or $\dim \tilde{Z} = \dim W$ and $\tilde{Z}$ is finite over $W - V \subset W$ where $V \subset W$ is a proper closed subset. In that last case, we note that for every closed irreducible subset $C \subset W$ which is not contained in V, we have $\dim(\pi_1^{-1} C \cap \tilde{Z}) = \dim C$: this is clear for an irreducible component of $\pi_1^{-1} C \cap \tilde{Z}$ which meets $\pi^{-1}(W - V)$ and any other irreducible component will be contained in a $\mathbb{P}^1$-bundle over $C \cap V$ and hence of dimension $1 + \dim(C \cap V) \leq \dim C$.

If $\pi_2 : \mathbb{P}^{n-1} \times U \to U$ is the projection, then (by induction) there exists an open-dense subset $U' \subset U$ such that the closed fibers of $W \to U$ resp. $V \to U$ all have dimension $\dim W - \dim U$ resp. have dimension smaller than $\dim W - \dim U$. So all the closed fibers of $\tilde{Z} \to U$ over U' have dimension $\dim \tilde{Z} - \dim U$. □

We mention a few corollaries.

COROLLARY 5.3. *Let X be a projective variety. Then any morphism from X to a variety is closed (and hence has closed image).*

PROOF. Assume that X is closed in $\mathbb{P}^n$. A morphism $f : X \to Y$ to a variety Y can be factored as the obvious isomorphism of X onto the graph Γ_f of f, the inclusion of this graph in $X \times Y$ (which is evidently closed), the inclusion of $X \times Y$ in $\mathbb{P}^n \times Y$ (which is closed since $X \subset \mathbb{P}^n$ is closed) and the projection onto Y (which is closed by Theorem 5.1). So f is closed. □

It is an elementary result from complex function theory (based on Liouville's thoerem) that a holomorphic function on the Riemann sphere is constant. This implies the corresponding assertion for holomorphic functions on complex projective n-space $\mathbb{P}^n_{\mathbb{C}}$ (to see that a holomorphic function on $\mathbb{P}^n_{\mathbb{C}}$ takes the same value on any two distinct points, simply apply the previous remark to its restriction to the complex projective line passing through them, viewed as a copy of the Riemann sphere). The following corollary is an algebraic version of this fact.

COROLLARY 5.4. *Let X be a projective variety. Then any morphism from X to a quasi-affine variety is constant. In particular, any regular function on X is constant.*

PROOF. If $f : X \to Y$ is a morphism to a quasi-affine variety Y, then its composite with an embedding of Y in some affine space $\mathbb{A}^n$ is given by n regular functions on X. So it suffices to prove the special case when $Y = \mathbb{A}^1$. By the previous corollary this image is closed in $\mathbb{A}^1$. But if we think of f as taking its values in $\mathbb{P}^1$ (via the embedding $y \in \mathbb{A}^1 \mapsto [1 : y] \in \mathbb{P}^1$), then we see that $f(X)$ is also closed in $\mathbb{P}^1$. So $f(X)$ cannot be all of $\mathbb{A}^1$. Since X is irreducible, so is the image and it follows that $f(X)$ is a singleton. In other words, f is constant. □

PROPOSITION 5.5. *Let $Z \subset \mathbb{P}^n$ an irreducible and closed subset. If $Q \subset \mathbb{P}^n$ is a linear subspace with the property that $Q \cap Z = \emptyset$, then $\dim Z + \dim Q < n$ and the projection $\pi : \mathbb{P}^n \to \mathbb{P}^n_Q$ maps Z onto an irreducible and closed subset $\pi(Z)$ with the property that every fiber of $Z \to \pi(Z)$ is finite.*

PROOF. Every fiber of $Z \to \pi(Z)$ is the intersection of Z with a linear subspace $\tilde{Q} \subset \mathbb{P}^n$ which contains Q a hyperplane. It is closed in $\tilde{Q}$ and hence this fiber is projective (or strictly speaking, every irreducible component of that fiber is). On the other hand it is contained in the hyperplane complement $\tilde{Q} - Q$, which is affine. So the fiber is also affine. Then Corollary 5.4 implies that each irreducible component of this fiber is a singleton. Hence the fiber is finite.

It follows from Theorem 5.1 that $\dim Z = \dim \pi(Z) \leq \dim \mathbb{P}^n_Q - \dim Q - 1$. □

EXERCISE 65. Let P be a projective space of dimension n.

(a) The *dual $\check{P}$ of P* is by definition the collection of hyperplanes in P. Prove that $\check{P}$ has a natural structure of a projective space.
(b) Identify the double dual of P with P itself.

(c) The *incidence locus* $I \subset P \times \check{P}$ is the set of pairs $(p, q) \in P \times \check{P}$ with the property that p lies in the hyperplane H_q defined by q. Prove that I is a nonsingular variety of dimension $2n - 1$.
(d) Show that we can find homogeneous coordinates $[Z_0 : \cdots : Z_n]$ for P and $[W_0 : \cdots : W_n]$ for $\check{P}$ such that I is given by $\sum_{i=0}^{n} Z_i W_i = 0$.

EXERCISE 66. Let $F \in k[X_0, \ldots, X_n]_d$ define a nonsingular hypersurface H in $\mathbb{P}^n$. Prove that the map $H \to \check{\mathbb{P}}^n$ which assigns to $p \in H$ the projectived tangent space of H at p is given by $[\frac{\partial F}{\partial Z_0} : \cdots : \frac{\partial F}{\partial Z_n}]$. Prove that the image of this map is closed in $\check{\mathbb{P}}^n$ (this image is called *the dual of* H). What can you say in case $d = 2$?

6. Constructible sets

We now ask about the image of an arbitrary morphism of varieties. This need not be a variety as the following simple example shows.

EXAMPLE 6.1. Consider the morphism $f : \mathbb{A}^2 \to \mathbb{A}^2$, $(x_1, x_2) \mapsto (x_1, x_1 x_2)$. A point $(y_1, y_2) \in \mathbb{A}^2$ is in the image of f if and only if the equation $y_2 = y_1 x_2$ has a solution in x_2. This is the case precisely when $y_1 \neq 0$ or when $y_1 = y_2 = 0$. So the image of f is the union of the open subset $y_1 \neq 0$ and the singleton $\{(0, 0)\}$. This is not a locally closed subset, but the union of two such.

DEFINITION 6.2. A subset of variety is called *constructible* if it can be written as the union of finitely many (locally closed) subvarieties.

THEOREM 6.3. *Let $f : X \to Y$ be a morphism of varieties. Then f takes constructible subsets of X to constructible subsets of Y. In particular, $f(X)$ is constructible.*

We first show that the theorem follows from

PROPOSITION 6.4. *Let X be an irreducible variety and let $f : X \to Y$ be a morphism of varieties. Then $f(X)$ contains a nonempty open subset of its closure (in other words, $f(X)$ contains a locally closed subvariety of Y which is dense in $f(X)$).*

PROOF THAT PROPOSITION 6.4 IMPLIES THEOREM 6.3. A constructible subset is a finite union of irreducible subvarieties and so it is clearly enough to prove that the image of each of these is constructible. In other words, it suffices to show that the image of a morphism $f : X \to Y$ of varieties with X irreducible is constructible. We prove this with induction on the dimension of X. According to Proposition 6.4 the closure of $f(X)$ contains a nonempty open subset U such that $f(X) \supset U$. It is clear that $f^{-1}U$ is a nonempty open subset of X. If $Z := X - f^{-1}U$, then $f(X) = U \cup f(Z)$. The irreducible components of Z have smaller dimension than X and so $f(Z)$ is constructible by induction. □

PROOF OF PROPOSITION 6.4. Since X is covered by finitely many of its open affine subsets, we may without loss of generality assume that X is affine. So we can assume that X is closed in some $\mathbb{A}^n$. Then the graph of f identifies X with a closed subset of $\mathbb{A}^n \times Y$ and so we see that we only need to prove that for every closed subset $X \subset \mathbb{A}^n \times Y$, $\pi_Y(X)$ contains a nonempty open subset of $\overline{\pi_Y(X)}$. Since we can factor π_Y in an obvious manner into successive line projections (by forgetting the last coordinate)

$$\mathbb{A}^n \times Y \to \mathbb{A}^{n-1} \times Y \to \cdots \to \mathbb{A}^1 \times Y \to Y,$$

it suffices to do the case $n = 1$. Upon replacing Y by $\overline{\pi_Y(X)}$, we are now left to show that if $X \subset \mathbb{A}^1 \times Y$ is closed and such that $\pi_Y(X)$ is dense in Y, then $\pi_Y(X)$ contains a nonempty open subset of Y.

Since X is irreducible, so is its image $\pi_Y(X)$ and hence also Y. Upon replacing Y be a nonempty affine open subset and X by the preimage of that open subset, we may also assume that Y is affine.

When $X = \mathbb{A}^1 \times Y$, there is nothing to show. Otherwise X is contained in a hypersurface $Z(f) \subset \mathbb{A}^1 \times Y$ with equation $f \in A(Y)[x]$, $f(x, y) = \sum_{i=0}^{N} a_i(y)x^i$, with $a_i \in A(Y)$ and a_N not identically zero. Next, by replacing Y by the nonzero set $U(a_N)$ and X by its preimage, we may assume that a_N is nowhere zero. We prove that then $\pi_Y(X) = Y$. Since is a_N now invertible in $A(Y)$, we may assume that f is a monic polynomial. Then $Z(f) \to Y$ is a finite morphism and hence closed by Exercise 37. Since X is a closed subset of $Z(f)$, it follows that $\pi_Y(X)$ is closed in Y. Since $\pi_Y(X)$ is also dense in Y, it follows that $\pi_Y(X) \supset Y$. □

7. The Veronese embedding

Let be given a positive integer d. We index the monomials in $Z_0, \dots, Z_n$ that are homogenous of degree d by their exponents: these are the sequences of non-negative integers $\mathbf{d} = (d_0, \dots, d_n)$ with sum d. They are $\binom{n+d}{d}$ in number. We use this index set to label the homogeneous coordinates $Z_{\mathbf{d}}$ of $\mathbb{P}^{\binom{n+d}{d}-1}$.

PROPOSITION 7.1 (The Veronese embedding). *The map $f_d : \mathbb{P}^n \to \mathbb{P}^{\binom{n+d}{d}-1}$ defined by $Z_{\mathbf{d}} = X_0^{d_0} \cdots X_n^{d_n}$ is an isomorphism onto a closed subset of the target projective space.*

PROOF. In order to prove that f_d is an isomorphism onto a closed subset, it is enough to show that for every chart domain $U_{\mathbf{d}}$ of the standard atlas of the target space, its preimage $f_d^{-1}U_{\mathbf{d}}$ is open in $\mathbb{P}^n$ and is mapped by f_d isomorphically onto a closed subset of $U_{\mathbf{d}}$. This preimage is defined by $X_0^{d_0} \cdots X_n^{d_n} \neq 0$. Let us renumber the coordinates such that $d_0, \dots, d_r$ are positive and $d_{r+1} = \cdots = d_n = 0$. Then $f_d^{-1}U_{\mathbf{d}} = U_0 \cap \cdots \cap U_r \subset U_0$. So if we use the standard coordinates $(x_1, \dots, x_n)$ on U_0, then $f_d^{-1}U_{\mathbf{d}}$ is defined by $x_1 \cdots x_r \neq 0$.

The coordinates on $U_{\mathbf{d}}$ are the functions $Z_{\mathbf{e}}/Z_{\mathbf{d}}$ with $\mathbf{e} \neq \mathbf{d}$. Let us write $z_{\mathbf{e}-\mathbf{d}} := z_{e_0-d_0, e_1-d_1, \dots, e_n-d_n}$ for this function. This notation is chosen as to make the expression f_d in terms of these coordinates simply:

$$f_d : U_0(x_1 \cdots x_r) = f_d^{-1}U_{\mathbf{d}} \to U_{\mathbf{d}}, \quad z_{\mathbf{e}-\mathbf{d}} = x_1^{e_1-d_1} \cdots x_n^{e_n-d_n} \quad (\mathbf{e} \neq \mathbf{d}).$$

Since the Laurent monomial $x_1^{e_1-d_1} \cdots x_n^{e_n-d_n}$ has degree $d_0 - e_0$, the components of the above morphism are all the nonconstant Laurent monomials $x_1^{k_1} \cdots x_n^{k_n}$ with $k_i \geq -d_i$ and of total degree $k_1 + \cdots + k_n \leq d_0$. In particular, each x_i appears as a component and so does the Laurent monomial $x_1^{-d_1} \cdots x_r^{-d_r}$. The graph of the regular function $x_1^{d_1} \cdots x_r^{d_r}$ on $U_0(x_1 \cdots x_r)$ identifies $U_0(x_1 \cdots x_r)$ with the closed hypersurface $Z = Z(yx_1^{d_1} \cdots x_r^{d_r} - 1)$ in $\mathbb{A}^{n+1}$. All other components of $f_d|U_0(x_1 \cdots x_r) : U_0(x_1 \cdots x_r) \to U_{\mathbf{d}}$ are products of $x_1, \dots, x_n, x_1^{-d_1} \cdots x_r^{-d_r}$ and so its image is the graph of a morphism $Z \to \mathbb{A}^{\binom{n+d}{d}-n-2}$. So we get a closed embedding. □

The following proposition is remarkable for its repercussions in intersection theory.

PROPOSITION 7.2. *Let $H \subset \mathbb{P}^n$ be a hypersurface. Then $\mathbb{P}^n - H$ is affine and for every closed irreducible subset $Z \subset \mathbb{P}^n$ of positive dimension, $Z \cap H$ is nonempty and of dimension $\geq \dim(Z) - 1$, with equality holding if Z is not contained in H.*

For the proof we need the following complement to Proposition 5.5.

PROPOSITION 7.3. *For every proper closed subset $Z \subsetneq \mathbb{P}^n$ there exists a linear subspace in P of dimension $n - \dim(Z) - 1$ which misses Z.*

PROOF. We may (and will) assume that Z is irreducible. Let i be a nonnegative integer $< n - \dim(Z)$. We prove with induction on i that Z misses a linear subspace of dimension i. If $i = 0$, then we must have $\dim(Z) < n$ and so any singleton in $\mathbb{P}^n - Z$ is as required. When $i > 0$, there exists by induction hypothesis a linear subspace $Q \subset \mathbb{P}^n$ of dimension $(i-1)$ which does not meet Z. Then projection from Q defines a morphism $\pi : Z \to \mathbb{P}^n_Q$ from Z to a projective space of dimension $n - i$. Any fiber of this map is an intersection of Z with a linear subspace in $\mathbb{P}^n$ of dimension i passing through Q. We claim that at least one of them is empty. For if not, then π is surjective and hence dominant. In particular, $\dim(Z) \geq \dim(\mathbb{P}^n_Q) = n - i$, which evidently contradicts our assumption that $i < n - \dim(Z)$. □

PROOF OF PROPOSITION 7.2. The hypersurface H is given by a homogeneous polynomial of degree d, say by $\sum_{\mathbf{d}} c_{\mathbf{d}} X_0^{d_0} \cdots X_n^{d_n}$. This determines a hyperplane $\tilde{H} \subset \mathbb{P}^{\binom{n+d}{d}-1}$ defined by $\sum_{\mathbf{d}} c_{\mathbf{d}} Z_{\mathbf{d}}$. It is clear that H is the preimage of $\tilde{H}$ under the Veronese morphism and hence the latter identifies $\mathbb{P}^n - H$ with a closed subset of the affine space $\mathbb{P}^{\binom{n+d}{d}-1} - \tilde{H}$. So $\mathbb{P}^n - H$ is affine.

For the rest of the argument we may, by passing to the Veronese embedding, assume that H is a hyperplane. If $\dim(Z \cap H) \leq \dim(Z) - 2$, then by Proposition 7.3 there exists a linear subspace $Q \subset H$ of dimension $\dim(H) - (\dim(Z \cap H) - 1 \leq (n-1) - (\dim(Z) - 2) - 1 = n - \dim(Z)$ which avoids $Z \cap H$. Then Q is a linear subspace of $\mathbb{P}^n$ which avoids Z and we thus contradict Proposition 5.5. This proves that $\dim(Z \cap H) \geq \dim(Z) - 1$. If Z is irreducible and not contained in H, then we have also $\dim(Z \cap H) \leq \dim(Z) - 1$. □

EXERCISE 67. Let d be a positive integer. The *universal hypersurface of degree d* is the hypersurface of $\mathbb{P}^n \times \mathbb{P}^{\binom{n+d}{d}-1}$ defined by $F(X, Z) := \sum_{\mathbf{d}} Z_{\mathbf{d}} X_0^{d_0} X_1^{d_1} \cdots X_n^{d_n}$. We denote it by H and let $\pi : H \to \mathbb{P}^{\binom{n+d}{d}-1}$ be the projection.

