ALGEBRAIC GEOMETRY

J.S. MILNE

ABSTRACT. These are the notes for Math 631, taught at the University of Michigan, Fall 1993. They are available at `www.math.lsa.umich.edu/~jmilne/`

Please send comments and corrections to me at jmilne@umich.edu.

v2.01 (August 24, 1996). First version on the web.

v3.01 (June 13, 1998). Added 5 sections (25 pages) and an index. Minor changes to Sections 0–8.

CONTENTS

Introduction 2
0. Algorithms for Polynomials 4
1. Algebraic Sets 14
2. Affine Algebraic Varieties 30
3. Algebraic Varieties 44
4. Local Study: Tangent Planes, Tangent Cones, Singularities 59
5. Projective Varieties and Complete Varieties 80
6. Finite Maps 101
7. Dimension Theory 109
8. Regular Maps and Their Fibres. 117
9. Algebraic Geometry over an Arbitrary Field 131
10. Divisors and Intersection Theory 137
11. Coherent Sheaves; Invertible Sheaves. 143
12. Differentials 149
13. Algebraic Varieties over the Complex Numbers 151
14. Further Reading 153
Index 156

Introduction

Just as the starting point of linear algebra is the study of the solutions of systems of linear equations,

$$\sum_{j=1}^{n} a_{ij}X_j = d_i, \quad i = 1, \dots, m, \qquad (*)$$

the starting point for algebraic geometry is the study of the solutions of systems of polynomial equations,

$$f_i(X_1, \dots, X_n) = 0, \quad i = 1, \dots, m, \quad f_i \in k[X_1, \dots, X_n].$$

Note immediately one difference between linear equations and polynomial equations: theorems for linear equations don't depend on which field k you are working over,[1] but those for polynomial equations depend on whether or not k is algebraically closed and (to a lesser extent) whether k has characteristic zero. Since I intend to emphasize the geometry in this course, we will work over algebraically closed fields for the major part of the course.

A better description of algebraic geometry is that it is the study of polynomial functions and the spaces on which they are defined (algebraic varieties), just as topology is the study of continuous functions and the spaces on which they are defined (topological spaces), differential geometry (=advanced calculus) the study of differentiable functions and the spaces on which they are defined (differentiable manifolds), and complex analysis the study of holomorphic functions and the spaces on which they are defined (Riemann surfaces and complex manifolds). The approach adopted in this course makes plain the similarities between these different fields. Of course, the polynomial functions form a much less rich class than the others, but by restricting our study to polynomials we are able to do calculus over any field: we simply define

$$\frac{d}{dX}\sum a_iX^i = \sum ia_iX^{i-1}.$$

Moreover, calculations (on a computer) with polynomials are easier than with more general functions.

Consider a differentiable function $f(x, y, z)$. In calculus, we learn that the equation

$$f(x, y, z) = C \qquad (**)$$

defines a surface S in $\mathbb{R}^3$, and that the tangent space to S at a point $P = (a, b, c)$ has equation[2]

$$\left(\frac{\partial f}{\partial x}\right)_P (x-a) + \left(\frac{\partial f}{\partial y}\right)_P (y-b) + \left(\frac{\partial f}{\partial z}\right)_P (z-c) = 0. \qquad (***).$$

The inverse function theorem says that a differentiable map $\alpha : S \to S'$ of surfaces is a local isomorphism at a point $P \in S$ if it maps the tangent space at P isomorphically onto the tangent space at $P' = \alpha(P)$.

[1] For example, suppose that the system (*) has coefficients $a_{ij} \in k$ and that K is a field containing k. Then (*) has a solution in k^n if and only if it has a solution in K^n, and the dimension of the space of solutions is the same for both fields. (Exercise!)

[2] Think of S as a level surface for the function f, and note that the equation is that of a plane through (a, b, c) perpendicular to the gradient vector $(\nabla f)_P$ at P.)

Consider a polynomial $f(x,y,z)$ with coefficients in a field k. In this course, we shall learn that the equation (**) defines a surface in k^3, and we shall use the equation (***) to define the tangent space at a point P on the surface. However, and this is one of the essential differences between algebraic geometry and the other fields, the inverse function theorem doesn't hold in algebraic geometry. One other essential difference: $1/X$ is not the derivative of any rational function of X; nor is X^{np-1} in characteristic $p \neq 0$. Neither can be integrated in the ring of polynomial functions.

Some notations. Recall that a field k is said to be *algebraically closed* if every polynomial $f(X)$ with coefficients in k factors completely in k. Examples: $\mathbb{C}$, or the subfield $\mathbb{Q}^{\text{al}}$ of $\mathbb{C}$ consisting of all complex numbers algebraic over $\mathbb{Q}$. Every field k is contained in an algebraically closed field.

A field of characteristic zero contains a copy of $\mathbb{Q}$, the field of rational numbers. A field of characteristic p contains a copy of $\mathbb{F}_p$, the field $\mathbb{Z}/p\mathbb{Z}$. The symbol $\mathbb{N}$ denotes the natural numbers, $\mathbb{N} = \{0, 1, 2, \dots\}$. Given an equivalence relation, $[*]$ sometimes denotes the equivalence class containing $*$.

"Ring" will mean "commutative ring with 1", and a homomorphism of rings will always carry 1 to 1. For a ring A, $A^\times$ is the group of units in A:

$$A^\times = \{a \in A \mid \exists b \in A \text{ such that } ab = 1\}.$$

A subset R of a ring A is a *subring* if it is closed under addition, multiplication, the formation of negatives, and contains the identity element.[3] We use Gothic (fraktur) letters for ideals:

$\mathfrak{a}$	$\mathfrak{b}$	$\mathfrak{c}$	$\mathfrak{m}$	$\mathfrak{n}$	$\mathfrak{p}$	$\mathfrak{q}$	$\mathfrak{A}$	$\mathfrak{B}$	$\mathfrak{C}$	$\mathfrak{M}$	$\mathfrak{N}$	$\mathfrak{P}$	$\mathfrak{Q}$
a	b	c	m	n	p	q	A	B	C	M	N	P	Q

We use the following notations:

$X \approx Y$	X and Y are isomorphic;
$X \cong Y$	X and Y are canonically isomorphic (or there is a given or unique isomorphism);
$X \stackrel{\text{df}}{=} Y$	X is defined to be Y, or equals Y by definition;
$X \subset Y$	X is a subset of Y (not necessarily proper).

[3] The definition on page 2 of Atiyah and MacDonald 1969 is incorrect, since it omits the condition that $x \in R \Rightarrow -x \in R$ — the subset $\mathbb{N}$ of $\mathbb{Z}$ satisfies their conditions, but it is not a subring of $\mathbb{Z}$.

0. Algorithms for Polynomials

In this section, we first review some basic definitions from commutative algebra, and then we derive some algorithms for working in polynomial rings. Those not interested in algorithms can skip the section.

Throughout the section, k will be a field (not necessarily algebraically).

Ideals. Let A be a ring. Recall that an *ideal* $\mathfrak{a}$ in A is a subset such that

(a) $\mathfrak{a}$ is a subgroup of A regarded as a group under addition;
(b) $a \in \mathfrak{a}$, $r \in A \Rightarrow ra \in A$.

The *ideal generated by a subset* S of A is the intersection of all ideals A containing $\mathfrak{a}$ — it is easy to verify that this is in fact an ideal, and that it consists of all finite sums of the form $\sum r_i s_i$ with $r_i \in A$, $s_i \in S$. When $S = \{s_1, \dots, s_m\}$, we shall write $(s_1, \dots, s_m)$ for the ideal it generates.

Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals in A. The set $\{a + b \mid a \in \mathfrak{a},\, b \in \mathfrak{b}\}$ is an ideal, denoted by $\mathfrak{a} + \mathfrak{b}$. The ideal generated by $\{ab \mid a \in \mathfrak{a},\, b \in \mathfrak{b}\}$ is denoted by $\mathfrak{ab}$. Note that $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$. Clearly $\mathfrak{ab}$ consists of all finite sums $\sum a_i b_i$ with $a_i \in \mathfrak{a}$ and $b_i \in \mathfrak{b}$, and if $\mathfrak{a} = (a_1, \dots, a_m)$ and $\mathfrak{b} = (b_1, \dots, b_n)$, then $\mathfrak{ab} = (a_1 b_1, \dots, a_i b_j, \dots, a_m b_n)$.

Let $\mathfrak{a}$ be an ideal of A. The set of cosets of $\mathfrak{a}$ in A forms a ring $A/\mathfrak{a}$, and $a \mapsto a + \mathfrak{a}$ is a homomorphism $\varphi\colon A \to A/\mathfrak{a}$. The map $\mathfrak{b} \mapsto \varphi^{-1}(\mathfrak{b})$ is a one-to-one correspondence between the ideals of $A/\mathfrak{a}$ and the ideals of A containing $\mathfrak{a}$.

An ideal $\mathfrak{p}$ if *prime* if $\mathfrak{p} \neq A$ and $ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. Thus $\mathfrak{p}$ is prime if and only if $A/\mathfrak{p}$ is nonzero and has the property that

$$ab = 0, \quad b \neq 0 \Rightarrow a = 0,$$

i.e., $A/\mathfrak{p}$ is an integral domain.

An ideal $\mathfrak{m}$ is *maximal* if $\mathfrak{m} \neq A$ and there does not exist an ideal $\mathfrak{n}$ contained strictly between $\mathfrak{m}$ and A. Thus $\mathfrak{m}$ is maximal if and only if $A/\mathfrak{m}$ has no proper nonzero ideals, and so is a field. Note that

$$\mathfrak{m} \text{ maximal } \Rightarrow \mathfrak{m} \text{ prime.}$$

The ideals of $A \times B$ are all of the form $\mathfrak{a} \times \mathfrak{b}$, with $\mathfrak{a}$ and $\mathfrak{b}$ ideals in A and B. To see this, note that if $\mathfrak{c}$ is an ideal in $A \times B$ and $(a, b) \in \mathfrak{c}$, then $(a, 0) = (a, b)(1, 0) \in \mathfrak{c}$ and $(0, b) = (a, b)(0, 1) \in \mathfrak{c}$. This shows that $\mathfrak{c} = \mathfrak{a} \times \mathfrak{b}$ with

$$\mathfrak{a} = \{a \mid (a, b) \in \mathfrak{c} \text{ some } b \in \mathfrak{b}\}$$

and

$$\mathfrak{b} = \{b \mid (a, b) \in \mathfrak{c} \text{ some } a \in \mathfrak{a}\}.$$

Proposition 0.1. *The following conditions on a ring A are equivalent:*

(a) *every ideal in A is finitely generated;*
(b) *every ascending chain of ideals $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$ becomes stationary, i.e., for some m, $\mathfrak{a}_m = \mathfrak{a}_{m+1} = \cdots$.*
(c) *every nonempty set of ideals in A has maximal element, i.e., an element not properly contained in any other ideal in the set.*

PROOF. (a) $\Rightarrow$ (b): If $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$ is an ascending chain, then $\cup\mathfrak{a}_i$ is again an ideal, and hence has a finite set $\{a_1, \dots, a_n\}$ of generators. For some m, all the a_i belong $\mathfrak{a}_m$ and then

$$\mathfrak{a}_m = \mathfrak{a}_{m+1} = \cdots = \mathfrak{a}.$$

(b) $\Rightarrow$ (c): If (c) is false, then there exists a nonempty set S of ideals with no maximal element. Let $\mathfrak{a}_1 \in S$; because $\mathfrak{a}_1$ is not maximal in S, there exists an ideal $\mathfrak{a}_2$ in S that properly contains $\mathfrak{a}_1$. Similarly, there exists an ideal $\mathfrak{a}_3$ in S properly containing $\mathfrak{a}_2$, etc.. In this way, we can construct an ascending chain of ideals $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \mathfrak{a}_3 \subset \cdots$ in S that never becomes stationary.

(c) $\Rightarrow$ (a): Let $\mathfrak{a}$ be an ideal, and let S be the set of ideals $\mathfrak{b} \subset \mathfrak{a}$ that are finitely generated. Let $\mathfrak{c} = (a_1, \dots, a_r)$ be a maximal element of S. If $\mathfrak{c} \neq \mathfrak{a}$, so that there exists an element $a \in \mathfrak{a}$, $a \notin \mathfrak{c}$, then $\mathfrak{c}' = (a_1, \dots, a_r, a) \subset \mathfrak{a}$ and properly contains $\mathfrak{c}$, which contradicts the definition of $\mathfrak{c}$. □

A ring A is *Noetherian* if it satisfies the conditions of the proposition. Note that, in a Noetherian ring, every ideal is contained in a maximal ideal (apply (c) to the set of all proper ideals of A containing the given ideal). In fact, this is true in any ring, but the proof for non-Noetherian rings requires the axiom of choice (Atiyah and MacDonald 1969, p3).

Algebras. Let A be a ring. An A-algebra is a ring B together with a homomorphism $i_B\colon A \to B$. A *homomorphism of A-algebras* $B \to C$ is a homomorphism of rings $\varphi\colon B \to C$ such that $\varphi(i_B(a)) = i_C(a)$ for all $a \in A$.

An A-algebra B is said to be *finitely generated* (or of *finite-type* over A) if there exist elements $x_1, \dots, x_n \in B$ such that every element of B can be expressed as a polynomial in the x_i with coefficients in $i(A)$, i.e., such that the homomorphism $A[X_1, \dots, X_n] \to B$ sending X_i to x_i is surjective.

A ring homomorphism $A \to B$ is *finite*, and B is a *finite* A-algebra, if B is finitely generated as an A-module[4].

Let k be a field, and let A be a k-algebra. If $1 \neq 0$ in A, then the map $k \to A$ is injective, and we can identify k with its image, i.e., we can regard k as a subring of A. If $1 = 0$ in a ring R, the R is the zero ring, i.e., $R = \{0\}$.

Polynomial rings. Let k be a field. A *monomial* in $X_1, \dots, X_n$ is an expression of the form

$$X_1^{a_1} \cdots X_n^{a_n}, \quad a_j \in \mathbb{N}.$$

The *total degree* of the monomial is $\sum a_i$. We sometimes abbreviate it by X^α, $\alpha = (a_1, \dots, a_n) \in \mathbb{N}^n$.

The elements of the polynomial ring $k[X_1, \dots, X_n]$ are finite sums

$$\sum c_{a_1 \cdots a_n} X_1^{a_1} \cdots X_n^{a_n}, \quad c_{a_1 \cdots a_n} \in k, \quad a_j \in \mathbb{N}.$$

with the obvious notions of equality, addition, and multiplication. Thus the monomials from a basis for $k[X_1, \dots, X_n]$ as a k-vector space.

[4]The term "module-finite" is used in this context only by the English-insensitive.

The ring $k[X_1,\dots,X_n]$ is an integral domain, and the only units in it are the nonzero constant polynomials. A polynomial $f(X_1,\dots,X_n)$ is *irreducible* if it is nonconstant and has only the obvious factorizations, i.e., $f = gh \Rightarrow g$ or h is constant.

THEOREM 0.2. *The ring $k[X_1,\dots,X_n]$ is a unique factorization domain, i.e., each nonzero nonconstant polynomial f can be written as a finite product of irreducible polynomials in exactly one way (up to constants and the order of the factors).*

PROOF. This is usually proved in basic graduate algebra courses. There is a detailed proof in Herstein, Topics in Algebra, 1975, 3.11. It proceeds by induction on the number of variables: if R is a unique factorization domain, then so also is $R[X]$. □

COROLLARY 0.3. *A nonzero principal ideal (f) in $k[X_1,\dots,X_n]$ is prime if and only f is irreducible.*

PROOF. Assume (f) is a prime ideal. Then f can't be a unit (otherwise (f) is the whole ring), and if $f = gh$ then $gh \in (f)$, which, because (f) is prime, implies that g or h is in (f), i.e., that one is divisible by f, say $g = fq$. Now $f = fq\,h$ implies that $q\,h = 1$, and that h is a unit. Conversely, assume f is irreducible. If $gh \in (f)$, then $f|gh$, which implies that $f|g$ or $f|h$ (here we use that $k[X_1,\dots,X_n]$ is a unique factorization domain), i.e., that g or $h \in (f)$. □

The two main results of this section will be:

(a) (Hilbert basis theorem) Every ideal in $k[X_1,\dots,X_n]$ has a finite set of generators (in fact, of a special sort).
(b) There exists an algorithm for deciding whether a polynomial belongs to an ideal.

This remainder of this section is a summary of Cox et al.1992, pp 1–111, to which I refer the reader for more details.

Division in $k[X]$. The division algorithm allows us to divide a nonzero polynomial into another: let f and g be polynomials in $k[X]$ with $g \neq 0$; then there exist unique polynomials $q, r \in k[X]$ such that $f = qg + r$ with either $r = 0$ or $\deg r < \deg g$. Moreover, there is an algorithm for deciding whether $f \in (g)$, namely, find r and check whether it is zero.

In Maple,

`quo(f,g,X)`; computes q
`rem(f,g,X)`; computes r

Moreover, the Euclidean algorithm allows you to pass from a finite set of generators for an ideal in $k[X]$ to a single generator by successively replacing each pair of generators with their greatest common divisor.

Orderings on monomials. Before we can describe an algorithm for dividing in $k[X_1,\dots,X_n]$, we shall need to choose a way of ordering monomials. Essentially this amounts to defining an ordering on $\mathbb{N}^n$. There are two main systems, the first of which is preferred by humans, and the second by machines.

(Pure) lexicographic ordering (lex). Here monomials are orderd by lexicographic (dictionary) order. More precisely, let $\alpha = (a_1,\dots,a_n)$ and $\beta = (b_1,\dots,b_n)$ be two

elements of $\mathbb{N}^n$; then

$$\alpha > \beta \text{ and } X^\alpha > X^\beta \text{ (lexicographic ordering)}$$

if, in the vector difference $\alpha - \beta \in \mathbb{Z}$, the left-most nonzero entry is positive. For example,

$$XY^2 > Y^3Z^4; \quad X^3Y^2Z^4 > X^3Y^2Z.$$

Note that this isn't quite how the dictionary would order them: it would put XXXYYZZZZ *after* XXXYYZ.

Graded reverse lexicographic order (grevlex). Here monomials are ordered by total degree, with ties broken by reverse lexicographic ordering. Thus, $\alpha > \beta$ if $\sum a_i > \sum b_i$, or $\sum a_i = \sum b_i$ and in $\alpha - \beta$ the right-most nonzero entry is negative. For example:

$$\begin{aligned} X^4Y^4Z^7 &> X^5Y^5Z^4 \quad \text{(total degree greater)} \\ XY^5Z^2 &> X^4YZ^3, \quad X^5YZ > X^4YZ^2. \end{aligned}$$

Orderings on $k[X_1, \dots, X_n]$. Fix an ordering on the monomials in $k[X_1, \dots, X_n]$. Then we can write an element f of $k[X_1, \dots, X_n]$ in a canonical fashion, by re-ordering its elements in decreasing order. For example, we would write

$$f = 4XY^2Z + 4Z^2 - 5X^3 + 7X^2Z^2$$

as

$$f = -5X^3 + 7X^2Z^2 + 4XY^2Z + 4Z^2 \qquad \text{(lex)}$$

or

$$f = 4XY^2Z + 7X^2Z^2 - 5X^3 + 4Z^2 \qquad \text{(grevlex)}$$

Let $f = \sum a_\alpha X^\alpha \in k[X_1, \dots, X_n]$. Write it in decreasing order:

$$f = a_{\alpha_0}X^{\alpha_0} + a_{\alpha_1}X^{\alpha_1} + \cdots, \quad \alpha_0 > \alpha_1 > \cdots, \quad a_{\alpha_0} \neq 0.$$

Then we define:

(a) the *multidegree* of f to be $\text{multdeg}(f) = \alpha_0$;
(b) the *leading coefficient* of f to be $\text{LC}(f) = a_{\alpha_0}$;
(c) the *leading monomial* of f to be $\text{LM}(f) = X^{\alpha_0}$;
(d) the *leading term* of f to be $\text{LT}(f) = a_{\alpha_0}X^{\alpha_0}$.

For example, for the polynomial $f = 4XY^2Z + \cdots$, the multidegree is $(1, 2, 1)$, the leading coefficient is 4, the leading monomial is XY^2Z, and the leading term is $4XY^2Z$.

The division algorithm in $k[X_1, \dots, X_n]$. Fix a monomial ordering in $\mathbb{N}^n$. Suppose given a polynomial f and an ordered set $(g_1, \dots, g_s)$ of polynomials; the division algorithm then constructs polynomials $a_1, \dots, a_s$ and r such that

$$f = a_1g_1 + \cdots + a_sg_s + r$$

where either $r = 0$ or no monomial in r is divisible by any of $\text{LT}(g_1), \dots, \text{LT}(g_s)$.

Step 1: If $\mathrm{LT}(g_1)|\mathrm{LT}(f)$, divide g_1 into f to get

$$f = a_1 g_1 + h, \quad a_1 = \frac{\mathrm{LT}(f)}{\mathrm{LT}(g_1)} \in k[X_1, \dots, X_n].$$

If $\mathrm{LT}(g_1)|\mathrm{LT}(h)$, repeat the process until

$$f = a_1 g_1 + f_1$$

(different a_1) with $\mathrm{LT}(f_1)$ not divisible by $\mathrm{LT}(g_1)$. Now divide g_2 into f_1, and so on, until

$$f = a_1 g_1 + \cdots + a_s g_s + r_1$$

with $\mathrm{LT}(r_1)$ not divisible by any of $\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_s)$.

Step 2: Rewrite $r_1 = \mathrm{LT}(r_1) + r_2$, and repeat Step 1 with r_2 for f:

$$f = a_1 g_1 + \cdots + a_s g_s + \mathrm{LT}(r_1) + r_3$$

(different a_i's).

Step 3: Rewrite $r_3 = \mathrm{LT}(r_3) + r_4$, and repeat Step 1 with r_4 for f. f=a

$$f = a_1 g_1 + \cdots + a_s g_s + \mathrm{LT}(r_1) + \mathrm{LT}(r_3) + r_3$$

(different a_i's).

Continue until you achieve a remainder with the required property. In more detail,[5] after dividing through once by $g_1, \dots, g_s$, you repeat the process until no leading term of one of the g_i's divides the leading term of the remainder. Then you discard the leading term of the remainder, and repeat ....

Example 0.4. (a) Consider

$$f = X^2Y + XY^2 + Y^2, \quad g_1 = XY - 1, \quad g_2 = Y^2 - 1.$$

First, on dividing g_1 into f, we obtain

$$X^2Y + XY^2 + Y^2 = (X + Y)(XY - 1) + X + Y^2 + Y.$$

This completes the first step, because the leading term of $Y^2 - 1$ does not divide the leading term of the remainder $X + Y^2 + Y$. We discard X, and write

$$Y^2 + Y = 1 \cdot (Y^2 - 1) + Y + 1.$$

Altogether

$$X^2Y + XY^2 + Y^2 = (X + Y) \cdot (XY - 1) + 1 \cdot (Y^2 - 1) + X + Y + 1.$$

(b) Consider the same polynomials, but with a different order for the divisors

$$f = X^2Y + XY^2 + Y^2, \quad g_1 = Y^2 - 1, \quad g_2 = XY - 1.$$

In the first step,

$$X^2Y + XY^2 + Y^2 = (X + 1) \cdot (Y^2 - 1) + X \cdot (XY - 1) + 2X + 1.$$

Thus, in this case, the remainder is $2X + 1$.

