Algebraic Geometry I

(2015 edition)

Eduard Looijenga

Introduction

These are notes that accompany my course Algebraic Geometry I. Every time I taught that course, I revised the text and although I do not expect drastic changes anymore, this is a process that will probably only stop when I cease teaching it. Such constant revisions are not the only reason that these digital notes differ from a text book: another is that they are tailored to the needs of the course and this may change with time, too. We sometimes do not give a topic the treatment it deserves, or just skip a nearby point of interest that would have merited discussion. Occasionally I allude to such omissions by remarks in a smaller font.

As I hope will become clear (and even more so in its sequel, Algebraic Geometry II), much of commutative algebra owes its existence to algebraic geometry and vice versa, and this is why there is no clear border between the two. This also explains why some familiarity with commutative algebra is a prerequisite, but as a service to students lacking such background, I occassionally recall basic facts from that area and from Galois theory (all standard fare in a first course on these subjects) in a smaller font. Propositions with an asterisk—of which there are only three: 8.14, 10.16 and 10.11—are in general not included in such a course, but their proofs were omitted for reasons of time. Otherwise these notes are essentially self-contained.

On <www.staff.science.uu.nl/∼looij101/> I maintain a web page of this course, where among other things, I briefly explain what this field is about and list some books for further reading. To repeat a recommendation that is made there, I strongly encourage you to buy a (paper!) text book as a companion to use with the course, for such a book generally covers more ground and tends to do so also in a more balanced manner. And it may be consulted, even long after these notes have perished. A good choice is Hartshorne's book (though certainly not the only one), which has the additional benefit that it can also serve you well for a sequel to this course. (That the content of these notes have a substantial overlap with Chapter 1 of that volume is unlikely to be a coincidence.)

You may occasionally find in the text forwarding references to course notes of Algebraic Geometry II. These indeed exist, but as they are in a much more tentative and preliminary form, I have not included them here.

Some conventions. In these notes rings are always supposed to be commutative and to possess a unit and a ring homomorphism is required to take unit to unit. We allow that $1 = 0$, but in that case we get of course the zero ring $\{0\}$ and there cannot be any ring homomorphism going from this ring to a nonzero ring, as it must take unit to unit. Since a prime ideal of a ring is by definition not the whole ring, the zero ring has no prime ideals and hence also no maximal ideals. When R and R' are two rings, then $R \times R'$ is also one for componentwise addition and multiplication, the unit being $(1, 1)$. The projections onto its factors are admitted as ring homomorphims, but not an inclusion obtained by putting one coordinate zero, as this is not unital, unless in that coordinate we have the zero ring ("$\times$" defines a categorical product but not a categorical sum).

We say that a ring is a *domain* if its zero ideal is a prime ideal, in other words, if the ring is not the zero ring ($1 \neq 0$) and has no zero divisors.

Given a ring R, then an *R-algebra* is a ring A endowed with a ring homomorphism $\phi : R \to A$. When is ϕ is understood, then for every $r \in R$ and $a \in A$, the

product $\phi(r)a$ is often denoted by ra. In case R is a field, ϕ will be injective so that R may be regarded as a subring of A, but this need not be so in general. We say that A is *finitely generated as an R-algebra* if we can find $a_1, \ldots, a_n$ in A such that every element of A can be written as a polynomial in these elements with coefficients in R; in other words, if the R-algebra homomorphism $R[x_1, \ldots, x_n] \to A$ which sends the variable x_i to a_i is onto. This is not to be confused with the notion of finite generation of an R-module M which merely means the existence of a surjective homomorphism of R-modules $R^n \to M$ for some $n \geq 0$.

Similarly, a field L is said to be *finitely generated as a field* over a subfield K if there exist $b_1, \ldots, b_n$ in L such that every element of L can be written as a fraction of two polynomials in these elements with coefficients in K.

We denote the multiplicative group of the invertible elements (units) of a ring R by $R^\times$.

Contents

CHAPTER 1

Affine varieties

Throughout these notes k stands for an algebraically closed field. 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 f is divisible by $x - x_1$ with quotient a polynomial of degree one less than f. Continuing in this manner we then find that f decomposes simply as $f(x) = c(x - x_1) \cdots (x - x_d)$ with $c \in k^\times = k \smallsetminus \{0\}$, $d = \deg(f)$ and $x_1, \ldots, x_d \in k$. Since an algebraic extension of k is obtained by the adjunction of certain 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 become 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 $f \in F[x]$.[1] So we could take for k an algebraic closure of the field of rational numbers $\mathbb{Q}$, of the finite field $\mathbb{F}_q$, where q is a prime power[2] or even of the field of fractions of any domain such as $\mathbb{C}[x_1, \ldots, x_r]$.

1. The Zariski topology

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

A *principal* subset of $\mathbb{A}^n$ is any subset of the form $\mathbb{A}^n_f$ and a *hypersurface* of $\mathbb{A}^n$ is any subset of the form $Z(f)$, with f nonconstant (that is, $f \notin k$).

EXERCISE 1. Prove that $f \in k[x_1, \ldots, x_n]$ is completely determined by the regular function it defines. (Hint: do first the case $n = 1$.) So the ring $k[x_1, \ldots, x_n]$

[1] This can not be done in one step: it is an infinite process which involves in general many choices. This is reflected by the fact that the final result is not canonical, although it is unique up to a (in general nonunique) isomorphism; whence the use of the indefinite article in 'an algebraic closure'.

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

can be regarded as a ring of functions on $\mathbb{A}^n$ under pointwise addition and multiplication. Show that this fails be so had we not assumed that k is algebraically closed (e.g., for the finite field $\mathbb{F}_q$).

EXERCISE 2. Prove that a hypersurface is nonempty.

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 of principal subsets of $\mathbb{A}^n$ is a basis of a topology on $\mathbb{A}^n$, called the* Zariski topology. *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. Recall that a collection $\mathfrak{U}$ of subsets of a set X may serve as a basis for a topology on X (and thus determines this topology) if and only if the intersection of any two its members is a union of members of $\mathfrak{U}$. As the collection of principal subsets is even closed under finite intersection: $\mathbb{A}^n_{f_1} \cap \mathbb{A}^n_{f_2} = \mathbb{A}^n_{f_1 f_2}$, the first assertion follows. Since an open subset of $\mathbb{A}^n$ is by definition a union of subsets of the form $\mathbb{A}^n_f$, a closed subset must be an intersection of subsets of the form $Z(f)$. □

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

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

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

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

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

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

In particular, both I and Z are inclusion reversing. Furthermore, the restriction of I to closed subsets defines a section of Z: if $Y \subset \mathbb{A}^n$ is closed, then $Z(I(Y)) = Y$. We also note that by Exercise 1 $I(\mathbb{A}^n) = (0)$, and that any singleton $\{p\} \subset \mathbb{A}^n$ 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 equal to the ideal generated by these degree one polynomials and that this ideal is maximal.

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

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

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

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

$$\begin{array}{ccc} \{\text{subsets of } Y\} & \xrightarrow{I_Y} & \{\text{ideals of } k[Y]\} \\ \cup & & \cap \\ \{\text{closed subsets of } Y\} & \xleftarrow{Z_Y} & \{\text{subsets of } k[Y]\}. \end{array}$$

We ask: which ideals of $k[x_1, \ldots, x_n]$ are of the form $I(Y)$ for some Y? Clearly, if $f \in k[x_1, \ldots, x_n]$ 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 an R-linear combination of monomials that are multiples of a^m or b^n and hence lie in J. □

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

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

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

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

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

$$\{\textit{closed subsets of } Y\} \leftrightarrow \{\textit{radical ideals of } k[Y]\}$$

that each others inverse and restrict to bijections

$$\{\textit{points of } Y\} \leftrightarrow \{\textit{maximal ideals of } k[Y]\}.$$

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

If $X = \{p\}$ with $p = (p_1, \ldots, p_n) \in \mathbb{A}^n$, then $\mathfrak{m}_p := (x_1 - p_1, \ldots, x_n - p_n)$ is a maximal ideal of $k[x_1, \ldots, x_n]$ by Exercise 4. Since $I(X) \supset \mathfrak{m}_p$ we must then have $I(X) = \mathfrak{m}_p$ (for $I(X) = k[x_1, \ldots, x_n]$ is clearly excluded). Conversely let $\mathfrak{m}$ be a maximal ideal of $k[x_1, \ldots, x_n]$. Such an ideal is certainly radical as it is a prime ideal. Hence it is of the form $I(X)$ for a closed subset X. Since the empty subset of $\mathbb{A}^n$ is defined by the radical ideal $k[x_1, \ldots, x_n]$, the preceding implies that X will be nonempty and (as $\mathfrak{m}$ is a maximal ideal) minimal for this property. In other words, X is a singleton $\{p\}$. So this yields a bijection between the points of $\mathbb{A}^n$ and the maximal ideals of $k[x_1, \ldots, x_n]$.

The general case now also follows, because an ideal of $k[Y]$ is of the form $J/I(Y)$ and this is a radical ideal if and only if J is one; a maximal ideal of $k[Y]$ corresponds to a maximal ideal of $\mathbb{A}^n$ which contains $I(Y)$. □

Via this (or a very similar) correspondence, algebraic geometry seeks to express geometric properties of Y in terms of algebraic properties of $k[Y]$ and vice versa. In the end we want to forget about the ambient $\mathbb{A}^n$.

2. Irreducibility and decomposition

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

DEFINITION 2.1. Let Y be a topological space. We say that Y is *irreducible* if it is nonempty and cannot be written as the union of two closed subsets $\neq Y$ (this last property is equivalent to: any nonempty open subset of Y is dense in Y).

An *irreducible component* of Y is a maximal irreducible subset of Y.

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

EXERCISE 8. Let $Y_1, \ldots, Y_s$ be closed subsets of a topological space Y whose union is Y. Prove that every irreducible subset of Y is contained in some Y_i. Deduce that $\{Y_i\}_{i=1}^s$ is the collection of irreducible components of Y if each Y_i is irreducible and $Y_i \subset Y_j$ implies $Y_i = Y_j$.

LEMMA 2.2. *Let Y be a topological space. If Y is irreducible, then every nonempty open subset of Y irreducible. Conversely, if $C \subset Y$ is an irreducible subspace, then $\overline{C}$ is also irreducible. In particular, an irreducible component of Y is always closed in Y.*

PROOF. Suppose Y is irreducible and let $U \subset Y$ be open and nonempty. A nonempty open subset of U is dense in Y and hence also dense in U. So U is irreducible.

Let now $C \subset Y$ be irreducible (and hence nonempty). Let $V \subset \overline{C}$ be nonempty and open in $\overline{C}$. Then $V \cap C$ is nonempty. It is also open in C and hence dense in C. But then $V \cap C$ is also dense in $\overline{C}$ and so V is dense in $\overline{C}$. So $\overline{C}$ is irreducible. □

Here is what irreducibility means in the Zariski topology.

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

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

Suppose that Y is the union of two closed subsets Y_1 and Y_2 that are both $\neq Y$. Then $I(Y)$ is not a prime ideal: since $Y_i \neq Y$ implies that there exist $f_i \in I(Y_i) - I(Y)$ $(i = 1, 2)$ and then $f_1 f_2$ vanishes on $Y_1 \cup Y_2 = Y$, so that $f_1 f_2 \in I(Y)$. □

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

2.4. UNIQUE FACTORIZATION DOMAINS. Let us first observe that in a ring R without zero divisors two nonzero elements a, b generate the same ideal if and only if b is a unit times a.

DEFINITION 2.5. A ring R is called a *unique factorization domain* if it has no zero divisors and every principal ideal $(a) := Ra$ in R which is neither the zero ideal nor all of R is in unique manner an (unordered) product of principal prime ideals: $(a) = (p_1)(p_2)\cdots(p_s)$ (so the ideals $(p_1), \ldots, (p_s)$ are unique up to order).

Note that last property amounts to the statement that a can be written as a product $a = p_1 p_2 \cdots p_s$ such that each p_i generates a prime ideal and this is unique up to order and multiplication by units: if $a = q_1 q_2 \cdots q_t$ is another such way of writing a, then $t = s$ and $q_i = u_i p_{\sigma(i)}$, where $\sigma \in \mathcal{S}_n$ is a permutation and $u_1 u_2 \cdots u_s = 1$.

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

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

The following proposition connects two notions of irreducibility.

PROPOSITION 2.6. *Let $f \in k[x_1, \ldots, x_n]$ have positive degree. If $f = f_1 f_2 \cdots f_s$ is a factoring into irreducible polynomials, then $Z(f_1), \ldots, Z(f_s)$ are the irreducible components of $Z(f)$ and their union equals $Z(f)$ (but we are not claiming that the $Z(f_i)$'s are pairwise distinct). In particular, a hypersurface is the union of its irreducible components; these irreducible components are hypersurfaces and finite in number (so that f is irreducible if and only if $Z(f)$ is irreducible).*

PROOF. We first note that when $g \in k[x_1, \ldots, x_n]$ is irreducible, then g generates a prime ideal and so $Z(g)$ is an irreducible hypersurface by Proposition 2.3.

It follows that if $f = f_1 f_2 \cdots f_s$ is as in the proposition, then $Z(f) = Z(f_1) \cup \cdots \cup Z(f_s)$ with each $Z(f_i)$ irreducible. To see that $\{Z(f_i)\}_{i=1}^s$ is the collection of irreducible components of $Z(f)$, it suffices, in view of Exercise 8, to observe that any inclusion relation $Z(f_i) \subset Z(f_j)$ is necessarily an identity. Since f_i is

irreducible it generates a prime ideal. A prime ideal is a radical ideal and so by the Nullstellensatz, $f_j \in (f_i)$. But f_j is irreducible also and so f_j is a unit times f_i. This proves that $Z(f_j) = Z(f_i)$. □

The discussion of irreducibility in general begins with the somewhat formal

LEMMA 2.7. *For a partially ordered set $(A, \leq)$ the following are equivalent:*

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

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

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

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

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

DEFINITIONS 2.8. We say that a ring R is *noetherian* if its collection of ideals satisfies the ascending chain condition.

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

EXERCISE 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 quasi-compact: every covering of such a space by open subsets contains a finite subcovering.

The interest of the noetherian property is that it is one which is possessed by almost all the rings we encounter and that it implies many finiteness properties without which we are often unable to go very far.

We give a nonexample first. The ring $\mathcal{H}(\mathbb{D})$ of holomorphic functions on the unit disk $\mathbb{D} \subset \mathbb{C}$ is not noetherian: choose $f_o \in \mathcal{H}(\mathbb{D})$ such that f_o has *simple* zeroes in a sequence $(z_i \in \mathbb{D})_{i \geq 1}$ whose terms are pairwise distinct (e.g., $\sin(\pi/(1-z))$). Let I_n denote the ideal of $f \in \mathcal{H}(\mathbb{D})$ having a zero in z_i for all $i \geq n$. Then $f_o(z)(z-z_1)^{-1} \cdots (z-z_n)^{-1}$ defines an element of $I_{n+1} - I_n$ and so $I_1 \subset I_2 \subset \cdots$ is a strictly ascending chain of ideals in $\mathcal{H}(\mathbb{D})$.

On the other hand, the ring of convergent power series $\mathbb{C}\{z\}$ is noetherian (we leave this as a little exercise). 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 encounter are noetherian is a consequence of the following theorem.

THEOREM 2.9 (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 2.10. *If R is a noetherian ring (for example, a field) then so is every finitely generated R-algebra. Also, the space $\mathbb{A}^n$ (and hence any closed subset of $\mathbb{A}^n$) is noetherian.*

PROOF. The Hilbert basis theorem implies (with induction on n) that the ring $R[x_1, \ldots, x_n]$ is noetherian. By Exercise 9, every quotient ring $R[x_1, \ldots, x_n]/I$ is then also noetherian. But a finitely generated R-algebra is (by definition) isomorphic to some such quotient and so the first statement follows.

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

PROPOSITION 2.11. *If Y is noetherian space, then its irreducible components are finite in number and their union equals Y.*

PROOF. Suppose Y is a noetherian space. We first show that every closed subset can be written as a finite union of closed irreducible subsets. First note that the empty set has this property (despite the fact that an irreducible set is nonempty by definition), for a union with empty index set is empty. Let B be the collection of closed subspaces of Y for which this is not possible, i.e., that can *not* be written as a finite union of closed irreducible subsets. Suppose that B is nonempty. According to 2.7 this collection has a minimal element, Z, say. This Z must be nonempty and cannot be irreducible. So Z is the union of two proper closed subsets Z' and Z''. The minimality of Z implies that neither Z' nor Z'' is in B and so both Z' and Z'' can be written as a finite union of closed irreducible subsets. But then so can Z and we get a contradiction.

In particular, there exist closed irreducible subsets $Y_1, \ldots, Y_s$ of Y whose union is Y (if $Y = \emptyset$, take $s = 0$). We may of course assume that no Y_i is contained in some Y_j with $j \neq i$. An application Exercise 8 then shows that the Y_i's are the irreducible components of Y. □

If we apply this to $\mathbb{A}^n$ (endowed as always with its Zariski topology), 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 2.12. *Let $Y \subset \mathbb{A}^n$ be a closed subset. If C is an irreducible component of Y, then the image $I_Y(C)$ of $I(C)$ in $k[Y]$ is a minimal prime ideal of $k[Y]$ and any minimal prime ideal of $k[Y]$ is so obtained: we thus get a bijective correspondence between the irreducible components of Y and the minimal prime ideals of $k[Y]$.*

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

EXAMPLE 2.13. First consider the set $C := \{(t, t^2, t^3) \in \mathbb{A}^3 \mid t \in k\}$. This is a closed subset of $\mathbb{A}^3$: if we use (x, y, z) instead of (x_1, x_2, x_3), then C is the common zero set of $y - x^2$ and $z - x^3$. Now the inclusion $k[x] \subset k[x, y, z]$ composed with the ring quotient $k[x, y, z] \to k[x, y, z]/(y - x^2, z - x^3)$ is easily seen to be an isomorphism. Since $k[x]$ has no zero divisors, $(y - x^2, z - x^3)$ must be a prime ideal. So C is irreducible and $I(C) = (y - x^2, z - x^3)$.

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

We begin with recalling the notion of localization and we do this in the generality that is needed later.

2.14. LOCALIZATION. Let R be a ring and let S be a *multiplicative subset* of R: $1 \in S$ and S closed under multiplication. Then a ring $S^{-1}R$, together with a ring homomorphism $R \to S^{-1}R$ is defined as follows. An element of $S^{-1}R$ is by definition written as a formal fraction r/s, with $r \in R$ and $s \in S$, with the understanding that $r/s = r'/s'$ if and only if $s''(s'r - sr') = 0$ for some $s'' \in S$. This is a ring indeed: multiplication and subtraction is defined as for ordinary fractions: $r/s.r'/s' = (rr')/(ss')$ and $r/s - r'/s' = (s'r - sr')/(ss')$; it has $0/1$ as zero and $1/1$ as unit element and the ring homomorphism $R \to S^{-1}R$ is simply $r \mapsto r/1$. Observe that the definition shows that $0/1 = 1/1$ if and only if $0 \in S$, in which case $S^{-1}R$ is reduced to the zero ring. We also note that any $s \in S$ maps to an invertible element of $S^{-1}R$, the inverse of $s/1$ being $1/s$ (this is also true when $0 \in S$, for 0 is its own inverse in the zero ring). In a sense (made precise in part (b) of Exercise 11 below) the ring homomorphism $R \to S^{-1}R$ 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, $r/1 = r'/1$ if and only if $r = r'$, so that $R \to S^{-1}R$ is then injective. If we take S maximal for this property, namely take it to be the set of nonzero divisors of R (which is indeed multiplicative), then $S^{-1}R$ is called the *fraction ring* $\mathrm{Frac}(R)$ of R. When R is a domain, $S = R \setminus \{0\}$ and so $\mathrm{Frac}(R)$ is a field, the *fraction field* of R. This gives the following corollary, which hints to the importance of prime ideals in the subject.

COROLLARY 2.15. *An ideal $\mathfrak{p}$ of a ring R is a prime ideal if and only if it is the kernel of a ring homomorphism from R to a field.*

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

Of special interest is when $S = \{s^n \mid n \geq 0\}$ for some $s \in R$. We then usually write $R[1/s]$ for $S^{-1}R$. Notice that the image of s in $R[1/s]$ is invertible and that $R[1/s]$ is the zero ring if and only if s is nilpotent.

EXERCISE 11. Let R be a ring and let S be a multiplicative subset of R.

(a) What is the the kernel of $R \to S^{-1}R$?
(b) Prove that a ring homomorphism $\phi : R \to R'$ with the property that $\phi(s)$ is invertible for every $s \in S$ factors in a unique manner through $S^{-1}R$.
(c) Consider the polynomial ring $R[x_s : s \in S]$ and the homomorphism of R-algebras $R[x_s : s \in S] \to S^{-1}R$ that sends x_s to $1/s$. Prove that this homomorphism is surjective and that its kernel consists of the $f \in R[x_s :$

$s \in S]$ which after multiplication by an element of S lie in the ideal generated the degree one polynomials $sx_s - 1$, $s \in S$.

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

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

LEMMA 2.16. *Let R be a ring. Then the intersection of all the prime ideals of R is the ideal of nilpotents $\sqrt{(0)}$ of R. Equivalently, for every nonnilpotent $a \in R$, there exists a ring homomorphism from R to a field that is nonzero on a.*

PROOF. It is easy to see that a nilpotent element lies in every prime ideal. Now for nonnilpotent $a \in R$ consider the homomorphism $R \to R[1/a]$. The ring $R[1/a]$ is nonzero, hence has a maximal ideal[3] $\mathfrak{m}$ so that $F := R[1/a]/\mathfrak{m}$ is a field. Then the kernel of the composite $\phi : R \to R[1/a] \to F$ is a prime ideal and a is not in this kernel (for $\phi(a) \in F$ is invertible with inverse the image of $1/a$). □

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.

We can do better if R is noetherian. The following proposition is the algebraic counterpart of Proposition 2.11. Note the similarity between the proofs.

PROPOSITION 2.17. *Let R be a noetherian ring. Then any radical ideal in R is an intersection of finitely many prime ideals. Also, the minimal prime ideals of R are finite in number and their intersection is equal to the ideal of nilpotents $\sqrt{(0)}$.*

PROOF. We first make the rather formal observation that R is a radical ideal and indeed appears as a finite (namely empty) intersection of prime ideals. So the collection B of the radical ideals $I \subset R$ that can *not* be written as an intersection of finitely many prime ideals does not contain R. We prove that B is empty. Suppose otherwise. Since R is noetherian, it will have a maximal member $I_0 \neq R$. We then derive a contradiction as follows.

Since I_0 cannot be a prime ideal, there exist $a_1, a_2 \in R - I_0$ with $a_1 a_2 \in I_0$. Consider the radical ideal $J_i := \sqrt{I_0 + Ra_i}$. Since J_i strictly contains I_0, it does not belong to B. In other words, J_i is an intersection of finitely many prime ideals. We next show that $J_1 \cap J_2 = I_0$, so that I_0 is an intersection of finitely many prime ideals also, thus arriving contradiction. 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 $a^{n_1+n_2} \in (I_0 + Ra_1)(I_0 + Ra_2) \subset I_0$, so that $a \in I_0$.

[3]Every nonzero 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.

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

EXERCISE 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 when R is noetherian, its minimal prime ideals are finite in number and that their common intersection is still $\sqrt{J}$. What do we get for $R = \mathbb{Z}$ and $J = \mathbb{Z}n$?

EXERCISE 15. Let R be a ring, $S \subset R$ be a multiplicative system and denote by $\phi : R \to S^{-1}R$ the natural homomorphism. Prove that the map which assigns to every prime ideal of $S^{-1}R$ its preimage in R under ϕ defines a bijection between the prime ideals of $S^{-1}R$ and the prime ideals of R disjoint with S. Prove also that if S has no zero divisors, then the preimage of the ideal of nilpotents of $S^{-1}R$ is the ideal of nilpotents of R.

3. Finiteness properties and the Hilbert theorems

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

We will use the notion of initial coefficient of a polynomial, which we recall. Given a ring R, then every nonzero $f \in R[x]$ is uniquely written as $r_d x^d + r_{d-1}x^{d-1} + \cdots + r_0$ with $r_d \neq 0$. We call $r_d \in R$ the *initial coefficient* of f and denote it by $\operatorname{in}(f)$. For the zero polynomial, we simply define this to be $0 \in R$. Notice that when $\operatorname{in}(f)\operatorname{in}(g)$ nonzero, then it is equal to $\operatorname{in}(fg)$.

PROOF OF THEOREM 2.9. 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 $\operatorname{in}(I) := \{\operatorname{in}(f) : f \in I\}$ of R. We first show that this is an ideal of R. If $r \in R$, $f \in I$, then $r\operatorname{in}(f)$ equals $\operatorname{in}(rf)$ or is zero and since $rf \in I$, it follows that $r\operatorname{in}(f) \in I$. If $f, g \in I$, then $\operatorname{in}(f) - \operatorname{in}(g)$ equals $\operatorname{in}(x^{\deg g}f - x^{\deg f}g)$ or is zero. So $\operatorname{in}(I)$ is an ideal as asserted.

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

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

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

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

For the Nullstellensatz we need another finiteness result.

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

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

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

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

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

Let $A_0 \subset A$ be the R-subalgebra of A generated by all the (finitely many) coefficients a_{ij}^k. This is a noetherian ring by Corollary 2.10. It is clear that $b_i b_j \in \sum_k A_0 b_k$

and so $\sum_k A_0 b_k$ is an R-subalgebra of B. Since the $b_1, \ldots, b_m$ generate B as an R-algebra, it then follows this is all of B: $B = \sum_k A_0 b_k$. So B is finitely generated as an A_0-module. Since A is an A_0-submodule of B, A is also finitely generated as an A_0-module by Proposition 3.4. It follows that A is a finitely generated R-algebra. □

This has a consequence for field extensions:

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

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

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

COROLLARY 3.8. *Let A be a finitely generated k-algebra. Then for every maximal ideal $\mathfrak{m} \subset A$, the natural map $k \to A \to A/\mathfrak{m}$ is an isomorphism of fields.*

PROOF. Since $\mathfrak{m}$ is maximal, $A/\mathfrak{m}$ is a field that is also finitely generated as a k-algebra. By corollary 3.7, $k \to A/\mathfrak{m}$ is then a finite extension of k. Since k is algebraically closed, this extension will be the identity. □

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

We deduce from the preceding corollary the Nullstellensatz.

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

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

is not the zero ring and so has a maximal ideal $\mathfrak{m} \subset A$. Observe that A is a finitely generated k-algebra (we can take the images of $x_1, \ldots, x_n$ and $1/\bar{f}$ as generators) and so the map $k \to A/\mathfrak{m}$ is by Corollary 3.8 an isomorphism. Denote by $\phi : k[x_1, \ldots, x_n] \to A \to A/\mathfrak{m} = k$ the corresponding surjection and put $p_i := \phi(x_i)$ and $p := (p_1, \ldots, p_n) \in \mathbb{A}^n$. So if we view x_i as a function on $\mathbb{A}^n$, then $\phi(x_i)$ is the value of x_i at p. The fact that ϕ is a homomorphism of k-algebras implies that it is then given as 'evaluation in p': for any $g \in k[x_1, \ldots, x_n]$ we have $\phi(g) = g(p)$. Since

the kernel of ϕ contains J, every $g \in J$ will be zero in p, in other words, $p \in Z(J)$. On the other hand, $f(p) = \phi(f)$ is invertible, for it has the image of $1/\bar{f}$ in $A/\mathfrak{m} = k$ as its inverse. So $f(p) \neq 0$. □

4. The affine category

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

DEFINITION 4.1. Let $X \subset \mathbb{A}^m$ and $Y \subset \mathbb{A}^n$ be closed subsets. We say that a map $f : X \to Y$ is *regular* if the components $f_1, \ldots, f_n$ 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 $g(y_1, \ldots, y_n)$ for every variable y_i a polynomial $f_i(x_1, \ldots, x_m)$ of m variables, we get a polynomial of m variables). So f then induces a k-algebra homomorphism $f^* : k[Y] \to k[X]$. This property is clearly equivalent to f being regular. The same argument shows that if $f : X \to Y$ and $g : Y \to Z$ are regular maps, then so is their composite $gf : X \to Z$. So we have a category (with objects the closed subsets of some affine space $\mathbb{A}^n$ and regular maps as defined above). In particular, we have a notion of isomorphism: a regular map $f : X \to Y$ is an *isomorphism* if is has a two-sided inverse $g : Y \to X$ which is also a regular map. This implies that $f^* : k[Y] \to k[X]$ has a two-sided inverse $g^* : k[X] \to k[Y]$ which is also an homomorphism of k-algebras, and hence is an isomorphism of k-algebras.

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 $\phi : k[Y] \to k[X]$. Then there is a unique regular map $f : X \to Y$ such that $f^* = \phi$.*

PROOF. The inclusion $j : Y \subset \mathbb{A}^n$ defines a k-algebra homomorphism $j^* : k[y_1, \ldots, y_n] \to k[Y]$ with kernel $I(Y)$. Put $f_i := \phi j^*(y_i) \in k[X]$ $(i = 1, \ldots, n)$ and define $f = (f_1, \ldots, f_n) : X \to \mathbb{A}^n$, so that $f^* y_i = f_i = \phi j^* y_i$. Since the k-algebra homomorphisms $f^*, \phi j^* : k[y_1, \ldots, y_n] \to k[X]$ coincide on the generators y_i, they must be equal: $f^* = \phi j^*$. It follows that f^* is zero on the kernel $I(Y)$ of j^*, which means that f takes its values in $Z(I(Y)) = Y$, and that the resulting map $k[Y] \to k[X]$ equals ϕ. The proof of uniqueness is left to you. □

In particular, an isomorphism of k-algebras $k[Y] \to k[X]$ comes from a unique isomorphism $X \to Y$. In the special case of an inclusion of a closed subset $Z \subset Y$, the induced map $k[Y] \to k[Z]$ is of course the formation of the quotient algebra $k[Z] = k[Y]/I_Y(X)$. So $f : X \to Y$ is an isomorphism of X onto a closed subset of Y (we then say that f is a *closed immersion*) if and only if $f^* : k[Y] \to k[X]$ is a surjection of k-algebras (with $\ker(f^*)$ being the ideal defining the image of f).

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

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

PROPOSITION 4.3. *The map which assigns to a closed subset of some $\mathbb{A}^n$ its coordinate ring defines an anti-equivalence between the category of closed subsets of affine spaces (whose morphisms are the regular maps) and the category of reduced finitely generated k-algebras (whose morphisms are k-algebra homomorphisms). It makes closed immersions correspond to epimorphisms of such k-algebras.*

EXAMPLE 4.4. Consider the regular map $f : \mathbb{A}^1 \to \mathbb{A}^2$, $f(t) = (t^2, t^3)$. The maps $\mathbb{A}^1$ bijectively onto the hypersurface (curve) C defined by $x^3 - y^2 = 0$: the image is clearly contained in C and the inverse sends $(0,0)$ to 0 and is on $C \setminus \{(0,0)\}$ given by $(x,y) \mapsto y/x$. The Zariski topology on $\mathbb{A}^1$ and C is the cofinite topology and so this is even a homeomorphism. In order to determine whether the inverse is regular, we consider f^*. We have $k[C] = k[x,y]/(x^3 - y^2)$, $k[\mathbb{A}^1] = k[t]$ and $f^* : k[C] \to k[t]$ is given by $x \mapsto t^2, y \mapsto t^3$. This algebra homomorphism is not surjective for its image misses $t \in k[t]$. In fact, f identifies $k[C]$ with the subalgebra $k + t^2k[t]$ of $k[t]$. So f is not an isomorphism.

EXAMPLE 4.5. An *affine-linear transformation* of k^n is of the form $x \in k^n \mapsto g(x) + a$, where $a \in k^n$ and $g \in \mathrm{GL}(n,k)$ is a linear transformation. Its inverse is $y \mapsto g^{-1}(y-a) = g^{-1}(y) - g^{-1}(a)$ and so of the same type. When we regard such an affine linear transformation as a map from $\mathbb{A}^n$ to itself, then it is regular: its coordinates $(g_1, \ldots, g_n)$ are polynomials of degree one. So an affine-linear transformation is also an isomorphism of $\mathbb{A}^n$ onto itself. When $n \geq 2$, there exist automorphisms of $\mathbb{A}^n$ not of this form. For instance $\sigma : (x,y) \mapsto (x, y + x^2)$ defines an automorphism of $\mathbb{A}^2$ with inverse $(x,y) \mapsto (x, y - x^2)$ (see also Exercise 18). This also shows that the group of affine-linear translations in $\mathbb{A}^n$ is not a normal subgroup, for conjugation by σ takes the transformation $(x,y) \mapsto (x+y, y)$ to an automorphism that is not affine-linear (check this). Hence the group of affine-linear transformations of $\mathbb{A}^n$ is not a "natural" subgroup of the automorphism group of $\mathbb{A}^n$ (this makes that the name *affine n-space* for $\mathbb{A}^n$ is a bit unfortunate).

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

(a) Prove that when $\mathrm{char}(k) \neq 2$, f defines an isomorphism[4] onto $\mathbb{A}^1 \setminus \{\pm\sqrt{-1}\}$.
(b) Consider the map $g : C \to \mathbb{A}^1$, $g(x,y) := x + \sqrt{-1}y$. Prove that when $\mathrm{char}(k) \neq 2$, g defines an isomorphism of C onto $\mathbb{A}^1 \setminus \{0\}$.
(c) Prove that when $\mathrm{char}(k) = 2$, the defining polynomial $x^2 + y^2 - 1$ for C is the square of a degree one polynomial so that C is a line.

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

[4] We have not really defined yet what is an isomorphism between two nonclosed subsets of an affine space. Interpret this here as: f^* maps $k[x,y][1/(x+1)]/(x^2+y^2-1)$ (the algebra of regular functions on $C \setminus \{p_0\}$) isomorphically onto $k[t][1/(t^2+1)]$ (the algebra of regular functions on $\mathbb{A}^1 \setminus \{\pm\sqrt{-1}\}$). This will be justified by Proposition 4.8.

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

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

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

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

We now have the following cases.

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

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

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

In particular, there are only a finite number of quadratic hypersurfaces up to isomorphism. (This is also true in characteristic two, but the discussion is a bit more delicate.)

The previous discussion (and in particular Proposition 4.3) leads us to associate to any finitely generated k-algebra A in a direct manner a space (which we shall denote by $\mathrm{Spm}(A)$) which for $A = k[X]$ yields a space homeomorphic to X. Since in that case the points of X correspond to maximal ideals of $k[X]$, we simply choose the underlying set of $\mathrm{Spm}(A)$ to be the collection of maximal ideals of A. For $x \in \mathrm{Spm}(A)$, we shall denote the corresponding maximal ideal of A by $\mathfrak{m}_x$. Since A is finitely generated as a k-algebra, $A/\mathfrak{m}_x$ can be identified with k by Corollary 3.8. We denote the resulting k-algebra homomorphism $A \to k$ by ρ_x. It is clear that any k-algebra homomorphism $A \to k$ has a maximal ideal of A as its kernel and so we may also think of $\mathrm{Spm}(A)$ as the set of k-algebra homomorphisms $A \to k$.