(a) Prove that H is nonsingular.
(b) Prove that projection π is *singular* at (X, Z) (in the sense that the derivative of π at (X, Z) is not a surjection) if and only the partial derivatives of $F_Z \in k[X_0, \ldots, X_n]$ have X as a common zero.
(c) Suppose from now on that $d \geq 2$. Prove that the singular set of π is a smooth subvariety of $\mathbb{P}^n \times \mathbb{P}^{\binom{n+d}{d}-1}$ of codimension $n + 1$.
(d) Prove that the set of $Z \in \mathbb{P}^{\binom{n+d}{d}-1}$ over which π has a singular point is a hypersurface. This hypersurface is called the *discriminant* of π.
(e) For $d = 2$ we denote the coordinates of $\mathbb{P}^{\binom{n+d}{d}-1}$ simply by Z_{ij} (where it is understood that $Z_{ij} = Z_{ji}$). Prove that the discriminant of π is then the zero set of $\det(Z_{ij})$.

8. Grassmannians

Let P be a projective space of dimension n and let $d \in \{0, \ldots, n\}$. We want to show that the collection $\mathrm{Gr}_d(P)$ of linear d-dimensional subspaces of P is a nonsingular projective variety. Let the projective structure on P be defined by the pair (V, ℓ) so that V is a $(n+1)$-dimensional k-vector space and P has been identified with $\mathbb{P}(V)$.

LEMMA 8.1. *Let $Q \subset P$ be a linear subspace of* codimension $d+1$. *Then the collection of linear d-dimensional subspaces of P contained in $P - Q$ has in a natural manner the structure of an affine space A_Q of dimension $(n-d)(d-1)$.*

PROOF. Let Q correspond to the linear subspace $W \subset V$ of dimension $(n+1) - (d+1) = n - d$. Then the elements of A_Q correspond to linear subspaces $L \subset V$ of dimension $d+1$ with $L \cap W = \{0\}$. This means that $V = L \oplus W$. The affine structure is best seen by fixing some L_0 with that property. Then every other such L is always the graph of a (unique) linear map $L_0 \to W$ and vice versa. So this identifies A_Q with $\mathrm{Hom}(L_0, W)$. It is easy to verify that this affine structure is independent of the choices (the translation vector space of A_Q is canonically identified with $\mathrm{Hom}(V/W, W)$). □

It can now be shown without much difficulty that $\mathrm{Gr}_d(P)$ admits a unique structure of a variety for which a subset as in this lemma is affine open and its identification with affine space an isomorphism. We will however proceed in a more direct manner to show that $\mathrm{Gr}_d(P)$ admits the structure of a projective variety.

We recall that the exterior algebra $\bigwedge^\bullet V = \oplus_{p=0}^\infty \bigwedge^p V$ is the quotient of the tensor algebra on V, $\oplus_{p=0}^\infty V^{\otimes p}$ (here $V^{\otimes 0} = k$ by convention), by the two-sided ideal generated by the 'squares' $v \otimes v$, $v \in V$. It is customary to denote the product by the symbol $\wedge$. So we can characterize $\bigwedge^\bullet V$ as (noncommutative) associative k-algebra with unit element by saying that is generated by the k-vector space V and is subject to the relations $v \wedge v = 0$ for all $v \in V$. It is a graded algebra ($\bigwedge^p V$ is the image of $V^{\otimes p}$) and 'graded-commutative' in the following sense: if $\alpha \in \bigwedge^p V$ and $\beta \in \bigwedge^q V$, then $\beta \wedge \alpha = (-1)^{pq} \alpha \wedge \beta$. If $e_0, \ldots, e_n$ is a basis for V, then a basis of $\bigwedge^p V$ is indexed by the p-element subsets $I \subset \{0, \ldots, n\}$: $I = \{0 \leq i_1 < i_2 < \cdots < i_p \leq n\}$ is associated to the basis element $e_I = e_{i_1} \wedge \cdots \wedge e_{i_p}$ (where the convention is that $e_\emptyset = 1 \in k = \bigwedge^0 V$). So $\dim \bigwedge^p V = \binom{n+1}{p}$. Notice that $\bigwedge^{n+1} V$ is one-dimensional and spanned by $e_0 \wedge \cdots \wedge e_n$, whereas $\bigwedge^p V = 0$ for $p > n+1$. Let us say that $\alpha \in \bigwedge^p V$ is *fully decomposable* if the exist linearly independent $v_1, \ldots, v_p$ in V such that $\alpha = v_1 \wedge \cdots \wedge v_p$. This is equivalent to the existence of a p-dimensional subspace $K \subset V$ such that α is a generator of $\wedge^p K$.

LEMMA 8.2. *Let $\alpha \in \bigwedge^p V$ be nonzero. Denote by $K(\alpha)$ the set of $e \in V$ with $e \wedge \alpha = 0$. Then $\dim K(\alpha) \leq p$ and equality holds if and only if α is fully decomposable and spans $\bigwedge^p K(\alpha)$.*

PROOF. Let $e_1, \ldots, e_r$ be a basis of $K(\alpha)$ and let $V' \subset V$ be a subspace supplementary to $K(\alpha)$. Then we have a decomposition

$$\bigwedge^\bullet V = \bigoplus_{I \subset \{1, \ldots, r\}} e_I \wedge \bigwedge^{\bullet - |I|} V'.$$

Wedging with e_i kills all the summands in which e_i appears and is injective on the sum of the others. So $\alpha \subset e_1 \wedge \cdots \wedge e_r \wedge \bigwedge^{p-r} V'$. In particular, $r \leq p$ with equality holding if and only if α is a multiple of $e_1 \wedge \cdots \wedge e_p$. □

If L is a linear subspace of V of dimension $d+1$, then $\bigwedge^{d+1} L$ is of dimension 1 and will be thought of as a one dimensional subspace of $\bigwedge^{d+1} V$. We thus have defined map $\delta : \mathrm{Gr}_d(P) \to \mathbb{P}(\bigwedge^{d+1} V)$, $[L] \mapsto [\bigwedge^{d+1} L]$. It is called the *Plücker embedding* because of:

PROPOSITION 8.3. *The map $\delta : \mathrm{Gr}_d(P) \to \mathbb{P}(\bigwedge^{d+1} V)$ maps $\mathrm{Gr}_d(P)$ bijectively onto a closed subset of $\mathbb{P}(\bigwedge^{d+1} V)$.*

PROOF. Let $\alpha \in \bigwedge^{d+1} V$. According to Lemma 8.2 , $[\alpha]$ is in the image of δ if and only if $K(\alpha)$ is of dimension $d+1$ and if that is the case, then $\delta^{-1}[\alpha]$ has $\mathbb{P}(K(\alpha))$ as its unique element. In particular, δ is injective. Consider the linear map

$$\bigwedge^{d+1} V \to \mathrm{Hom}(V, \bigwedge^{d+2} V), \quad \alpha \mapsto e_\alpha := \alpha\wedge$$

The set of linear maps $V \to \bigwedge^{d+2} V$ with kernel of dimension $\geq d+1$ are those of rank $< s := \dim(\bigwedge^{d+2} V) - d$. If we choose a basis for V, then this locus is given by set a homogeneous equations in $\mathrm{Hom}(V, \bigwedge^{d+2} V)$, namely the $s \times s$-minors of the corresponding matrices. Hence the set of $\alpha \in \bigwedge^{d+1} V$ for which $\dim K(\alpha) \geq d+1$ is also given by a set of homogeneous equations and thus defines a closed subset of $\mathbb{P}(\bigwedge^{d+1} V)$. This subset is the image of δ. □

Proposition 8.3 gives $\mathrm{Gr}_d(P)$ the structure of projective variety. In order to complete the construction, let $Q \subset P$ be a linear subspace of codimension d. Let $W \subset V$ correspond to Q and choose a generator $\beta \in \bigwedge^{n-d} W$. Then we have a nonzero linear form

$$e_\beta = \beta\wedge : \bigwedge^{d+1} V \to \bigwedge^{n+1} V \cong k.$$

Its kernel defines a hyperplane in $\mathbb{P}(\bigwedge^{d+1} V)$ and hence an affine subspace $U_{e_\beta} \subset \mathbb{P}(\bigwedge^{d+1} V)$.

LEMMA 8.4. *The preimage of U_{e_β} under the Plücker embedding is the affine space A_Q and δ maps A_Q isomorphically onto its image.*

PROOF. If α is the generator of $\bigwedge^{d+1} L$ for some $(d+1)$-dimensional subspace, then $L \cap W = \{0\}$ if and only if $\alpha \wedge \beta \neq 0$: if $L \cap W$ contains a nonzero vector v then both α and β are divisible by v and so $\alpha \wedge \beta = 0$; if $L \cap W = \{0\}$, then we have decomposition $V = L \oplus V$ and it is then easily seen (by picking a compatible basis of V for example) that $\alpha \wedge \beta \neq 0$. This implies that $\delta^{-1} U_{e_\beta} = A_Q$.

Let us now express the restriction $\delta : A_Q \to U_{e_\beta}$ in terms of coordinates. Choose a basis $e_0, \ldots, e_n$ for V such that $e_{d+1}, \ldots, e_n$ is a basis for W and $\beta = e_{d+1} \wedge \cdots \wedge e_n$. Then e_β simply assigns to an element α of $\bigwedge^{d+1} V$ the coefficient of $e_0 \wedge \cdots \wedge e_d$ in α. If $L_0 \subset V$ denotes the span of $e_0, \ldots, e_d$, then $A_Q \cong \mathrm{Hom}(L_0, W)$ is identified with the affine space $\mathbb{A}^{(d+1)\times(n-d)}$ of $(d+1) \times (n-d)$-matrices via

$$(a_i^j)_{0 \leq i \leq d < j \leq n} \mapsto \ k\text{-span in } V \text{ of the } d+1 \text{ vectors } \{e_i + \sum_{j=d+1}^{n} a_i^j e_j\}_{i=0}^{d},$$

so that δ is given by

$$(a_i^j)_{0\le i\le d<j\le n} \mapsto (e_0 + \sum_{j=d+1}^{n} a_0^j e_j) \wedge \cdots \wedge (e_d + \sum_{j=d+1}^{n} a_d^j e_j).$$

The coefficient of $e_{i_0} \wedge \cdots \wedge e_{i_d}$ is a determinant of which entry is 0, 1 or some a_i^j and hence is a polynomial in the matrix coefficients a_i^j. It follows that this restriction of δ is a morphism. Among the components of δ we find the matrix coefficients themselves: a_i^j appears up to sign as the matrix coefficient of $e_0 \wedge \cdots \wedge \widehat{e_i} \wedge \cdots \wedge e_d \wedge e_j$. So the image is really a graph of a morphism defined on $\mathbb{A}^{(d+1)\times(n-d)}$. Hence δ maps A_Q isomorphically onto its image in U_{e_β}. □

COROLLARY 8.5. *The Plücker embedding realizes* $\mathrm{Gr}_d(P)$ *as a nonsingular subvariety of* $\mathbb{P}(\bigwedge^{d+1} V)$ *of dimension* $(n-d)(d+1)$. *This structure is compatible with the affine structure that we have on each* A_Q.

PROOF. Every two open subsets of the form A_Q a have nonempty intersection and so $\mathrm{Gr}_d(P)$ is irreducible. The rest follows from the previous corollary. □

REMARK 8.6. The image of $\mathrm{Gr}_d(P)$ is a closed orbit of the natural $\mathrm{SL}(V)$-action on $\mathbb{P}(\bigwedge^{d+1} V)$. It lies in the closure of any other $\mathrm{SL}(V)$-orbit.

EXERCISE 68. Let P be a projective space. Given integers $0 \le d < e \le \dim P$, prove that the set of pairs of linear subspaces $R \subset Q \subset P$ with $\dim R = d$ and $\dim Q = e$ is a closed subvariety of $\mathrm{Gr}_d(P) \times \mathrm{Gr}_e(P)$.

The Grassmannian of hyperplanes in a projective space is itself a projective space (see Exercise 65). So the simplest example not of this type is the Grassmannian of lines in a 3-dimensional projective space.

Let V be vector space dimension 4. On the 6-dimensional space $\bigwedge^2 V$ we have a homogeneous polynomial $F : \bigwedge^2 V \to k$ of degree two defined by

$$F(\alpha) := \alpha \wedge \alpha \in \bigwedge^4 V \cong k$$

(the last identification is only given up to scalar and so the same is true for F). In coordinates F is quite simple: if $e_1, \ldots, e_4$ is a basis for V, then $(e_i \wedge e_j)_{1\le i<j\le 4}$ is basis for $\bigwedge^2 V$. So if we label the homogeneous coordinates of $\mathbb{P}(\bigwedge^2 V)$ accordingly: $[X_{1,2} : \cdots : X_{3,4}]$, then F is given by

$$F(X_{1,2}, \ldots, X_{3,4}) = X_{1,2}X_{3,4} - X_{1,3}X_{2,4} + X_{1,4}X_{2,3}.$$

Notice that F is irreducible. Its partial derivatives are the coordinates themselves (up to sign and order) and so F defines a smooth quadric hypersurface of dimension 4 in a 5-dimensional projective space.

PROPOSITION 8.7. *The image of the Plücker embedding of* $G_1(\mathbb{P}(V))$ *in* $\mathbb{P}(\bigwedge^2 V)$ *is the zero set of* F.

PROOF. The image of the Plücker embedding is of dimension 4 and so must be a hypersurface. Since the zero set of F is an irreducible hypersurface, it suffices to show that the Plücker embedding maps to the zero set of F. For this, let α be a generator of $\bigwedge^2 L$ for some linear subspace $L \subset V$ of dimension 2. If $e_1, \ldots, e_4$ is a basis of V such that $\alpha = e_1 \wedge e_2$, then it is clear that $\alpha \wedge \alpha = 0$. This proves that the Plücker embedding maps to the zero set of F. □

REMARK 8.8. The image of the Plücker embedding $\mathrm{Gr}_d(P) \hookrightarrow \mathbb{P}(\wedge^{d+1}V)$ is in fact always the common zero set of a collection of quadratic equations, called the *Plücker relations*. To exhibit these, we first recall that every $\phi \in V^*$ defines a linear 'inner contraction' map $\iota_\phi : \wedge^\bullet V \to \wedge^{\bullet-1}V$ of degree -1 characterized by the fact that for $v \in V$, $\iota_\phi(v) = \phi(v) \in k = \wedge^0 V$ and for $\alpha \in \wedge^p V, \beta \in \wedge^\bullet V$, $\iota_\phi(\alpha\wedge\beta) = \iota_\phi(\alpha)\wedge\beta + (-1)^p\alpha\wedge\iota_\phi(\beta)$. We then define a linear map $B : \wedge^{d+1}V \times \wedge^{d+1}V \to \wedge^{d+2}V \otimes \wedge^d V$ as follows: if $(e_0, \ldots, e_n)$ is a basis of V and $(e_0^*, \ldots, e_n^*)$ is the basis of V^* dual to $(e_0, \ldots, e_n)$, then

$$B(\alpha, \beta) := \sum_{r=0}^{n} (\alpha \wedge e_r) \otimes (\iota_{e_r^*}\beta).$$

It is easy to check that this is independent of the choice of basis. In particular, if α is fully decomposable, then we can choose $(e_0, \ldots, e_n)$ in such a manner that $\alpha = e_0 \wedge \cdots \wedge e_d$. We then find:

$$B(\alpha, \alpha) = \sum_r (e_0 \wedge \cdots \wedge e_d \wedge e_r) \otimes (\iota_{e_r^*} e_0 \wedge \cdots \wedge e_d \wedge e_r) = 0,$$

because $e_0 \wedge \cdots \wedge e_d \wedge e_r = 0$ for $r \leq d$ and $\iota_{e_r^*} e_0 \wedge \cdots \wedge e_d \wedge e_r = 0$ for $r > d$. This identity might be called the *universal Plücker relation*. One can show that conversely, any $\alpha \in \wedge^{d+1}V$ for which $B(\alpha, \alpha) = 0$ is either zero or fully decomposable.