[5] This differs from the algorithm in Cox et al. 1992, p63, which says to go back to g_1 after every successful division.

REMARK 0.5. (a) If $r = 0$, then $f \in (g_1, \dots, g_s)$.

(b) Unfortunately, the remainder one obtains depends on the ordering of the g_i's. For example, (lex ordering)

$$XY^2 - X = Y \cdot (XY + 1) + 0 \cdot (Y^2 - 1) + -X - Y$$

but

$$XY^2 - X = X \cdot (Y^2 - 1) + 0 \cdot (XY - 1) + 0.$$

Thus, the division algorithm (as stated) will *not* provide a test for f lying in the ideal generated by $g_1, \dots, g_s$.

Monomial ideals. In general, an ideal $\mathfrak{a}$ will contain a polynomial without containing the individual terms of the polynomial; for example, the ideal $\mathfrak{a} = (Y^2 - X^3)$ contains $Y^2 - X^3$ but not Y^2 or X^3.

DEFINITION 0.6. An ideal $\mathfrak{a}$ is *monomial* if

$$\sum c_\alpha X^\alpha \in \mathfrak{a} \Rightarrow X^\alpha \in \mathfrak{a} \text{ all } \alpha \text{ with } c_\alpha \neq 0.$$

PROPOSITION 0.7. *Let $\mathfrak{a}$ be a monomial ideal, and let $A = \{\alpha \mid X^\alpha \in \mathfrak{a}\}$. Then A satisfies the condition*

$$\alpha \in A, \quad \beta \in \mathbb{N}^n \Rightarrow \alpha + \beta \in A. \qquad (*)$$

and $\mathfrak{a}$ is the k-subspace of $k[X_1, \dots, X_n]$ generated by the X^α, $\alpha \in A$. Conversely, if A is a subset of $\mathbb{N}^n$ satisfying (*), then the k-subspace $\mathfrak{a}$ of $k[X_1, \dots, X_n]$ generated by $\{X^\alpha \mid \alpha \in A\}$ is a monomial ideal.

PROOF. It is clear from its definition that a monomial ideal $\mathfrak{a}$ is the k-subspace of $k[X_1, \dots, X_n]$ generated by the set of monomials it contains. If $X^\alpha \in \mathfrak{a}$ and $X^\beta \in k[X_1, \dots, X_n]$, then $X^\alpha X^\beta = X^{\alpha+\beta} \in \mathfrak{a}$, and so A satisfies the condition (*). Conversely,

$$\left(\sum_{\alpha \in A} c_\alpha X^\alpha\right)\left(\sum_{\beta \in \mathbb{N}^n} d_\beta X^\beta\right) = \sum_{\alpha,\beta} c_\alpha d_\beta X^{\alpha+\beta} \qquad \text{(finite sums)},$$

and so if A satisfies (*), then the subspace generated by the monomials X^α, $\alpha \in A$, is an ideal. □

The proposition gives a classification of the monomial ideals in $k[X_1, \dots, X_n]$: they are in one-to-one correspondence with the subsets A of $\mathbb{N}^n$ satisfying (*). For example, the monomial ideals in $k[X]$ are exactly the ideals (X^n), $n \geq 1$, and the zero ideal (corresponding to the empty set A). We write

$$\langle X^\alpha \mid \alpha \in A \rangle$$

for the ideal corresponding to A (subspace generated by the X^α, $\alpha \in A$).

LEMMA 0.8. *Let S be a subset of $\mathbb{N}^n$. Then the ideal $\mathfrak{a}$ generated by $\{X^\alpha \mid \alpha \in S\}$ is the monomial ideal corresponding to*

$$A \stackrel{df}{=} \{\beta \in \mathbb{N}^n \mid \beta - \alpha \in \mathbb{N}^n, \quad \text{some } \alpha \in S\}.$$

Thus, a monomial is in $\mathfrak{a}$ if and only if it is divisible by one of the X^α, $\alpha \in S$.

PROOF. Clearly A satisfies (*), and $\mathfrak{a} \supset \langle X^\beta \mid \beta \in A\rangle$. Conversely, if $\beta \in A$, then $\beta - \alpha \in \mathbb{N}^n$ for some $\alpha \in S$, and $X^\beta = X^\alpha X^{\beta-\alpha} \in \mathfrak{a}$. The last statement follows from the fact that $X^\alpha | X^\beta \iff \beta - \alpha \in \mathbb{N}^n$. □

Let $A \subset \mathbb{N}^2$ satisfy (*). From the geometry of A, it is clear that there is a finite set of elements $S = \{\alpha_1, \dots, \alpha_s\}$ of A such that

$$A = \{\beta \in \mathbb{N}^2 \mid \beta - \alpha_i \in \mathbb{N}^2, \text{ some } \alpha_i \in S\}.$$

(The α_i's are the "corners" of A.) Moreover, $\mathfrak{a} \stackrel{\text{df}}{=} \langle X^\alpha \mid \alpha \in A\rangle$ is generated by the monomials X^{α_i}, $\alpha_i \in S$. This suggests the following result.

THEOREM 0.9 (Dickson's Lemma). *Let $\mathfrak{a}$ be the monomial ideal corresponding to the subset $A \subset \mathbb{N}^n$. Then $\mathfrak{a}$ is generated by a finite subset of $\{X^\alpha \mid \alpha \in A\}$.*

PROOF. This is proved by induction on the number of variables — Cox et al. 1992, p70. □

Hilbert Basis Theorem.

DEFINITION 0.10. For a nonzero ideal $\mathfrak{a}$ in $k[X_1, \dots, X_n]$, we let $(\mathrm{LT}(\mathfrak{a}))$ be the ideal generated by

$$\{\mathrm{LT}(f) \mid f \in \mathfrak{a}\}.$$

LEMMA 0.11. *Let $\mathfrak{a}$ be a nonzero ideal in $k[X_1, \dots, X_n]$; then $(LT(\mathfrak{a}))$ is a monomial ideal, and it equals $(LT(g_1), \dots, LT(g_n))$ for some $g_1, \dots, g_n \in \mathfrak{a}$.*

PROOF. Since $(\mathrm{LT}(\mathfrak{a}))$ can also be described as the ideal generated by the leading monomials (rather than the leading terms) of elements of $\mathfrak{a}$, it follows from Lemma 0.8 that it is monomial. Now Dickson's Lemma shows that it equals $(\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_s))$ for some $g_i \in \mathfrak{a}$. □

THEOREM 0.12 (Hilbert Basis Theorem). *Every ideal $\mathfrak{a}$ in $k[X_1, \dots, X_n]$ is finitely generated; more precisely, $\mathfrak{a} = (g_1, \dots, g_s)$ where $g_1, \dots, g_s$ are any elements of $\mathfrak{a}$ whose leading terms generate $LT(\mathfrak{a})$.*

PROOF. Let $f \in \mathfrak{a}$. On applying the division algorithm, we find

$$f = a_1 g_1 + \cdots + a_s g_s + r, \quad a_i, r \in k[X_1, \dots, X_n],$$

where either $r = 0$ or no monomial occurring in it is divisible by any $\mathrm{LT}(g_i)$. But $r = f - \sum a_i g_i \in \mathfrak{a}$, and therefore $\mathrm{LT}(r) \in \mathrm{LT}(\mathfrak{a}) = (\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_s))$, which, according to Lemma 0.8, implies that *every* monomial occurring in r is divisible by one in $\mathrm{LT}(g_i)$. Thus $r = 0$, and $g \in (g_1, \dots, g_s)$. □

Standard (Gröbner) bases. Fix a monomial ordering of $k[X_1, \dots, X_n]$.

DEFINITION 0.13. A finite subset $S = \{g_1, \dots, g_s\}$ of an ideal $\mathfrak{a}$ is a *standard (Grobner, Groebner, Gröbner) basis* for [6] $\mathfrak{a}$ if

$$(\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_s)) = \mathrm{LT}(\mathfrak{a}).$$

[6] Standard bases were first introduced (under that name) by Hironaka in the mid-1960s, and independently, but slightly later, by Buchberger in his Ph.D. thesis. Buchberger named them after his thesis adviser Gröbner.

In other words, S is a standard basis if the leading term of every element of $\mathfrak{a}$ is divisible by at least one of the leading terms of the g_i.

THEOREM 0.14. *Every ideal has a standard basis, and it generates the ideal; if* $\{g_1, \dots, g_s\}$ *is a standard basis for an ideal* $\mathfrak{a}$*, then* $f \in \mathfrak{a} \iff$ *the remainder on division by the* g_i *is* 0*.*

PROOF. Our proof of the Hilbert basis theorem shows that every ideal has a standard basis, and that it generates the ideal. Let $f \in \mathfrak{a}$. The argument in the same proof, that the remainder of f on division by $g_1, \dots, g_s$ is 0, used only that $\{g_1, \dots, g_s\}$ is a standard basis for $\mathfrak{a}$.. □

REMARK 0.15. The proposition shows that, for $f \in \mathfrak{a}$, the remainder of f on division by $\{g_1, \dots, g_s\}$ is independent of the order of the g_i (in fact, it's always zero). This is not true if $f \notin \mathfrak{a}$ — see the example using Maple at the end of this section.

Let $\mathfrak{a} = (f_1, \dots, f_s)$. Typically, $\{f_1, \dots, f_s\}$ will fail to be a standard basis because in some expression

$$cX^\alpha f_i - dX^\beta f_j, \quad c, d \in k, \qquad (**)$$

the leading terms will cancel, and we will get a new leading term not in the ideal generated by the leading terms of the f_i. For example,

$$X^2 = X \cdot (X^2Y + X - 2Y^2) - Y \cdot (X^3 - 2XY)$$

is in the ideal generated by $X^2Y + X - 2Y^2$ and $X^3 - 2XY$ but it is not in the ideal generated by their leading terms.

There is an algorithm for transforming a set of generators for an ideal into a standard basis, which, roughly speaking, makes adroit use of equations of the form (**) to construct enough new elements to make a standard basis — see Cox et al. 1992, pp80–87.

We now have an algorithm for deciding whether $f \in (f_1, \dots, f_r)$. First transform $\{f_1, \dots, f_r\}$ into a standard basis $\{g_1, \dots, g_s\}$, and then divide f by $g_1, \dots, g_s$ to see whether the remainder is 0 (in which case f lies in the ideal) or nonzero (and it doesn't). This algorithm is implemented in Maple — see below.

A standard basis $\{g_1, \dots, g_s\}$ is *minimal* if each g_i has leading coefficient 1 and, for all i, the leading term of g_i does not belong to the ideal generated by the leading terms of the remaining g's. A standard basis $\{g_1, \dots, g_s\}$ is *reduced* if each g_i has leading coefficient 1 and if, for all i, no monomial of g_i lies in the ideal generated by the leading terms of the remaining g's. One can prove (Cox et al. 1992, p91) that every nonzero ideal has a *unique* reduced standard basis.

REMARK 0.16. Consider polynomials $f, g_1, \dots, g_s \in k[X_1, \dots, X_n]$. The algorithm that replaces $g_1, \dots, g_s$ with a standard basis works entirely within $k[X_1, \dots, X_n]$, i.e., it doesn't require a field extension. Likewise, the division algorithm doesn't require a field extension. Because these operations give well-defined answers, whether we carry them out in $k[X_1, \dots, X_n]$ or in $K[X_1, \dots, X_n]$, $K \supset k$, we get the same answer. Maple appears to work in the subfield of $\mathbb{C}$ generated over $\mathbb{Q}$ by all the constants occurring in the polynomials.

As we said earlier, the reader is referred to Cox et al. 1992 pp1–111 for more details on standard bases.

We conclude this section with the annotated transcript of a session in Maple applying the above algorithm to show that

$$q = 3x^3yz^2 - xz^2 + y^3 + yz$$

doesn't lie in the ideal

$$(x^2 - 2xz + 5, xy^2 + yz^3, 3y^2 - 8z^3).$$

A Maple Session

```
> with(grobner);
```

[This loads the grobner package, and lists the available commands:

`finduni, finite, gbasis, gsolve, leadmon, normalf, solvable, spoly`

To discover the syntax of a command, a brief description of the command, and an example, type "?command;"]

```
>G:=gbasis([x^2-2*x*z+5,x*y^2+y*z^3,3*y^2-8*z^3],[x,y,z]);
```

[This asks Maple to find the reduced Grobner basis for the ideal generated by the three polynomials listed, with respect to the indeterminates listed (in that order). It will automatically use grevlex order unless you add ,plex to the command.]

$G := [x^2 - 2xz + 5, -3y^2 + 8z^3, 8xy^2 + 3y^3, 9y^4 + 48zy^3 + 320y^2]$

```
> q:=3*x^3*y*z^2 - x*z^2 + y^3 + y*z;
```

$q := 3x^3yz^2 - xz^2 + y^3 + zy$

[This defines the polynomial q.]

```
> normalf(q,G,[x,y,z]);
```

$9z^2y^3 - 15yz^2x - \frac{41}{4}y^3 + 60y^2z - xz^2 + zy$

[Asks for the remainder when q is divided by the polynomials listed in G using the indeterminates listed. This particular example is amusing—the program gives different orderings for G, and different answers for the remainder, depending on which computer I use. This is O.K., because, since q isn't in the ideal, the remainder may depend on the ordering of G.]

Notes:

1. To start Maple on a Unix computer type "maple"; to quit type "quit".

2. Maple won't do anything until you type ";" or ":" at the end of a line.

3. The student version of Maple is quite cheap, but unfortunately, it doesn't have the Grobner package.

4. For more information on Maple:

(a) There is a brief discussion of the Grobner package in Cox et al. 1992, especially pp 487–489.

(b) The Maple V Library Reference Manual pp469–478 briefly describes what the Grobner package does (exactly the same information is available on line, by typing ?command).

(c) There are many books containing general introductions to Maple syntax.

5. Gröbner bases are also implemented in Macsyma, Mathematica, and Axiom, but for serious work it is better to use one of the programs especially designed for Gröbner basis computation, namely, **CoCoA** (Computations in Commutative Algebra) or **Macaulay** (available at: `ftp math.harvard.edu`, login `ftp`, password `any`, cd `Macaulay`; better, point your web browser to `ftp.math.harvard.edu`).

1. Algebraic Sets

We now take k to be an algebraically closed field.

Definition of an algebraic set. An *algebraic subset* $V(S)$ of k^n is the set of common zeros of some set S of polynomials in $k[X_1, \dots, X_n]$:

$$V(S) = \{(a_1, \dots, a_n) \in k^n \mid f(a_1, \dots, a_n) = 0 \text{ all } f(X_1, \dots, X_n) \in S\}.$$

Note that

$$S \subset S' \Rightarrow V(S) \supset V(S');$$

— the more equations we have, the fewer solutions.

Recall that the ideal $\mathfrak{a}$ generated by a set S consists of all finite sums

$$\sum f_i g_i, \quad f_i \in k[X_1, \dots, X_n], \quad g_i \in S.$$

Such a sum $\sum f_i g_i$ is zero at any point at which the g_i are zero, and so $V(S) \subset V(\mathfrak{a})$, but the reverse conclusion is also true because $S \subset \mathfrak{a}$. Thus $V(S) = V(\mathfrak{a})$—the zero set of S is the same as that of the ideal generated by S. Hence the algebraic sets can also be described as the sets of the form $V(\mathfrak{a})$, $\mathfrak{a}$ an ideal in $k[X_1, \dots, X_n]$.

Example 1.1. (a) If S is a system of homogeneous linear equations, then $V(S)$ is a subspace of k^n. If S is a system of nonhomogeneous linear equations, $V(S)$ is either empty or is the translate of a subspace of k^n.

(b) If S consists of the single equation

$$Y^2 = X^3 + aX + b, \quad 4a^3 + 27b^2 \neq 0,$$

then $V(S)$ is an *elliptic curve*. For more on elliptic curves, and their relation to Fermat's last theorem, see my notes on Elliptic Curves. The reader should sketch the curve for particular values of a and b. We generally visualize algebraic sets as though the field k were $\mathbb{R}$.

(c) If S is the empty set, then $V(S) = k^n$.

(d) The algebraic subsets of k are the finite subsets (including $\emptyset$) and k itself.

(e) Some generating sets for an ideal will be more useful than others for determining what the algebraic set is. For example, a Gröbner basis for the ideal

$$\mathfrak{a} = (X^2 + Y^2 + Z^2 - 1,\ X^2 + Y^2 - Y,\ X - Z)$$

is (according to Maple)

$$X - Z,\ Y^2 - 2Y + 1,\ Z^2 - 1 + Y.$$

The middle polynomial has (double) root 1, and it follows easily that $V(\mathfrak{a})$ consists of the single point $(0, 1, 0)$.

The Hilbert basis theorem. In our definition of an algebraic set, we didn't require the set S of polynomials to be finite, but the Hilbert basis theorem shows that every algebraic set will also be the zero set of a finite set of polynomials. More precisely, the theorem shows that every ideal in $k[X_1, \dots, X_n]$ can be generated by a finite set of elements, and we have already observed that any set of generators of an ideal has the same zero set as the ideal.

We sketched an algorithmic proof of the Hilbert basis theorem in the last section. Here we give the slick proof.

THEOREM 1.2 (Hilbert Basis Theorem). *The ring $k[X_1,\dots,X_n]$ is Noetherian, i.e., every ideal is finitely generated.*

PROOF. For $n = 1$, this is proved in advanced undergraduate algebra courses: $k[X]$ is a principal ideal domain, which means that every ideal is generated by a single element. We shall prove the theorem by induction on n. Note that the obvious map

$$k[X_1,\dots,X_{n-1}][X_n] \to k[X_1,\dots,X_n]$$

is an isomorphism—this simply says that every polynomial f in n variables $X_1,\dots,X_n$ can be expressed uniquely as a polynomial in X_n with coefficients in $k[X_1,\dots,X_{n-1}]$:

$$f(X_1,\dots,X_n) = a_0(X_1,\dots,X_{n-1})X_n^r + \cdots + a_r(X_1,\dots,X_{n-1}).$$

Thus the next lemma will complete the proof. □

LEMMA 1.3. *If A is Noetherian, then so also is $A[X]$.*

PROOF. For a polynomial

$$f(X) = a_0X^r + a_1X^{r-1} + \cdots + a_r, \quad a_i \in A, \quad a_0 \neq 0,$$

r is called the *degree* of f, and a_0 is its *leading coefficient*. We call 0 the leading coefficient of the polynomial 0.

Let $\mathfrak{a}$ be an ideal in $A[X]$. The leading coefficients of the polynomials in $\mathfrak{a}$ form an ideal $\mathfrak{a}'$ in A, and since A is Noetherian, $\mathfrak{a}'$ will be finitely generated. Let $g_1,\dots,g_m$ be elements of $\mathfrak{a}$ whose leading coefficients generate $\mathfrak{a}'$, and let r be the maximum degree of the g_i.

Now let $f \in \mathfrak{a}$, and suppose f has degree $s > r$, say, $f = aX^s + \cdots$. Then $a \in \mathfrak{a}'$, and so we can write

$$a = \sum b_ia_i, \quad b_i \in A, \quad a_i = \text{leading coefficient of } g_i.$$

Now

$$f - \sum b_ig_iX^{s-r_i}, \quad r_i = \deg(g_i),$$

has degree $< \deg(f)$. By continuing in this way, we find that

$$f \equiv f_t \mod (g_1,\dots,g_m)$$

with f_t a polynomial of degree $t < r$.

For each $d < r$, let $\mathfrak{a}_d$ be the subset of A consisting of 0 and the leading coefficients of all polynomials in $\mathfrak{a}$ of degree d; it is again an ideal in A. Let $g_{d,1},\dots,g_{d,m_d}$ be polynomials of degree d whose leading coefficients generate $\mathfrak{a}_d$. Then the same argument as above shows that any polynomial f_d in $\mathfrak{a}$ of degree d can be written

$$f_d \equiv f_{d-1} \mod (g_{d,1},\dots,g_{d,m_d})$$

with f_{d-1} of degree $\le d-1$. On applying this remark repeatedly we find that

$$f_t \in (g_{r-1,1},\dots,g_{r-1,m_{r-1}},\dots,g_{0,1},\dots,g_{0,m_0}).$$

Hence

$$f \in (g_1, \dots, g_m, g_{r-1,1}, \dots, g_{r-1,m_{r-1}}, \dots, g_{0,1}, \dots, g_{0,m_0}),$$

and so the polynomials $g_1, \dots, g_{0,m_0}$ generate $\mathfrak{a}$. □

ASIDE 1.4. One may ask how many elements are needed to generate an ideal $\mathfrak{a}$ in $k[X_1, \dots, X_n]$, or, what is not quite the same thing, how many equations are needed to define an algebraic set V. When $n = 1$, we know that every ideal is generated by a single element. Also, if V is a linear subspace of k^n, then linear algebra shows that it is the zero set of $n - \dim(V)$ polynomials. All one can say in general, is that *at least* $n - \dim(V)$ polynomials are needed to define V (see §6), but often more are required. Determining exactly how many is an area of active research. Chapter V of Kunz 1985 contains a good discussion of this problem.

The Zariski topology.

PROPOSITION 1.5. *There are the following relations:*

(a) $\mathfrak{a} \subset \mathfrak{b} \Rightarrow V(\mathfrak{a}) \supset V(\mathfrak{b})$;
(b) $V(0) = k^n$; $\quad V(k[X_1, \dots, X_n]) = \emptyset$;
(c) $V(\mathfrak{ab}) = V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$;
(d) $V(\sum \mathfrak{a}_i) = \cap V(\mathfrak{a}_i)$.

PROOF. The first two statements are obvious. For (c), note that

$$\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{a}, \mathfrak{b} \Rightarrow V(\mathfrak{ab}) \supset V(\mathfrak{a} \cap \mathfrak{b}) \supset V(\mathfrak{a}) \cup V(\mathfrak{b}).$$

For the reverse inclusions, observe that if $a \notin V(\mathfrak{a}) \cup V(\mathfrak{b})$, then there exist $f \in \mathfrak{a}$, $g \in \mathfrak{b}$ such that $f(a) \neq 0$, $g(a) \neq 0$; but then $(fg)(a) \neq 0$, and so $a \notin V(\mathfrak{ab})$. For (d) recall that, by definition, $\sum \mathfrak{a}_i$ consists of all finite sums of the form $\sum f_i$, $f_i \in \mathfrak{a}_i$. Thus (d) is obvious. □

Statements (b), (c), and (d) show that the algebraic subsets of k^n satisfy the axioms to be the closed subsets for a topology on k^n: both the whole space and the empty set are closed; a finite union of closed sets is closed; an arbitrary intersection of closed sets is closed. This topology is called the *Zariski topology*. It has many strange properties (for example, already on k one sees that it not Hausdorff), but it is nevertheless of great importance.

The closed subsets of k are just the finite sets and k. Call a *curve* in k^2 the set of zeros of a nonzero irreducible polynomial $f(X, Y) \in k[X, Y]$. Then we shall see in (1.25) below that, apart from k^2 itself, the closed sets in k^2 are finite unions of (isolated) points and curves. Note that the Zariski topologies on $\mathbb{C}$ and $\mathbb{C}^2$ are much coarser (have many fewer open sets) than the complex topologies.