Any $f \in A$ defines defines a 'regular function' $\bar{f} : \mathrm{Spm}(A) \to k$ which takes in $x \in \mathrm{Spm}(A)$ the value $\rho_x(f) \in k$. So its zero set $Z(f) \subset \mathrm{Spm}(A)$ is the set of $x \in \mathrm{Spm}(A)$ with $f \in \mathfrak{m}_x$. We denote the complement of $\mathrm{Spm}(A) - Z(f)$ by $\mathrm{Spm}(A)_f$. We have $Z(ff') = Z(f) \cup Z(f')$ (for $\rho_x(ff') = \rho_x(f)\rho_x(f')$) and hence $\mathrm{Spm}(A)_{ff'} = \mathrm{Spm}(A)_f \cap \mathrm{Spm}(A)_{f'}$. So the collection of $\{\mathrm{Spm}(A)_f\}_{f \in A}$ is the basis of a topology on $\mathrm{Spm}(A)$. Note that a subset $\mathrm{Spm}(A)$ is closed precisely if it is an intersection of subsets of the form $Z(f)$; this is equal to the common zero set of the set of functions defined by an ideal of A. For $A = k[x_1, \ldots, x_n]/I$, the above

discussion shows that $\mathrm{Spm}(A)$ can be identified with $Z(I) \subset \mathbb{A}^n$ as a topological space and that under this identification, $A/(0)$ becomes the ring of regular functions on $Z(I)$. More generally, for any finitely generated k-algebra A, the map $f \mapsto \bar{f}$ maps A onto a subalgebra of the algebra of k-valued functions on $\mathrm{Spm}(A)$ with kernel the ideal of nilpotents (Exercise 20).

The space $\mathrm{Spm}(A)$ is called the *maximal ideal spectrum*[5] *of* R (but our notation for it is less standard). In case A is a reduced finitely generated k-algebra, we refer to $\mathrm{Spm}(A)$ as an *affine variety* (we will give a more complete definition later). We then recover A as its algebra of regular functions.

We observe for later reference:

LEMMA 4.7. *The maximal ideal spectrum* $\mathrm{Spm}(A)$ *is quasi-compact: every open covering of* $\mathrm{Spm}(A)$ *admits a finite subcovering.*

PROOF. It suffices to verify this for an open covering by principal open subsets. So let $S \subset A$ be such that $\mathrm{Spm}(A) = \cup_{g\in S} \mathrm{Spm}(A)_g$. This means that $\cap_{s\in S} Z(g) = \emptyset$. So the ideal generated by S is not contained in any maximal ideal and hence must be all of A. In particular, $1 = \sum_{i=1}^n g_i f_i$ for certain $f_i \in A$ and $g_i \in S$. It follows that $\{g_i\}_{i=1}^n$ generates A so that $\mathrm{Spm}(A) = \cup_{i=1}^n \mathrm{Spm}(A)_{g_i}$. □

A homomorphism $\phi : A \to B$ of finitely generated k-algebras gives rise to a map $\mathrm{Spm}(\phi) : \mathrm{Spm}(B) \to \mathrm{Spm}(A)$: if $y \in \mathrm{Spm}(B)$, then the composite homomorphism $\rho_y\phi : A \to k$ is the identity map when restricted to k so that $\phi^{-1}\mathfrak{m}_y$ is a maximal ideal of A with residue field k. We thus get a map

$$\mathrm{Spm}(\phi) : \mathrm{Spm}(B) \to \mathrm{Spm}(A).$$

characterized by $\mathfrak{m}_{\mathrm{Spm}(\phi)(y)} = \phi^{-1}\mathfrak{m}_y$. For $g \in A$, the preimage of $Z(g)$ under $\mathrm{Spm}(\phi)$ is $Z(\phi(g))$ and hence the preimage of $\mathrm{Spm}(A)_g$ is $\mathrm{Spm}(B)_{\phi(g)}$. This shows that $\mathrm{Spm}(\phi)$ is continuous. We call the resulting pair $(\mathrm{Spm}(\phi), \phi)$ a *morphism*.

PROPOSITION 4.8. *Let A be a finitely generated k-algebra. Then for every $g \in A$, $A[1/g]$ is a finitely generated k-algebra (which is reduced when A is) and the natural k-algebra homomorphism $A \to A[1/g]$ induces a homeomorphism of* $\mathrm{Spm}(A[1/g])$ *onto* $\mathrm{Spm}(A)_g = X - Z(g)$. *Moreover, for $g, g' \in A$ the following are equivalent:*

(i) $\mathrm{Spm}(A)_g \subset \mathrm{Spm}(A)_{g'}$,
(ii) *g' divides some positive power of g,*
(iii) *there exists a A-homomorphism $A[1/g'] \to A[1/g]$ (which must then be unique).*

PROOF. It is clear that $A[1/g]$ is a k-algebra and is as such finitely generated (just add to a generating set for A the generator $1/g$). We show that if A is reduced, then so is $A[1/g]$. For this we may suppose that g is not nilpotent (otherwise $A[1/g]$ is the zero ring). Suppose that $f/g^r \in A[1/g]$ is nilpotent: $(f/g^r)^m = 0$ for some $m \geq 1$. This means that there exists an $n \geq 0$ such that $f^m g^n = 0$. Then $(fg^n)^m = 0$ and since A is reduced it follows that $fg^n = 0$. So $f/g^r = fg^n/g^{r+n} = 0$ in $A[1/g]$.

A point of $A[1/g]$ is given by a k-algebra homomorphism $A[1/g] \to k$. This is the same thing as to give a k-algebra homomorphism $A \to k$ that is nonzero on g, in other words a point of $\mathrm{Spm}(A)_g$. So the map $A \to A[1/g]$ induces an

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

injection of $\mathrm{Spm}(A[1/g])$ in $\mathrm{Spm}(A)$ with image $\mathrm{Spm}(A)_g$. The map $\mathrm{Spm}(A[1/g]) \to \mathrm{Spm}(A)$ is a morphism and hence continuous. To see that it is also open, note that a principal open subset of $\mathrm{Spm}(A[1/g])$ is of the form $\mathrm{Spm}(A[1/g])_{f/g^n}$, with $f \in A$. By the preceding discussion we may identify this with $\mathrm{Spm}(A[1/g][g^n/f]) = \mathrm{Spm}(A[1/(fg)])$ and so its image in $\mathrm{Spm}(A)$ is the open subset $\mathrm{Spm}(A)_{fg}$.

We check the equivalence of the three conditions.

$(i) \Rightarrow (ii)$ If $\mathrm{Spm}(A)_g \subset \mathrm{Spm}(A)_{g'}$, then $Z(g) \supset Z(g')$ and so by the Nullstellensatz, $g \in \sqrt{(g')}$. This implies that we can write $g^n = fg'$ for some $f \in A$ and some $n \geq 1$ and (ii) follows.

$(ii) \Rightarrow (iii)$ If (ii) holds, then we have defined a A-homomorphism $A[1/g'] \to A[1/(fg')] = A[1/g^n] = A[1/g]$ that is easily checked to be independent of the choices made for n and f' and so (iii) follows.

$(iii) \Rightarrow (i)$ If we have an A-homomorphism $A[1/g'] \to A[1/g]$, then we get a morphism $\mathrm{Spm}(A[1/g]) \to \mathrm{Spm}(A[1/g'])$ whose composition with the identification of $\mathrm{Spm}(A[1/g'])$ with the open subset $\mathrm{Spm}(A)_{g'} \subset \mathrm{Spm}(A)$ yields the identification of $\mathrm{Spm}(A[1/g])$ with the open subset $\mathrm{Spm}(A)_g \subset \mathrm{Spm}(A)$. This means that $\mathrm{Spm}(A)_g \subset \mathrm{Spm}(A)_{g'}$ and shows at the same time that such an A-homomorphism is unique. □

From now on we identify a principal open subset $X_g = \mathrm{Spm}(A)_g$ with the maximal ideal spectrum $\mathrm{Spm}(A[1/g])$.

EXERCISE 19. Give an example of ring homomorphism $\phi : S \to R$ and a maximal ideal $\mathfrak{m} \subset R$, such that $\phi^{-1}\mathfrak{m}$ is not a maximal ideal of S. (Hint: take a look at Exercise 12.)

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

Let $f : X \to Y$ be a morphism between affine varieties. Since f is continuous, a fiber $f^{-1}(y)$, or more generally, the preimage $f^{-1}Z$ of a closed subset $Z \subset Y$, will be closed in X. It is the zero set of the ideal in $k[X]$ generated by $f^*I(Z)$. In fact, any ideal $I \subset k[X]$ can arise this way, for if $(f_1, \ldots, f_r) \in k[X]$ generate I, then take $f = (f_1, \ldots, f_r) : X \to \mathbb{A}^r = Y$ and $y = 0$. We will later see that the failure of $f^*I(Z)$ to be a radical ideal is sometimes a welcome property, as it can be exploited to define multiplicity. Here is a very simple example.

EXAMPLE 4.9. Let $f : X = \mathbb{A}^1 \to \mathbb{A}^1 = Y$ be defined by $f(x) = x^2$. Then $f^* : k[y] \to k[x]$ is given by $f^*y = x^2$. If we assume k not to be of characteristic 2, and we take $a \in Y \smallsetminus \{0\}$, then the fiber $f^{-1}(a)$ is defined by the ideal generated by $f^*(y - a) = x^2 - a$. It consists of two distinct points that are the two roots of $x^2 = a$, denoted $\pm\sqrt{a}$ and the pair of evaluation maps $(\rho_{\sqrt{a}}, \rho_{-\sqrt{a}})$ identifies the coordinate ring $k[x]/(x^2 - a)$ with $k \oplus k$. However, the fiber over $0 \in Y = \mathbb{A}^1$ is the singleton $\{0\} \subset X = \mathbb{A}^1$ and the ideal generated by $f^*y = x^2$ is not a radical ideal. This example indicates that there might good reason to accept nilpotent elements in the coordinate ring of $f^{-1}(0)$ by endowing $f^{-1}(0)$ with the ring of functions $k[f^{-1}(0)] := k[x]/(x^2)$. This is a k-vector space of dimension 2 (a k-basis is defined by the pair $\{1, x\}$) and we thus retain the information that two points have come together. The fiber should indeed be thought of as a point with multiplicity 2.

Example 4.4 shows that a continuous bijection (and even a homeomorphism) of affine varieties need not be an isomorphism. We next discuss a class of examples of an entirely different nature. It involves a notion that plays a central role in algebraic geometry when the base field k has positive characteristic.

EXAMPLE 4.10 (THE FROBENIUS MORPHISM). Assume that k has positive characteristic p and consider the morphism $\Phi_p : \mathbb{A}^1 \to \mathbb{A}^1$, $a \mapsto a^p$. If we remember that $\mathbb{A}^1$ can be identified with k, then we observe that under this identification, Φ_p is a field automorphism: $\Phi_p(a-b) = (a-b)^p = a^p - b^p = \Phi_p(a) - \Phi_p(b)$ (and of course $\Phi_p(ab) = (ab)^p = \Phi_p(a)\Phi_p(b)$). This shows that Φ_p is injective. Since k is algebraically closed, every element of k has a pth root and so Φ_p is also surjective. But the endomorphism Φ_p^* of $k[x]$ induced by Φ_p sends x to x^p and has therefore image $k[x^p]$. Clearly, Φ_p^* is not surjective.

The fixed point set of Φ_p (the set of $a \in \mathbb{A}^1$ with $a^p = a$) is via the identification of $\mathbb{A}^1$ with k just the prime subfield $\mathbb{F}_p \subset k$ and we therefore denote it by $\mathbb{A}^1(\mathbb{F}_p) \subset \mathbb{A}^1$. Likewise, the fixed point set $\mathbb{A}^1(\mathbb{F}_{p^r})$ of Φ_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 Φ_p act coordinatewise on $\mathbb{A}^n$, we get a morphism $\mathbb{A}^n \to \mathbb{A}^n$ (which we still denote by Φ_p) which is also a bijection. The fixed point of Φ_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 21. Assume that k has positive characteristic p. Let $q = p^r$ be a power of p with $r > 0$ and denote by $\mathbb{F}_q \subset k$ the subfield of $a \in k$ satisfying $a^q = a$. We write Φ_q for $\Phi_p^r : a \in \mathbb{A}^n \mapsto a^q \in \mathbb{A}^n$.

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

REMARK 4.11. After this exercise we cannot resist to mention the Weil zeta function. This function and its relatives—among them the Riemann zeta function—codify arithmetic properties of algebro-geometric objects in a very intricate manner. In the situation of Exercise 21, we can use the numbers $|Y(\mathbb{F}_{q^m})|$ (= the number of fixed points of Φ^m in Y) to define a generating series $\sum_{m\geq 1} |Y(\mathbb{F}_{q^m})|t^m$. It appears to be more convenient to work with the *Weil zeta function*:

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

which has the property that $t\frac{d}{dt}\log Z_Y$ yields the generating series above. This series has remarkable properties. For instance, a deep theorem due to Bernard Dwork (1960) asserts that it represents a rational function of t. Another deep theorem, due to Pierre Deligne (1974), states that the roots of the numerator and denominator

have for absolute value a nonpositive half-integral power of q and that moreover, these powers have an interpretation in terms of an 'algebraic topology for algebraic geometry', as 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 22. Compute the Weil zeta function of affine n-space relative to the field of q elements.

REMARK 4.12. The Frobenius morphism as defined above should not be confused with pth power map $F_A : a \in A \mapsto a^p \in A$ that we have on any k-algebra A (with k of characteristic $p > 0$) and that is sometimes referred to as the *absolute Frobenius*. This is a ring endomorphism but *not* a k-algebra endomorphism, for it is on k also the pth power map (the usual Frobenius F_k) and so not the identity. We can in a sense remedy this by replacing the ring homomorphism $i : k \hookrightarrow A$ that makes A a k-algebra by its precomposite with the F_k, i.e., by replacing $i : k \hookrightarrow A$ by $iF_k : k \hookrightarrow A$ (so this sends λ to $i(\lambda^p) = i(\lambda)^p$). The resulting k-algebra is called the *Frobenius twist* of A, and is denoted $A^{(p)}$. We now have a factorization

$$F_A : A \xrightarrow{F_k \otimes 1} A^{(p)} \xrightarrow{F_{A^{(p)}/k}} A,$$

where the first map is essentially the identity (but is not k-linear), whereas the second map is homomorphism of k-algebras. The induced map $\mathrm{Spm}(A^{(p)}) \to \mathrm{Spm}(A)$ is the identity, but the map induced by $F_{A^{(p)}/k}$, $\mathrm{Spm}(A) \to \mathrm{Spm}(A^{(p)})$ is in general not. Observe that the other composite $(F_k \otimes 1)F_{A^{(p)}/k} : A^{(p)} \to A^{(p)}$ is just the pth power map of $A^{(p)}$, $F_{A^{(p)}}$ (if we put $B := A^{(p)}$ and write $B^{(1/p)}$ for A, this reads as $F_B = (F_k^{-1} \otimes 1_B)F_{B/k} : B \to B^{(1/p)} \to B$).

Iterating this r times yields a k-algebra $A^{(q)}$ with $q = p^r$. If it so happens that A is given to us as obtained from a $\mathbb{F}_q$-algebra A_o by extension of scalars: $A = k \otimes_{\mathbb{F}_q} A_o$ (where we have identified $\mathbb{F}_q$ with a subfield of k), then $A^{(q)} = k^{(q)} \otimes_{\mathbb{F}_q} A_o$, and since the qth power map $k \to k^{(q)}$ is a field isomorphism, we can use that isomorphism to identify $A^{(q)}$ with A *as a k-algebra*. So the qth power map then *does* determine a k-algebra homomorphism $A \to A$ (given by $c \otimes_{\mathbb{F}_q} a_o \mapsto c \otimes_{\mathbb{F}_q} a_o^q$). It called the *geometric Frobenius*. For $A_o = \mathbb{F}_q[x_1, \ldots, x_n]$ (and more generally for the coordinate ring of an Y as above), this yields our Φ_q^*.

5. The sheaf of regular functions

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 property for a function to be regular is also local in nature.

Let A be a reduced finitely generated k-algebra. We abbreviate $X := \mathrm{Spm}(A)$. A principal neighborhood of $x \in X$ is of the form X_g with $g \in A - \mathfrak{m}_x$ and a regular function f on that neighborhood is an element of $A[1/g]$. Let us say that two such pairs (X_g, f) and $(X_{g'}, f')$ *have the same germ at* x if there exists a neighborhood U of x in $X_g \cap X_{g'}$ such that $f|U = f'|U$. This is an equivalence relation; an equivalence class is called a *germ of a regular function on X at x*. The germs of regular functions on X at x form an k-algebra, which we shall denote by $\mathcal{O}_{X,x}$. In fact $\mathcal{O}_{X,x}$ is nothing but the localization $A_{\mathfrak{m}_x}$ (so that $\mathcal{O}_{X,x}$ is a local ring): any $\phi \in A_{\mathfrak{m}_x}$ is represented by a fraction f/g with $f \in A$ and $g \in A - \mathfrak{m}_x$, hence comes from a regular function on the principal neighborhood X_g of x. And if ϕ is also given as

f'/g', then we have $(fg' - f'g)g''$ for some $g'' \in A - \mathfrak{m}_x$, which just means that f/g and f'/g' define the same element of $A[1/(gg'g'')]$, where we note that $gg'g'' \notin \mathfrak{m}_x$ so that $\mathrm{Spm}(A[1/(gg'g'')]) = X_{gg'g''}$ is a principal neighborhood of x in X. Observe that ρ_x defines a surjective 'evaluation homomorphism' $\rho_{X,x} : \mathcal{O}_{X,x} \to k$: it takes any $\phi \in \mathcal{O}_{X,x}$ as above to $\rho_x(f)/\rho_x(g)$. So ϕ is invertible in $\mathcal{O}_{X,x}$ precisely when $\rho_x(f) \neq 0$, or equivalently, when $\rho_{X,x}(\phi) \neq 0$ (with its inverse represented by g/f) and hence the kernel of $\rho_{X,x}$ is the maximal ideal $\mathfrak{m}_{X,x}$ of the local ring $\mathcal{O}_{X,x}$.

DEFINITION 5.1. A k-valued function ϕ defined on an open subset U of X is said to be regular at $x \in U$ if it defines an element of $\mathcal{O}_{X,x}$, in other words, if it defines a regular function on some principal neighborhood of x in X. We denote by $\mathcal{O}(U)$ the set of k-valued functions $U \to k$ that are regular at every point of U .

Note that is $\mathcal{O}(U)$ is in fact a k-algebra. We would like to call an element of $\mathcal{O}(U)$ a *regular function on* U, but we have that notion already defined in case $U = X$, or more generally, when U is a principal open subset. Fortunately, there is no conflict here:

PROPOSITION 5.2. *Let X be an affine variety and $X_g \subset X$ a principal open subset. Then the natural k-algebra homomorphism $k[X][1/g] \to \mathcal{O}(X_g)$ is an isomorphism.*

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

PROOF. The map $k[X][1/g] \to \mathcal{O}(X_g)$ is injective: if $f/g^r \in k[X][1/g]$ is in the kernel (with $f \in A$ and $r \geq 0$), then f must be identically zero as a function on X_g. Hence fg is zero everywhere and so f/g^r is zero in $k[X][1/g]$.

For surjectivity, let $\phi : X_g \to k$ be regular in every point of X_g. We must show that ϕ is representable by $f/g^r \in k[X]$ for some $f \in k[X]$ and $r \geq 0$. By assumption there exist for every $x \in X$, $g_x \in k[X] \setminus \mathfrak{m}_x$ and $f_x \in k[X]$ such that $\phi|X_{g_x} \cap X_g$ is representable as f_x/g_x. Upon replacing g_x by $g_x g$ and f_x by $f_x g$, we may assume that $X_{g_x} \subset X_g$ so that f_x/g_x represents $\phi|X_{g_x}$.

Since X_g is quasicompact (Lemma 4.7), the covering $\{X_{g_x}\}_{x \in X}$ of X_g has a finite subcovering $\{X_{g_{x_i}}\}_{i=1}^N$. Let us write f_i for f_{x_i} and g_i for g_{x_i}. Then f_i/g_i and f_j/g_j define the same regular function on $X_{g_i} \cap X_{g_j} = X_{g_i g_j}$ and so $g_i f_j - g_j f_i$ is annihilated by $(g_i g_j)^{m_{ij}}$ for some $m_{ij} \geq 0$. Put $m := \max\{m_{ij}\}$, so that $g_i^{m+1} g_j^m f_j = g_j^{m+1} g_i^m f_i$ for all i, j. Upon replacing f_i by $f_i g_i^m$ and g_i by g_i^{m+1}, we may then assume that in fact $g_i f_j = g_j f_i$ for all i, j.

Since the $\cup_i X_{g_i} = X_g$, we have $\cap_i Z(g_i) = Z(g)$, and so by the Nullstellensatz there must exist an $r > 0$ such that $g^r = \sum_{i=1}^N h_i g_i$ for certain $h_i \in k[X]$. Now consider $f := \sum_{i=1}^N h_i f_i \in k[X]$. We have for every j,

$$fg_j = \sum_{i=1}^N h_i f_i g_j = \sum_{i=1}^N h_i g_i f_j = g^r f_j$$

and so the restriction of f/g^r to X_{g_j} is equal to f_j/g_j. As this is also the restriction of ϕ to X_{g_j} and $\cup_j X_{g_j} = X_g$, it follows that ϕ is represented by f/g^r.

The last statement is left as an exercise. □

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

DEFINITION 5.3. Let X be a topological space and R a ring. A *sheaf $\mathcal{O}$ of R-valued functions*[6] on X assigns to every open subset U of X an R-subalgebra $\mathcal{O}(U)$ of the R-algebra of R-valued functions on U with the property that

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

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

This definition simply expresses the fact that the functions we are considering are characterized by a local property—just as we have a sheaf of continuous $\mathbb{R}$-valued functions on a topological space, a sheaf of differentiable $\mathbb{R}$-valued functions on a manifold and a sheaf of holomorphic $\mathbb{C}$-valued functions on a complex manifold. In fact for the definition below of an affine variety (and the one of a variety that we shall give later), we take our cue from the definition of a manifold.

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

Note that a sheaf $\mathcal{O}$ of R-valued functions on X restricts to a sheaf $\mathcal{O}|U$ for every open $U \subset X$. We are now ready to introduce the notion of an affine variety in a more proper fashion.

DEFINITION 5.4. A topological space X endowed with a sheaf $\mathcal{O}_X$ of k-valued functions is called an *affine variety* when it is isomorphic to a pair $(\mathrm{Spm}(A), \mathcal{O}_{\mathrm{Spm}(A)})$ as above. We refer to $\mathcal{O}_X(X)$ as its *coordinate ring* and usually denote it by $k[X]$.

We call $(X, \mathcal{O}_X)$ a *quasi-affine variety* if it is isomorphic to an open subset of some pair $(\mathrm{Spm}(A), \mathcal{O}_{\mathrm{Spm}(A)})$.

Thus a reduced finitely generated k-algebra defines an affine variety and conversely, an affine variety determines a reduced finitely generated k-algebra. These two assignments are inverses of each other. The present definition lends itself better than the previous one to immediate generalization (e.g., when we will introduce the notion of a variety) and has other technical advantages as well. Here is an example.

EXAMPLE 5.5. Here is an example an affine open subset of an affine variety that is not principal. Take the cuspidal plane cubic curve $C \subset \mathbb{A}^2$ of Example 4.4 defined by $y^2 = x^3$ and assume that k *is of characteristic zero*. As we have seen, the parametrization $f : t \in \mathbb{A}^1 \mapsto (t^2, t^3) \in C$ identifies $k[C]$ with the subalgebra $k + t^2k[t]$ of $k[t]$. Now let $a \in \mathbb{A}^1 \smallsetminus \{0\}$. So $C \smallsetminus \{f(a)\}$ is quasi-affine. But $C \smallsetminus \{f(a)\}$ is not a principal open subset: it is not of the form C_g for some $g \in k[x, y]$. For then $f^*(g)$ would have a as its only zero, so that f^*g is a nonzero constant times $(t-a)^n$. But the coefficient of t in $(t-a)^n$ is $n(-a)^{n-1}$, and hence nonzero. This contradicts the fact that $f^*g \in k + t^2k[t]$.

We claim however that $C \smallsetminus \{f(a)\}$ is even affine with coordinate ring via f^* identified with $\mathrm{Spm}\, k[t^2, t^3, t^2/(t-a)]$. Let us first observe that $k[t^2, t^3, t^2/(t-a)]$ is a finitely generated k-algebra contained in the reduced k-algebra $k[t][1/(t-a)]$. So it defines an affine variety

[6] We give the general definition of a sheaf later. This will do for now. A defect of this definition is that a sheaf of R-valued functions on a space X need not restrict to one on a subspace of X.

$\tilde{C}$ and the inclusion $k[t^2,t^3] \subset k[t^2,t^3,t^2/(t-a)]$ defines a morphism $j : \tilde{C} \to C$. We prove that j is an isomorphism of $\tilde{C}$ onto $C \smallsetminus \{f(a)\}$ (it will then follow that $C \smallsetminus \{f(a)\}$ is affine).

We do this by localization: the ideal generated by $f^*x = t^2$ in $k[C]$ defines $\{f(0)\}$ and so $k[C \smallsetminus \{f(0)\}] = k[C][1/t^2] = k[t^2,t^3,t^{-2}] = k[t,t^{-1}]$. On the other hand,

$$k[\tilde{C} \smallsetminus j^{-1}\{f(0)\}] = k[t^2,t^3,t^2/(t-a)][t^{-2}]) = \\ = k[t,t^{-1},(t-a)^{-1}] = k[C \smallsetminus \{f(0)\}][1/(t-a)] = k[C \smallsetminus \{f(0),f(a)\}].$$

From this it is clear that $\tilde{C} \smallsetminus j^{-1}\{f(0)\}$ maps isomorphically onto $C \smallsetminus \{f(0),f(a)\}$. It remains to prove that there is neighborhood U of $(0,0) \in \mathbb{A}^2 \smallsetminus \{f(a)\}$ such that j maps $j^{-1}(C \cap U)$ isomorphically onto $C \cap U$. We take for U the principal open subset $\mathbb{A}^2_{x-a^2}$. Then $k[C \cap U] = k[t^2,t^3][1/(t^2-a^2)]$ and $k[j^{-1}(C \cap U)] = k[t^2,t^3,t^2/(t-a)][1/(t^2-a^2)]$. But these k-algebras are the same as $t^2/(t-a) \in k[t^2,t^3][1/(t^2-a^2)]$.

Other such examples (among them nonsingular plane cubic curves) that are also valid in positive characteristic are best understood after we have discussed the Picard group.

6. The product

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

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

It is clear that $\mathbb{A}^{m+n}_{f*g} = \mathbb{A}^m_f \times \mathbb{A}^n_g$, which shows that the Zariski topology on $\mathbb{A}^{m+n}$ refines the product topology on $\mathbb{A}^m \times \mathbb{A}^n$. Equivalently, if $X \subset \mathbb{A}^m$ and $Y \subset \mathbb{A}^n$ are closed, then $X \times Y$ is closed in $\mathbb{A}^{m+n}$. We give $X \times Y$ the topology it inherits from $\mathbb{A}^{m+n}$ (which is finer than the product topology when $m > 0$ and $n > 0$). For the coordinate rings we have defined a map:

$$k[X] \times k[Y] \to k[X \times Y], \quad (f,g) \mapsto f * g$$

which is evidently k-bilinear (i.e., k-linear in either variable). We want to prove that the ideal $I(X \times Y)$ defining $X \times Y$ in $\mathbb{A}^{m+n}$ is generated by $I(X)$ and $I(Y)$ (viewed as subsets of $k[x_1,\dots,x_m,y_1,\dots y_n]$) 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. This is the setting that is needed later anyhow.)

If R is a ring and M and N are R-modules, then we can form their *tensor product over* R, $M \otimes_R N$: as an abelian group $M \otimes_R N$ is generated by the expressions $a \otimes_R b$, $a \in M$, $b \in N$ and subject to the conditions $(ra) \otimes_R b = a \otimes_R (rb)$, $(a+a') \otimes_R b = a \otimes_R b + a' \otimes_R b$ and $a \otimes_R (b+b') = a \otimes_R b + a \otimes_R b'$. So a general element of $M \otimes_R N$ can be written like this: $\sum_{i=1}^N a_i \otimes_R b_i$, with $a_i \in M$ and $b_i \in N$. We make $M \otimes_R N$ an R-module if we stipulate that $r(a \otimes_R b) := (ra) \otimes_R b$ (which is then also equal to $a \otimes_R (rb)$). Notice that the map

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

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

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

EXERCISE 23. Prove that $\otimes_R$ is universal for this property in the sense that every R-bilinear map $M \times N \to P$ of R-modules is the composite of $\otimes_R$ and a *unique* R-homomorphism $M \otimes_R N \to P$. In other words, the map

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

is an isomorphism of R-modules.

EXERCISE 24. Let m and n be nonnegative integers. Prove that $\mathbb{Z}/(n) \otimes_{\mathbb{Z}} \mathbb{Z}/(m)$ can be identified with $\mathbb{Z}/(m, n)$.

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

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

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

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

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

EXERCISE 25. 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 6.1. *For closed subsets $X \subset \mathbb{A}^m$ and $Y \subset \mathbb{A}^n$ the bilinear map $k[X] \times k[Y] \to k[X \times Y]$, $(f, g) \mapsto f * g$ induces an isomorphism $\mu : k[X] \otimes k[Y] \to k[X \times Y]$ of k-algebras (so that in particular $k[X] \otimes k[Y]$ is reduced).*

If X and Y are irreducible, then so is $X \times Y$, or equivalently, if $k[X]$ and $k[Y]$ are domains, then so is $k[X] \otimes k[Y]$.

PROOF. Since the obvious map

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

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

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

Suppose now X and Y irreducible. We prove that $k[X] \otimes k[Y]$ is a domain so that $X \times Y$ is irreducible. Let $\phi, \psi \in k[X] \otimes k[Y]$ be such that $\phi\psi = 0$. Since the restriction of $\phi\psi = 0$ to $\{p\} \times Y \cong Y$ is $\phi_p \psi_p$ and $k[Y]$ is a domain, it follows that $\phi_p = 0$ or $\psi_p = 0$. So $X = X(\phi) \cup X(\psi)$. Since X is irreducible we have $X = X(\phi)$ or $X(\psi)$. This means that $\phi = 0$ or $\psi = 0$. □

EXERCISE 26. Let A and B be finitely generated k-algebras. Prove that $A \otimes_k B$ is a finitely generated algebra and define a natural map $\mathrm{Spm}(A \otimes_k B) \to \mathrm{Spm}(A) \times \mathrm{Spm}(B)$ and show that this is a bijection (hint: do *not* use Proposition 6.1).

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

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

7. Function fields and rational maps

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

Let X be an affine variety. Recall that an element $\phi \in \mathrm{Frac}(k[X])$ is by definition represented by a fraction f/g with $f, g \in k[X]$ and g not a zero divisor in $k[X]$. We need the following lemma.

LEMMA 7.1. *Let X be an affine variety and let $C_1, \ldots, C_r$ be its distinct irreducible components. Then for any $g \in k[X]$ the following are equivalent: (i) g is a zero divisor of $k[X]$, (ii) $C_i \subset Z(g_i)$ for some i and (iii) X_g is not dense in X. Moreover, any open-dense subset of X contains a principal open-dense subset defined by a nonzero divisor.*

The restriction maps (well-defined in view of the above) defines an isomorphism of k-algebras

$$R = (R_i)_{i=1}^r : \mathrm{Frac}(k[X]) \to \oplus_{i=1}^r \mathrm{Frac}(k[C_i]), \quad f/g \mapsto (f/g\big|_{C_i})_{i=1}^r$$

(note that the right hand side is a direct sum of fields).

PROOF. Choose for $i = 1, \ldots, r$ a nonzero $h_i \in I(\cup_{j \neq i} C_j)$.

$(i) \Rightarrow (ii)$ Let $g \in k[X]$ be a zero divisor. Then there exists a nonzero $g' \in k[X]$ with $gg' = 0$. Let C_i be such that $g'|C_i$ is nonzero. Then we must have $g|C_i = 0$.

$(ii) \Rightarrow (iii)$ If $C_i \subset Z(g)$, then clearly, X_g (and hence its closure) is contained in the proper closed subset $\cup_{j \neq i} C_j \neq X$.

$(iii) \Rightarrow (i)$ If X_g is not dense in X, then its closure is a proper closed subset of X and so there exists a nonzero $g' \in k[X]$ with $X_g \subset Z(g')$. This implies that $gg' = 0$ and so g is a zero divisor.

To prove the second assertion, let $U \subset X$ be open-dense. Then for every i, $(C_i \smallsetminus \cup_{j \neq i} C_j) \cap U$ is nonempty and so contains a nonempty principal open subset X_{f_i}. Then $f_i|C_j$ is nonzero if and only $j = i$. This is also so for $h_i|C_j$: it is nonzero if and only if $i = j$. We put $g := \prod_i (f_i + \sum_{j \neq i} h_j)$. Its restriction to C_i is $f_i h_i^{r-1}|C_i$ and so $C_i \cap X_g = C_i \cap X_{f_i} \cap X_{h_i}$. The latter is nonempty and open (hence dense) in C_i and contained in $C_i \cap U$. So X_g is an open-dense in X and contained in U.

As to the last assertion, if $f/g \in \mathrm{Frac}(k[X])$ is such that $R_i(f/g) = 0$ for all i, then $f|C_i = 0$ for all i and hence $f = 0$. So R is injective. To see that R is onto, let for $i = 1, \ldots, r$, $f_i/g_i \in \mathrm{Frac}(k[C_i])$. Let $\tilde{f}_i, \tilde{g}_i \in k[X]$ map to $f_i, g_i \in k[C_i]$ and put $f = \sum_i h_i \tilde{f}_i$ and $g := \sum_i h_i \tilde{g}_i$. Then $f|C_i = h_i|C_i.f_i$ and $g|C_i = h_i|C_i.g_i$ and the latter is nonzero. So g is not a zero divisor of $k[X]$ so that $f/g \in \mathrm{Frac}(k[X])$ and we have $R_i(f/g) = f_i/g_i$. □

COROLLARY 7.2. *If ϕ is a regular function defined on an open-dense subset U of X, then ϕ determines an element of $\mathrm{Frac}(k[X])$. All elements of $\mathrm{Frac}(k[X])$ are thus obtained and two pairs (U,ϕ) and (U',ϕ') determine the same element of $\mathrm{Frac}(k[X])$ if and only if $\phi|U\cap U' = \phi'|U\cap U'$.*

PROOF. Let $\phi \in \mathrm{Frac}(k[X])$ be represented as a fraction f/g. Since g is a nonzero divisor, Lemma 7.1 tells us that f/g defines a regular function on an principal open-dense subset of X (namely X_g). If ϕ is also represented by f'/g', then $fg' - f'g = 0$ and so the two associated regular functions on X_g and $X_{g'}$ have the same restriction to the principal open-dense subset $X_{gg'} = X_g \cap X_{g'}$ of X.