Let us rephrase this in terms of algebraic geometry: every nonzero linear form ℓ on $\wedge^{d+2}V \otimes \wedge^d V$, determines a quadratic form Q_ℓ on $\wedge^{d+1}V$ defined by $\alpha \mapsto \ell(B(\alpha, \alpha))$ whose zero set is a quadratic hypersurface in $\mathbb{P}(\wedge^{d+1}V)$. This quadric contains the Plücker locus and the latter is in fact the common zero set of the Q_ℓ, with ℓ running over the linear forms on $\wedge^{d+2}V \otimes \wedge^d V$. It can be shown that the Q_ℓ generate the full graded ideal defined by the Plücker locus.

PROPOSITION-DEFINITION 8.9. *Let X be a closed subvariety of the projective space P. If d is an integer between 0 and $\dim P$, then the set of d-linear subspaces of P which are contained in X defines a closed subvariety $F_d(X)$ of $\mathrm{Gr}_d(P)$, called the* Fano variety *(of d-planes) of X.*

PROOF. An open affine chart of $\mathrm{Gr}_d(P)$ is given by a decomposition $V = L \oplus W$ with $\dim L = d + 1$ and $\dim W = n - d$ and is then parametrized by $\mathrm{Hom}(L, W)$ by assigning to $A \in \mathrm{Hom}(L, W)$ the graph of A. It suffices to prove that via this identification $F_d(X)$ defines a closed subset of $\mathrm{Hom}(L, W)$.

Choose homogeneous coordinates $[Z_0 : \cdots : Z_n]$ such that L resp. W is given by $Z_{d+1} = \cdots = Z_n = 0$ resp. $Z_0 = \cdots Z_d = 0$. A linear map $A \in \mathrm{Hom}(L, W)$ is then given by $A^* Z_{d+i} = \sum_{j=0^d} a_{ij} Z_j$, $i = 1, \ldots, n - d$. It defines an element of $F_d(X)$ if and only for all $G \in \cup_{m\geq 0} I_m(X)$, $G(Z_0, \ldots, Z_d, A^*Z_{d+1}, \ldots A^*Z_n)$ is identically zero. This means that the coefficient of every monomial $Z_0^{m_0} \cdots Z_d^{m_d}$ in such an expression much vanish. Since this coefficient is a polynomial in the matrix coefficients a_{ij} of A, we find that the preimage of $F_d(X)$ in $\mathrm{Hom}(L, W)$ is the common zero set of a set of polynomials and hence is closed therein. □

EXAMPLE 8.10. Consider the case of a quadratic hypersurface $X \subset \mathbb{P}(V)$ and assume for simplicity that $\mathrm{char}(k) \neq 2$. So in terms of homogeneous coordinates $[X_0 : \cdots : X_n]$, X can be given by an equation $F(X_0, \ldots, X_n) = \frac{1}{2}\sum_{0\leq i,j\leq n} b_{ij} X_i X_j$ with $b_{ij} = b_{ji}$ (so $\frac{1}{2}b_{ii}$ is the coefficient of X_i^2). In more intrinsic terms: X is given by a symmetric bilinear form $B : V \times V \to k$ (namely by $B(v, v) = 0$). Let us assume that X is nonsingular. This means that the partial derivatives of F have no common zero in $\mathbb{P}(V)$. This translates into: $B : V \times V \to k$ is nonsingular, that is, the linear map $b : v \in V \mapsto B(\ , v) \in V^*$ is an isomorphism of vector spaces. A subspace

$L \subset V$ determines an element of the Fano variety of X precisely when $B(v,v) = 0$ for all $v \in L$. This implies that B is identically zero on $L \times L$. So b maps L to $(V/L)^* \subset V^*$. Since b is injective, this implies that $\dim L \leq \dim(V/L)$, in other words that $\dim L \leq \frac{1}{2}\dim V$.

This condition is optimal. If for instance $\dim V = 2m+2$ is even, then it not difficult to show that we can find coordinates $(X_0, \cdots, X_{2m+1})$ such that $F = \sum_{i=0}^{m} X_i X_{m+1+i}$. Let L resp. L' be the linear subspace defined by $X_{m+1} = \cdots = X_{2m+1} = 0$ resp. $X_0 = \cdots = X_m = 0$, so that $V = L \oplus L'$. Notice that both $[L]$ and $[L']$ are in $F_m(X)$. The vector space $\mathrm{Hom}(L, L')$ describes an affine open subset of the Grassmannian of m-planes in $\mathbb{P}(V)$. An element $A \in \mathrm{Hom}(L, L')$ is given by $A^* X_{m+i} = \sum_{j=0}^{m} a_{ij} X_j$, $j = 0, \ldots, m$. The corresponding m-plane is contained in X precisely when $\sum_{i,j=0}^{m} a_{ij} X_i X_j$ is identically zero, i.e., if (a_{ij}) is antisymmetric. It follows that $[L] \in F_m(X)$ has a neighborhood isomorphic to an affine space of dimension $\frac{1}{2}m(m+1)$.

EXERCISE 69. Let X be a quadratic hypersurface $\mathbb{P}(V)$ of odd dimension $2m+1$ and assume for simplicity that $\mathrm{char}(k) \neq 2$. Prove that $F_{m+1}(X) = \emptyset$ and that $F_m(X) \neq \emptyset$ (Hint: use the fact that we can choose coordinates $(X_0, \ldots, X_{2m+2})$ for V such that F is given by $X_0^2 + \sum_{i=1}^{m+1} X_i X_{m+1+i}$.) Prove that $F_m(X)$ is a smooth variety and determine its dimension.

EXERCISE 70. Let $X \subset \mathbb{P}^n$ be a hypersurface of degree d and let $0 \leq m \leq n$. Prove that the intersection of $F_m(X)$ with a standard affine subset of $\mathrm{Gr}_m(\mathbb{P}^n)$ is given by $\binom{m+d}{d}$ equations.

EXERCISE 71. Consider the universal hypersurface of degree d in $\mathbb{P}^n$, $H \subset \mathbb{P}^n \times \mathbb{P}^{\binom{n+d}{d}-1}$.

(a) For every m-plane $Q \subset \mathbb{P}^n$, let Y_z denote the set of $z \in \mathbb{P}^{\binom{n+d}{d}-1}$ for which the corresponding hypersurface H_z contains Q. Prove that Y_z is a linear subspace of $\mathbb{P}^{\binom{n+d}{d}-1}$ of codimension $\binom{m+d}{d}$.

(b) Let $Y \subset \mathbb{P}^{\binom{n+d}{d}-1}$ be the set of $z \in \mathbb{P}^{\binom{n+d}{d}-1}$ for which H_z contains an m-plane. Prove that Y is a closed subset of $\mathbb{P}^{\binom{n+d}{d}-1}$ of codimension at most $\binom{m+d}{d} - (m+1)(n-m)$.

(c) Conclude that every hypersurface of degree d in $\mathbb{P}^n$ contains an m-plane if $\binom{m+d}{d} \leq (m+1)(n-m)$. [1]

Let P be as before and let X be a nonsingular (not necessarily closed) subvariety of P of dimension d. For every $p \in X$, we have defined the tangent space $T_p X$ as a d-dimensional subspace of $T_p P$. There is precisely one d-dimensional linear subspace $\hat{T}(X,p)$ of P which contains p and has the same tangent space at p as X. In terms of a standard affine chart: if $U \subset P$ is the complement of a hyperplane which does not pass through p, then U has the structure of an affine space and $\hat{T}(X,p) \cap U$ is then the affine subspace of U spanned by $T_p X$.

PROPOSITION-DEFINITION 8.11. *The map $G : X \to \mathrm{Gr}_d(P)$, $p \in X \mapsto \hat{T}(X,p)$ is a morphism. This morphism is called the* Gauss map.

[1] For instance, every cubic surface in $\mathbb{P}^3$ (so here $n = 3$, $d = 3$ and $m = 1$) contains a line. If it is nonsingular, then it contains in fact exactly 27 lines. This famous result due to Cayley and Salmon published in 1849 is still subject of research.

PROOF. Let $p_0 \in X$. The tangent space $\hat{T}(X, p_0)$ defines a linear subspace $L \subset V$ of dimension $d+1$. This linear subspace contains the line ℓ_{p_0} defined by p_o. Choose homogeneous coordinates $Z_0, \dots, Z_n$ on P such that p_0 lies in the standard open subset $U_0 \subset P$ defined by $Z_0 \neq 0$. We use the standard coordinates $z_i := Z_i/Z_0$ to parametrize $U_0 \subset P$, but this time we find it convenient to include z_0, which is of course constant 1 on U_0. In this way U_0 is identified with the affine hyperplane $H_1 \subset V$ defined by $z_0 = 1$. The tangent space T_pU_0 ($p \in U_0$) is then just $p+H$, where $H \subset V$ is defined by $z_0 = 0$. In particular, if $p \in X \cap U_0$, then T_pX can be regarded as a linear subspace $K(p) \subset H_0$ of dimension d displaced over p. The span of p and $K(p)$ is then a linear subspace of V which corresponds to $\hat{T}(X, p)$.

According to Theorem 9.12 there exists a neighborhood U of p_0 in U_0, regular functions $f_1, \dots, f_{n-d}$ on U such that $X \cap U$ is their common zero set and $df_1, \dots, df_{n-d}$ are linearly independent on all of U. Then for every $p \in X \cap U$, $K(p)$ is the common zero set of $df_1(p), \dots, df_{n-d}(p)$. We regard $(df_1, \dots, df_{n-d})$ as a matrix-valued function on U, denoted $D : U \to \mathrm{Hom}(H_0, k^{n-d})$, so that for $p \in U \cap X$, $K(p)$ is the kernel of $D(p)$. We also assume our coordinates chosen in such a manner that $K(p_0)$ is spanned by $e_1, \dots, e_d$ and then write $H = H' \oplus H''$ with $H' = K(p_0)$ and H'' spanned by $e_{d+1}, \dots, e_n$. We write

$$D = (D', D''), \quad \text{with } D' : U \to \mathrm{Hom}(H', k^{n-d}), \quad D'' : U \to \mathrm{Hom}(H'', k^{n-d}).$$

Since $D''(p_0)$ is an isomorphism, the set of $p \in U$ for which $D''(p)$ is an isomorphism defines an open neighborhood of p_0 and so we may as well assume that that this is the case on all of U. Cramer's rule shows that $p \in U \mapsto D''(p)^{-1} \in \mathrm{Hom}(k^{n-d}, H'')$ has regular entries: it is a morphism. For every $p \in U$, the kernel of $D(p)$ is the graph of the linear map $B(p) := -D''(p)^{-1}D'(p) \in \mathrm{Hom}(H', H'')$. In particular, for $p \in X \cap U$, T_pX is parallel to the subspace spanned by $e_1 + B(p)(e_1), \dots, e_d + B(p)(e_d)$.

It follows that a linear subspace of V which corresponds to $\hat{T}(X, p)$ is spanned by $p = e_0 + \sum_{i=1}^n p_i e_i$ and the d vectors $e_1 + B(p)(e_1), \dots, e_d + B(p)(e_d)$. This is the graph of the linear map $A(p) : ke_0 \oplus H' \to k^{n-d}$ defined by

$$A(p)(e_0) := -\sum_{i=1}^{d} z_i(p)B(p)(e_i) + \sum_{j=d+1}^{n} p_j e_j, \quad A(p)(e_i) := B(p)(e_i)\ (i = 1, \dots d).$$

Since A is a morphism, this defines a morphism $X \cap U \to \mathrm{Gr}_d(P)$. □

For a closed irreducible subset $X \subset P$, the Gauss map is defined on its nonsingular part: $G : X_{\mathrm{reg}} \to \mathrm{Gr}_d(P)$. The closure of the graph of G in $X \times \mathrm{Gr}_d(P)$ is called the *Nash blowup* of X and denoted $\hat{X}$. The projection morphism $\hat{X} \to X$ is an isomorphism over the open-dense subset X_{reg} and hence birational. A remarkable property of $\hat{X}$ is that the Zariski tangent space of each point contains a distinguished d-dimensional subspace (prescribed by the second projection to $\mathrm{Gr}_d(P)$) in such a manner that these subspaces extend the tangent bundle in a regular manner.

9. Multiplicities of modules

Bézout's theorem asserts that two distinct irreducible curves C, C' in $\mathbb{P}^2$ of degrees d and d' intersect in dd' points. Strictly speaking this is only true if C and C' intersect as nicely as possible, but the theorem is true as stated if we count each

point of intersection with an appropriate multiplicity. There is in fact a generalization: the common intersection of n hypersurfaces in $\mathbb{P}^n$ has cardinality the product of the degrees of these hypersurfaces, provided that this intersection is as nice as possible and again, this is even true more generally when the locus of intersection is finite and each point of intersection is counted with an appropriate multiplicity. One of our aims is to define these multiplicities. The commutative algebra tools that we use for this have an interest in their own right.

DEFINITION 9.1. We say that an R-module *has length* $\geq d$ if there exist a d-step filtration by submodules $M = M^0 \supsetneq M^1 \supsetneq \cdots \supsetneq M^d = \{0\}$. The *length* of M is the supremum of such d (and so may be ∞).

EXERCISE 72. Suppose R is a noetherian local ring with maximal ideal $\mathfrak{m}$ and residue field K. Prove that the length of a finitely generated R-module M is finite precisely when $\mathfrak{m}^d M = 0$ for some d and is then equal to $\sum_{i=0}^{d-1} \dim_K(\mathfrak{m}^i M/\mathfrak{m}^{i+1}M)$.

Prove that if R is a K-algebra, then this is also equal to $\dim_K(M)$.

We fix a noetherian ring R and a finitely generated R-module M.

Recall that if $\mathfrak{p}$ is a prime ideal of R, then $R_\mathfrak{p}$ is a local ring with maximal ideal $\mathfrak{p}R_\mathfrak{p}$ whose residue field can be identified with the field of fractions of $R/\mathfrak{p}$. We define $M_\mathfrak{p} := R_\mathfrak{p} \otimes_R M$. So this is a $R_\mathfrak{p}$-module.

REMARK 9.2. We can describe $M_\mathfrak{p}$ and more generally, any localization $S^{-1}R \otimes_R M$, as follows. Consider the set $S^{-1}M$ of expressions m/s with $m \in M$ and $s \in S$ with the understanding that $m/s = m'/s'$ if the identity $s''s'm = s''sm$ holds in M for some $s'' \in S$ (so we are considering the quotient of $S \times M$ by an equivalence relation). Then the following rules put on $S^{-1}M$ the structure of a R-module:

$$m/s - m'/s' := (s'm - sm')/(ss'), \quad r \cdot m/s := rm/s.$$

The map $S^{-1}R \times M \to S^{-1}M$, $(r/s, m) \to (rm)/s$ is R-bilinear and hence factors through an R-homomorphism $S^{-1}R \otimes_R M \to S^{-1}M$. On the other hand, the map $S^{-1}M \to S^{-1}R \otimes_R M$, $m/s \mapsto 1/s \otimes_R m$ is also defined: if $m/s = m'/s'$, then $s''(s'm = sm)$ for some $s'' \in S$ and so

$$1/s \otimes_R m = 1/(ss's'') \otimes_R s's''m = 1/(ss's'') \otimes_R ss''m = 1/s' \otimes_R m.$$

It is an R-homomorphism and it immediately verified that it is a two-sided inverse of the map above. So $S^{-1}R \otimes_R M \to S^{-1}M$ is an isomorphism.

This description shows in particular that if $N \subset M$ is a submodule, then $S^{-1}N$ may be regarded as submodule of $S^{-1}M$ (this amounts to: S-localization is an exact functor).

DEFINITION 9.3. The *multiplicity* of M at a prime ideal $\mathfrak{p}$ of R, denoted $\mu_\mathfrak{p}(M)$, is the length of $M_\mathfrak{p}$ as an $R_\mathfrak{p}$-module. (For $x \in \mathrm{Spec}(R)$, we may also write $\mu_x(M)$ instead of $\mu_{\mathfrak{p}_x}(M)$.)

REMARK 9.4. Let X be a variety, $x \in X$ a closed point of X and $\mathcal{I} \subset \mathcal{O}_{X,x}$ an ideal with $\sqrt{\mathcal{I}} = \mathfrak{m}_{X,x}$. So $\mathcal{I} \supset \mathfrak{m}_{X,x}^r$ for some positive integer r. Then $\dim_k(\mathcal{O}_{X,x}/\mathcal{I})$ is finite (since $\dim_k(\mathcal{O}_{X,x}/\mathfrak{m}_{X,x}^r)$ is) and according to Exercise 72 equal to the length of $\mathcal{O}_{X,x}/\mathcal{I}$ of as an $\mathcal{O}_{X,x}$-module. Hence it is the multiplicity of $\mathcal{O}_{X,x}/\mathcal{I}$ at the prime ideal $\mathfrak{m}_{X,x}$: $\mu_x(\mathcal{O}_{X,x}/\mathcal{I}) = \dim_k(\mathcal{O}_{X,x}/\mathcal{I})$. If X is affine and we are given an ideal $I \subset A(X)$ whose image in $\mathcal{O}_{X,x}$ is $\mathcal{I}$, then $\mathcal{O}_{X,x}/\mathcal{I}$ is the localization of $A(X)/I$ at x and x is an isolated point of $Z(I)$. Then still $\mu_x(A(U)/I) = \dim_k(\mathcal{O}_{X,x}/\mathcal{I})$.