The Hilbert Nullstellensatz. We wish to examine the relation between the algebraic subsets of k^n and the ideals of $k[X_1, \dots, X_n]$, but first we consider the question of when a set of polynomials has a common zero, i.e., when the equations

$$g(X_1, \dots, X_n) = 0, \quad g \in \mathfrak{a},$$

are "consistent". Obviously, equations

$$g_i(X_1, \dots, X_n) = 0, \quad i = 1, \dots, m$$

are inconsistent if there exist $f_i \in k[X_1, \dots, X_n]$ such that

$$\sum f_i g_i = 1,$$

i.e., if $1 \in (g_1, \dots, g_m)$ or, equivalently, $(g_1, \dots, g_m) = k[X_1, \dots, X_n]$. The next theorem provides a converse to this.

THEOREM 1.6 (Hilbert Nullstellensatz). *Every proper ideal $\mathfrak{a}$ in $k[X_1, \dots, X_n]$ has a zero in k^n.*

PROOF. A point $\mathbf{a} \in k^n$ defines a homomorphism "evaluate at $\mathbf{a}$"

$$k[X_1, \dots, X_n] \to k, \quad f(X_1, \dots, X_n) \mapsto f(a_1, \dots, a_n),$$

and clearly

$$\mathbf{a} \in V(\mathfrak{a}) \iff \mathfrak{a} \subset \text{ kernel of this map.}$$

Conversely, if $\varphi\colon k[X_1, \dots, X_n] \to k$ is a homomorphism of k-algebras such that $\operatorname{Ker}(\varphi) \supset \mathfrak{a}$, then

$$(a_1, \dots, a_n) \stackrel{\text{df}}{=} (\varphi(X_1), \dots, \varphi(X_n))$$

lies in $V(\mathfrak{a})$. Thus, to prove the theorem, we have to show that there exists a k-algebra homomorphism $k[X_1, \dots, X_n]/\mathfrak{a} \to k$.

Since every proper ideal is contained in a maximal ideal, it suffices to prove this for a maximal ideal $\mathfrak{m}$. Then $K \stackrel{\text{df}}{=} k[X_1, \dots, X_n]/\mathfrak{m}$ is a field, and it is finitely generated as an algebra over k (with generators $X_1 + \mathfrak{m}, \dots, X_n + \mathfrak{m}$). To complete the proof, we must show $K = k$. The next lemma accomplishes this. □

Although we shall apply the lemma only in the case that k is algebraically closed, in order to make the induction in its proof work, we need to allow arbitrary k's in the statement.

LEMMA 1.7 (Zariski's Lemma). *Let $k \subset K$ be fields (k not necessarily algebraically closed). If K is finitely generated as an algebra over k, then K is algebraic over k. (Hence $K = k$ if k is algebraically closed.)*

PROOF. We shall prove this by induction on r, the minimum number of elements required to generate K as a k-algebra. Suppose first that $r = 1$, so that $K = k[x]$ for some $x \in K$. Write $k[X]$ for the polynomial ring over k in the single variable X, and consider the homomorphism of k-algebras $k[X] \to K$, $X \mapsto x$. If x is not algebraic over k, then this is an isomorphism $k[X] \to K$, which contradicts the condition that K be a field. Therefore x is algebraic over k, and this implies that every element of $K = k[x]$ is algebraic over k (because it is finite over k).

For the general case, we need to use results about integrality (see the Appendix to this Section). Consider an integral domain A with field of fractions K, and a field L containing K. An element of L is said to be *integral* over A if it satisfies an equation of the form

$$X^n + a_1 X^{n-1} + \cdots + a_n = 0, \quad a_i \in A.$$

We shall need three facts:

(a) The elements of L integral over A form a subring of L.

(b) If $\beta \in L$ is algebraic over K, then $a\beta$ is integral over A for some $a \in A$.
(c) If A is a unique factorization domain, then every element of K that is integral over A lies in A.

Now suppose that K can be generated (as a k-algebra) by r elements, say, $K = k[x_1, \dots, x_r]$. If the conclusion of the lemma is false for K/k, then at least one x_i, say x_1, is not algebraic over k. Thus, as before, $k[x_1]$ is a polynomial ring in one variable over k ($\approx k[X]$), and its field of fractions $k(x_1)$ is a subfield of K. Clearly K is generated as a $k(x_1)$-algebra by $x_2, \dots, x_r$, and so the induction hypothesis implies that $x_2, \dots, x_r$ are algebraic over $k(x_1)$. From (b) we find there exist $d_i \in k[x_1]$ such that $d_i x_i$ is integral over $k[x_1]$, $i = 2, \dots, r$. Write $d = \prod d_i$.

Let $f \in K$; by assumption, f is a polynomial in the x_i with coefficients in k. For a sufficiently large N, $d^N f$ will be a polynomial in the $d_i x_i$. Then (a) implies that $d^N f$ is integral over $k[x_1]$. When we apply this to an element f of $k(x_1)$, (c) shows that $d^N f \in k[x_1]$. Therefore, $k(x_1) = \cup_N d^{-N} k[x_1]$, but this is absurd, because $k[x_1]$ ($\approx k[X]$) has infinitely many distinct irreducible polynomials[7] that can occur as denominators of elements of $k(x_1)$. □

The correspondence between algebraic sets and ideals. For a subset W of k^n, we write $I(W)$ for the set of polynomials that are zero on W:

$$I(W) = \{f \in k[X_1, \dots, X_n] \mid f(\mathbf{a}) = 0 \text{ all } \mathbf{a} \in W\}.$$

It is an ideal in $k[X_1, \dots, X_n]$. There are the following relations:

(a) $V \subset W \Rightarrow I(V) \supset I(W)$;
(b) $I(\emptyset) = k[X_1, \dots, X_n]$; $I(k^n) = 0$;
(c) $I(\cup W_i) = \cap I(W_i)$.

Only the statement $I(k^n) = 0$, i.e., that every nonzero polynomial is nonzero at some point of k^n, is nonobvious. It is not difficult to prove this directly by induction on the number of variables—in fact it's true for any infinite field k—but it also follows easily from the Nullstellensatz (see (1.11a) below).

EXAMPLE 1.8. Let P be the point $(a_1, \dots, a_n)$. Clearly $I(P) \supset (X_1 - a_1, \dots, X_n - a_n)$, but $(X_1 - a_1, \dots, X_n - a_n)$ is a maximal ideal, because "evaluation at $(a_1, \dots, a_n)$" defines an isomorphism

$$k[X_1, \dots, X_n]/(X_1 - a_1, \dots, X_n - a_n) \to k.$$

As $I(P) \neq k[X_1, \dots, X_n]$, we must have $I(P) = (X_1 - a_1, \dots, X_n - a_n)$.

The *radical* $\operatorname{rad}(\mathfrak{a})$ of an ideal $\mathfrak{a}$ is defined to be

$$\{f \mid f^r \in \mathfrak{a}, \text{ some } r \in \mathbb{N}, \quad r > 0\}.$$

It is again an ideal, and $\operatorname{rad}(\operatorname{rad}(\mathfrak{a})) = \operatorname{rad}(\mathfrak{a})$.

An ideal is said to be *radical* if it equals its radical, i.e., $f^r \in \mathfrak{a} \Rightarrow f \in \mathfrak{a}$. Equivalently, $\mathfrak{a}$ is radical if and only if $A/\mathfrak{a}$ is a *reduced* ring, i.e., a ring without nonzero nilpotent elements (elements some power of which is zero). Since an integral domain is reduced, a prime ideal (*a fortiori* a maximal ideal) is radical.

[7] If k is infinite, then consider the polynomials $X - a$, and if k is finite, consider the minimum polynomials of generators of the extension fields of k. Alternatively, and better, adapt Euclid's proof that there are infinitely many prime numbers.

If $\mathfrak{a}$ and $\mathfrak{b}$ are radical, then $\mathfrak{a}\cap\mathfrak{b}$ is radical, but $\mathfrak{a}+\mathfrak{b}$ need not be — consider, for example, $\mathfrak{a}=(X^2-Y)$ and $\mathfrak{b}=(X^2+Y)$; they are both prime ideals in $k[X,Y]$, but $X^2\in\mathfrak{a}+\mathfrak{b}$, $X\notin\mathfrak{a}+\mathfrak{b}$.

As $f^r(\mathbf{a})=f(\mathbf{a})^r$, f^r is zero wherever f is zero, and so $I(W)$ is radical. In particular, $IV(\mathfrak{a})\supset\operatorname{rad}(\mathfrak{a})$. The next theorem states that these two ideals are equal.

THEOREM 1.9 (Strong Hilbert Nullstellensatz). (a) *The ideal $IV(\mathfrak{a})$ is the radical of $\mathfrak{a}$; in particular, $IV(\mathfrak{a})=\mathfrak{a}$ if $\mathfrak{a}$ is a radical ideal.*

(b) *The set $VI(W)$ is the smallest algebraic subset of k^n containing W; in particular, $VI(W)=W$ if W is an algebraic set.*

PROOF. (a) We have already noted that $IV(\mathfrak{a})\supset\operatorname{rad}(\mathfrak{a})$. For the reverse inclusion, consider $h\in IV(\mathfrak{a})$; we have to show that some power of h belongs to $\mathfrak{a}$. We may assume $h\neq 0$ as $0\in\mathfrak{a}$. We are given that h is identically zero on $V(\mathfrak{a})$, and we have to show that $h^N\in\mathfrak{a}$ for some $N>0$. Let $g_1,\dots,g_m$ be a generating set for $\mathfrak{a}$, and consider the system of $m+1$ equations in $n+1$ variables, $X_1,\dots,X_n,Y$,

$$\begin{cases} g_i(X_1,\dots,X_n) &= 0, \quad i=1,\dots,m\\ 1-Yh(X_1,\dots,X_n) &= 0.\end{cases}$$

If $(a_1,\dots,a_n,b)$ satisfies the first m equations, then $(a_1,\dots,a_n)\in V(\mathfrak{a})$; consequently, $h(a_1,\dots,a_n)=0$, and $(a_1,\dots,a_n,b)$ doesn't satisfy the last equation. Therefore, the equations are inconsistent, and so, according to the original Nullstellensatz, there exist $f_i\in k[X_1,\dots,X_n,Y]$ such that

$$1=\sum_{i=1}^{m} f_ig_i+f_{m+1}\cdot(1-Yh).$$

On regarding this as an identity in the field $k(X_1,\dots,X_n,Y)$ and substituting $1/h$ for Y, we obtain the identity

$$1=\sum_{i=1}^{m} f_i(X_1,\dots,X_n,\frac{1}{h})\cdot g_i(X_1,\dots,X_n)$$

in $k(X_1,\dots,X_n)$. Clearly

$$f_i(X_1,\dots,X_n,\frac{1}{h})=\frac{\text{polynomial in } X_1,\dots,X_n}{h^{N_i}}$$

for some N_i. Let N be the largest of the N_i. On multiplying the identity by h^N we obtain an equation

$$h^N=\sum(\text{polynomial in } X_1,\dots,X_n)\cdot g_i(X_1,\dots,X_n),$$

which shows that $h^N\in\mathfrak{a}$.

(b) Let V be an algebraic set containing W, and write $V=V(\mathfrak{a})$. Then $\mathfrak{a}\subset I(W)$, and so $V(\mathfrak{a})\supset VI(W)$. □

COROLLARY 1.10. *The map $\mathfrak{a}\mapsto V(\mathfrak{a})$ defines a one-to-one correspondence between the set of radical ideals in $k[X_1,\dots,X_n]$ and the set of algebraic subsets of k^n; its inverse is I.*

PROOF. We know that $IV(\mathfrak{a})=\mathfrak{a}$ if $\mathfrak{a}$ is a radical ideal, and that $VI(W)=W$ if W is an algebraic set. □

REMARK 1.11. (a) Note that $V(0) = k^n$, and so

$$I(k^n) = IV(0) = \text{rad}(0) = 0,$$

as claimed above.

(b) The one-to-one correspondence in the corollary is order inverting. Therefore the maximal proper radical ideals correspond to the minimal nonempty algebraic sets. But the maximal proper radical ideals are simply the maximal ideals in $k[X_1, \dots, X_n]$, and the minimal nonempty algebraic sets are the one-point sets. As $I((a_1, \dots, a_n)) = (X_1 - a_1, \dots, X_n - a_n)$, this shows that the maximal ideals of $k[X_1, \dots, X_n]$ are precisely the ideals of the form $(X_1 - a_1, \dots, X_n - a_n)$.

(c) The algebraic set $V(\mathfrak{a})$ is empty if and only if $\mathfrak{a} = k[X_1, \dots, X_n]$, because $V(\mathfrak{a})$ empty $\Rightarrow \text{rad}(\mathfrak{a}) = k[X_1, \dots, X_n] \Rightarrow 1 \in \text{rad}(\mathfrak{a}) \Rightarrow 1 \in \mathfrak{a}$.

(d) Let W and W' be algebraic sets. Then $W \cap W'$ is the largest algebraic subset contained in both W and W', and so $I(W \cap W')$ must be the smallest radical ideal containing both $I(W)$ and $I(W')$. Hence $I(W \cap W') = \text{rad}(I(W) + I(W'))$.

For example, let $W = V(X^2 - Y)$ and $W' = V(X^2 + Y)$; then $I(W \cap W') = \text{rad}(X^2, Y) = (X, Y)$ (assuming characteristic $\neq 2$). Note that $W \cap W' = \{(0, 0)\}$, but when realized as the intersection of $Y = X^2$ and $Y = -X^2$, it has "multiplicity 2". [The reader should draw a picture.]

Finding the radical of an ideal. Typically, an algebraic set V will be defined by a finite set of polynomials $\{g_1, \dots, g_s\}$, and then we shall need to find $I(V) = \text{rad}((g_1, \dots, g_s))$.

PROPOSITION 1.12. *The polynomial $h \in \text{rad}(\mathfrak{a})$ if and only if $1 \in (\mathfrak{a}, 1 - Yh)$ (the ideal in $k[X_1, \dots, X_n, Y]$ generated by the elements of $\mathfrak{a}$ and $1 - Yh$).*

PROOF. We saw that $1 \in (\mathfrak{a}, 1 - Yh)$ implies $h \in \text{rad}(\mathfrak{a})$ in the course of proving (1.9). Conversely, if $h^N \in \mathfrak{a}$, then

$$\begin{aligned} 1 &= Y^N h^N + (1 - Y^N h^N) \\ &= Y^N h^N + (1 - Yh) \cdot (1 + Yh + \cdots + Y^{N-1} h^{N-1}) \in \mathfrak{a} + (1 - Yh). \end{aligned}$$

□

Thus we have an algorithm for deciding whether $h \in \text{rad}(\mathfrak{a})$, but not yet an algorithm for finding a set of generators for $\text{rad}(\mathfrak{a})$. There do exist such algorithms (see Cox et al. 1992, p177 for references), and one has been implemented in the computer algebra system Macaulay. To start Macaulay on most computers, type: `Macaulay`; type `<radical` to find out the syntax for finding radicals.

The Zariski topology on an algebraic set. We now examine the Zariski topology on k^n and on an algebraic subset of k^n more closely. The Zariski topology on $\mathbb{C}^n$ is much coarser than the complex topology. Part (b) of (1.9) says that, for each subset W of k^n, $VI(W)$ is the closure of W, and (1.10) says that there is a one-to-one correspondence between the closed subsets of k^n and the radical ideals of $k[X_1, \dots, X_n]$.

Let V be an algebraic subset of k^n, and let $I(V) = \mathfrak{a}$. Then the algebraic subsets of V correspond to the radical ideals of $k[X_1, \dots, X_n]$ containing $\mathfrak{a}$.

PROPOSITION 1.13. *Let V be an algebraic subset of k^n.*

(a) The points of V are closed for the Zariski topology (thus V is a T_1-space).

(b) Every descending chain of closed subsets of V becomes constant, i.e., given

$$V_1 \supset V_2 \supset V_3 \supset \cdots \qquad \text{(closed subsets of } V\text{)},$$

eventually $V_N = V_{N+1} = \dots$. Alternatively, every ascending chain of open sets becomes constant.

(c) Every open covering of V has a finite subcovering.

PROOF. (a) We have already observed that $\{(a_1, \dots, a_n)\}$ is the algebraic set defined by the ideal $(X_1 - a_1, \dots, X_n - a_n)$.

(b) A sequence $V_1 \supset V_2 \supset \cdots$ gives rise to a sequence of radical ideals $I(V_1) \subset I(V_2) \subset \dots$, which eventually becomes constant because $k[X_1, \dots, X_n]$ is Noetherian.

(c) Let $V = \bigcup_{i\in I} U_i$ with each U_i open. Choose an $i_0 \in I$; if $U_{i_0} \neq V$, then there exists an $i_1 \in I$ such that $U_{i_0} \subsetneqq U_{i_0} \cup U_{i_1}$. If $U_{i_0} \cup U_{i_1} \neq V$, then there exists an $i_2 \in I$ etc.. Because of (b), this process must eventually stop. □

A topological space having the property (b) is said to be *Noetherian*. The condition is equivalent to the following: every nonempty set of closed subsets of V has a minimal element. A space having property (c) is said to be *quasi-compact* (by Bourbaki at least; others call it compact, but Bourbaki requires a compact space to be Hausdorff).

The coordinate ring of an algebraic set. Let V be an algebraic subset of k^n, and let $I(V) = \mathfrak{a}$. An element $f(X_1, \dots, X_n)$ of $k[X_1, \dots, X_n]$ defines a mapping $k^n \to k$, $\mathbf{a} \mapsto f(\mathbf{a})$ whose restriction to V depends only on the coset $f + \mathfrak{a}$ of f in the quotient ring

$$k[V] = k[X_1, \dots, X_n]/\mathfrak{a} = k[x_1, \dots, x_n].$$

Moreover, two polynomials $f_1(X_1, \dots, X_n)$ and $f_2(X_1, \dots, X_n)$ restrict to the same function on V only if they define the same element of $k[V]$. Thus $k[V]$ can be identified with a ring of functions $V \to k$.

We call $k[V]$ the *ring of regular functions* on V, or the *coordinate ring of* V. It is a finitely generated reduced k-algebra (because $\mathfrak{a}$ is radical), but need not be an integral domain.

For an ideal $\mathfrak{b}$ in $k[V]$, we set

$$V(\mathfrak{b}) = \{\mathbf{a} \in V \mid f(\mathbf{a}) = 0, \text{ all } f \in \mathfrak{b}\}.$$

Let $W = V(\mathfrak{b})$. The maps

$$k[X_1, \dots, X_n] \to k[V] = \frac{k[X_1, \dots, X_n]}{\mathfrak{a}} \to k[W] = \frac{k[V]}{\mathfrak{b}}$$

should be regarded as restricting a function from k^n to V, and then restricting that function to W.

Write π for the map $k[X_1, \dots, X_n] \to k[V]$. Then $\mathfrak{b} \mapsto \pi^{-1}(\mathfrak{b})$ is a bijection from the set of ideals of $k[V]$ to the set of ideals of $k[X_1, \dots, X_n]$ containing $\mathfrak{a}$, under which radical, prime, and maximal ideals correspond to radical, prime, and

maximal ideals (each of these conditions can be checked on the quotient ring, and $k[X_1,\dots,X_n]/\pi^{-1}(\mathfrak{b}) \approx k[V]/\mathfrak{b}$). Clearly

$$V(\pi^{-1}(\mathfrak{b})) = V(\mathfrak{b}),$$

and so $\mathfrak{b} \mapsto V(\mathfrak{b})$ gives a bijection between the set of radical ideals in $k[V]$ and the set of algebraic sets contained in V.

For $h \in k[V]$, we write

$$D(h) = \{a \in V \mid h(a) \neq 0\}.$$

It is an open subset of V, because it is the complement of $V((h))$.

PROPOSITION 1.14. *(a) The points of V are in one-to-one correspondence with the maximal ideals of $k[V]$.*

(b) The closed subsets of V are in one-to-one correspondence with the radical ideals of $k[V]$.

(c) The sets $D(h)$, $h \in k[V]$, form a basis for the topology of V, i.e., each $D(h)$ is open, and each open set is a union (in fact, a finite union) of $D(h)$'s.

PROOF. (a) and (b) are obvious from the above discussion. For (c), we have already observed that $D(h)$ is open. Any other open set $U \subset V$ is the complement of a set of the form $V(\mathfrak{b})$, $\mathfrak{b}$ an ideal in $k[V]$. If $f_1,\dots,f_m$ generate $\mathfrak{b}$, then $U = \cup D(f_i)$. □

The $D(h)$ are called the *basic* (or *principal*) *open subsets* of V. We sometimes write V_h for $D(h)$. Note that $D(h) \subset D(h') \iff V(h) \supset V(h') \iff \operatorname{rad}((h)) \subset \operatorname{rad}((h')) \iff h^r \in (h')$ some $r \iff h^r = h'g$, some g.

Some of this should look familiar: if V is a topological space, then the zero set of a family of continuous functions $f\colon V \to \mathbb{R}$ is closed, and the set where such a function is nonzero is open.

Irreducible algebraic sets. A nonempty subset W of a topological space V is said to be *irreducible* if it satisfies any one of the following equivalent conditions:

(a) W is not the union of two proper closed subsets;
(b) any two nonempty open subsets of W have a nonempty intersection;
(c) any nonempty open subset of W is dense.

The equivalences (a) $\iff$ (b) and (b) $\iff$ (c) are obvious. Also, one sees that if W is irreducible, and $W = W_1 \cup \dots \cup W_r$ with each W_i closed, then $W = W_i$ for some i.

This notion is not useful for Hausdorff topological spaces, because such a space is irreducible only if it consists of a single point — otherwise any two points have disjoint open neighbourhoods, and so (b) fails.

PROPOSITION 1.15. *An algebraic set W is irreducible and only if $I(W)$ is prime.*

PROOF. $\Rightarrow$: Suppose $fg \in I(W)$. At each point of W, either f or g is zero, and so $W \subset V(f) \cup V(g)$. Hence

$$W = (W \cap V(f)) \cup (W \cap V(g)).$$

As W is irreducible, one of these sets, say $W \cap V(f)$, must equal W. But then $f \in I(W)$. Thus $I(W)$ is prime.

$\Longleftarrow$: Suppose $W = V(\mathfrak{a}) \cup V(\mathfrak{b})$ with $\mathfrak{a}$ and $\mathfrak{b}$ radical ideals—we have to show that W equals $V(\mathfrak{a})$ or $V(\mathfrak{b})$. Recall that $V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b})$, and that $\mathfrak{a} \cap \mathfrak{b}$ is radical; hence $I(W) = \mathfrak{a} \cap \mathfrak{b}$. If $W \neq V(\mathfrak{a})$, then there is an $f \in \mathfrak{a}$, $f \notin I(W)$. But $fg \in \mathfrak{a} \cap \mathfrak{b} = I(W)$ for all $g \in \mathfrak{b}$, and, because $f \notin I(W)$ and $I(W)$ is prime, this implies that $\mathfrak{b} \subset I(W)$; therefore $W \subset V(\mathfrak{b})$. □

Thus, there are one-to-one correspondences

$$\begin{aligned} \text{radical ideals} &\leftrightarrow \text{algebraic subsets} \\ \text{prime ideals} &\leftrightarrow \text{irreducible algebraic subsets} \\ \text{maximal ideals} &\leftrightarrow \text{one-point sets.} \end{aligned}$$

These correspondences are valid whether we mean ideals in $k[X_1, \dots, X_n]$ and algebraic subsets of k^n, or ideals in $k[V]$ and algebraic subsets of V. Note that the last correspondence implies that the maximal ideals in $k[V]$ are of the form $(x_1 - a_1, \dots, x_n - a_n)$, $(a_1, \dots, a_n) \in V$.