Conversely, suppose ϕ is a regular function on an open-dense subset U of X. According to Lemma 7.1, $U \supset X_g$ for some nonzero divisor g and hence $\phi|X_g$ is by Proposition 5.2 given by $f/g^r \in \mathrm{Frac}(k[X])$ for some $f \in k[X]$. □

There is in general no best way to represent a given element of $\mathrm{Frac}(k[X])$ as a fraction (as there is in a UFD), and so we must be content with the corollary above. Note that it is essentially equivalent to the assertion that

$$\mathrm{Frac}(k[X]) = \varinjlim_{g \text{ nonzero divisor in } k[X]} k[X][1/g] = \varinjlim_{U \text{ open-dense in } X} \mathcal{O}_X(U).$$

An element of $\mathrm{Frac}(k[X])$ is often called a *rational function* on X. This is the algebro-geometric analogue of a meromorphic function in complex function theory. When X is irreducible, then $\mathrm{Frac}(k[X])$ is a field, called the *function field of X*, and will be denoted $k(X)$.

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

DEFINITION 7.3. Let X and Y be affine varieties. A *rational map* from X to Y is given by a pair (U,F), where U is an open-dense subset of X and $F : U \to Y$ is a morphism, with the understanding that a pair (U',F') defines the same rational map if F and F' coincide on an open-dense subset of $U\cap U'$ (then they coincide on all of $U\cap U'$ by continuity, but formulated in this way we see that we are dealing with an equivalence relation). We denote such a rational map as $f : X \dashrightarrow Y$.

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

So a rational map $f : X \dashrightarrow \mathbb{A}^1$ is same thing as a rational function on X.

Observe that for a morphism of affine varieties $f : X \to Y$, $g \in \ker(f^*)$ is equivalent to $f(X) \subset Z_g$ and hence equivalent to the closure $f(X)$ being contained in Z_g. It follows that f is dominant if and only if f^* is injective.

PROPOSITION 7.4. *Any finitely generated field extension of k is k-isomorphic to the function field of an irreducible affine variety. If X and Y are irreducible affine varieties, then a dominant rational map $f : X \dashrightarrow Y$ determines a k-linear field embedding $f^* : k(Y) \hookrightarrow k(X)$ and conversely, every k-linear field embedding $k(Y) \to k(X)$ is of this form for a unique dominant rational map f.*

PROOF. Let K/k be a finitely generated field extension of k. This means there exist elements $a_1,\dots,a_n \in K$ such that every element of K can be written as a fraction of polynomials in $a_1,\dots,a_n$ with coefficients in k. So the k-subalgebra of K generated by $a_1,\dots,a_n$ is a domain $A \subset K$ (since K is a field) that has K as its field of fractions. Since A is the coordinate ring of a closed irreducible subset $X \subset \mathbb{A}^n$

(defined by the kernel of the obvious ring homomorphism $k[x_1, \ldots, x_n] \to A$), it follows that K can be identified with $k(X)$.

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

It remains to show that every k-linear field homomorphism $\Phi : k(Y) \to k(X)$ is so obtained. For this, choose generators $b_1, \ldots, b_m$ of $k[Y]$. Then $\Phi(b_1), \ldots, \Phi(b_m)$ are rational functions on X and so are regular on a principal nonempty subset $X_h \subset X$. Since $b_1, \ldots, b_m$ generate $k[Y]$ as a k-algebra, it follows that Φ maps $k[Y]$ to $k[X_h] = k[X][1/h] \subset k(X)$. This k-algebra homomorphism defines a morphism $F : X_h \to Y$ such that $F^* = \Phi | k[Y]$. The image of F will be dense by the argument above: if $g \in k[Y]$ vanishes on $F(X_h)$, then $\Phi(g) = F^*(g) = 0$, which implies $g = 0$, since Φ is injective. It is clear that Φ is the extension of F^* to the function fields.

As to the uniqueness: if (U', F') is another solution, then choose a nonempty principal subset $U'' \subset U \cap U'$ such that F and F' both define morphisms $U'' \to Y$. These must be equal since the associated k-algebra homomorphisms $k[Y] \to k[U'']$ are the same (namely the restriction of Φ). □

The following exercise explains the focus on irreducible varieties when considering rational maps.

EXERCISE 28. Let X and Y be an affine varieties with distinct irreducible components $X_1, \ldots, X_r$ resp. $Y_1, \ldots, Y_s$. Prove that to give a rational map $f : X \dashrightarrow Y$ is equivalent to giving a rational map $f_i : X_i \dashrightarrow Y_{j_i}$ for $i = 1, \ldots, r$. Show that f is dominant if and only if for each $j \in \{1, \ldots, s\}$, there exists an $i_j \in \{1, \ldots, r\}$ such that f maps X_{i_j} to Y_j as a dominant map.

EXERCISE 29. Let $f \in k[x_1, \ldots, x_{n+1}]$ be irreducible of positive degree. Its zero set $X \subset \mathbb{A}^{n+1}$ is then closed and irreducible. Assume that the degree d of f in x_{n+1} is positive.

(a) Prove that the projection $\pi : X \to \mathbb{A}^n$ induces an injective k-algebra homomorphism $\pi^* : k[x_1, \ldots, x_n] \to k[X] = k[x_1, \ldots, x_n]/(f)$.
(b) Prove that π is dominant and that the resulting field homomorphism $k(x_1, \ldots, x_n) \to k(X)$ is a finite extension of degree d.

COROLLARY 7.5. *Two dominant maps $f : X \dashrightarrow Y$ and $g : Y \dashrightarrow Z$ between irreducible affine varieties can be composed to yield a dominant map $gf : X \dashrightarrow Z$ so that we have a category with the irreducible affine varieties as objects and the rational dominant maps as morphisms. Assigning to an irreducible affine variety its function field makes this category anti-equivalent to the category of finitely generated field extensions of the base field k.*

PROOF. The dominant maps yield k-linear field extensions $f^* : k(Y) \hookrightarrow k(X)$ and $g^* : k(Z) \hookrightarrow k(Y)$ and these can be composed to give a k-linear field extension $f^*g^* : k(Z) \hookrightarrow k(X)$. Proposition 7.4 says that this is induced by a unique rational map $X \dashrightarrow Z$. This we define to be gf. The rest of the corollary now follows. □

PROPOSITION-DEFINITION 7.6. *A rational map $f : X \dashrightarrow Y$ is an isomorphism in the above category (that is, induces a k-linear isomorphism of function fields) if and*

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

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

Suppose now we have a k-linear isomorphism $k(Y) \cong k(X)$. Represent this isomorphism and its inverse by (U, F) and (V, G) respectively. Since $F^{-1}V$ is a nonempty open subset of U, it contains a nonempty principal open subset X_g. Since GF induces the identity on $k(X)$, its restriction to X_g must be the inclusion $X_g \subset X$. Since X_g is dense in $F^{-1}V$, and GF is continuous, the same is then true of GF: it is the inclusion $F^{-1}V \subset X$. This implies that F maps $F^{-1}V$ injectively to $G^{-1}U$. For the same reason, G maps $G^{-1}U$ injectively to $F^{-1}V$. So F defines an isomorphism between the open subsets $F^{-1}V \subset X$ and $G^{-1}U \subset Y$. □

EXERCISE 30. Assume k not of characteristic 2. Let $X \subset \mathbb{A}^2$ be defined by $x_1^2 + x_2^2 = 1$. Prove that X is birationally equivalent to the affine line $\mathbb{A}^1$. (Hint: take a look at Exercise 17.) More generally, prove that the quadric in $\mathbb{A}^{n+1}$ defined by $x_1^2 + x_2^2 + \cdots x_{n+1}^2 = 1$ is birationally equivalent to $\mathbb{A}^n$. What about the zero set in $\mathbb{A}^{n+1}$ of a quadric function?

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

EXAMPLE 7.7. Suppose k has characteristic $p > 0$. We take $X = \mathbb{A}^1 = Y$ and let $f = \Phi_p$ be the Frobenius map: $f : a \in \mathbb{A}^1 \mapsto a^p \in \mathbb{A}^1$. Then f is homeomorphism, but $f^* : k[Y] = k[y] \to k[x] = k[X]$ is given by $y \mapsto x^p$ and so induces the field extension $k(y) = k(x^p) \subset k(x)$, which is of degree p. From the perspective of Y, we have enlarged its algebra of regular functions by introducing a formal pth root of its coordinate y (which yields another copy of $\mathbb{A}^1$, namely X). From the perspective of X, $k[Y]$ is just the subalgebra $f^*k[X]$.

This is in fact the basic example of a *purely inseparable* field extension, i.e., an algebraic field extension L/K with the property that every element of L has a minimal polynomial in $K[T]$ that has precisely one root in L Such a polynomial must be of the form $T^{p^r} - c$, with $c \in K$ not a p-th power of an element of K when $r > 0$, where p is the characteristic of K (for $p = 0$ we necessarily have $L = K$). So if $L \neq K$, then the absolute Frobenius map $a \in K \mapsto a^p \in K$ is not surjective. Purely inseparable extensions are not detected by Galois theory, for they have trivial Galois group as there is only one root to move around.

EXERCISE 31. Let $f : X \dashrightarrow Y$ be a dominant rational map of irreducible affine varieties which induces a purely inseparable field extension $k(Y)/k(X)$. Prove that there is an open-dense subset $V \subset Y$ such that f defines a homeomorphism $f^{-1}V \to V$. (Hint: show first that it suffices to treat the case when $k(X)$ is obtained from $k(Y)$ by adjoining the pth root of an element $f \in k(Y)$. Then observe that

if f is regular on the affine open-dense $V \subset Y$, then Y contains as an open dense subset a copy of the locus of $(x,t) \in V \times \mathbb{A}^1$ satisfying $t^p = f$.)

The following Corollary 7.8 suggests that if X is an irreducible affine veriety, then the transcendence degree of $k(X)/k$ may be understood as the dimension of X. We shall come back to this and then improve upon the corollary below.

COROLLARY 7.8. *Let X be an irreducible affine variety X and denote by r the transcendence degree of $k(X)/k$. Then there exists an irreducible hypersurface Y in $\mathbb{A}^{r+1}$ and a rational dominant map $f : X \dashrightarrow Y$ which is purely inseparable in the sense that $k(X)$ is a purely inseparable extension of $k(Y)$. In particular (in view of Exercise 31 above), there an open-dense subset $V \subset Y$ such that f defines a homeomorphism $f^{-1}V \to V$.*

Before we give the proof, we recall some basic facts from field theory. For any algebraic extension L/K, the elements of L that are separable over K make up an intermediate extension L^{sep}/K that is (of course) separable and is such that L/L^{sep} is purely inseparable. When L is an algebraic closure of K, then L^{sep} is called a *separable algebraic closure* of K: it is a separable algebraic extension of K which is maximal for that property. Then L is as an extension of L^{sep} obtained by successive adjunction of p-power roots of elements of L^{sep}.[7] In case L/K is a finitely generated extension, then by the theorem of the primitive element, L^{sep}/K has a single generator.

PROOF OF COROLLARY 7.8. Let $k[X]$ be generated by $b_1, \ldots, b_m$, say, then we may after renumbering assume that for some $r \leq m$, $b_1, \ldots, b_r$ are algebraically independent (so that the k-linear field homomorphism $k(\mathbb{A}^r) = k(x_1, \ldots, x_r) \to k(X)$ which sends x_i to b_i is injective) and that for $i > r$, b_i is algebraic over $k(b_1, \ldots, b_{i-1})$. Then $k(b_1, \ldots, b_r) \cong k(\mathbb{A}^r)$ is a purely transcendental extension of k and $k(X)$ is a finite extension of $k(\mathbb{A}^r)$ so that r is the *transcendence degree* of $k(X)/k$. It is clear that the inclusion $k(\mathbb{A}^r) \subset k(X)$ defines a dominant rational map $X \dashrightarrow \mathbb{A}^r$. The theorem of the primitive element implies that the separable closure of $k(\mathbb{A}^r)$ in $k(X)$ has a single generator b. This b is a root of an irreducible polynomial $F \in k(\mathbb{A}^r)[T]$. If we clear denominators, we may assume that the coefficients of F lie in $k[\mathbb{A}^r]$ so that $F \in k[\mathbb{A}^{r+1}]$ and then we can take for Y the hypersurface in $\mathbb{A}^{r+1}$ defined by F. We now have obtained a dominant rational map $f : X \dashrightarrow Y$ such that $k(X)/k(Y)$ is purely inseparable extension. □

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

Here is an observation which not only illustrates how affine varieties over algebraically nonclosed fields can arise when dealing with affine k-varieties, but one that also suggests that we ought to enlarge the maximal ideal spectrum. Let $f : X \to Y$ be a dominant morphism of irreducible affine varieties. This implies

[7] In case L/K is a finite normal extension (i.e., a finite extension with the property that every $f \in K[x]$ that is the minimal polynomial of some element of L has all its roots in L), then the fixed point set of the Galois group of L/K is a subextension L^{insep}/L that is purely inseparable, whereas L/L^{insep} separable. Then the natural map $L^{\text{sep}} \otimes_K L^{\text{insep}} \to L$ is an isomorphism of K-algebras.

that $f^* : k[Y] \to k[X]$ is injective and that $f(X)$ contains an open-dense subset of Y. Then we may ask whether there exists something like a general fiber: is there an open-dense subset $V \subset Y$ such that the fibers $f^{-1}(y)$, $y \in V$ all "look the same"? The question is too vague for a clear answer and for most naive ways of making this precise, the answer will be no. For instance, we could simply refuse to specify one such V by allowing it to be arbitrarily small, but if we then want to implement this idea by taking the (projective) limit $\varprojlim_{V \text{ open-dense in } Y} f^{-1}V$, then we end up with the empty set unless Y is a singleton. However, its algebraic counterpart, which amounts to making all the nonzero elements of $k[Y]$ in $k[X]$ invertible,

$$\varinjlim_{V \text{ open-dense in } Y} k[f^{-1}V] = (k[Y] \smallsetminus \{0\})^{-1}k[X] = k(Y) \otimes_{k[Y]} k[X]$$

(these equalities follow from the fact that $k[X] = k[Y] \otimes_{k[Y]} k[X]$), is nontrivial. It is in fact a reduced finitely generated $k(Y)$-algebra and this hints that an adequate geometric description requires that we include more points. First of all, we would like to regard the maximal ideal spectrum of $k(Y) \otimes_{k[Y]} k[X]$ as an affine variety over the (algebraically nonclosed) field $k(Y)$ so that every regular function on X which comes from Y is now treated as a scalar (and will be invertible when nonzero).[8] And secondly, in order to give this a geometric content, we would like that every irreducible variety Z defines a point η_Z (its *generic point*) with 'residue field' $k(Z)$, which for a singleton must give us back its unique element with the field k. For we then can extend f to the points defined by closed irreducible subsets $Z \subset X$ by putting $f(\eta_Z) := \eta_{\overline{f(Z)}}$. Then as a set, the generic fiber of f is the fiber of this extension over η_Y, i.e., the set of η_Z for which $f|Z : Z \to Y$ is dominant. Such considerations directly lead to the notion of a scheme that we shall discuss later.

8. Finite morphisms

In this section A is a ring and B is a A-algebra. In other words, we are given a ring homomorphism $A \to B$ (that is sometimes denoted by B/A). We adopt the following standard terminology: we say that B is *finite over* A if B is a finitely generated A-module and we say that B is an *extension* of A if $A \to B$ is injective (so that we may regard A as subring of B). So B/A is called a finite extension if both $A \to B$ is injective and B is a finitely generated A-module.

PROPOSITION-DEFINITION 8.1. *We say that $b \in B$ is* integrally dependent *on A if one the following equivalent properties is satisfied.*

(i) *b is a root of a monic polynomial $x^n + a_1x^{n-1} + \cdots + a_n \in A[x]$,*
(ii) *$A[b]$ is finitely generated as an A-module,*
(iii) *b is contained in a A-subalgebra $C \subset B$ which is finitely generated as an A-module.*

PROOF. $(i) \Rightarrow (ii)$. If b is a root of $x^n + a_1x^{n-1} + \cdots + a_n \in A[x]$, then clearly $A[b]$ is generated as a A-module by $1, b, b^2, \ldots, b^{n-1}$.

$(ii) \Rightarrow (iii)$ is obvious.

[8] Our notion of affine variety required that we work over an algebraically closed field. This is of course arranged by choosing an algebraic closure L of $k(Y)$. The maximal ideal spectrum of $L \otimes_{k[Y]} k[X]$ is then an affine L-variety, and yields a notion of a *general fiber* that is even closer to our geometric intuition.

$(iii) \Rightarrow (i)$. Suppose that C is as in (iii). Choose an epimorphism $\pi : A^n \to C$ of A-modules and denote the standard basis of A^n by $(e_1, \dots, e_n)$. We may (and will) assume that $\pi(e_1) = 1_B$. Since $b \in C$, this extends to an epimorphism $A[b]^n \to C$, that we will also denote by π. By assumption, $b\pi(e_i) = \sum_{j=1}^n a_{ij}\pi(e_j)$ for certain $a_{ij} \in A$. We regard the $n \times n$-matrix $\sigma := (b\delta_{ij} - a_{ij})_{i,j}$ with entries in $A[b]$ as an $A[b]$-endomorphism of $A[b]^n$. Then $\pi\sigma(e_i) = 0$ for all i, in other words, $\pi\sigma = 0$.

Now Cramer's rule can be understood as stating that if σ' is the matrix of cofactors of σ, then $\sigma\sigma' = \det(\sigma)1_n$, where we note that $\det(\sigma)$ is a monic polynomial in b with coefficients in A. We thus find that in B,

$$\det(\sigma) = \det(\sigma)\pi(e_1) = \pi(\det(\sigma)e_1) = \pi(\sigma\sigma'(e_1)) = (\pi\sigma)(\sigma'(e_1)) = 0. \qquad \square$$

COROLLARY-DEFINITION 8.2. *The set elements of B that are integrally dependent on A is an A-subalgebra of B. We call this subalgebra the* integral closure *of A in B (and denoted it by $\overline{A}^B$).*

PROOF. It is enough to prove that if $b, b' \in B$ are integrally dependent over A, then so is every element of $A[b, b']$. Or what amounts to the same: if $A[b]$ and $A[b']$ are finitely generated A-modules, then so is $A[b, b']$. This is clear: if $\{b^k\}_{k=0}^{n-1}$ generates $A[b]$ and $\{b'^k\}_{k=0}^{n'-1}$ generates $A[b']$, then $\{b^k b'^{k'}\}_{k=0,k'=0}^{n,n'}$ generates $A[b, b']$. $\square$

DEFINITION 8.3. We say that B is *integral over* A if every element of B is integral over A (so that $B = \overline{A}^B$). If in addition the given homomorphism $A \to B$ is injective (so that A may be regarded as a subring of B), then we say that B is an *integral extension* of A.

The characterization (iii) of Proposition 8.1 shows that when B is finite over A (resp. a finite extension of A), then B is integral over A (resp. an integral extension of A). An important class of example appears in algebraic number theory: if L is a finite field extension of $\mathbb{Q}$ (also called an *algebraic number field*), then the integral closure of $\mathbb{Z} \subset \mathbb{Q}$ defines a subring of L, called the *ring of integers* of L. This ring is often denoted by $\mathcal{O}_L$.

EXERCISE 32. Prove that 'being integral over' is transitive: if B is an A-algebra integral over A, then any B-algebra that is integral over B is as an A-algebra integral over A.

PROPOSITION 8.4. *Let $A \subset B$ be an integral extension and suppose B is a domain. Then $\mathrm{Frac}(B)$ is an algebraic field extension of $\mathrm{Frac}(A)$, which is finite whenever B is a finite extension of A.*

PROOF. We first show that $\mathrm{Frac}(B) = \mathrm{Frac}(A)B$. Let $b \in B \smallsetminus \{0\}$. It is a root of a monic polynomial $x^n + a_1x^{n-1} + \cdots + a_n = 0$ ($a_i \in A$) with $a_n \neq 0$ and so $1/b = -1/a_n.(b^{n-1} + a_1b^{n-2} + \cdots + a_{n-1}) \in \mathrm{Frac}(A)B$.

Since B is a union of finitely generated A-modules, $\mathrm{Frac}(A)B$ is a union of finite dimensional $\mathrm{Frac}(A)$-vector spaces and hence an algebraic extension of $\mathrm{Frac}(A)$. The last assertion follows from the observation that any set of A-module generators of B is also a set of $\mathrm{Frac}(A)$-vector space generators of $\mathrm{Frac}(A)B$. $\square$

There are two simple ways of producing new integral extensions out of a given one, namely reduction and localization: Suppose $A \to B$ is integral. Then for every ideal $J \subset B$, $J \cap A$ is (clearly) an ideal of A and $A/J \cap A \subset B/J$ is an integral extension. And if $S \subset A$ is a multiplicative subset, then the induced ring

homomorphism $S^{-1}A \to S^{-1}B$ is integral. Both appear in the proof of the 'Going up theorem' below. For this we will also need:

LEMMA 8.5 (Nakayama's Lemma). *Let R be a local ring with maximal ideal $\mathfrak{m}$ and M a finitely generated R-module. Then a finite subset $S \subset M$ generates M as a R-module if (and only if) the image of S in $M/\mathfrak{m}M$ generates the latter as a $R/\mathfrak{m}$-vector space. In particular (take $S = \emptyset$), $\mathfrak{m}M = M$ implies $M = 0$.*

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

PROPOSITION 8.6 (Going up). *Let $A \subset B$ be an integral extension and let $\mathfrak{p} \subset A$ be a prime ideal of A. Then the* going up *property holds: $\mathfrak{p}$ is of the form $\mathfrak{q} \cap A$, where $\mathfrak{q}$ is a prime ideal of B. If also is given is a prime ideal $\mathfrak{q}'$ of B with the property that $\mathfrak{p} \supset \mathfrak{q}' \cap A$, then we can take $\mathfrak{q} \supset \mathfrak{q}'$. Moreover the* incomparability *property holds: two distinct prime ideals of B having the same intersection with A cannot obey an inclusion relation.*

PROOF. The localization $A \to A_{\mathfrak{p}}$ yields a local ring with maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$ and the prime ideals of $A_{\mathfrak{p}}$ correspond (by taking the preimage in A) to the prime ideals of A that contain $\mathfrak{p}$. The localization $A_{\mathfrak{p}}B$ (as a A-module) is by the observation above, an integral extension of $A_{\mathfrak{p}}$. If we find a prime ideal $\tilde{\mathfrak{q}}$ of $A_{\mathfrak{p}}B$ with $\tilde{\mathfrak{q}} \cap A_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$, then the preimage $\mathfrak{q}$ of $\tilde{\mathfrak{q}}$ in B is a prime ideal of B with the property that $\mathfrak{q} \cap A$ is the preimage of $\mathfrak{p}A_{\mathfrak{p}}$ in A and so this is just $\mathfrak{p}$. Hence for the first assertion there is no loss in generality in assuming that A is a local ring and $\mathfrak{p}$ is its unique maximal ideal $\mathfrak{m}_A$.

We claim that $\mathfrak{m}_A B \neq B$. Suppose this is not so. Then write $1 \in B$ as an $\mathfrak{m}_A$-linear combination of a finite set elements of B. Denote by B' the A-subalgebra of B generated by this finite set. Since B is an integral extension of A, B' is finite over A. Since $1 \in \mathfrak{m}_A B'$, we have $B' = \mathfrak{m}_A B'$, and it then follows from Nakayama's Lemma 8.5 that $B' = 0$. It follows that $1 = 0$ so that A is the zero ring. This contradicts our assumption that A has a maximal ideal.

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

For the refinement and the incomparability property we can, simply by passing to $A/(\mathfrak{q}' \cap A) \subset B/\mathfrak{q}'$ (which is still an integral extension by the observation above), assume that $\mathfrak{q}' = 0$. This reduces the refinement to the case already treated and for the incomparability property we apply this reduction to the case $\mathfrak{q}' = \mathfrak{q}$: then this amounts showing that for any nonzero prime ideal $\mathfrak{q}''$ of B, $\mathfrak{q}'' \cap A$ is nonzero. To see this, let $b \in \mathfrak{q}'' \smallsetminus \{0\}$. Then b is a root of a monic polynomial: $b^n + a_1 b^{n-1} + \cdots + a_{n-1}b + a_n = 0$ ($a_i \in A$), where we can of course assume that $a_n \neq 0$ (otherwise divide by b). We then find that $0 \neq a_n \in Bb \cap A \subset \mathfrak{q}'' \cap A$. □

REMARK 8.7. Let us agree to call a *prime chain* (of length n) in a ring R a strictly ascending sequence $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ of prime ideals in R. The going up property may then be restated as saying that for an integral extension $A \subset B$,

any prime chain in A is the intersection with A of a prime chain in B, where we even may prescribe the first member of the latter in advance. The incomparability property says that the intersection a prime chain in B with A is a prime chain in A.

DEFINITION 8.8. We say that a morphism of affine varieties $f : X \to Y$ is *finite* if the k-algebra homomorphism $f^* : k[Y] \to k[X]$ is finite, i.e., makes $k[X]$ a finitely generated $k[Y]$-module (so $k[X]$ is then integral over $k[Y]$).

So $f^* : k[Y] \to k[X]$ is a finite extension if and only if f is finite and dominant.

EXERCISE 33. Prove that if Y is an affine variety, then the disjoint union of its irreducible components is finite over Y.

Propositions 8.4 and 8.6 give in the algebro-geometric setting:

COROLLARY 8.9. *Let $f : X \to Y$ be a finite, dominant morphism of affine varieties. Then f is surjective and every closed irreducible subset $P \subset Y$ is the image of a closed irreducible subset $Q \subset X$. If furthermore is given a closed irreducible subset $Q' \subset X$ with $P \subset f(Q')$, then we may choose $Q \subset Q'$. If in addition X is irreducible, then so is Y and $f^* : k(Y) \to k(X)$ is a finite algebraic extension of fields.*

PROOF. To see that f is surjective, let $p \in Y$. Then there exists by Proposition 8.6 a prime ideal $\mathfrak{q} \subset k[X]$ such that $\mathfrak{m}_p = (f^*)^{-1}\mathfrak{q}$. So if $q \in Z(\mathfrak{q})$, then $\mathfrak{m}_p = (f^*)^{-1}\mathfrak{q} \subset (f^*)^{-1}\mathfrak{m}_q$ and hence $f(q) = p$. Similarly, if $P \subset Y$ is irreducible, then $\mathfrak{p} := I(P)$ is a prime ideal and so $(f^*)^{-1}\mathfrak{q} = \mathfrak{p}$ for some prime ideal $\mathfrak{q}$. Then $Q := Z(\mathfrak{q})$ is irreducible. Note that f^* induces the morphism $k[P] = k[Y]/\mathfrak{p} \to k[X]/\mathfrak{q} = k[Q]$. This is a finite extension and so by what we just proved, f induces a surjective morphism $Q \to P$. In other words, $f(Q) = P$. The other two assertions are easy consequences of Proposition 8.6. □

EXERCISE 34. Let $f : X \to Y$ be a finite morphism of affine varieties. Prove that f is closed and that every fiber $f^{-1}(y)$ is finite (possibly empty). Assuming that in addition that f is surjective, prove that if $Y' \subset Y$ is closed or a principal open subset of Y, then the restriction $f : f^{-1}Y' \to Y'$ is also a finite morphism.

THEOREM 8.10 (Noether normalization). *Let K be a field and m an integer ≥ 0. Every K-algebra A with m generators is a finite (hence integral) extension of a polynomial algebra over K with $\leq m$ generators: there exist an integer $0 \leq r \leq m$ and an injection $K[x_1, \dots, x_r] \hookrightarrow A$ such that A is finite over $K[x_1, \dots, x_r]$.*

The proof will be with induction on m. The following lemma provides the induction step.

LEMMA 8.11. *Let $\phi : K[x_1, \dots, x_m] \to A$ be an epimorphism of K-algebras which is not an isomorphism. Then there exists a surjective K-algebra homomorphism $\phi' : K[x_1, \dots, x_m] \to A$ such that $\phi'(x_m) = \phi(x_m)$ and $\phi'(x_m)$ is integral over $\phi'(K[x_1, \dots, x_{m-1}])$.*

PROOF. We define for any positive integer s a K-algebra automorphism σ_s of $K[x_1, \dots, x_m]$ by $\sigma_s(x_i) := x_i + x_m^{s^{m-i}}$ when $i \leq m-1$ and $\sigma_s(x_m) = x_m$. This is indeed an automorphism with inverse given by $\sigma_s^{-1}(x_i) = x_i - x_m^{s^{m-i}}$ for $i < m-1$ and $\sigma_s(x_m) = x_m$. So if $I = (i_1, \dots, i_m) \in \mathbb{Z}^m_{\geq 0}$, then

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

When viewed as an element of $K[x_1,\dots,x_{m-1}][x_m]$, this is a monic polynomial in x_m of degree $p_I(s) := i_1 s^{m-1} + i_2 s^{m-2} + \cdots + i_m$. Now give $\mathbb{Z}^m_{\geq 0}$ the lexicographic ordering. Then $I > J$ implies $p_I(s) > p_J(s)$ for s large enough. Choose a nonzero $f \in \ker(\phi)$. If $I \in \mathbb{Z}^m_{\geq 0}$ is the largest multi-exponent of a monomial that appears in f with nonzero coefficient, then for s large enough, $\sigma_s(f)$ is a constant times a monic polynomial in x_m of degree $p_I(s)$ with coefficients in $K[x_1,\dots,x_{m-1}]$. In other words, the image of x_m in $K[x_1,\dots,x_m]/(\sigma_s(f))$ is integral over the image of $K[x_1,\dots,x_{m-1}]$ in $K[x_1,\dots,x_m]/(\sigma_s(f))$. This is then certainly true for their images in $K[x_1,\dots,x_m]/\sigma_s(\ker(\phi)) = K[x_1,\dots,x_m]/\ker(\phi\sigma_s^{-1})$. This is equivalent to the image of $\sigma_s^{-1}(x_m) = x_m$ in $K[x_1,\dots,x_m]/\ker(\phi) \cong A$ being integral over $\phi\sigma_s^{-1}(K[x_1,\dots,x_{m-1}])$. Hence $\phi' := \phi\sigma_s^{-1}$ is as desired. □

PROOF OF NOETHER NORMALIZATION. Let $\phi : K[x_1,\dots,x_m] \to A$ be an epimorphism of K-algebras. When ϕ is an isomorphism, there is nothing to show. Otherwise, Lemma 8.11 tells us that there exists a K-algebra homomorphism $\phi' : K[x_1,\dots,x_m] \to A$ such that $\phi'(x_m)$ is integral over $A' := \phi'(K[x_1,\dots,x_{m-1}])$. Since the K-algebra A' has $\leq m-1$ generators, it is by induction a finite extension of some polynomial algebra $K[x_1,\dots,x_r]$ with $r \leq m-1$. Hence so is A. □

REMARK 8.12. If A is a domain, then according to Proposition 8.4, $\mathrm{Frac}(A)$ will be a finite extension of $K(x_1,\dots,x_r)$ and so r must be the transcendence degree of $\mathrm{Frac}(A)/K$. In particular, r is an invariant of A.

COROLLARY 8.13. *For every affine variety X there exists an integer $r \geq 0$ and a finite surjective morphism $f : X \to \mathbb{A}^r$.*

This corollary gives us a better grasp on the geometry of X, especially when X is irreducible, for it shows that X can be 'spread' in a finite-to-one manner over affine r-space. Proposition 8.4 has a kind of converse, also due to Noether, which we state without proof.

*THEOREM 8.14 (Emmy Noether). *Let A be a domain that contains a field over which it is finitely generated as an algebra. Then for any finite field extension $L/\mathrm{Frac}(A)$, the integral closure $\overline{A}^L$ of A in L is finite over A.*

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

LEMMA 8.15. *Any unique factorization domain is normal.*

PROOF. Let A be a UFD. Any $b \in \mathrm{Frac}(A)$ integral over A obeys an equation $b^d + a_1 b^d + \cdots + a_d = 0$ with $a_i \in A$. Write $b = r/s$ with $r, s \in A$ such that r and s are relatively prime. The identity $r^d + a_1 r s^{d-1} + \cdots + a_d s^d = 0$ shows that any prime divisor which divides s must divide r^d and hence also r. As there is no such prime, it follows that s is a unit so that $b \in A$. □

Proposition 8.14 has a remarkable geometric interpretation: let be given an irreducible affine variety Y and a finite field extension $L/k(Y)$. Then Proposition 8.14 asserts that $\overline{A}^L$ is a finitely generated $k[Y]$-module. It is also a domain (because it is contained in a field) and so it defines an irreducible variety $Y_L := \mathrm{Spec}(\overline{A}^L)$. Since $A \subset \overline{A}^L$ is an integral extension, we have a finite surjective

morphism $Y_L \to Y$. This morphism induces the given field extension $L/k(Y)$. So every finite field extension of $k(Y)$ is canonically realized by a finite morphism of irreducible affine varieties!

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

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

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

Of special interest is the case of a finite normal[9] field extension.

NORMAL EXTENSIONS. We recall that an algebraic field extension L/K is *normal* if an irreducible polynomial in $K[x]$ that has one root in L has *all* its roots in L, i.e., factors in $L[x]$ into polynomials of degree one. A Galois extension L/K is the same thing as a normal separable extension (this property can be used as a definition). But a purely inseparable extension L/K is also normal, for then these irreducible (monic) polynomials are of the form $(x-b)^q$, with $b \in L$ and q the smallest power such that $b^q \in K$ (if $q \neq 1$, then the characteristic p of k must be positive and q will be a power of p). Clearly an algebraic closure $\overline{K}$ of K is normal.

Part of Galois theory still works for normal extensions. If L/K is normal, then all the K-linear field embeddings $L \hookrightarrow \overline{K}$ have the same image and so this image is invariant under the full Galois group of $\overline{K}/K$. The latter then restricts to the group of K-linear field automorphisms of L (the Galois group of L/K) and this group permutes the roots of a minimal polynomial in $K[x]$ of any element of L transitively.

For an arbitrary algebraic field extension F/K, one defines its *normal closure* in $\overline{K}$ as the smallest normal extension of K in $\overline{K}$ that admits a K-linear embedding of F into it. It is obtained as the subfield of $\overline{K}$ generated by the roots of all the irreducible polynomials of $K[x]$ that have a root in F. When F is finite over K, then so is its normal closure in $\overline{K}$.

We begin with the corresponding result in commutative algebra. This has also important applications in algebraic number theory.

PROPOSITION 8.16. *Let A be a normal domain and $L/\operatorname{Frac}(A)$ be a finite normal extension with Galois group G. Then G leaves invariant the integral closure $\overline{A}^L$ of A in L, and for every prime ideal $\mathfrak{p} \subset A$, G acts transitively on the set of prime ideals $\mathfrak{q} \subset \overline{A}^L$ that lie over $\mathfrak{p}$ (i.e., with $\mathfrak{q} \cap A = \mathfrak{p}$).*

For the proof we need:

LEMMA 8.17 (The prime avoidance lemma). *Any ideal of a ring that is contained in a finite union of prime ideals is contained in one of them.*

PROOF. Let R be a ring, $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ prime ideals in R and $I \subset R$ an ideal contained in $\cup_{i=1}^{n} \mathfrak{q}_i$. We prove with induction on n that $I \subset \mathfrak{q}_i$ for some i. The case $n = 1$ being trivial, we may assume that $n > 1$ and that for every $i = 1, \ldots, n$, I

[9] As the statement of Proposition 8.16 illustrates, this adjective is a bit overused in mathematics: a *normal* field extension should not be confused with the *normality* of a ring.

is not contained in $\cup_{j\neq i}\mathfrak{q}_j$. Choose $a_i \in I \smallsetminus \cup_{j\neq i}\mathfrak{q}_j$. So then $a_i \in \mathfrak{q}_i$. Consider $a := a_1a_2\cdots a_{n-1} + a_n$. Then $a \in I$ and hence $a \in \mathfrak{q}_i$ for some i. If $i < n$, then $a_n = a - a_1a_2\cdots a_{n-1} \in \mathfrak{q}_i$ and we get a contradiction. If $i = n$, then $a_1a_2\cdots a_{n-1} = a - a_n \in \mathfrak{q}_n$ and hence $a_j \in \mathfrak{q}_n$ for some $j \leq n-1$. This is also a contradiction. □

PROOF OF PROPOSITION 8.16. That any $g \in G$ leaves $\overline{A}^L$ invariant is clear, for g fixes the coefficients of an equation of integral dependence over A.