If X is nonsingular at x of dimension n and I has exactly n generators $f_1, \dots, f_n$, then we will see that $\mu_p(\mathcal{O}_{X,x}/(f_1, \dots, f_n)) = \dim_k(\mathcal{O}_{\mathbb{A}^n,p}/(f_1, \dots, f_n))$ can be interpreted as the multiplicity of p as a common zero of $f_1, \dots, f_n$.

We wish to discuss the graded case parallel to the ungraded case. This means that if R is graded: $R = \oplus_{i=0}^{\infty} R_i$, then we assume M to be graded as well, that is, M is endowed with a decomposition as an abelian group $M = \oplus_{i\in\mathbb{Z}} M_i$ such that R_j sends M_i to M_{i+j} (we do not assume that $M_i = 0$ for $i < 0$). For example, a homogeneous ideal in R is a graded R-module. In that case we have the notion of *graded length* of M, which is the same as the definition above, except that we only allow chains of *graded* submodules.

The *annihilator* of an R-module M, $\mathrm{Ann}(M)$, is the set of $r \in R$ with $rM = 0$. It is clearly an ideal of R. We denote by $\mathcal{P}(M)$ the set of prime ideals of R which contain $\mathrm{Ann}(M)$ and are minimal for that property. According to Exercise 15 these are finite in number and their common intersection equals $\sqrt{\mathrm{Ann}(M)}$. In the graded setting, $\mathrm{Ann}(M)$ is a graded ideal and then according to Lemma 2.3 the members of $\mathcal{P}(M)$ are all graded.

We further note that the annihilator of any $m \in M$, $\mathrm{Ann}(m) := \{r \in R : rm \neq 0\}$ is an ideal of R, which is graded when m is homogeneous.

LEMMA 9.5. *Let M be a finitely generated and nonzero (graded) R-module. Then the collection of annihilators of nonzero (homogeneous) elements of M contains a maximal element and any such maximal element is a (graded) prime ideal of R.*

PROOF. We only do the graded case. The first assertion follows from the noetherian property of R. Let now $\mathrm{Ann}(m)$ be a maximal element of the collection (so with $m \in M$ homogeneous and nonzero). It suffices to show that this is a prime ideal in the graded sense (see Exercise 58), i.e., to show that if $a, b \in R$ are homogeneous and $ab \in \mathrm{Ann}(m)$, but $b \notin \mathrm{Ann}(m)$, then $a \in \mathrm{Ann}(m)$. So $bm \neq 0$ and $a \in \mathrm{Ann}(bm)$. Since $\mathrm{Ann}(bm) \supset \mathrm{Ann}(m)$, the maximality property of the latter implies that this must be an equality: $\mathrm{Ann}(bm) = \mathrm{Ann}(m)$, and so $a \in \mathrm{Ann}(m)$. □

If l is an integer and M is graded, then $M[l]$ denotes the same module M, but with its grading shifted over l, meaning that $M[l]_i := M_{l+i}$.

Let us call a (graded) R-module *elementary* if it is isomorphic to $R/\mathfrak{p}$ ($(R/\mathfrak{p})[l]$), where $\mathfrak{p}$ is a (homogeneous) prime ideal (and $l \in \mathbb{Z}$). So the above lemma says that every nonzero (graded) R-module contains an elementary submodule.

PROPOSITION 9.6. *Every finitely generated (graded) R-module M can be obtained as a successive extension of elementary modules in the sense that there exists a finite filtration by (graded) R-submodules $M = M^0 \supsetneq M^1 \supsetneq \cdots \supsetneq M^d = \{0\}$ such that each quotient M^i/M^{i+1} is elementary.*

PROOF. We do the graded case only. Since M is noetherian, the collection of graded submodules of M that can be written as a successive extension of elementary modules has a maximal member, M', say. We claim that $M' = M$. If M/M' were nonzero, then according to Lemma 9.5, it contains an elementary submodule. But then the preimage N of this submodule in M is a successive extension of an extension of elementary modules which strictly contains M'. This contradicts the maximality of M. □

PROPOSITION 9.7. *In the situation of the preceding proposition, let $\mathfrak{p}^i$ be the prime ideal of R such that $M^{i-1}/M^i \cong R/\mathfrak{p}^i$. Then $\mathcal{P}(M)$ is the set of minimal members of the collection $\{\mathfrak{p}^i\}_{i=1}^d$ and every $\mathfrak{p} \in \mathcal{P}(M)$ occurs precisely $\mu_{\mathfrak{p}}(M)$ times in the sequence $(\mathfrak{p}^1, \dots, \mathfrak{p}^d)$.*

PROOF. We first show that $\sqrt{\mathrm{Ann}(M)} = \mathfrak{p}^1 \cap \cdots \cap \mathfrak{p}^d$. If $r \in \mathfrak{p}^1 \cap \cdots \cap \mathfrak{p}^d$, then r maps M^{i-1} to M^i and so $r^d \in \mathrm{Ann}(M)$. This proves that $\mathfrak{p}^1 \cap \cdots \cap \mathfrak{p}^d \subset \sqrt{\mathrm{Ann}(M)}$. Conversely, if $r \in R$ and $l \geq 1$ are such that $r^l \in \mathrm{Ann}(M)$, then $r^l \in \mathfrak{p}^i$ for all i. This implies that $r \in \mathfrak{p}^i$ for all i.

So the collection of minimal members of $\{\mathfrak{p}^i\}_{i=1}^d$ is just the set $\mathcal{P}(M)$ of minimal prime ideals containing $\mathrm{Ann}(M)$. In particular, no $\mathfrak{p}^i$ can be strictly contained in a member of $\mathcal{P}(M)$.

Fix $\mathfrak{p} \in \mathcal{P}(M)$. We then have a filtration $M_{\mathfrak{p}} = M^0_{\mathfrak{p}} \supset \cdots \supset M^d_{\mathfrak{p}} = \{0\}$ (for an inclusion of R-modules induces an inclusion of $R_{\mathfrak{p}}$-modules). We have $M^{i-1}_{\mathfrak{p}}/M^i_{\mathfrak{p}} \cong R_{\mathfrak{p}}/\mathfrak{p}^i R_{\mathfrak{p}}$ and the latter is the residue field $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ or trivial according to whether or not $\mathfrak{p}^i = \mathfrak{p}$ (if $\mathfrak{p}^i \neq \mathfrak{p}$, then $\mathfrak{p}^i$ contains an element not in $\mathfrak{p}$; this gives in $R_{\mathfrak{p}}$ an invertible element, and hence $\mathfrak{p}^i R_{\mathfrak{p}} = R_{\mathfrak{p}}$). Following our definition the first case occurs precisely $\mu_{\mathfrak{p}}(M)$ times. □

We can of course pass from the graded case to the nongraded case by just forgetting the grading. But more interesting and useful is the following construction, where we pass from a projective setting to an affine one and vice versa. The example to keep in mind is when we associate to a homogeneous polynomial of degree d, $F \in k[X_0, \dots, X_n]$ the inhomogeneous polynomial $f \in k[x_1, \dots, x_n]$ of degree $\leq d$ by $f(x_1, \dots, x_n) := F(1, x_1, \dots, x_n)$ and go back via $F(X_0, \dots, X_n) := X_0^d f(X_1/X_0, \dots, X_n/X_0)$.

Let $\mathfrak{p} \subset R$ be a graded prime ideal. Then denote by $R_{\mathfrak{p},0}$ the set of fractions r/s with $r \in R_i$ and $s \in R_i - \mathfrak{p}_i$ for some i. This is clearly a subring of $R_{\mathfrak{p}}$; it is in fact a local ring whose maximal ideal $\mathfrak{m}_{\mathfrak{p}}$ is obtained by taking in the previous sentence $r \in \mathfrak{p}_i$. For instance, if $R = k[X_0, \dots, X_n]$ and $\mathfrak{p} = (X_1, \dots, X_n)$, then $\mathfrak{p}$ defines the point $p = [1 : 0 : \cdots : 0] \in \mathbb{P}^n$ and $R_{\mathfrak{p}}$ can be identified with $\mathcal{O}_{\mathbb{P}^n,p}$. This definition makes also sense for any graded R-module M: $M_{\mathfrak{p},0}$ is the set of fractions m/s with $m \in M_i$ and $s \in R_i - \mathfrak{p}_i$ for some i. Note that this is a $R_{\mathfrak{p},0}$-module.

Suppose now that $\mathfrak{p}_1 \neq R_1$ and choose $s_1 \in R_1 - \mathfrak{p}_1$ so that $s_1^{-1} \in (R_{\mathfrak{p}})_{-1}$. Then $R[l]_{\mathfrak{p},0}$ is the the set of fractions r/s with $r \in R_{i+l}$ and $s \in R_i - \mathfrak{p}_i$ for some i. For such a fraction we have $r/s = s_1^l r/(s_1^l s) \in s_1^l R_{\mathfrak{p},0}$, so that $R[l]_{\mathfrak{p},0} = s_1^l R_{\mathfrak{p},0}$, which as an $R_{\mathfrak{p},0}$-module is of course isomorphic to $R_{\mathfrak{p},0}$. So the graded iterated extension $M = M^0 \supsetneq M^1 \supsetneq \cdots \supsetneq M^d = \{0\}$ of M by elementary R-modules yields an iterated extension of $M_{\mathfrak{p},0}$ by trivial or by elementary $R_{\mathfrak{p},0}$-modules: $M_{\mathfrak{p},0} = M^0_{\mathfrak{p},0} \supset M^1_{\mathfrak{p},0} \supset \cdots \supset M^d_{\mathfrak{p},0} = \{0\}$ and the number of times a nonzero successive quotient appears is $\mu_{\mathfrak{p}}(M)$. In other words, we have $\mu_{\mathfrak{p}}(M) = \mu_{\mathfrak{m}_{\mathfrak{p}}}(M_{\mathfrak{p},0})$. We use this observation mainly via the following example.

EXAMPLE 9.8. Let $J \subset k[X_0, \dots, X_n]$ be a homogeneous ideal and let $p \in \mathbb{P}^n$ be a closed isolated point of Z_J. We take here $M := k[X_0, \dots, X_n]/J$ and take for $\mathfrak{p}$ the graded ideal $I_p \subset k[X_0, \dots, X_n]$ defining p. Then $k[X_0, \dots, X_n]_{I_p,0}$ can be identified with the local k-algebra $\mathcal{O}_{\mathbb{P}^n,p}$. Moreover, J defines an ideal $\mathfrak{J} \subset \mathcal{O}_{\mathbb{P}^n,p}$ and we can identify $M_{I_p,0}$ with $\mathcal{O}_{\mathbb{P}^n,p}/\mathfrak{J}$. Notice that $\sqrt{\mathfrak{J}} = \mathfrak{m}_{\mathbb{P}^n,p}$. According to the above discussion $\mu_I(M) = \mu_p(\mathcal{O}_{\mathbb{P}^n,p}/\mathfrak{J})$ and by Exercise 72 this is just $\dim_k(\mathcal{O}_{\mathbb{P}^n,p}/\mathfrak{J})$.

10. Hilbert functions and Hilbert polynomials

We shall be dealing with polynomials in $\mathbb{Q}[z]$ which take integral values on integers. Such polynomials are called *numerical*. An example is the *binomial function* of degree $n \geq 0$:

$$\binom{z}{n} := \frac{z(z-1)(z-2)\cdots(z-n+1)}{n!}.$$

It has the property that its value in *any* integer k is an integer, namely $\binom{k}{n}$ if $k \geq n$, 0 if $0 \leq k \leq n-1$ and $(-1)^n\binom{-k+n-1}{n}$ if $k \leq -1$.

Let $\Delta : \mathbb{Q}[z] \to \mathbb{Q}[z]$ denote the difference operator: $\Delta(f)(z) := f(z+1) - f(z)$. It clearly sends numerical polynomials to numerical polynomials. It is also clear that the kernel of Δ consists of the constants $\mathbb{Q}$. Notice that $\Delta\binom{z}{n+1} = \binom{z}{n}$.

LEMMA 10.1. *Every $P \in \mathbb{Q}[z]$ which takes integral values on sufficiently large integers is numerical and a $\mathbb{Z}$-basis of the abelian group of numerical polynomials is provided by the binomial functions.*

If $f : \mathbb{Z} \to \mathbb{Z}$ is a function such that for sufficiently large integers $\Delta(f)$ is given by a polynomial, then so is f.

PROOF. The first assertion is proved with induction on the degree d of P. If $d = 0$, then P is constant and the assertion is obvious. Suppose $d > 0$ and the assertion known for lower values of d. So $\Delta(P)(z) = \sum_{i=0}^{d-1} c_i\binom{z}{i}$ for certain $c_i \in \mathbb{Z}$. Then $P(z) - \sum_{i=0}^{d-1} c_i\binom{z}{i+1}$ is in the kernel of Δ and hence is constant. As this expression takes integral values on large integers, this constant is an integer. This proves that P is an integral linear combination of binomial functions.

For the second assertion, let $P \in \mathbb{Q}[z]$ be such that $P(i) = \Delta(f)(i) \in \mathbb{Z}$ for large i. By the preceding, $P(z) = \sum_i a_i\binom{z}{i}$ for certain $a_i \in \mathbb{Z}$. So if we put $Q(z) := \sum_i a_i\binom{z}{i+1}$, then Q is a numerical polynomial with $\Delta(f-Q)(i) = 0$ for large i. This implies that $f - Q$ is constant for large i, say equal to $a \in \mathbb{Z}$. So $f(i) = Q(i) + a$ for large i and hence $Q + a$ is as required. □

We shall see that examples of such functions are provided by the Hilbert functions of graded noetherian modules.

REMARK 10.2. A function $f : \mathbb{Z} \to \mathbb{Z}$ which is zero for sufficiently negative integers determines a Laurent series $L_f := \sum_{k\in\mathbb{Z}} f(k)u^k \in \mathbb{Z}((u))$. For the function $k \mapsto \max\{0, \binom{k}{n}\}$ this gives

$$\sum_{k\geq n} \frac{k(k-1)\cdots(k-n+1)}{n!}u^k = \frac{u^n}{n!}\frac{d^n}{du^n}\sum_{k\geq 0} u^k = \frac{u^n}{n!}\frac{d^n}{du^n}\frac{1}{1-u} = \frac{u^n}{n!(1-u)^n}.$$

So if we also know that for sufficiently large integers f is the restriction of a polynomial function, then Lemma 10.1 implies that L_f is a $\mathbb{Z}$-linear combination of powers of u and the rational functions $\frac{u^n}{n!(1-u)^n}$. In particular, $P_f \in \mathbb{Q}[u][u^{-1}, (1-u)^{-1}]$.

In the rest of this section R stands for the graded ring $k[X_0, \ldots, X_n]$ where each X_i has degree one. An R-module is always assumed to be graded and finitely generated.

Let M be a graded noetherian R-module. We define the *Hilbert function of M*, $\phi_M : \mathbb{Z} \to \mathbb{Z}$, by $\phi_M(i) := \dim_k M_i$.

EXAMPLE 10.3. The Hilbert function of R is given by $\phi_R(i) = \binom{i+n}{n}$.

LEMMA 10.4. *Let $F \in R_d$ and denote by $\mathrm{Ann}(F, M) \subset M$ the set of $m \in M$ with $Fm = 0$ (this is a graded submodule of M). Then we have $\phi_{M/FM}(i) = \phi_M(i) - \phi_M(i-d) + \phi_{\mathrm{Ann}(F,M)}(i-d)$.*

PROOF. In degree i, multiplication by F defines a k-linear map between finite dimensional k-vector spaces $M_{i-d} \to M_i$ whose kernel is $\mathrm{Ann}(F, M)_{i-d}$ and whose cokernel is $(M/FM)_i$. The lemma easily follows from this. □

The zero set of the graded ideal $\mathrm{Ann}(M)$ in $\mathbb{P}^n$ will be called the *support* of M and denoted $\mathrm{supp}(M)$.

