

A first course on Algebraic Geometry

Eduard Looijenga

Throughout this course we fix a field k , which we assume is algebraically closed. 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 $c \in k - \{0\}$ and $x_1, \dots, x_d \in k$. 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 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 power¹ or even of the quotient field of any integral domain such as $\mathbb{C}[x_1, \dots, x_r]$.

Rings are always supposed to possess a unit element 1 and a ring homomorphism will always take unit to unit. We also assume them to be commutative unless the contrary is stated. If R is a ring, then we denote the multiplicative group of invertible elements of R by R^\times . An R -algebra is a ring A endowed with a ring homomorphism $\phi: R \rightarrow A$, 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 .

¹Since 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.

Affine varieties

1. The Zariski topology

Any $f \in k[x_1, \dots, x_n]$ determines in an evident manner a function $k^n \rightarrow k$. 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 $k[x_1, \dots, x_n]$ 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}_k^n , 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 function $\mathbb{A}^n \rightarrow k$ is then said to be *regular* if it is defined by some $f \in k[x_1, \dots, x_n]$. 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 $f \in k[x_1, \dots, x_n]$ is completely determined by the regular function it defines. (Hint: do first the case $n = 1$.) So the ring $k[x_1, \dots, x_n]$ 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. (Hint: use Exercise 1.)

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 $\{U(f) : f \in k[x_1, \dots, x_n]\}$ is a basis of a topology on \mathbb{A}^n , called the Zariski topology¹. 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 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 $U(f_1) \cap U(f_2) = U(f_1 f_2)$. 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 $Z(f)$. \square

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.

¹We shall later modify the definition of both \mathbb{A}^n and the Zariski topology.

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

$$I : \{\text{subsets of } \mathbb{A}^n\} \rightarrow \{\text{ideals of } k[x_1, \dots, x_n]\},$$

$$X \subset \mathbb{A}^n \mapsto I(X) := \{f \in k[x_1, \dots, x_n] : f|_X = 0\}.$$

$$Z : \{\text{subsets of } k[x_1, \dots, x_n]\} \rightarrow \{\text{closed subsets of } \mathbb{A}^n\}.$$

$$J \subset k[x_1, \dots, x_n] \mapsto Z(J) := \bigcap_{f \in J} Z(f).$$

Observe that

$$I(X_1 \cup X_2) = I(X_1) \cap I(X_2), \quad Z(J_1 \cup J_2) = Z(J_1) \cap Z(J_2),$$

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

EXERCISE 4. Prove that $I(\{p\})$ is in fact equal to the ideal generated by these 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 $f, g \in k[x_1, \dots, x_n]$ have the same restriction to Y if and only if $f - g \in I(Y)$. So the quotient ring $k[x_1, \dots, x_n]/I(Y)$ can be regarded as a ring of k -valued functions on Y . Notice that this ring does not change if we replace Y by its Zariski closure.

DEFINITION 1.3. Suppose Y is closed in \mathbb{A}^n . Then $k[x_1, \dots, x_n]/I(Y)$ is called the *coordinate ring* of Y and we denote this ring by $A(Y)$. A function $Y \rightarrow k$ is said to be *regular* if it lies in this ring.

Let $Y \subset \mathbb{A}^n$ be closed. If $X \subset Y$, then $I(X) \supset I(Y)$, so that $I_Y(X) := I(X)/I(Y)$ 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:

$$I_Y : \{\text{subsets of } Y\} \rightarrow \{\text{ideals of } A(Y)\},$$

$$Z_Y : \{\text{subsets of } A(Y)\} \rightarrow \{\text{closed subsets of } Y\}.$$

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 . \square

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 $I(Z(J)) = \sqrt{J}$.*

The inclusion \supset is clear; the hard part is the opposite inclusion. 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:*

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

These bijections are inclusion reversing and each others inverse.

PROOF. We first prove this for $Y = \mathbb{A}^n$. It is clear 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 . \square

Let \mathfrak{m} be a maximal ideal of $k[x_1, \dots, x_n]$. 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 $k[x_1, \dots, x_n]$. 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 $k[x_1, \dots, x_n]$, Corollary 1.6 implies that Y will be nonempty and minimal for this property. In other words, Y is a singleton $\{y\}$ (and if $y = (a_1, \dots, a_n)$, then $\mathfrak{m} = (x_1 - a_1, \dots, x_n - a_n)$, 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 $A(Y) = k[x_1, \dots, x_n]/I(Y)$. 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 quite useful (and natural) for spaces equipped with 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 closed subset of Y .

EXERCISE 7. Prove that no Hausdorff space with more than one point is irreducible. Prove also that an infinite set with the cofinite topology is irreducible.

EXERCISE 8. Let C be an irreducible subspace of a topological space Y . Prove that if G_1, \dots, G_s are closed subsets of Y whose union contains C , then one of these contains C .

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 $G \supset \bar{C}$. So \bar{C} is irreducible. \square

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

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

PROOF. Suppose Y is irreducible and $f, g \in k[x_1, \dots, x_n]$ 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 $f_i \in I(Y_i)$ such that $f_i \in I(Y_i) - I(Y)$. 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. \square

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 $k[x_1, \dots, x_n]$ 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) 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 $(p_1), \dots, (p_s)$ are unique up to order).

Here are two basic examples.

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.

More relevant here is the case $k[x_1, \dots, x_n]$ with $n > 0$. A principal ideal of this ring is prime precisely when it is generated by an irreducible polynomial of positive degree. It is indeed true that every $f \in k[x_1, \dots, x_n]$ of positive degree can be written as a product of irreducible polynomials and that this factorization is unique up to order and multiplication of each factor by a nonzero element of k .

PROPOSITION 2.5. *If $f \in k[x_1, \dots, x_n]$ is irreducible, then the hypersurface $Z(f)$ it defines is irreducible. If $f \in k[x_1, \dots, x_n]$ is of positive degree and $f = f_1 f_2 \cdots f_s$ is a decomposition into irreducible polynomials, then $Z(f_1), \dots, Z(f_s)$ are the irreducible components of $Z(f)$ and $Z(f) = Z(f_1) \cup \cdots \cup Z(f_s)$ (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 $f \in k[x_1, \dots, x_n]$ is irreducible, then f generates a prime ideal and so $Z(f)$ is an irreducible hypersurface by Proposition 2.3.

If $f \in k[x_1, \dots, x_n]$ is of positive degree and $f = f_1 f_2 \cdots f_s$ as 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 and contains $Z(f_i)$. We must show that $C = Z(f_i)$.

Since $C \subset Z(f) = Z(f_1) \cup \cdots \cup Z(f_s)$ and C is irreducible, we have $C \subset Z(f_j)$ for some j (by Exercise 8). Hence $Z(f_i) \subset Z(f_j)$. By the Nullstellensatz this is equivalent to $f_j \in (f_i)$, in other words, f_i divides f_j . Since f_j is irreducible this can only be so if $f_j = c f_i$ for some $c \in k - \{0\}$. This implies that $C = Z(f_j) = Z(f_i)$. \square

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 we never have $b > b_0$ for some $b \in B$.

PROOF. (i) \Rightarrow (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) \Leftarrow (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. \square

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

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

EXERCISE 9. Prove that a subspace of a noetherian space is noetherian. Prove also that a ring quotient of a noetherian ring is noetherian.

EXERCISE 10. 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 almost all the rings we encounter possess and that it implies many finiteness properties without which we would not be able 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, then so is every finitely generated R -algebra. In particular, any ring quotient of $k[x_1, \dots, x_n]$ is noetherian. Also, the space \mathbb{A}^n is noetherian.*

PROOF. The Hilbert basis theorem implies (with induction on n) that $R[x_1, \dots, x_n]$ is noetherian. Hence every quotient ring $R[x_1, \dots, x_n]/I$ is also noetherian. By definition, a finitely generated R -algebra is as such 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 $I(Y_1) \subset I(Y_2) \subset \cdots$ is an ascending chain of ideals. As the latter becomes stationary, so will become the former. \square

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. 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. Since $Z \in B$, Z is reducible: 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 : 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, \dots, Y_k of Y such that $Y = Y_1 \cup \cdots \cup Y_k$. 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. \square

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 of $I(C)$ in $A(Y)$ is a minimal prime ideal of $A(Y)$. Conversely the preimage of a minimal prime ideal of $A(Y)$ is the ideal defined by an irreducible component of Y . 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 $k[x_1, \dots, x_n]$, 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 $A(Y)$. \square

EXAMPLE 2.12. 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 $k[x, y, z] \rightarrow k[x, y, z]/(y - x^2, z - x^3)$ 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 $I(C) = (y - x^2, z - x^3)$.

Now consider 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 $R \rightarrow S^{-1}R$ 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: $r/s \cdot r'/s' = (rr')/(ss')$ 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 $R \rightarrow S^{-1}R$ 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 11 below) the ring homomorphism $R \rightarrow S^{-1}R$ is universal for that property. This construction is called the *localization away from S* .

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, $r/1 = 0/1$ if and only if $r = 0$, so that $R \rightarrow S^{-1}R$ 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* $K(R)$ of R . In case R is an integral domain, $S = R - \{0\}$ and so $K(R)$ is a field, the *fraction field* of R .

We take the occasion here to note the following simple consequence: every prime ideal \mathfrak{p} of a ring R appears as the kernel of a ring homomorphism from that ring to a field: just take the composite $R \rightarrow R/\mathfrak{p} \rightarrow K(R/\mathfrak{p})$ (it is clear that conversely the kernel of a ring homomorphism from R to a field is always a prime ideal).

The case of immediate 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 11. Let R be a ring and let S be a multiplicative subset of R .

- What is the kernel of $R \rightarrow S^{-1}R$?
- Prove that a ring homomorphism $\phi : R \rightarrow R'$ with the property that $\phi(s)$ is invertible for every $s \in S$ factors in a unique manner through $S^{-1}R$.
- Consider the polynomial ring $R[x_s : s \in S]$ and the homomorphism of R -algebras $R[x_s : s \in S] \rightarrow S^{-1}R$ that sends x_s to $1/s$. Prove that this homomorphism is surjective and that its kernel is generated by the ideal generated by the degree one polynomials $sx_s - 1$, $s \in S$.

EXERCISE 12. Let R be a ring and let \mathfrak{p} be a prime ideal of R .

- 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 $R_{\mathfrak{p}}$.
- 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*.)
- Prove that the localization map $R \rightarrow R_{\mathfrak{p}}$ drops to an isomorphism of fields $K(R/\mathfrak{p}) \rightarrow R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$.
- Work this out for $R = \mathbb{Z}$ and $\mathfrak{p} = (p)$, where p is a prime number.
- Same for $R = k[x, y]$ and $\mathfrak{p} = (x)$.

LEMMA 2.14. *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. Consider the homomorphism $R \rightarrow R[1/a]$. The ring $R[1/a]$ has a maximal ideal² and hence admits a ring homomorphism to some field F : $\phi : R[1/a] \rightarrow F$. Then the kernel of the composite $R \rightarrow R[1/a] \rightarrow F$ is a prime ideal (for F has no zero divisors) and a is not in this kernel (for its image is invertible with inverse $\phi(1/a)$). \square

EXERCISE 13. 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.

The following proposition is the algebraic counterpart of Proposition 2.10. There is also a similarity between the proofs.

²Every 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.

PROPOSITION-DEFINITION 2.15. *An associated prime of a ring R is a minimal prime ideal $\mathfrak{p} \subset R$. If R is noetherian, then the number of its associated primes is finite and their intersection equals $\sqrt{(0)}$.*

PROOF. Assume R is noetherian. We first show that any radical ideal $J \subsetneq R$ is an intersection of finitely many prime ideals. Let B be the collection of the radical ideals $I \subsetneq R$ that do not have this property and suppose that B is nonempty. Then B contains a minimal member I_0 . Since I_0 cannot be a prime ideal, there exist $a_1, a_2 \in R - I_0$ with $a_1 a_2 \in I_0$. 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 , J_i is an intersection of 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 $i = 1, \dots, s$ 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. \square

EXERCISE 14. 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 is ultimately only interested in rings.

We fix a ring R . 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 $\text{End}(M)$ of group homomorphisms $M \rightarrow M$ is a ring for which subtraction is pointwise defined and multiplication is composition (so if $f, g \in \text{End}(M)$, 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. This ring may fail to obey our standard conventions: it is usually noncommutative and if $M = \{0\}$, then $\text{End}(M) = \{0\}$ so that $1 = 0$ in this case. 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 $R \rightarrow \text{End}(M)$.

So any $r \in R$ defines a homomorphism $M \rightarrow M$; 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: $r(m_1 - m_2) = rm_1 - rm_2$, $(r_1 - r_2)m = r_1m - r_2m$, $1 \cdot m = m$, $r_1(r_2m) = (r_1r_2)m$. 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 natural if you think about it. For instance, a linear space M of $(p \times q)$ -matrices in which the coefficients are allowed to lie in a ring R of functions is an R -module. Also, every ideal $I \subset R$ is an R -module. An

\mathbb{Z} -module structure on an abelian group M is empty: it does not add to M anything else than the structure it already has an abelian group.

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

DEFINITIONS 3.2. In what follows is M an R -module. A map $f : M \rightarrow N$ from M to an R -modules 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 $f : R \rightarrow R'$, 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 $M \rightarrow M/N$ 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 $r_1s_1 + \dots + r_ks_k$ 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 $N_1 \subset N_2 \subset \dots$ 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 (so 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 $N_0 \neq N$, then 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 $N_1 \subset N_2 \subset \dots$ is an ascending chain of R -modules, then the union $N := \bigcup_{i=1}^{\infty} N_i$ is a R -submodule. Let $\{s_1, \dots, s_k\}$ be a finite set of generators of N . If $s_{i_\kappa} \in N_{i_\kappa}$, and $j := \max\{i_1, \dots, i_k\}$, then it is clear that $N_j = N$. So the chain becomes stationary as of index j . \square

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 $S \neq \emptyset$. Choose $s \in S$, so that our induction hypothesis applies to $M' := R(S - \{s\})$. Let $N_1 \subset N_2 \subset \dots$ be an ascending

chain of R -submodules of M . Consider the R -module homomorphism $\phi : R \rightarrow M$, $\phi(r) := rs$. Then $\phi^{-1}N_1 \subset \phi^{-1}N_2 \subset \dots$ is an ascending chain of ideals of R . Since R is noetherian this chain stabilizes, as of index j_1 , say. Our induction hypothesis implies that $N_1 \cap M' \subset N_2 \cap M' \subset \dots$ becomes stationary, say as of index j_2 . Put $j_0 := \max\{j_1, j_2\}$. Then for $j \geq j_0$, N_j and N_{j_0} have the same intersection with M' and the same image in M/M' . It easily follows that $N_j = N_{j_0}$. \square

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 $r_d x^d + r_{d-1} x^{d-1} + \dots + r_0$ with $r_d \neq 0$. We call $r_d \in R$ the *initial coefficient* of f and denote it by $\text{in}(f)$. For the zero polynomial, we simply define this to be $0 \in R$. Notice that $\text{in}(fg) = \text{in}(f)\text{in}(g)$.

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 $\text{in}(I) := \{\text{in}(f) : f \in I\}$ of R . If $f, g \in I$ with $d := \deg(f) - \deg(g) \geq 0$, then $\text{in}(f) - \text{in}(g)$ is zero or equal to $\text{in}(f - t^d g)$. From this it easily follows that $\text{in}(I)$ is an ideal of R . Since R is noetherian, $\text{in}(I)$ is finitely generated: there exist $f_1, \dots, f_k \in I$ such that $\text{in}(I) = R\{\text{in}(f_1), \dots, \text{in}(f_k)\}$. Let d_i be the degree of f_i , $d_0 := \max\{d_1, \dots, d_k\}$ and $N \subset R[x]$ the set of polynomials of degree $< d_0$. So N is the R -submodule of $R[x]$ generated by $1, x, \dots, x^{d_0-1}$. We claim that

$$I = R[x]\{f_1, \dots, f_k\} + (I \cap N),$$

in other words, that every $f \in I$ is modulo $R[x]\{f_1, \dots, f_k\}$ 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 $\text{in}(f) = r_1 \text{in}(f_1) + \dots + r_k \text{in}(f_k)$ for certain $r_1, \dots, r_k \in R$. Now notice that

$$\text{in}(f) = \sum_i r_i \text{in}(f_i) = \sum_i \text{in}(r_i f_i) = \text{in}\left(\sum_i r_i f_i x^{d-d_i}\right).$$

It follows that $f - \sum_i r_i f_i x^{d-d_i}$ is an element of I of degree $< d$. It therefore lies in $R[x]\{f_1, \dots, f_k\} + (I \cap N)$ by our induction hypothesis. Hence so does f .

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

For the Nullstellensatz we need another finiteness result.