Let $\mathfrak{q}$ and $\mathfrak{q}'$ be prime ideals of $\overline{A}^L$ that lie over $\mathfrak{p}$. We show that $\mathfrak{q}' \subset \cup_{g\in G} g\mathfrak{q}$. This suffices, for then the prime avoidance lemma implies that $\mathfrak{q}' \subset g\mathfrak{q}$ for some $g \in G$. As both $\mathfrak{q}'$ and $g\mathfrak{q}$ lie over $\mathfrak{p}$, we must have $\mathfrak{q}' = g\mathfrak{q}$ by incomparability.

Let $b \in \mathfrak{q}'$ be nonzero. Let $f(x) = x^n + a_1x^{n-1} + \cdots + a_n \in \mathrm{Frac}(A)[x]$ be a minimum polynomial for b. Since $L/\mathrm{Frac}(A)$ is a normal extension, f completely factors in L with roots in Gb: $f(x) = (x - g_1(b))\cdots(x - g_n(b))$ for certain $g_i \in G$. Since $g_i(b) \in \overline{A}^L$ we have $g_1(b)\cdots g_n(b) \in \overline{A}^L$. On the other hand, $g_1(b)\cdots g_n(b) = (-1)^n a_n \in \mathrm{Frac}(A)$ and since A is normal it follows that $g_1(b)\cdots g_n(b) \in A$. One of the factors is b and so $g_1(b)\cdots g_n(b) \in A \cap (b) \subset A \cap \mathfrak{q}' = \mathfrak{p} \subset \mathfrak{q}$. Since $\mathfrak{q}$ is a prime ideal, some factor g_ib lies in $\mathfrak{q}$ and hence $b \in \cup_{g\in G} g\mathfrak{q}$. □

We translate this into geometry:

COROLLARY 8.18. *Let Y be a normal variety and $L/k(Y)$ a normal finite extension with Galois group G. Then G acts naturally on Y_L in such a manner that for any closed irreducible $Z \subset Y$, G acts transitively on the irreducible components of the preimage of Z in Y_L, In particular any fiber of $Y_L \to Y$ is a G-orbit.*

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

COROLLARY 8.19 (Going down). *Let $A \subset B$ be a finite extension with B a domain and A normal. Given prime ideals $\mathfrak{p}$ in A and $\mathfrak{q}'$ in B such that $\mathfrak{p} \subset \mathfrak{q}' \cap A$, then there exists a prime ideal $\mathfrak{q}$ in B with $\mathfrak{q} \subset \mathfrak{q}'$ and $\mathfrak{q} \cap A = \mathfrak{p}$.*

PROOF. Put $K := \mathrm{Frac}(A)$ and let L be the normal closure of $\mathrm{Frac}(B)$ in an algebraic closure of $\mathrm{Frac}(B)$. Since B is integral over A, we have $B \subset \overline{A}^L$. Now L is a finite normal extension of $\mathrm{Frac}(B)$ (with Galois group G, say), and this brings us in the situation of Proposition 8.16 above. Since $\mathrm{Frac}(B)$ is finite over K, L is finite over K and so $\overline{A}^L$ is by 8.14 finite over A (and hence also over B).

Put $\mathfrak{p}' := \mathfrak{q}' \cap A$ so that $\mathfrak{p}' \supset \mathfrak{p}$. According to Proposition 8.6 we can find in a prime ideal $\tilde{\mathfrak{q}}'$ in $\overline{A}^L$ which meets B in $\mathfrak{q}'$. The same proposition tells us that there exist nested prime ideals $\tilde{\mathfrak{p}}' \supset \tilde{\mathfrak{p}}$ in $\overline{A}^L$ which meet A in $\mathfrak{p}' \supset \mathfrak{p}$. Since $\tilde{\mathfrak{q}}'$ and $\tilde{\mathfrak{p}}'$ both meet A in $\mathfrak{p}'$, there exists according to Proposition 8.16 a $g \in G$ such that $g\tilde{\mathfrak{p}}' = \tilde{\mathfrak{q}}'$. Upon replacing $\tilde{\mathfrak{p}}' \supset \tilde{\mathfrak{p}}$ by $g'\tilde{\mathfrak{p}}' \supset g\tilde{\mathfrak{p}}$, we may then assume that $\tilde{\mathfrak{p}}' = \tilde{\mathfrak{q}}'$. Now $\mathfrak{q} := \tilde{\mathfrak{p}} \cap B$ is as desired, for it meets A in $\mathfrak{p}$ and is contained in $\tilde{\mathfrak{p}}' \cap B = \tilde{\mathfrak{q}}' \cap B = \mathfrak{q}$. □

REMARK 8.20. We can rephrase this in the spirit of Remark 8.7 by saying that any prime chain in A is the intersection of prime chain in B for which the *last* member has been prescribed in advance.

9. Dimension

One way to define the dimension of a topological space X is with induction: agree that the empty set has dimension -1 and that X has dimension $\leq n$ if it

admits a basis of open subsets such that the boundary of every basis element has dimension $\leq n-1$. This is close in spirit to the definition that we shall use here (which is however adapted to the Zariski topology; as you will find in Exercise 35, it is useless for Hausdorff spaces).

DEFINITION 9.1. 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 $X^0 \supsetneq X^1 \supsetneq \cdots \supsetneq X^d$ 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 9.2. *For a locally closed subset Z of a topological space X we have* $\dim Z \leq \dim X$.

PROOF. Our hypothesis implies that if Y is closed in Z, then its closure $\overline{Y}$ in X has the property that $\overline{Y} \cap Z = Y$. We also know that if $Y \subset Z$ is irreducible, then so is $\overline{Y}$. So if we have an irreducible chain of length d in Z, then the closures of the members of this chain yield an irreducible chain of length d in X. This proves that $\dim Z \leq \dim X$. □

EXERCISE 35. What is the Krull dimension of a nonempty Hausdorff space?

EXERCISE 36. 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 37. Suppose that X is a noetherian space. Prove that the dimension of X is the maximum of the dimensions of its irreducible components. Prove also that if all the singletons (= one element subsets) in X are closed, then $\dim(X) = 0$ if and only if X is finite.

It is straightforward to translate this notion into algebra:

DEFINITION 9.3. The *Krull dimension* $\dim(R)$ of a ring R is the supremum of the integers d for which there exists an *prime chain of length* d in R, where we stipulate that the zero ring (i.e., the ring which has no prime ideals) has Krull dimension -1.

It is clear that for a closed subset $X \subset \mathbb{A}^n$, $\dim k[X] = \dim X$. Since any prime ideal of a ring R contains the ideal $\sqrt{(0)}$ of nilpotents, R and its 'reduction' $R_{\mathrm{red}} := R/\sqrt{(0)}$ have the same Krull dimension. So the Krull dimension of a finitely generated k-algebra A is that of the affine variety $\mathrm{Spm}(A)$.

Remark 8.7 shows immediately:

LEMMA 9.4. *The Krull dimension is invariant under integral extension: if B is integral over A, then A and B have the same Krull dimension.*

REMARK 9.5. For a domain A the zero ideal (0) is a prime ideal and so $\dim(A) = 0$ if and only if A (0) is maximal, i.e., A is a field. We say that a noetherian domain A is a *Dedekind domain* if $\dim(A) \leq 1$, in other words, if every nonzero prime ideal is maximal. For instance, a unique factorization domain (such as $\mathbb{Z}$ and $K[X]$ with K a field) is a Dedekind domain. The importance of this notion comes from the fact that a converse holds on the level of ideals: any ideal of a Dedekind domain is uniquely written a product of prime ideals. Lemma 9.4 shows that any finite extension of a Dedekind domain (such as the ring of integers of an algebraic number field and a finite extension of $K[X]$) is a Dedekind domain.

The Krull dimension was easy to define, but seems difficult to compute in concrete cases. How can we be certain that a given prime chain has maximal possible length? It is not even clear how to tell whether the Krull dimension of a given ring is finite. We will settle this in a satisfactory manner for a domain B containing a field K over which it is a finitely generated: we show that a length of a prime chain in B is bounded by the transcendence degree $\mathrm{Frac}(B)/K$ and that we have equality when the prime chain is maximal (so that the length of *any* maximal prime chain is the Krull dimension).

THEOREM 9.6. *Let K be a field and B a finitely generated K-algebra without zero divisors. Then the Krull dimension of B equals the transcendence degree of $\mathrm{Frac}(B)/K$ and every maximal prime chain in B (i.e., one that cannot be extended to a longer prime chain) has length $\dim B$.*

PROOF. We prove both assertions with induction on the transcendence degree of $\mathrm{Frac}(B)/K$. By Noether normalization there exists an integer $r \geq 0$ and a K-algebra monomorphism $K[x_1, \ldots, x_r] \hookrightarrow B$ such that B is finite over $K[x_1, \ldots, x_r]$. We put $A := K[x_1, \ldots, x_r]$. Then $\mathrm{Frac}(B)$ is a finite extension of $\mathrm{Frac}(A) = K(x_1, \ldots, x_r)$ and so the transcendence degree of $\mathrm{Frac}(B)/K$ is r. In A we have the length r prime chain $(0) \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq \cdots \subsetneq (x_1, x_2, \ldots, x_r)$. By Remark 8.7 this is the intersection of A with a prime chain in B and so the Krull dimension of B is at least r.

To prove the remaining assertions, let $\mathfrak{q}_\bullet := ((0) = \mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_m)$ be a prime chain in B. We prove that its length m is at most r with equality when $\mathfrak{q}_\bullet$ is a maximal prime chain. By the incomparability property of 'going up' (Proposition 8.6), $\mathfrak{p}_\bullet := \mathfrak{q}_\bullet \cap A$ will be a prime chain in A, also of length m. The idea is to show that $\mathfrak{p}_1$ defines a closed subset of $\mathbb{A}^r_K$ of dimension $\leq m-1$. Choose an irreducible $f \in \mathfrak{p}_1$. After renumbering the coordinates, we may assume that f does not lie in $K[x_1, \ldots, x_{r-1}]$. So if we write $f = \sum_{i=0}^N a_i x_r^i$ with $a_i \in K[x_1, \ldots, x_{r-1}]$ and $a_N \neq 0$, then $N \geq 1$. Since f is irreducible, $A/(f)$ is a domain. The image of x_r in $\mathrm{Frac}(A/(f))$ is a root of the monic polynomial $t^N + \sum_{i=0}^{N-1}(a_i/a_0)t^i \in K(x_1, \ldots, x_{r-1})[t]$, and so $\mathrm{Frac}(A/(f))$ is a finite extension of $K(x_1, \ldots, x_{r-1})$. In particular, $\mathrm{Frac}(A/(f))$ has transcendence degree $r-1$ over K. By our induction induction hypothesis, $A/(f)$ has then Krull dimension $r-1$. Since the image of $\mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_m$ in $A/(f)$ is a prime chain of length $m-1$ (it is strictly ascending, because it is so in $A/\mathfrak{p}_1$), it follows that $m-1 \leq r-1$. Hence $m \leq r$.

If $\mathfrak{q}_\bullet$ is a maximal prime chain in B, then by 'going down' (Corollary 8.19), we find a prime ideal $\mathfrak{q} \subset \mathfrak{q}_1$ such that $\mathfrak{q} \cap A = (f)$, and the maximality of $\mathfrak{q}_\bullet$ then implies that $\mathfrak{q} = \mathfrak{q}_1$ and hence that $(f) = \mathfrak{p}_1$. Since $\mathrm{Frac}(B/\mathfrak{q}_1)$ is a finite extension of $\mathrm{Frac}(A/(f))$ (which in turn is a finite extension of $K(x_1, \ldots, x_{r-1})$), it has transcendence degree $r-1$ over k. As $\mathfrak{q}_1 \subsetneq \mathfrak{q}_2 \cdots \subsetneq \mathfrak{q}_m$ defines a maximal prime chain in $B/\mathfrak{q}_1$, it follows from our induction hypothesis that $m-1 = r-1$ and so $m = r$. □

COROLLARY 9.7. *In the situation of Theorem 9.6, let $\mathfrak{m}$ be a maximal ideal of B. Then the Krull dimension of the localization $B_\mathfrak{m} = (B \setminus \mathfrak{m})^{-1}B$ is that of B.*

PROOF. Any prime chain in $B_\mathfrak{m}$ is a prime chain in B contained in $\mathfrak{m}$. So by Theorem 9.6, the Krull dimension of $B_\mathfrak{m}$ is finite. If such a chain is maximal for this property, then it will end with $\mathfrak{m}$ and will also be maximal in B (for there is no

prime ideal strictly containing $\mathfrak{m}$) and again by Theorem 9.6 its length is then the Krull dimension of B. □

COROLLARY 9.8. *Let X be an irreducible affine variety of dimension d. Then every maximal irreducible chain in X has length d. Moreover, every nonempty open affine $U \subset X$ has dimension d and for every $p \in X$, the Krull dimension of $\mathcal{O}_{X,p}$ is d.*

REMARK 9.9. If $S \subset R$ is a multiplicative system, then the preimage of a prime ideal $\tilde{\mathfrak{q}}$ of $S^{-1}R$ under the ring homomorphism $R \to S^{-1}R$ is a prime ideal $\mathfrak{q}$ of R which does not meet S and we have $\tilde{\mathfrak{q}} = S^{-1}\mathfrak{q}$. This sets up a bijection between the prime ideals of $S^{-1}R$ and those of R not meeting S. If we take $S = R - \mathfrak{p}$, with $\mathfrak{p}$ a prime ideal, then this implies that $\dim R_{\mathfrak{p}}$ is the supremum of the prime chains in R which end with $\mathfrak{p}$. Since the prime chains in R which begin with $\mathfrak{p}$ correspond to prime chains in $R/\mathfrak{p}$, it follows that $\dim R_{\mathfrak{p}} + \dim R/\mathfrak{p}$ is the supremum of the prime chains in R having $\mathfrak{p}$ as a member. When R is a domain finitely generated over a field, then this is $\dim R$ by Theorem 9.6.

REMARK 9.10. An affine variety C of dimension 1 is called a *curve*. When C is irreducible this amounts to $k(C)$ being of transcendence degree one. It follows from Remark 9.5 that this is also equivalent to: $k[C]$ is a Dedekind domain $\neq k$.

EXERCISE 38. Prove that a hypersurface in $\mathbb{A}^n$ has dimension $n-1$.

EXERCISE 39. Let X be an irreducible affine variety and $Y \subset X$ a closed irreducible subset. Prove that $\dim X - \dim Y$ is equal to the Krull dimension of $k[X]_{I(Y)}$.

EXERCISE 40. Prove that when X and Y are irreducible affine varieties, then $\dim(X \times Y) = \dim X + \dim Y$. (Hint: Embed each factor as a closed subset of some affine space. You may also want to use the fact that the equality to be proven holds in case $X = \mathbb{A}^m$ and $Y = \mathbb{A}^n$.)

10. Nonsingular points

In this section we focus on the local properties of an affine variety $X = \mathrm{Spm}(A)$ (so $A := k[X]$ is here a reduced finitely generated k-algebra) at a point p. Therefore a central role will be played by the local algebra $\mathcal{O}_{X,p} = A_{\mathfrak{m}_p}$ whose maximal ideal is $\mathfrak{m}_{X,p} = (A - \mathfrak{m}_p)^{-1}\mathfrak{m}_p$.

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

Our point of departure is the implicit function theorem. One version states that if $U \subset \mathbb{R}^n$ is an open neighborhood of $p \in \mathbb{R}^n$ and $f_i : U \to \mathbb{R}$, $i = 1, \ldots n-d$ are differentiable functions zero in p such that the total differentials at p, $df_1(p), \ldots, df_{n-d}(p)$ are linearly independent in p (this is equivalent to: the Jacobian matrix of $(\partial f_j/\partial x_i)(p))_{i,j}$ has maximal rank $n-d$), then the common zero set of $f_1, \ldots, f_{n-d}$ is a submanifold of dimension d at p whose tangent space at p is the common zero set of $df_1(p), \ldots, df_{n-d}(p)$. In fact, one shows that this solution set is near p the graph of a map: we can express $n-d$ of the coordinates

as differentiable functions in the d remaining ones. Conversely, any submanifold of $\mathbb{R}^n$ at p of dimension d is locally thus obtained.

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

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

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

EXERCISE 41. Prove that $f \in k[x]$ has zero derivative, if and only if f is constant or (when $\mathrm{char}(k) = p > 0$) a pth power of some $g \in k[x]$.

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

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, when $k = \mathbb{C}$, the projection $f : C \to \mathbb{A}^1$, $(x, y) \mapsto y$, would be a local-analytic isomorphism at o. But the map is not locally invertible within our category: the inverse requires us to find a rational function $x = u(y)$ which solves the equation $y^2 = x^3 + x$ and it is easy to verify that none exists. (We can solve for x formally: $x = u(y) = y^2 - y^6 + 3y^{10} + \cdots$, where it is important to note that the coefficients are all integers so that this works for every characteristic.) In fact, the situation is worse: no open neighborhood U of o in C is isomorphic to an open subset V of $\mathbb{A}^1$. The reason is that this would imply that $k(C) = k(U)$ is isomorphic to $k(V) = k(x)$ and one can show that this is not so.

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

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

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

of this overload is by passing formal to power series. This is accomplished by what is known as formal completion[10].

10.3. FORMAL COMPLETION. Let R be a ring and $I \subsetneq R$ a proper ideal. For every R-module M, the descending sequence of submodules $M \supset IM \supset I^2M \supset \cdots \supset I^nM \supset \cdots$ gives rise to a sequence of surjective R-homomorphisms

$$0 = M/M \twoheadleftarrow M/IM \twoheadleftarrow M/I^2M \twoheadleftarrow M/I^3M \twoheadleftarrow \cdots \twoheadleftarrow M/I^nM \leftarrow \cdots$$

from which we can form the R-module $\hat{M}_I := \varprojlim_n M/IM^n$, called the *$I$-adic completion* of M. So any $\hat{a} \in \hat{M}_I$ is uniquely given by a sequence $(\alpha_n \in M/I^nM)_{n\geq 0}$ whose terms are compatible in the sense that α_n is the reduction of α_{n+1} for all n. In this way $\hat{M}_I$ can be regarded as an R-submodule of $\prod_{n\geq 0}(M/I^nM)$. The natural R-homomorphisms $M \to M/I^nM$ combine to define a R-homomorphism $M \to \hat{M}_I$. Its kernel is $\cap_{n=0}^{\infty} I^nM$ and this turns out to be trivial in many cases of interest. If we do this for the ring R, we get a ring $\hat{R}_I$ and $R \to \hat{R}_I$ is then a ring homomorphism.

The R-module structure on $\hat{M}_I$ extends naturally to a $\hat{R}_I$-module structure: for any $\hat{r} = (\rho_n \in R/I^n)_{n=0}^{\infty} \in \hat{R}_I$ we define $\hat{r}\hat{a}$ simply as given by the sequence $(\rho_n\alpha_n)_{n\geq 0}$ (note that $\rho_n\alpha_n$ is indeed the reduction of $\rho_{n+1}\alpha_{n+1}$). Any R-homomorphism $\phi : M \to N$ of R-modules sends M/I^nM to N/I^nN, and the resulting homomorphisms $M/I^nM \to N/I^nN$ are compatible in the sense that they determine a map $\hat{\phi}_I : \hat{M}_I \to \hat{N}_I$. This is in fact a $\hat{R}_I$-homomorphism. We have thus defined a functor from the category of R-modules to the category of $\hat{R}_I$-modules. It is easily verified that if ϕ is an epimorphism, then a compatible sequence in $(N/I^nN)_{n\geq 0}$ is the image of one in $(M/I^nM)_{n\geq 0}$ so that $\hat{\phi}_I$ is an epimorphism as well. This need not be true for monomorphisms, but we will see that this is so in the noetherian setting.

EXAMPLE 10.4. Take the ring $k[x_1, \ldots, x_n]$. Its completion with respect to the maximal ideal $(x_1, \ldots, x_n)$ is just the ring of formal power series $k[[x_1, \ldots, x_n]]$. We get the same result if we do this for the localization $\mathcal{O}_{\mathbb{A}^n,o}$ of $k[x_1, \ldots, x_n]$ at $(x_1, \ldots, x_n)$. We will find that for (C, o) in Example 10.1 resp. 10.2 the completion of $\mathcal{O}_{C,o}$ with respect to the maximal ideal is isomorphic to $k[[x]]$ resp. $k[[x, y]]/(xy)$.

EXAMPLE 10.5. Take the ring $\mathbb{Z}$. Its completion with respect to the ideal (n), n an integer ≥ 2, yields the ring of n-adic integers $\hat{\mathbb{Z}}_{(n)}$: an element of $\hat{\mathbb{Z}}_{(n)}$ is given by a sequence $(\rho_i \in \mathbb{Z}/(n^i))_{i=1}^{\infty}$ with the property that ρ_i is the image of ρ_{i+1} under the reduction $\mathbb{Z}/(n^{i+1}) \to \mathbb{Z}/(n^i)$. We get the same result if we do this for the localization $\mathbb{Z}_{(n)} = \{a/b : a \in \mathbb{Z}, b \in \mathbb{Z} - (n)\}$. It follows from the Chinese remainder theorem that $\hat{\mathbb{Z}}_{(n)} = \prod_{p|n} \hat{\mathbb{Z}}_{(p)}$.

10.6. ADIC TOPOLOGIES. We can understand $\hat{M}_I$ and $\hat{R}_I$ as completions with regard to a topology on M and R. This often helps to clearify their dependence on I (which is weaker than one might be inclined to think). For this we endow every R-module M with a topology, the *I-adic topology*, of which a basis is the collection of

[10]Another approach would be to allow 'algebraic' functions of the type that we encountered in the two examples above, but then we would have to address the question what the domain of such a function should be. This can not be achieved by refining the Zariski topology. Rather, this forces us to generalize the very notion of a topology, leading up to what is called the *étale topos*. Despite its rather abstract nature this is closer to our geometric intuition than the Zariski topology.

additive translates of the submodules I^nM, i.e., the collection of subsets $a + I^nM$, $a \in M$, $n \geq 0$. This is a topology indeed: given two basic open subsets $a + I^nM$, $a' + I^{n'}M$, then for any element c in their intersection, the basic open subset $c + I^{\max\{n,n'\}}M$ is also in their intersection. So a sequence $(a_n \in M)_{n\geq 1}$ converges to $a \in M$ precisely when for every integer $k \geq 0$, $a_n \in a + I^kM$ for n large enough. The fact that our basis is translation invariant implies that with this topology, M is a topological abelian group ($(a, b) \in M \times M \mapsto a - b \in M$ is continuous). If we endow R also with the I-adic topology and $R \times M$ with the product topology, then the map $(r, a) \in R \times M \to ra \in M$ which gives the action by R is also continuous. It is clear that any R-module homomorphism is continuous for the I-adic topology.

If $J \subset I$ is an ideal with $J \supset I^r$ for some $r \geq 0$, then the J-adic topology on M is the same as the J-adic topology. Also, for any $n_0 \geq 0$, the collection $\{I^{n+n_0}M\}_{n\geq 0}$ is a neighborhood basis of 0 in M and hence also defines the I-adic topology. Note that the topology on M comes from one on $M/\cap_{n\geq 0} I^nM$ in the sense that the open subsets of M are pre-images of open subsets of $M/\cap_{n\geq 0} I^nM$.

When M is Hausdorff, then its topology is even metrizable: if $\phi : \mathbb{Z}_+ \to (0, \infty)$ is any function with $\phi(n + 1) \leq \phi(n)$ and $\lim_{n\to\infty} \phi(n) = 0$ (one often takes $\phi(n) = u^{-n}$ for some $u > 1$), then a metric δ on M is defined by

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

This metric is *nonarchimedean* in the sense that $\delta(a, a'') \leq \max\{\delta(a, a'), \delta(a', a'')\}$. A sequence $(a_n \in M)_{n=0}^{\infty}$ is then a Cauchy sequence if and only if for every integer $k \geq 0$ all but finitely many terms lie in the same coset of I^kM in M; in other words, there exists an index $n_k \geq 0$ such that $a_m - a_n \in I^kM$ for all $m, n \geq n_k$. This makes it clear that the notion of Cauchy sequence is independent of the choice of ϕ. Such a Cauchy sequence defines a compatible sequence of cosets $(\alpha_n \in M/I^nM)_{n\geq 0}$ and hence an element of $\hat{M}_I$. Recall that a metric space is said to be *complete* if every Cauchy sequence in that space converges. A standard construction produces a completion of every metric space M: its points are represented by Cauchy sequences in M, with the understanding that two such sequences represent the same point if the distance between the two nth terms goes to zero as $n \to \infty$. In the present situation we thus recover $\hat{M}_I$. Note that the homomorphism $M \to \hat{M}_I$ is a continuous injection with image dense in $\hat{M}_I$.

EXERCISE 42. Let I and J be ideals of a ring R and m a positive integer with $J^m \subset I$. Prove that the J-adic topology is finer than the I-adic topology and that there is a natural continuous ring homomorphism $\hat{R}_J \to \hat{R}_I$. Conclude that when R is noetherian, $\hat{R}_I$ can be identified with $\hat{R}_{\sqrt{I}}$.

If M is an R-module, then the inclusion $M' \subset M$ of any submodule is continuous for the I-adic topology. The Artin-Rees lemma says among other things that when R is noetherian, this is in fact a closed embedding (so that M' has the induced topology).

*LEMMA 10.7 (Artin-Rees). *Let R be a noetherian ring, $I \subset R$ an ideal, M a finitely generated R-module and $M' \subset M$ an R-submodule. Then there exists an integer $n_0 \geq 0$ such that for all $n \geq 0$:*

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

The proof (which is ingeneous, but not difficult) can be found in any standard text book on commutative algebra (e.g., [**?**]). The lemma implies that for every $n \geq 0$ there exists a $n' \geq 0$ such that $M' \cap I^{n'}M \subset I^nM'$ (we can take $n' = n + n_0$).

So the inclusion $M' \subset M$ is not merely continuous, but M' inherits its I-adic topology from that of M. We will use the Artin-Rees lemma via this property only. A special case is when $M' := \cap_{n\geq 0} I^n M$: it then follows that $M' = I^{n+n_0}M \cap M' = I^n(M' \cap I^{n_0}M) = I^n M'$. By taking $n = 1$, Nakayama's lemma 8.5 then yields that $M' = 0$, provided that R is a local ring. We record this as:

COROLLARY 10.8. *If R is a noetherian local ring, then any finitely generated R-module M is Hausdorff for the I-adic topology: $\cap_{n\geq 0} I^n M = 0$.*

COROLLARY 10.9. *In the situation of Lemma 10.7, the homomorphism $\hat{M}'_I \to \hat{M}_I$ induced by the inclusion $M' \subset M$ is a closed embedding and $\hat{M}_I/\hat{M}'_I$ can be identified with the I-adic completion of M/M'. In case R is also a local ring so that by Corollary 10.8 we may regard M resp. M' as a submodule of $\hat{M}_I$ resp. $\hat{M}'_I$, then $M \cap \hat{M}'_I = M'$.*

Note that the first part of this corollary says that when R is noetherian, I-adic completion is an exact functor on the category of finitely generated R-modules.

PROOF OF COROLLARY 10.9. Observe that we have epimorphisms

$$M'/I^{n+n_0}M' \twoheadrightarrow M'/(M' \cap I^{n+n_0}M) = M'/I^n(M' \cap I^{n_0}M) \twoheadrightarrow M'/I^n M',$$

where we note that the middle term is the image of M' in $M/I^{n+n_0}M$. So if $j : M \to \hat{M}_I$ denotes the obvious map, then after taking the projective limits we obtain continuous epimorphisms $\hat{M}'_I \twoheadrightarrow \overline{j(M')} \twoheadrightarrow \hat{M}'_I$. Their composite is the identity and so this is in fact a homeomorphism followed by its inverse. In particular, $\hat{M}'_I \to \hat{M}_I$ is a closed embedding. We next show that the $\hat{R}_I$-epimorphism $\hat{M}_I \to \widehat{M/M'_I}$ induced by the projection $M \to M/M'$ has kernel $\hat{M}'$. It is clear that this kernel contains $\hat{M}'$. For the converse, we observe that the kernel of $M/I^n M \to (M/M')/I^n(M/M') \cong M/(M' + I^n M)$ is $(M' + I^n M)/I^n M \cong M'/(M' \cap I^n M)$, which we may identify for $n \geq n_0$ with $M'/I^n(M' \cap I^{n_0}M)$. So the kernel of $\hat{M}_I \to \widehat{M/M'_I}$ is represented by compatible sequences in $(M'/I^n(M' \cap I^{n_0}M))_{n\geq n_0}$. Such sequences represent elements of $\hat{M}'_I$.

The last assertion follows from the identity $j^{-1}\overline{j(M')} = M' + \cap_{n\geq 0} I^n M$ and the fact that $\cap_{n\geq 0} I^n M = 0$ by Corollary 10.8. □

Let R be a local ring with maximal ideal $\mathfrak{m}$ and residue field κ. We use the roof symbol $\hat{}$ for completion with respect to $\mathfrak{m}$.

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

DEFINITION 10.10. The *Zariski cotangent space* $T^*(R)$ of R is the κ-vector space $\mathfrak{m}/\mathfrak{m}^2$ and its κ-dual, $T(R) := \mathrm{Hom}_\kappa(\mathfrak{m}/\mathfrak{m}^2, \kappa)$ (which is also equal to $\mathrm{Hom}_R(\mathfrak{m}, \kappa)$), is called the *Zariski tangent space* $T(R)$ of R. The *embedding dimension* $\mathrm{embdim}(R)$ is the dimension of $\mathfrak{m}/\mathfrak{m}^2$ as a vector space over κ.

If X is an affine variety and $p \in X$, then we define the Zariski cotangent space $T^*_p X$, the Zariski tangent space $T_p X$ and the embedding dimension $\mathrm{embdim}_p X$ of X at p to be that of $\mathcal{O}_{X,p}$.

For instance, the embedding dimension of $\mathbb{A}^n$ at any point $p \in \mathbb{A}^n$ 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 $\mathfrak{m}_{\mathbb{A}^n,p}/\mathfrak{m}^2_{\mathbb{A}^n,p} \cong k^n$. We note in passing that we here

have a way of understanding the total differential at $p \in \mathbb{A}^n$ in more intrinsic terms as the map $d_p : \mathcal{O}_{\mathbb{A}^n,p} \to \mathfrak{m}_{\mathbb{A}^n,p}/\mathfrak{m}^2_{\mathbb{A}^n,p}$ 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 $\mathfrak{m}_{\mathbb{A}^n,p}/\mathfrak{m}^2_{\mathbb{A}^n,p}$. Thus, a differential of f at p can be understood as a k-linear function $df(p) : T_p\mathbb{A}^n \to k$ and $(d_p(x_i) = dx_i(p))_{i=1}^n$ is a basis of $\mathfrak{m}_{\mathbb{A}^n,p}/\mathfrak{m}^2_{\mathbb{A}^n,p} = T_p^*\mathbb{A}^n$.

Let us observe that since embedding dimension and Zariski tangent space of a local ring R are defined in terms of $\mathfrak{m}/\mathfrak{m}^2$, these notions only depend on $\hat{R}$.

EXERCISE 43. Let $(R', \mathfrak{m}')$ and $(R, \mathfrak{m})$ be local rings with residue fields κ resp. κ' and let $\phi : R' \to R$ be a ring homomorphism with the property that $\phi^{-1}\mathfrak{m} = \mathfrak{m}'$ (we then say that ϕ is a *local homomorphism*). Prove that ϕ induces a field embedding $\kappa' \hookrightarrow \kappa$ and a linear map of κ-vector spaces $T(\phi) : T(R) \to \kappa \otimes_{\kappa'} T(R')$.

An application of Nakayama's lemma to the R-module $\mathfrak{m}$ yields:

COROLLARY 10.11. *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 10.12. A noetherian local ring R is said to be *regular* if its Krull dimension equals its embedding dimension. A point p of an affine variety X is called *regular* if its local ring $\mathcal{O}_{X,p}$ is so; otherwise it is called *singular*. The corresponding subsets of X are called the *regular locus* resp. *singular locus* of X and will be denoted X_{reg} resp. X_{sing}. An affine variety without singular points is said to be *nonsingular*.

We shall see that the regularity of a local ring $\mathcal{O}_{X,p}$ indeed amounts to X being 'like a manifold' at p. We begin with a formal version of the implicit function theorem.