THEOREM 10.5 (Hilbert-Serre). *Let M be a finitely generated graded module over the graded ring $R = k[X_0, \dots, X_n]$ (where each X_i has degree 1). Then there exists a unique numerical polynomial $P_M \in \mathbb{Q}[z]$, the* Hilbert polynomial of M, *such that $\phi_M(i) = P_M(i)$ for i sufficiently large. The degree of P_M is equal to $\dim(\mathrm{supp}(M))$ if we agree that the zero polynomial has the same degree as the dimension of the empty set (namely -1).*

PROOF. We proceed with induction on $n \geq -1$. For $n = -1$, M is a finite dimensional graded k-vector space and hence $M_i = 0$ for i sufficiently large. So assume $n \geq 0$ and the theorem verified for lower values of n. We first reduce to the case when M is of the form $R/\mathfrak{p}$, with $\mathfrak{p}$ a graded prime ideal. If N is a graded submodule of M, then $\mathrm{Ann}(M) = \mathrm{Ann}(N) \cap \mathrm{Ann}(M/N)$ and so $\mathrm{supp}(M) = \mathrm{supp}(N) \cup \mathrm{supp}(M/N)$. Since $\dim_k(M_i) = \dim_k N_i + \dim_k(M_i/N_i)$, we have $\phi_M = \phi_N + \phi_{M/N}$. It follows that if the theorem holds for N and M/N, then it holds for M. As M is a successive extension of elementary modules, it suffices to do the case $M = (R/\mathfrak{p})[l]$ with $\mathfrak{p}$ a graded prime ideal. Since $\phi_M(i) = \phi_{R/\mathfrak{p}}(l+i)$, it is enough to do the case $M = R/\mathfrak{p}$.

So let $M = R/\mathfrak{p}$. Then $\mathrm{supp}(M) = \mathrm{supp}(R/\mathfrak{p})$ is defined by the graded ideal $\mathfrak{p}$. In case $\mathfrak{p} = (X_0, \dots, X_n)$, the theorem holds trivially: we have $\dim_k M_i = 0$ for $i > 0$ (so that we may take P_M to be identically zero) and $\mathrm{supp}(M) = \emptyset$. Suppose therefore that $\mathfrak{p} \neq (X_0, \dots, X_n)$, say that $X_n \notin \mathfrak{p}$. Now multiplication by X_n sends M isomorphically onto $X_n M$ with quotient $\bar{M} := M/X_n M$ and so for $i \geq 0$, $\phi_{\bar{M}}(i) = \phi_M(i) - \phi_M(i-1) = \Delta\phi_M(i-1)$. Since $\mathrm{Ann}(\bar{M}) = \mathrm{Ann}(M) + X_n R$, we have $\mathrm{supp}(\bar{M}) = \mathrm{supp}(M) \cap \mathbb{P}^{n-1}$. According to Proposition 7.2 we then have $\dim \mathrm{supp}(\bar{M}) = \dim \mathrm{supp}(M) - 1$. By regarding $\bar{M}$ as a finitely generated module over $\bar{R} := k[X_0, \cdots, X_{n-1}]$, our induction hypothesis tells us that there exists a polynomial $P_{\bar{M}}$ of degree $\dim \mathrm{supp}(\bar{M})$ such that $\phi_{\bar{M}}$ and $P_{\bar{M}}$ coincide on large integers. Since $\Delta\phi_M(i-1) = P_{\bar{M}}(i)$ for large i, Lemma 10.1 implies that there exists a polynomial P_M of degree one higher than that of $P_{\bar{M}}$ (so of degree $\dim(\mathrm{supp}(M))$) which coincides with ϕ_M for sufficiently large integers. □

It follows from Lemma 10.1 that when P_M is nonzero, then its leading term has the form $c_d z^d/d!$, where d is the dimension of $\mathrm{supp}(M)$ and c_d is a positive integer.

REMARK 10.6. For M as in this theorem we may also form the Laurent series $L_M(u) := \sum_i \dim(M_i) u^i$ (this is usually called the the *Poincaré series* of M). It follows from Remark 10.2 and Theorem 10.5 that $L_M(u) \in \mathbb{Q}[u][u^{-1}, (1-u)^{-1}]$.

DEFINITION 10.7. If $d = \dim \mathrm{supp}(M)$, then the *degree* $\deg(M)$ is $d!$ times the leading coefficient of its Hilbert polynomial (an integer, which we stipulate to be zero in case $\mathrm{supp}(M) = \emptyset$). For a closed subset $Y \subset \mathbb{P}^n$, the Hilbert polynomial P_Y resp. the *degree* $\deg(Y)$ of Y are those of R/I_Y as a R-module.

Let M be a finitely generated graded R-module. Recall that $\mathcal{P}(M)$ denotes the set of minimal prime ideals containing $\mathrm{Ann}(M)$. The support of M is defined by the ideal $\mathrm{Ann}(M)$ and is graded. So it defines a closed subset in $\mathbb{P}^n$ which in our previous notation is just $Z_{\mathrm{Ann}(M)}$. For every $\mathfrak{p} \in \mathcal{P}(M)$ not equal to $(X_0, \ldots, X_n)$, $Z_{\mathfrak{p}} \subset \mathbb{P}^n$ is an irreducible component of $Z_{\mathrm{Ann}(M)}$ whose degree is $\deg(R/\mathfrak{p})$ and all irreducible components of $Z_{\mathrm{Ann}(M)}$ are so obtained (for $\mathfrak{p} = (X_0, \ldots, X_n)$ we get $Z_{\mathfrak{p}} = \emptyset$, but $\deg(R/(X_0, \ldots, X_n) = 0$).

PROPOSITION 10.8. *Let M be a finitely generated graded R-module. Then*

$$\deg(M) = \sum_{\mathfrak{p} \in \mathcal{P}(M)} \mu_{\mathfrak{p}}(M) \deg(R/\mathfrak{p}),$$

where we note that the right hand side can also be written as a sum over the irreducible components of $Z_{\mathrm{Ann}(M)}$ of maximal dimension, where we then may replace $\deg(R/\mathfrak{p})$ by the degree of that component.

PROOF. Write M as an iterated extension by elementary modules: $M = M^0 \supsetneq M^1 \supsetneq \cdots \supsetneq M^d = \{0\}$ with $M^{i-1}/M^i \cong R/\mathfrak{p}_i[l_i]$. Then $\phi_M(i) = \sum_{i=1}^d \phi_{R/\mathfrak{p}_i}(i - l_i)$. Now $\phi_{R/\mathfrak{p}_i}$ is a polynomial of degree equal to the dimension of $\mathrm{supp}(R/\mathfrak{p}_i) = Z_{\mathfrak{p}_i} \subset \mathbb{P}^n$. This degree does not change if we replace the variable i by $i - l_i$. In view of Proposition 9.7 we only get a contribution to the leading coefficient of ϕ_M when $\mathfrak{p}_i \in \mathcal{P}(M)$ and for any given $\mathfrak{p} \in \mathcal{P}(M)$ this happens exactly $\mu_{\mathfrak{p}}(M_{\mathfrak{p}})$ times. We only need to consider the cases $\mathfrak{p}$ for which the degree of $\phi_{R/\mathfrak{p}}$ is maximal (i.e., equals the degree of ϕ_M). The proposition follows. □

EXERCISE 73. Compute the Hilbert polynomial and the degree of

(a) the image of the d-fold Veronese embedding of $\mathbb{P}^n$ in $\mathbb{P}^{\binom{n+d}{n}-1}$,
(b) the image of the Segre embedding of $\mathbb{P}^m \times \mathbb{P}^n$ in $\mathbb{P}^{mn+m+n}$.

EXERCISE 74. Let $Y \subset \mathbb{P}^m$ and $Z \subset \mathbb{P}^n$ be closed and consider $Y \times Z$ as a closed subset of $\mathbb{P}^{mn+m+n}$ via the Segre embedding. Prove that the Hilbert function resp. polynomial of $Y \times Z$ is the product of the Hilbert functions resp. polynomials of the factors.

One can show that there exists a nonempty open subset of $(n-d)$-planes $Q \subset \mathbb{P}^n$ which meet Y in exactly $\deg(Y)$ points (see Exercise 75). This characterization is in fact the classical way of defining the degree of Y.

Observe that if $Y \subset \mathbb{P}^n$ is nonempty, then $\deg(Y) > 0$. For then $I_{Y,d} \neq R_d$ for every $d \geq 0$ and so the Hilbert function of $S(Y)$ is positive on all nonnegative integers. This implies that P_Y is nonzero with positive leading coefficient.

We also note that since $\deg(Y)$ only depends on the dimensions of the graded pieces $S(Y)_i$ of the homogenenous coordinate ring the degree of Y will not change if we regard Y as sitting in a higher dimensional projective space $Y \subset \mathbb{P}^n \subset \mathbb{P}^m$ (with $m \geq n$).

We verify some other properties we expect from a notion of degree.

PROPOSITION 10.9. *A hypersurface $H \subset \mathbb{P}^n$ defined by an irreducible polynomial of degree d has degree d.*

PROOF. Let $F \in R_d$ be the polynomial in question and apply Lemma 10.4 to $M = R$. Since the Hilbert function of R takes at the positive integer i the value

$\binom{n+i}{n}$, the one of H takes at i the value $\binom{n+i}{n} - \binom{n+i-d}{n}$. Its Hilbert polynomial is therefore

$$\binom{z+n}{n} - \binom{z-d+n}{n} = \frac{d}{(n-1)!} z^{n-1} + \text{ lower order terms},$$

and so $\deg(H) = d$. □

PROPOSITION 10.10. *Let $Y_1, \ldots, Y_r$ be the distinct irreducible components of Y of maximal dimension ($= \dim Y$). Then $\deg(Y) = \sum_{i=1}^{r} \deg(Y_i)$.*

PROOF. Put $Y' := Y_2 \cup \cdots \cup Y_r$. By proceeding with induction on r, we see that it is enough to show that $\deg(Y)$ equals $\deg(Y_1) + \deg(Y')$ or $\deg(Y_1)$ depending on whether $r \geq 2$ or $r = 1$. Since $I_Y = I_{Y_1} \cap I_{Y'}$, we have an exact sequence of graded R-modules

$$0 \to S(Y) \to S(Y_1) \oplus S(Y') \to M \to 0,$$

where $M := R/(I_{Y_1} + I_{Y'})$. This implies that $P_Y = P_{Y_1} + P_{Y'} - P_M$. We have $\operatorname{supp}(M) = Y_1 \cap Y'$ and so $\dim \operatorname{supp}(M) < \dim Y$. Hence $\deg(P_M) < \dim(Y)$. The assertion then follows from comparing the coefficients of $z^{\dim Y}$. □

We can now state and prove a theorem of Bézout type.

COROLLARY 10.11. *Let M be a graded R-module. Let $F \in R_d \setminus \operatorname{Ann}(M)$. Then M/FM has degree $d \deg(M)$ as a R-module and if we put $m := \dim(Z_{\operatorname{Ann}(M)})$, then*

$$\sum_{Z \text{ irred. comp of } Z_{\operatorname{Ann}(M/FM)} \text{ of dim. } m-1} \mu_Z(M/FM) \deg(Z) = d \deg(M).$$

PROOF. The exact sequence

$$0 \to M[-d] \xrightarrow{\cdot F} M \to M/FM \to 0$$

shows that $P_{M/FM}(z) = P_M(z) - P_M(z-d)$. Since P_M is of degree m with leading coefficient $\deg(M)/m!$, it follows that $P_{M/FM}$ is of degree $m-1$ with leading coefficient $d \deg(M)/(m-1)!$. An irreducible component C of $\operatorname{Ann}(M)$ is not contained in Z_F and so $\dim(C \cap Z_F) = \dim(C) - 1$. This produces all the irreducible components of $\operatorname{Ann}(M/FM) = \operatorname{Ann}(M) + FR$. It remains to apply Proposition 10.8 to M/FM. □

COROLLARY 10.12. *Let $Y \subset \mathbb{P}^n$ be closed with all irreducible components of the same dimension m. If $Q \subset \mathbb{P}^n$ is a linear subspace of codimension m with the property that $Q \cap Y$ is finite, then the degree of Y is equal to $\sum_{p \in Y \cap Q} \mu_p(S_\bullet(Y)/I_Q S_\bullet(Y))$.*

PROOF. Let $H_1, \ldots, H_m$ be hyperplanes in $\mathbb{P}^n$ such that $Q = H_1 \cap \cdots \cap H_m$ and put $Y^k := Y \cap H_1 \cap \cdots \cap H_k$ ($k = 0, \ldots m$). We are given that $Y^m = Q \cap Y$ is finite. Since intersecting a subvariety of $\mathbb{P}^n$ with with a hyperplane makes its dimension drop by at most one, we see that each irreducible component of Y^k has dimension $m - k$. If we apply the first part of Corollary 10.11 to a defining linear form for H_k, we find that Y^k has the same degree as Y^{k-1}. □

For $p \in Q \cap Y$, let $\mathcal{I}_{Y,p}$ resp. $\mathcal{I}_{Q,p}$ be the ideal in $\mathcal{O}_{\mathbb{P}^n,p}$ defining Y resp. Q at that point. Then we observed that

$$\mu_p(S_\bullet(Y)/I_Q) = \dim_k \mathcal{O}_{\mathbb{P}^n,p}/(\mathcal{I}_{Y,p} + \mathcal{I}_{Q,p}).$$

EXERCISE 75. Prove that $\deg(Y)$ is the cardinality of $Q \cap Y$ if and only if $\mathcal{I}_{Y,p} + \mathcal{I}_{Q,p} = \mathfrak{m}_{\mathbb{P}^n,p}$ for all $p \in Q \cap Y$. (We then say that Q and Y *are in general position with respect to each other*.)

THEOREM 10.13 (Theorem of Bézout). *Let or $i = 1, \dots n$, $H_i \subset \mathbb{P}^n$ be a hypersurface of degree $d_i > 0$ and assume that $H_1 \cap \cdots \cap H_n$ is finite. Each H_i determines at $p \in H_1 \cap \cdots \cap H_n$ a principal ideal in $\mathcal{O}_{\mathbb{P}^n,p}$; denote by $\mathcal{I}_p \subset \mathcal{O}_{\mathbb{P}^n,p}$ the sum of these ideals. Then*

$$d_1 d_2 \cdots d_n = \sum_{p \in H_1 \cap \cdots \cap H_n} \dim_k(\mathcal{O}_{\mathbb{P}^n,p}/\mathcal{I}_p).$$

PROOF. Put $Z^k := H_1 \cap \cdots \cap H_k$. Since Z^n is finite, all irreducible components of Z^k are of dimension $n-k$ (by the same argument as in Corollary 10.12). Repeated application of Corollary10.11 then yields that $d_1 d_2 \cdots d_n$ is the degree of Z^n. With the help of Exercise 75 we see that this degree is computed as stated. □

EXAMPLE 10.14. Assume $\mathrm{char}(k) \neq 2$. We compute the intersection multiplicities of the conics C and C' in $\mathbb{P}^2$ whose affine equations are $x^2 + y^2 - 2y = 0$ and $x^2 - y = 0$. There are three points of intersection: $(0,0)$, $(-1,1)$ and $(1,1)$ (so none at infinity). The intersection multiplicity at $(0,0)$ is the dimension of $\mathcal{O}_{\mathbb{A}^2,(0,0)}/(x^2+y^2-2y, x^2-y)$ as a k-vector space. But $\mathcal{O}_{\mathbb{A}^2,(0,0)}/(x^2+y^2-2y, x^2-y) = \mathcal{O}_{\mathbb{A}^1,0}/(x^4 - x^2) = k[x]/(x^2)$ (for (x^2-1) is invertible in $\mathcal{O}_{\mathbb{A}^1,0}$). Clearly $\dim_k(k[x]/(x^2)) = 2$ and so this is also the intersection multiplicity at $(0,0)$. The intersection multiplicities at $(-1,1)$ and $(1,1)$ are easily calculated to be 1 and thus the identity $2 + 1 + 1 = 2 \cdot 2$ illustrates the Bézout theorem.

REMARK 10.15. If $Y \subset \mathbb{P}^n$ is closed, then $P_Y(0)$ can be shown to be an invariant of Y in the sense that it is independent of the projective embedding. In many ways, it behaves like an Euler characteristic. (It is in fact the Euler characteristic of $\mathcal{O}_Y$ in a sense that will become clear once we know about sheaf cohomology.) For example, $P_{Y \times Z}(0) = P_Y(0) P_Z(0)$.