EXAMPLE 1.16. Let $f \in k[X_1, \dots, X_n]$. As we noted in §0, $k[X_1, \dots, X_n]$ is a unique factorization domain, and so (f) is a prime ideal $\iff$ f is irreducible. Thus

$$V(f) \text{ is irreducible} \iff f \text{ is irreducible.}$$

On the other hand, suppose f factors, $f = \prod f_i^{m_i}$, with the f_i distinct irreducible polynomials. Then $(f) = \cap(f_i^{m_i})$, $\operatorname{rad}((f)) = (\prod f_i) = \cap(f_i)$, and $V(f) = \cup V(f_i)$ with $V(f_i)$ irreducible.

PROPOSITION 1.17. *Let V be a Noetherian topological space. Then V is a finite union of irreducible closed subsets, $V = V_1 \cup \dots \cup V_m$. Moreover, if the decomposition is irredundant in the sense that there are no inclusions among the V_i, then the V_i are uniquely determined up to order.*

PROOF. Suppose the first assertion is false. Then, because V is Noetherian, there will be a closed subset W of V that is minimal among those that cannot be written as a finite union of irreducible closed subsets. But such a W cannot itself be irreducible, and so $W = W_1 \cup W_2$, with each W_i a proper closed subset of W. From the minimality of W, it follows that each W_i is a finite union of irreducible closed subsets, and so therefore is W. We have arrived at a contradiction.

Suppose that $V = V_1 \cup \dots \cup V_m = W_1 \cup \dots \cup W_n$ are two irredundant decompositions. Then $V_i = \cup_j (V_i \cap W_j)$, and so, because V_i is irreducible, $V_i \subset V_i \cap W_j$ for some j. Consequently, there is a function $f\colon \{1, \dots, m\} \to \{1, \dots, n\}$ such that $V_i \subset W_{f(i)}$ for each i. Similarly, there is a function $g\colon \{1, \dots, n\} \to \{1, \dots, m\}$ such that $W_j \subset V_{g(j)}$. Since $V_i \subset W_{f(i)} \subset V_{gf(i)}$, we must have $gf(i) = i$ and $V_i = W_{f(i)}$; similarly $fg = id$. Thus f and g are bijections, and the decompositions differ only in the numbering of the sets. □

The V_i given uniquely by the proposition are called the *irreducible components* of V. They are the maximal closed irreducible subsets of V. In Example 1.16, the $V(f_i)$ are the irreducible components of $V(f)$.

COROLLARY 1.18. *A radical ideal $\mathfrak{a}$ of $k[X_1, \dots, X_n]$ is a finite intersection of prime ideals, $\mathfrak{a} = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_n$; if there are no inclusions among the $\mathfrak{p}_i$, then the $\mathfrak{p}_i$ are uniquely determined up to order.*

PROOF. Write $V(\mathfrak{a}) = \cup V_i$, and take $\mathfrak{p}_i = I(V_i)$. □

REMARK 1.19. (a) In a Noetherian ring, every ideal $\mathfrak{a}$ has a decomposition into primary ideals: $\mathfrak{a} = \cap \mathfrak{q}_i$ (see Atiyah and MacDonald 1969, IV, VII). For radical ideals, this becomes a much simpler decomposition into prime ideals, as in the corollary.

(b) In $k[X]$, $(f(X))$ is radical if and only if f is square-free, in which case f is a product of distinct irreducible polynomials, $f = p_1 \dots p_r$, and $(f) = (p_1) \cap \dots \cap (p_r)$ (a polynomial is divisible by f if and only if it is divisible by each p_i).

(c) A Hausdorff space is Noetherian if and only if it is finite, in which case its irreducible components are the one-point sets.

Dimension. We briefly introduce the notion of the dimension of an algebraic variety. In Section 7 we shall discuss this in more detail.

Let V be an irreducible algebraic subset. Then $I(V)$ is a prime ideal, and so $k[V]$ is an integral domain. Let $k(V)$ be its field of fractions—$k(V)$ is called the *field of rational functions* on V. The *dimension* of V is defined to be the transcendence degree of $k(V)$ over k.

For those who know some commutative algebra, according to the last theorem in Atiyah and MacDonald 1969, this is equal to the Krull dimension of $k[V]$; we shall prove this later.

EXAMPLE 1.20. (a) Let $V = k^n$; then $k(V) = k(X_1, \dots, X_n)$, and so $\dim(V) = n$. Later we shall see that the Noether normalization theorem implies that V has dimension n if and only if there is a surjective finite-to-one map $V \to k^n$.

(b) If V is a linear subspace of k^n (or a translate of such a subspace), then it is an easy exercise to show that the dimension of V in the above sense is the same as its dimension in the sense of linear algebra (in fact, $k[V]$ is canonically isomorphic to $k[X_{i_1}, \dots, X_{i_d}]$ where the X_{i_j} are the "free" variables in the system of linear equations defining V).

In linear algebra, we justify saying V has dimension n by pointing out that its elements are parametrized by n-tuples; unfortunately, it is not true in general that the points of an algebraic set of dimension n are parametrized by n-tuples; the most one can say is that there is a finite-to-one map to k^n.

(c) An irreducible algebraic set has dimension 0 if and only if it consists of a single point. Certainly, for any point $P \in k^n$, $k[P] = k$, and so $k(P) = k$. Conversely, suppose $V = V(\mathfrak{p})$, $\mathfrak{p}$ prime, has dimension 0. Then $k(V)$ is an algebraic extension of k, and so equals k. From the inclusions

$$k \subset k[V] \subset k(V) = k$$

we see that $k[V] = k$. Hence $\mathfrak{p}$ is maximal, and we saw in (1.11b) that this implies that $V(\mathfrak{p})$ is a point.

The zero set of a single nonconstant nonzero polynomial $f(X_1, \dots, X_n)$ is called a *hypersurface* in k^n.

PROPOSITION 1.21. *An irreducible hypersurface in k^n has dimension $n - 1$.*

PROOF. Let $k[x_1, \dots, x_n] = k[X_1, \dots, X_n]/(f)$, $x_i = X_i + \mathfrak{p}$, and let $k(x_1, \dots, x_n)$ be the field of fractions of $k[x_1, \dots, x_n]$. Since $x_1, \dots, x_n$ generate $k(x_1, \dots, x_n)$ and

they are algebraically dependent, the transcendence degree must be $< n$ (because $\{x_1, \dots, x_n\}$ contains a transcendence basis — see 6.12 of my notes on Fields and Galois Theory). To see that it is not $< n-1$, note that if X_n occurs in f, then it occurs in all nonzero multiples of f, and so no nonzero polynomial in $X_1, \dots, X_{n-1}$ belongs to (f). This means that $x_1, \dots, x_{n-1}$ are algebraically independent. □

For a reducible algebraic set V, we define the *dimension* of V to be the maximum of the dimensions of its irreducible components. When these all have the same dimension d, we say that V has *pure dimension* d.

PROPOSITION 1.22. *If V is irreducible and Z is a proper closed subvariety of V, then* $\dim(Z) < \dim(V)$.

PROOF. We may assume that Z is irreducible. Then Z corresponds to a nonzero prime ideal $\mathfrak{p}$ in $k[V]$, and $k[Z] = k[V]/\mathfrak{p}$.

Suppose $V \subset k^n$, so that $k[V] = k[X_1, \dots, X_n]/I(V) = k[x_1, \dots, x_n]$. If X_i is regarded as a function on k^n, then its image x_i in $k[V]$ is the restriction of this function to V.

Let $f \in k[V]$. The image $\bar{f}$ of f in $k[V]/\mathfrak{p} = k[Z]$ can be regarded as the restriction of f to Z. With this notation, $k[Z] = k[\bar{x}_1, \dots, \bar{x}_n]$. Suppose that $\dim Z = d$ and that $\bar{x}_1, \dots, \bar{x}_d$ are algebraically independent. I will show that, for any nonzero $f \in \mathfrak{p}$, the $d+1$ elements $x_1, \dots, x_d, f$ are algebraically independent, which implies that $\dim V \geq d+1$.

Suppose otherwise. Then there is a nontrivial algebraic relation among the x_i and f, which we can write

$$a_0(x_1, \dots, x_d)f^m + a_1(x_1, \dots, x_d)f^{n-1} + \cdots + a_m(x_1, \dots, x_d) = 0,$$

with $a_i(x_1, \dots, x_d) \in k[x_1, \dots, x_d]$. Because the relation is nontrivial, at least one of the a_i is nonzero (in the polynomial ring $k[x_1, \dots, x_d]$). After cancelling by a power of f if necessary, we can assume $a_m(x_1, \dots, x_d) \neq 0$ (in this step, we use that $k[V]$ is an integral domain). On restricting the functions in the above equality to Z, i.e., applying the homomorphism $k[V] \to k[Z]$, we find that

$$a_m(\bar{x}_1, \dots, \bar{x}_d) = 0,$$

which contradicts the algebraic independence of $\bar{x}_1, \dots, \bar{x}_d$. □

EXAMPLE 1.23. Let $F(X,Y)$ and $G(X,Y)$ be nonconstant polynomials with no common factor. Then $V(F(X,Y))$ has dimension 1 by (1.21), and so $V(F(X,Y)) \cap V(G(X,Y))$ must have dimension zero; it is therefore a finite set.

REMARK 1.24. Later we shall show that if, in the situation of (1.22), Z is a *maximal* proper irreducible subset of V, then $\dim Z = \dim V - 1$. This implies that the dimension of an algebraic set V is the maximum length of a chain

$$V_0 \supsetneqq V_1 \supsetneqq \cdots \supsetneqq V_d$$

with each V_i closed and irreducible and V_0 an irreducible component of V. Note that this description of dimension is purely topological—it makes sense for any Noetherian topological space.

On translating the description in terms of ideals, we see immediately that the dimension of V is equal to the *Krull dimension* of $k[V]$—the maximal length of a chain of prime ideals,

$$\mathfrak{p}_d \supsetneqq \mathfrak{p}_{d-1} \supsetneqq \cdots \supsetneqq \mathfrak{p}_0.$$

EXAMPLE 1.25. We classify the irreducible closed subsets V of k^2. If V has dimension 2, then (by 1.22) it can't be a proper subset of k^2, so it is k^2. If V has dimension 1, then $V \neq k^2$, and so $I(V)$ contains a nonzero polynomial, and hence a nonzero irreducible polynomial f (being a prime ideal). Then $V \supset V(f)$, and so equals $V(f)$. Finally, if V has dimension zero, it is a point. Correspondingly, we can make a list of all the prime ideals in $k[X,Y]$: they have the form (0), (f) (with f irreducible), or $(X-a, Y-b)$.

Appendix A: Integrality. Throughout this subsection, A is an integral domain. An element α of a field L containing A is said to be *integral* over A if it is a root of a *monic* polynomial with coefficients in A, i.e., if it satisfies an equation

$$\alpha^n + a_1\alpha^{n-1} + \ldots + a_n = 0, \quad a_i \in A.$$

Before proving that the elements of L integral over A form a ring, we need to review symmetric polynomials.

Symmetric polynomials. A polynomial $P(X_1, ..., X_r) \in A[X_1, \ldots, X_r]$ is said to be *symmetric* if it is unchanged when its variables are permuted, i.e., if

$$P(X_{\sigma(1)}, \ldots, X_{\sigma(r)}) = P(X_1, \ldots, X_r), \quad \text{all } \sigma \in \mathrm{Sym}_r.$$

For example

$$S_1 = \sum X_i, \quad S_2 = \sum_{i<j} X_iX_j, \quad \ldots, \quad S_r = X_1 \cdots X_r,$$

are all symmetric. These particular polynomials are called the *elementary symmetric polynomials*.

THEOREM 1.26 (Symmetric function theorem). *Let A be a ring. Every symmetric polynomial $P(X_1, ..., X_r)$ in $A[X_1, ..., X_r]$ is equal to a polynomial in the symmetric elementary polynomials with coefficients in A, i.e., $P \in A[S_1, ..., S_r]$.*

PROOF. We define an ordering on the monomials in the X_i by requiring that

$$X_1^{i_1}X_2^{i_2}\cdots X_r^{i_r} > X_1^{j_1}X_2^{j_2}\cdots X_r^{j_r}$$

if either

$$i_1 + i_2 + \cdots + i_r > j_1 + j_2 + \cdots + j_r$$

or equality holds and, for some s,

$$i_1 = j_1, \quad \ldots, \quad i_s = j_s, \text{ but } i_{s+1} > j_{s+1}.$$

Let $X_1^{k_1}\cdots X_r^{k_r}$ be the highest monomial occurring in P with a coefficient $c \neq 0$. Because P is symmetric, it contains all monomials obtained from $X_1^{k_1}\cdots X_r^{k_r}$ by permuting the X's. Hence $k_1 \geq k_2 \geq \cdots \geq k_r$.

Clearly, the highest monomial in S_i is $X_1 \cdots X_i$, and it follows that the highest monomial in $S_1^{d_1} \cdots S_r^{d_r}$ is

$$X_1^{d_1+d_2+\cdots+d_r} X_2^{d_2+\cdots+d_r} \cdots X_r^{d_r}.$$

Therefore

$$P(X_1, \dots, X_r) - cS_1^{k_1-k_2} S_2^{k_2-k_3} \cdots S_r^{k_r} < P(X_1, \dots, X_r).$$

We can repeat this argument with the polynomial on the left, and after a finite number of steps, we will arrive at a representation of P as a polynomial in $S_1, \dots, S_r$. (For more details, see Jacobson, Basic Algebra I, 2.20, p139.) □

Let $f(X) = X^n + a_1X^{n-1} + \cdots + a_n \in A[X]$, and let $\alpha_1, \dots, \alpha_n$ be the roots of $f(X)$ in some ring containing A, i.e., $f(X) = \prod(X - \alpha_i)$. Then

$$a_1 = -S_1(\alpha_1, \dots, \alpha_n), \quad a_2 = S_2(\alpha_1, \dots, \alpha_n), \quad \dots, \quad a_n = \pm S_n(\alpha_1, \dots, \alpha_n).$$

Thus the *elementary* symmetric polynomials in the roots of $f(X)$ lie in A, and so the theorem implies that *every* symmetric polynomial in the roots of $f(X)$ lie in A.

Integral elements.

THEOREM 1.27. *The set of elements of L integral over A forms a ring.*

PROOF. Let α and β be integral over A; we have to show that $\alpha \pm \beta$ and $\alpha\beta$ are integral over A. Let Ω be an algebraically closed field containing L.

We are given that α is a root of a polynomial $f(X) = X^m + a_1X^{m-1} + \cdots + a_m$, $a_i \in A$. Write

$$f(X) = \prod(X - \alpha_i),\ \alpha_i \in \Omega.$$

Similarly, β is a root of polynomial $g(X) = X^n + b_1X^{n-1} + \dots + b_n$, $b_i \in A$, and we write

$$f(X) = \prod(X - \beta_i),\ \beta_i \in \Omega.$$

Let $\gamma_1, \gamma_2, \dots, \gamma_{mn}$ be the family of numbers of the form $\alpha_i + \beta_j$ (or $\alpha_i - \beta_j$, or $\alpha_i\beta_j$). I claim that

$$h(X) \stackrel{\text{df}}{=} \prod_{1 \le i \le m,\ 1 \le j \le n} (X - \gamma_{ij})$$

has coefficients in A. This will prove that $\alpha+\beta$ is integral over A because $h(\alpha+\beta) = 0$.

The coefficients of h are symmetric in the α_i and β_j. Let $P(\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n)$ be one of these coefficients, and regard it as a polynomial $Q(\beta_1, \dots, \beta_n)$ in the β's with coefficients in $A[\alpha_1, \dots, \alpha_m]$; then its coefficients are symmetric in the α_i, and so lie in A. Thus $P(\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n)$ is a symmetric polynomial in the β's with coefficients in A—it therefore lies in A, as claimed. □

DEFINITION 1.28. The ring of elements of L integral over A is called the *integral closure* of A in L.

PROPOSITION 1.29. *Let K be the field of fractions of A, and let L be a field containing K. If $\alpha \in L$ is algebraic over K, then there exists a $d \in A$ such that $d\alpha$ is integral over A.*

PROOF. By assumption, α satisfies an equation

$$\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0,\ a_i \in K.$$

Let d be a common denominator for the a_i, so that $da_i \in A$, all i, and multiply through the equation by d^m:

$$d^m\alpha^m + a_1d^m\alpha^{m-1} + \cdots + a_md^m = 0.$$

We can rewrite this as

$$(d\alpha)^m + a_1d(d\alpha)^{m-1} + \cdots + a_md^m = 0.$$

As $a_1d, \dots, a_md^m \in A$, this shows that $d\alpha$ is integral over A. □

COROLLARY 1.30. *Let A be an integral domain with field of fractions K, and let L be an algebraic extension of K. If B is the integral closure of A in L, then L is the field of fractions of B.*

PROOF. The proposition shows that every $\alpha \in L$ can be written $\alpha = \beta/d$ with $\beta \in B$, $d \in A$. □

DEFINITION 1.31. A ring A is *integrally closed* if it is its own integral closure in its field of fractions K, i.e., if

$$\alpha \in K, \quad \alpha \text{ integral over } A \Rightarrow \alpha \in A.$$

PROPOSITION 1.32. *A unique factorization domain (e.g. a principal ideal domain) is integrally closed.*

PROOF. Suppose a/b, $a, b \in A$, is an element of the field of fractions of A and is integral over A. If b is a unit, then $a/b \in A$. Otherwise we may suppose that there is an irreducible element p of A dividing b but not a. As a/b is integral over A, it satisifies an equation

$$(a/b)^n + a_1(a/b)^{n-1} + \cdots + a_n = 0,\ a_i \in A.$$

On multiplying through by b^n, we obtain the equation

$$a^n + a_1a^{n-1}b + \ldots + a_nb^n = 0.$$

The element p then divides every term on the left except a^n, and hence must divide a^n. Since it doesn't divide a, this is a contradiction. □

PROPOSITION 1.33. *Let K be the field of fractions of A, and let L be an extension of K of finite degree. Assume A is integrally closed. An element α of L is integral over A if and only if its minimum polynomial over K has coefficients in A.*

PROOF. Assume α is integral over A, so that

$$\alpha^m + a_1\alpha^{m-1} + \ldots + a_m = 0, \quad \text{some } a_i \in A.$$

Let α' be a conjugate of α, i.e., a root of the minimum polynomial of α over K. Then there is an K-isomorphism[8]

$$\sigma\colon K[\alpha] \to K[\alpha'], \quad \sigma(\alpha) = \alpha'.$$

[8]If $f(X)$ is the minimum polynomial of α, hence also of α', over K, then the map $h(X) \mapsto h(\alpha) : K[X] \to K[\alpha]$ induces an isomorphism $\tau : K[X]/(f(X)) \to K[\alpha]$. Similarly, $h(X) \mapsto h(\alpha') : K[X] \to K[\alpha']$ induces an isomorphism $\tau' : K[X]/(f(X)) \to K[\alpha']$, and we set $\sigma = \tau' \circ \tau^{-1}$.

On applying σ to the above equation we obtain the equation

$$\alpha'^m + a_1\alpha'^{m-1} + ... + a_m = 0,$$

which shows that α' is integral over A. Hence all the conjugates of α are integral over A, and it follows from (1.27) that the coefficients of $f(X)$ are integral over A. They lie in K, and A is integrally closed, and so they lie in A. This proves the "only if" part of the statement, and the "if" part is obvious. □

Appendix B: Transcendence degree. I have deleted this subsection from the notes since it was merely a copy of Section 6 of my notes Fields and Galois Theory.

2. Affine Algebraic Varieties

In this section we define on an algebraic set the structure of a ringed space, and then we define the notion of affine algebraic variety—roughly speaking, this is an algebraic set with no preferred embedding into k^n. This is in preparation for §3, where we define an algebraic variety to be a ringed space that is a finite union of affine algebraic varieties satisfying a natural separation axiom (in the same way that a topological manifold is a union of subsets homeomorphic to open subsets of $\mathbb{R}^n$ satisfying the Hausdorff axiom).

Ringed spaces. Let V be a topological space and k a field.

Definition 2.1. Suppose that for every open subset U of V we have a set $\mathcal{O}_V(U)$ of functions $U \to k$. Then $\mathcal{O}_V$ is called a *sheaf of k-algebras* if it satisfies the following conditions:

(a) $\mathcal{O}_V(U)$ is an k-subalgebra of the algebra of all functions $U \to k$, i.e., for each $c \in k$, the constant function c is in $\mathcal{O}_V(U)$, and if $f, g \in \mathcal{O}_V(V)$, then so also do $f \pm g$, and fg.
(b) If U' is an open subset of U and $f \in \mathcal{O}_V(U)$, then $f|U' \in \mathcal{O}_V(U')$.
(c) Let $U = \cup U_\alpha$ be an open covering of an open subset U of V; then a function $f\colon U \to k$ is in $\mathcal{O}_V(U)$ if $f|U_\alpha \in \mathcal{O}_V(U_\alpha)$ for all α (i.e., the condition for f to be in $\mathcal{O}_V(U)$ is *local*.

Example 2.2. (a) Let V be any topological space, and for each open subset U of V let $\mathcal{O}_V(U)$ be the set of all continuous real-valued functions on U. Then $\mathcal{O}_V$ is a sheaf of $\mathbb{R}$-algebras.

(b) Recall that a function $f\colon U \to \mathbb{R}$, where U is an open subset of $\mathbb{R}^n$, is said to be C^∞ (or *infinitely differentiable*) if its partial derivatives of all orders exist and are continous. Let V be an open subset of $\mathbb{R}^n$, and for each open subset U of V let $\mathcal{O}_V(U)$ be the set of all infinitely differentiable functions on U. Then $\mathcal{O}_V$ is a sheaf of $\mathbb{R}$-algebras.

(c) Recall that a function $f\colon U \to \mathbb{C}$, where U is an open subset of $\mathbb{C}^n$, is said to be *analytic* (or *holomorphic*) if it is described by a convergent power series in a neighbourhood of each point of U. Let V be an open subset of $\mathbb{C}^n$, and for each open subset U of V let $\mathcal{O}_V(U)$ be the set of all analytic functions on U. Then $\mathcal{O}_V$ is a sheaf of $\mathbb{C}$-algebras.

(d) Nonexample: let V be a topological space, and for each open subset U of V let $\mathcal{O}_V(U)$ be the set of all real-valued constant functions on U; then $\mathcal{O}_V$ is not a sheaf, unless V is irreducible! If "constant" is replaced with "locally constant", then $\mathcal{O}_V$ becomes a sheaf of $\mathbb{R}$-algebras (in fact, the smallest such sheaf).