LEMMA 10.13. *Let $p \in \mathbb{A}^n$ and let $f_1, \ldots, f_{n-d} \in \mathfrak{m}_{\mathbb{A}^n,p}$ be such that the differentials $df_1(p), \ldots, df_{n-d}(p)$ are linearly independent. Then $\mathfrak{p} := (f_1, \ldots, f_{n-d}) \subset \mathcal{O}_{\mathbb{A}^n,p}$ is a prime ideal and $\mathcal{O}_{\mathbb{A}^n,p}/\mathfrak{p}$ is a regular local ring of dimension d whose completion with respect to its maximal ideal is isomorphic to $k[[x_1, \ldots, x_d]]$ as a complete local k-algebra. Moreover, there exists an affine neighborhood U of p in $\mathbb{A}^n$ on which $f_1, \ldots, f_{n-d}$ admit representatives $\tilde{f}_1, \ldots, \tilde{f}_{n-d} \in k[U]$ which generate in $k[U]$ a prime ideal P and then $Z(P) = \cap_i Z(\tilde{f}_i) \subset U$ is an irreducible affine variety having p as a regular point of dimension d with Zariski tangent space equal to the kernel of the linear surjection $(df_1(p), \ldots, df_{n-d}(p)) : T_p\mathbb{A}^n \to k^{n-d}$.*

PROOF. Let us abbreviate $\mathcal{O}_{\mathbb{A}^n,p}$ by $\mathcal{O}$ and its maximal ideal $\mathfrak{m}_{\mathbb{A}^n,p}$ by $\mathfrak{m}$. Extend $f_1, \ldots, f_{n-d}$ to a system of regular functions $f_1, \ldots, f_n \in \mathfrak{m}$ such that the $df_1(p), \ldots, df_n(p)$ are linearly independent. This means that their images in $\mathfrak{m}/\mathfrak{m}^2$ are linearly independent over k. After an affine-linear transformation, we then may (and will) assume that p is the origin o of $\mathbb{A}^n$ and that $f_i \equiv x_i \pmod{\mathfrak{m}^2}$. Hence the monomials of degree r in $f_1, \cdots, f_n$ map to a k-basis of $\mathfrak{m}^r/\mathfrak{m}^{r+1}$. With induction on r it then follows that the monomials of degree $\leq r$ in $f_1, \cdots, f_n$ make up a k-basis of $\mathcal{O}/\mathfrak{m}^{r+1}$. This amounts to the assertion that the map

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

defines an isomorphism $k[[y_1, \ldots, y_n]] \cong \hat{\mathcal{O}}$ of complete local rings (a ring isomorphism that is also a homeomorphism). The restriction of its inverse to $\mathcal{O}$ is a topological embedding of $\mathcal{O}$ in $k[[y_1, \ldots, y_n]]$ (sending f_i to y_i). The ideal generated

by $(y_1, \ldots, y_{n-d})$ in $k[[y_1, \ldots, y_n]]$ is the closure $\overline{\mathfrak{p}}$ of the image of $\mathfrak{p}$. The quotient ring is the domain $k[[y_{n-d+1}, \ldots, y_n]]$ and so this is clearly a prime ideal. According to Corollary 10.9, the preimage of $\overline{\mathfrak{p}}$ in $\mathcal{O}$ is $\mathfrak{p}$ (hence $\mathfrak{p}$ is a prime ideal) and the embedding

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

realizes the $\mathfrak{m}$-adic completion of $\mathcal{O}/\mathfrak{p}$. This argument applied applied to the ideal $\mathfrak{p}_i \subset \mathcal{O}_{\mathbb{A}^n,p}$ generated by $f_1, \ldots, f_i$ shows that $\mathfrak{p}_i$ a prime ideal for all $i = 0, \ldots, n-1$. So we have prime chain $(0) = \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ in $\mathcal{O}$ of length n. According to Corollary 9.7, $\mathcal{O}$ has Krull dimension n, and so this prime chain is maximal. Theorem 9.6 then implies that $\mathcal{O}/\mathfrak{p} = \mathcal{O}/\mathfrak{p}_{n-d}$ has Krull dimension d. This is also the embedding dimension of $\mathcal{O}/\mathfrak{p}$, for $f_{n-d+1}, \ldots, f_n$ map to a k-basis of $\mathfrak{m}/(\mathfrak{m}^2 + (f_1, \ldots, f_{n-d}))$. So $\mathcal{O}/\mathfrak{p}$ is a regular local ring of dimension d.

Let $g' \in k[x_1, \ldots, x_n]$ be a common denominator for $f_1, \ldots, f_{n-d}$ with $g(o) \neq 0$ and denote by $P' \subset k[x_1, \ldots, x_n][1/g']$ the preimage of $\mathfrak{p}$ under the localization map $k[x_1, \ldots, x_n][1/g'] \to \mathcal{O}$. This is a prime ideal which contains (the images of) $f_1, \ldots, f_{n-d}$ and has the property that its localization at $o \in \mathbb{A}^n$ is $\mathfrak{p}$. Choose a finite set of generators $\phi_1, \ldots, \phi_r$ of P'. We may write in $\mathcal{O}$, $\phi_i = \sum_{j=1}^{n-d} u_{ij} f_j$ with $u_{ij} \in \mathcal{O}$. If $g \in (g')$ with $g(o) \neq 0$ is a common denominator for the u_{ij}, then put $U = \mathbb{A}^n_g$. Then $P := P'[1/g]$ is a prime ideal in $k[U]$. It is generated by the images of $\phi_1, \ldots, \phi_r$ and hence also by the images $\tilde{f}_1, \ldots, \tilde{f}_{n-d}$ of $f_1, \ldots, f_{n-d}$ in $k[U]$. So $(U; \tilde{f}_1, \ldots, \tilde{f}_{n-d})$ is as desired. □

THEOREM 10.14. *Let $X \subset \mathbb{A}^n$ be locally closed and let $p \in X$. Then the local ring $\mathcal{O}_{X,p}$ is regular of dimension d if and only there exist regular functions $f_1, \ldots, f_{n-d}$ on a principal neighborhood U of p in $\mathbb{A}^n$ such that these functions generate the ideal in $k[U]$ defining $X \cap U$ and $df_1, \ldots, df_{n-d}$ are linearly independent in every point of U. In that case $X \cap U$ is regular and for every $q \in X \cap U$ the Zariski tangent space T_qX is the kernel of the linear map $(df_1(q), \ldots, df_{n-d}(q)) : T_q\mathbb{A}^n \to k^{n-d}$.*

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

According to Lemma 10.13, the ideal $\mathfrak{p}_i \subset \mathcal{O}_{\mathbb{A}^n,p}$ generated by $f_1, \ldots, f_i$ is prime and so we have a prime chain

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

Since $\dim \mathcal{O}_{X,p} = d$, there also exists a prime chain of length d containing $\mathcal{I}_{X,p}$:

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

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

In particular, $f_1, \ldots, f_{n-d}$ generate $\mathcal{I}_{X,p}$. Let U' be an affine neighborhood of p in $\mathbb{A}^n$ on which the f_i's are regular, generate a prime ideal in $k[U']$ and are such

that their common zero set is $X \cap U'$. Since the $df_1(p), \dots, df_{n-d}(p)$ are linearly independent, there exist $n-d$ indices $1 \leq \nu_1 < \nu_2 < \cdots < \nu_{n-d} \leq n$ such that $\delta := \det((\partial f_i/\partial x_{\nu_j})_{i,j}) \in k[U']$ is nonzero in p. Then $U := U_\delta \subset U'$ has all the asserted properties (with the last property following from Lemma 10.13).

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 of dimension d. This follows Lemma 10.13. □

PROPOSITION 10.15. *The regular points of an affine variety X form an open-dense subset X_{reg} of X.*

For the proof we will assume Proposition 10.16 below, which we will leave unproved for now. (Note that it tells us only something new in case k has positive characteristic.)

*PROPOSITION 10.16. *Every finitely generated field extension L/k (with k as in these notes, i.e., algebraically closed) is* separably generated, *by which we mean that there exists an intermediate extension $k \subset K \subset L$ such that K/k is purely transcendental (i.e., of the form $k(x_1, \dots, x_r)$) and L/K is a finite separable extension (which by the theorem of the primitive element is then obtained by adjoining the root of an irreducible, separable polynomial in $K[x]$).*

This improves upon Corollary 7.8, as this implies that every irreducible affine variety is birationally equivalent to a hypersurface.

PROOF OF PROPOSITION 10.15. Without loss of generality we may assume that X is irreducible. Since we already know that X_{reg} is open, it remains to see that it is nonempty. It thus becomes an issue which only depends on $k(X)$. Hence it suffices to treat the case of a hypersurface in $\mathbb{A}^n$ so that $I(X)$ is generated by an irreducible polynomial $f \in k[x_1, \dots, x_n]$. In view of Lemma Lemma 10.13 it then suffices to show that df is not identically zero on X. Suppose otherwise, i.e., that each partial derivative $\partial f/\partial x_i$ vanishes on X. Then each $\partial f/\partial x_i$ must be multiple of f and since the degree of $\partial f/\partial x_i$ is less than that of f, this implies that it is identically zero. But then we know from Exercise 41 that the characteristic p of k must then be positive (so ≥ 2) and that f is of the form g^p. This contradicts the fact that f is irreducible. □

EXERCISE 44. Let X be a nonsingular variety. Prove that X is connected if and only if it is irreducible.

REMARK 10.17. This enables us to find for an affine variety X of dimension d (with downward induction) a descending chain of closed subsets $X = X^d \supset X^{d-1} \supset \cdots \supset X^0$ such that $\dim X^i \leq i$ and all the (finitely many) connected components of $X^i \smallsetminus X^{i-1}$ are nonsingular subvarieties of dimension i (such a chain is called a *stratification* of X): if X^i has been defined, then we take for X^{i-1} the union of the singular locus X^i_{reg} and the irreducible components of dimension $\leq i-1$. Then $\dim X^{i-1} \leq i-1$ and every connected component of $X^i \smallsetminus X^{i-1}$ is an nonempty open subset of some X^i_{reg} and hence a nonsingular subvariety of dimension i.

10.18. DIFFERENTIALS AND DERIVATIONS. The differential that we defined earlier has an intrinsic, coordinate free description that turns out to be quite useful. Let us begin with the observation that the formation of the total differential of a polynomial, $\phi \in k[x_1, \dots, x_n] \mapsto$

$d\phi := \sum_{i=1}^{n}(\partial\phi/\partial x_i)(p)dx_i$ is a k-linear map which satisfies the Leibniz rule: $d(\phi\psi) = \phi d\psi + \psi d\phi$. This property is formalized with the following definition. Fix a ring R (the *base ring*) and an R-algebra A.

DEFINITION 10.19. Let M be a A-module. An *R-derivation of A with values in M* is an R-module homomorphism $D : A \to M$ which satisfies the Leibniz rule: $D(a_1a_2) = a_1D(a_2) + a_2D(a_2)$ for all $a_1, a_2 \in A$.

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

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

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

If we combine this with the formula for $D(1/a)$, we see that not just determines D on the R-subalgebra A' of A generated by the a_i's, but also on the biggest localization of A' contained in A. In particular, if we are given a field extension L/K, then a K-derivation of L with values in some L-vector space is determined by its values on a set of generators of L as a field extension of K.

Observe that the set of R-derivations of A in M form an R-module: if D_1 and D_2 are R-derivations of A with values in M, and $a_1, a_2 \in A$, then $a_1D_1 + a_2D_2$ is also one. We denote this module by $\mathrm{Der}_R(A, M)$.

EXERCISE 45. Prove that if $D_1, D_2 \in \mathrm{Der}_R(A, A)$, then $[D_1, D_2] := D_1D_2 - D_2D_1 \in \mathrm{Der}_R(A, A)$. What do we get for $R = k$ and $A = k[x_1, \ldots, x_n]$?

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

The universal derivation of a finitely generated R-algebra A can be constructed in a more direct manner as follows. We first do the case when A is a polynomial algebra $P := R[x_1, \ldots, x_n]$. For any R-derivation $D : P \to M$ we have $Df = \sum_{i=1}^{n}(\partial f/\partial x_i)Dx_i$ and this yields $(Dx_1, \ldots, Dx_n) \in M^n$. Conversely, for any n-tuple $(m_1, \ldots, m_n) \in M^n$, we have an R-derivation $D : P \to M$ defined by $Df = \sum_{i=1}^{n}(\partial f/\partial x_i)m_i$. So Dx_i can be prescribed

arbitrarily as an element of M. But to give an element of M^n is to give a P-homomorphism $P^n, M)$ and hence $\Omega_{P/R}$ is the free P-module generated by $dx_1, \ldots, dx_n$. Thus the universal R-derivation $d : P \to \Omega_{P/R}$, which is given by $f \mapsto \sum_{i=1}^n (\partial f/\partial x_i) dx_i$, may be regarded as the intrinsic way of forming the total differential.

Next consider a quotient $A := P/I$ of P, where $I \subset P$ is an ideal. If M is an A-module and $D' : A \to M$ is an R-derivation, then its composite with the projection $\pi : P \to A$, $D = D'\pi : P \to M$, is an R-derivation of P with the property that $Df = 0$ for every $f \in I$. Conversely, every R-derivation $D : P \to M$ in an A-module M which is zero on I factors through an an R-derivation $D' : A \to M$. Note that for *any* R-derivation $D : P \to M$, its restriction to I^2 is zero, for if $f, g \in I$, then $D(fg) = fDg + gDf \in IM = \{0\}$. Now I/I^2 is a module over $P/I = A$ and so we obtain a short exact sequence of A-modules

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

It follows from our computation of $\Omega_{P/R}$ that the middle term is the free A-module generated by $dx_1, \ldots, dx_n$. So if I is generated by $f_1, \ldots, f_m$, then $\Omega_{A/R}$ can be identified with the quotient of $\sum_{i=1}^n A dx_i$ by the A-submodule generated by the A-submodule generated by the $df_j = \sum_{i=1}^n (\partial f_j/\partial x_i) dx_i$, $j = 1, \ldots, m$.

Note that if R is a noetherian ring, then so is A (by the Hilbert basis theorem) and since $\Omega_{A/R}$ is a finitely generated A-module, it is noetherian as an A-module. This applies for instance to the case when $R = k$ and $A = k[X]$ for some affine variety X. We then write $\Omega(X)$ for $\Omega_{k[X]/k}$.

EXERCISE 46. Prove that $\Omega_{A/R}$ behaves well with localization: if $S \subset A$ is a multiplicative subset, then every R-derivation with values is some A-module M extends naturally to an R-derivation of $S^{-1}A$ with values in $S^{-1}M$. Prove that we have a natural map $S^{-1}\Omega_{A/R} \to \Omega_{S^{-1}A/R}$ and that this map is a A-homomorphism.

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

EXERCISE 47. Let X be an affine variety and let $p \in X$. Show that the Zariski tangent space of X at p can be understood (and indeed, be defined) as the space of k-derivations of $\mathcal{O}_{X,p}$ with values in k, where we regard k as a $\mathcal{O}_{X,p}$-module via $\mathcal{O}_{X,p}/\mathfrak{m}_{X,p} \cong k$. Prove that this identifies its dual, the Zariski cotangent space, with $\Omega_{X,p}/\mathfrak{m}_{X,p}\Omega_{X,p}$.

EXERCISE 48. Show (perhaps with the help of the preceding exercises) that if $p \in \mathbb{A}^n$, then $\Omega_{\mathcal{O}_{\mathbb{A}^n,p}/k}$ is the free $\mathcal{O}_{\mathbb{A}^n,p}$-module generated by $dx_1, \ldots, dx_n$ and that if X is an affine variety in $\mathbb{A}^n$ that has p a regular point, then $\Omega_{X,p}$ is a free $\mathcal{O}_{X,p}$-module of rank $\dim \mathcal{O}_{X,p}$.

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

EXERCISE 49. Prove that the composite $d : A \to \Omega_{A/R} \to (\hat{\Omega}_{A/R})_I$ factors through a derivation $\hat{d}_I : \hat{A}_I \to (\hat{\Omega}_{A/R})_I$ and prove that it is universal among all the R-derivations of A in R-modules that are complete for the I-adic topology (i.e., for which $M = \hat{M}_I$).

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

11. The notion of a variety

We begin with a 'predefinition'.

DEFINITION 11.1. A *prevariety* is a topological space X endowed with a sheaf $\mathcal{O}_X$ of k-valued functions such that X can be covered by *finitely many* open subsets U such that $(U, \mathcal{O}_X|U)$ is an affine variety. Given prevarieties $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$, then a *morphism of prevarieties* $f : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ is simply a morphism in the category of spaces endowed with a sheaf $\mathcal{O}_X$ of k-valued functions: f is continuous and for every open $V \subset Y$, composition with f takes $\mathcal{O}_Y(V)$ to $\mathcal{O}_X(f^{-1}V)$.

We often designate a prevariety and its underlying topological space by the same symbol, a habit which rarely leads to confusion. The composite of two morphisms is evidently a morphism so that we are dealing here with a category. The prefix '*pre*' in prevariety refers to the fact that we have not imposed a separation requirement which takes the place of the Hausdorff property that one normally imposes on a manifold (see Example 11.5 below).

Let X be a prevariety. By assumption X is covered by finitely many affine open subvarieties $\{U_i\}_{i\in I}$ (I is a finite index set). Suppose κ_i is an isomorphism of U_i onto an affine variety X_i which is given as a closed subset in some $\mathbb{A}^{n_i}$. 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 $\coprod_{i\in I} X_i$ by means of a gluing process, for 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 $\{(U_i, \kappa_i)\}_{i\in I}$ is called an *affine atlas* for X and $\kappa_{i,j}$ is called a *transition map*.

EXERCISE 50. Let $(X, \mathcal{O}_X)$ be a prevariety.

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

Much of what we did for affine varieties extends in a straightforward manner to this more general context. Here are some examples.

Rational functions. A *rational function* $f : X \dashrightarrow k$ is defined as before: it is represented by a regular function on a subset of X that is open-dense in its set of closed points and two such represent the same rational function if they coincide on a nonempty open-dense subset in their common domain of definition.

Function field and dimension. When X is irreducible, the rational functions on X form a field $k(X)$, the *function field of* X and for an open nonempty affine open subset $U \subset X$, we have $k(X) = k(U) = \mathrm{Frac}(\mathcal{O}(U))$ (but we will see that it is not true in general that $k(X) = \mathrm{Frac}(\mathcal{O}(X))$). In particular, any nonempty affine open subset of X has dimension $\mathrm{trdeg}_k\, k(X)$. According to Exercise 36, this is then also the (Krull) dimension of X.

Rational and dominant maps. Similarly, if X and Y are prevarieties, then a *rational map* $f : X \dashrightarrow Y$ is represented by morphism from a nonempty open-dense subset of X to Y with the understanding that two such define the same map if and only if they coincide on a nonempty open-dense subset. If some representative morphism has dense image in Y, then f is said to be *dominant*. If in addition both

X and Y are irreducible, then f induces a field extension $f^* : k(Y) \hookrightarrow k(X)$. Conversely, a k-linear field embedding $k(Y) \hookrightarrow k(X)$ 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.

Finite morphisms. A morphism $f : X \to Y$ between prevarieties is called *finite* if it is locally so over Y, that is, if we can cover Y by open affine subsets V with the property that $f^{-1}V$ is affine and the restriction $f^{-1}V \xrightarrow{f} V$ is finite. According to Exercise 34 a finite morphism between affine varieties is closed. It then follows that a finite morphism between prevarieties is also closed.

Regular and singular points. Since the notion of a regular point is a local one, it automatically carries over to this setting. The regular locus of X is an open-dense subset X_{reg} of X.

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 of course also require that $\mathcal{O}_{X\times Y}((U \times V)_h) = (\mathcal{O}(U) \otimes \mathcal{O}(V))[1/h]$.

EXERCISE 51. Prove that this product has the usual categorical characterization: the two projections $X \times Y \to X$ and $X \times Y \to Y$ are morphisms and if Z is a prevariety, then a pair of maps $(f : Z \to X, g : Z \to Y)$ defines a morphism $(f, g) : Z \to X \times Y$ if and only both f and g are morphisms.

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

DEFINITION 11.2. 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). A subset of a variety X is called a *subvariety* if it is open in a closed subset of X. We say that a morphism of varieties $f : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ is an *immersion* if it defines an isomorphism onto a subvariety of Y, that is, is the composite of such an isomorphism and an inclusion.

Strictly speaking, the last part of this definition only makes sense after we have observed that a subvariety is in a natural manner a variety that makes the inclusion a morphism. We leave this as an exercise (see also Exercise 50).

The proof of the following assertion is also left as an exercise.

PROPOSITION 11.3. *The product of two varieties is a variety.*

EXAMPLE 11.4. The diagonal in $\mathbb{A}^n \times \mathbb{A}^n$ is closed, so $\mathbb{A}^n$ is a variety. This implies that the same is true for any quasi-affine subset of $\mathbb{A}^n$. Hence a quasi-affine prevariety is in fact a variety.

EXAMPLE 11.5. 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 $\mathbb{A}^1_+ \smallsetminus \{0\}$ with $\mathbb{A}^1_- \smallsetminus \{0\}$ by means of the identity map. If $o_\pm \in X$ denotes the image of origin of $\mathbb{A}^1_\pm$, then $(o_+, o_-) \in X \times X$ lies in the closure of the diagonal, but is not contained in the diagonal.

EXAMPLE 11.6. Let $f : X \to Y$ be a morphism of varieties. Consider the graph of f, $\Gamma_f := \{(x, y) \in X \times Y\} : x \in U, y = f(x)\}$. It is easy to see that Γ_f is a subvariety of $X \times Y$. The map $x \in X \mapsto (x, f(x)) \in \Gamma_f$ and the projection $\Gamma_f \to X$ are regular and each others inverse. So they define an isomorphism $\Gamma_f \to X$. Notice that via this isomorphism f appears as a projection mapping: $(x, y) \in \Gamma_f \mapsto y \in Y$.

EXERCISE 52. The goal of this exercise is to show that $U := \mathbb{A}^2 \smallsetminus \{(0, 0)\}$ 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.

This exercise also leads to an interesting example. Let X be obtained as the obvious generalization of Example 11.5 where $\mathbb{A}^1$ is replaced by $\mathbb{A}^2$ so that X is covered by two copies of $\mathbb{A}^2$ (appearing as open affine subsets) whose intersection is a copy of $\mathbb{A}^2 \smallsetminus \{(0, 0)\}$ (which is not affine). Hence, on a prevariety the intersection of two affine subsets need not be affine. This cannot happen on a variety and that is one of the reasons why we like them:

PROPOSITION 11.7. *Let X be a variety. Then for any pair U, U' of affine open subsets of X, $U \cap U'$ is also an affine open subset of X and $\mathcal{O}_X(U \cap U')$ is as a k-algebra generated by $\mathcal{O}_X(U)|U \cap U'$ and $\mathcal{O}_X(U')|U \cap U'$.*

PROOF. First note that $U \times U'$ is an affine open subset of $X \times X$. Since the diagonal $\Delta(X)$ of $X \times X$ is closed, its intersection with $U \times U'$ is a closed subset of $U \times U'$ and hence affine. But the diagonal map sends $U \cap U'$ isomorphically onto this intersection (the inverse being given by one of the projections) and so $U \cap U'$ is affine. Since the diagonal defines a closed embedding $U \cap U' \to U \times U'$ of affine varieties, the map $k[U] \otimes k[U'] \cong k[U \times U'] \to k[U \cap U']$ is onto. Since the image of $f \otimes f' \in k[U] \otimes k[U']$ equals $f_{|U \cap U'} \cdot f'_{|U \cap U'}$, the last assertion follows. □

12. Constructible sets

The image of a morphism of varieties need not be a variety as the following simple example shows.

EXAMPLE 12.1. Consider the morphism $f : \mathbb{A}^2 \to \mathbb{A}^2$, $(x_1, x_2) \mapsto (x_1, x_1x_2)$. A point $(y_1, y_2) \in \mathbb{A}^2$ is of the form (x_1, x_1x_2) if and only if y_2 is a multiple of y_1.

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. This turns out to represent the general situation and the following definition will help us to express this fact.

DEFINITION 12.2. A subset of variety is called *constructible* if it can be written as the union of finitely many (locally closed) subvarieties.

THEOREM 12.3. *Let $f : X \to Y$ be a morphism of varieties. Then f takes constructible subsets of X to constructible subsets of Y. In particular, $f(X)$ is constructible.*

We first show that the theorem follows from the following proposition.

PROPOSITION 12.4. *Let $f : X \to Y$ be a morphism of varieties with X irreducible. Then $f(X)$ contains a nonempty open subset of its closure.*

PROOF THAT PROPOSITION 12.4 IMPLIES THEOREM 12.3. A constructible subset is a finite union of irreducible subvarieties and so it is clearly enough to prove that the image of each of these is constructible. In other words, it suffices to show that the image of a morphism $f : X \to Y$ of varieties with X irreducible is constructible. We prove this with induction on the dimension of X. According to Proposition 12.4 the closure of $f(X)$ contains a nonempty open subset U such that $f(X) \supset U$. It is clear that $f^{-1}U$ is a nonempty open subset of X. If $Z := X - f^{-1}U$, then $f(X) = U \cup f(Z)$. The irreducible components of Z have smaller dimension than X and so $f(Z)$ is constructible by induction. □

PROOF OF PROPOSITION 12.4. Since Y is covered by finitely many open affine subsets $V_j \subset Y$ we may (upon replacing f by its restriction to $f^{-1}V_j$) assume without loss of generality that Y is affine. For a similar reason we may assume that X is affine and hence is closed in some $\mathbb{A}^n$. Then the graph of f identifies X with a closed subset of $\mathbb{A}^n \times Y$ so that f becomes the restriction of the projection $\pi : \mathbb{A}^n \times Y \to Y$ to X. In other words, we need to prove that for every closed subset $X \subset \mathbb{A}^n \times Y$, $\pi(X)$ contains a nonempty open subset of its closure in Y. Since we can factor π_Y in an obvious manner into successive line projections (by forgetting the last coordinate)

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

it suffices to do the case $n = 1$, so that now f factors as $X \subset \mathbb{A}^1 \times Y \xrightarrow{\pi} Y$. Upon replacing Y by $\overline{\pi(X)}$, we may then also may assume that $\pi|X : X \to Y$ is dominant. When $X = \mathbb{A}^1 \times Y$, there is nothing to show. Otherwise $I(X) \subset k[\mathbb{A}^1 \times Y] = k[Y][t]$ contains a nonzero $g \in k[Y][t]$. Write $g = a_0 t^N + a_1 t^{N-1} + \cdots + a_N$ with $a_i \in k[Y]$ and a_0 nonzero. Since $\pi|X$ is dominant, we have $I(X) \cap k[Y] = \{0\}$ and so $N > 0$. Hence g/a_0 yields for the image of t in $k[X][1/a_0] = k[X_{a_0}]$ an equation of integral dependence over $k[Y_{a_0}]$. This implies that X_{a_0} is finite over Y_{a_0} and so its image in Y_{a_0} is closed by Exercise 34. Since this image is also dense in Y_{a_0}, it follows that $\pi(X)$ contains the open-dense subset Y_{a_0}. □

CHAPTER 2

Projective varieties

1. Projective spaces

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

Given a finite dimensional k-vector space V, then we denote by $\mathbb{P}(V)$ the collection of its 1-dimensional linear subspaces. Observe that any linear injection $J : V \to V'$ of vector spaces induces an injection $\mathbb{P}(J) : \mathbb{P}(V) \to \mathbb{P}(V')$ (in general $\mathbb{P}(J)$ only makes sense on $\mathbb{P}(V) \smallsetminus \mathbb{P}(\ker(J))$). In particular, when J is an isomorphism isomorphism, then $\mathbb{P}(J)$ is a bijection. The following definition makes this notion slightly more abstract by suppressing the vector space as part of the data.

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 $\ell : P \to \mathbb{P}(V)$ is a bijection, where it is understood that another such pair (V', ℓ') defines the same structure if and only if there exists a k-linear isomorphism $J : V \to V'$ such that $\ell' = \mathbb{P}(J)\ell'$. (We are in fact saying that thus is defined an equivalence relation on the collection of such pairs and that a projective structure is given by an equivalence class.)

So for a finite dimensional k-vector space V, the identity map of $\mathbb{P}(V)$ makes $\mathbb{P}(V)$ in a natural manner a projective space. It is called the *projective space associated to V*. When $V = k^{n+1}$ we often write $\mathbb{P}^n$ or $\mathbb{P}^n_k$ and call it simply *projective n-space (over k)*. The difference between a projectivized vector space and an abstract projective space is perhaps elucidated by the following exercise.

EXERCISE 53. Prove that the linear isomorphism ϕ in Definition 1.1 is unique up to scalar multiplication. Conclude that a projective space P determines a vector space up to scalar multiplication. Illustrate this by showing that for a 2-dimensional vector space V we have a canonical isomorphism $\mathbb{P}(V) \cong \mathbb{P}(V^*)$, but that there is no canonical isomorphism between V and V^*.

Let P be a projective space of dimension n. We can of course describe its structure by a pair (k^{n+1}, ℓ). This gives rise to a 'coordinate system' on P as follows: if we denote the coordinates of k^{n+1} by $(T_0, \ldots, T_n)$, then every point $p \in \mathbb{P}(V)$ is representable as a ratio $[p_0 : \cdots : p_n]$ of $n + 1$ elements of k that are not all zero: choose a generator $\tilde{p}$ of the line $\ell(p)$ and let $p_i = T_i(\tilde{p})$. Any other generator is of the form $\lambda\tilde{p}$ with $\lambda \in k \smallsetminus \{0\}$ and indeed, $[\lambda p_0 : \cdots : \lambda p_n] = [p_0 : \cdots : p_n]$. This is

why $[T_0 : \cdots : T_n]$ is called a *homogeneous coordinate system on* $\mathbb{P}(V)$ even though an individual T_i is not a function on $\mathbb{P}(V)$ (but the ratios T_i/T_j are, albeit that for $i \neq j$ they are not everywhere defined).

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

A map $j : P \to P'$ between two projective spaces over k is said to be *linear morphism* if for corresponding structural data (V, ℓ) and (V', ℓ') for P resp. P' there exists a linear *injection* $J : V \to V'$ such that $\ell' = \mathbb{P}(J)\ell$.

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* and 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.

We put on a projective space P the structure of a k-variety as follows. A homogeneous coordinate system $[T_0, \ldots, T_n]$ for P defines a chart for every $i = 0, \ldots, n$: if $P_{T_i} \subset P$ is the hyperplane complement defined by $T_i \neq 0$, then

$$\kappa_i : P_{T_i} \xrightarrow{\cong} \mathbb{A}^n, \quad [T_0 : \cdots : T_n] \mapsto (T_0/T_i, \ldots, \widehat{T_i/T_i}, \ldots, T_n/T_i),$$

is a bijection (chart) with inverse

$$\kappa_i^{-1} : (a_1, \ldots, a_n) \in \mathbb{A}^n \mapsto [a_1 : \cdots : a_i : 1 : a_{i+1} : \cdots : a_n] \in U.$$

Clearly, $\cup_{i=0}^n P_{T_i} = P$. We show that the collection of charts $\{P_{T_i}, \kappa_i\}_{i=0}^n$ can serve as an affine atlas for P. The coordinate change for a pair of charts, say for $\kappa_n \kappa_0^{-1}$ is as follows: the image of $P_{T_0} \cap P_{T_n}$ under κ_0 resp. κ_n is the open subset $\mathbb{A}^n_{x_n}$ resp. $\mathbb{A}^n_{x_1}$ of $\mathbb{A}^n$ and the transition map is

$$\kappa_n \kappa_0^{-1} : \mathbb{A}^n_{x_n} \to \mathbb{A}^n_{x_1}, \quad (a_1, a_2, \ldots, a_n) \mapsto (1/a_n, a_1/a_n, \ldots, a_{n-1}/a_n),$$

and hence an isomorphism of affine varieties with inverse $\kappa_0 \kappa_n^{-1}$. An atlas thus obtained from a homogeneous coordinate system $(T_0, \ldots, T_n)$ will be called a *standard atlas* for P; it gives P the structure of a prevariety $(P, \mathcal{O}_P)$: $U \subset P$ is open if and only if for $i = 0, \ldots, n$, $\kappa_i(U \cap P_{T_i})$ is open in $\mathbb{A}^n$ and $f \in \mathcal{O}_P(U)$ if and only if $f\kappa_i^{-1} \in \mathcal{O}(\kappa_i(U))$. One can easily check that this structure is in fact that of a k-variety and that it is independent of the coordinate system. We will not do this here as we will give in Section 3 a more direct proof of these assertions.

Any hyperplane $H \subset P$ can be given as $T_0 = 0$, where $[T_0 : \cdots : T_n]$ is a homogeneous coordinate system on P and so its complement $U = P \smallsetminus H = P_{T_0}$ is isomorphic to $\mathbb{A}^n$. This can also (and more intrinsically) be seen without the help of such a coordinate system. Let the projective structure on P be given by the pair (V, ℓ). Then the hyperplane H corresponds to a hyperplane $V_H \subset V$ and U corresponds to the set of 1-dimensional linear subspaces of V not contained in

H. If $e \in V^*$ is a linear form whose zero set is V_H, then $A = e^{-1}(1)$ is an affine space for V_H (it has V_H as its vector space of translations). Assigning to $v \in A$ the 1-dimensional linear subspace spanned by v defines a bijection $A \cong U$ that puts on U a structure of an affine space. This structure is easily checked to be independent of (V, ℓ, ϕ).

We could also proceed in the opposite direction and start with an affine space A and realize it as the hyperplane complement of a projective space. For this consider the vector space $F(A)$ of affine-linear functions on A and denote by $e \in F(A)$ the function on A that is constant equal to 1. Then $e^{-1}(1)$ is an affine hyperplane in $F(A)^*$. Any $a \in A$ defines a linear form on $F(A)$ by evaluation: $f \in F(A) \mapsto f(a) \in k$. Note that this form takes the value 1 on e so that we get in fact a map $A \to e^{-1}(1)$. It is not hard to check that this is an affine-linear isomorphism and so the projective space $\overline{A} := \mathbb{P}(F(A)^*)$ can serve as the projective completion of A. Paraphrasing the classical Renaissance painters, we might say that $\overline{A} \smallsetminus A$ consists of "points at infinity" of A; such a point can be given by an affine line in A with the understanding that parallel lines define the same point at infinity.

2. The Zariski topology on a projective space

We begin with giving a simpler characterization of the Zariski topology on a projective space. Let P be a projective space of dimension n over k and let $[T_0 : \cdots : T_n]$ be a homogeneous coordinate system for P. Suppose $F \in k[X_0, \ldots, X_n]$ is homogeneous of degree d so that $F(tT_0, \ldots, tT_n) = t^d F(T_0, \ldots, T_n)$ for $t \in k$. The property of this being zero only depends on $[T_0 : \cdots : T_n]$ and hence the zero set of F defines a subset of P. We shall denote this subset by $Z[F]$ and its complement $P \smallsetminus Z[F]$ by P_F. We will show in the next section that P_F is in fact affine.

PROPOSITION 2.1. *The collection $\{P_F\}_F$, where F runs over the homogeneous polynomials in $k[X_0, \ldots, X_n]$, is a basis for the Zariski topology on P. This topology is independent of the choice of our homogeneous coordinate system $[T_0, \ldots, T_n]$ and (so) every linear chart is a homeomorphism onto $\mathbb{A}^n$ that identifies the sheaf of regular functions on its domain with $\mathcal{O}_{\mathbb{A}^n}$. If $G \in k[X_0, \ldots, X_n]$ is homogeneous of the same degree as F, then G/F defines a regular function on P_F.*

PROOF. We first observe that the obvious equality $P_F \cap P_{F'} = P_{FF'}$ implies that the collection $\{P_F\}_F$ is a basis of a topology. The independence of this topology of the coordinate choice results from the observation that under a linear substitution a homogeneous polynomial transforms into a homogeneous polynomial.

Let us verify that this is the Zariski topology defined earlier. First note that the domain of each member $\kappa_i : P_{T_i} \cong \mathbb{A}^n$ is of the standard atlas is also a basis element (hence open) for the topology in question. So we must show that each κ_i is a homeomorphism. If $F \in k[T_0, \ldots, T_n]$ is homogeneous of degree d, then $\kappa_i(P_F \cap P_{T_i}) = \mathbb{A}^n_{f_i}$, where $f_i(y_1, \ldots, y_n) := F(y_1, \ldots, y_i, 1, y_{i+1}, \ldots, y_n)$ and so κ_i is open. Conversely, if $f \in k[y_1, \ldots, y_n]$ is nonzero of degree d, then its 'homogenization' $F(T_0, \ldots, T_n) := T_i^d f(T_1/T_0, \ldots \widehat{T_i/T_i} \ldots T_n/T_0)$ is homogeneous of degree d and $\kappa_i^{-1}(\mathbb{A}^n_f) = P_F \cap P_{T_i}$. So κ_i is also continuous.

For the last statement first observe that G/F indeed defines a function on P_F (think of it as regular function on $\mathbb{A}^{n+1}_F$ that is constant under scalar multiplication). Its pull-back under κ_i is $g_i(y_1, \ldots, y_n)/f_i(y_1, \ldots y_n)$, where $g_i(y_1, \ldots, y_n) := G(y_1, \ldots, 1, \ldots y_n)$, which is indeed regular on $\mathbb{A}^n_{f_i}$. □

EXERCISE 54. Let $0 \neq F \in k[X_0, \ldots, X_n]$ be homogeneous of degree d. Prove that every function $P_F \to k$ of the form G/F^r, with $r \geq 0$ and G homogeneous of the same degree as F^r, is regular and that conversely, every regular function on P_F is of this form.