We have seen that for a hypersurface $Y \subset \mathbb{P}^n$ of degree $d > 0$, $P_Y(z) = \binom{z+n}{n} - \binom{z-d+n}{n}$ and so $P_Y(0) = 1 - \binom{-d+n}{n} = 1 - (-1)^n \binom{d-1}{n}$. For $n = 2$ (so that Y is a curve), we get $P_Y(0) = 1 - \frac{1}{2}(d-1)(d-2)$. The number $1 - P_Y(0) = \frac{1}{2}(d-1)(d-2)$ is then called the arithmetic genus of the curve. If the curve is smooth and $k = \mathbb{C}$, then we may regard it as a topological surface (a Riemann surface) and g is then just the genus of this surface (and so $P_Y(0)$ is half its Euler characteristic).

CHAPTER 3

Schemes

1. Presheaves and sheaves

The notion of a prevariety as well as its generalizations are best understood in the general context of ringed spaces. This involves the even more basic notion of a sheaf.

DEFINITION 1.1. Let X be a topological space. An *abelian presheaf* $\mathcal{F}$ on X consists of giving for every open subset $U \subset X$ an abelian group $\mathcal{F}(U)$ (whose elements are called *sections of $\mathcal{F}$ over U*) and for every inclusion of open subsets $U \subset U'$ a homomorphism of groups (called the *restriction map*) $\mathcal{F}(U') \to \mathcal{F}(U)$ such that:

(i) for the identity $U = U$ we get the identity in $\mathcal{F}(U)$,
(ii) if $U \subset U' \subset U''$ are open sets, then the homomorphism $\mathcal{F}(U'') \to \mathcal{F}(U)$ is equal to the composite $\mathcal{F}(U'') \to \mathcal{F}(U') \to \mathcal{F}(U)$ and

If you are familiar with the language of categories, then you might observe that a presheaf is nothing but a contravariant functor $\mathcal{F} : \mathfrak{O}(X)^\circ \to \mathfrak{Ab}$ from the category $\mathfrak{O}(X)$ of open subsets of X (whose morphisms are inclusions of open subsets of X) to the category of abelian groups $\mathfrak{Ab}$. The terminology 'section over U' and 'restriction' is suggestive, although it sometimes can be a bit misleading. This terminology is mirrored by the notation: if we are given an inclusion of open subsets $U' \subset U$, then the image of $s \in \mathcal{F}(U)$ under the restriction map $\mathcal{F}(U) \to \mathcal{F}(U')$ is often denoted $s|U'$ (a natural notation for the restriction map would be $\mathcal{F}(U' \subset U)$, but this is rarely used; more common is $\mathrm{res}_{U,U'}$).

In case the groups $\mathcal{F}(U)$ come with the structure of a ring and the restriction maps are ring homomorphisms, then we say that $\mathcal{F}$ is a *presheaf of rings* (in other words, the contravariant functor takes values in the category $\mathfrak{Ring}$ of rings). Likewise, we have the notion of a presheaf of modules over a fixed ring R. In some situations no structure on $\mathcal{F}(U)$ is imposed at all (the target category is then the one of sets), but we will only deal here with presheaves that are at least abelian.

EXAMPLE 1.2 (The constant presheaf). Given an abelian group G and a topological space X, then we have an abelian presheaf defined on X if we take for every nonempty open $U \subset X$ the group G and for each inclusion between two such sets the identity map of G.

EXAMPLE 1.3. Given a topological space X and an abelian topological group G, then assigning to every nonempty open $U \subset X$ the group of continuous maps $U \to G$ (with the obvious restriction maps) is an abelian presheaf $\mathcal{C}_{X,G}$. Of special interest are $G = \mathbb{R}$ and $G = \mathbb{C}$, in which we get a presheaf of $\mathbb{R}$-algebras (resp. of $\mathbb{C}$-algebras). Another case of interest is when G has been given the discrete topology: then this assigns to U the space of locally constant maps $U \to G$.

EXAMPLE 1.4. For a smooth manifold M, we have defined the presheaf $\mathcal{E}_M$ of $\mathbb{R}$-algebras which assigns to every nonempty open $U \subset M$ the $\mathbb{R}$-algebra of differentiable functions $U \to \mathbb{R}$.

EXAMPLE 1.5. On a complex manifold M, we have defined the presheaf $\mathcal{O}_M^{\mathrm{an}}$ of $\mathbb{C}$-algebras which assigns to every nonempty open $U \subset M$ the $\mathbb{C}$-algebra $\mathcal{O}^{\mathrm{an}}(U)$ of holomorphic functions $U \to \mathbb{C}$.

EXAMPLE 1.6. On a k-prevariety X, we have defined the presheaf $\mathcal{O}_X$ of regular functions.

DEFINITION 1.7. Given a presheaf $\mathcal{F}$ on X and a point $p \in X$, then a *germ of a section* of $\mathcal{F}$ at p, is a section of $\mathcal{F}$ on an unspecified neighborhood of p, with the understanding that two such sections represent the same germ if they coincide on a neighborhood of p contained in their common domain of definition. The set of germs of sections of $\mathcal{F}$ at p is called the *stalk* of $\mathcal{F}$ at p and denoted by $\mathcal{F}_p$. (In categorical language, this is expressed as an inductive limit $\mathcal{F}_p = \varinjlim_{U \ni p} \mathcal{F}(U)$, where one observes that the collection of neighborhoods of p in X form a projective system: the intersection of two neighborhoods of p is another one.)

For instance in the case of Example 1.5, when M is an open subset of $\mathbb{C}$, then the stalk $\mathcal{O}_{M,p}^{\mathrm{an}}$ can be identified with the ring of convergent power series in $z - p$.

Let us observe that an $s \in \mathcal{F}(U)$ determines an element $s_p \in \mathcal{F}_p$ for every $p \in U$. We will also write $s^+(p)$ for s_p, where we view s^+ as a map $U \to \prod_{p \in U} \mathcal{F}_p$.

The last three examples differ from the first in that they satisfy two additional properties:

DEFINITION 1.8. An abelian presheaf $\mathcal{F}$ on X is called an abelian *sheaf* if for every open $U \subset X$ and open covering $\{U_i\}_{i \in I}$ of U,

(iv) every system of sections $\{s_i \in \mathcal{F}(U_i)\}_{i \in I}$ that is *compatible* in the sense that for each pair (i, j) in I, $s_i|U_i \cap U_j = s_j|U_i \cap U_j$ comes from some section $s \in \mathcal{F}(U)$ in the sense $s|U_i = s_i$ for all $i \in I$, and

(v) two sections $s, s' \in \mathcal{F}(U)$ coincide if $s|U_i = s'|U_i$ for all $i \in I$.

In other words, the sequence

$$0 \to \mathcal{F}(U) \to \prod_{i \in I} \mathcal{F}(U_i) \to \prod_{(i,j) \in I^2} \mathcal{F}(U_i \cap U_j)$$

in which the first map is given by $s \mapsto (s|U_i)_{i \in I}$ and the second by $(s_i)_{i \in I} \mapsto (s_i|U_i \cap U_j - s_j|U_i \cap U_j)_{i,j}$ is exact. This implies that $\mathcal{F}(\emptyset)$ is the trivial group $\{0\}$. The argument relies on a categorical notion of product[1], but for our purposes we may just as well stipulate that this is so.

A space X endowed with with a sheaf of rings is also called a *ringed space*. Examples are 1.3, 1.4, 1.5 and 1.6. A constant presheaf is usually not a sheaf: if U_1, U_2 are disjoint open subsets and we take $g_i \in \mathcal{F}(U_i) = G$ distinct for $i = 1, 2$,

[1] If we are given a product of abelian groups with index set I, $\prod_{i \in I} G_i$, then for every subset $J \subset I$, this product maps isomorphically to the product $(\prod_{i \in J} G_i) \times (\prod_{i \in I - J} G_i)$. By taking $J = I$, we see that a product with empty index set must be the trivial group. Similarly, every union of sets $\cup_{i \in I} X_i$, can be written as $(\cup_{i \in J} X_i) \cup (\cup_{i \in I - J} X_i)$, from which deduce (by taking $J = I$), that a union with empty index set must be empty. If we then apply the above exact sequence to $U = \emptyset$ by taking an open covering with empty index set, we find that $\mathcal{F}(\emptyset) = \{0\}$.

then clearly these elements cannot be the restriction of a single $g \in \mathcal{F}(U_1 \cup U_2) = G$. There is however a simple modification which is a sheaf, namely the *constant sheaf* G_X which assigns to $U \subset X$ the space of continuous maps from to U to G, where we endow G with the discrete topology (so these are the maps which are locally constant). This turns it into a special case of Example 1.3.

1.9. SHEAFIFICATION. This modification is a special case of a general construction which produces a sheaf $\mathcal{F}^+$ out of a presheaf $\mathcal{F}$ with the same stalks: a section $\tilde{s}$ of $\mathcal{F}^+$ over an open subset U is by definition a map from U to the disjoint union of the stalks $\mathcal{F}_p$, $p \in U$, with the property that locally this map is of the form s^+: we may cover U by open subsets U_i for which there exist $s_i \in \mathcal{F}(U_i)$ such that $\tilde{s}_p = s_{i,p}$ for all $p \in U_i$. It is straightforward to verify that this is well-defined, defines a sheaf and that $\mathcal{F}^+ = \mathcal{F}$ in case $\mathcal{F}$ happens to be a sheaf.

The sheaf $\mathcal{F}^+$ has a universal property. In order to explain this, we need the notion of a homomorphism of presheaves. Let $\mathfrak{C}$ be one of our categories. If $\mathcal{F}$ and $\mathcal{G}$ are $\mathfrak{C}$-valued presheaves on X, then a *homomorphism of presheaves* $\phi : \mathcal{F} \to \mathcal{G}$ is what is called in category theory a natural transformation of functors: for every open $U \subset X$, we are given $\mathfrak{C}$-homomorphism $\phi(U) : \mathcal{F}(U) \to \mathcal{G}(U)$ such that this collection is compatible with restriction: if $U' \subset U$ and $s \in \mathcal{F}(U)$, then $\phi(U)(s)|U' = \phi(U')(s|U')$.

For example, the formation of $\mathcal{F}^+$ defines a homomorphism of presheaves $\mathcal{F} \to \mathcal{F}^+$. It is universal in the sense that if $\phi : \mathcal{F} \to \mathcal{G}$ is a homomorphism of presheaves and $\mathcal{G}$ is a sheaf, then there is unique sheaf homomorphism $\phi^+ : \mathcal{F}^+ \to \mathcal{G}$ such that ϕ is the composite of $\mathcal{F} \to \mathcal{F}^+$ and ϕ^+.

In general a homomorphism of presheaves $\phi : \mathcal{F} \to \mathcal{G}$ induces a sheaf homomorphism $\phi^+ : \mathcal{F}^+ \to \mathcal{G}^+$.

EXERCISE 76 (Local nature of a sheaf). Let X be a topological space and $\mathcal{U}$ a basis of open subsets of X. Prove that an abelian sheaf $\mathcal{F}$ on the space X is determined by its restriction to that basis, that is, by the collection $\mathcal{F}(U)$, and the restriction maps $\mathcal{F}(U') \to \mathcal{F}(U)$, for the pairs $(U, U') \in \mathcal{U} \times \mathcal{U}$ with $U \subset U'$.

Prove also a converse: suppose that the basis $\mathcal{U}$ is closed under finite intersections and assume that for every $U \in \mathcal{U}$ is given an abelian group $\mathcal{F}(U)$ and for every inclusion $U \subset U'$ of members of $\mathcal{U}$ a homomorphism $\mathcal{F}(U') \to \mathcal{F}(U)$ such that the properties (i) through (iii) are satisfied. Then $\mathcal{F}$ generates a sheaf $\mathcal{F}^+$ on X.

EXERCISE 77 (Direct image of a sheaf). Suppose we are given a continuous map $f : X \to Y$ between topological spaces and an abelian presheaf $\mathcal{F}$ on X. Then a presheaf $f_*\mathcal{F}$ on Y is defined by assigning to an open $V \subset Y$ the group $\mathcal{F}(f^{-1}V)$. Prove that if $\mathcal{F}$ is a sheaf, then so is $f_*\mathcal{F}$. Is it true that $(f_*\mathcal{F})^+ = f_*(\mathcal{F}^+)$?

EXAMPLE 1.10. Let $f : S^1 \to S^1$ be defined by $f(z) = z^2$ and let $\mathbb{Z}_{S^1}$ be the constant sheaf on S^1 with stalks $\mathbb{Z}$. Then $f_*\mathbb{Z}_{S^1}$ is a sheaf on S^1 which is locally like the constant sheaf $\mathbb{Z}^2$. But $(f_*\mathbb{Z}_{S^1})(S^1) = \mathbb{Z}_{S^1}(S^1) = \mathbb{Z}$ and so is of rank less than 2. Other examples in the same spirit are gotten as the sheaf on $\mathbb{C} - \{0\}$ that is the direct image of the constant sheaf on $\mathbb{C} - \{0\}$ with stalk $\mathbb{Z}$ under the map $z \in \mathbb{C} - \{0\} \mapsto z^n \in \mathbb{C} - \{0\}$ ($n \in \mathbb{Z} - \{0\}$) or of the direct image of the constant sheaf on $\mathbb{Z}$ with stalk $\mathbb{C}$ under the map $z \in \mathbb{C} \mapsto e^z \in \mathbb{C} - \{0\}$.

1.11. KERNELS AND COKERNELS. We begin with some obvious definitions: given a presheaf $\mathcal{F}$ on X, then a *subpresheaf* of $\mathcal{F}$ is simply a presheaf $\mathcal{F}'$ on X

with the property that $\mathcal{F}'(U) \subset \mathcal{F}(U)$ for every open subset U of X. If $\mathcal{F}'$ happens to be a sheaf, then we call it a *subsheaf of* $\mathcal{F}$.

Suppose and $\mathcal{F}$ and $\mathcal{G}$ are abelian presheaves over X and let $\phi : \mathcal{F} \to \mathcal{G}$ be a homomorphism of presheaves. So for every open $U \subset X$, we then have a homomorphism $\phi(U) : \mathcal{F}(U) \to \mathcal{G}(U)$. By assigning to U, $\mathrm{Ker}(\phi)(U)$, $\mathrm{Im}\,\phi(U)$, $\mathrm{Coker}(\phi(U))$ we have defined three presheaves, of first two being subpresheaves of $\mathcal{F}$ and $\mathcal{G}$ respectively. If $\mathrm{Ker}(\phi)$ is the zero sheaf, then clearly $\mathcal{F}$ can be thought of a subpresheaf of $\mathcal{G}$. Suppose now that $\mathcal{F}$ and $\mathcal{G}$ are in fact sheaves. Then $\mathrm{Ker}(\phi)(U)$ is easily seen to be a sheaf (and indeed denoted by $\mathrm{Ker}(\phi)$). But the other two need not be (see Example 1.12 below) and so we define the image sheaf $\mathrm{Im}(\phi)$ resp. the cokernel sheaf $\mathrm{Coker}(\phi)$ as the sheaf associated to the corresponding presheaves. Since this process does not affect the stalks, we have that for every $x \in X$, $\mathrm{Im}(\phi)_x$ resp. $\mathrm{Coker}(\phi)_x$ is the image resp. the cokernel of $\phi_x : \mathcal{F}_x \to \mathcal{G}_x$. Moreover, $\mathrm{Im}(\phi)_x$ is a subsheaf of $\mathcal{G}$. The possible failure of the image presheaf being a sheaf is expressed by the fact that the image of $\phi(U) : \mathcal{F}(U) \to \mathcal{G}(U)$ is contained in $\mathrm{Im}(\phi)(U)$ but need not equal it and a similar statement can be made for the cokernel sheaf.

We finally note that the homomorphisms from $\mathcal{F}$ to $\mathcal{G}$ form an abelian group; we denote that group by $\mathrm{Hom}(\mathcal{F}, \mathcal{G})$.

If $\mathcal{F}$ is a sheaf on X, then $\mathcal{F}(X)$ is called its *group of global sections*. One often denotes this group by $\Gamma(X, \mathcal{F})$ or $H^0(X, \mathcal{F})$ instead. The reason for the latter notation will become clear later.

An interesting twist to the notion of a constant sheaf is that of a *local system* (and called by some algebraic topologists a *system of twisted coefficients*): this is a locally constant sheaf. For instance, if G is an abelian group, then a *local system of type* G on X is an abelian sheaf $\mathcal{F}$ on X with the property that X can be covered by open subsets U such that $\mathcal{F}|U$ is isomorphic to the sheaf associated to the constant presheaf G on U. Examples were given in 1.10. Here is another one, which illustrates some other phenomena as well.