A pair $(V, \mathcal{O}_V)$ consisting of a topological space V and a sheaf of k-algebras will be called a *ringed space.* For historical reasons, we often write $\Gamma(U, \mathcal{O}_V)$ for $\mathcal{O}_V(U)$ and call its elements *sections* of $\mathcal{O}_V$ over U.

Let $(V, \mathcal{O}_V)$ be a ringed space. For any open subset U of V, the restriction $\mathcal{O}_V|U$ of $\mathcal{O}_V$ to U, defined by

$$\Gamma(U', \mathcal{O}_V|U) = \Gamma(U', \mathcal{O}_V), \text{ all open } U' \subset U,$$

is a sheaf again.

Let $(V, \mathcal{O}_V)$ be ringed space, and let $P \in V$. Consider pairs (f, U) consisting of an open neighbourhood U of P and an $f \in \mathcal{O}_V(U)$. We write $(f, U) \sim (f', U')$ if $f|U'' = f'|U''$ for some $U'' \subset U \cap U'$. This is an equivalence relation, and an equivalence class of pairs is called a *germ* of a function at P. The set of equivalence classes of such pairs forms a k-algebra denoted $\mathcal{O}_{V,P}$ or $\mathcal{O}_P$. In all the interesting cases, it is a local ring with maximal ideal the set of germs that are zero at P.

In a fancier terminology,

$$\mathcal{O}_P = \varinjlim \mathcal{O}_V(U), \text{ (direct limit over open neighbourhoods } U \text{ of } P).$$

EXAMPLE 2.3. Let $V = \mathbb{C}$, and let $\mathcal{O}_V$ be the sheaf of holomorphic functions on $\mathbb{C}$. For $c \in \mathbb{C}$, call a power series $\sum_{n\geq 0} a_n(z-c)^n$, $a_n \in \mathbb{C}$, *convergent* if it converges on some neighbourhood of c. The set of such power series is a $\mathbb{C}$-algebra, and I claim that it is canonically isomorphic to the ring of germs of functions $\mathcal{O}_c$. From basic complex analysis, we know that if f is a holomorphic function on a neighbourhood U of c, then f has a power series expansion $f = \sum a_n(z-c)^n$ in some (possibly smaller) neighbourhood. Moreover another pair (g, U') will define the same power series if and only if g agrees with f on some neighbourhood of c contained in $U \cap U'$. Thus we have injective map from the ring of germs of holomorphic functions at c to the ring of convergent power series, and it is obvious that it is an isomorphism.

Review of rings of fractions. Before defining the sheaf of regular functions on an algebraic set, we need to review some of the theory of rings of fractions. When the initial ring is an integral domain (the most important case), the theory is very easy because all the rings are subrings of the field of fractions.

A *multiplicative subset* of a ring A is a subset S with the property:

$$1 \in S, \quad a, b \in S \Rightarrow ab \in S.$$

Define an equivalence relation on $A \times S$ by

$$(a, s) \sim (b, t) \iff u(at - bs) = 0 \text{ for some } u \in S.$$

Write $\frac{a}{s}$ for the equivalence class containing (a, s), and define addition and multiplication in the obvious way:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \quad \frac{a}{s}\frac{b}{t} = \frac{ab}{st}.$$

We then obtain a ring $S^{-1}A = \{\frac{a}{s} \mid a \in A, s \in S\}$, and a canonical homomorphism $a \mapsto \frac{a}{1} \colon A \to S^{-1}A$, not necessarily injective. For example, if S contains 0, then $S^{-1}A$ is the zero ring.

Write i for the homomorphism $a \mapsto \frac{a}{1} \colon A \to S^{-1}A$. Then $(S^{-1}A, i)$ has the following universal property: every element $s \in S$ maps to a unit in $S^{-1}A$, and any other homomorphism $\alpha \colon A \to B$ with this property factors uniquely through i:

$$\begin{array}{ccc} A & \xrightarrow{i} & S^{-1}A \\ & \searrow^{\alpha} & \vdots\ \exists! \\ & & \downarrow \\ & & B. \end{array}$$

The uniqueness is obvious—the map $S^{-1}A \to B$ must be $\frac{a}{s} \mapsto \alpha(a)\cdot\alpha(s)^{-1}$ — and it is easy to check that this formula does define a homomorphism $S^{-1}A \to B$. For example, to see that it is well-defined, note that

$$\frac{a}{c} = \frac{b}{d} \Rightarrow s(ad-bc) = 0 \text{ some } s \in S \Rightarrow \alpha(a)\alpha(d) - \alpha(b)\alpha(c) = 0,$$

because $\alpha(s)$ is a unit in B, and so

$$\alpha(a)\alpha(c)^{-1} = \alpha(b)\alpha(d)^{-1}.$$

As usual, this universal property determines the pair $(S^{-1}A, i)$ uniquely up to a unique isomorphism.

In the case that A is an integral domain we can form the field of fractions $F = S^{-1}A$, $S = A - \{0\}$, and then for any other multiplicative subset S of A not containing 0, $S^{-1}A$ can be identified with $\{\frac{a}{s} \in F \mid a \in A,\ s \in S\}$.

We shall be especially interested in the following examples.

(i) Let $h \in A$. Then $S_h \stackrel{\text{df}}{=} \{1, h, h^2, \dots\}$ is a multiplicative subset of A, and we write $A_h = S_h^{-1}A$. Thus every element of A_h can be written in the form a/h^m, $a \in A$, and

$$\frac{a}{h^m} = \frac{b}{h^n} \iff h^N(ah^n - bh^m) = 0, \text{ some } N.$$

In the case that A is an integral domain, with field of fractions F, A_h is the subring of F of elements of the form a/h^m, $a \in A$, $m \in \mathbb{N}$.

(ii) Let $\mathfrak{p}$ be a prime ideal in A. Then $S_{\mathfrak{p}} \stackrel{\text{df}}{=} A \smallsetminus \mathfrak{p}$ is a multiplicative subset of A, and we write $A_{\mathfrak{p}} = S_{\mathfrak{p}}^{-1}A$. Thus each element of $A_{\mathfrak{p}}$ can be written in the form $\frac{a}{c}$, $c \notin \mathfrak{p}$, and

$$\frac{a}{c} = \frac{b}{d} \iff s(ad-bc) = 0, \text{ some } s \notin \mathfrak{p}.$$

The subset $\mathfrak{m} = \{\frac{\mathfrak{a}}{\mathfrak{s}} \mid a \in \mathfrak{p},\ s \notin \mathfrak{p}\}$ is a maximal ideal in $A_{\mathfrak{p}}$, and it is the only maximal ideal [9] . Therefore $A_{\mathfrak{p}}$ is a local ring. Again, when A is an integral domain with field of fractions F, $A_{\mathfrak{p}}$ is the subring of F consisting of elements expressible in the form $\frac{a}{s}$, $a \in A$, $s \notin \mathfrak{p}$.

LEMMA 2.4. *For any ring A, the map $\sum a_iX^i \mapsto \sum \frac{a_i}{h^i}$ defines an isomorphism*

$$A[X]/(1-hX) \xrightarrow{\approx} A_h.$$

PROOF. In the ring $A[x] = A[X]/(1-hX)$, $1 = hx$, and so h is a unit. Consider a homomorphism of rings $\alpha\colon A \to B$ such that $\alpha(h)$ is a unit in B. Then α extends to a homomorphism

$$\sum a_iX^i \mapsto \sum \alpha(a_i)\alpha(h)^{-i}\colon A[X] \to B.$$

Under this homomorphism $1 - hX \mapsto 1 - \alpha(h)\alpha(h)^{-1} = 0$, and so the map factors through $A[x]$. The resulting homomorphism $\gamma\colon A[x] \to B$ has the property that its composite with $A \to A[x]$ is α, and (because $hx = 1$ in $A[x]$) it is the unique

[9] First check $\mathfrak{m}$ is an ideal. Next, if $\mathfrak{m} = A_{\mathfrak{p}}$, then $1 \in \mathfrak{m}$; but $1 = \frac{a}{s}$, $a \in \mathfrak{p}$, $s \notin \mathfrak{p}$ means $u(s-a) = 0$ some $u \notin \mathfrak{p}$, and so $a = us \notin \mathfrak{p}$. Finally, $\mathfrak{m}$ is maximal, because any element of $A_{\mathfrak{p}}$ not in $\mathfrak{m}$ is a unit.

homomorphism with this property. Therefore $A[x]$ has the same universal property as A_h, and so the two are (uniquely) isomorphic by an isomorphism that makes h^{-1} correspond to x. □

For more on rings of fractions, see Atiyah and MacDonald 1969, Chapt 3.

The ringed space structure on an algebraic set. We now take k to be an algebraically closed field. Let V be an algebraic subset of k^n. An element h of $k[V]$ defines functions

$$\mathbf{a} \mapsto h(\mathbf{a}) \colon V \to k, \text{ and } \mathbf{a} \mapsto 1/h(\mathbf{a}) \colon D(h) \to k.$$

Thus a pair of elements $g, h \in k[V]$ with $h \neq 0$ defines a function

$$\mathbf{a} \mapsto \frac{g(\mathbf{a})}{h(\mathbf{a})} \colon D(h) \to k.$$

We say that a function $f \colon U \to k$ on an open subset U of V is *regular* if it is of this form in a neighbourhood of each of its points, i.e., if for all $\mathbf{a} \in U$, there exist $g, h \in k[V]$ with $h(\mathbf{a}) \neq 0$ such that the functions f and $\frac{g}{h}$ agree in a neighbourhood of $\mathbf{a}$. Write $\mathcal{O}_V(U)$ for the set of regular functions on U.

For example, if $V = k^n$, then a function $f \colon U \to k$ is regular at a point $\mathbf{a} \in U$ if there are polynomials $g(X_1, \dots, X_n)$ and $h(X_1, \dots, X_n)$ with $h(\mathbf{a}) \neq 0$ and $f(\mathbf{b}) = \frac{g(\mathbf{b})}{h(\mathbf{b})}$ for all $\mathbf{b}$ such that the expression on the right is defined.

PROPOSITION 2.5. *The map $U \mapsto \mathcal{O}_V(U)$ defines a sheaf of k-algebras on V.*

PROOF. We have to check the conditions (2.1).

(a) Clearly, a constant function is regular. Suppose f and f' are regular on U, and let $\mathbf{a} \in U$. By assumption, there exist $g, g', h, h' \in k[V]$, with $h(\mathbf{a}) \neq 0 \neq h'(\mathbf{a})$ such that f and f' agree with $\frac{g}{h}$ and $\frac{g'}{h'}$ respectively near $\mathbf{a}$. Then ff' agrees with $\frac{gh'+g'h}{hh'}$ near $\mathbf{a}$, and so ff' is regular on U. Similarly $f \pm f'$ are regular on U. Thus $\mathcal{O}_V(U)$ is a k-algebra.

(b) It is clear from the definition that the restriction of a regular function to an open subset is again regular.

(c) The condition for f to be regular is obviously local. □

LEMMA 2.6. *The element g/h^m of $k[V]_h$ defines the zero function on $D(h)$ if and only if $gh = 0$ (in $k[V]$) (and hence $g/h^m = 0$ in $k[V]_h$).*

PROOF. If g/h^m is zero on $D(h)$, then gh is zero on V because h is zero on the complement of $D(h)$. Therefore gh is zero in $k[V]$. Conversely, if $gh = 0$, then $g(\mathbf{a})h(\mathbf{a}) = 0$ for all $\mathbf{a} \in k^n$, and so $g(\mathbf{a}) = 0$ for all $\mathbf{a} \in D(h)$. □

PROPOSITION 2.7. *(a) The canonical map $k[V]_h \to \mathcal{O}_V(D(h))$ is an isomorphism.*

(b) For any $\mathbf{a} \in V$, there is a canonical isomorphism $\mathcal{O}_\mathbf{a} \to k[V]_{\mathfrak{m}_\mathbf{a}}$, where $\mathfrak{m}_\mathbf{a}$ is the maximal ideal $(x_1 - a_1, \dots, x_n - a_n)$.

PROOF. (a) The preceding lemma shows that $k[V]_h \to \mathcal{O}_V(D(h))$ is injective, and so it remains to show that every regular function f on $D(h)$ arises from an element of $k[V]_h$.

By definition, we know that there is an open covering $D(h) = \cup V_i$ and elements g_i, $h_i \in k[V]$ with h_i nowhere zero on V_i such that $f|V_i = \frac{g_i}{h_i}$. Since the sets of the form $D(a)$ form a basis for the topology on V, we can assume that $V_i = D(a_i)$, some $a_i \in k[V]$. By assumption $D(a_i) \subset D(h_i)$, and so $a_i^N = h_i g_i'$ for some $h_i' \in k[V]$ (see paragraph after 1.14). On $D(a_i)$, $f = \frac{g_i}{h_i} = \frac{g_i g_i'}{h_i g_i'} = \frac{g_i g_i'}{a_i^N}$. Note that $D(a_i^N) = D(a_i)$. Therefore, after replacing g_i with $g_i g_i'$ and h_i with a_i^N, we can suppose that $V_i = D(h_i)$.

We now have that $D(h) = \cup D(h_i)$ and that $f|D(h_i) = \frac{g_i}{h_i}$. Because $D(h)$ is quasicompact[10], we can assume that the covering is finite. As $\frac{g_i}{h_i} = \frac{g_j}{h_j}$ on $D(h_i) \cap D(h_j) = D(h_i h_j)$, we have (by the lemma) that

$$h_i h_j (g_i h_j - g_j h_i) = 0. \qquad (*)$$

Because $D(h) = \cup D(h_i) = \cup D(h_i^2)$, $V((h)) = V((h_1^2, \dots, h_m^2))$, and so there exist $a_i \in k[V]$ such that

$$h^N = \sum a_i h_i^2. \qquad (**)$$

I claim that f is the function on $D(h)$ defined by $\frac{\sum a_i g_i h_i}{h^N}$.

Let $\mathbf{a}$ be a point of $D(h)$. Then $\mathbf{a}$ will be in one of the $D(h_i)$, say $D(h_j)$. We have the following equalities in $k[V]$:

$$\begin{aligned} h_j^2 \sum_{i=1}^n a_i g_i h_i &= \sum_{i=1}^n a_i g_j h_i^2 h_j \qquad \text{by } (*) \\ &= g_j h_j h^N \qquad \text{by } (**). \end{aligned}$$

But $f|D(h_j) = \frac{g_j}{h_j}$, i.e., $f h_j$ and g_j agree as functions on $D(h_j)$. Therefore we have the following equality of functions on $D(h_j)$:

$$h_j^2 \sum a_i g_i h_i = f h_j^2 h^N.$$

Since h_j^2 is never zero on $D(h_j)$, we can cancel it, to find that, as claimed, the function $f h^N$ on $D(h_j)$ equals that defined by $\sum a_i g_i h_i$.

(b) First a general observation: in the definition of the germs of a sheaf at $\mathbf{a}$, it suffices to consider pairs (f, U) with U lying in a fixed basis for the neighbourhoods of $\mathbf{a}$. Thus each element of $\mathcal{O}_\mathbf{a}$ is represented by a pair $(f, D(h))$ where $h(\mathbf{a}) \neq 0$ and $f \in k[V]_h$, and two pairs $(f_1, D(h_1))$ and $(f_2, D(h_2))$ represent the same element of $\mathcal{O}_\mathbf{a}$ if and only if f_1 and f_2 restrict to the same function on $D(h)$ for some $\mathbf{a} \in D(h) \subset D(h_1 h_2)$.

For each $h \notin \mathfrak{p}$, there is a canonical homomorphism $\alpha_h \colon k[V]_h \to k[V]_\mathfrak{p}$, and we map the element of $\mathcal{O}_\mathbf{a}$ represented by $(f, D(h))$ to $\alpha_h(f)$. It is now an easy exercise to check that this map is well-defined, injective, and surjective. □

The proposition gives us an explicit description of the value of $\mathcal{O}_V$ on any basic open set and of the ring of germs at any point $\mathbf{a}$ of V. When V is irreducible, this

[10]Recall (1.13) that V is Noetherian, i.e., has the ascending chain condition on open subsets. This implies that any open subset of V is also Noetherian, and hence is quasi-compact.

becomes a little simpler because all the rings are subrings of $k(V)$. We have:

$$\begin{aligned}\Gamma(D(h),\mathcal{O}_V) &= \{\frac{g}{h^N}\in k(V)\mid g\in k[V],\quad N\in\mathbb{N}\};\\ \mathcal{O}_{\mathbf{a}} &= \{\frac{g}{h}\in k(V)\mid h(\mathbf{a})\neq 0\};\\ \Gamma(U,\mathcal{O}_V) &= \cap\mathcal{O}_{\mathbf{a}}\text{ (intersection over all }\mathbf{a}\in U\}\\ &= \cap\Gamma(D(h_i),\mathcal{O}_V)\text{ if }U=\cup D(h_i).\end{aligned}$$

Note that every element of $k(V)$ defines a function on some nonempty open subset of V . Following tradition, we call the elements of $k(V)$ *rational functions* on V (even though they are not functions on V). The last equality then says that the regular functions on U are the rational functions on V that are defined at each point of U.

EXAMPLE 2.8. (a) Let $V=k^n$. Then the ring of regular functions on V, $\Gamma(V,\mathcal{O}_V)$, is $k[X_1,\dots,X_n]$. For any nonzero polynomial $h(X_1,\dots,X_n)$, the ring of regular functions on $D(h)$ is

$$\{\frac{g}{h^N}\in k(X_1,\dots,X_n)\mid g,h\in k[X_1,\dots,X_n]\}.$$

For any point $\mathbf{a}=(a_1,\dots,a_n)$, the ring of germs of functions at $\mathbf{a}$ is

$$\mathcal{O}_{\mathbf{a}}=\{\frac{g}{h}\in k(X_1,\dots,X_n)\mid h(\mathbf{a})\neq 0\}=k[X_1,\dots,X_n]_{(X_1-a_1,\dots,X_n-a_n)},$$

and its maximal ideal consists of those g/h with $g(\mathbf{a})=0$.

(b) Let $U=\{(a,b)\in k^2\mid (a,b)\neq(0,0)\}$. It is an open subset of k^2, but it is not a basic open subset, because its complement $\{(0,0)\}$ has dimension 0, and therefore can't be of the form $V((f))$ (see 1.21). Since $U=D(X)\cup D(Y)$, the ring of regular functions on U is

$$\Gamma(D(X),\mathcal{O})\cap\Gamma(D(Y),\mathcal{O})=k[X,Y]_X\cap k[X,Y]_Y.$$

Thus (as an element of $k(X,Y)$), a regular function on U can be written

$$f=\frac{g(X,Y)}{X^N}=\frac{h(X,Y)}{Y^M}.$$

Since $k[X,Y]$ is a unique factorization domain, we can assume that the fractions are in their lowest terms. On multiplying through by X^NY^M, we find that

$$g(X,Y)Y^M=h(X,Y)X^N.$$

Because X doesn't divide the left hand side, it can't divide the right either, and so $N=0$. Similarly, $M=0$, and so $f\in k[X,Y]$: every regular function on U extends to a regular function on k^2.

Morphisms of ringed spaces. A *morphism of ringed spaces* $(V,\mathcal{O}_V)\to(W,\mathcal{O}_W)$ is a continuous map $\varphi\colon V\to W$ such that

$$f\in\mathcal{O}_W(U)\Rightarrow f\circ\varphi\in\mathcal{O}_V(\varphi^{-1}U)$$

for all open subsets U of W. Sometimes we write $\varphi^*(f)$ for $f\circ\varphi$. If U is an open subset of V, then the inclusion $(U,\mathcal{O}_V|V)\hookrightarrow(V,\mathcal{O}_V)$ is a morphism of ringed spaces. A morphism of ringed spaces is an *isomorphism* if it is bijective and its inverse is also a morphism of ringed spaces (in particular, it is a homeomorphism).

EXAMPLE 2.9. (a) Let V and V' be topological spaces endowed with their sheaves $\mathcal{O}_V$ and $\mathcal{O}_{V'}$ of continuous real valued functions. Any continuous map $\varphi\colon V \to V'$ is a morphism of ringed structures $(V, \mathcal{O}_V) \to (V', O_{V'})$.

(b) Let U and U' be open subsets of $\mathbb{R}^n$ and $\mathbb{R}^m$ respectively. Recall from advanced calculus that a mapping

$$\varphi = (\varphi_1, \dots, \varphi_m)\colon U \to U' \subset \mathbb{R}^m$$

is said to be infinitely differentiable (or C^∞) if each φ_i is infinitely differentiable, in which case $f \circ \varphi$ is infinitely differentiable for every infinitely differentiable function $f\colon U' \to \mathbb{R}$. Note that $\varphi_i = x_i \circ \varphi$, where x_i is the coordinate function $(a_1, \dots, a_n) \mapsto a_i$.

Let V and V' be open subsets of $\mathbb{R}^n$ and $\mathbb{R}^m$ respectively, endowed with their sheaves of infinitely differentiable functions $\mathcal{O}_V$ and $\mathcal{O}_{V'}$. The above statements show that a continuous map $\varphi\colon V \to V'$ is infinitely differentiable if and only if it is a morphism of ringed spaces.

(c) Same as (b), but replace $\mathbb{R}$ with $\mathbb{C}$ and "infinitely differentiable" with "analytic".

REMARK 2.10. A morphism of ringed spaces maps germs of functions to germs of functions. More precisely, a morphism $\varphi\colon (V, \mathcal{O}_V) \to (V', \mathcal{O}_{V'})$ induces a map

$$\mathcal{O}_{V,P} \leftarrow \mathcal{O}_{V',\varphi(P)},$$

namely, $[(f, U)] \mapsto [(f \circ \varphi, \varphi^{-1}(U))]$.

Affine algebraic varieties. We have just seen that every algebraic set gives rise to a ringed space $(V, \mathcal{O}_V)$. We define an *affine algebraic variety over k* to be a ringed space that is isomorphic to a ringed space of this form. A *morphism of affine algebraic varieties* is a morphism of ringed spaces; we often call it a *regular map* $V \to W$ or a *morphism* $V \to W$, and we write $\mathrm{Mor}(V, W)$ for the set of such morphisms. With these definitions, the affine algebraic varieties become a category. Since we consider no nonalgebraic affine varieties, we shall often drop the "algebraic".

In particular, every algebraic set has a natural structure of an affine variety. We usually write $\mathbb{A}^n$ for k^n regarded as an affine algebraic variety. Note that the affine varieties we have constructed so far have all been embedded in $\mathbb{A}^n$. We shall now see how to construct "unembedded" affine varieties.

A reduced finitely generated k-algebra is called an *affine k-algebra*. For such an algebra A, there exist $x_i \in A$ (not necessarily algebraically independent), such that $A = k[x_1, \dots, x_n]$, and the kernel of the homomorphism

$$X_i \mapsto x_i\colon k[X_1, \dots, X_n] \to A$$

is a radical ideal. Zariski's Lemma 1.7 implies that, for any maximal ideal $\mathfrak{m} \in A$, the map $k \to A \to A/\mathfrak{m}$ is an isomorphism. Thus we can identify $A/\mathfrak{m}$ with k. For $f \in A$, we write $f(\mathfrak{m})$ for the image of f in $A/\mathfrak{m} = k$, i.e., $f(\mathfrak{m}) = f \pmod{\mathfrak{m}}$.