In order to discuss the projective analogue of the (affine) $I \leftrightarrow Z$ correspondence, we shall need the following notions from commutative algebra.

DEFINITION 2.2. Let R be a ring. A *(nonnegatively) graded R-algebra* is an R-algebra A whose underlying additive group comes with a direct sum decomposition $A_\bullet = \oplus_{k=0}^{\infty} A_d$ into R-submodules such that the product maps $A_d \times A_e$ in A_{d+e}, or equivalently, is such that $\sum_{d=0}^{\infty} A_d t^d$ is an R-subalgebra of $A[t]$. An ideal I of such an algebra is said to be *homogeneous* if it is the direct sum of its homogeneous parts $I_d := I \cap A_d$. We shall say that an ideal I of A is *properly homogeneous*[1] if it is homogeneous and contained in the ideal $A_+ := \oplus_{d \geq 1} A_d$.

If A is a graded ring, then clearly A_0 is a subring of A so that we may also regard A as a graded A_0-algebra. In fact, A_0 is an R-subalgebra of A and A acquires its R-algebra structure via the one on A_0.

If I is a homogeneous ideal of A, then $A/I = \oplus_{d=0}^{\infty} A_d/I_d$ is again a graded R-algebra. We will be mostly concerned with the case when $A_0 = k$, so that A_+ is then a maximal ideal (and the only one that is homogeneous).

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

PROOF. The proofs of the statements in the first sentence are not difficult and so we omit them. As to the last, it suffices to show that if $\mathfrak{p} \subset A$ is a prime ideal, then the direct sum of its homogeneous parts, $\mathfrak{p}_\bullet := \oplus_n (\mathfrak{p} \cap A_n)$ is also a prime ideal. Indeed, suppose $a, b \in A$ nonzero and such that $ab \in \mathfrak{p}_\bullet$. Let a_k resp. b_l be the highest degree part of a resp. b. We prove with induction on $k + l$ that a or b is in $\mathfrak{p}_\bullet$. Since we have $a_k b_l = (ab)_{k+l} \in \mathfrak{p}_{k+l} \subset \mathfrak{p}$, it follows that $a_k \in \mathfrak{p}$ or $b_l \in \mathfrak{p}$. Let us assume that $a_k \in \mathfrak{p}$. Then $a_k \in \mathfrak{p}_\bullet$ and so $(a - a_k)b \in \mathfrak{p}_\bullet$. By our induction assumption, then $a - a_k$ or b is in $\mathfrak{p}_\bullet$. It follows that a or b is in $\mathfrak{p}_\bullet$. □

The prime example of a graded k-algebra is furnished by a vector space V of finite positive dimension ($n + 1$, say), which we consider as an affine variety, but (in contrast to an affine space) one of which we remember that it comes with the action of the multiplicative group of k by scalar multiplication. The space of $F \in k[V]$ that are homogeneous of degree d in the sense that $F(tv) = t^d F(v)$ for all $v \in V$ and $t \in k$ make up a k-linear subspace $k[V]_d$ of finite dimension. This makes $k[V] = \oplus_{d \geq 0} k[V]_d$ a graded k-algebra and the decomposition is the one into eigenspaces with respect to the action of scalar multiplication. (A choice of basis $(T_0, \ldots, T_n)$ of V^* identifies V with $\mathbb{A}^{n+1}$ and then $k[V]_d$ becomes the space of homogeneous polynomials in $(T_0, \ldots, T_n)$ of degree d.) Note that for any $F \in k[V]_d$ the zero set $Z(F) \subset V$ is invariant under scalar multiplication. This is still true for an intersection of such zero sets, in other words, for a properly homogeneous ideal $I_\bullet \subset k[V]_+$, $Z(I) \subset V$ is a closed subset of V that is invariant under scalar multiplication. Such a closed subset is called an *affine cone*. The origin is called the *vertex* of that cone. Since $k[V]_+$ defines the vertex, we always have

[1] This is not a generally adopted terminology.

$0 \in Z(I)$. The intersection of the $Z[F]$, with $F \in \cup_{d\geq 1} I_d$ defines a closed subset $Z[I]$ of $\mathbb{P}(V)$, whose points correspond to the one-dimensional subspaces of V that are contained in $Z(I)$.

LEMMA 2.4. *For an affine cone $C \subset V$, $I(C)$ is a properly homogeneous radical ideal of $k[V]$ and hence defines a closed subset $\mathbb{P}(C) := Z[I(C)]$ of $\mathbb{P}(V)$.*

PROOF. Let $F \in I(C)$. Write $F = \sum_{d\geq 0} F_d$. We must show that each homogeneous component of F_i lies in $I(C)$. As C is invariant under scalar multiplication, the polynomial $F(tv) = \sum_{d\geq 1} t^d F_d(v)$ (as an element of $k[\mathbb{A}^1 \times V]$) vanishes on $\mathbb{A}^1 \times C$ in $\mathbb{A}^1 \times V$. Clearly the zero set of $I(C)[t]$ is $\mathbb{A}^1 \times C \subset \mathbb{A}^1 \times V$ and since the quotient is $k[V][t]/I(C)[t] = k[C][t]$ is reduced, we have $I(\mathbb{A}^1 \times C) = I(C)[t]$. It follows that $F_d \in I(C)$ for all d. □

Conversely, given a closed subset $X \subset \mathbb{P}(V)$, let for $d \geq 1$, $I_{X,d}$ be the set of $F \in k[V]_d$ for which $X \subset Z[F]$ and put $I_{X,0} = 0$. Then $I_{X,d}$ is a k-vector space and $I_{X,d} \cdot k[V]_e \subset I_{X,d+e}$ so that $I_X := \oplus_{d\geq 1} I_{X,d}$ is a properly homogeneous ideal of $k[V]$. It is also a radical ideal and we have $X = Z[I_X]$. So $\mathrm{Cone}(X) := Z(I_X)$ is the cone in V that as a set is just the union of the 1-dimensional linear subspaces of V parameterized by X.

COROLLARY 2.5. *The maps $C \mapsto \mathbb{P}(C)$ and $X \mapsto I(X)$ set up bijections between (i) the collection of affine cones in V, (ii) the collection of closed subsets of $\mathbb{P}^n$, and (iii) the collection of properly homogeneous radical ideals contained in $k[V]$. This restricts to bijections between (i) the collection of irreducible affine cones in V strictly containing $\{0\}$, (ii) the collection of irreducible subsets of $\mathbb{P}(V)$ and (iii) the collection of homogeneous prime ideals of $k[V]$ strictly contained in $k[V]_+$.*

PROOF. The first assertion sums up the preceding discussion. The last assertion follows from the observation that the degenerate cone $\{0\} \subset V$ corresponds to the empty subset of $\mathbb{P}(V)$ and to the homogeneous ideal $k[V]_+$. □

DEFINITION 2.6. The *homogeneous coordinate ring* of a closed subset X of $\mathbb{P}(V)$ is the coordinate ring of the affine cone over X, $k[\mathrm{Cone}(X)] = k[V]/I_X$, endowed with the grading defined by $k[\mathrm{Cone}(X)]_d = k[T_0, \ldots T_n]_d/I_{X,d}$. More generally, if Y is an affine variety, and X is a closed subset of $\mathbb{P}(V) \times Y$, then the *homogeneous coordinate ring of X relative to Y* of a closed subset is the coordinate ring of the corresponding closed cone in $V \times Y$ over Y, endowed with the grading defined by the coordinates of V.

EXERCISE 55. Let A be a graded ring.

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

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

EXERCISE 56. Let $S_\bullet$ be a graded k-algebra that is reduced, finitely generated and has $S_0 = k$.

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

EXERCISE 57. Let Y be an affine variety.

(a) Show that a homogeneous element of the graded ring $k[Y][T_0, \ldots, T_n]$ defines a closed subset of $Y \times \mathbb{P}^n$ as its zero set.
(b) Prove that every closed subset of $Y \times \mathbb{P}^n$ is an intersection of finitely many zero set of homogeneous elements of $k[Y][T_0, \ldots, T_n]$.
(c) Prove that we have a bijective correspondence between closed subsets of $Y \times \mathbb{P}^n$ and the homogeneous radical ideals in $k[Y][T_0, \ldots, T_n]_+$.

3. The Segre embeddings

First we show how a product of projective spaces can be realized as a closed subset of a projective space. This will imply among other things that a projective space is a variety. Consider the projective spaces $\mathbb{P}^m$ and $\mathbb{P}^n$ with their homogeneous coordinate systems $[T_0 : \cdots : T_m]$ and $[W_0 : \cdots : W_n]$. We also consider a projective space whose homogeneous coordinate system is the set of matrix coefficients of an $(m+1)\times(n+1)$-matrix $[Z_{00} : \cdots : Z_{ij} : \cdots : Z_{mn}]$; this is just $\mathbb{P}^{mn+m+n}$ with an unusual indexing of its homogeneous coordinates.

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

PROOF. For the first part it is enough to show that for every chart domain $\mathbb{P}^{mn+m+n}_{Z_{ij}}$ of the standard atlas of $\mathbb{P}^{mn+m+n}$, $f^{-1}\mathbb{P}^{mn+m+n}_{Z_{ij}}$ is open in $\mathbb{P}^m \times \mathbb{P}^n$ and is mapped by f isomorphically onto a closed subset of $\mathbb{P}^{mn+m+n}_{Z_{ij}}$. For this purpose we may (simply by renumbering) assume that $i = j = 0$. So then $\mathbb{P}^{mn+m+n}_{Z_{00}} \subset \mathbb{P}^{mn+m+n}$ 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 $f^{-1}\mathbb{P}^{mn+m+n}_{Z_{00}}$ is defined by $T_0 W_0 \neq 0$. This is just $\mathbb{P}^m_{T_0} \times \mathbb{P}^n_{W_0}$ and hence is parametrized by $x_1 := T_1/T_0, \ldots, x_m := T_m/T_0$ and $y_1 := W_1/W_0, \ldots, y_n := W_n/W_0$. In terms of these coordinates, $f : f^{-1}\mathbb{P}^{mn+m+n}_{Z_{00}} \to \mathbb{P}^{mn+m+n}_{Z_{00}}$ 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 among these are $z_{i0} = x_i$ and $z_{0j} = y_j$ and since these generate $k[\mathbb{A}^m \times \mathbb{A}^n] = k[x_1, \ldots, x_m, y_1, \ldots, y_n]$, f indeed restricts to a closed immersion $f^{-1}\mathbb{P}^{mn+m+n}_{Z_{00}} \to \mathbb{P}^{mn+m+n}_{Z_{00}}$.

In case $m = n$, we must also show that the condition $T_i W_j = T_j W_i$ for $0 \leq i < j \leq m$ implies that $[T_0 : \cdots : T_m] = [W_0 : \cdots : W_m]$, assuming that not all T_i resp. W_j are zero. Suppose $T_i \neq 0$. Since $W_j = (W_i/T_i).T_j$ for all j, it follows that $W_i \neq 0$ and so $[W_0 : \cdots : W_m] = [T_0 : \cdots : T_m]$. □

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

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

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

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

PROOF. The first statement follows from Proposition 11.3 of Ch. 1 and the second from Proposition 3.1. □

EXERCISE 58. (a) Prove that the image of the Segre embedding is the common zero set of the homogenenous polynomials $Z_{ij}Z_{kl} - Z_{il}Z_{kj}$.
(b) Show that for every $(p, q) \in \mathbb{P}^m \times \mathbb{P}^n$ the image of $\{p\} \times \mathbb{P}^n$ and $\mathbb{P}^m \times \{q\}$ in $\mathbb{P}^{mn+m+n}$ is a linear subspace.
(c) Prove that the map $\mathbb{P}^n \to \mathbb{P}^{(n^2+3n)/2}$ defined by $Z_{ij} = T_iT_j$, $0 \le i \le j \le n$ is an isomorphism on a closed subset defined by quadratic equations. Find these equations for $n = 2$.
(d) As a special case we find that the quadric hypersurface in $\mathbb{P}^3$ defined by $Z_0Z_1 - Z_2Z_3 = 0$ is isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$. Identify in this case the two systems of lines on this quadric.

EXERCISE 59 (Intrinsic Segre embedding). Let V and W be finite dimensional k-vector spaces. Describe the Segre embedding for $\mathbb{P}(V) \times \mathbb{P}(W)$ intrinsically as a morphism $\mathbb{P}(V) \times \mathbb{P}(W) \to \mathbb{P}(V \otimes W)$.

4. Blowing up and projections

By way of introduction we first explain the blowup of a linear subspace of an affine space. Fix an integer $1 \le c \le n$ and denote by $Y \subset \mathbb{A}^n$ the linear codimension c subspace defined by $x_1 = \cdots = x_c = 0$. Consider the morphism $\pi : \mathbb{A}^n \setminus Y \to \mathbb{P}^{c-1}$ defined by $\pi(x_1, \ldots, x_n) = [x_1 : \cdots : x_c]$. The graph Γ_π of π is the set of $((x_1, \ldots, x_n), [T_1 : \cdots : T_c]) \in (\mathbb{A}^n \setminus Y) \times \mathbb{P}^{c-1}$ with $[T_1 : \cdots : T_c] = [x_1 : \cdots : x_c]$. Such points satisfy the equations $x_iT_j = x_jT_i$, $1 \le i < j \le c$. The common zero set of these equations defines a closed subset of $\mathbb{A}^n \times \mathbb{P}^{c-1}$, called the *blowup of* $\mathbb{A}^n$ *along* Y and denoted by $\mathrm{Bl}_Y(\mathbb{A}^n)$. It is easily seen to be the union of Γ_π and $Y \times \mathbb{P}^{c-1}$. We claim that Γ_π is dense in $\mathrm{Bl}_Y(\mathbb{A}^n)$. For this it is of course enough to show that the closure $\overline{\Gamma}_\pi$ of Γ_π contains $Y \times \mathbb{P}^{c-1}$. To see this, we note that for instance $\mathrm{Bl}_Y(\mathbb{A}^n) \cap (\mathbb{A}^n \times \mathbb{P}^{c-1}_{T_1})$ is the set of $(x_1, \ldots, x_n), [1 : t_2 : \cdots ; t_c])$ satisfying $x_i = t_ix_1$ for $i = 2, \ldots, c$ and hence is parametrized by $\mathbb{A}^n$ via

$$(x_1, t_2, \ldots, t_c, x_{c+1}, \ldots, x_n) \mapsto ((x_1, t_2x_1, \ldots, t_cx_1, x_{c+1}, \ldots, x_n), [1 : t_2 : \cdots ; t_c]).$$

In terms of this parametrization, $\mathbb{A}^n_{x_1}$ maps onto $\Gamma_\pi \cap (\mathbb{A}^n_{x_1} \times \mathbb{P}^{c-1})$, whereas $Z(x_1) \subset \mathbb{A}^n$ maps isomorphically onto $Y \times \mathbb{P}^{c-1}_{T_1}$. It follows that $\overline{\Gamma}_\pi \supset Y \times \mathbb{P}^{c-1}_{T_1}$. Similarly, $\overline{\Gamma}_\pi \supset Y \times \mathbb{P}^{c-1}_{T_i}$ for $i = 2, \ldots, c$ and hence $\overline{\Gamma}_\pi \supset Y \times \mathbb{P}^{c-1}$. We call $Y \times \mathbb{P}^{c-1}$ the *exceptional divisor* of this blowup. The term blowup sometimes also refers to projection on the first factor, $p : \mathrm{Bl}_Y(\mathbb{A}^n) \to \mathbb{A}^n$, rather than just to its domain.

This construction has a more geometric interpretation. We can think of a point of $\mathbb{P}^{c-1}$ as a one dimensional subspace of k^c, but here it is better is to think of it as a codimension $c-1$ linear subspace of $k^n = \mathbb{A}^n$ which contains Y. For then $\mathrm{Bl}_Y(\mathbb{A}^n)$ can be regarded as the set of pairs (p, Y'), where $p \in \mathbb{A}^n$ and Y' is codimension $c-1$ subspace of $\mathbb{A}^n$ which contains both Y and p and π is then understood as assigning to $x \in \mathbb{A}^n - Y$ the linear span of x and Y. The projection onto the second factor, $\mathrm{Bl}_Y(\mathbb{A}^n) \to \mathbb{P}^{c-1}$, extends π and is often called the *projection away from* Y.

REMARK 4.1. The homogeneous coordinate ring of $\mathrm{Bl}_Y(\mathbb{A}^n)$ is the graded $k[x_1, \dots, x_n]$-algebra $k[x_1, \dots, x_n][T_1, \dots, T_c]$ modulo the ideal generated by the $x_i T_j - x_j T_i$, $1 \le i < j \le c$, with each T_i of degree 1. It admits the following elegant description: consider the homomorphism of graded $k[x_1, \dots, x_n]$-algebras

$$k[x_1, \dots, x_n][T_1, \dots, T_c]/(x_i T_j - x_j T_i, 1 \le i < j \le c) \to \sum_{d \ge 0} I(Y)^d T^d, \quad T_i \mapsto T x_i,$$

where $I(Y)$ is the ideal defining Y (so generated by $x_1, \dots, x_c$) and $I(Y)^0 := k[x_1, \dots, x_n]$. The right hand side is to be viewed as a $k[x_1, \dots, x_n]$-subalgebra of the graded algebra $k[x_1, \dots, x_n][T]$, with $\deg(T) = 1$ (so as a $k[x_1, \dots, x_n]$-algebra generated by $x_1 T, \dots, x_c T$) and can also be written as $\oplus_{d \ge 0} I(Y)^d$. This is in fact an isomorphism whose inverse is defined as follows: a k-basis of the right hand side consists of the monomials $x_1^{d_1} \cdots x_n^{d_n} T^d$ with $d_1 + \cdots + d_c \ge d$ and then the inverse assigns to $x_1^{d_1} \cdots x_n^{d_n} T^d$ the image in the left hand side of a monomial $x_1^{d_1} \cdots x_n^{d_n} T_1^{e_1} \cdots T_c^{e_c}$, where $0 \le e_i \le d_i$ are such that $\sum_i e_i = d$ (check that the image is independent of this choice). The exceptional divisor is defined by the ideal $I(Y) = (x_1, \dots, x_c)$. The associated quotient ring is a graded $k[x_1, \dots, x_n]/I(Y) = k[Y]$-algebra, which in the first description yields $k[Y][T_1, \dots, T_c]$ (this is indeed the homogeneous coordinate ring of $Y \times \mathbb{P}^{c-1}$) and in the second yields $\sum_{d \ge 0} I(Y)^d / I(Y)^{d+1} T^d \cong \oplus_{d \ge 0} I(Y)^d / I(Y)^{d+1}$. These must of course be isomorphic as $k[Y]$-algebras, but the second description is more canonical in the sense that it identifies the exceptional divisor with the projectivized normal bundle of Y in $\mathbb{A}^n$. [2]

The projection $p : \mathrm{Bl}_Y(\mathbb{A}^n) \to \mathbb{A}^n$ induces a $k[x_1, \dots, x_n]$-algebra homomorphism $p^* : k[x_1, \dots, x_n] \to \sum_{d \ge 0} I(Y)^d T^d$ that is *not* the obvious inclusion, but is defined by $p^*(x_i) = x_i T$ for $i \le c$ and $p^*(x_i) = x_i$ for $i > c$. So if $H \subset \mathbb{A}^n$ is a hypersurface, and defined by $f \in k[x_1, \dots, x_n]$ say, then $p^{-1}H$ (also called the *total transform* of H under p) is defined by $f(x_1 T, \dots, x_c T, x_{c+1}, \dots, x_n)$, which we view here as an element of $\sum_{d \ge 0} I(Y)^d T^d$ by writing it as $\sum_{d \ge 0} T^d f_d(x_1, \dots, x_n)$. The *strict transform of* H under p is by definition the closure of $H \setminus H \cap Y$ in $\mathrm{Bl}_Y(X)$ and if $m \ge 0$ is such that $f_0 = \cdots = f_{m-1} = 0 \ne f_m$, then a defining equation for it is $(p^* f)_{\text{str}} := T^{-m} p^* f = \sum_{d \ge 0} T^d f_{m+d}$. More generally, if $X \subset \mathbb{A}^n$ is a closed subset, then the ideal generated by the $p^* f$, $f \in I(X)$, defines of course its total transform $p^{-1}(X)$, whereas the ideal generated by the $(p^* f)_{\text{str}}$, $f \in I(X)$, defines the strict transform of X under p, that is, the closure of $X \setminus X \cap Y$ in $\mathrm{Bl}_Y(X)$.

This blowing up process models a projective analogue that we will discuss next. Let P be a projective space of dimension n and $Q \subset P$ a linear subspace of codimension $c (= \dim P - \dim Q)$. Let us denote by $\mathbb{P}(P; Q)$ the collection of linear subspaces Q' of P which contain Q as a hyperplane (and so are of dimension $\dim Q + 1$).

[2] Nothing stops us now in defining for an arbitrary ring R the 'blowup' of an ideal $I \subset R$ as the graded R-algebra $\oplus_{d \ge 0} I^d$ (where $I^0 = R$) and to regard the graded quotient $\oplus_{d \ge 0} I^d / I^{d+1}$ as defining its 'exceptional divisor'. If Y a closed subset of an affine variety X, then the blowup $\mathrm{Bl}_Y(X)$ is defined by applying this to $R = k[X]$ and $I = I(Y)$: if $I(Y)$ has $d > 0$ generators, then this is a closed subset of $X \times \mathbb{P}^{d-1}$; for $I(Y) = (0)$ (so that $Y = \emptyset$) we get of course X. When Y is nowhere dense in X and $f_1, \dots, f_d$ generate $I(X)$ in $k[X]$, then $\mathrm{Bl}_Y(X)$ is the closure in $X \times \mathbb{P}^{d-1}$ of the graph of $[f_1 : \cdots : f_d] : X \setminus Y \to \mathbb{P}^{d-1}$.

LEMMA 4.2. *The space $\mathbb{P}(P;Q)$ has in a natural manner the structure of a projective space of dimension $c-1$ (where dimension -1 means empty). Through every $p \in P \smallsetminus Q$ passes exactly one member of $\mathbb{P}(P;Q)$ and this defines a morphism $\pi_Q : P \smallsetminus Q \to \mathbb{P}(P;Q)$. Concretely, if $n := \dim P$ and we choose a system of homogeneous coordinates $[T_0 : \dots T_n]$ for P such that Q is given by $T_0 = \cdots = T_{c-1}$, then $[T_0 : \cdots : T_{c-1}]$ defines a system of homogeneous coordinates for $\mathbb{P}(P;Q)$ and π_Q is simply given by $[T_0 : \cdots : T_n] \mapsto [T_0 : \cdots : T_{c-1}]$.*

PROOF. Let $\ell : P \cong \mathbb{P}(V)$ be a structural bijection. Then $Q = \ell^{-1}\mathbb{P}(W)$ for some linear subspace $V_Q \subset V$ and so the Q' correspond to the linear subspaces $V_{Q'} \subset V$ which contain V_Q as a hyperplane. These in turn correspond to the one-dimensional subspaces of V/V_Q and so we get a bijection $\mathbb{P}(P;Q) \cong \mathbb{P}(V/V_Q)$. For another choice of structural bijection (V', ℓ') there must exist a linear isomorphism $V \cong V'$ which then automatically takes V_Q onto V'_Q and so induces a linear isomorphism $V/V_Q \cong V'/V'_Q$. We thus see that the projective space structure on $\mathbb{P}(P;Q)$ is intrinsically defined. The proof of the last assertion is left to you. □

DEFINITION-LEMMA 4.3. *The* blowup of P along Q, *denoted* $\mathrm{Bl}_Q P$, *is the closure of the graph of $\pi_Q : P \smallsetminus Q \to \mathbb{P}(P;Q)$ in $P \times \mathbb{P}(P;Q)$ (hence is a projective variety). It enjoys the following properties:*

(i) *The variety $\mathrm{Bl}_Q P$ is nonsingular and irreducible and the projection on the first factor, $p_1 : \mathrm{Bl}_Q P \to P$, is an isomorphism over $P \smallsetminus Q$.*
(ii) *The preimage over Q is $Q \times \mathbb{P}(P;Q)$ and is a nonsingular hypersurface in $\mathrm{Bl}_Q P$, called the* exceptional divisor *of the blowup.*
(iii) *The projection to the second factor defines a* locally trivial bundle

$$p_2 : (\mathrm{Bl}_Q P, Q \times \mathbb{P}(P;Q)) \to \mathbb{P}(P;Q)$$

of pairs of projective spaces of dimension $1+\dim Q$ and $\dim Q$. To be precise, if $U \subset \mathbb{P}(P;Q)$ is a hyperplane complement (hence an affine space), then there exists a linear subspace $Q' \subset P$ which contains Q as a hyperplane and an isomorphism $p_2^{-1}U \cong Q' \times U$ which is the identity on $Q \times U$ and whose second component is given by p_2.

PROOF. We use a homogeneous coordinate system $[T_0 : \cdots : T_n]$ for P as above (so that Q is given by $T_0 = \cdots = T_{c-1} = 0$). If we denote the corresponding coordinate system for $\mathbb{P}(P;Q)$ by $[S_0 : \cdots : S_{c-1}]$, then the graph of π_Q in $P \times \mathbb{P}(P;Q)$ is given by the pairs $([T_0 : \cdots : T_n], [S_0 : \cdots : S_{c-1}])$ with $(T_0, \dots, T_{c-1}) \neq (0, \dots, 0)$ and $[T_0 : \cdots : T_{c-1}] = [S_0 : \cdots : S_{c-1}]$. The last proportionality property is equivalent to: $T_i S_j = T_j S_i$ for all $0 \leq i < j < c$. Let Γ be the closed subset of $P \times \mathbb{P}(P;Q)$ defined by these equations. We shall eventually see that $\Gamma = \mathrm{Bl}_Q P$. As the equations in question are satisfied when $(T_0, \dots, T_{c-1}) = (0, \dots, 0)$, we have $Q \times \mathbb{P}(P;Q) \subset \Gamma$. On the other hand, for any $([T_0 : \cdots : T_n], [S_0 : \cdots : S_{c-1}]) \in \Gamma \smallsetminus (Q \times \mathbb{P}(P;Q))$, we have $T_i \neq 0$ for some $i < c$ and so $S_j = (S_i/T_i).T_j$ for all $j < c$. Since not all S_j are zero, we must have $S_i \neq 0$ as well and so then $[T_0 : \cdots : T_{c-1}] = [S_0 : \cdots : S_{c-1}]$. Hence $\Gamma \smallsetminus (Q \times \mathbb{P}(P;Q))$ is the graph of π_Q.

Let us now see what the projection $\Gamma \to \mathbb{P}(P;Q)$ is like over $\mathbb{P}(P;Q)_{S_0}$ in terms of the standard chart $(y_1, \dots, y_{c-1}) \in \mathbb{A}^m \mapsto [1 : y_1 : \cdots : y_{c-1}] \in \mathbb{P}(P;Q)_{S_0}$. We let $Q' \subset P$ be defined by $T_1 = \cdots = T_{c-1} = 0$. It is clear that Q' contains Q as a hyperplane (defined by $T_0 = 0$). Note that $\Gamma_{S_0} := \Gamma \cap (P \times \mathbb{P}(P;Q)_{S_0})$ is

parametrized by $Q' \times \mathbb{P}(P;Q)_{S_0}$ by means of the morphism

$$([T_0 : T_c : T_{c+1} : \cdots : T_n], [1 : y_1 : \cdots : y_{c-1}]) \in Q' \times \mathbb{P}(P;Q)_{S_0} \mapsto$$
$$([T_0 : T_0 y_1 : \cdots : T_0 y_{c-1} : T_c : T_{c+1} : \cdots : T_n], [1 : y_1 : \cdots : y_{c-1}]) \in \Gamma_{S_0},$$

This is an isomorphism (the inverse is obvious) which commutes with the projection on $\mathbb{P}(P;Q)_{S_0}$. Since $Q \times \mathbb{P}(P;Q)_{S_0}$ is defined in Γ_{S_0} by $T_0 = T_1 = \cdots T_{c-1} = 0$, it follows that its preimage in $Q' \times \mathbb{P}(P;Q)_{S_0}$ is also $Q \times \mathbb{P}(P;Q)_{S_0}$. In particular, $Q \times \mathbb{P}(P;Q)_{S_0}$ lies in the closure of the graph of π_Q. This remains true if we replace $\mathbb{P}(P;Q)_{S_0}$ by $\mathbb{P}(P;Q)_{S_i}$, $i = 1, \ldots, c-1$, or by any other hyperplane complement in $\mathbb{P}(P;Q)$. It follows that $\Gamma = \mathrm{Bl}_Q P$ and that $\mathrm{Bl}_Q P$ enjoys the stated properties. □

COROLLARY 4.4. *Suppose that in the situation of Definition-Lemma 4.3, $Z \subset P$ is an irreducible and closed subset such that $Z \cap Q = \emptyset$. Then $\pi_Q | Z : Z \to \mathbb{P}(P;Q)$ is a finite morphism and (so)* $\dim Z < c$.

Note that the dimension inequality amounts to the assertion that Z will meet every linear subspace of P whose codimension is equal to the dimension of Z. For its proof we shall need the following lemma.

LEMMA 4.5. *Let P a projective space, $U \subset P$ a hyperplane complement, X be a variety and $Z \subset U \times X$ a subset that is closed in $P \times X$. Then the projection $\pi_X | Z : Z \to X$ is a finite morphism.*

PROOF. Without loss of generality we may assume that X is affine. Since U is also affine, it follows that Z, being a closed subset of $U \times X$ is affine.

Choose homogeneous coordinates $[T_0 : \ldots ; T_n]$ for P such that $U = P_{T_0}$. So if $I \subset k[X][T_0, \ldots, T_n]$ is the homogeneous ideal defining Z, then the ideal $J \subset k[X][T_0, \ldots, T_n]$ generated by I and T_0 defines the empty set in $P \times X$ and so its radical is $k[X][T_0, \ldots, T_n]_+$. In particular, there exists an integer $r > 0$ such that $T_i^r \in J$ for $i \in \{1, \ldots, n\}$. Write $T_i^r \equiv T_0 G_i \pmod{I_r}$ with $G \in k[X][T_0, \ldots, T_n]_{r-1}$. We pass to the affine coordinates of U by substituting 1 for T_0 and t_i for T_i. Then G_i defines a $g_i \in k[X][t_1, \ldots, t_n] = k[X \times \mathbb{A}^n]$ of degree $\leq r-1$ in the t-variables and we have $t_i^r \equiv g_i \pmod{I(Z)}$. So if we write $\bar{t}_i$ for the image of t_i in $k[Z]$, then $\bar{t}_i^r$ is a $k[X]$-linear combination of monomials $\bar{t}_1^{s_1} \cdots \bar{t}_n^{s_n}$ with $s_i < r$ for all i. This proves that $k[Z]$ is a finitely generated $k[X]$-module so that $\pi_X | Z : Z \to X$ is a finite morphism. □

PROOF OF COROLLARY 4.4. We use the notation of Definition-Lemma 4.3. Put $\tilde{Z} := p_1^{-1} Z$. This is closed subset of $\mathrm{Bl}_Q(P)$ which is disjoint with $Q \times \mathbb{P}(P;Q)$ and is mapped by p_1 isomorphically onto Z. So it suffices to prove that $p_2 | \tilde{Z} : \tilde{Z} \to \mathbb{P}(P;Q)$ is finite. According to 4.3, $p_2 : (\mathrm{Bl}_Q(P), Q \times \mathbb{P}(P;Q)) \to \mathbb{P}(P;Q)$ admits a local trivialization over a hyperplane complement $\mathbb{P}(P;Q)_{S_i}$ which identifies $\tilde{Z}_{S_i}$ with a closed subset of $Q' \times \mathbb{P}(P;Q)_{S_i}$, where $Q' \subset P$ is a linear subspace which contains Q as a hyperplane. Our assumption implies that $\tilde{Z}_{S_i} \subset (Q' \setminus Q) \times \mathbb{P}(P;Q)_{S_i}$ and so it satisfies the hypotheses of Lemma 4.5 (with $U = Q' \setminus Q$). So the projection $\tilde{Z}_{S_i} \to \mathbb{P}(P;Q)_{S_i}$ is finite. This implies that the projection $\tilde{Z} \to \mathbb{P}(P;Q)$ is finite and in particular that $\dim Z = \dim \tilde{Z} \leq \dim \mathbb{P}(P;Q) = c - 1$. □

We have also a kind of converse to Corollary 4.4:

PROPOSITION 4.6. *For every closed subset Z of a projective space P there exists a linear subspace in P of codimension* $\dim(Z) + 1$ *which misses Z.*

PROOF. We may (and will) assume that Z is irreducible and $\neq P$. Let $i \in \{-1, \ldots, \operatorname{codim}(Z) - 1\}$. We prove with induction on i that Z misses a linear subspace of dimension i. For $i = -1$, the empty subspace will do. For $i = 0$, we must have $Z \neq P$ and so we can take for our linear subspace any singleton in $P - Z$. When $i > 0$, there exists by induction hypothesis a linear subspace $Q \subset P$ of dimension $(i-1)$ which does not meet Z. By Corollary 4.4, $\pi_Q | Z : Z \to \mathbb{P}(P, Q)$ is a finite morphism and so $\dim \pi_Q(Z) = \dim Z < \dim P - i = \dim \mathbb{P}(P, Q)$. Hence there exist a point in $\mathbb{P}(P, Q) - \pi_Q(Z)$. This defines a linear subspace Q' in P of dimension i which passes through Q and misses Z. □

5. Elimination theory and projections

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

THEOREM 5.1. *Let P be a projective space. Then for any variety X, the projection $\pi_X : P \times X \to X$ is closed.*

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

Given an integer $d \geq 0$, let us write V_d for $k[T_0, T_1]_d$, the k-vector space of homogeneous polynomials in $k[T_0, T_1]$ of degree d. The monomials $(T_0^i T_1^{d-i})_{i=0}^d$ form a basis, in particular, $\dim V_d = d + 1$. Given $F \in V_m$ and $G \in V_n$, then

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

is a linear map between two k-vector spaces of the same dimension $m + n$. The *resultant* $R(F, G)$ of F and G is defined as the determinant of this linear map with respect to the monomial bases of the summands of $V_{n-1} \oplus V_{m-1}$ and of V_{n+m-1}. So $R(F, G) = 0$ if and only if $u_{F,G}$ fails to be injective. Notice that if $F = \sum_{i=0}^m a_i T_0^i T_1^{m-i}$ and $G = \sum_{j=0}^n b_i T_0^i T_1^{n-i}$, then the matrix of $u_{F,G}$ with respect to the monomial bases is

$$\begin{pmatrix}
a_0 & 0 & 0 & \cdots & 0 & b_0 & 0 & \cdots & \cdots & 0 \\
a_1 & a_0 & 0 & \cdots & 0 & b_1 & b_0 & \cdots & \cdots & 0 \\
a_2 & a_1 & a_0 & \cdots & 0 & b_2 & b_1 & \cdots & \cdots & 0 \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
a_m & a_{m-1} & * & \cdots & * & * & * & \cdots & \cdots & * \\
0 & a_m & * & \cdots & * & * & * & \cdots & \cdots & * \\
0 & 0 & a_m & \cdots & * & * & * & \cdots & \cdots & * \\
0 & 0 & 0 & \cdots & * & * & * & \cdots & \cdots & * \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
0 & 0 & \cdots & \cdots & a_{m-1} & 0 & 0 & \cdots & \cdots & b_{n-1} \\
0 & 0 & 0 & \cdots & a_m & 0 & 0 & 0 & \cdots & b_n
\end{pmatrix}$$

from which we see that its determinant $R(F, G)$ is a polynomial in the coefficients of F and G. So the resultant defines an element of $k[V_m \times V_n] = k[V_m] \otimes k[V_n]$.