EXAMPLE 1.12. Let X be $\mathbb{C} - \{0\}$ with its usual Hausdorff topology. On X we define a local system $\mathcal{L}$ of 2-dimensional complex vector spaces by letting $\mathcal{L}(U)$ be the space of $\mathbb{C}$-valued functions that are of the form $f + c$ with $f : U \to \mathbb{C}$ continuous and satisfying $e^{f(z)} = z$. In other words, f is a branch of the logarithm function. But recall that branch need not defined and that

The constant functions define a constant subsheaf $\mathbb{C}_X \subset \mathcal{L}$. The quotient sheaf $\mathcal{L}/\mathbb{C}_X$ is also isomorphic to $\mathbb{C}_X$, for it admits as a global generating section the function "$\log$" (note that the multivaluedness of this function disappears if we work modulo constants). But the section "$\log$" cannot be lifted to X: the only global sections of $\mathcal{L}(X)$ are the constants. So the exact sequence of abelian sheaves

$$0 \to \mathbb{C}_X \to \mathcal{L}_X \to \mathcal{L}_X/\mathbb{C}_X \to 0$$

evaluated on X yields a sequence of abelian groups

$$0 \to \Gamma(X, \mathbb{C}_X) \to \Gamma(X, \mathcal{L}_X) \to \Gamma(X, \mathcal{L}_X/\mathbb{C}_X) \to 0.$$

We observed that the last sequence can be identified with $0 \to \mathbb{C} = \mathbb{C} \xrightarrow{0} \mathbb{C} \to 0$. So it fails to be exact at $\Gamma(X, \mathbb{C}_X)$. This also shows that the image presheaf of $\mathcal{L} \to \mathcal{L}_X/\mathbb{C}_X$ and the cokernel presheaf of $\mathbb{C}_X \to \mathcal{L}$ are not sheaves.

1.13. THE PREIMAGE OF A SHEAF. Here is a relative version of the sheafification process. Suppose we are given a continuous map $f : X \to Y$ between topological

spaces and an abelian sheaf $\mathcal{G}$ on Y. We want to define a sheaf $f^{-1}\mathcal{G}$ on X with the property that the stalk of $f^{-1}\mathcal{G}$ at $x \in X$ is $\mathcal{G}_{f(x)}$. If $U \subset X$ is open and s assigns to $x \in X$, $s_x \in \mathcal{G}_{f(x)}$, then we stipulate that s defines a section of $f^{-1}\mathcal{F}$ if for each $x \in U$ there exists a neighborhood V_x of y in Y and a section $t \in \mathcal{G}(V_y)$ such that for x' in a neighborhood of x in $f^{-1}V_x \cap U$, we have $s_{x'} = t_{f(x)}$. This is indeed a sheaf, called the *sheaf pull-back* of $\mathcal{G}$. If Y is a single point $\{y\}$, so that $\mathcal{G}$ is given by a single group $G = \mathcal{G}_y$, then this reproduces the sheaf of locally constant maps from open subsets of X to G.

If $Y \subset X$ is a subspace, then we often write $\Gamma(Y, \mathcal{F})$ for the group of global sections of $i^{-1}\mathcal{F}$, where $i : Y \subset X$ denotes the inclusion. Notice that when Y is open, this is just $\mathcal{F}(Y)$.

EXERCISE 78 (Adjunction). Suppose that $f : X \to Y$ is a continuous map and let $\mathcal{F}$ resp. $\mathcal{G}$ be an abelian sheaf on X resp. Y.

(a) Prove that we may identify $\mathrm{Hom}(\mathcal{G}, f_*\mathcal{F})$ with $\mathrm{Hom}(f^{-1}\mathcal{G}, \mathcal{F})$. (In categorical language: $\mathcal{G} \mapsto f^{-1}\mathcal{G}$ is the *left adjoint* of $\mathcal{F} \mapsto f_*\mathcal{F}$ and the latter is the *right adjoint* of the former, the convention being that 'left' acts on the item before the comma in Hom and 'right' on what comes after it.)
(b) Deduce the existence of natural sheaf homomorphisms $\mathcal{G} \to f_*f^{-1}\mathcal{G}$ and $f^{-1}f_*\mathcal{F} \to \mathcal{F}$.
(c) Give examples to show that neither of these needs to be an isomorphism. (Hint for the second case: look at Example 1.10.)
(d) Suppose that f is a homeomorphism. Show that under the identification (a) a sheaf isomorphism from $\mathcal{G} \to f_*\mathcal{F}$ yields a sheaf isomorphism $f^{-1}\mathcal{G} \to \mathcal{F}$ and vice versa. (If any such an isomorphism exists, we say that $(X, \mathcal{F})$ and $(Y, \mathcal{G})$ are isomorphic.)

A space X endowed with a sheaf of rings $\mathcal{O}_X$ is called a *ringed space*; the sheaf in question is then often referred to as its *structure sheaf*. This notion becomes much more useful if we also have a notion of morphism of ringed spaces: if $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ are ringed spaces, then by a morphism from $(X, \mathcal{O}_X)$ to $(Y, \mathcal{O}_Y)$ we mean a pair consisting of a continuous map $f : X \to Y$ and a sheaf homomorphism of rings $\mathcal{O}_Y \to f_*\mathcal{O}_X$. According to Exercise 78 the latter is equivalent to giving a sheaf homomorphism of rings $f^{-1}\mathcal{O}_Y \to \mathcal{O}_X$. (We often abuse notation by denoting this pair by the single symbol f.)

REMARK 1.14. Via Exercise 76 we can (at least formally) characterize certain extra structures on spaces in a uniform manner. For example, given a topological m-manifold M, then a *C^k-differentiable structure* on M is simply given by a subsheaf of the sheaf $\mathbb{R}$-valued continuous functions on M which has the property that locally it is isomorphic to the sheaf of C^k-differentiable functions on $\mathbb{R}^m$. It is a sheaf of $\mathbb{R}$-algebras. A C^k-map between two C^k-manifolds is then simply a morphism between the corresponding ringed spaces (or rather, spaces endowed with a sheaf of $\mathbb{R}$-algebras). This is a more conceptual (and perhaps also more concise) than the definition based on an atlas. A *holomorphic structure* on M (which turns M into a complex manifold) and a holomorphic map between complex manifolds can be defined in a similar manner. An affine variety is naturally a ringed space and indeed, a k-prevariety, is a a ringed space locally isomorphic as a ringed space to an affine k-variety. This is why such sheaves are often referred to as *structure sheaves*. We shall define in the same spirit a structure sheaf on the spectrum of a ring.

2. The spectrum of a ring as a locally ringed space

Let R be a ring. We recall that its spectrum $\mathrm{Spec}(R)$ is the set of its prime ideals. We agreed that for a prime ideal $\mathfrak{p}$ of R, the corresponding element of $\mathrm{Spec}(R)$ is denoted $x_{\mathfrak{p}}$, and that the prime ideal associated to $x \in \mathrm{Spec}(R)$ is denoted $\mathfrak{p}_x \subset R$.

For $s \in R$, $Z(s) \subset \mathrm{Spec}(R)$ denotes the set of $x_{\mathfrak{p}} \in \mathrm{Spec}(R)$ with $s \in \mathfrak{p}$ and $U(s) := \mathrm{Spec}(R) - Z(s)$. The collection $\{U(s)\}_{s\in R}$, is basis for a topology on $\mathrm{Spec}(R)$, the *Zariski topology*. We therefore refer to any $U(s)$ as a *basic open subset* of $\mathrm{Spec}(R)$. So the closed subsets of this topology are of the form $Z(S) = \cap_{s\in S} Z(s)$, where $S \subset R$ is a subset (but note that $Z(S)$ does not change if we replace S by the radical of the ideal generated by S). We found in Remark 10.3 that $\mathrm{Spec}(R)$ is quasicompact.

The spectrum of a ring R is a singleton precisely when R has just one prime ideal. Since $\sqrt{(0)}$ is the intersection of all the prime ideals of R, it follows that this prime ideal equals $\sqrt{(0)}$ and must be a maximal ideal. (So if R is noetherian it will have finite length.) We have $\sqrt{(0)} = (0)$ precisely when R is a field.

The spectrum of a local ring has just one closed point (namely the one defined by its maximal ideal), but can have plenty of nonclosed points, of course.

We observed that a ring homomorphism $\phi : R' \to R$ determines a map

$$\mathrm{Spec}(\phi) : \mathrm{Spec}(R) \to \mathrm{Spec}(R'), \quad x_{\mathfrak{p}} \mapsto x_{\mathfrak{p}'},$$

where $\mathfrak{p}' := \phi^{-1}\mathfrak{p}$. It has the property that $\mathrm{Spec}(\phi)^{-1}(U(r')) = U(\phi(r'))$ so that $\mathrm{Spec}(\phi)$ is continuous. The ring homomorphism $R' \to R \to R_{\mathfrak{p}}$ factors through $R'_{\mathfrak{p}'}$ (by Exercise 12) and so we have an associated homomorphism of local rings $\phi_{\mathfrak{p}} : R'_{\mathfrak{p}'} \to R_{\mathfrak{p}}$. We have $\phi_{\mathfrak{p}}^{-1}(\mathfrak{p}R_{\mathfrak{p}}) = \mathfrak{p}'R_{\mathfrak{p}'}$ and so this homomorphism is local in the sense of:

DEFINITION 2.1. A homomorphism $\psi : A' \to A$ of local rings is said to be a *local homomorphism* if $\psi^{-1}\mathfrak{m}_A = \mathfrak{m}_{A'}$ (so that it defines an embedding of residue fields $A'/\mathfrak{m}_{A'} \hookrightarrow A/\mathfrak{m}$).

Hence a homomorphism of local rings is local precisely if the induced map on spectra sends the closed point to the closed point. For instance, the inclusion of the local ring $k[[t]]$ in its quotient field $k((t))$ is not local, for the maximal ideal of $k((t))$ is the zero ideal, but the zero ideal is not equal to the maximal ideal $tk[[t]]$ of $k[[t]]$. Thus the singleton $\mathrm{Spec}(k((t)))$ maps to the nonclosed point of $\mathrm{Spec}(k[[t]])$ defined by the zero ideal.

For every subset $Y \subset \mathrm{Spec}(R)$, we may consider the set $I(Y)$ of $r \in R$ which 'vanish' on Y, that is for which $Z(r) \supset Y$. This is clearly an ideal in R. In this context, a Nullstellensatz comes easily as it is basically the content of Lemma 2.15:

PROPOSITION 2.2. *Given a ring R, then for every ideal $J \subset R$, $I(Z(J)) = \sqrt{J}$.*

PROOF. The property $r \in I(Z(J))$ means $Z(r) \supset Z(J)$. This in turn means that every prime ideal which contains J must contain r. In other words, $I(Z(J))$ is the intersection of all the prime ideals that contain J. According to Exercise 15 this intersection is precisely $\sqrt{J}$ and so $r \in \sqrt{J}$. □

PROPOSITION 2.3. *Let R be a ring.*

(i) *The closure of the singleton $\{x_{\mathfrak{p}}\}$ consists of the $x_{\mathfrak{q}} \in \mathrm{Spec}(R)$ with $\mathfrak{q} \supset \mathfrak{p}$.*

(ii) *A singleton* $\{x_{\mathfrak{p}}\}$ *is closed if and only if* $\mathfrak{p}$ *is a maximal ideal (so that* $\mathrm{Spec}(R)$ *contains* $\mathrm{Specm}(R)$ *as the set of its closed points).*
(iii) *A closed subset of* $\mathrm{Spec}(R)$ *is irreducible if and only if it is the closure of a singleton.*
(iv) *A subset of* $\mathrm{Spec}(R)$ *is an irreducible component of* $\mathrm{Spec}(R)$ *if and only if it is of the form* $\overline{\{x_{\mathfrak{p}}\}}$ *with* $\mathfrak{p}$ *a minimal prime ideal of* R.

PROOF. The proofs of (i) and (ii) are left to you as an exercise. As for (iii) and (iv), let $C \subset \mathrm{Spec}(R)$ be a closed irreducible subset. We first prove that $I(C)$ is prime. For suppose that $r_1 r_2 \in I(C)$ for certain $r_1, r_2 \in R$. Then $Z(r_1 r_2) = Z(r_1) \cup Z(r_2)$ contains C and since C is irreducible it follows that $Z(r_1) \supset C$ or $Z(r_2) \supset C$ or equivalently, that $r_1 \in I(C)$ or $r_2 \in I(C)$. By definition, $x \in C$ if and only if $\mathfrak{p}_x \supset I(C)$ and so C is the closure of the singleton $\{x_{I(C)}\}$. On the other hand, a singleton is irreducible and hence so is its closure. Now (iii) and (iv) follow. □

EXERCISE 79. Let $\phi : R' \to R$ be a ring homomorphism. Prove that if $I' \subset R'$ is a proper ideal, then the natural map $\mathrm{Spec}(R'/I') \to \mathrm{Spec}(R')$ is injective with image the closed subset of $\mathrm{Spec}(R')$ defined by I'. Show that the preimage of this closed subset under $\mathrm{Spec}(\phi) : \mathrm{Spec}(R) \to \mathrm{Spec}(R')$ is the closed subset of $\mathrm{Spec}(R)$ defined by the ideal of R generated by $\phi(I)$.

When s is nilpotent, $U(s) = \emptyset$. Let us agree that then $R[1/s]$ denotes the zero ring. Since a prime ideal must always be proper ideal, we then also have $\mathrm{Spec}(R[1/s]) = \emptyset$. The following proposition identifies basic open subsets with spectra of simple localizations and shows that inclusions between them come from obvious ring homomorphisms.

PROPOSITION 2.4. *Given* $s \in R$, *denote by* $j_s : R \to R[1/s]$ *the natural map. Then* $\mathrm{Spec}(j_s) : \mathrm{Spec}\, R[1/s] \to \mathrm{Spec}(R)$ *is a homeomorphism onto* $U(s)$. *We have* $U(s) \subset U(s')$ *if and only if* $s \in \sqrt{(s')}$ *and the inclusion is then induced by the associated homomorphism* $R[1/s'] \to R[1/s]$.

PROOF. When $R[1/s]$ is the zero ring there is nothing to prove and so let us assume that this is not the case. Then s is not nilpotent. If $\tilde{\mathfrak{p}}$ is a prime ideal $R[1/r]$, then $\mathfrak{p} = j_s^{-1}\tilde{\mathfrak{p}}$ is a prime ideal with $s \notin \mathfrak{p}$ and we have $\tilde{\mathfrak{p}} = \mathfrak{p}[1/s]$. On the other hand, for a prime ideal $\mathfrak{p}$ of R with $s \notin \mathfrak{p}$, $\mathfrak{p}[1/s]$ is a prime ideal of $R[1/r]$ and the preimage of $j_s^{-1}\mathfrak{p}[1/s] = \mathfrak{p}$. In other words, $\mathrm{Spec}(j_s)$ is injective with image $U(s)$. This map is continuous. It is also open: a nonempty basic open subset of $\mathrm{Spec}\, R[1/s]$ is defined by a nonnilpotent $s' \in R[1/s]$. If $s'' \in R$ denotes the product of s and the numerator of s', then $R[1/s][1/s'] = R[1/s'']$ and so this basic open set is also a basic open subset of $\mathrm{Spec}(R)$.

We have $U(s) \subset U(s')$ if and only if $Z(s) \supset Z(s')$ and by Proposition 2.2 this means that $s^n = s'r$ for some $r \in R$ and some integer $n > 0$. Hence $R[1/s']$ maps to $R[1/(s'r)] = R[1/s]$ and this map of course defines the inclusion $U(s) \subset U(s')$. □

Henceforth we will use $\mathrm{Spec}(j_s)$ to identify $U(s)$ with $\mathrm{Spec}\, R[1/s]$.

The following theorem is of fundamental conceptual importance. It interprets in a geometric manner the localizations of R and the natural maps between them.

THEOREM-DEFINITION 2.1. *Let* R *be a ring and put* $X := \mathrm{Spec}(R)$. *There is a sheaf of rings* $\mathcal{O}_X$ *on* X *characterized by the property that for a basic open set* $U(s)$,

$\mathcal{O}_X(U(s)) = R[1/s]$ and the restriction map defined by an inclusion $U(s) \subset U(s')$ is the associated homomorphism $R[1/s'] \to R[1/s]$. Its stalk $\mathcal{O}_{X,x}$ at $x \in X$ is the local ring $R_{\mathfrak{p}_x}$. We call $\mathcal{O}_X$ the structure sheaf *of X.*

PROOF. For the existence and uniqueness of $\mathcal{O}_X$, it suffices, in view of Exercise 76, to prove the following:

Let be given a collection of nonempty basic open subsets $\{U(s_\alpha)\}_{\alpha\in A}$ of X whose union is a basic open subset $U(s)$ and let $\{u_\alpha \in R[1/s_\alpha]\}_{\alpha\in A}$ be a collection with the property that for every pair $\alpha, \beta \in A$, u_α and u_β become equal in $R[1/(s_\alpha s_\beta)]$. Then the members of this collection come from a unique element $u \in R[1/s]$.