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

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

If there exist $a_1, \dots, a_n \in A$ which generate A as an R -algebra: $A = R[a_1, \dots, a_n]$, then $a_1, \dots, a_n, b_1, \dots, b_m$ 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, \dots, b_m , we may assume that b_1, \dots, 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, \dots, 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 $B = R[b_1, \dots, b_m] \subset \sum_k A_0 b_k$. 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. \square

This has a consequence for field extensions:

COROLLARY 3.7. *Let L/K be an extension of fields. Then this extension 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 there exist fractions $f_1/g_1, \dots, f_n/g_n \in K(b_1, \dots, b_r)$ (with $f_i, g_i \in K[b_1, \dots, b_r]$ and $g_i \neq 0$) which generate $K(b_1, \dots, b_r)$ as a K -algebra. Clearly not all the g_i can lie in K (for $K(b_1, \dots, b_r)$ strictly contains $K[b_1, \dots, b_r]$). So the degree of $g := g_1 g_2 \cdots g_n$ is positive. Since the fraction $1/(1+g) \in K(b_1, \dots, b_r)$ must be a polynomial in $f_1/g_1, \dots, f_n/g_n$, it follows that it 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 and we get a contradiction. \square

EXERCISE 15. Prove that a field which is finite generated as a ring (that is, which 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

$$A := (k[x_1, \dots, x_n]/J)[1/\bar{f}] = k[x_0, x_1, \dots, x_n]/(J, x_0 \bar{f} - 1).$$

The second description shows that this is a finitely generated k -algebra. 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. Let a_i denote the image of x_i in $A/\mathfrak{m} = k$ for $i = 0, \dots, n$ and put $p := (a_1, \dots, a_n) \in \mathbb{A}^n$. Since $(a_0; p) = (a_0, \dots, a_n)$ is a common zero of the elements of the ideal $(J, x_0 \bar{f} - 1)$, we have $p \in Z(J)$ and $a_0 \bar{f}(p) = 1$, so that $f(p) \neq 0$. \square

4. The affine category

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

DEFINITION 4.1. Let $X \subset \mathbb{A}^m$ and $Y \subset \mathbb{A}^n$ be closed subsets. We say that a map $f : X \rightarrow Y$ is a *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 $f^* : A(Y) \rightarrow A(X)$. 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 $\phi : A(Y) \rightarrow A(X)$. Then there is a unique regular map $f : X \rightarrow Y$ such that $f^* = \phi$.*

PROOF. Put $f_i := \phi(y_i|Y) \in A(X)$ ($i = 1, \dots, n$). Then $f = (f_1, \dots, f_n) : X \rightarrow \mathbb{A}^n$ has the property that for every $g \in k[y_1, \dots, y_n]$, $f^*g = \phi(g|Y)$. So f^* factors through $A(Y)$ and the resulting map $A(Y) \rightarrow A(X)$ coincides with ϕ . \square

The same argument shows that if $f : X \rightarrow Y$ and $g : Y \rightarrow Z$ are regular maps, then so is their composite $gf : X \rightarrow Z$. 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 $f : X \rightarrow Y$ is an *isomorphism* if it is bijective and the inverse is also a regular map. This implies that $f^* : A(Y) \rightarrow A(X)$ is a k -isomorphism of k -algebras. Proposition 4.2 implies that conversely, an isomorphism of k -algebras $A(Y) \rightarrow A(X)$ comes from a unique isomorphism $X \rightarrow Y$.

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 exist $a_1, \dots, a_n \in A$ such that every element is a polynomial expression in a_1, \dots, a_n with coefficients in k . Said differently, the k -algebra homomorphism $\phi : k[x_1, \dots, x_n] \rightarrow A$ which sends x_i to a_i is surjective. If we put $I := \text{Ker}(\phi)$, 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 we then have a k -algebra isomorphism $A(Y) \cong A$.

The formal way to sum up the preceding is 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 $f : \mathbb{A}^1 \rightarrow \mathbb{A}^2$, $f(t) = (t^2, t^3)$. 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 $f^* : k[x, y]/(x^3 - y^2) \rightarrow k[t]$ 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 $g \in \text{GL}(n, k)$ 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, \dots, g_n) are polynomials of degree one. So an affine-linear transformation is also an isomorphism of \mathbb{A}^n onto itself.

EXERCISE 16. 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 $t^2 + 1 = 0$.

- Prove that when $\text{char}(k) \neq 2$, f defines an isomorphism of $C - \{p_0\}$ onto $\mathbb{A}^1 - \{\pm\sqrt{-1}\}$.
- Consider the map $g : C \rightarrow \mathbb{A}^1$, $g(x, y) := x + \sqrt{-1}y$. Prove that when $\text{char}(k) \neq 2$, g defines an isomorphism of C onto $\mathbb{A}^1 - \{0\}$.
- Prove that when $\text{char}(k) = 2$, 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 17. Let $f_1, \dots, f_n \in k[x_1, \dots, x_n]$ be such that $f_1 = x_1$ and $f_i - x_i \in k[x_1, \dots, x_{i-1}]$ for $i = 2, \dots, x_n$. Prove that f defines an isomorphism $\mathbb{A}^n \rightarrow \mathbb{A}^n$.

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

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

By means of a linear transformation (this involves splitting off squares, hence requires the existence of $1/2 \in k$), the quadratic form $\sum_{1 \leq i < j \leq n} a_{ij} x_i x_j$ 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 $f(x_1, \dots, x_n) = \sum_{i=1}^r x_i^2 + \sum_{i=r+1}^n a_i x_i + a_0$ 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

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

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, \dots, 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 $\sum_{i=1}^r x_i^2 = 1$.

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 involved.

4.7. THE MAXIMAL IDEAL SPECTRUM. The previous discussion (and in particular Proposition 4.3) suggests to associate to a finitely generated k -algebra A a space $\text{Specm}(A)$ with a topology as follows. As a set, $\text{Specm}(A)$ is the collection of maximal ideals of A . In order to avoid confusion about whether a maximal ideal is to be viewed as a subset of A or as a point of $\text{Specm}(A)$ we agree that if \mathfrak{m} is a maximal ideal of A , then the corresponding element of $\text{Specm}(A)$ is denoted $x_{\mathfrak{m}}$ and if $x \in \text{Specm}(A)$, then the corresponding maximal ideal of A is denoted \mathfrak{m}_x . For every maximal ideal \mathfrak{m} of A , the residue field A/\mathfrak{m} is a finitely generated k -algebra and hence equal to k by Corollary 3.7. This implies that every $a \in A$ defines a function $f_a : \text{Specm}(A) \rightarrow k$ by letting $f_a(x)$ be the image of a in $A/\mathfrak{m}_x = k$. We denote by $Z(a) \subset \text{Specm}(A)$ (or $Z(f_a)$) the zero set of this function and by $U(a)$ or $(U(f_a))$ its complement, the nonzero set. The collection of $\{U(a)\}_{a \in A}$ is the basis of a topology on $\text{Specm}(A)$. So a subset $\text{Specm}(A)$ is closed precisely if it is an intersection of subsets of the form $Z(a)$; this is equal to the common zero set of the set of functions defined by an ideal of A . The space $\text{Specm}(A)$ is called the *maximal ideal spectrum of R* (but our notation for it is less standard). Notice, that if $A = A(Y)$ for a closed subset $Y \subset \mathbb{A}^n$, then the above discussion shows that $\text{Specm}(A)$ can be identified with Y as a topological space.

Suppose we are given k -algebra homomorphism $\phi : B \rightarrow A$. Then every maximal ideal $\mathfrak{m} \subset A$ is the kernel of a k -algebra homomorphism $v : A \rightarrow k$. The composite $v\phi : B \rightarrow k$ is also k -algebra homomorphism, hence surjective, and so its kernel, which is just $\phi^{-1}\mathfrak{m}$, is a maximal ideal as well. We thus get a map

$$\text{Specm}(\phi) : \text{Specm}(A) \rightarrow \text{Specm}(B), \quad x_{\mathfrak{m}} \mapsto x_{\phi^{-1}\mathfrak{m}}.$$

For $b \in B$, the preimage of $U(b)$ is $U(\phi(b))$. This shows that $\text{Specm}(\phi)$ is continuous.

EXERCISE 18. Let A be a finitely generated k -algebra. Prove that $a \in A \mapsto f_a$ is an algebra homomorphism from A to the algebra of k valued functions on $\text{Specm}(A)$. Show that its kernel is $\sqrt{(0)}$.

5. The product

Let m and n be nonnegative integers. We have already noted that the Zariski topology on \mathbb{A}^{m+n} is not the product topology on $\mathbb{A}^m \times \mathbb{A}^n$ (unless $mn = 0$). The product topology on \mathbb{A}^{m+n} is coarser: the bijection $\mathbb{A}^{m+n} \rightarrow \mathbb{A}^m \times \mathbb{A}^n$ is continuous, for if $f \in k[x_1, \dots, x_m]$ and $g \in k[y_1, \dots, y_n]$, then $U(f) \times U(g) = U(f * g)$, where

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

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). There is a similarly defined map:

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

which is evidently k -bilinear (i.e., 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 $k[x_1, \dots, x_m, y_1, \dots, y_n]$) 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. It is also the generality that that we will need later.)

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 $r(a \otimes_R b) := (ra) \otimes_R b$. Notice that the map

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

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 in \otimes_k .

EXERCISE 19. Prove that \otimes_R is universal for this property in the sense that every R -bilinear map $M \times N \rightarrow P$ of R -modules is the composite of \otimes_R and a *unique* R -homomorphism $M \otimes_R N \rightarrow P$. In other words, the map

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

is an isomorphism of R -modules.

EXERCISE 20. 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 $A \rightarrow A \otimes_R B$, $a \mapsto a \otimes_R 1$ and $B \rightarrow A \otimes_R B$, $b \mapsto 1 \otimes_R b$ are R -algebra homomorphisms. For example, $A \otimes_R R[x] = A[x]$ as A -algebras (and hence $A \otimes_R R[x_1, \dots, x_n] = A[x_1, \dots, x_n]$ with induction).

EXERCISE 21. 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 $A(X) \times A(Y) \rightarrow A(X \times Y)$, $(f, g) \mapsto f * g$ induces an isomorphism $\mu : A(X) \otimes A(Y) \rightarrow A(X \times Y)$ of k -algebras (so that in particular $A(X) \otimes A(Y)$ is reduced).

If X and Y are irreducible, then so is $X \times Y$.

PROOF. Since the obvious map

$$k[x_1, \dots, x_m] \otimes k[y_1, \dots, y_n] \rightarrow k[x_1, \dots, x_m, y_1, \dots, y_n]$$

is an isomorphism, it follows that μ is onto. In order to prove that μ is injective, let $u := \sum_{i=1}^N f_i \otimes g_i$ be in the kernel of μ . The k -vector subspace of $A(Y)$ spanned

by the g_i 's is finite dimensional. By choosing a basis of this subspace and writing each g_i out as a k -linear combination of basis vectors, we may as well assume that u was written accordingly. In other words, we may assume that g_1, \dots, g_N are k -linearly independent. We have $0 = \mu(u) = \sum_{i=1}^N f_i * g_i$. The restriction of $\mu(u)$ to $\{p\} \times Y \cong Y$ ($p \in X$) is the regular function $u_p := \sum_{i=1}^N f_i(p)g_i \in A(Y)$. Since this function is identically zero and the g_i 's are linearly independent, we must have $f_i(p) = 0$ for all i . As this is true for all $p \in X$, we must have $f_i = 0$ for all i . This proves that $u = 0$.

Suppose now X and Y irreducible, or equivalently, that $A(X)$ and $A(Y)$ are domains. We must show that $A(X \times Y)$ is then a domain. For this we identify $A(X \times Y)$ with $A(X) \otimes A(Y)$. Let $u \in A(X \times Y)$ and write u as above: $u = \sum_{i=1}^N f_i * g_i$ with $g_1, \dots, g_N \in A(Y)$ k -independent. It is clear that the set $X(u) \subset X$ of $p \in X$ for which $u_p = \sum_{i=1}^N f_i(p)g_i$ is zero is the common zero set of f_1, \dots, f_r and hence closed in X . Suppose now that u is a zero divisor: $uv = 0$ for some $v \in A(X \times Y)$. Then restriction of uv to $\{p\} \times Y$ shows that $u_p v_p = 0$ in $A(Y)$. Since $A(Y)$ is a domain, we must have $u_p = 0$ or $v_p = 0$. Since this is true for every $p \in X$, it follows that $X = X(u) \cup X(v)$. But since X is irreducible we have $X = X(u)$ or $X(v)$. This means that $u = 0$ or $v = 0$. \square

EXERCISE 22. 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 $\pi_X : X \times Y \rightarrow X$ and $\pi_Y : X \times Y \rightarrow Y$ 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, which almost seems to obvious to mention: if Z is a closed subset of some affine space, then any pair of regular maps $f : Z \rightarrow X, g : Z \rightarrow Y$ defines a regular map $Z \rightarrow X \times Y$ characterized by the property that its compositie with π_X resp. π_Y yields f resp. g (this is of course (f, g)).

6. Dimension

On way to define the dimension of a topological space X is inductively: the empty set had 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 more adapted to the Zariski topology).

DEFINITION 6.1. 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 $Y^0 \supsetneq Y^1 \supsetneq \dots \supsetneq Y^d$ 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 6.2. 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 $\dim Z \leq \dim X$. \square

EXERCISE 23. Prove that \mathbb{A}^n has Krull dimension at least n and is equal to n for $d = 1$. What is the Krull dimension of a nonempty Hausdorff space?

EXERCISE 24. 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 25. Suppose that X is a noetherian space. Prove that the dimension of X is the maximum of the dimensions of its irreducible components.

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

DEFINITION 6.3. 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 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 $\dim R = d$.

The prime ideals of a ring R are the preimages of the prime ideals of $R_{\text{red}} := R/\sqrt{(0)}$ 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 , $\dim A = \dim \text{Specm}(A)$.

The Krull dimension is easy to define, but is difficult to use directly (for instance it is not easy to see that $\dim \mathbb{A}^n \leq n$). The following theorem (the proof of which we omit) helps to calculate dimensions:

*THEOREM 6.4. *Let F be a field and let A be a finitely generated F -algebra without zero divisors. Then $\dim A$ is finite and the length of every maximal prime chain in A is equal to the transcendence degree of $K(A)$ over F . In particular, $\dim A = \text{trdeg}_F K(A)$.*

Since the field of fractions of $k[x_1, \dots, x_n]$ has transcendental degree n it follows that $\dim \mathbb{A}^n = n$. So every subset of \mathbb{A}^n has finite Krull dimension.

COROLLARY 6.5. *Let $X \subset \mathbb{A}^n$ be closed and irreducible. Then every maximal irreducible chain in X has length $\dim X$. Moreover, every nonempty open $U \subset X$ has the same dimension as X .*

PROOF. The first assertion follows from Theorem 6.4 applied to $A(X)$. For the second assertion we must show that $\dim U \geq \dim X$. Choose $p \in U$. Extend the singleton $\{p\}$ (which is closed in X and irreducible) to a maximal irreducible chain in X . According to first assertion this chain has length $\dim X$. By Exercise 24 this chain restricts to an irreducible chain in U . So $\dim U \geq \dim X$. \square

EXERCISE 26. Prove that a hypersurface in \mathbb{A}^n has dimension $n - 1$.

EXERCISE 27. Prove that when X and Y are closed subsets of affine spaces, the $\dim(X \times Y) = \dim X + \dim Y$. (Hint: use Exercise 22.)

7. The notion of a morphism

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. We restrict ourselves here to irreducible closed sets, but what follows generalizes to arbitrary closed sets.

In this section we fix an *irreducible closed* subset $Y \subset \mathbb{A}^n$. We shall make frequent use of the fact (Lemma 2.2) that a nonempty open subset of the irreducible Y is dense in Y (so that any two such will always have a nonempty intersection).

For $0 \neq f \in A(Y)$, $U(f)$ is nonempty in Y and hence dense in Y . The coordinate ring $A(Y)$ is an integral domain and so its ring of fractions $K(A(Y))$ is a field. An element of $K(A(Y))$ is by definition of the form f/g with $f, g \in A(Y)$ and $g \neq 0$. So this is well-defined k -valued function on the open-dense subset $U(g)$ of Y .

DEFINITION 7.1. Let $p \in Y$. Then a k -valued function on a neighborhood of p in the affine variety Y is said to be *regular* at p if on a (perhaps smaller) neighborhood of p in Y , this function is of the form f/g with $f, g \in A(Y)$ and $g(p) \neq 0$. A k -valued function defined on an open subset U of Y is said to be *regular* if it is regular in every point of U ; we denote the k -algebra of such functions by $\mathcal{O}(U)$.

A *rational function* on Y is represented by a regular function on a nonempty open subset of Y , with the understanding that two such functions are regarded as equal if they coincide on a nonempty open subset contained in a common domain of definition. The set of such functions defines a field, called the *function field* of Y , which we denote by $k(Y)$.

For $U = Y$ we now seem to have two definitions of a regular function. This is only apparently so:

PROPOSITION 7.2. *The natural maps $A(Y) \rightarrow \mathcal{O}(Y)$ and $K(A(Y)) \rightarrow k(Y)$ are isomorphisms of k -algebras. In particular, $\dim Y = \text{trdeg}_k k(Y)$.*

The proof uses localization at a prime ideal (which was introduced in Exercise 12).