LEMMA 5.2. *$R(F, G) = 0$ if and only if F and G have a common linear factor.*

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

Conversely, if F and G have a common linear factor L: $F=LF_1$, $G=LG_1$, then $G_1F=F_1G$ and so $(G_1,-F_1)\in V_{n-1}\oplus V_{m-1}$ is a nonzero element of the kernel of $u_{F,G}$. □

PROOF OF THEOREM 5.1. Let $Z\subset P\times X$ be closed. It is clear that $\pi_X(Z)$ is closed in X if for every open affine subset $X'\subset X$, $\pi_X(Z)\cap X'$ is closed in X'. Since $\pi_X(Z)\cap X'=\pi_{X'}(Z\cap(\mathbb{P}^n\times X'))$ we may (and will) assume that is X affine. We put $n:=\dim P$ and choose a homogeneous coordinate system $[T_0:\cdots:T_n]$ for P. We proceed with induction on n, starting with the crucial case $n=1$.

Denote by I_Z the homogeneous ideal in the graded algebra $k[X][T_0,T_1]$ of functions vanishing on Z. Then Z is the common zero set of the members of I_Z (see Exercise 57). For every homogeneous pair $F,G\in\cup_m k[X][T_0,T_1]_m$, we can form the resultant $R(F,G)\in k[X]$. We claim that $\pi_X(Z)$ is the common zero set $Z(\mathcal{R})\subset X$ of the set of resultants $R(F,G)$ of pairs of homogeneous forms F,G taken in $\cup_m I_{Z,m}$, hence is closed in X.

Suppose that $y\in\pi_X(Z)$. Then $(y,p)\in Z$ for some $p\in\mathbb{P}^1$ and so p is a common zero of each pair F_y,G_y, where $F,G\in\cup_m I_{Z,m}$ and the subscript y refers to substituting y for the first argument. So $R(F,G)(y)=0$ and hence $y\in Z(\mathcal{R})$.

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

Now assume $n\geq 2$. Let $q=[0:\cdots:0:1]$ and consider the blowup $\tilde{\mathbb{P}}^n:=\mathrm{Bl}_{\{q\}}\mathbb{P}^n\to\mathbb{P}^n$. Recall that an element of $\tilde{\mathbb{P}}^n$ is the set of pairs in $([T_0:\cdots:T_n],[S_0:\cdots:S_{n-1}])$ in $\mathbb{P}^n\times\mathbb{P}^{n-1}$ with $[T_0:\cdots:T_{n-1}]=[S_0:\cdots:S_{n-1}]$. We have seen that over the open subset $\mathbb{P}^{n-1}_{S_i}\subset\mathbb{P}^{n-1}$ defined by $S_i\neq 0$, the projection $\tilde{\mathbb{P}}^n_{S_i}\to\mathbb{P}^{n-1}$ is isomorphic to the projection $\mathbb{P}^1\times\mathbb{P}^{n-1}_{S_i}\to\mathbb{P}^{n-1}_{S_i}$. Hence the projection $\pi_1:\tilde{\mathbb{P}}^n\times X\to\mathbb{P}^{n-1}\times X$ is over $\mathbb{P}^{n-1}_{S_i}\times X$ like $\mathbb{P}^1\times\mathbb{P}^{n-1}_{S_i}\times X\to\mathbb{P}^{n-1}_{S_i}\times X$. So this projection is closed over $\mathbb{P}^{n-1}_{S_i}\times X$. It follows that the projection π_1 is closed. The preimage $\tilde{Z}$ of Z under the projection $\tilde{\mathbb{P}}^n\times X\to\mathbb{P}^n\times X$ is closed and by what we just proved, $\pi_1(\tilde{Z})$ is closed in $\mathbb{P}^{n-1}\times X$. By induction, the image of the latter under the projection $\pi_2:\mathbb{P}^{n-1}\times X\to X$ is closed. But this is just $\pi_X(Z)$. □

REMARK 5.3. This proof can be adapted to show more, namely that given a closed and irreducible subset $Z\subset P\times X$, then for any $x\in\pi_X(Z)$, $Z_x:=\{p\in P:(p,x)\in Z\}$ has dimension $\geq\dim Z-\dim\pi_X(Z)$ with equality holding over an open-dense subset of $\pi_X(Z)$.

Here are two corollaries.

COROLLARY 5.4. *Let X be a projective variety. Then any morphism from X to a variety is closed (and hence has closed image).*

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

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

COROLLARY 5.5. *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. If $f : X \to Y$ is a morphism to a quasi-affine variety Y, then its composite with an embedding of Y in some affine space $\mathbb{A}^n$ is given by n regular functions on X. So it suffices to prove the special case when $Y = \mathbb{A}^1$. By the previous corollary this image is closed in $\mathbb{A}^1$. But if we think of f as taking its values in $\mathbb{P}^1$ (via the embedding $y \in \mathbb{A}^1 \mapsto [1 : y] \in \mathbb{P}^1$), then we see that $f(X)$ is also closed in $\mathbb{P}^1$. So $f(X)$ cannot be all of $\mathbb{A}^1$. Since X is irreducible, so is the image and it follows that $f(X)$ is a singleton. In other words, f is constant. □

EXERCISE 60. 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 61. Let $F \in k[X_0, \ldots, X_n]_d$ define a nonsingular hypersurface H in $\mathbb{P}^n$. Prove that the map $H \to \check{\mathbb{P}}^n$ which assigns to $p \in H$ the projected tangent space of H at p is given by $[\frac{\partial F}{\partial Z_0} : \cdots : \frac{\partial F}{\partial Z_n}]$. Prove that the image of this map is closed in $\check{\mathbb{P}}^n$ (this image is called *the dual of H*). What can you say in case $d = 2$?

6. The Veronese embeddings

Let be given a positive integer d. We index the monomials in $Z_0, \ldots, Z_n$ that are homogenous of degree d by their exponents: these are the sequences of non-negative integers $\mathbf{k} = (k_0, \ldots, k_n)$ of length $n + 1$ with sum d. They are $\binom{n+d}{d}$ in number.[3] We use this to label the homogeneous coordinates $Z_{\mathbf{k}}$ of $\mathbb{P}^{\binom{n+d}{d}-1}$.

[3] If we expand $\prod_{i=0}^n (1 - tZ_i)^{-1}$, we see that the coefficient of t^d is the sum of the monomials in $Z_0, \ldots, Z_n$ of degree d. So we get the number of such monomials by substituting $Z_i = 1$ for all i: it the

PROPOSITION 6.1 (The Veronese embedding). *The map* $f_d : \mathbb{P}^n \to \mathbb{P}^{\binom{n+d}{d}-1}$ *defined by* $Z_{\mathbf{k}} = T_0^{d_0} \cdots T_n^{d_n}$ *is a closed immersion.*

PROOF. It is enough to show that for every chart domain $U_{\mathbf{k}} := \mathbb{P}^{\binom{n+d}{d}-1}_{Z_{\mathbf{k}}}$ of the standard atlas of the target space, its preimage $f_d^{-1}U_{\mathbf{k}}$ is open in $\mathbb{P}^n$ and is mapped by f_d isomorphically onto a closed subset of $U_{\mathbf{k}}$. This preimage is defined by $T_0^{k_0} \cdots T_n^{k_n} \neq 0$. Let us renumber the coordinates such that $k_0, \ldots, k_r$ are positive and $k_{r+1} = \cdots = k_n = 0$. Then $f_d^{-1}U_{\mathbf{k}} = \mathbb{P}^n_{T_0 \cdots T_r} \subset \mathbb{P}^n_{T_0}$. So if we use the standard coordinates $(t_1, \ldots, t_n)$ to identify $\mathbb{P}^n_{T_0}$ with $\mathbb{A}^n$, then $f_d^{-1}U_{\mathbf{k}}$ is identified with $\mathbb{A}^n_{t_1 \cdots t_r}$.

The coordinates on $U_{\mathbf{k}}$ are the functions $Z_{\mathbf{l}}/Z_{\mathbf{k}}$ with $\mathbf{l} \neq \mathbf{k}$. If we write $z_{\mathbf{l}-\mathbf{k}}$ for this function, then f_d is in terms of these coordinates simply:

$$f_d : \mathbb{A}^n_{t_1 \cdots t_r} \cong f_d^{-1}U_{\mathbf{k}} \to U_{\mathbf{k}}, \quad z_{\mathbf{l}-\mathbf{k}} = t_1^{-k_1} \cdots t_r^{-k_r}.t_1^{l_1} \cdots t_n^{l_n},$$

with $(l_1, \ldots, l_n)$ running over all the n-tuples of nonnegative integers with sum $\leq d$ and distinct from $(k_1, \ldots, k_r, 0, \ldots, 0)$. Among the components of this map are $(t_1 \ldots t_r)^{-1}$ (take $l_i = k_i - 1$ for $i \leq r$ and $l_i = 0$ for $i > r$) and t_i (take $l_i = k_i + 1$ and $l_j = k_j$ for $j \neq i$; this is allowed because then $l_1 + \cdots + l_n = 1 + k_1 + \cdots + k_n \leq k_0 + k_1 + \cdots + k_n = d$). These generate the coordinate ring $k[t_1, \ldots, t_n][1/(t_1 \ldots t_r)]$ of $\mathbb{A}^n_{t_1 \cdots t_r}$ and so f_d defines a closed immersion of $\mathbb{A}^n_{t_1 \cdots t_r}$ in $U_{\mathbf{k}}$. □

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

PROPOSITION 6.2. *Let* $H \subset \mathbb{P}^n$ *be a hypersurface. Then* $\mathbb{P}^n \smallsetminus H$ *is affine and for every closed irreducible subset* $Z \subset \mathbb{P}^n$ *of positive dimension,* $Z \cap H$ *is nonempty and of dimension* $\geq \dim(Z) - 1$*, with equality holding if* Z *is not contained in* H*.*

PROOF. The hypersurface H is given by a homogeneous polynomial of degree d, say by $\sum_{\mathbf{k}} c_{\mathbf{k}} T_0^{k_0} \cdots T_n^{k_n}$. This determines a hyperplane $\tilde{H} \subset \mathbb{P}^{\binom{n+d}{d}-1}$ defined by $\sum_{\mathbf{k}} c_{\mathbf{k}} Z_{\mathbf{k}}$. It is clear that H is the preimage of $\tilde{H}$ under the Veronese morphism and hence the latter identifies $\mathbb{P}^n \smallsetminus H$ with a closed subset of the affine space $\mathbb{P}^{\binom{n+d}{d}-1} \smallsetminus \tilde{H}$. So $\mathbb{P}^n \smallsetminus H$ is affine.

For the rest of the argument we may, by passing to the Veronese embedding, assume that H is a hyperplane. If $\dim(Z \cap H) \leq \dim(Z) - 2$, then by Proposition 4.6 there exists a linear subspace $Q \subset H$ of dimension $\dim(H) - (\dim(Z \cap H) - 1 \leq (n-1) - (\dim(Z) - 2) - 1 = n - \dim(Z)$ which avoids $Z \cap H$. Since this is a linear subspace of $\mathbb{P}^n$ which avoids Z, we thus contradict Corollary 4.4. This proves that $\dim(Z \cap H) \geq \dim(Z) - 1$. If Z is not contained in H, then we have also $\dim(Z \cap H) \leq \dim(Z) - 1$. □

REMARK 6.3. A theorem of Lefschetz asserts that if in the situation of Proposition 6.2 above $\dim Z \geq 2$ (so that $\dim(Z \cap H) \geq 1$), $Z \cap H$ is connected.

EXERCISE 62. Let d be a positive integer. The *universal hypersurface of degree* d is the hypersurface of $\mathbb{P}^n \times \mathbb{P}^{\binom{n+d}{d}-1}$ defined by $F(X, Z) := \sum_{\mathbf{d}} Z_{\mathbf{d}} T_0^{d_0} T_1^{d_1} \cdots T_n^{d_n}$. We denote it by H and let $\pi : H \to \mathbb{P}^{\binom{n+d}{d}-1}$ be the projection. As of item (c) we assume that $d \geq 2$.

---

coefficient of t^d of in $(1-t)^{-(n+1)}$ and hence the value of $1/d!.(d/dt)^d(1-t)^{-(n+1)}$ in $t = 0$, which is $1/d!.(n+1)(n+2)\cdots(n+d) = \binom{n+d}{d}$.

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

7. Grassmannians

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

LEMMA 7.1. *Let $Q \subset P$ be a linear subspace of* codimension $d+1$. *Then the collection $\mathrm{Gr}_d(P)_Q$ of linear d-dimensional subspaces of P contained in $P \smallsetminus Q$ has in a natural manner the structure of an affine space of dimension $(n-d)(d-1)$.*

PROOF. Let Q correspond to the linear subspace $V_Q \subset V$ of dimension $(n+1)-(d+1) = n-d$. Then the elements of $\mathrm{Gr}_d(P)_Q$ correspond to linear subspaces $L \subset V$ that complement V_Q in the sense that $L \oplus V_Q \to V$ is an isomorphism. We claim that the vector space $\mathrm{Hom}(V/V_Q, V_Q)$ acts simply transitively on $\mathrm{Gr}_d(P)_Q$ (so that $\mathrm{Gr}_d(P)_Q$ becomes an affine space with $\mathrm{Hom}(V/V_Q, V_Q)$ as its group of translations). The action is given by letting to $\sigma \in \mathrm{Hom}(V/V_Q, V_Q)$ send L to the graph of the map $L \subset V \to V/V_Q \xrightarrow{\sigma} V_Q$ in $L \oplus V_Q \cong V$. Indeed, any L' with $V \cong L' \oplus V_Q$ is so obtained for a unique σ. □

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

For this we recall that the exterior algebra $\wedge^\bullet V = \oplus_{p \geq 0} \wedge^p V$ is the quotient of the tensor algebra on V, $\oplus_{p=0}^\infty V^{\otimes p}$ (here $V^{\otimes 0} = k$ by convention), by the two-sided ideal generated by the 'squares' $v \otimes v$, $v \in V$. It is customary to denote the product by the symbol $\wedge$. So we can characterize $\wedge^\bullet V$ as a (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 ($\wedge^p V$ is the image of $V^{\otimes p}$) and 'graded-commutative' in the sense that if $\alpha \in \wedge^p V$ and $\beta \in \wedge^q V$, then $\beta \wedge \alpha = (-1)^{pq} \alpha \wedge \beta$. If $(\varepsilon_0, \ldots, \varepsilon_n)$ is a basis for V, then a basis of $\wedge^p V$ is indexed by the p-element subsets $I \subset \{0, \ldots, n\}$: to $I = \{0 \leq i_1 < i_2 < \cdots < i_p \leq n\}$ is associated to the basis element $\varepsilon_I = \varepsilon_{i_1} \wedge \cdots \wedge \varepsilon_{i_p}$ (where the convention is that $\varepsilon_\emptyset = 1 \in k = \wedge^0 V$). So $\dim \wedge^p V = \binom{n+1}{p}$. Notice

that $\wedge^{n+1}V$ is one-dimensional and spanned by $\varepsilon_0 \wedge \cdots \wedge \varepsilon_n$, whereas $\wedge^p V = 0$ for $p > n+1$. We also recall that if V' and V'' are subspaces of V, then the map

$$\wedge^\bullet V' \otimes \wedge^\bullet V'' \to \wedge^\bullet V, \quad \alpha \otimes \beta \mapsto \alpha \wedge \beta,$$

is a linear map of graded vector spaces which is injective (resp. surjective) when this is so in degree 1 (i.e., when $V' \oplus V'' \to V$ is).

We say that $\alpha \in \wedge^p V$ is *fully decomposable* if there exist linearly independent $v_1, \ldots, v_p$ in V such that $\alpha = v_1 \wedge \cdots \wedge v_p$. This is equivalent to the existence of a p-dimensional subspace $K \subset V$ such that α is a generator of $\wedge^p K$.

LEMMA 7.2. *Let $\alpha \in \wedge^p V$ be nonzero. Denote by $K(\alpha)$ the set of $v \in V$ with $v \wedge \alpha = 0$. Then $\dim K(\alpha) \leq p$ and equality holds if and only if α is fully decomposable and spans $\wedge^p K(\alpha)$.*

PROOF. Let $\varepsilon_1, \ldots, \varepsilon_r$ be a basis of $K(\alpha)$ and let $V' \subset V$ be a subspace supplementary to $K(\alpha)$. Then we have a decomposition

$$\wedge^\bullet V = \bigoplus_{I \subset \{1,\ldots,r\}} \varepsilon_I \wedge (\wedge^\bullet V').$$

The kernel of $\varepsilon_i \wedge : \wedge^\bullet V \to \wedge^\bullet V$ is the subsum of the $\varepsilon_I \wedge (\wedge^\bullet V')$ with $i \in I$. It follows that $\alpha \subset \varepsilon_1 \wedge \cdots \wedge \varepsilon_r \wedge (\wedge^{p-r} V')$. In particular, $r \leq p$ with equality holding if and only if α is a multiple of $\varepsilon_1 \wedge \cdots \wedge \varepsilon_p$. □

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 a map $\delta : \mathrm{Gr}_d(P) \to \mathbb{P}(\wedge^{d+1} V)$, $[L] \mapsto [\wedge^{d+1} L]$. It is called the *Plücker embedding* because of:

PROPOSITION 7.3. *The map $\delta : \mathrm{Gr}_d(P) \to \mathbb{P}(\wedge^{d+1} V)$ maps $\mathrm{Gr}_d(P)$ bijectively onto a closed subset of $\mathbb{P}(\wedge^{d+1} V)$.*

PROOF. Let $\alpha \in \wedge^{d+1} V$ be nonzero. According to Lemma 7.2 , $[\alpha]$ 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 $[K(\alpha)]$ as its unique element. In particular, δ is injective.

The subset $K_{d+1}(V, \wedge^{d+2} V) \subset \mathrm{Hom}(V, \wedge^{d+2} V)$ of linear maps whose kernel is of dimension $\geq d+1$ is (after we have chosen a basis for V) the common zero set of a system of homogeneous equations in $\mathrm{Hom}(V, \wedge^{d+2} V)$, namely the $(n+1-d) \times (n+1-d)$-minors of the corresponding matrices. Consider the linear map

$$\sigma : \wedge^{d+1} V \to \mathrm{Hom}(V, \wedge^{d+2} V), \quad \alpha \mapsto (v \mapsto \alpha \wedge v).$$

Since $\sigma^{-1} K_{d+1}(V, \wedge^{d+2} V)$ is given by a set of homogeneous equations it defines a closed subset of $\mathbb{P}(\wedge^{d+1} V)$. This is just the image of δ, for by Lemma 7.2, $\sigma^{-1} K_{d+1}(V, \wedge^{d+2} V) \smallsetminus \{0\}$ is the set of fully decomposable elements of $\wedge^{d+1} V$. □

Proposition 7.3 gives $\mathrm{Gr}_d(P)$ the structure of projective variety. In order to complete the construction, let $Q \subset P$ be a linear subspace of codimension d. Let $V_Q \subset V$ correspond to Q and choose a generator $\beta \in \wedge^{n-d} V_Q$. Then we have a nonzero linear map to the one-dimensional $\wedge^{n+1} V$:

$$e_\beta : \wedge^{d+1} V \to \wedge^{n+1} V, \quad \alpha \mapsto \alpha \wedge \beta.$$

Its kernel is a hyperplane whose complement defines principal open subset of $\mathbb{P}(\wedge^{d+1} V)$ that we shall denote by $\mathbb{P}(\wedge^{d+1} V)_Q$. Such principal open subsets cover

$\mathbb{P}(\wedge^{d+1}V)$ (to see this, choose a basis $(\varepsilon_0,\dots,\varepsilon_n)$ of V and observe that if V_Q runs over the codimension d subspaces of V spanned by basis vectors, then $\mathbb{P}(\wedge^{d+1}V)_Q$ runs over a collection of principal open subsets defined by the basis $(\varepsilon_I)_{|I|=d+1}$ of $\wedge^{d+1}V$).

LEMMA 7.4. *The preimage of $\mathbb{P}(\wedge^{d+1}V)_Q$ under the Plücker embedding δ is the affine space $\mathrm{Gr}_d(P)_Q$ and δ maps this affine space isomorphically onto its image.*

PROOF. Let $V_Q \subset V$ be the linear subspace defining Q and let β be a generator of $\wedge^{n-d}V_Q$ as above. If $\alpha \in \wedge^{d+1}V$ is fully decomposable (and hence generates $\wedge^{d+1}L$ for a unique $(d+1)$-dimensional subspace $L \subset V$), then $L \cap V_Q = \{0\}$ if and only if $\alpha \wedge \beta \neq 0$: if $L \cap V_Q$ contains a nonzero vector v then both α and β are divisible by v and so $\alpha \wedge \beta = 0$ and if $L \cap V_Q = \{0\}$, then we have a decomposition $V \cong L \oplus V$ and so $\alpha \wedge \beta \neq 0$. This implies that $\delta^{-1}\mathbb{P}(\wedge^{d+1}V)_Q = \mathrm{Gr}_d(P)_Q$.

Let us now express the restriction $\delta : \mathrm{Gr}_d(P)_Q \to \mathbb{P}(\wedge^{d+1}V)_Q$ in terms of coordinates. Choose a basis $(\varepsilon_0,\dots,\varepsilon_n)$ for V such that $(\varepsilon_{d+1},\dots,\varepsilon_n)$ is a basis for V_Q and $\beta = \varepsilon_{d+1} \wedge \cdots \wedge \varepsilon_n$. Then e_β simply assigns to an element α of $\wedge^{d+1}V$ the coefficient of $\varepsilon_0 \wedge \cdots \wedge \varepsilon_d$ in α. If $L_0 \subset V$ denotes the span of $\varepsilon_0,\dots,\varepsilon_d$, then $\mathrm{Gr}_d(P)_Q$ is identified with the affine space $\mathrm{Hom}(L_0, V_Q) \cong \mathbb{A}^{(d+1)\times(n-d)}$ of $(d+1)\times(n-d)$-matrices via

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

so that δ is given by

$$(a_i^j)_{0\le i\le d<j\le n} \mapsto (\varepsilon_0 + \textstyle\sum_{j=d+1}^n a_0^j\varepsilon_j) \wedge \cdots \wedge (e_d + \sum_{j=d+1}^n a_d^j\varepsilon_j).$$

The coefficient of $\varepsilon_{i_0} \wedge \cdots \wedge \varepsilon_{i_d}$ is a determinant of which each 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, for a_i^j appears up to sign as the coefficient of $\varepsilon_0 \wedge \cdots \wedge \widehat{\varepsilon_i} \wedge \cdots \wedge \varepsilon_d \wedge \varepsilon_j$. Since these generate the coordinate ring of $\mathbb{A}^{(d+1)\times(n-d)}$, it follows that δ defines a closed immersion of $\mathrm{Gr}_d(P)_Q$ in $\mathbb{P}(\wedge^{d+1}V)_Q$. □

COROLLARY 7.5. *The Plücker embedding realizes $\mathrm{Gr}_d(P)$ as a nonsingular irreducible subvariety of $\mathbb{P}(\wedge^{d+1}V)$ of dimension $(n-d)(d+1)$. This structure makes each subset $\mathrm{Gr}_d(P)_Q$ open and isomorphic to affine $(n-d)(d+1)$-space in a way that is compatible with the one obtained in Lemma 7.1.*

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

REMARK 7.6. The image of $\mathrm{Gr}_d(P)$ is a closed orbit of the natural $\mathrm{SL}(V)$-action on $\mathbb{P}(\wedge^{d+1}V)$. It lies in the closure of any other $\mathrm{SL}(V)$-orbit.

EXERCISE 63. Let V be a finite dimensional k-vector space. For every linear subspace $W \subset V$ we identify $(V/W)^*$ with the subspace of V^* of linear forms on V that are zero on W. Prove that for every $0 \le r \le \dim V$ the resulting map $\mathrm{Gr}_r(V) \to \mathrm{Gr}_{\dim V - r}(V^*)$ is an isomorphism of projective varieties.

EXERCISE 64. Let V and W be finite dimensional k-vector spaces and let r be a nonnegative integer $\le \min\{\dim V, \dim W\}$.

(a) Prove that the subset $\mathrm{Hom}_r(V,W) \subset \mathrm{Hom}(V,W)$ of linear maps of rank r is a (locally closed) subvariety of $\mathrm{Hom}(V,W)$.
(b) Prove that the map $\mathrm{Hom}_r(V,W) \to \mathrm{Gr}_{\dim V - r}(V)$ resp. $\mathrm{Hom}_r(V,W) \to \mathrm{Gr}_r(W)$ which assigns to $\phi \in \mathrm{Hom}_r(V,W)$ its kernel resp. image is a morphism.
(c) Prove that the resulting morphism $\mathrm{Hom}_r(V,W) \to \mathrm{Gr}_{\dim V - r}(V) \times \mathrm{Gr}_r(W)$ is trivial over any product of principal open subsets with fiber the general linear group $\mathrm{GL}_r(k)$. Conclude that $\mathrm{Hom}_r(V,W)$ is nonsingular of codimension $(\dim V - r)(\dim W - r)$.

The Grassmannian of hyperplanes in a projective space is itself a projective space (see Exercise 60). 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 $\wedge^2 V$ we have a homogeneous polynomial $F : \wedge^2 V \to k$ of degree two defined by

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

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

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

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

PROPOSITION 7.7. *The image of the Plücker embedding of $G_1(\mathbb{P}(V))$ in $\mathbb{P}(\wedge^2 V)$ is the zero set of F.*

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

If the characteristic of k is not 2, then the nonsingular quadric hypersurfaces of the same dimension are isomorphic to one another and so this proposition shows that any nonsingular quadric hypersurface of dimension 4 is isomorphic to the Grassmannian of lines in a three dimensional projective space.

REMARK 7.8. The image of the Plücker embedding $\mathrm{Gr}_d(P) \hookrightarrow \mathbb{P}(\wedge^{d+1} V)$ is in fact always the common zero set of a collection of quadratic equations, called the *Plücker relations*. To exhibit these, we first recall that every $\phi \in V^*$ defines a linear 'inner contraction' map $\iota_\phi : \wedge^\bullet V \to \wedge^\bullet V$ of degree -1 characterized by the fact that for $v \in V$, $\iota_\phi(v) = \phi(v) \in k = \wedge^0 V$ and for $\alpha \in \wedge^p V, \beta \in \wedge^\bullet V$, $\iota_\phi(\alpha \wedge \beta) = \iota_\phi(\alpha) \wedge \beta + (-1)^p \alpha \wedge \iota_\phi(\beta)$. Under the natural isomorphism $\mathrm{End}(V,V) \cong V \otimes V^*$, the identity of V defines a tensor in $V \otimes V^*$. The wedge-contraction with this tensor defines a linear map $B_V : \wedge^\bullet V \otimes \wedge^\bullet V \to \wedge^\bullet V \otimes \wedge^\bullet V$ of bidegree $(1,-1)$. Concretely, if $(e_0, \ldots, e_n)$ is a basis of V and $(e_0^*, \ldots, e_n^*)$ is the basis of V^* dual to $(e_0, \ldots, e_n)$, then

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

Notice that if $W \subset V$ is a subspace, then B_W is just the restriction of B_V to $\wedge^\bullet W \otimes \wedge^\bullet W$. So if $\alpha \in \wedge^{d+1}V$ is fully decomposable so that $\alpha \in \wedge^{d+1}L$ for some $(d+1)$-dimensional subspace $L \subset V$, then $B_V(\alpha \otimes \alpha) = B_L(\alpha \otimes \alpha) = 0$. This is the *universal Plücker relation*.

Conversely, any nonzero $\alpha \in \wedge^{d+1}V$ for which $B_V(\alpha \otimes \alpha) = 0$ is fully decomposable. The proof proceeds with induction on n. For $n = 0$ there is nothing to show. Assume $n \geq 1$, let $e \in V$ be nonzero and let $V' \subset V$ be a hyperplane not containing e. If we write $\alpha = \alpha' + e \wedge \alpha''$ with $\alpha', \alpha'' \in \wedge^\bullet V'$, then the component of $B(\alpha \otimes \alpha)$ in $\wedge^\bullet V' \otimes \wedge^\bullet V'$ is $B_{V'}(\alpha' \otimes \alpha')$ and so α' is zero or fully decomposable by our induction hypothesis: there exists a subspace $L' \subset V'$ of dimension $d+1$ such that $\alpha' \in \wedge^{d+1}L'$. Then the vanishing of the component of $B(\alpha \otimes \alpha)$ in $\wedge^\bullet V' \otimes e \wedge (\wedge^\bullet V')$ is seen to imply that $\iota_\phi \alpha'' = 0$ for all $\phi \in (V'/L')^* \subset V'^*$. This means that $\alpha'' \in \wedge^d L'$. So if we put $M := ke + L'$, then $\dim M = d+2$ and $\alpha \in \wedge^{d+1}M$. But then $\alpha \in \iota_\phi \wedge^{d+2} M$ for some nonzero $\phi \in M^*$. Then α is a generator of $\wedge^{d+1} \operatorname{Ker}(\phi)$ and hence fully decomposable.

Let us rephrase this in terms of algebraic geometry: every nonzero linear form ℓ on $\wedge^{d+2}V \otimes \wedge^d V$, determines a quadratic form Q_ℓ on $\wedge^{d+1}V$ defined by $\alpha \mapsto \ell(B(\alpha, \alpha))$ whose zero set is a quadratic hypersurface in $\mathbb{P}(\wedge^{d+1}V)$. This hypersurface contains the Plücker locus and the latter is in fact the common zero set of the Q_ℓ, with ℓ running over the linear forms on $\wedge^{d+2}V \otimes \wedge^d V$. It can be shown that the Q_ℓ generate the full graded ideal defined by the Plücker locus. The quadratic forms Q_ℓ are called the Plücker relations.[4]

8. Fano varieties and the Gauß map

The Fano variety of a projective variety is defined in the following proposition.

PROPOSITION-DEFINITION 8.1. *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 $\operatorname{Gr}_d(P)$, called the* Fano variety *(of d-planes) of X.*

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

Choose homogeneous coordinates $[T_0 : \cdots : T_n]$ such that L resp. W is given by $T_{d+1} = \cdots = T_n = 0$ resp. $T_0 = \cdots T_d = 0$. A linear map $A \in \operatorname{Hom}(L, W)$ is then given by $A^*T_{d+i} = \sum_{j=0}^d a_i^j T_j$, $i = 1, \ldots, n-d$. It defines an element of $F_d(X)$ if and only for all $G \in \cup_{m \geq 0} I_m(X)$, $G(T_0, \ldots, T_d, A^*T_{d+1}, \ldots A^*T_n)$ is identically zero. This means that the coefficient of every monomial $T_0^{m_0} \cdots T_d^{m_d}$ in such an expression much vanish. Since this coefficient is a polynomial in the matrix coefficients a_i^j of A, we find that the preimage of $F_d(X)$ in $\operatorname{Hom}(L, W)$ is the common zero set of a set of polynomials and hence is closed therein. □

EXAMPLE 8.2. Consider the case of a quadratic hypersurface $X \subset \mathbb{P}(V)$ and assume for simplicity that $\operatorname{char}(k) \neq 2$. So X can be given by a nonzero quadratic form $F \in k[V]_2$. With F is associated a symmetric bilinear form $B : V \times V \to k$ defined by $B(v, v') = F(v+v') - F(v) - F(v')$ so that $B(v, v) = 2F(v)$ (so nonzero, because $\operatorname{char}(k) \neq 2$). Let us assume that X is nonsingular. This means that the partial derivatives of F have no common zero in $\mathbb{P}(V)$. This translates into: $B : V \times V \to k$ is nonsingular, that is, the linear map $b : v \in V \mapsto B(\text{-}, v) \in V^*$ is an isomorphism of vector spaces (here we use that $\operatorname{char}(k) \neq 2$). A subspace

[4] These show up in the algebro-analytic setting of the Sato Grassmannian (for which both d and $n - d$ are infinity) and are then known as the *Hirota bilinear relations*.

$L \subset V$ 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. It not difficult to show that we can find coordinates $(T_0, \cdots, T_n)$ such that $F = \frac{1}{2}\sum_{i=0}^{n} T_i T_{n-i}$ so that the matrix of B is the unit antidiagonal. If for instance $\dim X = n-1$ is even, say $2m$, then let L resp. L' be the linear subspace defined by $T_{m+1} = \cdots = T_{2m+1} = 0$ resp. $T_0 = \cdots = T_m = 0$, so that $V = L \oplus L'$. Notice that both $[L]$ and $[L']$ are in $F_m(X)$. The vector space $\mathrm{Hom}(L, L')$ describes an affine open subset of the Grassmannian of m-planes in $\mathbb{P}(V)$. An element $A \in \mathrm{Hom}(L, L')$ is given by $A^* T_{n-i} = \sum_{j=0}^{m} a_{ij} T_j$, $i = 0, \ldots, m$. The corresponding m-plane is contained in X precisely when $\sum_{i,j=0}^{m} a_{ij} T_i T_j$ 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 $\frac{1}{2}m(m+1)$. In particular, $F_m(X)$ is nonsingular.

EXERCISE 65. Let X be a quadratic hypersurface $\mathbb{P}(V)$ of odd dimension $2m+1$ and assume for simplicity that $\mathrm{char}(k) \neq 2$. Prove that $F_{m+1}(X) = \emptyset$ and that $F_m(X) \neq \emptyset$. Prove that $F_m(X)$ is a nonsingular variety and determine its dimension.

EXERCISE 66. Let $X \subset \mathbb{P}^n$ be a hypersurface of degree d and let $0 \leq m \leq n$. Prove that the intersection of $F_m(X)$ with a standard affine subset of $\mathrm{Gr}_m(\mathbb{P}^n)$ is given by $\binom{m+d}{d}$ equations.

EXERCISE 67. Consider the universal hypersurface of degree d in $\mathbb{P}^n$, $H \subset \mathbb{P}^n \times \mathbb{P}^{\binom{n+d}{d}-1}$.

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

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

(c) Prove that the family of m-planes contained in a generic hypersurface of degree d in $\mathbb{P}^n$ is of dimension $(m+1)(n-m) - \binom{m+d}{d}$ or empty. In particular, this is a finite set when $(m+1)(n-m) = \binom{m+d}{d}$.[5]

Let $P = \mathbb{P}(V)$ be as before and let X be an irreducible closed subset of P of dimension d. For every nonsingular point $p \in X$, there is precisely one d-dimensional linear subspace $\hat{T}(X,p)$ of P which contains p and has the same tangent space at p as X. In other words, it is characterized by the property that the ideals in $\mathcal{O}_{P,p}$ defining X resp. $\hat{T}(X,p)$ have the same image in $\mathcal{O}_{P,p}/\mathfrak{m}_{P,p}^2$.