We can associate with any affine k-algebra A a ringed space $(V, \mathcal{O}_V)$. First, V is the set of maximal ideals in A. For $h \in A$, $h \neq 0$, let

$$D(h) = \{\mathfrak{m} \mid h(\mathfrak{m}) \neq 0, \text{ i.e., } h \notin \mathfrak{m}\},$$

and endow V with the topology for which the $D(h)$ form a basis. A pair of elements $g, h \in A$, $h \neq 0$, defines a function

$$\mathfrak{m} \mapsto \frac{g(\mathfrak{m})}{h(\mathfrak{m})} \colon D(h) \to k,$$

and we call a function $f \colon U \to k$ on an open subset U of V *regular* if it is of this form on a neighbourhood of each point of U. Write $\mathcal{O}_V(U)$ for the set of regular functions on U.

PROPOSITION 2.11. *The pair $(V, \mathcal{O}_V)$ is an affine variety with $\Gamma(V, \mathcal{O}_V) = A$.*

PROOF. Represent A as a quotient $k[X_1, \dots, X_n]/\mathfrak{a} = k[x_1, \dots, x_{\mathfrak{n}}]$. Then the map

$$(a_1, \dots, a_n) \mapsto (x_1 - a_1, \dots, x_n - a_n) \qquad \text{(ideal in } A\text{)}$$

is a bijection $\varphi \colon V(\mathfrak{a}) \to V$ with inverse

$$\mathfrak{m} \mapsto (x_1(\mathfrak{m}), \dots, x_n(\mathfrak{m})) \colon V \to V(\mathfrak{a}) \subset k^{\mathfrak{n}}.$$

It is easy to check that this is a homeomorphism, and that a function f on an open subset of V is regular (according to the above definition) if and only if $f \circ \varphi$ is regular. □

We write $\operatorname{specm}(A)$ for the topological space V, and $\operatorname{Specm}(A)$ for the ringed space $(V, \mathcal{O}_V)$. If we start with an affine variety V and let $A = \Gamma(V, \mathcal{O}_V)$, then the $\operatorname{Specm}(A) \approx (V, \mathcal{O}_V)$ (canonically). We again write $k[V]$ for $\Gamma(V, \mathcal{O}_V)$, the ring of functions regular on the whole of V.

Thus, for each affine k-algebra A, we have an affine variety $\operatorname{Specm}(A)$, and conversely, for each affine variety $(V, \mathcal{O}_V)$, we have an affine k-algebra $\Gamma(V, \mathcal{O}_V)$. We now make this correspondence into an equivalence of categories.

REMARK 2.12. I claim that a radical ideal $\mathfrak{a}$ in $k[X_1, \dots, X_n]$ is equal to the intersection of the maximal ideals containing it. Indeed, the maximal ideals in $k[X_1, \dots, X_n]$ are all of the form $\mathfrak{m}_{\mathbf{a}} = (X_1 - a_1, \dots, X_n - a_n)$, and $f \in \mathfrak{m}_{\mathbf{a}} \iff f(\mathbf{a}) = 0$. Thus $\mathfrak{m}_{\mathbf{a}} \supset \mathfrak{a} \iff \mathbf{a} \in V(\mathfrak{a})$, and if $f \in \mathfrak{m}_{\mathbf{a}}$ for all $\mathbf{a} \in V(\mathfrak{a})$, then f is zero on $V(\mathfrak{a})$, i.e., $f \in IV(\mathfrak{a}) = \mathfrak{a}$.

This remark implies that, for any affine k-algebra A, the intersection of the maximal ideals of A is zero, because A is isomorphic to a k-algebra $k[X_1, \dots, X_n]/\mathfrak{a}$ and we can apply the remark to $\mathfrak{a}$. Hence the map that associates with $f \in A$ the map $\mathit{specm} A \to k$, $\mathfrak{m} \mapsto f(\mathfrak{m})$, is injective: A can be identified with a ring of functions on $\operatorname{specm} A$.

The category of affine algebraic varieties. Let $\alpha \colon A \to B$ be a homomorphism of affine k-algebras. For any $h \in A$, $\alpha(h)$ is invertible in $B_{\alpha(h)}$, and so the homomorphism $A \to B \to B_{\alpha(h)}$ extends to a homomorphism

$$\frac{g}{h^m} \mapsto \frac{\alpha(g)}{\alpha(h)^m} \colon A_h \to B_{\alpha(h)}.$$

For any maximal ideal $\mathfrak{n}$ of B, $\mathfrak{m} \overset{\text{df}}{=} \alpha^{-1}(\mathfrak{n})$ is maximal in A, because $A/\mathfrak{m} \to B/\mathfrak{n} = k$ is an injective map of k-algebras and this implies $A/\mathfrak{m} = k$. Thus α defines a map

$$\varphi \colon \operatorname{specm} B \to \operatorname{specm} A, \quad \varphi(\mathfrak{n}) = \alpha^{-1}(\mathfrak{n}) = \mathfrak{m}.$$

For $\mathfrak{m} = \alpha^{-1}(\mathfrak{n}) = \varphi(\mathfrak{n})$, we have a commutative diagram:

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ \downarrow & & \downarrow \\ A/\mathfrak{m} & \xrightarrow{=} & A/n. \end{array}$$

Recall that the image of an element f of A in $A/\mathfrak{m} = k$ is denoted $f(\mathfrak{m})$. Therefore, the commutativity of the diagram means that, for $f \in A$,

$$f(\varphi(\mathfrak{n})) = \alpha(f)(\mathfrak{n}), \text{ i.e., } f \circ \varphi = \alpha. \qquad (*).$$

Since $\varphi^{-1}D(f) = D(f \circ \varphi)$ (obviously), it follows from (*) that

$$\varphi^{-1}(D(f)) = D(\alpha(f)),$$

and so φ is continuous.

Let f be a regular function on $D(h)$, and write $f = g/h^m$, $g \in A$. Then, from (*) we see that $f \circ \varphi$ is the function on $D(\alpha(h))$ defined by $\alpha(g)/\alpha(h)^m$. In particular, it is regular, and so $f \mapsto f \circ \varphi$ maps regular functions on $D(h)$ to regular functions on $D(\alpha(h))$. It follows that $f \mapsto f \circ \varphi$ sends regular functions on any open subset of $\operatorname{specm}(A)$ to regular functions on the inverse image of the open subset. Thus α defines a morphism $\operatorname{Specm}(B) \to \operatorname{Specm}(A)$.

Conversely, by definition, a morphism of $\varphi\colon (V, \mathcal{O}_V) \to (W, \mathcal{O}_W)$ of affine algebraic varieties defines a homomorphism of the associated affine k-algebras $k[W] \to k[V]$. Since these maps are inverse, we have shown:

PROPOSITION 2.13. *For any affine algebras A and B,*

$$\operatorname{Hom}_{k\text{-}alg}(A, B) \xrightarrow{\approx} \operatorname{Mor}(\operatorname{Specm}(B), \operatorname{Specm}(A));$$

for any affine varieties V and W,

$$Mor(V, W) \xrightarrow{\approx} \operatorname{Hom}_{k\text{-}alg}(k[W], k[V]).$$

A covariant functor $F\colon \mathbf{A} \to \mathbf{B}$ of categories is said to be an *equivalence of categories* if

(a) for all objects A, A' of $\mathbf{A}$,

$$\operatorname{Hom}(A, A') \to \operatorname{Hom}(F(A), F(A'))$$

is a bijection (F is fully faithful);

(b) every object of $\mathbf{B}$ is isomorphic to an object of the form $F(A)$, $A \in \operatorname{Ob}(\mathbf{A})$ (*F* is essentially surjective).

One can show that such a functor F has a *quasi-inverse*, i.e., there is a functor $G\colon \mathbf{B} \to \mathbf{A}$, which is also an equivalence, and is such that $G(F(A)) \approx A$ (functorially) and $F(G(B)) \approx B$ (functorially). Hence the relation of equivalence is an equivalence relation. (In fact one can do better—see, for example, Bucur and Deleanu, Introduction to the Theory of Categories and Functors, 1968, I.6.)

Similarly one defines the notion of a contravariant functor being an equivalence of categories. Proposition 2.13 can now be restated in stronger form as:

PROPOSITION 2.14. *The functor $A \mapsto \operatorname{Specm} A$ is a (contravariant) equivalence from the category of affine k-algebras to that of affine varieties with quasi-inverse $(V, \mathcal{O}_V) \mapsto \Gamma(V, \mathcal{O}_V)$.*

Explicit description of morphisms of affine varieties.

PROPOSITION 2.15. *Let $V = V(\mathfrak{a}) \subset k^{\mathfrak{m}}$, $W = V(\mathfrak{b}) \subset k^{\mathfrak{n}}$. The following conditions on a continuous map $\varphi\colon V \to W$ are equivalent:*

(a) *φ is regular;*
(b) *the components $\varphi_1, \dots, \varphi_m$ of φ are all regular;*
(c) *$f \in k[W] \Rightarrow f \circ \varphi \in k[V]$.*

PROOF. (a) $\Rightarrow$ (b). By definition $\varphi_i = y_i \circ \varphi$ where y_i is the coordinate function $(b_1, \dots, b_n) \mapsto b_i\colon W \to k$. Hence this implication follows directly from the definition of a regular map.

(b) $\Rightarrow$ (c). The map $f \mapsto f \circ \varphi$ is a k-algebra homomorphism from the ring of all functions $W \to k$ to the ring of all functions $V \to k$, and (b) says that the map sends the coordinate functions y_i on W into $k[V]$. Since the y_i's generate $k[W]$ as a k-algebra, this implies that this map sends $k[W]$ into $k[V]$.

(c) $\Rightarrow$ (a). The map $f \mapsto f \circ \varphi$ is a homomorphism $\alpha\colon k[W] \to k[V]$. It therefore defines a map $\operatorname{specm} k[V] \to \operatorname{specm} k[W]$, and it remains to show that this coincides with φ when we identify $\operatorname{specm} k[V]$ with V and $\operatorname{specm} k[W]$ with W. Let $\mathbf{a} \in V$, let $\mathbf{b} = \varphi(\mathbf{a})$, and let $\mathfrak{m}_{\mathbf{a}}$ and $\mathfrak{m}_{\mathbf{b}}$ be the ideals of elements of $k[V]$ and $k[W]$ that are zero at $\mathbf{a}$ and $\mathbf{b}$ respectively. Then, for $f \in k[W]$,

$$\alpha(f) \in \mathfrak{m}_{\mathbf{a}} \iff f(\varphi(\mathbf{a})) = 0 \iff f(\mathbf{b}) = 0 \iff f \in \mathfrak{m}_{\mathbf{b}}.$$

Therefore $\alpha^{-1}(\mathfrak{m}_{\mathbf{a}}) = \mathfrak{m}_{\mathbf{b}}$, which is what we needed to show. □

REMARK 2.16. For all $\mathbf{a} \in V$, $f \mapsto f \circ \varphi$ maps germs of regular functions at $\varphi(\mathbf{a})$ to germs of regular functions at $\mathbf{a}$; in fact, it induces a local homomorphism $\mathcal{O}_{V,\varphi(\mathbf{a})} \to \mathcal{O}_{V,\mathbf{a}}$.

Now consider equations

$$\begin{aligned} Y_1 &= P_1(X_1, \dots, X_m) \\ &\dots \\ Y_n &= P_n(X_1, \dots, X_m). \end{aligned}$$

On the one hand, they define a mapping $\varphi\colon k^m \to k^n$, namely,

$$(a_1, \dots, a_m) \mapsto (P_1(a_1, \dots, a_m), \dots, P_n(a_1, \dots, a_m)).$$

On the other, they define a homomorphism of k-algebras $\alpha\colon k[Y_1, \dots, Y_n] \to k[X_1, \dots, X_n]$, namely, that sending

$$Y_i \mapsto P_i(X_1, \dots, X_n).$$

This map coincides with $f \mapsto f \circ \varphi$, because

$$\alpha(f)(\mathbf{a}) = f(\dots, P_i(\mathbf{a}), \dots) = f(\varphi(\mathbf{a})).$$

Now consider closed subsets $V(\mathfrak{a}) \subset k^{\mathfrak{m}}$ and $V(\mathfrak{b}) \subset k^{\mathfrak{n}}$ with $\mathfrak{a}$ and $\mathfrak{b}$ radical ideals. I claim that φ maps $V(\mathfrak{a})$ into $V(\mathfrak{b})$ if and only if $\alpha(\mathfrak{b}) \subset \mathfrak{a}$. Indeed, suppose $\varphi(V(\mathfrak{a})) \subset V(\mathfrak{b})$, and let $f \in \mathfrak{b}$; for $\mathbf{b} \in V(\mathfrak{b})$,

$$\alpha(f)(\mathbf{b}) = f(\varphi(\mathbf{b})) = 0,$$

and so $\alpha(f) \in IV(\mathfrak{b}) = \mathfrak{b}$. Conversely, suppose $\alpha(\mathfrak{b}) \subset \mathfrak{a}$, and let $\mathbf{a} \in V(\mathfrak{a})$; for $f \in \mathfrak{a}$,

$$f(\varphi(\mathbf{a})) = \alpha(f)(\mathbf{a}) = 0,$$

and so $\varphi(\mathbf{a}) \in V(\mathfrak{a})$. When these conditions hold, φ is the morphism of affine varieties $V(\mathfrak{a}) \to V(\mathfrak{b})$ corresponding to the homomorphism $k[Y_1, \dots, Y_m]/\mathfrak{b} \to k[X_1, \dots, X_{\mathfrak{n}}]/\mathfrak{a}$ defined by α.

Thus, we see that the morphisms

$$V(\mathfrak{a}) \to V(\mathfrak{b})$$

are all of the form

$$\mathbf{a} \mapsto (P_1(\mathbf{a}), \dots, P_m(\mathbf{a})), \quad P_i \in k[X_1, \dots, X_n].$$

EXAMPLE 2.17. (a) Consider a k-algebra R. From a k-algebra homomorphism $\alpha\colon k[X] \to R$, we obtain an element $\alpha(X) \in R$, and $\alpha(X)$ determines α completely. Moreover, $\alpha(X)$ can be any element of R. Thus

$$\alpha \mapsto \alpha(X)\colon \operatorname{Hom}_{k-\text{alg}}(k[X], R) \xrightarrow{\approx} R.$$

According to (2.13)

$$\operatorname{Mor}(V, \mathbb{A}^1) = \operatorname{Hom}_{k\text{-alg}}(k[X], k[V]).$$

Thus the regular maps $V \to \mathbb{A}^1$ are simply the regular functions on V (as we would hope).

(b) Define $\mathbb{A}^0$ to be the ringed space $(V_0, \mathcal{O}_{V_0})$ with V_0 consisting of a single point, and $\Gamma(V_0, \mathcal{O}_{V_0}) = k$. Equivalently, $\mathbb{A}^0 = \operatorname{Specm} k$. Then, for any affine variety V,

$$\operatorname{Mor}(\mathbb{A}^0, V) \cong \operatorname{Hom}_{k\text{-alg}}(k[V], k) \cong V$$

where the last map sends α to the point corresponding to the maximal ideal $\operatorname{Ker}(\alpha)$.

(c) Consider $t \mapsto (t^2, t^3)\colon \mathbb{A}^1 \to \mathbb{A}^2$. This is bijective onto its image, the variety $V\colon Y^2 = X^3$, but it is not an isomorphism onto its image — the inverse map is not a morphism. Because of (2.14), it suffices to show that $t \mapsto (t^2, t^3)$ doesn't induce an isomorphism on the rings of regular functions. We have $k[\mathbb{A}^1] = k[T]$ and $k[V] = k[X, Y]/(Y^2 - X^3) = k[x, y]$. The map on rings is

$$x \mapsto T^2, \quad y \mapsto T^3, \quad k[x, y] \to k[T],$$

which is injective, but the image is $k[T^2, T^3] \neq k[T]$. In fact, $k[x, y]$ is not integrally closed: $(y/x)^2 - x = 0$, and so (y/x) is integral over $k[x, y]$, but $y/x \notin k[x, y]$ (it maps to T under the inclusion $k(x, y) \hookrightarrow k(T)$).

(d) Assume that k has characteristic $p \neq 0$, and consider $x \mapsto x^p\colon \mathbb{A}^n \to \mathbb{A}^n$. This is a bijection, but it is not an isomorphism because the corresponing map on rings,

$$X_i \mapsto X_i^p\colon k[X_1, \dots, X_n] \to k[X_1, \dots, X_n],$$

is not surjective.

This map is the famous *Frobenius map.* Take k to be the algebraic closure of $\mathbb{F}_p$, the field with p elements, and write F for the map. Then the fixed points of F^m are precisely the points of $\mathbb{A}^n$ with coordinates in $\mathbb{F}_{p^m}$, the field with p^m-elements (recall from Galois theory that $\mathbb{F}_{p^m}$ is the subfield of k consisting of those elements satisfying the equation $X^{p^m} = X$). Let $P(X_1, \dots, X_n)$ be a polynomial with coefficients in $\mathbb{F}_{p^m}$, $P = \sum c_\alpha X^\alpha$, $c_\alpha \in \mathbb{F}_{p^m}$. If $P(\mathbf{a}) = 0$, $\mathbf{a} \in k^n$, i.e., $\sum c_\alpha a_1^{i_1} \cdots a_n^{i_n} = 0$, then

$$0 = \left(\sum c_\alpha a_1^{i_1} \cdots a_n^{i_n}\right)^{p^m} = \sum c_\alpha a_1^{p^m i_1} \cdots a_n^{p^m i_n},$$

and so $P(F^m\mathbf{a}) = 0$. Thus F^m maps $V(P)$ into $V(P)$, and its fixed points are the solutions of

$$P(X_1, \dots, X_n) = 0$$

in $\mathbb{F}_{p^m}$.

In one of the most beautiful pieces of mathematics of the last fifty years, Grothendieck defined a cohomology theory (étale cohomology) that allowed him to obtain an expression for the number of solutions of a system of polynomial equations with coordinates in $\mathbb{F}_{p^n}$ in terms of a Lefschetz fixed point formula, and Deligne used the theory to obtain very precise estimates for the number of solutions. See my course notes: Lectures on Etale Cohomology.

Subvarieties. For any ideal $\mathfrak{a}$ in A, we define

$$\begin{aligned} V(\mathfrak{a}) &= \{P \in \operatorname{specm} A \mid f(P) = 0 \text{ all } f \in \mathfrak{a}\} \\ &= \{\mathfrak{m} \text{ maximal ideal in } A \mid \mathfrak{a} \subset \mathfrak{m}\}. \end{aligned}$$

This is a closed subset of $\operatorname{specm} A$, and every closed subset is of this form.

Now assume $\mathfrak{a}$ is radical, so that $A/\mathfrak{a}$ is again reduced. Corresponding to the homomorphism $A \to A/\mathfrak{a}$, we get a regular map

$$\operatorname{Specm} A/\mathfrak{a} \to \operatorname{Specm} AA$$

The image is $V(\mathfrak{a})$, and $\operatorname{specm} A/\mathfrak{a} \to V(\mathfrak{a})$ is a homeomorphism. Thus every closed subset of $\operatorname{specm} A$ has a natural ringed structure making it into an affine algebraic variety. We call $V(\mathfrak{a})$ with this structure a *closed subvariety* of V.

Aside 2.18. If $(V, \mathcal{O}_V)$ is a ringed space, and Z is a closed subset of V, we can define a ringed space structure on Z as follows: let U be an open subset of Z, and let f be a function $U \to k$; then $f \in \Gamma(U, \mathcal{O}_Z)$ if for each $P \in U$ there is a germ (U', f') of a function at P (regarded as a point of V) such that $f'|Z \cap U' = f$. One can check that when this construction is applied to $Z = V(\mathfrak{a})$, the ringed space structure obtained is that described above.

Proposition 2.19. *Let $(V, \mathcal{O}_V)$ be an affine variety and let $h \in k[V]$, $h \neq 0$. Then $(D(h), \mathcal{O}_V|D(h))$ is an affine variety; in fact if $V = \operatorname{specm}(A)$, then $D(h) = \operatorname{specm}(A_h)$. More explicitly, if $V = V(\mathfrak{a}) \subset k^{\mathfrak{n}}$, then*

$$(a_1, \dots, a_n) \mapsto (a_1, \dots, a_n, h(a_1, \dots, a_n)^{-1}) \colon D(h) \to k^{n+1},$$

defines an isomorphism of $D(h)$ onto $V(\mathfrak{a}, 1 - hX_{n+1})$.

Proof. The map $A \to A_h$ defines a morphism $\operatorname{specm} A_h \to \operatorname{specm} A$. The image is $D(h)$, and it is routine (using (2.4)) to verify the rest of the statement. □

For example, there is an isomorphism of affine varieties

$$x \mapsto (x, 1/x)\colon \mathbb{A}^1 - \{0\} \to V \subset \mathbb{A}^2,$$

where V is the subvariety $XY = 1$ of $\mathbb{A}^2$ — the reader should draw a picture.

REMARK 2.20. We have seen that all closed subsets, and all basic open subsets, of an affine variety V are again affine varieties, but it need not be true that $(U, \mathcal{O}_V|U)$ is an affine variety when U open in V. Note that if $(U, \mathcal{O}_V|U)$ is an affine variety, then we must have $(U, \mathcal{O}_V) \cong \operatorname{Specm}(A)$, $A = \Gamma(U, \mathcal{O}_V)$. In particular, the map

$$P \mapsto \mathfrak{m}_P = \{f \in A \mid f(P) = 0\}$$

will be a bijection from U onto $\operatorname{specm}(A)$.

Consider $U \subset \mathbb{A}^2 \setminus (0,0) = D(X) \cup D(Y)$. We saw in (2.8b) that $\Gamma(U, \mathcal{O}_{\mathbb{A}^2}) = k[X, Y]$. Now $U \to \operatorname{specm} k[X, Y]$ is not a bijection, because the ideal (X, Y) is not in the image.

However, U is clearly a union of affine algebraic varieties — we shall see in the next section that it is a (nonaffine) algebraic variety.

Properties of $\operatorname{specm}(\alpha)$**.**

PROPOSITION 2.21. *Let $\alpha\colon A \to B$ be a homomorphism of affine k-algebras, and let $\varphi\colon \operatorname{Specm}(B) \to \operatorname{Specm}(A)$ be the corresponding morphism of affine varieties (so that $\alpha(f) = \varphi \circ f$).*

(a) *The image of φ is dense for the Zariski topology if and only if α it is injective.*
(b) *φ defines an isomorphism of $\operatorname{Specm}(B)$ onto a closed subvariety of $\operatorname{Specm}(A)$ if and only if α is surjective.*

PROOF. (a) Let $f \in A$. If the image of φ is dense, then

$$f \circ \varphi = 0 \Rightarrow f = 0.$$

Conversely, if the image of φ is not dense, there will be a nonzero function $f \in A$ that is zero on its image, i.e., such that $f \circ \varphi = 0$.