LEMMA 7.3. *Let R be an integral domain, so that for every maximal ideal $\mathfrak{m} \subset R$ the localization $R_{\mathfrak{m}} = (R - \mathfrak{m})^{-1}R$ is contained in the quotient field $K(R)$. Then the common intersection in $K(R)$ of the localizations of R at the maximal ideals equals R (regarded as a subring of $K(R)$).*

PROOF. Suppose $u \in K(R)$ lies in the localization of every maximal ideal of R . Consider the set I of $r \in R$ with $ru \in R$. This is clearly an ideal of R . If $I \neq R$, then I is contained in some maximal ideal $\mathfrak{m} \subset R$. But since $u \in R_{\mathfrak{m}}$, there exists a $r \in R - \mathfrak{m}$ such that $ru \in R$ and we get a contradiction. So $I = R$, in particular, $u = 1 \cdot u \in R$. \square

PROOF OF PROPOSITION 7.2. Let $\phi \in k(Y)$. We can represent ϕ by a nonempty open $U \subset Y$ and some $\phi_U \in \mathcal{O}(U)$. By definition there exists for every $p \in U$ an open neighborhood U_p of p in U such that $\phi_U|_{U_p}$ is given by a fraction $f/g \in K(A(Y))$ with $U_p \subset U(g)$. Then f/g maps to ϕ under the map $K(A(Y)) \rightarrow k(Y)$. It remains to see that f/g is unique. If $f'/g' \in K(A(Y))$ also maps to ϕ , then the two fractions coincide as functions on a nonempty open subset V contained in $U(g) \cap U(g')$. This means that $fg' - f'g$ vanishes on V . Since V is dense in Y , it follows that $fg' - f'g$ vanishes on all of Y . But then $fg' - f'g = 0$ as an element of $A(Y)$, so that $f/g = f'/g'$ in $K(A(Y))$.

It also shows that every $\phi \in \mathcal{O}(Y)$ can be regarded as an element of $K(A(Y))$ with the property that it lies in the localization $A(Y)_{\mathfrak{m}_p}$ for every $p \in Y$. Since

every maximal ideal of $A(Y)$ is of the form \mathfrak{m}_p , it follows from Lemma 7.3 that $\phi \in A(Y)$. \square

We are now ready to describe the maps which we want to consider.

DEFINITION 7.4. A subset of \mathbb{A}^n is called *quasi-affine* if it is open in a closed irreducible subset.

Given two quasi-affine subsets $U \subset \mathbb{A}^m$ and $V \subset \mathbb{A}^n$, then a map $f : U \rightarrow V$ is called a *morphism* if the components f_1, \dots, f_n of f are regular functions on U . We say that f is an *isomorphism* if f is bijective and both f and f^{-1} are morphisms³.

It is clear that a morphism $f : U \rightarrow V$ is continuous and determines a homomorphism of k -algebras $f^* : \mathcal{O}(V) \rightarrow \mathcal{O}(U)$. So if f is an isomorphism, then f is a homeomorphism and f^* is an isomorphism of k -algebras.

EXAMPLE 7.5 (The Frobenius morphism). Here is an important example of a bijection which is not an isomorphism. Assume that k has positive characteristic p and consider the morphism $F_p : \mathbb{A}^1 \rightarrow \mathbb{A}^1$, $x \mapsto x^p$. It is not only surjective (every element of k has a p th root since k is algebraically closed), but also injective: if $a^p = b^p$, then $0 = a^p - b^p = (a - b)^p$ and so $a = b$. But the endomorphism of $k[x]$ induced by f^* sends x to x^p and has therefore image $k[X^p]$. Clearly, this endomorphism is not surjective.

Notice that the fixed point set $\mathbb{A}^1(\mathbb{F}_p)$ 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 $\mathbb{F}_p \subset k$. 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 $\overline{\mathbb{F}_p}$ of \mathbb{F}_p in k is the union of the finite subfields of k , the affine line over $\overline{\mathbb{F}_p}$ 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 $\mathbb{A}^n \rightarrow \mathbb{A}^n$ (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 $\mathbb{A}^n(\overline{\mathbb{F}_p}) = \cup_{r \geq 1} \mathbb{A}^n(\mathbb{F}_{p^r})$.

EXERCISE 28. Assume that k has positive characteristic p and suppose $Y \subset \mathbb{A}^n$ that is the common zero set of polynomials with coefficients in \mathbb{F}_q , where $q = p^r$ is a positive integral power of p . Write F for $F_p^r : \mathbb{A}^n \rightarrow \mathbb{A}^n$.

- Prove that $f \in k[x_1, \dots, x_n]$ has its coefficients in \mathbb{F}_q if and only if $F^* f = f^q$.
- Prove that an affine-linear transformation of \mathbb{A}^n with coefficients in \mathbb{F}_q commutes with F .
- Prove that F restricts to a bijection $F_Y : Y \rightarrow Y$ and that the fixed point set of F_Y^m is $Y(\mathbb{F}_{q^m}) := Y \cap \mathbb{A}^n(\mathbb{F}_{q^m})$.

REMARK 7.6. After this exercise it is impossible not 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 28, 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*:

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

³We will later extend these notions to a wider category.

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 (late 1970s), 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 29. Compute the Weil zeta function of affine n -space relative to the field of q elements.

DEFINITION 7.7. We say that a quasi-affine subset of \mathbb{A}^m is *affine*⁴ if it is isomorphic to a closed subset of some \mathbb{A}^n .

EXAMPLE 7.8. Let $f \in k[x_1, \dots, x_n]$ be nonconstant and consider the hypersurface $Z \subset \mathbb{A}^{n+1}$ defined by $f(x_1, \dots, x_n)x_{n+1} - 1 = 0$. The projection $(x_1, \dots, x_n) : Z \rightarrow \mathbb{A}^n$ is evidently a morphism with image $U(f)$. The inverse $U(f) \rightarrow Z$ has components $(x_1, \dots, x_n, 1/f)$, so is a morphism as well. It follows that $U(f)$ and Z are isomorphic, in particular, $U(f)$ is affine. Since

$$\mathcal{O}(Z) = A(Z) = k[x_1, \dots, x_{n+1}]/(fx_{n+1} - 1),$$

we see that the isomorphism $Z \cong U(f)$ identifies $\mathcal{O}(U(f))$ with $k[x_1, \dots, x_n][1/f]$.

This example generalizes to the case of a nonconstant $f \in \mathcal{O}(Y)$ with Y affine: we find that $U(f)$ is affine and $\mathcal{O}(U(f)) = \mathcal{O}(Y)[1/f]$.

EXAMPLE 7.9. We can take this further: if $U \subset \mathbb{A}^m$ and $f : U \rightarrow V \subset \mathbb{A}^n$ are as above, 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 quasi-affine in \mathbb{A}^{m+n} . The map $x \in U \mapsto (x, f(x)) \in \tilde{U}$ and the projection $\tilde{U} \rightarrow U$ are regular and each others inverse. So they define an isomorphism $\tilde{U} \rightarrow U$. Notice that via this isomorphism f appears as a projection mapping: $(x, y) \in \tilde{U} \mapsto y \in V$.

EXERCISE 30. 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. (Hint: Observe that the maximal ideal $(x, y) \subset k[x, y] = \mathcal{O}(U)$ is not represented by a point of U .)

8. Rational maps

We shall now also give a geometric interpretation of finitely generated field extensions of k and the k -homomorphisms between them.

⁴Our definition deviates slightly from the one in Hartshorne’s book.

DEFINITION 8.1. Let Y and Y' be affine varieties. A *rational map* from Y to Y' is given by a pair (U, F) , where U is a nonempty open subset of Y and $F : U \rightarrow Y'$ 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 $f : Y \dashrightarrow Y'$.

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 8.2. *Any finitely generated field extension of k is k -isomorphic to the function field of an affine variety. Let Y and Y' be affine varieties. A dominant rational map $f : Y \dashrightarrow Y'$ determines a k -linear homomorphism of fields $f^* : k(Y') \rightarrow k(Y)$. Every k -linear homomorphism of fields $k(Y') \rightarrow k(Y)$ is induced by a unique dominant rational map.*

PROOF. Let K/k be a finitely generated field extension of k : there exist $a_1, \dots, a_n \in K$ such that every element of K can be written as a fraction of polynomials in a_1, \dots, a_n . So if R denotes the k -subalgebra of K generated by a_1, \dots, 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 $Y \subset \mathbb{A}^n$ (defined by the kernel of the obvious ring homomorphism $k[x_1, \dots, x_n] \rightarrow R$), it follows that K can be identified with $k(Y)$.

Suppose we are given an open and nonempty $U \subset Y$ and a morphism $F : U \rightarrow Y'$ with $f(Y)$ dense in Y' . By taking U smaller is necessary, we may assume that U is affine. Now $F^* : A(Y') \rightarrow A(U)$ will be injective, for if $F^*(g') = 0$, then F has image in $Z(g')$, so that $Z(g') = Y'$. This implies $g' = 0$. It follows that we can extend F^* to the fields of fractions $F^* : k(Y') \rightarrow k(U) = k(Y)$.

It remains to show that every k -algebra homomorphism $\Phi : k(Y') \rightarrow k(Y)$ is so obtained. For this, choose generators b_1, \dots, b_m of $A(Y')$. Then $\Phi(b_1), \dots, \Phi(b_m)$ are rational functions on Y' and so are regular on a nonempty open affine subset $U \subset Y$. Then we have a morphism $F : U \rightarrow Y' \subset \mathbb{A}^m$ whose coordinates are $\Phi(b_1), \dots, \Phi(b_m)$ (more formally, characterized by $F^*(b_i) = \Phi(b_i)$). So F^* is the restriction of Φ to $A(U)$. The image of F will be dense by the argument above: if F maps to a closed subset of Y' distinct from Y' , then it 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. The uniqueness of the rational map defined by (U, F) is clear. \square

COROLLARY 8.3. *There is a category with objects the affine k -varieties and morphisms the rational dominant maps. Assigning to an affine variety its function field makes this category anti-equivalent to the category of finitely generated field extensions of k .*

PROPOSITION-DEFINITION 8.4. *A rational map $f : Y \dashrightarrow Y'$ is an isomorphism in the above category (that is, induces an 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 such a birational map exists, we say that Y and Y' are birationally equivalent.*

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

Suppose now we have a k -linear isomorphism $k(Y') \cong k(Y)$. Represent this isomorphism and its inverse by (U, F) and (U', F') respectively. Then $F^{-1}U'$ is

open in U and $F'F : F^{-1}U' \rightarrow Y$ is defined. Since $F'F$ induces the identity on $k(Y)$, $F'F$ is the identity on a nonempty open subset of $F^{-1}U'$ and hence on all of $F^{-1}U'$. This implies that F maps $F^{-1}U'$ injectively to $F'^{-1}U$. For the same reason, F' maps $F'^{-1}U$ injectively to $F^{-1}U'$. So F defines an isomorphism between the open subsets $F^{-1}U' \subset Y$ and $F'^{-1}U \subset Y'$. \square

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 properties of varieties are an invariant of their birational equivalence class.

9. Sheaves and varieties

The notion of a quasi-affine variety as well as its later generalizations are best understood in the general context of ringed spaces. This involves the even more basic notion of a sheaf.

DEFINITION 9.1. 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*) $\mathcal{F}(U') \rightarrow \mathcal{F}(U)$ 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 $\mathcal{F}(U'') \rightarrow \mathcal{F}(U)$ is equal to the composite $\mathcal{F}(U'') \rightarrow \mathcal{F}(U') \rightarrow \mathcal{F}(U)$ and
- (iii) $\mathcal{F}(\emptyset)$ is the trivial group 0.

In case the groups of sections come with the structure of a ring (allowing the trivial ring in view of condition (iii)) and the restriction maps are ring homomorphisms, then we say that \mathcal{F} is a *presheaf of rings*. Likewise, we have the notion of a presheaf of modules over a fixed ring R . If \mathcal{F}' and \mathcal{F} are abelian presheaves on X such that $\mathcal{F}'(U) \subset \mathcal{F}(U)$ for every open $U \subset X$, then we say that \mathcal{F}' is *subpresheaf* of \mathcal{F} .

The terminology ‘section over U ’ and ‘restriction’ is suggestive, albeit sometimes a bit misleading.

EXAMPLE 9.2 (The constant presheaf). Give an abelian group G and a topological space X , then we have a 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 9.3. 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 $U \rightarrow G$ (with the obvious restriction maps) defines a 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).

EXAMPLE 9.4. 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 $U \rightarrow \mathbb{R}$. This is a subpresheaf of $\mathcal{C}_{M,\mathbb{R}}$ which in fact characterizes the differentiable structure on M .

EXAMPLE 9.5. On a complex manifold M , we have defined the presheaf $\mathcal{O}_M^{\text{an}}$ of \mathbb{C} -algebras which assigns to every nonempty open $U \subset M$ the \mathbb{C} -algebra $\mathcal{O}^{\text{an}}(U)$ of holomorphic functions $U \rightarrow \mathbb{C}$. This subsheaf of $\mathcal{C}_{M,\mathbb{C}}$ characterizes the complex structure on M .

EXAMPLE 9.6. For a quasi-affine subset $Y \subset \mathbb{A}^n$, we have defined the presheaf \mathcal{O}_Y of k -algebras which assigns to every nonempty open $U \subset Y$ the k -algebra $\mathcal{O}(U)$ of regular functions $U \rightarrow k$.

DEFINITION 9.7. 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 germs of sections of \mathcal{F} at p form an abelian group, the *stalk* of \mathcal{F} at p , denoted by \mathcal{F}_p .

For instance in the case of Example 9.5, when M is an open subset of \mathbb{C} , then the stalk $\mathcal{O}_{M,p}^{\text{an}}$ can be identified with the ring of convergent power series in $z - p$.

The last four examples differ from the first in that they satisfy an important additional property:

DEFINITION 9.8. An abelian presheaf \mathcal{F} on X is called a *sheaf* if

- (iv) every system of sections $\{s_i \in \mathcal{F}(U_i)\}_{i \in I}$ that is *compatible* in the sense that each pair s_i, s_j has the same restriction to their common domain $U_i \cap U_j$, is obtained as the collection of restrictions of a section of \mathcal{F} over $\cup_{i \in I} U_i$ and that section is unique.

A space X endowed with with a sheaf of rings is also called a *ringed space*. Examples are 9.3, 9.4 and 9.6. 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 $i = 1, 2$, 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 group of locally constant maps $U \rightarrow G$ (these are the maps constant on connectedness components of U).

This modification is a special case of a general construction which produces a sheaf \mathcal{F}^+ out of a presheaf \mathcal{F} : a section of \mathcal{F}^+ over an open U is represented a compatible collection of sections of \mathcal{F} relative to an open covering of U , with the understanding that two such collections define the same section of \mathcal{F}^+ if they become equal on a common refinement. It is straightforward to verify that this is well-defined and defines a sheaf.

EXERCISE 31 (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 $\mathcal{F}(U') \rightarrow \mathcal{F}(U)$, for $U, U' \in \mathcal{U}$ and $U \subset U'$.

Prove also a converse: suppose that \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 $\mathcal{F}(U') \rightarrow \mathcal{F}(U)$ such that the properties (i) through (iv) are satisfied (so for (iv) we must assume not only that $U_i \in \mathcal{U}$ for every $i \in I$, but also that $\cup_{i \in I} U_i \in \mathcal{U}$). Then \mathcal{F} extends to a sheaf on X .

REMARK 9.9. Via Exercise 31 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 sheaf of \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 . This is more conceptual (and perhaps also more concise) than the definition based on an atlas. (Implicit here is that we know what ‘locally isomorphic’ means—a notion you can guess.) A holomorphic structure on M can be defined in a similar manner. The notion of a scheme which we shall encounter later is modeled after these characterizations. This is why such sheaves are often referred to as *structure sheaves*.

EXAMPLE 9.10 (Maximal ideal spectrum as a ringed space). If A is a finitely generated k -algebra without zero divisors, then A appears as the coordinate ring of an affine variety and so by transcribing Example 9.6 to this more abstract setting we find a sheaf \mathcal{O} of k -valued functions on open subsets of $\text{Specm}(A)$; this is the structure sheaf on $\text{Specm}(A)$. In view of Proposition 7.2 it will have the property that its ring of sections on a basic open subset $U(a)$, $a \in A - \{0\}$ is equal to $A[1/a]$ and Exercise 31 tells us that this in fact characterizes \mathcal{O} . This formulation also makes sense if A has zero divisors (the basic subsets are then $U(a)$, $a \in A - \sqrt{(0)}$). And indeed, one can show that thus is obtained a sheaf of rings \mathcal{O} on $\text{Specm}(A)$. It has the property that we recover A as the set of sections of \mathcal{O} over $\text{Specm}(A)$ (take $a = 1$ so that $U(a) = \text{Specm}(A)$). But A may have nilpotent elements and so \mathcal{O} need no longer be a sheaf of k -valued functions. This is not so difficult to verify, but since the proof works for an arbitrary ring, we delay it until that stage has been set.

A continuous map $f : M \rightarrow N$ between manifolds (or if you prefer, between open subsets of \mathbb{R}^m and \mathbb{R}^n) is differentiable precisely, when composing f with any differentiable function on an open subset of N yields a differentiable function on an open subset of M . This shows that differentiability can be expressed in terms of the structure sheaves. With this example in mind, we make the following definition:

DEFINITION 9.11. A k -prevariety is an irreducible topological space X equipped with a sheaf of k -valued functions (X, \mathcal{O}_X) with the property that X can be covered with finitely many open subsets U for which $(U, \mathcal{O}_X|_U)$ is isomorphic to an affine variety with its structure sheaf (in the sense that there exists a homeomorphism κ of U onto an affine variety Z such that for every open $V \subset Z$, composition with κ maps $\mathcal{O}(V)$ onto $\mathcal{O}_X(\kappa^{-1}V)$). A morphism of k -prevarieties $f : (X, \mathcal{O}_X) \rightarrow (Y, \mathcal{O}_Y)$ consists of a continuous map $f : X \rightarrow Y$ such that for every $\phi \in \mathcal{O}_Y(V)$, $f^*\phi (= \phi f) \in \mathcal{O}_X(f^{-1}V)$.