PROPOSITION-DEFINITION 8.3. *For every $p \in X_{\mathrm{reg}}$, $\hat{T}(X,p)$ is the common zero set of the linear forms defined by the differentials of the homogeneous elements of*

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

$I(X)$ evaluated in some representative of p in $V \smallsetminus \{0\}$. This defines a morphism $X_{\mathrm{reg}} \to \mathrm{Gr}_d(P)$, called the Gauß map.[6]

PROOF. If $F \in I(X)$ and $G \in k[V]$ are homogeneous of the same degree m say, with $p \in X_G$, then $\phi := F/G$ is a regular function on P_G which vanishes on X_G. The kernel of the linear form $d\phi(p) : T_pP \to k$ contains the tangent space $T_p(X)$. As such ϕ generate the ideal defining X at p, $T_p(X)$ is the intersection of such kernels.

We have on V_G the identity of differentials $d(F/G) = G^{-1}dF - G^{-2}FdG$. We interpret such a differential as a morphism from $V_G \to V^*$ (the differential at a point of V is regarded as a linear form on V). Note that if $\tilde{p} \in \mathrm{Cone}(X)_G$ lies over p, then its value in any $\tilde{p} \in \mathrm{Cone}(X)_G$ is $G^{-1}(\tilde{p})dF(\tilde{p}) \in V^*$. The kernel of this linear form is that of $dF(\tilde{p}) \in V^*$ and since $dF(t\tilde{p}) = t^m dF(\tilde{p})$, this kernel depends only on p. It follows that $\hat{T}(X,p)$ is the linear subspace defined by the kernels of the linear forms $dF(\tilde{p})$, where F runs over $\cup_{m\geq 1} I(X)_m$, and that this is also the projectivized tangent space of $\mathrm{Cone}(X)$ at $\tilde{p}$.

Theorem 10.14 of Ch. 1 tells us that we can choose $F_1, \ldots, F_{n-d} \in I(X)$ and $G \in k[V]$ such that $\tilde{p} \in \mathrm{Cone}(X)_G \subset \mathrm{Cone}(X)_{\mathrm{reg}}$ and $F_1, \ldots, F_{n-d}$ generate the ideal defining $\mathrm{Cone}(X)_G$ in V_G such that for every $\tilde{q} \in \mathrm{Cone}(X)_G$, the tangent space of $\mathrm{Cone}(X)_G$ at $\tilde{q}$ is $\cap_{i=1}^{n-d} \mathrm{Ker}(dF_i(\tilde{q}))$. We may (and will) assume that G is homogeneous. Now $dF_1 \wedge \cdots \wedge dF_{n-d}$ defines a morphism $V_G \to \wedge^{n-d}V^*$ whose image clearly consists of nonzero fully decomposable elements. In other words, it defines a morphism $V_G \to \mathrm{Gr}_{n-d}(V^*)$. Via the identification $\mathrm{Gr}_{n-d}(V^*) \cong \mathrm{Gr}_{d+1}(V) = \mathrm{Gr}_d(P)$ we regard this as a morphism taking values in $\mathrm{Gr}_d(P)$. Its restriction to $\mathrm{Cone}(X)_G$ is then just the map which assigns to $\tilde{q}$ the space $\hat{T}(X,q)$, in other words, factors through the Gauß map $X_G \to \mathrm{Gr}_d(P)$. Since $\mathrm{Cone}(X)_G \to \mathrm{Gr}_d(P)$ is a morphism, so will be the induced map $X_G \to \mathrm{Gr}_d(P)$ (why?). Hence the Gauß map is a morphism. □

REMARK 8.4. The closure of the graph of the Gauss map in $X \times \mathrm{Gr}_d(P)$ is called the *Nash blowup* of X. Its projection to X is clearly an isomorphism over the open-dense subset X_{reg} and hence birational. A remarkable property of the Nash blowup is that the Zariski tangent space of each of its points contains a distinguished d-dimensional subspace (prescribed by the second projection to $\mathrm{Gr}_d(P)$) in such a manner that these subspaces extend the tangent bundle of X_{reg} in a regular manner.

9. Multiplicities of modules

Bézout's theorem asserts that two distinct irreducible curves C, C' in $\mathbb{P}^2$ of degrees d and d' intersect in dd' points. Strictly speaking this is only true if C and C' intersect as nicely as possible, but the theorem is true as stated if we count each point of intersection with an appropriate multiplicity. There is in fact a generalization: the common intersection of n hypersurfaces in $\mathbb{P}^n$ has cardinality the product of the degrees of these hypersurfaces, provided that this intersection is finite and each point of intersection is counted with an appropriate multiplicity. One of our aims is to define these multiplicities. The tools from commutative algebra that we use for this have an interest in their own right.

[6]Thus named because it is related to the map that Gauß studied for an oriented surface Σ in Euclidian 3-space $\mathbb{E}^3$: it is then the map $\Sigma \to \mathbb{S}^2$ which assigns to $p \in \Sigma$ the unit outward normal vector of Σ at p.

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

EXERCISE 68. Suppose R is a noetherian local ring with maximal ideal $\mathfrak{m}$ and residue field K. Prove that the length of a finitely generated R-module M is finite precisely when $\mathfrak{m}^d M = 0$ for some d and is then equal to $\sum_{i=0}^{d-1} \dim_K(\mathfrak{m}^i M/\mathfrak{m}^{i+1}M)$.

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

In the remainder of this section R is a noetherian ring R and M a finitely generated (and hence noetherian) R-module.

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

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

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

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

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

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

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

DEFINITION 9.3. The *multiplicity* of M at a prime ideal $\mathfrak{p}$ of R, denoted $\mu_\mathfrak{p}(M)$, is the length of $M_\mathfrak{p}$ as an $R_\mathfrak{p}$-module.

In an algebro-geometric context we may modify this notation accordingly. For instance, if we are given an affine variety X and an irreducible subvariety Y, then we may write $\mu_Y(\text{-})$ for $\mu_\mathfrak{p}(\text{-})$, where it is understood that $R = k[X]$ and $\mathfrak{p} = I(Y)$.

REMARK 9.4. Let X be a variety, $x \in X$ and $\mathcal{I} \subset \mathcal{O}_{X,x}$ an ideal with $\sqrt{\mathcal{I}} = \mathfrak{m}_{X,x}$. So $\mathfrak{m}_{X,x}^r \subset \mathcal{I} \subset \mathfrak{m}_{X,x}$ for some positive integer r. Then $\dim_k(\mathcal{O}_{X,x}/\mathcal{I})$ is finite (since $\dim_k(\mathcal{O}_{X,x}/\mathfrak{m}_{X,x}^r)$ is) and according to Exercise 68 equal to the length of $\mathcal{O}_{X,x}/\mathcal{I}$ as an $\mathcal{O}_{X,x}$-module and hence the multiplicity of $\mathcal{O}_{X,x}/\mathcal{I}$ at the maximal ideal $\mathfrak{m}_{X,x}$. In agreement with our convention, we will denote this multiplicity by $\mu_x(\mathcal{O}_{X,x}/\mathcal{I})$. If X is affine and we are given an ideal $I \subset k[X]$ whose image in $\mathcal{O}_{X,x}$ is $\mathcal{I}$, then $\mathcal{O}_{X,x}/\mathcal{I}$ is the localization of $k[X]/I$ at x and so $\mu_x(k[X]/I) = \mu_x(\mathcal{O}_{X,x}/\mathcal{I}) = \dim_k(\mathcal{O}_{X,x}/\mathcal{I})$. Note that x is then an isolated point of $Z(I)$.

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

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

CONVENTION 9.5. Given an integer l and a graded module M over a graded ring, 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 $R/\mathfrak{p}$ ($(R/\mathfrak{p})[l]$), for some (homogeneous) prime ideal $\mathfrak{p}$ (and some $l \in \mathbb{Z}$).

Given a (graded) R-module M, then every $m \in M$ ($m \in M_l$) defines a homomorphism or R-modules $r \in R \mapsto rm \in M$. Its kernel is a (graded) ideal of R, the annihilator $\mathrm{Ann}(m)$ of m, so that M contains a copy $R/\mathrm{Ann}(m)$ ($R/\mathrm{Ann}(m)[l]$) as a (graded submodule).

LEMMA 9.6. *Let M be a finitely generated nonzero (graded) R-module. Then the collection of annihilators of nonzero (homogeneous) elements of M contains a maximal element and any such maximal element is a (homogeneous) prime ideal of R. In particular, M contains an elementary (graded) submodule.*

PROOF. We only do the graded case. The first assertion follows from the noetherian property of R. Let now $\mathrm{Ann}(m)$ be a maximal element of the collection (so with $m \in M$ homogeneous and nonzero). It suffices to show that this is a prime ideal in the graded sense (see Exercise 55), i.e., to show that if $a, b \in R$ are homogeneous and $ab \in \mathrm{Ann}(m)$, but $b \notin \mathrm{Ann}(m)$, then $a \in \mathrm{Ann}(m)$. So $bm \neq 0$ and $a \in \mathrm{Ann}(bm)$. Since $\mathrm{Ann}(bm) \supset \mathrm{Ann}(m)$, the maximality property of the latter implies that this must be an equality: $\mathrm{Ann}(bm) = \mathrm{Ann}(m)$, and so $a \in \mathrm{Ann}(m)$. □

PROPOSITION 9.7. *Every finitely generated (graded) R-module M can be obtained as a successive extension of elementary modules in the sense that there exists a finite filtration by (graded) R-submodules $M = M^0 \supsetneq M^1 \supsetneq \cdots \supsetneq M^d = \{0\}$ such that each quotient M^{i-1}/M^i, $i = 1, \ldots, d$, is elementary.*

PROOF. We do the graded case only. Since M is noetherian, the collection of graded submodules of M that can be written as a successive extension of elementary modules has a maximal member, M', say. We claim that $M' = M$. If M/M' were nonzero, then according to Lemma 9.6, 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. □

Recall that the *annihilator* of M, $\mathrm{Ann}(M)$, is the set of $r \in R$ with $rM = 0$. It is clearly an ideal of R. We denote by $\mathcal{P}(M)$ the set of prime ideals of R which contain $\mathrm{Ann}(M)$ and are minimal for that property. According to Exercise 14 these are finite in number and their common intersection equals $\sqrt{\mathrm{Ann}(M)}$ (recall that here R is noetherian). In the graded setting, $\mathrm{Ann}(M)$ is a graded ideal and then according to Lemma 2.3 the members of $\mathcal{P}(M)$ are all graded.

PROPOSITION 9.8. *In the situation of the preceding proposition, let $\mathfrak{p}^{(i)}$ be the prime ideal of R such that $M^{i-1}/M^i \cong R/\mathfrak{p}^{(i)}$. Then $\mathcal{P}(M)$ is the set of minimal members of the collection $\{\mathfrak{p}^{(i)}\}_{i=1}^d$ and for every $\mathfrak{p} \in \mathcal{P}(M)$, $\mu_{\mathfrak{p}}(M)$ is finite and $\mathfrak{p}$ occurs precisely $\mu_{\mathfrak{p}}(M)$ times in the sequence $(\mathfrak{p}^{(1)}, \dots, \mathfrak{p}^{(d)})$.*

PROOF. We first show that $\sqrt{\mathrm{Ann}(M)} = \mathfrak{p}^{(1)} \cap \cdots \cap \mathfrak{p}^{(d)}$. If $r \in \mathfrak{p}^{(1)} \cap \cdots \cap \mathfrak{p}^{(d)}$, then r maps M^{i-1} to M^i and so $r^d \in \mathrm{Ann}(M)$ and hence $r \in \sqrt{\mathrm{Ann}(M)}$. Conversely, if $r \in R$ and $l \geq 1$ are such that $r^l \in \mathrm{Ann}(M)$, then for all i, $r^l \in \mathfrak{p}^{(i)}$ and hence $r \in \mathfrak{p}^{(i)}$. Since every prime ideal containing $\sqrt{\mathrm{Ann}(M)} = \mathfrak{p}^{(1)} \cap \cdots \cap \mathfrak{p}^{(d)}$ contains some $\mathfrak{p}^{(i)}$ it also follows that $\mathcal{P}(M)$ is the collection of minimal members of $\{\mathfrak{p}^{(i)}\}_{i=1}^d$.

Fix $\mathfrak{p} \in \mathcal{P}(M)$. We then have a filtration $M_{\mathfrak{p}} = M_{\mathfrak{p}}^0 \supset \cdots \supset M_{\mathfrak{p}}^d = \{0\}$ (for an inclusion of R-modules induces an inclusion of $R_{\mathfrak{p}}$-modules). We have $M_{\mathfrak{p}}^{i-1}/M_{\mathfrak{p}}^i \cong R_{\mathfrak{p}}/\mathfrak{p}^{(i)}R_{\mathfrak{p}}$. Either $\mathfrak{p}^{(i)} = \mathfrak{p}$, and then the latter is equal to the residue field $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ and hence of length 1. Or $\mathfrak{p}^{(i)} \neq \mathfrak{p}$, and then we cannot have $\mathfrak{p}^{(i)} \subset \mathfrak{p}$ by the minimality of $\mathfrak{p}$. So there exists an $r \in \mathfrak{p}^{(i)} \smallsetminus \mathfrak{p}$. This means that $r/1 \in \mathfrak{p}^{(i)}R_{\mathfrak{p}}$ is invertible so that $\mathfrak{p}^{(i)}R_{\mathfrak{p}} = R_{\mathfrak{p}}$, or equivalently $M_{\mathfrak{p}}^{i-1}/M_{\mathfrak{p}}^i = 0$. Following our definition the first case occurs precisely $\mu_{\mathfrak{p}}(M)$ times. □

We can of course pass from the graded case to the nongraded case by just forgetting the grading. But more interesting is the following construction, which we shall use to pass from a projective setting to an affine one and vice versa.

Let $\mathfrak{p} \subset R$ be a homogeneous prime ideal and let us write $\mathfrak{m}_{\mathfrak{p}}$ for the maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$ of the ring $R_{\mathfrak{p}}$. Given $l \in \mathbb{Z}$, let $R_{\mathfrak{p},l}$ denote the set of $R_{\mathfrak{p}}$ that are representable as r/s with $r \in R_{i+l}$ and $s \in R_i \smallsetminus \mathfrak{p}_i$ for some i and put $R_{\mathfrak{p},\bullet} := \oplus_{l\in\mathbb{Z}} R_{\mathfrak{p},l}$. Note that $R_{\mathfrak{p},0} \subset R_{\mathfrak{p},\bullet} \subset R_{\mathfrak{p}}$ are ring inclusions of which $R_{\mathfrak{p},0}$ and $R_{\mathfrak{p}}$ are local rings (the maximal ideal $\mathfrak{m}_{\mathfrak{p},0}$ of $R_{\mathfrak{p},0}$ is obtained by taking in the previous sentence $r \in \mathfrak{p}_i$), but $R_{\mathfrak{p},\bullet}$ has maximal ideals other than $\mathfrak{m}_{\mathfrak{p}} \cap R_{\mathfrak{p},\bullet}$ (see below).

Suppose now that $\mathfrak{p}_1 \neq R_1$ and choose $s \in R_1 \smallsetminus \mathfrak{p}_1$ so that $1/s \in R_{\mathfrak{p},-1}$. Then multiplication with s^l defines an $R_{\mathfrak{p},0}$-module isomorphism of $R_{\mathfrak{p},0} \cong R_{\mathfrak{p},l}$ (the inverse is given by multiplication with s^{-l}). So $R_{\mathfrak{p},\bullet}$ is the ring of Laurent polynomials $R_{\mathfrak{p},0}[s, s^{-1}]$ with $\mathfrak{m}_{\mathfrak{p}} \cap R_{\mathfrak{p},\bullet}$ corresponding to $\mathfrak{m}_{\mathfrak{p},0}[s, s^{-1}]$. So we have $R_{\mathfrak{p},0}/\mathfrak{m}_{\mathfrak{p},0}[s, s^{-1}] \cong R_{\mathfrak{p},\bullet}/\mathfrak{m}_{\mathfrak{p}} \cap R_{\mathfrak{p},\bullet})$. But $R_{\mathfrak{p},\bullet}/(\mathfrak{m}_{\mathfrak{p}} \cap R_{\mathfrak{p},\bullet})$ is a subring of the residue field $R_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}$ and generates the latter as a field. It follows that $R_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}} \cong R_{\mathfrak{p},0}/\mathfrak{m}_{\mathfrak{p},0}(s)$ is a purely transcendental field extension of $R_{\mathfrak{p},0}/\mathfrak{m}_{\mathfrak{p},0}$.

This also makes sense for any graded R-module M: $M_{\mathfrak{p},l}$ is the set of fractions m/s with $m \in M_{i+l}$ and $s \in R_i \smallsetminus \mathfrak{p}_i$ for some i. Note that this is a $R_{\mathfrak{p},0}$-module.

COROLLARY 9.9. *If M is noetherian, then $\mu_{\mathfrak{p}}(M) = \mu_{\mathfrak{m}_{\mathfrak{p},0}}(M_{\mathfrak{p},0})$.*

PROOF. An iterated extension $M = M^0 \supsetneq M^1 \supsetneq \cdots \supsetneq M^d = \{0\}$ of M by elementary graded R-modules yields an iterated extension of $M_{\mathfrak{p}}$ resp. $M_{\mathfrak{p},0}$ by trivial or by elementary $R_{\mathfrak{p}}$ resp. $R_{\mathfrak{p},0}$-modules. The corollary then follows from the observation that a successive quotient $M_{\mathfrak{p}}^{i-1}/M_{\mathfrak{p}}^i$ is nonzero (which is then isomorphic to the big residue field $R_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}$) if and only $M_{\mathfrak{p},0}^{i-1}/M_{\mathfrak{p},0}^i$ is (which is then isomorphic to the small residue field $R_{\mathfrak{p},0}/\mathfrak{m}_{\mathfrak{p},0}$). □

We use this observation mainly via the following example.

EXAMPLE 9.10. Let V be a vector space of dimension $n+1$, $J \subset k[V]$ a homogeneous ideal and $p \in \mathbb{P}(V)$ an isolated point of the closed subset $Z[J] \subset \mathbb{P}(V)$

defined by J. We take here $M := k[V]/J$ and take for $\mathfrak{p}$ the graded ideal $I_p \subset k[V]$ defining p. Then $k[V]_{I_p,0}$ can be identified with the local k-algebra $\mathcal{O}_{\mathbb{P}(V),p}$. If $\mathcal{J}_p \subset \mathcal{O}_{\mathbb{P}(V),p}$ denotes the ideal corresponding to $J_{I_p,0} \subset k[V]_{I_p,0}$, then $\sqrt{\mathcal{J}_p} = \mathfrak{m}_{\mathbb{P}(V),p}$ and we can identify $M_{I_p,0}$ with $\mathcal{O}_{\mathbb{P}(V),p}/\mathcal{J}_p$. According to the above discussion $\mu_{I_p}(M) = \mu_p(k[V]_{I_p,0}/J_{I_p,0})$ and by Exercise 68 this is just $\dim_k(\mathcal{O}_{\mathbb{P}(V),p}/\mathcal{J}_p)$.

10. Hilbert functions and Hilbert polynomials

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

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

It has the property that its value in *any* integer i is an integer, for $i \geq n$ this is an ordinary binomial coefficient and hence an integer, for $i \leq -1$ this is so up to sign, for then we get $(-1)^n\binom{n-1-i}{n}$ and for $0 \leq i \leq n-1$ it is 0.

Let $\Delta : \mathbb{Q}[z] \to \mathbb{Q}[z]$ denote the difference operator: $\Delta f(z) := f(z+1) - f(z)$. This is a $\mathbb{Q}$-linear map with kernel $\mathbb{Q}$ and has the property that it decreases the degree of nonconstant polynomials. It clearly sends numerical polynomials to numerical polynomials and a simple verification shows that it maps $\binom{z}{n+1}$ to $\binom{z}{n}$.

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

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

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

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

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

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

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

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

In the remainder of this section V is a k-vector space of dimension $n+1$ (we allow $n=-1$). We equip $k[V]$ with the usual grading (for which each linear form on V has degree one) and view it as the homogeneneous coordinate ring of $\mathbb{P}(V)$. A $k[V]$-module is always assumed to be graded and finitely generated.

Let M be a graded finitely generated $k[V]$-module. Then for every $i \in \mathbb{Z}$, M_i is a finite dimensional k-vector space and so we may define the *Hilbert function* of M, $\phi_M : \mathbb{Z} \to \mathbb{Z}$, by $\phi_M(i) := \dim_k M_i$. For example, the Hilbert function of $k[V]$ itself is $i \mapsto \binom{i+n}{n}$ and so is given by a numerical polynomial of degree n.

The graded ideal $\mathrm{Ann}(M)$ defines a closed subset of $\mathbb{P}(V)$ that is called the *(projective) support* of M and denoted $\mathrm{supp}(M)$.

THEOREM 10.3 (Hilbert-Serre). *Let M be a graded finitely generated $k[V]$-module. Then there exists a unique numerical polynomial $P_M \in \mathbb{Q}[z]$, the* Hilbert polynomial *of M, such that $\phi_M(i) = P_M(i)$ for i sufficiently large. The degree of P_M is equal to $\dim \mathrm{supp}(M)$ if we agree that the zero polynomial has the same degree as the dimension of the empty set (namely -1).*

PROOF. When $V = \{0\}$, then $M = 0$ and there is nothing to show. So assume $\dim V > 0$ and the theorem proved for vector spaces of dimension $< \dim V$.

If N is a graded submodule of M, then $\mathrm{Ann}(N) \cap \mathrm{Ann}(M/N)$ has the same radical as $\mathrm{Ann}(M)$ (in fact, $\mathrm{Ann}(M) \supset \mathrm{Ann}(N) \cap \mathrm{Ann}(M/N) \supset \mathrm{Ann}(M)^2$) and so $\mathrm{supp}(M) = \mathrm{supp}(N) \cup \mathrm{supp}(M/N)$. It is clear that $\dim_k M_i = \dim_k N_i + \dim_k(M_i/N_i)$ and so 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 $M = A[l]$, where $A = k[V]/\mathfrak{p}$ with $\mathfrak{p}$ a graded prime ideal. But $\phi_{(A[l])}(i) = \phi_A(i+l)$ and since the degree of a polynomial does not change after the substitution $z \mapsto z+l$, it is even enough to do the case A.

Then $\mathrm{supp}(A) = Z[\mathfrak{p}]$ is the closed irreducible subset of $\mathbb{P}(V)$ defined by the graded ideal $\mathfrak{p}$. In case $\mathfrak{p} = k[V]_+$, the theorem holds trivially: we have $\dim_k A_i = 0$ for $i > 0$ (so that we may take P_A to be identically zero) and $\mathrm{supp}(A) = \emptyset$. Suppose therefore that $\mathfrak{p} \neq k[V]_+$, so that there exists a $T \in k[V]_1 = V^*$ that is not in $\mathfrak{p}_1$. Denote by $V' \subset V$ its zero hyperplane. Since $k[V]/\mathfrak{p}$ is a domain, multiplication by T induces an injection $A \to A$ (increasing the degree by one) with cokernel $A' := A/TA$ and so $\phi_{A'}(i) = \phi_A(i) - \phi_A(i-1) = \Delta\phi_A(i-1)$. Since $\mathrm{Ann}(A') = \mathfrak{p} + (T)$, we have $\mathrm{supp}(A') = \mathrm{supp}(A) \cap \mathbb{P}(V')$. According to Proposition 6.2 we then have $\dim \mathrm{supp}(A') = \dim \mathrm{supp}(A) - 1$. Since A' is a quotient of $k[V']$, our induction hypothesis tells us that there exists a polynomial $P_{A'}$ of degree $\dim \mathrm{supp}(A')$ such that $\phi_{A'}$ and $P_{A'}$ coincide on large integers. Since $\Delta\phi_A(i-1) = P_{A'}(i)$ for large i, Lemma 10.1 implies that there exists a polynomial P_A of degree one higher than that of $P_{A'}$ (so of degree $\dim \mathrm{supp}(A)$) which coincides with ϕ_A for sufficiently large integers. □

REMARK 10.4. For M as in this theorem we may also form the Laurent series $L_M(u) := \sum_i \dim(M_i)u^i$ (this is usually called the *Poincaré series* of M). It follows from Remark 10.2 and Theorem 10.3 that $L_M(u) \in \mathbb{Z}[u][(u-1)^{-1}]$.

It follows from Lemma 10.1 that when P_M is nonzero, then its leading term has the form $c_d z^d/d!$, where d is the dimension of $\mathrm{supp}(M)$ and c_d is a positive integer. This observation leads to a notion of degree (that is not to be confused with the degree of P_M):

DEFINITION 10.5. If $d = \dim \mathrm{supp}(M)$, then the *(projective) degree* $\deg(M)$ is $d!$ times the leading coefficient of its Hilbert polynomial (an integer, which we stipulate to be zero in case $\mathrm{supp}(M) = \emptyset$). For a closed subset $Y \subset \mathbb{P}(V)$, the Hilbert polynomial P_Y resp. the *degree* $\deg(Y)$ of Y is that of $k[V]/I(Y)$ as a $k[V]$-module.

REMARK 10.6. Observe that if $Y \subset \mathbb{P}(V)$ is nonempty, then $\deg(Y) > 0$. For then $I_{Y,d} \neq k[V]_d$ for every $d \geq 0$ and so the Hilbert function of the homogeneous coordinate ring $k[\mathrm{Cone}(Y)] = k[V]/I(Y)$ 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 of $k[\mathrm{Cone}(Y)]$, it is for this notion irrelevant whether Y happens to lie in a lower dimensional projective space $Y \subset \mathbb{P}(V') \subset \mathbb{P}(V)$ for some $V' \subset V$. For example, the degree of a singleton $\{y\} \subset \mathbb{P}(V)$ is the degree of the $k[T]$-module $k[T]$ and hence equal to 1.

One can show that there exists a nonempty open subset of linear subspaces $Q \subset \mathbb{P}(V)$ of codimension equal to $\dim Y$ which meet Y in exactly $\deg(Y)$ points. This characterization is in fact the classical way of defining the degree of Y.

EXERCISE 69. Suppose that M is not of finite length. Prove that there is a unique integer $d \geq 0$ such that $i \mapsto \Delta^d \phi_M(i)$ is a nonzero constant for i sufficiently large. Show that d is the dimension of the support of M and that the constant is its degree.

EXERCISE 70. Compute the Hilbert polynomial and the degree of

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

EXERCISE 71. Let $Y \subset \mathbb{P}^m$ and $Z \subset \mathbb{P}^n$ be closed and consider $Y \times Z$ as a closed subset of $\mathbb{P}^{mn+m+n}$ via the Segre embedding. Prove that the Hilbert function resp. polynomial of $Y \times Z$ is the product of the Hilbert functions resp. polynomials of the factors.

We may now supplement Theorem 10.3 as follows. Let M be as in that theorem: a finitely generated graded $k[V]$-module. Recall that $\mathcal{P}(M)$ denotes the set of minimal prime ideals containing $\mathrm{Ann}(M)$. For every $\mathfrak{p} \in \mathcal{P}(M)$ not equal to $k[V]_+$, the associated closed subset $Z[\mathfrak{p}] \subset \mathbb{P}(V)$ is an irreducible component of $\mathrm{supp}(M)$ and all irreducible components of $\mathrm{supp}(M)$ are so obtained (for $\mathfrak{p} = k[V]_+$ we get the empty set, but we also have $\deg(k[V]/k[V]_+) = 0$). Denote by $\mathcal{P}_o(M)$ the set of $\mathfrak{p} \in \mathcal{P}(M)$ that define an irreducible component of $\mathrm{supp}(M)$ of the same dimension as $\mathrm{supp}(M)$.

PROPOSITION 10.7. *Let M be a finitely generated graded $k[V]$-module. Then*

$$\deg(M) = \sum_{\mathfrak{p} \in \mathcal{P}_o(M)} \mu_{\mathfrak{p}}(M) \deg(Z[\mathfrak{p}]).$$

PROOF. We write M as an iterated extension by elementary modules: $M = M^0 \supsetneq M^1 \supsetneq \cdots \supsetneq M^d = \{0\}$ with $M^{i-1}/M^i \cong k[V]/\mathfrak{p}_i[l_i]$. Then $\phi_M(i) = \sum_{i=1}^d \phi_{k[V]/\mathfrak{p}_i}(i+l_i)$. Now $\phi_{k[V]/\mathfrak{p}_i}$ is a polynomial of degree equal to the dimension of $\mathrm{supp}(k[V]/\mathfrak{p}_i) = Z[\mathfrak{p}_i] \subset \mathbb{P}(V)$. This degree does not change if we replace the variable i by $i + l_i$. In view of Proposition 9.8 we only get a contribution to the leading coefficient of ϕ_M when $\mathfrak{p}_i \in \mathcal{P}_o(M)$ and for any given $\mathfrak{p} \in \mathcal{P}_o(M)$ this happens exactly $\mu_{\mathfrak{p}}(M_{\mathfrak{p}})$ times. The proposition follows. □

REMARK 10.8. Note the special case when M has finite support: then $\mathcal{P}_o(M) = \mathcal{P}(M) \setminus \{k[V]_+\}$ and this set is in bijective correspondence with the points of $\operatorname{supp}(M)$. For $\mathfrak{p} \in \mathcal{P}_o(M)$, $Z[\mathfrak{p}] \subset \mathbb{P}(V)$ is just a singleton $\{p\}$ and so $\deg(Z[\mathfrak{p}]) = 1$. Furthermore, $\mu_{\mathfrak{p}}(M)$ is the length of $M_{\mathfrak{p}}$ as a $k[V]$-module and this is by Remark 9.10 equal to $\dim_k \mathcal{M}_p$, where $\mathcal{M}_p := M_{\mathfrak{p},o}$ is a $\mathcal{O}_{\mathbb{P}(V),p} = k[V]_{\mathfrak{p},o}$-module of finite length. So the above formula then says that $\deg(M) = \sum_{p \in \operatorname{supp}(M)} \dim_k(\mathcal{M}_p)$.

EXERCISE 72. Let $Y \subset \mathbb{P}(V)$ be closed. Prove that if $Y_1, \dots, Y_r$ are the distinct irreducible components of Y of maximal dimension ($= \dim Y$), then $\deg(Y) = \sum_{i=1}^r \deg(Y_i)$.

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

PROPOSITION 10.9. *Let M be a graded $k[V]$-module and $F \in k[V]_d$ with $F \notin \operatorname{Ann}(M)$. Then $\deg(M/FM) = d \deg(M)$.*

PROOF. Our assumption implies that the sequence

$$0 \to M(-d) \xrightarrow{\cdot F} M \to M/FM \to 0$$

is exact. This shows that $P_{M/FM}(z) = P_M(z) - P_M(z-d)$. Put $m := \dim \operatorname{supp}(M)$ so that is we write $P_M(z) = \sum_{i=0}^m a_i z^i/i!$, then $a_m = \deg(M)$. Since we have $z^i/i! - (z-d)^i/i! = dz^{i-1}/(i-1)!+$ lower order terms, we find that $P_{M/FM}(z) = da_m z^{m-1}/(m-1)!+$ lower order terms. So $\deg(M/FM) = da_m = d \deg(M)$. □

Note the special case for which $M = k[V]$ and F is a generator of the ideal defining a hypersurface $H \subset \mathbb{P}(V)$. Then $P_M(z) = \binom{n+z}{n}$ and so the degree of M (which is also the degree of $\mathbb{P}(V)$) is 1 and hence the degree of H is d, just as we would expect. We can now state:

THEOREM 10.10 (Theorem of Bézout). *Let $H_i \subset \mathbb{P}(V)$ be a hypersurface of degree $d_i > 0$ ($i = 1, \dots n$), and assume that $H_1 \cap \dots \cap H_n$ is finite. Each H_i determines at $p \in H_1 \cap \dots \cap H_n$ a principal ideal in $\mathcal{O}_{\mathbb{P}(V),p}$; denote by $\mathcal{I}_p \subset \mathcal{O}_{\mathbb{P}(V),p}$ the sum of these ideals. Then*

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

Here $\dim_k(\mathcal{O}_{\mathbb{P}(V),p}/\mathcal{I}_p)$ should be interpreted as the intersection multiplicity the hypersurfaces $H_1, \dots, H_n$ at p. So the theorem can be paraphrased as saying that $H_1, \dots, H_n$ meet in $d_1 d_2 \cdots d_n$ points, provided we count each such point with its intersection multiplicity.

We shall need the following result which we state without proof.

*PROPOSITION 10.11. *Let $F_1, \dots, F_r$ be $r \leq n+1$ homogeneous elements of $k[V]$ such that $\dim(k[V]/(F_1, \dots, F_r)) = n + 1 - r$. Then the image of F_r in $k[V]/(F_1, \dots, F_{r-1})$ is not a zero divisor.*

PROOF OF THEOREM 10.10. Let $F_i \in k[V]_{d_i}$ define H_i. Denote by M^i the $k[V]$-module $k[V]/(F_1, \dots, F_i)$ (so that $M^0 = k[V]$). Then according to Propositions 10.9 and 10.11 we have $\deg(M^i) = d_i \deg(M^{i-1})$. Since $\deg M^0 = 1$, it follows that $\deg(M^n) = d_1 d_2 \cdots d_n$. The support of M^n is $H_1 \cap \dots \cap H_n$ and hence finite. Its degree is then also computed as $\sum_{\mathfrak{p} \in \mathcal{P}_o(M^n)} \mu_{\mathfrak{p}}(M^n)$. But according to Remark 10.8 this is just $\sum_{p \in H_1 \cap \dots \cap H_n} \dim_k(\mathcal{O}_{\mathbb{P}(V),p}/\mathcal{I}_p)$. □

EXAMPLE 10.12. Assume $\mathrm{char}(k) \neq 2$. We compute the intersection multiplicities of the conics C and C' in $\mathbb{P}^2$ whose affine equations are $x^2 + y^2 - 2y = 0$ and $x^2 - y = 0$. There are three points of intersection: $(0,0)$, $(-1,1)$ and $(1,1)$ (so none at infinity). The intersection multiplicity at $(0,0)$ is the dimension of $\mathcal{O}_{\mathbb{A}^2,(0,0)}/(x^2+y^2-2y, x^2-y)$ as a k-vector space. But $\mathcal{O}_{\mathbb{A}^2,(0,0)}/(x^2+y^2-2y, x^2-y) = \mathcal{O}_{\mathbb{A}^1,0}/(x^4-x^2) = k[x]/(x^2)$ (for (x^2-1) is invertible in $\mathcal{O}_{\mathbb{A}^1,0}$). Clearly $\dim_k(k[x]/(x^2)) = 2$ and so this is also the intersection multiplicity at $(0,0)$. The intersection multiplicities at $(-1,1)$ and $(1,1)$ are easily calculated to be 1 and thus the identity $2+1+1 = 2\cdot 2$ illustrates the Bézout theorem.

REMARK 10.13. If $Y \subset \mathbb{P}^n$ is closed, then $P_Y(0)$ can be shown to be an invariant of Y in the sense that it is independent of the projective embedding. In many ways, it behaves like an Euler characteristic. (It is in fact the Euler characteristic of $\mathcal{O}_Y$ in a sense that will become clear once we know about sheaf cohomology.) For example, $P_{Y\times Z}(0) = P_Y(0)P_Z(0)$.

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