(b) If α is surjective, then it defines an isomorphism $A/\mathfrak{a} \to B$ where $\mathfrak{a}$ is the kernel of α. This induces an isomorphism of $\operatorname{Specm}(B)$ with its image in $\operatorname{Specm}(A)$. □

A regular map $\varphi\colon V \to W$ of affine algebraic varieties is said to be a *dominating* if the image is dense in W. The proposition then says that:

$$\varphi \text{ is dominating} \iff f \mapsto f \circ \varphi\colon \Gamma(W, \mathcal{O}_W) \to \Gamma(V, \mathcal{O}_V) \text{ is injective.}$$

A little history. We have associated with any affine k-algebra A an affine variety whose underlying topological space is the set of maximal ideals in A. It may seem strange to be describing a topological space in terms of maximal ideals in a ring, but the analysts have been doing this for more than 50 years. Gel'fand and Kolmogorov in 1939 proved that if S and T are completely regular topological spaces, and the rings of real-valued continuous functions on S and T are isomorphic (just as rings), then S and T are homeomorphic. The first step in the proof showed that, for such a space S, the map

$$P \mapsto \mathfrak{m}_P = \{f\colon S \to \mathbb{R} \mid f(P) = 0\}$$

defines a one-to-one correspondence between the points in the space and maximal ideals in the ring. (See Shields's article in Math. Intelligencer, Summer 1989, pp 15-17.) (A space S is completely regular if it is T_1 and for every closed subset C and point $P \notin C$, there is a real-valued continuous function f on the space such that $f(P) = 0$ and f is identically 1 on C.)

3. Algebraic Varieties

An algebraic variety is a ringed space that is locally isomorphic to an affine algebraic variety, just as a topological manifold is a ringed space that is locally isomorphic to an open subset of $\mathbb{R}^n$; both are required to satisfy a separation axiom.

Algebraic prevarieties. As motivation, recall the following definitions.

Definition 3.1. (a) A *topological manifold* is a ringed space $(V, \mathcal{O}_V)$ such that V is Hausdorff and every point of V has an open neighbourhood U for which $(U, \mathcal{O}_V|U)$ is isomorphic to the ringed space of continuous functions on an open subset of $\mathbb{R}^n$ (cf. (2.2a)).

(b) A *differentiable manifold* is a ringed space such that V is Hausdorff and every point of V has an open neighbourhood U for which $(U, \mathcal{O}_V|U)$ is isomorphic to a ringed space as in (2.2b).

(c) *A complex manifold* is a ringed space such that V is Hausdorff and every point of V has an open neighbourhood U for which $(U, \mathcal{O}_V|U)$ is isomorphic to a ringed space as in (2.2c).

The above definitions are easily seen to be equivalent to the more classical definitions in terms of charts and atlases. Often one imposes additional conditions on V, for example, that it is second countable or connected.

Definition 3.2. An *algebraic prevariety* is a ringed space $(V, \mathcal{O}_V)$ such that V is quasi-compact and every point of V has an open neighbourhood U such that $(V, \mathcal{O}_V|U)$ is an affine algebraic variety.

Equivalently, a ringed space $(V, \mathcal{O}_V)$ is an algebraic prevariety if there is a finite open covering $V = \cup V_i$ such that $(V_i, \mathcal{O}_V|V_i)$ is an affine algebraic variety for all i.

An algebraic variety will be defined to be an algebraic prevariety satisfying a certain separation condition.

An open subset U of an algebraic prevariety V such that $(U, \mathcal{O}_V|U)$ is an affine algebraic variety is called an *open affine (subvariety)* in V.

Let $(V, \mathcal{O}_V)$ be an algebraic variety, and let U be an open subset of V. The functions $f\colon U \to k$ lying in $\Gamma(U, \mathcal{O}_V)$ are called *regular*. Note that if (U_i) is an open covering of V by affine varieties, then $f\colon U \to k$ is regular if and only if $f|U_i \cap U$ is regular for all i (this is just a special case of condition (c) to be a sheaf, p12). Thus understanding the regular functions on open subsets of V amounts to understanding the regular functions on the open affine subvarieties and how these subvarieties fit together to form V.

Example 3.3. Any open subset of an affine variety together with its induced ringed structure is an algebraic prevariety (in fact variety). For example, $\mathbb{A}^2 \setminus \{(0,0)\}$ is an algebraic variety.

Example 3.4. (Projective space). Let

$$\mathbb{P}^n = k^{n+1} \setminus \{(0, \dots, 0)\}/\!\sim$$

where $(a_0, \dots, a_n) \sim (b_0, \dots, b_n)$ if there is a $c \in k^\times$ such that $(a_0, \dots, a_n) = (cb_0, \dots, cb_n)$. Thus the equivalence classes are the lines through the origin in k^{n+1}.

Write $(a_0\colon \ldots : a_n)$ for the equivalence class containing $(a_0, \ldots, a_n)$. For each i, let

$$U_i = \{(a_0 : \ldots : a_i : \ldots : a_n) \in \mathbb{P}^n \mid a_i \neq 0\}.$$

Then $\mathbb{P}^n = \cup U_i$, and the map u_i

$$(a_1, \ldots, a_n) \mapsto (a_0 : \ldots : a_{i-1} : 1 : a_{i+1}, \ldots : a_n) : k^n \to U_i$$

is a bijection. We use this map to transfer the Zariski topology on k^n to U_i, and we endow $\mathbb{P}^n$ with the topology such that $U \subset \mathbb{P}^n$ is open if and only if $U \cap U_i$ is open in U_i for all i. Define a function $f\colon U \to k$ on an open subset U of $\mathbb{P}^n$ to be regular if $f \circ u_i$ is a regular function on k^n for all i. These definitions endow $\mathbb{P}^n$ with the structure of a ringed space, and each map u_i is an isomorphism of ringed spaces $(\mathbb{A}^n, \mathcal{O}_{\mathbb{A}^n}) \to (U_i, \mathcal{O}_V|U_i)$. Thus $\mathbb{P}^n$ is an algebraic prevariety. Later (see Section 5), we shall study $\mathbb{P}^n$ in detail.

Regular maps. In each of the examples (3.1a,b,c), a morphism of manifolds (continuous map, differentiable map, analytic map respectively) is just a morphism of ringed spaces. This motivates the following definition.

Let $(V, \mathcal{O}_V)$ and $(W, \mathcal{O}_W)$ be algebraic prevarieties. A map $\varphi\colon V \to W$ is said to be *regular* if it is a morphism of ringed spaces. A composite of regular maps is again regular (this is a general fact about morphisms of ringed spaces).

Note that we have four categories:

$$(\text{Affine varieties}) \subset (\text{Alg. prevarieties}) \subset (\text{ringed spaces}).$$

Each subcategory is full (i.e., the morphisms $\mathrm{Mor}(V, W)$ are the same in the four categories).

PROPOSITION 3.5. *Let $(V, \mathcal{O}_V)$ and $(W, \mathcal{O}_W)$ be prevarieties, and let $\varphi\colon V \to W$ be a continuous map (of topological spaces). Let $W = \cup W_i$ be a covering of W by open affines, and let $\varphi^{-1}(W_j) = \cup V_{ji}$ be a covering of $\varphi^{-1}(W_j)$ by open affines. Then φ is regular if and only if its restrictions*

$$\varphi|V_{ji}\colon V_{ji} \to W_j$$

are regular for all i, j.

PROOF. We assume that φ satisfies this condition, and prove that it is regular. Let f be a regular function on an open subset U of W. Then $f|U \cap W_j$ is regular for each W_j (because the regular functions form a sheaf), and so $f \circ \varphi|\varphi^{-1}(U) \cap V_{ji}$ is regular for each j, i (this is our assumption). It follows that $f \circ \varphi$ is regular on $\varphi^{-1}(U)$ (sheaf condition). Thus φ is regular. The converse is equally easy. □

ASIDE 3.6. A differentiable manifold of dimension d is locally isomorphic to an open subset of $\mathbb{R}^d$. In particular, all manifolds of the same dimension are locally isomorphic. This is not true for algebraic varieties, for two reasons:

(a) We are not assuming our varieties are nonsingular (see the next section).

(b) The inverse function theorem fails in our context. If P is a nonsingular point on variety of dimension d, we shall see (in the next section) that there is a neighbourhood U of P and a regular map $\varphi\colon U \to \mathbb{A}^d$ such that map $(d\varphi)_P\colon T_P \to T_{\varphi(P)}$ on the tangent spaces is an isomorphism. If the inverse function theorem were true in our context, it would tell us that an open neighbourhood of P is isomorphic to an open neighbourhood of $\varphi(P)$.

Algebraic varieties. In the study of topological manifolds, the Hausdorff condition eliminates such bizarre possibilities as the line with the origin doubled, where a sequence tending to the origin has two limits.

It is not immediately obvious how to impose a separation axiom on our algebraic varieties, because even affine algebraic varieties are not Hausdorff. The key is to restate the Hausdorff condition. Intuitively, the significance of this condition is that it implies that a sequence in the space can have at most one limit. Thus a continuous map into the space should be determined by its values on a dense subset, i.e., if φ and ψ are continuous maps $Z \to U$ that agree on a dense subset of Z then they should agree on the whole of Z. Equivalently, the set where two continuous maps $\varphi, \psi\colon Z \to U$ agree should be closed. Surprisingly, affine varieties have this property, provided φ and ψ are required to be regular maps.

LEMMA 3.7. *Let φ and ψ be regular maps of affine algebraic varieties $Z \rightrightarrows V$. The subset of Z on which φ and ψ agree is closed.*

PROOF. There are regular functions x_i on V such that $P \mapsto (x_1(P), \dots, x_n(P))$ identifies V with a closed subset of $\mathbb{A}^n$ (take the x_i to be any set of generators for $k[V]$ as a k-algebra). Now $x_i \circ \varphi$ and $x_i \circ \varphi$ are regular functions on Z, and the set where φ and ψ agree is $\bigcap_{i=1}^n V(x_i \circ \varphi - x_i \circ \psi)$, which is closed. □

DEFINITION 3.8. An algebraic prevariety V is said to be *separated*, or to be an *algebraic variety*, if it satisfies the following additional condition:

separation axiom: for every pair of regular maps $\varphi, \psi\colon Z \rightrightarrows V$ with Z an algebraic prevariety, the set $\{z \in Z \mid \varphi(z) = \psi(z)\}$ is closed in Z.

The terminology not completely standardized: often one requires a variety to be irreducible, and sometimes one calls a prevariety a variety.

REMARK 3.9. In order to check that a prevariety V is separated, it suffices to show that for every pair of regular maps $\varphi, \psi\colon Z \to V$ with Z an *affine* algebraic variety $\{z \in Z \mid \varphi(z) = \psi(z)\}$ is closed in Z. To prove this remark, cover Z with open affines. Thus (3.7) shows that affine varieties are separated.

EXAMPLE 3.10. (The affine line with the origin doubled.) Let V_1 and V_2 be copies of $\mathbb{A}^1$. Let $V^* = V_1 \amalg V_2$ (disjoint union), and give it the obvious topology. Define an equivalence relation on V^* by

$$x \text{ (in } V_1) \sim y \text{ (in } V_2) \iff x = y \text{ and } x \neq 0.$$

Let V be the quotient space $V = V^*/\!\sim$ with the quotient topology (a set is open if and only if its inverse image in V^* is open). Then V_1 and V_2 are open subspaces of V, $V = V_1 \cup V_2$, and $V_1 \cap V_2 = \mathbb{A}^1 - \{0\}$. Define a function on an open subset to be regular if its restriction to each V_i is regular. This makes V into a prevariety, but not a variety: it fails the separation axiom because the two maps

$$\mathbb{A}^1 = V_1 \hookrightarrow V^*, \quad \mathbb{A}^1 = V_2 \hookrightarrow V^*$$

agree exactly on $\mathbb{A}^1 - \{0\}$, which is not closed in $\mathbb{A}^1$.

Subvarieties. Let $(V, \mathcal{O}_V)$ be a prevariety. Then V is a finite union of open affines, and in each open affine the open affines (in fact the basic open subsets) form a basis for the topology. From this it follows the open affines form a basis for the topology on V, i.e., every open subset U of V is a union of open affines (of V). It follows that, for any open subset U of V, $(U, \mathcal{O}_V|U)$ is a prevariety. Obviously the inclusion $U \hookrightarrow V$ is regular. A regular map $\varphi\colon W \to V$ is an *open immersion* if $\varphi(W)$ is open in V and φ defines an isomorphism $W \to \varphi(W)$ (of prevarieties).

Any closed subset Z in V has a canonical structure of an algebraic prevariety: endow it with the induced topology, and say that a function f on an open subset of Z is regular if each point P in the open subset has an open neighbourhood U in V such that f extends to a regular function on U. To show that Z, with this ringed space structure is a prevariety, check that for every open affine $U \subset V$, the ringed space $(U \cap Z, \mathcal{O}_Z|U \cap Z)$ is isomorphic to $U \cap Z$ with its ringed space structure acquired as a closed subset of U (see p45). A regular map $\varphi\colon W \to V$ is a *closed immersion* if $\varphi(W)$ is closed in V and φ defines an isomorphism $W \to \varphi(W)$ (of prevarieties).

A subset W of a topological space V is said to be *locally closed* if every point P in W has an open neighbourhood U in V such that $W \cap U$ is closed in U; equivalently, W is the intersection of an open and a closed subset of V. A locally closed subset W of a prevariety V acquires a natural structure as a prevariety: write it as the intersection $W = U \cap Z$ of an open and a closed subset; Z is a prevariety, and W (being open in Z) therefore acquires the structure of a prevariety. This structure on W has the following characterization: the inclusion map $W \hookrightarrow V$ is regular, and a map $\varphi\colon V' \to W$ with V' a prevariety is regular if and only if it is regular when regarded as a map into V. With this structure, W is called a *sub(pre)variety* of V. A morphism $\varphi\colon V' \to V$ is called an *immersion* if it induces an isomorphism of V' onto a subvariety of V. Every immersion is the composite of an open immersion with a closed immersion (in both orders).

A subprevariety of a variety is automatically separated.

PROPOSITION 3.11. *A prevariety V is separated if and only if it has the following property: if two regular maps $\varphi, \psi\colon Z \rightrightarrows V$ agree on a dense subset of Z, then they agree on the whole of Z.*

PROOF. If V is separated, then the set where φ and ψ agree is closed, and so must be the whole of Z.

Conversely, consider a pair of maps $\varphi, \psi\colon Z \rightrightarrows V$, and let S be the subset of Z on which they agree. We assume V has the property in the statement of the lemma, and show that S is closed. Let $\bar{S}$ be the closure of S in Z. According to the above discussion, $\bar{S}$ has the structure of a closed prevariety of Z, and the maps $\varphi|\bar{S}$ and $\psi|\bar{S}$ are regular. Because they agree on a dense subset of $\bar{S}$ they agree on the whole of $\bar{S}$, and so $S = \bar{S}$ is closed. □

Prevarieties obtained by patching. Let $V = \cup V_i$ (finite union), and suppose that each V_i has the structure of an algebraic prevariety satisfying the following condition: for all i, j, $V_i \cap V_j$ is open in both V_i and V_j and the structures of an algebraic prevariety induced on it by V_i and V_j are equal. Then we can define the structure of a ringed space on V as follows: $U \subset V$ is open if and only if $U \cap V_i$ is open for all i, and

$f\colon U \to k$ is regular if and only if $f|U \cap V_i$ is regular for all i. It is straightforward to check that this does make V into a ringed space $(V, \mathcal{O}_V)$.

PROPOSITION 3.12. *The ringed space $(V, \mathcal{O}_V)$ is a prevariety, and the inclusions $V_i \hookrightarrow V$ are regular maps.*

PROOF. One only has to check that the ringed space structure on each V_i induced by that of V is the original one. □

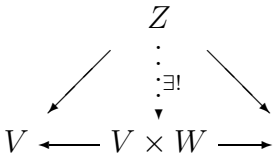
Products of varieties. Let V and W be objects in a category $\mathbf{C}$. A triple

$$(V \times W, \quad p\colon V \times W \to V, \quad q\colon V \times W \to W)$$

is said to be the product of V and W if, for all objects Z in $\mathbf{C}$, the map $\varphi \mapsto (p\circ\varphi, q\circ\varphi)$ is a bijection

$$\mathrm{Hom}(Z, V \times W) \to \mathrm{Hom}(Z, V) \times \mathrm{Hom}(Z, W),$$

i.e., if every pair of morphisms $Z \to V$, $Z \to W$ factors uniquely through $V \times W$:



Clearly, the product, if it exists, is uniquely determined up to a unique isomorphism[11].

For example, the product of two sets (in the category of sets) is the usual cartesion product of the sets, and the product of two topological spaces (in the category of topological spaces) is the cartesian product of the spaces (as sets) with the usual product topology.

We shall show that products exist in the category of algebraic varieties. Suppose, for the moment, that $V \times W$ exists. It follows from (2.17b) that for any prevariety Z, $\mathrm{Mor}(\mathbb{A}^0, Z)$ is the underlying set of Z, i.e., for any $z \in Z$, the map $\mathbb{A}^0 \to Z$ with image z is regular, and these are all the regular maps. Thus, from the definition of products we have

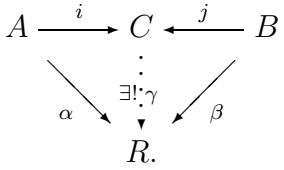
$$\begin{aligned}(\text{underlying set of } V \times W) &= \mathrm{Mor}(\mathbb{A}^0, V \times W)\\ &= \mathrm{Mor}(\mathbb{A}^0, V) \times \mathrm{Mor}(\mathbb{A}^0, W)\\ &= (\text{underlying set of } V) \times (\text{underlying set of } W).\end{aligned}$$

Thus our problem can be restated as follows: given two prevarieties V and W, define on the set $V \times W$ the structure of a prevariety such that the projection maps $p, q\colon V \times W \rightrightarrows V, W$ are regular, and such that a map $\varphi\colon T \to V \times W$ of sets (with T an algebraic prevariety) is regular if and only if its components $p \circ \varphi, q \circ \varphi$ are regular. Clearly, there can be at most one such structure on the set $V \times W$ (because the identity map will identify any two structures having these properties).

[11] If $(P, p' : P \to V, q' : P \to W)$ also has this property, then there exists a unique morphism $\gamma : P \to V \times W$ such that $p \circ \gamma = p'$ and $q \circ \gamma = q'$ (universal property of $V \times W$), and there exists a unique morphism $\gamma' : V \times W \to P$ such that $p' \circ \gamma' = p$ and $q' \circ \gamma' = q$ (universal property of P). The composite $\gamma \circ \gamma'$ is the unique morphism $V \times W \to V \times W$ such that $p \circ \gamma \circ \gamma' = p$ and $q \circ \gamma \circ \gamma' = q$. But we already know one such morphism, namely, the identity morphism, and so $\gamma \circ \gamma' = \mathrm{id}$. Similarly $\gamma' \circ \gamma = \mathrm{id}$, and so γ and γ' are inverse isomorphisms.

Before we can define products of algebraic varieties, we need to review tensor products.

Review of tensor products. Let A and B be k-algebras. A k-algebra C together with homomorphisms $i\colon A \to C$ and $j\colon B \to C$ is called the *tensor product* of A and B if it has the following universal mapping property: for every pair of homomorphisms (of k-algebras) $\alpha\colon A \to R$ and $\beta\colon B \to R$, there is a unique homomorphism $\gamma\colon C \to R$ such that $\gamma \circ i = \alpha$ and $\gamma \circ j = \beta$:



Clearly, if the tensor product exists, it is uniquely determined up to a unique isomorphism (same argument as in the above footnote). We write it $A \otimes_k B$.

Construction. Let C^* be the k-vector space with basis $A \times B$. Thus the elements of C^* are finite sums $\sum c_i(a_i, b_i)$ with $c_i \in k$, $a_i \in A$, $b_i \in B$. Let D be the subspace of C^* generated by the following elements,

$$\begin{aligned}
(a + a', b) - (a, b) - (a', b), &\qquad a, a' \in A,\ b \in B,\\
(a, b + b') - (a, b) - (a, b'), &\qquad a \in A,\ b, b' \in B,\\
(ca, b) - c(a, b), &\qquad a \in A,\ b \in B,\ c \in k,\\
(a, cb) - c(a, b), &\qquad a \in A,\ b \in B,\ c \in k,
\end{aligned}$$

and define $C = C^*/D$. Write $a \otimes b$ for the class of (a, b) in C — we have imposed the fewest conditions forcing $(a, b) \mapsto a \otimes b$ to be k-bilinear. Every element of C can be written as a finite sum, $\sum a_i \otimes b_i$, $a_i \in A$, $b_i \in B$, and the map

$$A \times B \to C, \quad (a, b) \mapsto a \otimes b$$

is k-bilinear. By definition, C is a k-vector space, and there is a product structure on C such that $(a \otimes b)(a' \otimes b') = aa' \otimes bb'$ — for this one has to check that the map

$$C^* \times C^* \to C, \quad ((a, b), (a', b')) \mapsto aa' \otimes bb'$$

factors through $C \times C$. It becomes a k-algebra by means of the homomorphism $c \mapsto c(1 \otimes 1) = c \otimes 1 = 1 \otimes c$. The maps

$$a \mapsto a \otimes 1\colon A \to C \text{ and } b \mapsto 1 \otimes b\colon B \to C$$

are homomorphisms, and it is routine to check that they make C into the tensor product of A and B in the above sense.

Example 3.13. The algebra B, together with the given map $k \to B$ and the identity map $B \to B$, has the universal property characterizing $k \otimes_k B$. In terms of the constructive definition of tensor products, the map $c \otimes b \mapsto cb\colon k \otimes_k B \to B$ is an isomorphism.

EXAMPLE 3.14. (a) The ring $k[X_1,\dots,X_m,X_{m+1},\dots,X_{m+n}]$, together with the maps

$$k[X_1,\dots,X_m] \xrightarrow{\text{obvious inclusion}} k[X_1,\dots,X_{m+n}] \xleftarrow{\text{obvious inclusion}} k[X_{m+1},\dots,X_{m+n}]$$

is the tensor product of $k[X_1,\dots,X_m]$ and $k[X_{m+1},\dots,X_{m+n}]$. To verify this we only have to check that, for every k-algebra R, the map

$$\mathrm{Hom}_{k\text{-alg}}(k[X_1,\dots,X_{m+n}],R) \to \mathrm{Hom}_{k\text{-alg}}(k[X_1,\dots],R)\times \mathrm{Hom}_{k\text{-alg}}(k[X_{m+1},\dots],R)$$

induced by the inclusions is a bijection. But this map can be identified with the bijection

$$R^{m+n} \to R^m \times R^n.$$

In terms of the constructive definition of tensor products, the map

$$f\otimes g \mapsto fg\colon k[X_1,\dots,X_m]\otimes_k k[X_{m+1},\dots,X_{m+n}] \to k[X_1,\dots,X_{m+n}]$$

is an isomorphism.