The ‘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 below). The composite of two morphisms is evidently a morphism: we have here a category. For quasi-affine varieties this yields our previous definition, so there is no conflict here. In fact, this suggests to extend our definition of (quasi-)affine variety by saying that a k -prevariety is *affine* (resp. *quasi-affine*) if it is isomorphic to one in the old sense.

We often designate an prevariety and its underlying topological space by the same symbol, a habit which rarely leads to confusion.

Let X be a prevariety. Since X is irreducible, every nonempty open subset of X is irreducible and dense in X by Lemma 2.2. By assumption X is covered by finitely many affine open subvarieties U_1, \dots, 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, \dots, 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 32. Prove that a prevariety is a noetherian space. Prove also that every irreducible subset of a prevariety which is *locally closed* (i.e., the intersection of a closed subset with an open subset) is in natural manner a prevariety in such a manner that the inclusion 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 section of \mathcal{O}_X over a nonempty open subset of X and two such sections represent the same rational function if they coincide on a nonempty open subset in their domain of definition. The rational functions on X form a field $k(X)$, the *function field of X* . If $U \subset X$ is an affine subvariety, then $k(X) = k(U) = K(\mathcal{O}(U))$ (but we will see that it is not true in general that $k(X)$ is the field of fractions of $\mathcal{O}(X)$). In particular, U_1, \dots, U_N all have the same dimension $\text{trdeg}_k k(X)$. According to Exercise 24, this is then also the 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 subset of X to Y with the understanding that two such defined the same map if they coincide on a nonempty open 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.

9.12. 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 $\mathcal{O}(U) \otimes \mathcal{O}(V)[1/h]$. This product has the usual categorical characterization: the two projections $X \times Y \rightarrow X$ and $X \times Y \rightarrow Y$ are morphisms and if Z is a prevariety, then a pair of maps $(f : Z \rightarrow X, g : Z \rightarrow Y)$ defines a morphism $(f, g) : Z \rightarrow X \times Y$ if and only both f and g are morphisms.

The Hausdorff property is not of a local nature, for 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 and so requiring that the diagonal is closed is not totally unreasonable a priori. In fact, this condition turns out to be the

appropriate way of avoiding the pathologies that can result from an unfortunate gluing procedure.

DEFINITION 9.13. 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).

EXAMPLE 9.14. 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}_\pm^1 , then $(o_+, o_-) \in X \times X$ lies in the closure of the diagonal, but is not contained in the diagonal.

The proof of the following assertion is left as an exercise (see also Exercise 32).

PROPOSITION-DEFINITION 9.15. An subset of a variety X is called a subvariety if it is irreducible and locally closed in X . A subvariety is in a natural manner a variety such that the inclusion becomes a morphism. The product of two varieties is a variety.

10. Nonsingular points

If $Y \subset \mathbb{C}^n$ is an affine variety over \mathbb{C} of dimension d , then we hope that there is a nonempty open subset of Y where Y is ‘smooth’, i.e., where Y 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 $p \in \mathbb{R}^n$ and $f_i : U \rightarrow \mathbb{R}$, $i = 1, \dots, n-d$ are such that $f_i(p) = 0$ and the total differentials at p , $df_1(p), \dots, df_{n-d}(p)$ are linearly independent in p (this is equivalent to: the Jacobian matrix of (f_1, \dots, f_{n-d}) at p is of rank $n-d$), then the common zero set of f_1, \dots, f_{n-d} is a submanifold of dimension d at p whose tangent space there is the common zero set of $df_1(p), \dots, df_{n-d}(p)$. 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 p of dimension d is locally thus obtained.

We first note that partial differentiation of a polynomial $f \in k[x_1, \dots, x_n]$ is well-defined and produces another polynomial. The same goes for a rational function $\phi = f/g$: its partial derivatives are rational functions with denominator g^2 . We define the *total differential* of a rational function $\phi \in k(x_1, \dots, x_n)$ as usual:

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

where we do not worry about interpreting the symbols dx_i : for now we think of this 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, \dots, dx_n , leaving its intrinsic characterization for later. We must be careful with this notion when the characteristic of k is positive:

EXERCISE 33. Prove that $f \in k[x]$ has zero derivative, if and only if f is constant ($\text{char}(k) = 0$) or a p th power of some $g \in k[x]$ ($\text{char}(k) = p > 0$).

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

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

EXAMPLE 10.1. 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 $o = (0, 0)$ as a smooth point of C . Indeed, the projection $f : C \rightarrow \mathbb{A}^1, (x, y) \mapsto y$, 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: $x = u(y) = y^2 - y^6 + 3y^{10} + \dots$, where it is important to note that the coefficients are all integers, so that this works for every k .) In fact, the situation is worse: no local isomorphism between (C, o) and (\mathbb{A}^1, o) exists. The reason is that a local ring $\mathcal{O}_{Y,p}$ has the function field $k(Y)$ as its field of fractions. So if $k(Y)$ is not isomorphic to $k(x_1, \dots, x_n)$, then (Y, p) is not isomorphic to (\mathbb{A}^n, o) . This is the case here, for one can show that $k(C) \not\cong k(x)$.

Somewhat related to this is another issue, illustrated by the following

EXAMPLE 10.2. Consider the curve $C' \subset \mathbb{A}^2$ defined by $xy = x^3 + y^3$. The polynomial $x^3 + y^3 - xy$ is irreducible in $k[x, y]$, so that $A(C')$ is without zero divisors. Hence $\mathcal{O}_{C',o}$ 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 $y = u(x) = x^2 + x^5 + 3x^8 + \dots$ and the other by interchanging the roles of x and y : $x = v(y) = y^2 + y^5 + 3y^8 + \dots$. 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 Y at p , the local ring $\mathcal{O}_{Y,p}$ still carries too much global information, and that one way to get rid of that might be by passing formal power series. This is accomplished by passage to what is known as

10.3. 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 subsets $a + I^n M$, $a \in M$, $n \geq 0$. So this topology is translation invariant (translation over a fixed $a \in M$: $u \in M \mapsto u + a \in M$ is a homeomorphism) and the action of any $r \in R$ is continuous. The topology is Hausdorff precisely when $\bigcap_{n \geq 0} I^n M = 0$ and in that case it is even definable by a metric: if $\phi : \mathbb{Z}_+ \rightarrow (0, \infty)$ is any strictly monotonously decreasing function with $\lim_{n \rightarrow \infty} \phi(n) = 0$, then a metric d is defined by

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

This metric is *nonarchimedean* in the sense that $d(a, a'') \leq \max\{d(a, a'), d(a', a'')\}$. Recall that a metrized 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 n th terms goes to zero as $n \rightarrow \infty$. In the present situation this yields what is called the *I-adic completion*, \hat{M}_I . It can be described without any reference to ϕ : an element of \hat{M}_I is given by a sequence $(a_n \in M/I^n M)_{n \geq 0}$ whose terms are compatible in the sense that a_n is the reduction of a_{n+1} for all n . It is an R -module for componentwise addition and multiplication so that the obvious map $M \rightarrow \hat{M}_I, a \mapsto (a + I^n)_{n \geq 0}$ is a R -module homomorphism. It is easy to verify that \hat{M}_I is complete for the \hat{I} -adic topology and that the homomorphism $M \rightarrow \hat{M}_I$ is

continuous, has kernel $\cap_n I^n M$ and has dense image. Notice that \hat{R}_I is in fact a ring (multiplication is componentwise) such that $R \rightarrow \hat{R}_I$ is 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).

EXAMPLE 10.4. Take the ring $k[x_1, \dots, x_n]$. Its completion relative the maximal ideal (x_1, \dots, x_n) is just the ring of formal power series $k[[x_1, \dots, x_n]]$. We get the same result if we do this for the localization $\mathcal{O}_{\mathbb{A}^n, o}$ of $k[x_1, \dots, x_n]$ at (x_1, \dots, x_n) .

EXAMPLE 10.5. Take the ring \mathbb{Z} . Its completion with respect to the ideal (p) , p prime, yields the ring of p -adic integers $\hat{\mathbb{Z}}_{(p)}$. 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 34. Let I and J be ideals of a ring R with $J^p \subset I$. Prove that the J -adic topology is finer than the I -adic topology and that there is a natural continuous ring homomorphism $\hat{R}_J \rightarrow \hat{R}_I$. Conclude that when R is noetherian, \hat{R}_I can be identified with $\hat{R}_{\sqrt{I}}$.

*LEMMA 10.6 (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 ingenuous, but not difficult) can be found in any book on commutative algebra (e.g., Atiyah-Macdonald). The fact that $I^n M' \subset M' \cap I^n M$ implies that $M' \subset M$ is continuous for the I -adic topologies. But Artin-Rees tells us that we also have $M' \cap I^{n+n_0} M \subset I^n M'$. This shows more, namely that the I -adic topology M' is induced by that of M . So the closure of the image of M' in \hat{M}_I is a \hat{R}_I -submodule of the latter that can be identified with \hat{M}'_I .

COROLLARY 10.7. Suppose that in the previous lemma $\cap_{n \geq 0} I^n = (0)$ (so that M embeds in \hat{M}_I). Then M' is the intersection of M with the closure of M' in \hat{M}_I and \hat{M}_I/\hat{M}'_I can be identified with the I -adic completion of M/M' .

(This can be expressed as: when $\cap_{n \geq 0} I^n = (0)$, then I -adic completion is a faithfully exact functor.)

If R is a local ring, then \hat{R} denotes its completion with respect to the maximal ideal.

Let R be a noetherian local ring with maximal ideal \mathfrak{m} and residue field F . Then \mathfrak{m} is a finitely generated R -module. Since the ring R acts on $\mathfrak{m}/\mathfrak{m}^2$ via $R/\mathfrak{m} = F$, $\mathfrak{m}/\mathfrak{m}^2$ is a finite dimensional vector space over F .

DEFINITION 10.8. The *embedding dimension* $\text{embdim}(R)$ of a local ring R with maximal ideal \mathfrak{m} is the dimension of $\mathfrak{m}/\mathfrak{m}^2$ as a vector space over its residue field $F = R/\mathfrak{m}$. The *Zariski tangent space* $T(R)$ of R is the dual of the F -vector space $\mathfrak{m}/\mathfrak{m}^2$. If p is a point of a variety Y , then the embedding dimension $\text{embdim}_p Y$ and the Zariski tangent space $T_p Y$ of Y at p are by definition that of $\mathcal{O}_{Y,p}$.

For instance, the embedding dimension of \mathbb{A}^n at any point p is n . This follows from the fact that the map $d_p : f \in \mathfrak{m}_{\mathbb{A}^n, p} \mapsto df(p) \in k^n$ defines an isomorphism of k -vector spaces $\mathfrak{m}_{\mathbb{A}^n, p}/\mathfrak{m}_{\mathbb{A}^n, p}^2 \cong k^n$. We note in passing that we here have a way of understanding the total differential at p in more intrinsic terms as the map

$d_p : \mathcal{O}_{\mathbb{A}^n, p} \rightarrow \mathfrak{m}_{\mathbb{A}^n, p} / \mathfrak{m}_{\mathbb{A}^n, p}^2$ which assigns to $f \in \mathcal{O}_{\mathbb{A}^n, p}$ the image of $f - f(p) \in \mathfrak{m}_{\mathbb{A}^n, p}$ in $\mathfrak{m}_{\mathbb{A}^n, p} / \mathfrak{m}_{\mathbb{A}^n, p}^2$. Thus, a differential at p can be understood a k -linear function $T_p \mathbb{A}^n \rightarrow k$ and $(d_p(x_i) = dx_i(p))_{i=1}^n$ is a basis of $\mathfrak{m}_{\mathbb{A}^n, p} / \mathfrak{m}_{\mathbb{A}^n, p}^2$.

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

EXERCISE 35. Let (R', \mathfrak{m}) and (R, \mathfrak{m}') be local rings with the same residue field F . Prove that a ring homomorphism $\phi : R' \rightarrow R$ which is *local* (in the sense that it sends \mathfrak{m} to \mathfrak{m}') induces an F -linear map of Zariski tangent spaces $T(\phi) : T(R) \rightarrow T(R')$.

In order to understand the terminology, we first show:

LEMMA 10.9 (Nakayama's lemma). *Let 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.*

PROOF. Our assumptions say that $M = RS + \mathfrak{m}M$. So the (finite generated) R -module $M' := M/\mathfrak{m}M$ satisfies $M' = \mathfrak{m}M'$. We must show that $M' = 0$. Let e_1, \dots, e_s be R -generators of M' . By assumption there exist $x_{ij} \in \mathfrak{m}$ such that $e_i = \sum_{j=1}^s x_{ij} e_j$. So if $a_{ij} := \delta_{ij} - x_{ij}$, then $\sum_{j=1}^s a_{ij} e_j = 0$ for all i . The matrix $A = (a_{ij})_{i,j}$ has determinant in $1 + \mathfrak{m}$. Since $1 + \mathfrak{m}$ consists of invertible elements, Cramer's rule shows that A is invertible as a matrix. So $e_i = A^{-1}(0) = 0$ for all i and hence $M' = 0$. \square

If we apply this to $M = \mathfrak{m}$, we get:

COROLLARY 10.10. *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 10.11. A local ring R with maximal ideal \mathfrak{m} is said to be *regular* if it noetherian and its dimension equals its embedding dimension. A point of a variety Y is called *regular* or *nonsingular* if its local ring is regular; a point that is not regular is called *singular*.

We will show that this is indeed an intrinsic characterization of 'being like a submanifold'. We begin with a formal version of the implicit function theorem.

LEMMA 10.12. *Let f_1, \dots, f_{n-d} be regular functions at $p \in \mathbb{A}^n$ which vanish in p and for which $df_1(p), \dots, df_{n-d}(p)$ are linearly independent. Then these functions generate a prime ideal \mathfrak{p} in the local ring $\mathcal{O}_{\mathbb{A}^n, p}$ and the formal completion of $\mathcal{O}_{\mathbb{A}^n, p} / \mathfrak{p}$ with respect to its maximal ideal is isomorphic to $k[[x_1, \dots, x_d]]$ as a complete local k -algebra.*

PROOF. Let us abbreviate $\mathcal{O}_{\mathbb{A}^n, p}$ by \mathcal{O} and its maximal ideal by \mathfrak{m} . For $f \in \mathfrak{m}$, the image of f in $\mathfrak{m}/\mathfrak{m}^2$ is represented by $\sum_{i=1}^n \frac{\partial f}{\partial x_i}(p)(x_i - p_i)$ and so is essentially given by $df(p)$.

Now extend f_1, \dots, f_{n-d} to a system of regular functions $f_1, \dots, f_n \in \mathfrak{m}$ such that $df_1(p), \dots, df_n(p)$ are linearly independent. This means that f_1, \dots, f_n map to a basis of $\mathfrak{m}/\mathfrak{m}^2$. According to Nakayama's lemma, f_1, \dots, f_n then generate \mathfrak{m} . Hence the monomials of degree N in f_1, \dots, f_n generate \mathfrak{m}^N and hence also $\mathfrak{m}^N / \mathfrak{m}^{N+1}$. The latter is a k -vector space of dimension equal to the number of

degree N monomials in n variables. So these monomials form in fact a basis of $\mathfrak{m}^N/\mathfrak{m}^{N+1}$. It now easily follows that we have an isomorphism of complete local rings (a ring isomorphism that is also a homeomorphism) $k[[y_1, \dots, y_n]] \rightarrow \hat{\mathcal{O}}$ which sends y_i to the image of f_i in $\hat{\mathcal{O}}$. Its inverse defines a topological embedding of \mathcal{O} in $k[[y_1, \dots, y_n]]$ (sending f_i to y_i). The ideal generated by (y_1, \dots, y_{n-d}) in $k[[y_1, \dots, y_n]]$ is the closure of the image of \mathfrak{p} . It is clearly a prime ideal. According to Corollary 10.7 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} in $k[[y_1, \dots, y_n]]/(y_1, \dots, y_{n-d}) = k[[y_{n-d+1}, \dots, y_n]]$ realizes the completion of \mathcal{O}/\mathfrak{p} . \square

THEOREM 10.13. *Let $Y \subset \mathbb{A}^n$ be irreducible and closed and let $p \in Y$. Then the local ring $\mathcal{O}_{Y,p}$ is regular of dimension d if and only there exist regular functions f_1, \dots, f_{n-d} on an affine neighborhood U of p in \mathbb{A}^n such that these functions generate $I(Y \cap U)$ and df_1, \dots, df_{n-d} are linearly independent in every point of U . In that case, the formal completion $\hat{\mathcal{O}}_{Y,p}$ is as a complete local k -algebra isomorphic to $k[[x_1, \dots, x_d]]$. The Zariski tangent space $T_p Y$ is as a subspace of the Zariski tangent space $T_p \mathbb{A}^n$ equal to the kernel of the linear map $(df_1(p), \dots, df_{n-d}(p)) : T_p \mathbb{A}^n \rightarrow k^{n-d}$.*

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

According to Lemma 10.12, the ideal in $\mathcal{O}_{\mathbb{A}^n,p}$ generated by f_1, \dots, f_i is prime. Denote its intersection with $k[x_1, \dots, x_n]$ by \mathfrak{p}_i . This is also prime, of course. The elements of \mathfrak{p}_i vanish on a neighborhood of p in Y , hence vanish on all of Y (for Y is irreducible). Since \mathfrak{p}_i is strictly contained in \mathfrak{p}_{i+1} , we thus find a prime sequence of length $n-d$ in $I(Y)$: $(0) = \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_{n-d} \subset I(Y)$. As Y is irreducible of dimension d , there also exists a prime sequence of length d containing $I(Y)$ which begins with $I(Y)$: $I(Y) = \mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \dots \subsetneq \mathfrak{q}_d \subsetneq k[x_1, \dots, x_n]$. Since $k[x_1, \dots, x_n]$ has dimension n , these two prime sequences cannot make up a prime sequence of length $n+1$ and so we must have $\mathfrak{p}_{n-d} = \mathfrak{q}_0$. It follows that if $I(Y) = \mathfrak{p}_{n-d}$ is generated by h_1, \dots, h_s , then every h_i can be written as a $\mathcal{O}_{\mathbb{A}^n,p}$ -linear combination of f_1, \dots, f_{n-d} . If $g \in k[x_1, \dots, x_n]$ is a common denominator of these coefficients and the f_i 's (with $g(p) \neq 0$), then $Y \cap U(g)$ is clearly the common zero set of f_1, \dots, f_{n-d} . The locus of $q \in U(g)$ where $df_1(q), \dots, df_{n-d}(q)$ has rank $< n-d$ is defined by the vanishing of the $(n-d) \times (n-d)$ -minors and hence closed in $U(g)$. The complement U of this closed set has now all the asserted properties (with the last property following from Lemma 10.12).