The verification of this property is modeled after the proof of Proposition 10.2. Since $U(s) = \operatorname{Spec} R[1/s]$ is quasicompact, there is a *finite* subset $K \subset A$ such that $U(s) = \cup_{\kappa\in K} U(s_\kappa)$. For $\kappa \in K$, we write $u_\kappa = r_\kappa/s_\kappa^{N_\kappa}$. We can take N_κ larger if we want to and so we may assume that they are all equal to some N'.

For $\kappa, \lambda \in K$, $r_\kappa/s_\kappa^{N'}$ and $r_\lambda/s_\lambda^{N'}$ become equal in $R[1/(s_\kappa s_\lambda)]$, and so $r_\kappa s_\lambda^{N'} - r_\lambda s_\kappa^{N'}$ is annihilated by $(s_\kappa s_\lambda)^{N_{\kappa,\lambda}}$ for some $N_{\kappa,\lambda} \geq 0$. We can take $N_{\kappa,\lambda}$ larger if we want to, and so we may assume that they are all equal to some N''. Now put $\tilde{r}_\kappa := r_\kappa s_\kappa^{N''}$ and $N := N' + N''$. Then $u_\kappa = \tilde{r}_\kappa/s^N$ and $\tilde{r}_\kappa s_\lambda^N = \tilde{r}_\lambda s_\kappa^N$ for all $\kappa, \lambda \in K$.

Since $U(s) = \cup_{\kappa\in K} U(s_\kappa)$, we have

$$Z(s) = \cap_{\kappa\in K} Z(s_\kappa) = \cap_{\kappa\in K} Z(s_\kappa^N) = Z(\sum_{\kappa\in K} R s_\kappa^N).$$

Then s^M of s will lie in the ideal $\sum_{\kappa\in K} R s_\kappa^N$ for some $M > 0$ by Proposition 2.2:

$$s^M = \sum_{\kappa\in K} t_\kappa s_\kappa^N$$

for certain $t_\kappa \in R$. We put $r := \sum_{\kappa\in K} t_\kappa \tilde{r}_\kappa \in R$. Then for every $\lambda \in K$,

$$r s_\lambda^N = \sum_{\kappa\in K} t_\kappa \tilde{r}_\kappa s_\lambda^N = \sum_{\kappa\in K} t_\kappa \tilde{r}_\lambda s_\kappa^N = \tilde{r}_\lambda s^M$$

This proves that $u := r/s^M \in R[1/s]$ maps to u_κ in $R[1/s_\kappa]$ for $\kappa \in K$. This does not prove yet that u has this property for an arbitrary $\alpha \in A$. Still we could in the above argument replace K by $K \cup \{\alpha\}$ and thus come up with a $u' \in R[1/s]$ which is such that it not only maps to u_κ in $R[1/s_\kappa]$ for $\kappa \in K$, but also to u_α in $R[1/s_\alpha]$. It therefore remains to show $u = u'$ (which then also would establish uniqueness). The fact that $u - u' \in R[1/s]$ maps to the zero element of $R[1/s_\kappa]$ means that $s_\kappa^{n_\kappa}(u - u') = 0$ for some $n_\kappa > 0$. Since some power s^n of s lies in the ideal $\sum_{\kappa\in K} R s^{n_\kappa}$, it follows that $s^n(u - u') = 0$. This means that $u = u'$ in $R[1/s]$.

It remains to prove the assertion about the stalks. An element of this stalk at $x_\mathfrak{p}$ is represented by a fraction $r/s \in R[1/s]$ with $s \notin \mathfrak{p}$, with the understanding that two such fractions $r/s \in R[1/s]$ and $r'/s' \in R[1/s']$ are considered equal if they coincide in some $R[1/s'']$ with $s'' \notin \mathfrak{p}$, where s and s' divide s''. This means that $rs' - r's$ is annihilated by some power of s''. This implies that they define the same element of $R_\mathfrak{p}$. In other words, the stalk at $x_\mathfrak{p}$ embeds in $R_\mathfrak{p}$. On the other hand, any element of $R_\mathfrak{p}$ thus appears as it is represented by a fraction r/s with $s \notin \mathfrak{p}$ (and so nonnilpotent). □

REMARK 2.5. If in the previous proposition we take $s = 1$, we find that $R = \Gamma(X, \mathcal{O}_X)$ and so no information is lost when we pass from R to the associated ringed space.

EXERCISE 80. Determine the points and the stalks of the spectrum of the local rings $K[[t]]$, $K[t]_{(t)}$ (with K a field) and $\mathbb{Z}_{(p)}$ (the fractions whose denominator is not divisible by p).

EXERCISE 81 (Follows up on Exercise 32). Prove that any prime ideal $\mathfrak{p}$ of the ring $\mathbb{Z}[x]$ is one the following

(i) the zero ideal,
(ii) the ideal generated by a positive degree polynomial whose coefficients have no common divisor > 1 and which is irreducible in $\mathbb{Q}[x]$,
(iii) the ideal generated by a prime number p and the cyclotomic polynomial $\Phi_{p^r} \in \mathbb{Z}[x]$ for some $r \geq 1$).

Conclude that every algebraic integer resp. every element of a finite field determines an element of $\mathbb{A}^1_{\mathbb{Z}}$ with two such defining the same element if and only if they have the same minimum polynomial over their prime field ('are Galois conjugate') and that every element under (ii) resp. (iii) is obtained this way. (The spectrum of $\mathbb{Z}[x]$ is called the *affine line over the ring of integers* and is usually denoted by $\mathbb{A}^1_{\mathbb{Z}}$.)

Proposition 2.1 associated to a ring R a ringed space. We expect a ring homomorphism $\phi : R' \to R$ to induce a morphism of ringed spaces. This is indeed the case.

PROPOSITION 2.6. *Let R and R' be rings and put $X := \mathrm{Spec}(R)$, $X' := \mathrm{Spec}(R')$.*

Every ring homomorphism $\phi : R' \to R$ defines a continuous map $f = \mathrm{Spec}(\phi) : X \to X'$ and gives rise to a natural sheaf homomorphism of rings $\tilde{\phi} : \mathcal{O}_{X'} \to f_*\mathcal{O}_X$ whose value on X', $\tilde{\phi}(X') : R' = \Gamma(X', \mathcal{O}_{X'})' \to \Gamma(X', f_*\mathcal{O}_X) = \Gamma(X, \mathcal{O}_X) = R$, is ϕ. If we think of $\tilde{\phi}$ as a sheaf homomorphism $f^{-1}\mathcal{O}_{X'} \to \mathcal{O}_X$, then its stalk at $x = x_{\mathfrak{p}}$ is given by the local sheaf homomorphism $R'_{\phi^{-1}\mathfrak{p}} \to R_{\mathfrak{p}}$ induced by ϕ.

Conversely, any pair $(f, \tilde{\phi})$ with $f : X \to Y$ a continuous map and $\tilde{\phi} : \mathcal{O}_{X'} \to f_*\mathcal{O}_X$ a sheaf homomorphism $\tilde{\phi} : \mathcal{O}_{X'} \to f_*\mathcal{O}_X$ such that the induced map on stalks is local, comes from the ring homomorphism $R' \to R$ defined by $\tilde{\phi}(X')$.

PROOF. For the first assertion, we explain how $\tilde{\phi}$ is defined on a basic open $U(r') \subset X'$, i.e., we give the homomorphism $\Gamma(U(r'), \mathcal{O}_{X'}) \to \Gamma(U(r'), f_*\mathcal{O}_X)$. This will determine $\tilde{\phi}$ as a sheaf homomorpism. We have $\Gamma(U(r'), \mathcal{O}_{X'}) = R'[1/r']$. Put $r := \phi(r')$. We have already seen that $f^{-1}U(r') = U(r)$. The ring homomorphism $R'[1/r'] \to R[1/r]$ induced by ϕ can be understood as a ring homomorphism

$$\Gamma(U(r'), \mathcal{O}_{X'}) = R'[1/r'] \to R[1/r] = \Gamma(U(r), \mathcal{O}_X) = \Gamma(U(r'), f_*\mathcal{O}_X)$$

(when r is nilpotent, $U(r) = \emptyset$ and the right hand side is the zero ring). We thus have defined a homomorphism $\tilde{\phi} : \mathcal{O}_{X'} \to f_*\mathcal{O}_X$ of sheaves of rings. It is clear that this homomorphism is on the stalks as asserted.

Suppose now given $(f, \tilde{\phi})$ is as in the proposition and let $\phi : R' \to R$ be the ring homomorphism that is the value of $\tilde{\phi}$ on X'. The sheaf property implies that

for every $x = x_{\mathfrak{p}} \in X$ we have a commutative diagram

$$\begin{array}{ccc} R' = \Gamma(X', \mathcal{O}_{X'}) & \xrightarrow{\phi} & \Gamma(X', f_*\mathcal{O}_X) = R \\ \downarrow & & \downarrow \\ R'_{\mathfrak{p}'} = \mathcal{O}_{X',x'} & \xrightarrow{\tilde{\phi}_{\mathfrak{p}}} & \mathcal{O}_{X,x} = R_{\mathfrak{p}} \end{array}$$

where $\mathfrak{p}'$ is the prime ideal of R' associated to $x' := f(x)$. The bottom map is local and so the preimage of $\mathfrak{p}R_{\mathfrak{p}}$ is $\mathfrak{p}'R'_{\mathfrak{p}'}$. The commutativity of the diagram implies that then $\phi^{-1}\mathfrak{p} = \mathfrak{p}'$. In other words, $\mathrm{Spec}(\phi)$ and f take the same value on x and define the same map on the stalk at this point. Hence ϕ induces the pair $(f, \tilde{\phi})$. □

Let us say that a *locally ringed space* is a ringed space whose stalks are local rings and let us agree that a *morphism of locally ringed spaces* is a morphism of ringed spaces that are locally ringed and which has the additional property that it gives local homomorphisms on the stalks. This defines the *category of locally ringed spaces*. To any ring R we have associated a locally ringed space (which we denote $\mathrm{Spec}(R)$ by abuse of notation) and we found that ring homomorphims $R' \to R$ are in bijective correspondence with the morphisms $\mathrm{Spec}(R) \to \mathrm{Spec}(R')$ as locally ringed spaces. Thus the spec construction identifies the dual of the category of rings as a full subcategory of the category of locally ringed spaces. We enlarge this category by taking the full subcategory whose objects are locally like the spectrum of a ring and thus arrive at the central notions of algebraic geometry:

DEFINITION 2.7. An *affine scheme* is a ringed space that is isomorphic to $\mathrm{Spec}(R)$ for some ring R. A *quasi-affine scheme* is a ringed space that is isomorphic to an open subset to $\mathrm{Spec}(R)$ for some ring R. A *scheme* is a ringed space that is locally an affine scheme (hence this is always a locally ringed space). A *morphism of schemes* is a morphism between such objects in the category of locally ringed spaces.

It is often useful the fix a 'base scheme' S and to consider *S-schemes*, that is, schemes X endowed with a morphism $X \to S$. We often refrain from giving this morphism a name and write X/S instead. An S-morphism between S-schemes, $X/S \to Y/S$, is then a morphism $X \to Y$ whose composite with the given morphism $Y \to S$ yields the given morphism $X \to S$. But when $S = \mathrm{Spec}(R)$, we usually say that X is an *R-scheme* (rather than a $\mathrm{Spec}(R)$-scheme) and we write X/R accordingly. This simply means that $\mathcal{O}_X$ is a sheaf of R-algebras and that the R-morphisms $f : X/R \to Y/R$ are those with the property that the induced homomorphisms on stalks are R-algebra homomorphisms. In particular, every scheme is a $\mathbb{Z}$-scheme. We also observe that the category of k-prevarieties is a full subcategory of the category of k-schemes.

3. The proj construction

We describe a way of producing a scheme out of a graded ring, such that the relation between the algebra and the geometry generalizes the way a projective variety defines a homogeneous coordinate ring. We start out with a graded ring $R = \oplus_{k=0}^{\infty} R_k$. This has a distinguished ideal, $R_+ := \oplus_{k=1}^{\infty} R_k$. We define a scheme $\mathrm{Proj}(R)$ whose underlying set is the set of *homogeneous prime ideals strictly contained in* R_+ (briefly: strict homogeneous prime ideals). Given a homogeneous element of positive degree d, $s \in R_d$, then the strict homogeneous prime ideals

of R which contain s define a subset $Z_s \subset \mathrm{Proj}(R)$. We denote its complement by U_s. We have $U_s \cap U_{s'} = U_{ss'}$ as usual and so the subsets U_s are a basis for a topology on $\mathrm{Proj}(R)$. We give $\mathrm{Proj}(R)$ with this topology. When s is not nilpotent, the monotone union $R[1/s]_0 := \cup_{k\geq 0} R_{dk}/s^k$ is the subring of $R[1/s]$ of degree zero. This monotone union makes $R[1/s]_0$ a *filtered ring*: $R_{dk}/s^k.R_{dl}/s^l \subset R_{dkl}/s^{kl}$ (think of the case of $k[t]$ filtered by the subspaces of polynomials of degree $\leq k$, $k = 0, 1, 2 \cdots$).

We claim that as a topological space, U_s can be identified with $\mathrm{Spec}(R[1/s]_0)$. For if $\mathfrak{p} \subset R$ is a strict homogeneous prime ideal which does not contain s, then you easily check that $\cup_{k\geq 0}\mathfrak{p}_{dk}/s^k$ is a prime ideal of $R[1/s]_0$. Conversely, if $\mathfrak{p}'$ is a prime ideal of $R[1/s]_0$, then denote by $\mathfrak{p}_k \subset R_k$ the set of $a \in R_k$ for which $aR_{dl-k}/s^{dl} \subset \mathfrak{p}'$ for l large enough (if this inclusion holds for some l, then it holds also for any larger l). This is a homogeneous ideal which does contain s. It is also a prime ideal: if $a \in R_k$ and $a' \in R_{k'}$ are such that $aa'R_{dm-k-k'}/s^{dm} \subset \mathfrak{p}'$ for some m, then by enlarging m we may assume that we can write $m = l + l'$ such that $k \leq dl$ and $k' \leq dl'$. If neither $aR_{dl-k}/s^{dl} \subset \mathfrak{p}'$ nor $a'R_{dl-k'}/s^{dl'} \subset \mathfrak{p}'$, then choose $r \in R_{dl-k}$ and $r' \in R_{dl-k'}$ such that neither ar/s^{dl} nor $a'r'/s^{dl'}$ is in $\mathfrak{p}'$. But since their product is in $\mathfrak{p}'$ we get a contradiction. You can check that the two constructions are each others inverse.

Given $s' \in R_{d'}$, then we have an inclusion of basic open sets $U_s \subset U_{s'}$ if and only s' divides some positive power of s, and then such an inclusion is covered by an obvious ring homomorphism $R[1/s']_0 \to R[1/s]_0$. Hence $\mathrm{Proj}(R)$ is in a natural way a scheme:

PROPOSITION-DEFINITION 3.1. *Denote by X the set $\mathrm{Proj}(R)$ with the topology as just defined. The map $U_s \mapsto R[1/s]_0$ extends to a sheaf $\mathcal{O}_X$ of rings on X with the property that its restriction to U_s equals $\mathrm{Spec}(R[1/s]_0)$ as a ringed space. This makes X a scheme. If $\mathfrak{p}$ is a strict homogeneous prime ideal of R, then the stalk of $\mathcal{O}_X$ at the point associated to $\mathfrak{p}$ is the degree zero subring $R_{\mathfrak{p},0} = \cup_{k\geq 1} R_k/(R_k - \mathfrak{p}_k)$ (a monotone union) of $R_{\mathfrak{p}}$. A scheme that arises from this construction is called a* projective scheme.

In case A is a ring and we take for R the graded ring $A[X_0, \ldots, X_n]$ (with $\deg(X_i) = 1$ for all i), then the associated projective scheme $\mathrm{Proj}(A[X_0, \ldots, X_n])$ is called projective n-space over A and is denoted $\mathbb{P}^n_A$. In case $A = k$, this indeed reproduces our $\mathbb{P}^n_k$.