The converse says that if U , p 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}_p in $\mathcal{O}_{\mathbb{A}^n,p}$ such that $\mathcal{O}_{\mathbb{A}^n,p}/\mathcal{I}_p$ is regular. This follows Lemma 10.12.

The last assertion is clear from the preceding. \square

PROPOSITION 10.14. *The regular points of a variety Y form an open and dense subset Y_{reg} of that variety. Equivalently: the singular points of Y form a proper closed subset $Y_{\text{sing}} = Y - Y_{\text{reg}}$ of Y .*

PROOF. We know already that Y_{reg} is open; we must show it is nonempty. Let $d := \dim Y$ so that $k(Y)$ is of transcendence degree d over k . This means that there exist algebraically independent $y_1, \dots, y_d \in k(Y)$ such that $k(Y)$ is a finite extension of the purely transcendental extension $K := k(y_1, \dots, y_d)$ of k . A basic result in field theory (the theorem of the primitive element) states that $k(Y)$ is generated over K by a single element. This means that if $f \in K[y]$ is its minimal polynomial, then $k(Y) \cong K[y]/(f)$. By clearing the denominators of the coefficients of f , we may assume that these all lie in $k[y_1, \dots, y_d]$, but have no common divisor. Then $f \in k[y_1, \dots, y_{d+1}]$ (we wrote y_{d+1} for y) is irreducible in $k[y_1, \dots, y_{d+1}]$ and defines an irreducible hypersurface Y' in \mathbb{A}^{d+1} with $k(Y') \cong k(Y)$ by construction. Since Y' contains an open subset isomorphic to an open subset of Y , it suffices to show that Y' has a regular point.

Let $p \in Y'$. A basis for $\mathfrak{m}_{\mathbb{A}^{d+1}, p} / \mathfrak{m}_{\mathbb{A}^{d+1}, p}^2$ is given by $dy_1(p), \dots, dy_{d+1}(p)$. This basis projects onto a generating set of the quotient space $\mathfrak{m}_{Y', p} / \mathfrak{m}_{Y', p}^2$ and since $\mathcal{I}_{Y', p} \subset \mathcal{O}_{\mathbb{A}^{d+1}, p}$ is generated by f , the only relation among them is $\sum_i \frac{\partial f}{\partial y_i}(p) dy_i(p) = 0$. Hence the dimension of $\mathfrak{m}_{Y', p} / \mathfrak{m}_{Y', p}^2$ fails to be d precisely when $\frac{\partial f}{\partial y_i}(p) = 0$ for all i . As this characterizes the property $p \in Y'_{\text{sing}}$, we must show that this cannot happen for all $p \in Y'$.

Suppose it does, i.e., suppose that every partial derivative $\partial f / \partial y_i$ of f vanishes on Y' . Then it lies in (f) and since $\partial f / \partial y_i$ has lower degree than f , this implies that $\partial f / \partial y_i$ is the zero polynomial. This is true for all i and so f is constant or (if $\text{char}(k) = p$) a p th power. The latter is excluded because f is irreducible and f constant is excluded because f has a positive degree in y_{d+1} . We thus get a contradiction. \square

REMARK 10.15. This enables us to find for a variety Y of dimension d a descending chain of closed subsets $Y = Y_d \supset Y_{d-1} \supset \dots \supset Y_0$ such that $\dim Y_i \leq i$ and all the (finitely many) connected components of $Y_i - Y_{i-1}$ are nonsingular subvarieties of dimension i (such a chain is called a *stratification* of Y). We let $Y_{d-1} := Y_{\text{sing}}$ and if (with downward induction) Y_i has been defined, and S_1, \dots, S_K are the distinct irreducible components of Y_i of dimension exactly i , then we take for Y_{i-1} the union of

- (i) the remaining irreducible components,
- (ii) the intersections $S_\kappa \cap S_\lambda$, with $\kappa \neq \lambda$ and
- (iii) the singular loci $(S_\kappa)_{\text{sing}}$.

Then $\dim Y_{i-1} \leq i - 1$ and every connected component of $Y_i - Y_{i-1}$ is a nonempty open subset of some $(S_\kappa)_{\text{reg}}$ and hence a nonsingular subvariety of dimension i .

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 much 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 $\phi : V \rightarrow V'$ such that for every $p \in P$, ϕ sends ℓ_p to ℓ'_p . (We are in fact saying that this 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}_k^n for $\mathbb{P}(k^{n+1})$ and call it simply *projective n -space (over k)*.

EXERCISE 36. 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 $f : P \rightarrow P'$ 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* $F : V \rightarrow V'$ 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 and describe its structure by a pair (V, ℓ) for which $V = k^{n+1}$. We denote the coordinates of k^{n+1} by (X_0, \dots, X_n) . Then every point $p \in \mathbb{P}(V)$ is representable as a ratio $[p_0 : \dots : p_n]$ 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, $[\lambda p_0 : \dots : \lambda p_n] = [p_0 : \dots : p_n]$. This is why $[X_0 : \dots : X_n]$ is called a *homogeneous coordinate system on $\mathbb{P}(V)$* even though the individual X_i are not functions on $\mathbb{P}(V)$ (but their ratios X_i/X_j are, albeit that they are not everywhere defined).

1.3. LINEAR CHARTS AND STANDARD ATLAS. Let $U \subset P$ be a *hyperplane complement* in $\mathbb{P}(V)$, 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 $V_H \subset V$. The cosets of V_H in V are affine hyperplanes in the classical sense of the word. If we take $A \neq V_H$, then assigning to $v \in A$ the 1-dimensional linear subspace spanned by v defines a bijection $\kappa_A : P - H \rightarrow A$. 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 $V_L \cap A$. We can restate this in more intrinsic terms by saying that any linear subspace of P meets U in an affine subspace of U .

If we choose a linear isomorphism $X : V \cong k^{n+1}$ such that V_H is given by $X_0 = 0$ and A by $X_0 = 1$, then (X_1, \dots, X_n) maps A bijectively onto k^n . Under this bijection $X_i|_A$ corresponds to the function X_i/X_0 on U and $(X_1/X_0, \dots, X_n/X_0) : U \cong k^n$ is an affine-linear isomorphism. We call such an isomorphism a *linear chart* for P .

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

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

is a chart with inverse $(x_1, \dots, x_n) \mapsto [x_1 : \dots : x_i : 1 : x_{i+1} : \dots : x_n]$. Notice that the U_i 's cover P . We call such a collection of charts $(U_i, \kappa_i)_{i=0}^n$ 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

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

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 $(x_1, \dots, x_n) \mapsto [1 : x_1 : \dots : x_n]$ with image the hyperplane complement defined by $X_0 \neq 0$.

2. The Zariski topology on a projective space

We shall define a topology on a projective space whose restriction to every linear chart is a homeomorphism if we endow \mathbb{A}^n with the Zariski topology.

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 . Then we have $F(\lambda X_0, \dots, \lambda X_n) = \lambda^d F(X_0, \dots, X_n)$ 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-DEFINITION 2.1. *The collection U_F , where F runs over the homogeneous polynomials in $k[X_0, \dots, X_n]$, is a basis for a topology on P , called 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. Let \mathcal{O}_P be the sheaf of ring of k -valued functions on P which on every hyperplane complement is its sheaf of regular functions. Then (P, \mathcal{O}_P) is a prevariety¹.*

PROOF. The first statement 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 $[X_0, \dots, X_n]$ such that U is defined by $X_0 \neq 0$ and denote by $j : \mathbb{A}^n \cong U$, $(x_1, \dots, x_n) \mapsto [1 : x_1 : \cdots : x_n]$ the inverse. If $F \in k[X_0, \dots, X_n]$ is homogeneous, then $j^{-1}U_F = U(f)$, where $f(x_1, \dots, x_n) := F(1, x_1, \dots, x_n)$. So the inclusion j is continuous.

Conversely, if $f \in k[x_1, \dots, x_n]$ is nonzero of degree d , then its 'homogenization' $F(X_0, \dots, X_n) := X_0^d f(X_1/X_0, \dots, X_n/X_0)$ is homogeneous of degree d and $U(f) = j^{-1}U_F$. So j is also open.

The coordinate system $[X_0, \dots, X_n]$ determines $n + 1$ charts $\{(U_i, \kappa_i)\}_{i=0}^n$ for P which cover P . We already observed that coordinate changes $\kappa_j \kappa_i^{-1}$ are isomorphisms of affine varieties and thus P acquires the structure of a prevariety. It is easy to verify that this is independent of any choices. \square

EXERCISE 37. Let $F \in k[X_0, \dots, X_n]$ be nonzero and homogeneous of degree d .

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

We now discuss the projective analogue of the (affine) $I - Z$ correspondence.

Any $F \in k[X_0, \dots, X_n]$ is uniquely written as a sum of homogeneous polynomials: $F = F_0 + F_1 + F_2 + \cdots$ (with of course only a finite number of nonzero terms): the term F_d is simply the coefficient of t^d in $F(tX_0, \dots, tX_n) \in k[X_0, \dots, X_n, t] = k[X_0, \dots, X_n][t]$. We call F_d the d th homogeneous part of F . This makes $k[X_0, \dots, X_n]$ a graded ring in the sense below.

DEFINITION 2.2. A graded ring is a ring R whose underlying additive group comes with a direct sum decomposition $R_\bullet = \bigoplus_{k=0}^{\infty} R_k$ such that the ring product

¹We will shortly see that (P, \mathcal{O}_P) is in fact a variety.

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 $R/I = \bigoplus_{d=0}^{\infty} R_d/I_d$ is again a graded ring. Of special interest is the homogeneous ideal that is maximal among the proper homogeneous ideals, $R_+ := \bigoplus_{k=1}^{\infty} R_k$, for which we have $R/R_+ = R_0$.

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} .*

We omit the easy proofs.

A proper homogeneous ideal $J \subset k[X_0, \dots, X_n]_+$ defines a closed subset

$$Z_J = \bigcap \{Z_F : F \in \bigcup_{d \geq 0} J_d\}.$$

of \mathbb{P}^n . Since $k[X_0, \dots, X_n]$ is noetherian, J has finitely many generators. By taking the homogeneous parts of these generators we find in fact that J has a finite set of homogeneous generators. It is easy to see that Z_J is their common zero set. Its relation with the closed subset $Z(J) \subset k^{n+1}$ is quite simple: $Z(J)$ is homogeneous in the sense that if $x \in Z(J)$, then $tx \in Z(J)$ for all $t \in k$, in fact, $Z(J)$ is the union of one dimensional subspaces of k^{n+1} parametrized by Z_J (here $Z_J = \emptyset$ corresponds to $Z(J) = \{0\}$).

Conversely, a subset $Y \subset \mathbb{P}^n$ determines a proper homogeneous ideal $I(Y)$ in the ideal $k[X_0, \dots, X_n]_+$, with its degree $d \geq 1$ -summand $I(Y)_d$ being the vector space of homogeneous polynomials F of degree d which vanish on Y (i.e., for which $Z_F \supset Y$). Notice that with this definition we have $I(\emptyset) = k[X_0, \dots, X_n]_+$.

PROPOSITION 2.4. *If $J \subset k[X_0, \dots, X_n]_+$ is a proper homogeneous ideal, then $I(Z_J) = \sqrt{J}$.*

PROOF. We have $I(Z(J)) = \sqrt{J}$ by the Nullstellensatz, and so it suffices to prove that $I(Z_J) = I(Z(J))$. Clearly, $I(Z_J) \supset I(Z(J))$. Since $J \subset k[X_0, \dots, X_n]_+$, $0 \in Z(J)$ and so $F \in k[X_0, \dots, X_n]$ vanishes on $Z(J)$, then F has no constant term. As $Z(J)$ is invariant under scalar multiplication, $F(tX_0, \dots, tX_n) = \sum_{d \geq 1} t^d F_d(X_0, \dots, X_n)$ vanishes on $Z(J) \times \mathbb{A}^1$ so that $F_d \in Z(J)$ for all d . It follows that $I(Z(J)) \subset I(Z_J)$. \square

EXERCISE 38. Let R_{\bullet} be a graded ring.

- Prove that the set of its zero divisors is a homogeneous ideal. The same for its ideal of nilpotents.
- 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.
- Prove that the intersection of all homogeneous prime ideals of R_{\bullet} is its ideal of nilpotents.

EXERCISE 39. Prove that a closed subset $Y \subset \mathbb{P}^n$ is irreducible if and only if $I(Y)$ is a prime ideal.

Since $k[X_0, \dots, X_n]$ is a noetherian ring, any ascending chain of homogeneous ideals in this ring stabilizes. This implies that any projective space is noetherian. In particular, every subset of a projective space has a finite number of irreducible components whose union is all of that subset.

DEFINITION 2.5. The *homogeneous coordinate ring* of a closed subset Y of \mathbb{P}^n is the graded ring

$$S(Y)_\bullet := k[X_0, \dots, X_n]/I(Y), \quad S(Y)_d = k[X_0, \dots, X_n]_d/I(Y)_d.$$

Notice that $S(Y)_\bullet$ is a reduced finitely generated k -algebra and that $S(Y)_0 = k$. The following exercise shows that every such algebra so arises:

EXERCISE 40. Let S_\bullet be a graded k -algebra that is reduced, finitely generated and has $S_0 = k$.

- Prove that S_\bullet is a graded k -algebra isomorphic to the homogeneous coordinate ring of a closed subset Y .
- Prove that under such an isomorphism, the homogeneous radical ideals contained in the maximal ideal $S_+ := \bigoplus_{d \geq 1} S_d$ 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 .
- 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 41. Let Y be an affine variety.

- 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.
- Prove that every closed subset of $Y \times \mathbb{P}^n$ is an intersection of finitely many zero set of homogeneous elements of $A(Y)[X_0, \dots, X_n]$.
- 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 projective variety. This will imply among other things that projective space is a variety. Consider the projective spaces \mathbb{P}^m and \mathbb{P}^n with their homogeneous coordinate systems $[X_0 : \dots : X_m]$ and $[Y_0 : \dots : Y_n]$. We also consider a projective space whose homogeneous coordinate system is the set of matrix coefficients of an $(m+1) \times (n+1)$ -matrix $[Z_{00} : \dots : Z_{ij} : \dots : Z_{mn}]$; this is just \mathbb{P}^{mn+m+n} with an unusual indexing of its homogeneous coordinates.

PROPOSITION 3.1 (The Segre embedding). *The map $f : \mathbb{P}^m \times \mathbb{P}^n \rightarrow \mathbb{P}^{mn+m+n}$ 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 $\mathbb{P}^n \times \mathbb{P}^n$ is the preimage of the linear subspace of \mathbb{P}^{n^2+2n} defined by $Z_{ij} = Z_{ji}$ and hence is closed in $\mathbb{P}^n \times \mathbb{P}^n$.*

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 the domain of the product of two standard charts 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, $f : f^{-1}U_{00} \rightarrow U_{00}$ 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 $\mathbb{A}^n \times \mathbb{A}^m \rightarrow \mathbb{A}^{nm}$ with coordinates $x_i y_j$, $1 \leq i \leq n$, $1 \leq j \leq m$. This graph is closed in $\mathbb{A}^n \times \mathbb{A}^m \times \mathbb{A}^{nm}$ and isomorphic to $\mathbb{A}^n \times \mathbb{A}^m$. 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 $0 \leq i < j \leq n$ implies that $[X_0 : \dots : X_n] = [Y_0 : \dots : Y_n]$, assuming that not all X_i resp. Y_j are zero. If $X_i \neq 0$, then we cannot have $Y_i = 0$, because $X_i Y_j = X_j Y_i$ would then imply that $Y_j = 0$ for every j . So $Y_i \neq 0$. Let $t := Y_i/X_i \in k^\times$ so that $Y_i = tX_i$. Substituting this in $X_i Y_j = X_j Y_i$ yields in $Y_j = tX_j$ for all j and so $[Y_0 : \dots : Y_n] = [X_0 : \dots : X_n]$. \square

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

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

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 it 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 9.15 and the second from Proposition 3.1. \square

- EXERCISE 42.**
- (a) Prove that the image of the Segre embedding is the common zero set of the homogenous 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 $\mathbb{P}^{m+n+m+n}$ is a linear subspace.
 - (c) Prove that the map $\mathbb{P}^n \rightarrow \mathbb{P}^{(n^2+3n)/2}$ defined by $Z_{ij} = X_i X_j$, $0 \leq i \leq j \leq n$ 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 $Z_0 Z_1 - Z_2 Z_3 = 0$ is isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$. Identify in this case the two systems of lines on this quadric.

EXERCISE 43 (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 $\mathbb{P}(V) \times \mathbb{P}(W) \rightarrow \mathbb{P}(V \otimes W)$.

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 $\pi : V \rightarrow V/W$. We cannot projectivize this as a morphism from $\mathbb{P}(V)$ to $\mathbb{P}(V/W)$, but we shall see that if $W \neq V$, then it defines at least a morphism $\mathbb{P}(V) - \mathbb{P}(W) \rightarrow \mathbb{P}(V/W)$. As a map it 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 let the image of p in $\mathbb{P}(V/W)$ be represented the latter. To see that this is morphism, we choose a coordinate system (X_0, \dots, X_n) for V

such that W is given by $X_0 = \cdots = X_m = 0$. Then (X_0, \dots, X_m) serves as a coordinate system for V/W and $\pi : V \rightarrow V/W$ is simply given by $(X_0, \dots, X_n) \rightarrow (X_0, \dots, X_m)$. In projective coordinates this is of course given by $[X_0 : \cdots : X_n] \rightarrow [X_0 : \cdots : X_m]$ and so indeed a morphism where it is defined (namely where X_0, \dots, X_m not all vanish, that is, on the complement of $\mathbb{P}(W)$).

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 and has dimension one more than W and that every such subspace so arises. So the linear subspaces of $\mathbb{P}(V)$ containing $\mathbb{P}(W)$ having dimension one more than $\mathbb{P}(W)$ form a projective space (which can be identified with $\mathbb{P}(V/W)$).

This projective structure on this collection of linear subspaces is intrinsic. This means that if P is a projective space and $Q \subset P$ is a linear subspace of codimension $m > 0$, then the collection of linear subspaces of P which contain Q and have dimension one more than Q is in a natural manner a projective space of dimension $m - 1$. We denote that projective space by P_Q . The morphism described above should go from $P - Q$ to P_Q . As a map it simply assigns to $p \in P - Q$ the point of P_Q represented by the *projective linear span* of p and Q (i.e., the smallest linear subspace containing p and Q). We denote this morphism $\pi_Q : P - Q \rightarrow P_Q$. It is clearly surjective.

EXERCISE 44. Show that every fiber of π_Q is in a natural manner an affine space of dimension one more than the dimension of Q .

We define the *blowup of P along Q* as the closure of the graph of π_Q in $P \times P_Q$ and denote it by $\text{Bl}_Q P$ (we will later discuss this notion in greater generality). This is a closed subset of $P \times P_Q$ which contains a copy of $P - Q$ as an open dense subset. So $\text{Bl}_Q P$ is a projective variety. The projection $\text{Bl}_Q P \rightarrow P_Q$ extends π_Q and is called the *projection from Q* . As long there is no danger of confusion we continue to denote it by π_Q .

LEMMA 4.1. *The morphism $\pi_Q : \text{Bl}_Q P \rightarrow P_Q$ is a locally trivial fibration in projective spaces of dimension $1 + \dim Q$. More precisely, if $U \subset P_Q$ is hyperplane complement, then there is a morphism $\rho : \pi_Q^{-1}U \rightarrow \mathbb{P}^{1+\dim Q}$ so that the morphism $(\pi_Q, \rho) : \pi_Q^{-1}U \rightarrow U \times \mathbb{P}^{1+\dim Q}$ is an isomorphism. In particular, $\text{Bl}_Q P$ is nonsingular.*

PROOF. Choose a homogeneous coordinate system $[X_0 : \cdots : X_n]$ for P as above and denote the corresponding coordinate system for P_Q by $[Y_0 : \cdots : Y_m]$. Since π_Q is on $P - Q$ given by $Y_i = X_i$, the graph of this map in $(P - Q) \times P_Q$ is given by $[X_0 : \cdots : X_m] = [Y_0 : \cdots : Y_m]$, or equivalently, by $X_i Y_j - X_j Y_i = 0$ for $0 \leq i < j \leq m$. These equations define a closed subspace $Z \subset P \times P_Q$ which contains the graph in question. We show that Z is the closure of the graph and has the required properties. For this we focus on the second part of the lemma and assume (without loss of generality) that U is given by $Y_0 \neq 0$. We use on U the standard coordinates $y_i = Y_i/Y_0$, $i = 1, \dots, m$. Then $Z_U := Z \cap (P \times U)$ is given by $X_i y_j - X_j y_i = 0$ for $0 \leq i < j \leq m$, where we should read 1 for y_0 . This amounts to $X_i = y_i X_0$ for $i = 1, \dots, m$. So if we define $\rho : Z_U \rightarrow \mathbb{P}^{1+n-m}$, by $([X_0 : \cdots : X_n], y_1, \dots, y_m) \rightarrow [X_0 : X_{m+1} : \cdots : X_n]$, then the resulting map $Z_U \rightarrow U \times \mathbb{P}^{1+n-m}$ is invertible with inverse $(y_1, \dots, y_m, [X_0 : X_{m+1} : \cdots : X_n]) \mapsto [X_0 : y_1 X_0 : \cdots : y_m X_0 : X_{m+1} : \cdots : X_n]$. Under this isomorphism the intersection

of Z_U with the graph of π_Q is mapped to open subset $U \times U_0 \subset U \times \mathbb{P}^{1+n-m}$. Since this is dense in $U \times \mathbb{P}^{1+n-m}$, it follows that $Z_U \subset \text{Bl}_Q P$. So $Z \subset \text{Bl}_Q P$ and hence $Z = \text{Bl}_Q P$. \square

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 $K \times Y \rightarrow Y$ is closed for every Y . In this sense the following theorem states a kind of compactness property for projective varieties.

THEOREM 4.2. *Let X be a projective variety. Then for every variety Y , the projection $X \times Y \rightarrow Y$ is closed.*

We first reduce this theorem to the case where $X = \mathbb{P}^1$, Y affine and then show that it is for this case a consequence of the main theorem of elimination theory.

REDUCTION TO THE CASE $X = \mathbb{P}^1$ AND Y AFFINE. We must prove that for every closed subset $Z \subset X \times Y$ the projection $\pi_Y(Z)$ is closed in Y . For this it suffices to verify that for every open affine subset $U \subset Y$, $\pi_Y(Z) \cap U$ is closed in U . Since $\pi_Y(Z) \cap U = \pi_U(Z \cap (X \times U))$ we may assume that Y is affine.

Since X projective, we may assume it to be a closed subset of some projective space P . With induction on $\dim P$ we reduce to the case $\dim P = 1$. If $\dim P \geq 2$, we choose a singleton $Q \subset P$ and consider the blowup $\text{Bl}_Q P \rightarrow P$. The preimage \tilde{Z} of Z in $\text{Bl}_Q P \times Y$ is closed and since $\text{Bl}_Q P \rightarrow P$ is surjective, it is enough to show that the image of \tilde{Z} in Y is closed. In other words, we must show that $\text{Bl}_Q P \times Y \rightarrow Y$ is closed. We factor this projection as $\text{Bl}_Q P \times Y \rightarrow P_Q \times Y \rightarrow Y$. Since P_Q is a projective space of dimension one less than P , the second projection is closed by induction. So it is enough to see that the first projection is closed. Now $\text{Bl}_Q P \rightarrow P_Q$ is locally trivial fibration in projective lines (P_Q is covered by affine open subsets U over which the morphism $\text{Bl}_Q P \rightarrow P_Q$ is isomorphic to $U \times \mathbb{P}^1 \rightarrow U$) and hence the same is true for $\text{Bl}_Q P \times Y \rightarrow P_Q \times Y$. This proves that it suffices to verify the theorem for $X = \mathbb{P}^1$. \square

We shall now state the main result of elimination theory. Given an integer $n \geq 0$, denote by P_n the k -vector space of homogeneous polynomials $F \in k[X_0, X_1]$ of degree n . The monomials $(X_0^{n-i} X_1^i)_{i=0}^n$ form a basis, in particular, $\dim P_n = n + 1$. Given $F \in P_m$ and $G \in P_n$, then the map

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

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 $P_{n-1} \oplus P_{m-1}$ and of P_{n+m-1} . So $R(F, G) = 0$ if and only if $u_{F,G}$ fails to be injective.

LEMMA 4.3. *$R(F, G) = 0$ 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 $(A, B) \in P_{n-1} \oplus P_{m-1}$ 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 $(G_1, -F_1) \in P_{n-1} \oplus P_{m-1}$ is nonzero and in the kernel of $u_{F,G}$. \square

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

$$R(F, G) = \det \begin{pmatrix} f_0 & f_1 & \cdots & f_m & 0 & \cdots & \cdots & 0 \\ 0 & f_0 & f_1 & \cdots & f_m & \cdots & \cdots & 0 \\ 0 & 0 & f_0 & & & & \cdots & 0 \\ & & & \cdots & & & & \\ 0 & 0 & \cdots & 0 & f_0 & f_1 & \cdots & f_m \\ g_0 & g_1 & \cdots & \cdots & g_n & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & \cdots & g_n & 0 \cdots & 0 \\ 0 & 0 & g_0 & & & & \cdots & 0 \\ & & & \cdots & & & & \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & \cdots & g_n \end{pmatrix}$$

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

PROOF OF THEOREM 4.2 IN CASE $X = \mathbb{P}^1$ AND Y AFFINE. Let $Z \subset \mathbb{P}^1 \times Y$ be closed. Denote by $I(Z)_\bullet$ the homogeneous ideal in the graded algebra $A(Y)[X_0, X_1]$ of functions vanishing on Z . Then Z is the common zero set of the members of $I(Z)_\bullet$ (see Exercise 41). For every homogeneous pair $F, G \in \cup_m A(Y)[X_0, X_1]_m$, we can form the resultant $R(F, G) \in A(Y)$. We claim that $\pi_Y(Z)$ is the common zero set $R \subset Y$ of the $R(F, G)$, with $F, G \in \cup_m I(Z)_m$. This will certainly prove that $\pi_Y(Z)$ is closed in Y .

Suppose that $y \in \pi_Y(Z)$ so that $(y, [X_0 : X_1]) \in Z$ for some $[X_0 : X_1] \in \mathbb{P}^1$. Then $[X_0 : X_1]$ 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 $y \in R$.

If $y \notin \pi_Y(Z)$, then in particular $\{y\} \times \mathbb{P}^1$ is not contained in Z , so that there exists a $F \in \cup_m I(Z)_m$ with $F_y \neq 0$. Denote by $p_1, \dots, p_r \in \mathbb{P}^1$ the distinct zeroes of F_y . Since $(y, p_i) \notin Z \cup \cup_{j \neq i} \{(y, p_j)\}$, there exists a $G^{(i)} \in \cup_m I(Z)_m$ with $G_y^{(i)}$ zero in all the p_j with $j \neq i$ and nonzero in p_i . By replacing each $G^{(i)}$ by some power, we may assume that $G^{(1)}, \dots, G^{(r)}$ all have the same degree. Then $G := G^{(1)} + \cdots + G^{(r)} \in \cup_m I(Z)_m$ and F_y, G_y have no common zero in \mathbb{P}^1 . This means that $R(F_y, G_y) \neq 0$ and so $y \notin R$. \square

We mention a few corollaries.

COROLLARY 4.4. *Let X be a projective variety. Then any morphism from X to a variety has closed image.*

PROOF. If $f : X \rightarrow Y$ is a morphism to a variety Y , then the graph $\Gamma_f \subset X \times Y$ is closed in $X \times Y$. According to Theorem 4.2, the projection $\pi_Y(\Gamma_f)$ is then closed in Y . But it is clear that $\pi_Y(\Gamma_f) = f(Y)$. \square

It is an elementary result from complex function theory that a holomorphic function on the Riemann sphere is constant. This implies the corresponding assertion for holomorphic functions on complex projective n -space $\mathbb{P}_{\mathbb{C}}^n$ (to see that a holomorphic function on $\mathbb{P}_{\mathbb{C}}^n$ 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 4.5. *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. We first prove the special case. A regular function ϕ on X can be regarded as a morphism $f : X \rightarrow \mathbb{A}^1$. We think of \mathbb{A}^1 as the complement of the single point $[1 : 0]$ in \mathbb{P}^1 . So the resulting morphism $X \rightarrow \mathbb{P}^1$ has image contained in $\mathbb{A}^1 \subset \mathbb{P}^1$. By the previous corollary this image is closed in \mathbb{P}^1 and so must be finite. Since X is irreducible, it follows that the image is a singleton. In other words, ϕ is constant.

If $f : X \rightarrow Y$ 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 . These are all constant and hence f is constant. \square

EXERCISE 45. Let P be a projective space, $Q \subset P$ a linear subspace and $Y \subset P - Q$ irreducible and closed in P . Prove that the restriction of $\pi_Q : P - Q \rightarrow P_Q$ to Y has finite fibers and that $\pi_Q(Y)$ is closed in P_Q . Assuming that this implies that $k(Y)$ is a finite extension of $k(\pi_Q(Y))$, deduce that $\dim Y$ must be smaller than the codimension of Q in P .

EXERCISE 46. Regard \mathbb{A}^n as the standard open subset of \mathbb{P}^n (defined by $X_0 \neq 0$) and denote by $\mathbb{P}_\infty \subset \mathbb{P}^n$ its complement (defined by $X_0 = 0$).

- (i) Show that a linear subspace $Q \subset \mathbb{P}_\infty$ of dimension k determines a linear subspace $L_Q \subset \mathbb{A}^n$ of dimension $k+1$ (strictly speaking, up to translation) and that the projection π_Q restricted to \mathbb{A}^n is isomorphic to the projection $\mathbb{A}^n \rightarrow \mathbb{A}^n/L_Q$.
- (ii) Let now $Y \subset \mathbb{A}^n$ be irreducible and closed and $Y \not\subset \mathbb{A}^n$. Prove that there is a line $L \subset \mathbb{A}^n$, such that the projection $\mathbb{A}^n \rightarrow \mathbb{A}^n/L$ restricted to Y is closed and has finite fibers. (Hint: use Exercise 45.)
- (iii) Prove that there exists a linear surjection $\mathbb{A}^n \rightarrow \mathbb{A}^{\dim Y}$ whose restriction to Y is closed and has finite fibers. (This is a form of what is known as the *Noether normalization lemma*.)

EXERCISE 47. 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 48. Let $F \in k[X_0, \dots, X_n]_d$ define a nonsingular hypersurface H in \mathbb{P}^n . Prove that the map $H \rightarrow \check{\mathbb{P}}^n$ which assigns to $p \in H$ the projective 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 $d = 2$?

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 4.6. Consider the morphism $f : \mathbb{A}^2 \rightarrow \mathbb{A}^2$, $(x_1, x_2) \mapsto (x_1, x_1 x_2)$. 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 4.7. A subset of variety is called *constructible* if it can be written as the union of finitely many (locally closed) subvarieties.

THEOREM 4.8. *Let $f : X \rightarrow Y$ 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 4.9. *Let $f : X \rightarrow Y$ 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 4.9 IMPLIES THEOREM 4.8. A constructible subset is a finite union of subvarieties and so it is clearly enough to prove that the image of subvariety of X is constructible. In other words, it suffices to show that the image of a morphism $f : X \rightarrow Y$ of varieties is constructible. We prove this with induction on the dimension of X . According to Proposition 4.9 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. \square

PROOF OF PROPOSITION 4.9. Since X is covered by finitely many of its open affine subsets, we may without loss of generality assume that X is affine: X closed in some \mathbb{A}^n . By identifying X with the graph of f in $\mathbb{A}^n \times Y$, we see that we 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 in the ‘line projections’ $\mathbb{A}^{k+1} \times Y \rightarrow \mathbb{A}^k \times Y$, $k = 1, \dots, n-1$, it is enough to do the case $n = 1$. It is also enough to prove this over an affine subset of Y and so we may in addition assume that Y is affine. 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 .

If $X = \mathbb{A}^1 \times Y$, 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 $a_i \in A(Y)$, $a_N \neq 0$ ($N > 0$). We prove that $\pi_Y(X)$ contains the nonzero set $U := U(a_N)$ of a_N .

The equation $F(X_0, X_1, y) = \sum_{i=0}^N a_i(y)X_0^{N-i}X_1^i$ defines a closed subset Z_F of $\mathbb{P}^1 \times Y$. Let $([X_0 : X_1], y) \in Z_F$. If $X_0 = 0$, then we must have $a_N(y) = 0$ (so that $y \notin U$) and if $X_0 \neq 0$, then $([X_0 : X_1], y) \in Z(f)$. So $Z(f) \cap (\mathbb{A}^1 \times U)$ is closed in $\mathbb{P}^1 \times U$, and hence so is $X \cap (\mathbb{A}^1 \times U)$. It follows that $\pi_Y(X) \cap U$ is closed in U . Since $\pi_Y(X)$ is also dense in Y , it follows that $\pi_Y(X) \supset U$. \square

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 $d_\bullet = (d_0, \dots, d_n)$ with sum d . They are $\binom{n+d}{d}$ in number.

PROPOSITION 4.10 (The Veronese embedding). *The map $f_d : \mathbb{P}^n \rightarrow \mathbb{P}^{\binom{n+d}{d}-1}$ defined by $Z_{d_\bullet} = X_0^{d_0} \cdots X_n^{d_n}$ 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_{d_\bullet} of the standard atlas of the target space $f_d^{-1}U_{d_\bullet}$ is open in \mathbb{P}^n and is mapped by f_d isomorphically onto a closed subset of U_{d_\bullet} . The preimage of U_{d_\bullet} in \mathbb{P}^n 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 $f_d^{-1}U_{d_\bullet} = U_0 \cap \cdots \cap U_r \subset U_0$. So if we use the standard coordinates (x_1, \dots, x_n) on U_0 , then $f_d^{-1}U_{d_\bullet}$ is defined by $x_1 \cdots x_r \neq 0$.

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

$$f_d : f_d^{-1}U_{d_\bullet} \rightarrow U_{d_\bullet}, \quad z_{e_\bullet - d_\bullet} = x_1^{e_1 - d_1} \cdots x_n^{e_n - d_n} \quad (e_\bullet \neq d_\bullet).$$

So its components are the nonconstant Laurent monomials $x_1^{k_1} \cdots x_n^{k_n}$ of total degree $\leq d_0$ with $k_i \geq -d_i$. We see that each x_i appears as a component, and if $d_\bullet \neq (d, 0, \dots, 0)$, then so does the Laurent monomial $y := x_1^{-d_1} \cdots x_r^{-d_r}$. Since all other components are products of these monomials, the image of this restriction is the graph of a morphism defined on the closed hypersurface $yx_1^{d_1} \cdots x_r^{d_r} = 1$ in \mathbb{A}^{n+1} ($d_\bullet \neq (d, 0, \dots, 0)$) or on \mathbb{A}^n ($d_\bullet = (d, 0, \dots, 0)$). So we get a closed embedding. \square

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

PROPOSITION 4.11. *Let $H \subset \mathbb{P}^n$ be a hypersurface. Then $\mathbb{P}^n - H$ is affine and for every closed subset $Z \subset \mathbb{P}^n$ of positive dimension, $Z \cap H$ is nonempty and of dimension $\geq \dim(Z) - 1$. If Z is irreducible and not contained in H , then $\dim(Z \cap H) = \dim(Z) - 1$.*

In the last case it is even true that every irreducible component of $Z \cap H$ has dimension $\dim(Z) - 1$. The proof is based on:

The proof uses:

LEMMA 4.12. *Let P be a projective space, $Z \subset P$ be closed subset, and i a non-negative integer with $i + \dim(Z) < \dim(P)$. Then there exists an i -plane in \mathbb{P}^n which does not meet Z .*

PROOF. We may (and will) assume that Z is irreducible. If $i = 0$, then we must have $\dim(Z) < \dim(P)$ and so $Z \neq P$. In that case any singleton in $P - Z$ is as required. We next proceed with induction on i . So we can assume $i > 0$ and that there exists a $(i - 1)$ -plane $Q \subset \mathbb{P}^n$ which does not meet Z . Then projection from Q defines a morphism $\pi : Z \rightarrow P_Q$ from Z to a projective space of dimension $\dim(P) - i$. Any fiber of this map is an intersection of Z with an i -plane in P 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, $\dim(Z) \geq \dim(P_Q) = \dim(P) - i$, which evidently contradicts our assumption that $i + \dim(Z) < \dim(P)$. \square

PROOF OF PROPOSITION 4.11. The hypersurface H is given by a homogeneous polynomial of degree d , say by $\sum_{d_\bullet} c_{d_\bullet} X_0^{d_0} \cdots X_n^{d_n}$. This determines a hyperplane $\tilde{H} \subset \mathbb{P}^{\binom{n+d}{d}-1}$ defined by $\sum_{d_\bullet} c_{d_\bullet} Z_{d_\bullet}$. It is clear that H is the preimage of \tilde{H} under the Veronese morphism and so 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 there exists a plane $Q \subset H$ of dimension $\dim(H) - (\dim(Z) - 2) - 1 = \dim(P) - \dim(Z)$ which avoids $Z \cap H$. But if we regard Q as a plane in P which avoids Z , we contradict Lemma 4.12. This proves that $\dim(Z \cap H) \geq \dim(Z) - 1$. If Z is irreducible and not contained in H , then we have also $\dim(Z \cap H) \leq \dim(Z) - 1$. \square

EXERCISE 49. 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 $F(X, Z) := \sum_{d \bullet} Z_{d \bullet} X_0^{d_0} X_1^{d_1} \cdots X_n^{d_n}$. We denote it by H and let $\pi : H \rightarrow \mathbb{P}^{\binom{n+d}{d}-1}$ be the projection.

- Prove that H is nonsingular.
- 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 if the partial derivatives of $F_Z \in k[X_0, \dots, X_n]$ have X as a common zero.
- 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 $n + 1$.
- 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 .
- 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 $\det(Z_{ij})$.

5. Grassmannians

Let P be a projective space of dimension n and let $d \in \{0, \dots, n\}$. We want to show that the collection $\text{Gr}_d(P)$ of linear d -dimensional subspaces of P is a nonsingular projective variety. Let the projective structure on P be defined the pair (V, ℓ) .

LEMMA 5.1. *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 $W \subset P$. Notice that $\dim V = n + 1$ and $\dim W = n - d$. 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 $L_0 \rightarrow W$ and vice versa. So this identifies A_Q with $\text{Hom}(L_0, W)$. It is easy to verify that this affine structure is independent of the choices. \square

We recall that the exterior algebra $\bigwedge^\bullet V = \bigoplus_{p=0}^\infty \bigwedge^p V$ is the quotient of the tensor algebra on V , $\bigoplus_{p=0}^\infty V^{\otimes p}$ (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, \dots, e_n is a basis for V , then a basis of $\bigwedge^p V$ is indexed by the p -element subsets $I \subset \{0, \dots, n\}$:

$I = \{0 \leq i_1 < i_2 < \cdots < i_p \leq n\}$ is associated to the basis element $e_I = e_{i_1} \wedge \cdots \wedge e_{i_p}$ (where the convention is that $e_\emptyset = 1 \in k = \wedge^0 V$). So $\dim \wedge^p V = \binom{n+1}{p}$. Notice that $\wedge^{n+1} V$ is one-dimensional and spanned by $e_0 \wedge \cdots \wedge e_n$, whereas $\wedge^p V = 0$ for $p > n + 1$.

LEMMA 5.2. *Let $\alpha \in \wedge^p V$ 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 spans $\wedge^p K(\alpha)$.*

PROOF. Let e_1, \dots, 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

$$\wedge^p V = \bigoplus_{I \subset \{1, \dots, r\}} e_I \wedge \wedge^{p-|I|} V'.$$

Wedging with e_i kills all the summands in which e_i appears and is injective on the sum of the others. So $K(\alpha) \subset e_1 \wedge \cdots \wedge e_r \wedge \wedge^{p-r} V'$. It follows that $r \leq p$ with equality if and only if α is a multiple of $e_1 \wedge \cdots \wedge e_p$. \square

If L is a linear subspace of V of dimension $d + 1$, then $\wedge^{d+1} L$ is of dimension 1 and will be thought of as a one dimensional subspace of $\wedge^{d+1} V$. We thus have defined the so-called *Plücker embedding*:

$$\delta : \text{Gr}_d(P) \rightarrow \mathbb{P}(\wedge^{d+1} V), \quad [L] \mapsto [\wedge^{d+1} L].$$

PROPOSITION 5.3. *The Plücker embedding maps $\text{Gr}_d(P)$ bijectively onto a closed subset of $\mathbb{P}(\wedge^{d+1} V)$.*

PROOF. Let $\alpha \in \wedge^{d+1} V$. According to Lemma 5.2, $[\alpha]$ 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

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

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

Proposition 5.3 almost gives $\text{Gr}_d(P)$ the structure of projective variety (we have not proved irreducibility yet). 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 $\beta \in \wedge^{n-d} W$. Then wedging with β defines a nonzero linear map

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

So e_β defines a hyperplane in $\mathbb{P}(\wedge^{d+1} V)$ and hence an affine subspace $U_Q \subset \mathbb{P}(\wedge^{d+1} V)$.

LEMMA 5.4. *The preimage of U_Q 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 $V = L \oplus W$ and it is then easily seen (by picking a compatible basis of V for example) that $\alpha \wedge \beta \neq 0$. This implies that $\delta^{-1}U_Q = A_Q$.

Let us now express the restriction $\delta : A_Q \rightarrow U_Q$ in terms of coordinates. Choose a basis e_0, \dots, e_n for V such that e_{d+1}, \dots, e_n is a basis for W and $\beta = e_{d+1} \wedge \dots \wedge e_n$. Then e_β simply assigns to an element α of $\bigwedge^{d+1} V$ the coefficient of $e_0 \wedge \dots \wedge e_d$ in α . If $L_0 \subset V$ denotes the span of e_0, \dots, e_d , then $A_Q \cong \text{Hom}(L_0, W)$ 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

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

The coefficient of $e_{i_0} \wedge \dots \wedge e_{i_d}$ 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 as the matrix coefficient of $e_0 \wedge \dots \wedge \widehat{e_i} \wedge \dots \wedge e_d \wedge e_j$. 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_Q . \square

COROLLARY 5.5. *The Plücker embedding realizes $\text{Gr}_d(P)$ 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 have nonempty intersection and so $\text{Gr}_d(P)$ is irreducible. The rest follows from the previous corollary. \square

REMARK 5.6. The image of $\text{Gr}_d(P)$ is an orbit of the natural $\text{SL}(V)$ -action on $\mathbb{P}(\bigwedge^{d+1} V)$.

EXERCISE 50. Let P be a projective space. Given integers $0 \leq d < e \leq \dim P$, 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 $\text{Gr}_d(P) \times \text{Gr}_e(P)$.

The Grassmannian of hyperplanes in a projective space is itself a projective space (see Exercise 47). 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 $F : \bigwedge^2 V \rightarrow k$ 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, \dots, e_4 is a basis for V , then $(e_i \wedge e_j)_{1 \leq i < j \leq 4}$ 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

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

Notice that F is irreducible. Its partial derivatives are the coordinates themselves (up to sign and order) and so F defines a smooth hypersurface.

PROPOSITION 5.7. *The zero set of F is nonsingular and equal to the image of the Plücker embedding of $G_1(\mathbb{P}(V))$ in $\mathbb{P}(\bigwedge^2 V)$.*

PROOF. The image of the Plücker embedding is of dimension 3 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, \dots, 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 . \square

REMARK 5.8. One can prove directly (with a little bit of linear algebra) that if $\alpha \in \bigwedge^2 V$ is such that $\alpha \wedge \alpha = 0$, then $e_\alpha : V \rightarrow \bigwedge^3 V$ has rank ≤ 2 . In fact, a similar argument will show that the image of a general Plücker embedding is the common zero set of a collection of quadratic equations.

PROPOSITION-DEFINITION 5.9. *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 $\text{Gr}_d(P)$, called the Fano variety (of d -planes) of X .*

PROOF. Choose homogeneous coordinates $[Z_0 : \cdots : Z_n]$ and let $I(Z)_\bullet$ be the homogeneous ideal defining X . An open subset U of $\text{Gr}_d(P)$ is parametrized by the space of linear maps $\text{Hom}(k^{d+1}, k^{n-d})$ and $\text{Gr}_d(P)$ is covered by such open subsets. So it is enough to show that $F_d(X)$ meets U is a closed subset. We write $Z = (Z', Z'') \in k^{d+1} \times k^{n-d}$. A linear map $A \in \text{Hom}(k^{d+1}, k^{n-d})$ defines an element of $F_d(X)$ if and only if for all $G \in \cup_{m \geq 0} I_m$, $G(Z', A(Z'))$ is identically zero. We expand $G(Z', A(Z'))$ as $\sum_{m_\bullet} G_{m_\bullet} Z_0^{m_0} \cdots Z_d^{m_d}$. It is clear that each coefficient G_{m_\bullet} is a polynomial in the matrix coefficients of A . Since $F_d(X)$ is the common zero set of the G_{m_\bullet} , $G \in \cup_{m \geq 0} I_m$, it follows that $F_d(X) \cap U$ is closed in U . \square

EXAMPLE 5.10. Consider the case of a quadratic hypersurface $X \subset \mathbb{P}(V)$ and assume for simplicity that $\text{char}(k) \neq 2$. So in terms of homogeneous coordinates $[X_0 : \cdots : X_n]$, X can be given by an equation $F(X_0, \dots, X_n) = \frac{1}{2} \sum_{0 \leq i, j \leq n} b_{ij} X_i X_j$ 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 $B : V \times V \rightarrow k$ (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: $B : V \times V \rightarrow k$ is nonsingular, that is, the linear map $b : v \in V \mapsto B(\cdot, v) \in V^*$ 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 is not difficult to show that we can find coordinates (X_0, \dots, 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 $F(X)$. The vector space $\text{Hom}(L, L')$ describes an affine open subset of the Grassmannian of m -planes in $\mathbb{P}(V)$. An element $A \in \text{Hom}(L, L')$ is given by $X_{m+i} = \sum_{j=0}^m a_{ij} X_j$, $j = 0, \dots, m$. 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 51. Let X be a quadratic hypersurface $\mathbb{P}(V)$ of odd dimension $2m+1$ and assume for simplicity that $\text{char}(k) \neq 2$. 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, \dots, 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 52. 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 $\text{Gr}_m(\mathbb{P}^n)$ is given by $\binom{m+d}{d}$ equations.

EXERCISE 53. Consider the universal hypersurface of degree d in \mathbb{P}^n , $H \subset \mathbb{P}^n \times \mathbb{P}^{\binom{n+d}{d}-1}$.

- 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 $\binom{m+d}{d}$.
- 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 $\binom{m+d}{d} - (m+1)(n-m)$.

Let P be a projective space 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 .

PROPOSITION-DEFINITION 5.11. *The map $G : X \rightarrow \text{Gr}_d(P)$, $p \in X \mapsto \hat{T}(X, p)$ is a morphism. This morphism is called the Gauss map.*

PROOF. Let $p \in X$. Let $n := \dim P$. Choose homogenous coordinates $[Z_0 : \cdots : Z_n]$ on P such that $\hat{T}(X, p)$ is given by $Z_{d+1} = \cdots = Z_n = 0$ and $Z_0(p) \neq 0$. We identify the standard open subset U_0 defined by $Z_0 \neq 0$ with the affine hyperplane in k^{n+1} defined by $Z_0 = 1$. So for $q \in X \cap U_0$, $U_0 \cap \hat{T}(X, q)$ is an affine-linear subspace of U_0 which passes through q . The $(d+1)$ -dimensional linear subspace $W(X, q) \subset k^{n+1}$ associated to $\hat{T}(X, q)$ is of course the subspace which meets U_0 in $U_0 \cap \hat{T}(X, q)$.

According to Theorem 10.13 there exists a neighborhood U of p 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 $q \in X \cap U$, the tangent space $T_q X$ is parallel to the common zero set of $df_1(q), \dots, df_{n-d}(q)$. We regard (df_1, \dots, df_{n-d}) as a matrix-valued function on U , denoted $D : U \rightarrow \text{Hom}(k^n, k^{n-d})$, so that for $q \in U \cap X$, $T_q X$ is the kernel of $D(q)$. Let us write

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

Since $D''(p)$ is nonsingular, the nonzero set defined by $\det(D'')$ defines an open neighborhood of p and so we may as well assume that $\det(D'')$ is nonzero on all of U . Cramer's rule shows that $q \in U \mapsto D''(q)^{-1} \in \text{Hom}(k^{n-d}, k^{n-d})$ is matrix valued function with regular entries: it is a morphism. For every $q \in U$, the kernel of $D(q)$ is the graph of the linear map $A(q) := -D''(q)^{-1}D'(q) \in \text{Hom}(k^d, k^{n-d})$. In particular, for $Q \cap X \cap U$, T_qX is parallel to the subspace spanned by $e_1 + A(q)(e_1), \dots, e_d + A(q)(e_d)$.

It follows that $W(X, q)$ is spanned by $q = e_0 + \sum_{i=1}^n q_i e_i$ and the d vectors $e_1 + A(q)(e_1), \dots, e_d + A(q)(e_d)$. This is the graph of the linear map $\tilde{A}(q) : k^{d+1} \rightarrow k^{n-d}$ which sends e_0 to $-\sum_{i=1}^d q_i A(q)(e_i) + \sum_{j=d+1}^n q_j e_j$ and e_i to $A(q)(e_i)$, $i = 1, \dots, d$. Since $\tilde{A} : X \cap U \rightarrow \text{Hom}(k^{d+1}, k^{n-d})$ is regular, this defines a morphism $X \cap U \rightarrow \text{Gr}_d(P)$. \square

For a closed irreducible subset $X \subset P$, the Gauss map is defined on its nonsingular part: $G : X_{\text{reg}} \rightarrow \text{Gr}_d(P)$. The closure of the graph of G in $X \times \text{Gr}_d(P)$ is called the *Nash blowup* of X and denoted \hat{X} . The projection morphism $\hat{X} \rightarrow X$ 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 $\text{Gr}_d(P)$) in such a manner that these subspaces extend the tangent bundle in a regular manner.

6. Intersection multiplicities

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 it is even true more generally when the locus of intersection is finite and each point of intersection is counted 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 6.1. We say that an R -module has *length* $\geq d$ if there exist a d -step filtration by submodules $0 = M^0 \subsetneq M^1 \subsetneq \dots \subsetneq M^d = M$. The *length* of M is the supremum of such d (and so may be ∞).

EXERCISE 54. 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 equal to the sum $\sum_{i \geq 0} \dim_K(\mathfrak{m}^i M / \mathfrak{m}^{i+1} M)$ and is finite precisely when $\mathfrak{m}^d M = 0$ for some d . (Although M is not in any natural manner a K -vector space, its length is somewhat like the K -dimension of 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 6.2. We can describe $M_{\mathfrak{p}}$ somewhat more concretely as follows. Consider the set $M'_{\mathfrak{p}}$ of expressions m/s with $m \in M$ and $s \in R - \mathfrak{p}$ with the understanding that $m/s = m'/s'$ if the identity $s'm = sm'$ holds in M (so we are considering

the quotient of $M \times (R - \mathfrak{p})$ by an equivalence relation). Then the following rules put on $M'_\mathfrak{p}$ the structure of a R -module:

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

The map $R_\mathfrak{p} \times M \rightarrow M'_\mathfrak{p}$, $(r/s, m) \rightarrow (rm)/s$ is R -bilinear and hence factors through an R -homomorphism $M_\mathfrak{p} \rightarrow M'_\mathfrak{p}$. On the other hand, the map $M'_\mathfrak{p} \rightarrow M_\mathfrak{p}$, $m/s \mapsto 1/s \otimes_R m$ is also defined: if $m/s = m'/s'$, then $1/s \otimes_R m = 1/s' \otimes_R m'$. It is an R -homomorphism and it is immediately verified that it is a two-sided inverse of the map above. So $M_\mathfrak{p} \rightarrow M'_\mathfrak{p}$ is an isomorphism.

This description shows in particular that if $N \subset M$ is a submodule, then $N_\mathfrak{p}$ may be regarded as submodule of $M_\mathfrak{p}$.

DEFINITION 6.3. 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 a $R_\mathfrak{p}$ -module.

The *annihilator* $\text{Ann}(M)$ 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 $\text{Ann}(M)$ and are minimal for that property. According to Exercise 14 these are finite in number and their common intersection equals $\sqrt{\text{Ann}(M)}$.

We wish to discuss the graded case parallel to the ungraded case. This means that if R is graded: $R = \bigoplus_{i=0}^{\infty} R_i$, then we assume M to be graded as well, that is, M is endowed with a decomposition as an abelian group $M = \bigoplus_{i \in \mathbb{Z}} M_i$ such that R_j sends M_i to M_{i+j} . For example, a homogeneous ideal in R is a graded R -module. We recall that if $\mathfrak{p} \subset R$ is prime ideal in the graded sense (meaning that if a product of homogeneous elements of R lies in \mathfrak{p} , then so does one of its factors), then it is a prime ideal (Exercise 38). This implies that for every prime ideal $\mathfrak{p} \subset R$, the graded ideal $\bigoplus_{i=0}^{\infty} (\mathfrak{p} \cap R_i)$ is also a prime ideal. It follows for instance, that every minimal prime ideal \mathfrak{p} containing a given graded ideal $I \subset R$ is itself graded. In other words, the minimal distinct prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ containing I (these occur in the primary decomposition $\sqrt{I} = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_r$) are all graded.

Clearly, $\text{Ann}(M)$ is a graded ideal and hence so by the above discussion the members of $\mathcal{P}(M)$ are graded as well. We further note that the annihilator of any homogenous element m , $\text{Ann}(m) := \{r \in R : rm = 0\}$ is a graded ideal.

LEMMA 6.4. *If M is finitely generated and nonzero (graded), 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 M .*

PROOF. We only do the graded case. The first assertion follows from the noetherian property of R . Let now $\text{Ann}(m)$ 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 38), i.e., we must prove that if $a, b \in R$ are homogeneous and $ab \in \text{Ann}(m)$, but $b \notin \text{Ann}(m)$, then $a \in \text{Ann}(m)$. So $bm \neq 0$ and $a \in \text{Ann}(bm)$. Since $\text{Ann}(bm) \supset \text{Ann}(m)$, the maximality property of the latter implies that this must be an equality: $\text{Ann}(bm) = \text{Ann}(m)$, and so $a \in \text{Ann}(m)$. \square

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 6.5. *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 $0 = M^0 \subsetneq M^1 \subsetneq \dots \subsetneq M^d = M$ 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 prove that $M' = M$. If M/M' were nonzero, then according to Lemma 6.4, 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' . \square

PROPOSITION 6.6. *Suppose that in the preceding proposition $M^i/M^{i-1} \cong R/\mathfrak{p}_i$. Then $\mathcal{P}(M)$ is precisely the set of minimal members of the set $\{\mathfrak{p}_1, \dots, \mathfrak{p}_d\}$. Moreover, 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 $\sqrt{\text{Ann}(M)} = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_d$. If $r \in \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_d$, then r maps M_i to M_{i-1} and so $r^d \in \text{Ann}(M)$. This proves that $\mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_d \subset \sqrt{\text{Ann}(M)}$. Conversely, if $r \in R$ and $l \geq 1$ are such that $r^l \in \text{Ann}(M)$, then $r^l \in \mathfrak{p}_i$ for all i . This implies that $r \in \mathfrak{p}_i$ for all i . It follows that the set of minimal members of $\{\mathfrak{p}_1, \dots, \mathfrak{p}_d\}$ is in fact the set of minimal prime ideals containing $\text{Ann}(M)$.

Fix $\mathfrak{p} \in \mathcal{P}(M)$ and put $K := K(R/\mathfrak{p})$. We then have a filtration $0 = M_{\mathfrak{p}}^0 \subset \dots \subset M_{\mathfrak{p}}^d = M$ (for an inclusion of R -modules induces an inclusion of $R_{\mathfrak{p}}$ -modules).

For $i = 1, \dots, d$, either $\mathfrak{p}_i = \mathfrak{p}$ or there exists some $r \in \mathfrak{p}_i \cap (R - \mathfrak{p})$. Now $\mathfrak{p}_i R_{\mathfrak{p}}$ is the set of fractions a/b with $a \in \mathfrak{p}_i$ and $b \in R - \mathfrak{p}$ with the understanding that $a/b = a'/b'$ if $ab' - a'b = 0$. When $\mathfrak{p}_i = \mathfrak{p}$, $\mathfrak{p}_i R_{\mathfrak{p}} = \mathfrak{p} R_{\mathfrak{p}}$ is the maximal ideal of $R_{\mathfrak{p}}$ and $R_{\mathfrak{p}}/\mathfrak{p}_i R_{\mathfrak{p}} = K$. In the second case, we have in $R_{\mathfrak{p}}$ the identity $1/1 = r/r \in \mathfrak{p}_i R_{\mathfrak{p}}$; so then $\mathfrak{p}_i R_{\mathfrak{p}} = R_{\mathfrak{p}}$ and hence $R_{\mathfrak{p}}/\mathfrak{p}_i R_{\mathfrak{p}} = 0$.

In other words, $M_{\mathfrak{p}}^{i-1} = M_{\mathfrak{p}}^i$ unless $\mathfrak{p}_i = \mathfrak{p}$, in which case the quotient is isomorphic to K . Following our definition that case occurs precisely $\mu_{\mathfrak{p}}(M)$ times. \square

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* of degree $d \geq 0$:

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

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

Let $\Delta : \mathbb{Q}[z] \rightarrow \mathbb{Q}[z]$ 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 $\Delta\left(\binom{z}{d+1}\right) = \binom{z}{d}$.

LEMMA 6.7. *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 binomials.*

If $f : \mathbb{Z} \rightarrow \mathbb{Z}$ 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 binomials.

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 . \square

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

In what follows R denotes the graded ring $R = k[X_0, \dots, X_n]$ where each X_i has degree 1 and M is a finitely generated graded R -module.

We define the Hilbert function of M , $\phi_M : \mathbb{Z} \rightarrow \mathbb{Z}$, by $\phi_M(i) := \dim_k M_i$. The zero set of the graded ideal $\text{Ann}(M)$ in \mathbb{P}^n will be called the support of M and denoted $\text{supp}(M)$.

THEOREM 6.8 (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 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 $\dim(\text{supp}(M))$ if we convene 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 $\text{Ann}(M) = \text{Ann}(N) \cap \text{Ann}(M/N)$ and so $\text{supp}(M) = \text{supp}(N) \cup \text{supp}(M/N)$. 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 $M = R/\mathfrak{p}$.

Now $\text{supp}(M)$ is simply 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 $\text{supp}(M) = \emptyset$. 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 $\bar{M} := M/X_n M$. Since $\text{Ann}(\bar{M}) = \text{Ann}(M) + X_n R$, we have $\text{supp}(\bar{M}) = \text{supp}(M) \cap \mathbb{P}^{n-1}$. According to Proposition 4.11 we then have $\dim \text{supp}(\bar{M}) = \dim \text{supp}(M) - 1$. Since we may regard \bar{M} as a finitely generated module over $\bar{R} := k[X_0, \dots, X_{n-1}]$, our induction hypothesis applies and says that there exists a polynomial $P_{\bar{M}}$ of degree $\dim \text{supp}(\bar{M})$ such that $\phi_{\bar{M}}$ and $P_{\bar{M}}$ coincide on large integers.

Now for $i \geq 0$, $\phi_{\bar{M}}(i) = \phi_M(i) - \phi_M(i-1) = \Delta \phi_M(i-1)$. It follows that $\Delta \phi_M(i-1) = P_{\bar{M}}(i)$ for large i . According to Lemma 6.7 implies that there exists a polynomial P_M of degree one higher than that of $P_{\bar{M}}$ (so of degree $\dim(\text{supp}(M))$) which coincides with ϕ_M for sufficiently large integers. \square

It follows from Lemma 6.7 that P_M will have a leading term of the form $c_d/d!z^d$, where d is the dimension of $\text{supp}(M)$.

DEFINITION 6.9. If $d = \dim \text{supp}(M)$, then the *degree* $\deg(M)$ is $d!$ times the leading coefficient of its Hilbert polynomial (which we stipulate to be zero in case $\text{supp}(M) = \emptyset$). 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.

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. 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 homogenous 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 6.10. *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. We have an exact sequence of graded R -modules

$$0 \rightarrow R \xrightarrow{F \cdot} R \rightarrow S(Y) \rightarrow 0$$

The Hilbert function of R takes at the positive integer i the value $\binom{n+i}{n}$. So for $i \geq d$ the Hilbert function 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 hence $\deg(H) = d$. □

PROPOSITION 6.11. *Let Y_1, \dots, Y_r be the distinct irreducible components of Y of the same dimension as Y . Then $\deg(Y) = \sum_{i=1}^r \deg(Y_i)$.*

PROOF. 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

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

where $M := R/(I(Y_1) + I(Y'))$. This implies that $P_Y = P_{Y_1} + P_{Y'} - P_M$. We have $\text{supp}(M) = Y_1 \cap Y'$ and so $\dim \text{supp}(M) < \dim Y$. This implies that P_M had degree smaller than $\dim(Y)$ and the assertion follows from comparing the coefficients of $z^{\dim Y}$. □

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

THEOREM-DEFINITION 6.1. *Let $Y \subset \mathbb{P}^n$ be closed with all irreducible components of the same dimension m and let $H \subset \mathbb{P}^n$ be a hypersurface containing no irreducible component of Y . If for an irreducible component Z of $Y \cap H$, we define the multiplicity*

$i(Y, H; Z)$ of Y and H along Z as $\mu_{I(Z)}(R/(I(Y)+I(H)))$ (= the length of $(R/(I(Y)+I(H)))_{I(Z)}$ as a $R_{I(Z)}$ -module), then we have

$$\sum_{Z \text{ irred. comp of } Y \cap H \text{ of dim. } m-1} i(Y, H; Z) \deg(Z) = \deg(Y) \deg(H).$$

PROOF. Write M for $R/(I(Y) + I(H))$ and regard M as a R -module. Denote by d resp. e the degree of H resp. Y and let $F \in R_d$ generate $I(H)$. The exact sequence

$$0 \rightarrow R/I(Y)[-d] \xrightarrow{\cdot F} R/I(Y) \rightarrow M \rightarrow 0$$

shows that $P_M(z) = P_Y(z) - P_Y(z-d)$. Since P_Y is of degree m with leading coefficient $e/m!$, it follows that P_M is of degree $m-1$ with leading coefficient $de/(m-1)!$.

If we write M as a successive extension of elementary R -modules: $0 = M^0 \subsetneq M^1 \subsetneq \dots \subsetneq M^r = M$ with $M^i/M^{i-1} \cong R/\mathfrak{p}_i[l_i]$, then $P_M(z) = \sum_{i=1}^r P_{R/\mathfrak{p}_i}(z-l_i)$. The homogeneous prime ideal \mathfrak{p}_i defines an irreducible subvariety Z_i of \mathbb{P}^n . Since $\mathfrak{p}_i \supset I(Y) \cap I(H)$, Z_i is contained in $Y \cap H$. The degree and leading coefficient of $P_{R/\mathfrak{p}_i}(z-l_i)$ are the same as that of $P_{R/\mathfrak{p}_i}(z)$ and hence equal to $\dim Z_i$ resp. $\deg(Z_i)/(\dim Z_i)!$. In particular, the leading coefficient of P_{R/\mathfrak{p}_i} contributes to that of P_M if and only if $\dim Z_i = m-1$ (this contribution then being $\deg(Z_i)/(m-1)!$). Such a Z_i will be an irreducible component of $Y \cap H$.

If Z is an irreducible component of dimension $m-1$ of $Y \cap H$, then according to 6.8 the number of times that $\mathfrak{p}_i = I(Z)$ is equal to the length of $(R/(I(Y) + I(H)))_{I(Z)}$ as a $R_{I(Z)}$ -module. So the leading term of P_M is the sum of $\mu_{I(Z)}(M) \deg(Z)/(m-1)!$ over all such Z . The theorem follows. \square

COROLLARY 6.12 (Bézout). *If C and C' are curves in \mathbb{P}^2 such that $C \cap C'$ is finite, then $\deg(C) \deg(C') = \sum_{z \in C \cap C'} i(C, C'; \{z\})$.*

PROOF. Immediate from the previous theorem and the fact that a singleton $\{z\}$ in \mathbb{P}^2 has degree 1. \square

REMARK 6.13. So if the curves C and C' have finite intersection, then they intersect in $\deg(C) \deg(C')$ points, if each intersection point is counted with appropriate multiplicity. This multiplicity at $p \in C \cap C'$ can be calculated as follows. Let $d := \deg C$ and choose a generator $F \in k[X_0, X_1, X_2]_d$ of $I(C)$. Do likewise for C' . If $[X_0 : X_1 : X_2]$ are homogenous coordinates in \mathbb{P}^2 such that $p = [1 : 0 : 0]$, then $i(C, C'; \{p\})$ is (by definition) the length of $(k[X_0, X_1, X_2]/(F, F'))_{(X_1, X_2)}$ as a $k[X_0, X_1, X_2]_{(X_1, X_2)}$ -module. If we pass to affine coordinates: $(x_1, x_2) = (X_1/X_0, X_2/X_0)$, so that we can write $F(X_0, X_1, X_2) = X_0^d f(x_1, x_2)$ and likewise for F' , then one can show that $i(C, C'; \{p\})$ is also the length of $(k[x_1, x_2]/(f_1, f_2))_{(x_1, x_2)}$ as a module over the local ring $\mathcal{O}_{\mathbb{P}^2, p} = k[x_1, x_2]_{(x_1, x_2)}$. This is just the dimension of $k[[x_1, x_2]]/(f, f')$ as a k -vector space.

EXAMPLE 6.14. Assume $\text{char}(k) \neq 2$. 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 $k[[x, y]]/(x^2 + y^2 - 2y, x^2 - y)$ as a k -vector space. But $k[[x, y]]/(x^2 + y^2 - 2y, x^2 - y) = k[[x]]/(x^4 - x^2) = k[[x]]/(x^2)$ (for $(x^2 - 1)$ is invertible in $k[[x]]$). 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.