(b) Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals in $k[X_1,\dots,X_m]$ and $k[X_{m+1},\dots,X_{m+n}]$ respectively, and let $(\mathfrak{a},\mathfrak{b})$ be the ideal in $k[X_1,\dots,X_{m+n}]$ generated by the elements of $\mathfrak{a}$ and $\mathfrak{b}$. Then there is an isomorphism

$$f\otimes g \mapsto fg\colon \frac{k[X_1,\dots,X_m]}{\mathfrak{a}}\otimes_k \frac{k[X_{m+1},\dots,X_{m+n}]}{\mathfrak{b}} \to \frac{k[X_1,\dots,X_{m+n}]}{(\mathfrak{a},\mathfrak{b})}.$$

Again this comes down to checking that the natural map from $\mathrm{Hom}_{k\text{-alg}}(k[X_1,\dots,X_{m+n}]/(\mathfrak{a},\mathfrak{b}),R)$ to

$$\mathrm{Hom}_{k\text{-alg}}(k[X_1,\dots,X_m]/\mathfrak{a},R)\times \mathrm{Hom}_{k\text{-alg}}(k[X_{m+1},\dots,X_{m+n}]/\mathfrak{b},R)$$

is a bijection. But the three sets are respectively

$V(\mathfrak{a},\mathfrak{b})$ = zero-set of $(\mathfrak{a},\mathfrak{b})$ in R^{m+n},

$V(\mathfrak{a})$ = zero-set of $\mathfrak{a}$ in R^m,

$V(\mathfrak{b})$ = zero-set of $\mathfrak{b}$ in R^n,

and so this is obvious.

REMARK 3.15. (a) If (b_α) is a family of generators (resp. basis) for B as a k-vector space, then $(1\otimes b_\alpha)$ is a family of generators (resp. basis) for $A\otimes_k B$ as an A-module.

(b) Let $k\hookrightarrow\Omega$ be fields. Then

$$\Omega\otimes_k k[X_1,\dots,X_n] \cong \Omega[1\otimes X_1,\dots,1\otimes X_n] \cong \Omega[X_1,\dots,X_n].$$

If $A=k[X_1,\dots,X_n]/(g_1,\dots,g_m)$, then

$$\Omega\otimes_k A \cong \Omega[X_1,\dots,X_n]/(g_1,\dots,g_m).$$

For more details on tensor products, see Atiyah and MacDonald 1969, Chapter 2 (but note that the description there (p31) of the homomorphism $A\to D$ making the tensor product into an A-algebra is incorrect — the map is $a\mapsto f(a)\otimes 1 = 1\otimes g(a)$.

Products of affine varieties. The tensor product of two k-algebras A and B has the universal property to be a product, but with the arrows reversed. Because of the category anti-equivalence (2.14), this will show that $\operatorname{Specm}(A \otimes_k B)$ is the product of $\operatorname{Specm} A$ and $\operatorname{Specm} B$ in the category of affine algebraic varieties once we have shown that $A \otimes_k B$ is an affine k-algebra.

PROPOSITION 3.16. *Let A and B be finitely generated k-algebras; if A and B are reduced, then so also is $A \otimes_k B$; if A and B are integral domains, then so also is $A \otimes_k B$.*

PROOF. Assume A and B to be reduced, and let $\alpha \in A \otimes_k B$. Then $\alpha = \sum_{i=1}^{n} a_i \otimes b_i$, some $a_i \in A$, $b_i \in B$. If one of the b_i's is a linear combination of the remaining b's, say, $b_n = \sum_{i=1}^{n-1} c_i b_i$, $c_i \in k$, then, using the bilinearity of $\otimes$, we find that

$$\alpha = \sum_{i=1}^{n-1} a_i \otimes b_i + \sum_{i=1}^{n-1} c_i a_n \otimes b_i = \sum_{i=1}^{n-1} (a_i + c_i a_n) \otimes b_i.$$

Thus we can suppose that in the original expression of α, the b_i's are linearly independent over k.

Now suppose that α is nilpotent, and let $\mathfrak{m}$ be a maximal ideal in A. From $a \mapsto \bar{a}\colon A \to A/\mathfrak{m} = k$ we obtain homomorphisms

$$a \otimes b \mapsto \bar{a} \otimes b \mapsto \bar{a}b\colon A \otimes_k B \to k \otimes_k B \xrightarrow{\approx} B$$

The image $\sum \bar{a}_i b_i$ of α under this homomorphism is a nilpotent element of B, and hence is zero (because B is reduced). As the b_i's are linearly independent over k, this means that the $\bar{a}_i$ are all zero. Thus, for all i, a_i lies in every maximal ideal $\mathfrak{m}$ of A, and so is zero (by 2.12). Hence $\alpha = 0$. This shows that $A \otimes_k B$ is reduced.

Assume A and B to be integral domains, and let α, $\alpha' \in A \otimes B$ be such that $\alpha\alpha' = 0$. As before, we can write $\alpha = \sum a_i \otimes b_i$ and $\alpha' = \sum a_i' \otimes b_i'$ with the sets $\{b_1, b_2, \dots\}$ and $\{b_1', b_2', \dots\}$ each linearly independent over k. For each maximal ideal $\mathfrak{m}$ of A, we know $(\sum \bar{a}_i b_i)(\sum \bar{a}_i' b_i') = 0$ in B, and so either $(\sum \bar{a}_i b_i) = 0$ or $(\sum \bar{a}_i' b_i') = 0$. Thus either all the $a_i \in \mathfrak{m}$ or all the $a_i' \in \mathfrak{m}$. This shows that

$$\operatorname{specm}(A) = V(a_1, \dots, a_m) \cup V(a_1', \dots, a_n').$$

Since $\operatorname{specm}(A)$ is irreducible (see 1.15), we must have $\operatorname{specm}(A) = V(a_1, \dots, a_m)$ or $V(a_1', \dots, a_n')$. In the first case $\alpha = 0$, and in the second $\alpha' = 0$. □

EXAMPLE 3.17. We give some examples to illustrate that k must be taken to be algebraically closed in the proposition.

(a) Suppose k is nonperfect of characteristic p. To say that k is not perfect means that there is an element α in an algebraic closure of k such that $\alpha \notin k$ but $\alpha^p \in k$. Let $k' = k[\alpha]$, $\alpha^p = a \in k$, $\alpha \notin k$. Then $(\alpha \otimes 1 - 1 \otimes \alpha) \neq 0$ in $k' \otimes_k k'$ (in fact, the elements $\alpha^i \otimes \alpha^j$, $0 \leq i, j \leq p-1$, form a basis for $k' \otimes_k k'$ as a k-vector space), but

$$(\alpha \otimes 1 - 1 \otimes \alpha)^p = (a \otimes 1 - 1 \otimes a) = (1 \otimes a - 1 \otimes a) = 0.$$

Thus $k' \otimes_k k'$ is not reduced, even though k' is a field.

(b) Let K be a finite separable extension of k and let Ω be a "big" field containing k (for example an algebraic closure of k). Write $K = k[\alpha] = k[X]/(f(X))$, and assume

$f(X)$ splits in $\Omega[X]$, say, $f(X) = \prod X - \alpha_i$. Because K/k is separable, the α_i are distinct, and so

$$K \otimes_k \Omega \cong \Omega[X]/(f(X)) \cong \prod \Omega[X]/(X - \alpha_i),$$

and so it is not an integral domain. (The second isomorphism follows from the Chinese remainder theorem.)

Having (3.16), we can make the following definition: let V and W be affine varieties, and let $\Gamma(V, \mathcal{O}_V) = A$ and $\Gamma(W, \mathcal{O}_W) = B$; then $V \times W = \text{Specm}(A \otimes_k B)$ with the projection maps $p\colon V \times W \to V$ and $q\colon V \times W \to W$ defined by the maps $a \mapsto a \otimes 1\colon A \to A \otimes_k B$ and $b \mapsto 1 \otimes b\colon B \to A \otimes_k B$.

PROPOSITION 3.18. *Let V and W be affine varieties; the projection maps $p\colon V \times W \to V$, $q\colon V \times W \to W$ are regular, and a map $\varphi\colon U \to V \times W$ is regular if and only if $p \circ \varphi$ and $q \circ \varphi$ are regular. Therefore $(V \times W, p, q)$ is the product of V and W in the category of algebraic prevarieties. If V and W are irreducible, then so also is $V \times W$.*

PROOF. The projection maps are regular because they correspond to the k-algebra homomorphisms $k[V] \to k[V] \otimes_k k[W]$ and $k[W] \to k[V] \otimes_k k[W]$. Let $\varphi\colon U \to V \times W$ be a map (of sets) such that $p \circ \varphi$ and $q \circ \varphi$ are regular. If U is affine, then φ corresponds to the map $k[V] \otimes k[W] \to k[U]$ induced by

$$f \mapsto f \circ (p \circ \varphi)\colon k[V] \to k[U] \text{ and } f \mapsto f \circ (q \circ \varphi)\colon k[W] \to k[U],$$

and so is regular. This shows that, for a general U, the restriction of φ to every open affine of U is regular, and this implies that φ is regular (see 3.5).

The final statement follows from the second statement in 3.16. □

EXAMPLE 3.19. (a) It follows from (3.14a) that

$$\mathbb{A}^m \xleftarrow{p} \mathbb{A}^{m+n} \xrightarrow{q} \mathbb{A}^n,$$

where

$$\begin{aligned} p(a_1, \dots, a_{m+n}) &= (a_1, \dots, a_m), \\ q(a_1, \dots, a_{m+n}) &= (a_{m+1}, \dots, a_{m+n}), \end{aligned}$$

is the product of $\mathbb{A}^m$ and $\mathbb{A}^n$.

(b) It follows from (3.14b) that

$$V(\mathfrak{a}) \xleftarrow{p} V(\mathfrak{a}, \mathfrak{b}) \xrightarrow{q} V(\mathfrak{b})$$

is the product of $V(\mathfrak{a})$ and $V(\mathfrak{b})$.

Warning! The topology on $V \times W$ is not the product topology; for example, the topology on $\mathbb{A}^2 = \mathbb{A}^1 \times \mathbb{A}^1$ is not the product topology.

Products in general. Now let V and W be two algebraic prevarieties V and W. We define their product as follows: As a set, we take $V \times W$. Now write V and W as unions of open affines, $V = \cup V_i$, $W = \cup W_j$. Then $V \times W = \cup V_i \times W_j$, and we give $V \times W$ the topology for which $U \subset V \times W$ is open if and only if $U \cap (V_i \times W_j)$ is open for all i and j. Finally, we define a ringed space structure by saying that a

function $f\colon U \to k$ on an open subset U is regular if its restriction to $U \cap (U_i \times V_j)$ is regular for all i and j.

PROPOSITION 3.20. *With the above structure, $V \times W$ is a prevariety, the projection maps*

$$p\colon V \times W \to V,\ q\colon V \times W \to W$$

are regular, and a map $\varphi\colon U \to V \times W$ is regular if and only if $p \circ \varphi$ and $q \circ \varphi$ are regular. Therefore $(V \times W, p, q)$ is the product of V and W in the category of prevarieties.

PROOF. Straightforward. □

PROPOSITION 3.21. *If V and W are separated, then so also is $V \times W$.*

PROOF. Straightforward. □

EXAMPLE 3.22. An *algebraic group* is a variety G together with regular maps

$$\text{mult}\colon G \times G \to G,\ \text{inverse}\colon G \to G,$$

and an element $e \in G$ that make G into a group in the usual sense. For example, SL_n and GL_n are algebraic groups, and any finite group can be regarded as an algebraic group. Connected affine algebraic groups are called linear algebraic groups because they can all be realized as closed subgroups of GL_n for some n, and connected algebraic groups that can be realized as *closed* algebraic subvarieties of a projective space are called *abelian* because they are related to the integrals studied by Abel.

Coarse Classification: every algebraic group contains a sequence of normal subgroups $G \supset G^0 \supset G_1 \supset \{e\}$ with G/G^0 a finite group, G^0/G_1 an abelian variety, and G_1 a linear algebraic group.

The separation axiom. Now that we have the notion of the product of varieties, we can restate the separation axiom in terms of the diagonal.

By way of motivation, consider a topological space V and the diagonal $\Delta \subset V \times V$,

$$\Delta \stackrel{\text{df}}{=} \{(x, x) \mid x \in V\}.$$

If Δ is closed (for the product topology), then every pair of points $(x, y) \notin \Delta$ has a neighbourhood $U \times U'$ such that $U \times U' \cap \Delta = \varnothing$. In other words, if x and y are distinct points in V then there are neighbourhoods U and U' of x and y respectively such that $U \cap U' = \varnothing$. Thus V is Hausdorff. Conversely, if V is Hausdorff, the reverse argument shows that Δ is closed.

For a variety V, we let $\Delta = \Delta_V$ (the diagonal) be the subset $\{(v, v) \mid v \in V\}$ of $V \times V$.

PROPOSITION 3.23. *An algebraic prevariety V is separated if and only if Δ_V is closed.*

PROOF. Assume Δ to be closed, and let φ and ψ be regular maps $Z \to V$. The map

$$(\varphi, \psi)\colon Z \to V \times V,\ z \mapsto (\varphi(z), \psi(z))$$

is regular, because its composites with the projections to V are φ and ψ. In particular, it is continuous, and so $(\varphi,\psi)^{-1}(\Delta)$ is closed. But this is precisely the subset on which φ and ψ agree.

Conversely, suppose V is separated. By definition, this means that for any prevariety Z and regular maps $\varphi,\psi\colon Z\to V$, the set on which φ and ψ agree is closed in Z. Apply this with φ and ψ the two projection maps $V\times V\to V$, and note that the set on which they agree is Δ. □

COROLLARY 3.24. *For any prevariety V, the diagonal is a locally closed subset of $V\times V$.*

PROOF. Let $P\in V$, and let U be an open affine neighbourhood of P. Then $U\times U$ is a neighbourhood of (P,P) in $V\times V$, and $\Delta_V\cap(U\times U)=\Delta_U$, which is closed in $U\times U$ because U is separated. □

Thus Δ_V is always a subvariety of $V\times V$, and it is closed if and only if V is separated.

The graph Γ_φ of a regular map $\varphi\colon V\to W$ is defined to be

$$\{(v,\varphi(v))\in V\times W\mid v\in V\}.$$

At this point, the reader should draw a picture, suggested by calculus.

COROLLARY 3.25. *For any morphism $\varphi\colon V\to W$ of prevarieties, the graph Γ_φ of φ is locally closed in $V\times W$, and it is closed if W is separated. The map $v\mapsto(v,\varphi(v))$ is an isomorphism of V onto Γ_φ.*

PROOF. The first statement follows from the preceding corollary because the graph is the inverse image of the diagonal of $W\times W$ under the regular map

$$(v,w)\mapsto(\varphi(v),w)\colon V\times W\to W\times W.$$

The second follows from the fact that the regular map $\Gamma_\varphi\hookrightarrow V\times W\xrightarrow{p}V$ is an inverse to $v\mapsto(v,\varphi(v))\colon V\to\Gamma_\varphi$. □

THEOREM 3.26. *The following three conditions on a prevariety are equivalent:*

(a) *V is separated;*
(b) *for every pair of open affines U and U' in V, $U\cap U'$ is an open affine, and $\Gamma(U\cap U',\mathcal{O}_V)$ is generated by the functions $P\mapsto f(P)g(P)$, $f\in\Gamma(U,\mathcal{O}_V)$, $g\in\Gamma(U',\mathcal{O}_V)$, i.e., the map $k[U]\otimes_k k[U']\to k[U\cap U']$ is surjective;*
(c) *the condition in (b) holds for the sets in some open affine covering of V.*

PROOF. Let U_i and U_j be open affines in V. We shall prove:

(i) Δ closed $\Rightarrow U_i\cap U_j$ affine.

(ii) If $U_i\cap U_j$ is affine, then

$$(U_i\times U_j)\cap\Delta\text{ is closed}\iff\text{the map }k[U_i]\otimes_k k[U_j]\to k[U_i\cap U_j]\text{ is surjective.}$$

If $\{U_i\times U_j\}_{(i,j)\in I\times J}$ is an open covering of $V\times V$, Δ is closed in $V\times V\iff\Delta\cap(U_i\times U_j)$ is closed in $U_i\times U_j$ for each pair (i,j). Thus these statements show that (a)⇒(b) and (c)⇒(a). Since the implication (b)⇒(c) is trivial, this shows that (i) and (ii) imply the theorem.

Proof of (i): The graph of the inclusion $\iota\colon U_i\cap U_j\hookrightarrow V$ is $\Gamma_\iota=(U_i\times U_j)\cap\Delta\subset(U_i\cap U_j)\times V$. If Δ is closed, $(U_i\times U_j)\cap\Delta$ is a closed subvariety of an affine variety, and hence is affine (see p45). Since $U_i\cap U_j\approx\Gamma_\iota$, it also is affine.

Proof of (ii): Now assume that $U_i\cap U_j$ is affine. Then $(U_i\times U_j)\cap\Delta_V$ is closed in $U_i\times U_j\iff v\mapsto(v,v)\colon U_i\cap U_j\to U_i\times U_j$ is a closed immersion $\iff$ the morphism $k[U_i\times U_j]\to k[U_i\cap U_j]$ is surjective (see 2.21). Since $k[U_i\times U_j]=k[U_i]\otimes_k k[U_j]$, this completes the proof of (ii). □

Example 3.27. (a) Let $V=\mathbb{P}^1$, and let U_0 and U_1 be the standard open subsets ($U_i=\mathbb{A}^1$). Then $U_0\cap U_1=\mathbb{A}^1-\{0\}$, and the maps on rings corresponding to the inclusions $U_i\hookrightarrow U_0\cap U_1$ are $k[X]\to k[X,X^{-1}]$, $X\mapsto X$, and $k[X]\to k[X,X^{-1}]$, $X\mapsto X^{-1}$. Thus the sets U_0 and U_1 satisfy the condition in (b).

(b) Let V be $\mathbb{A}^1$ with the origin doubled (see 3.10), and let U and U' be the upper and lower copies of $\mathbb{A}^1$ in V. Then $U\cap U'$ is affine, but $k[U]\otimes k[U']\to k[U\cap U']$ is not surjective. In fact the map is

$$k[X]\otimes k[Y]=k[X,Y]\to k[X,X^{-1}],\quad X\mapsto X,\quad Y\mapsto X.$$

(c) Let V be $\mathbb{A}^2$ with the origin doubled, and let U and U' be the upper and lower copies of $\mathbb{A}^2$ in V. Then $U\cap U'$ is not affine (see 2.20).

Dimension. Let V be an irreducible algebraic variety. Then every open subset of V is dense, and is irreducible. If $U\supset U'$ are open affines in V, then we have

$$k[U]\subset k[U']\subset k(U).$$

Therefore $k(U)$ is also the field of fractions of $k[U']$. This remark shows that we can attach to V a field $k(V)$, called *the field of rational functions on* V, such that for every open affine U in V, $k(V)$ is the field of fractions of $k[U]$. The *dimension* of V is defined to be the transcendence degree of $k(V)$ over k. Note the $\dim(V)=\dim(U)$ for any open subset U of V. In particular, $\dim(V)=\dim(U)$ for U an open affine in V. It follows that some of the results in §1 carry over — for example, if Z is a proper closed subvariety of V, then $\dim(Z)<\dim(V)$.

Proposition 3.28. *Let V and W be irreducible varieties. Then*

$$\dim(V\times W)=\dim(V)+\dim(W).$$

Proof. We can assume V and W to be affine, and write $k[V]=k[x_1,\dots,x_m]$ and $k[W]=k[y_1,\dots,y_n]$ where $\{x_1,\dots,x_d\}$ and $\{y_1,\dots,y_e\}$ are maximal algebraically independent sets of elements of $k[V]$ and $k[W]$. Thus $d=\dim(V)$ and $e=\dim(W)$. Then[12]

$$k[V\times W]=k[V]\otimes_k k[W]\supset k[x_1,\dots,x_d]\otimes_k k[y_1,\dots,y_e]\approx k[x_1,\dots,x_d,y_1,\dots,y_e].$$

Therefore $\{x_1\otimes1,\dots,x_d\otimes1,1\otimes y_1,\dots,1\otimes y_e\}$ will be algebraically independent in $k[V]\otimes_k k[W]$. Obviously $k[V\times W]$ is generated as a k-algebra by the elements $x_i\otimes1$, $1\otimes y_j$, $1\le i\le m$, $1\le j\le n$, and all of them are algebraic over

$$k[x_1,\dots,x_d]\otimes_k k[y_1,\dots,y_e].$$

[12]In general, it is not true that if M' and N' are R-submodules of M and N, then $M'\otimes_R N'$ is an R-submodule of $M\otimes_R N$. However, this is true if R is a field, because then M' and N' will be direct summands of M and N, and tensor products preserve direct summands.

Thus the transcendence degree of $k(V \times W)$ is $d + e$. □

We extend the definition to an arbitrary variety V as follows. A variety is a finite union of Noetherian topological spaces, and so is Noetherian. Consequently (see 1.17), V is a finite union $V = \cup V_i$ of its irreducible components, and we define $\dim(V) = \max \dim(V_i)$.

An algebraic variety as a functor of affine k-algebras. Let A be an affine k-algebra, and let V be an algebraic variety. We define a *point of V with coordinates in A* to be a regular map $\operatorname{Specm}(A) \to V$. For example, if $V = V(\mathfrak{a}) \subset k^n$, then

$$V(A) = \{(a_1, \dots, a_n) \in A^n \mid f(a_1, \dots, a_n) = 0 \text{ all } f \in \mathfrak{a}\},$$

which is what you expect. In particular $V(k) = V$ (as a set), i.e., V (as a set) can be identified with the set of points of V with coordinates in k. Note that $(V \times W)(A) = V(A) \times W(A)$.

THEOREM 3.29. *A regular map $\varphi\colon V \to W$ of algebraic varieties defines a family of maps of sets, $\varphi(A)\colon V(A) \to W(A)$, one for each affine k-algebra A, such that for every homomorphism $\alpha\colon A \to B$ of k-algebras,*

$$\begin{array}{ccc} A & V(A) & \xrightarrow{\varphi(A)} W(A) \\ \downarrow{\scriptstyle \alpha} & \downarrow{\scriptstyle V(\alpha)} & \downarrow{\scriptstyle W(\alpha)} \\ B & V(B) & \xrightarrow{\varphi(B)} V(B) \end{array} \qquad (*)$$

commutes. Every family of maps with this property arises from a unique morphism of algebraic varieties.

The proof is trivial, once one has made the correct definitions, which we do in the next subsection.

Categories and functors. A *category* **C** consists of

(a) a class of objects $\operatorname{ob}(\mathbf{C})$;
(b) for each pair (A, B) of objects, a set $\operatorname{Mor}(A, B)$, whose elements are called morphisms from A to B, and are written $\alpha\colon A \to B$;
(c) for each triple of objects (A, B, C) a map (called *composition*)

$$(\alpha, \beta) \mapsto \beta \circ \alpha\colon \operatorname{Mor}(A, B) \times \operatorname{Mor}(B, C) \to \operatorname{Mor}(A, C).$$

Composition is required to be associative, i.e., $(\gamma \circ \beta) \circ \alpha = \gamma \circ (\beta \circ \alpha)$, and for each object A there is required to be an element $\mathrm{id}_A \in \operatorname{Mor}(A, A)$ such that $\mathrm{id}_A \circ \alpha = \alpha$, $\beta \circ \mathrm{id}_A = \beta$, for all (appropriate) α and β. The sets $\operatorname{Mor}(A, B)$ are required to be disjoint (so that a morphism α determines its source and target).

EXAMPLE 3.30. (a) There is a category of sets, **Sets**, whose objects are the sets and whose morphisms are the usual maps of sets.

(b) There is a category $\mathbf{Aff}_k$ of affine k-algebras, whose objects are the affine k-algebras and whose morphisms are the homomorphisms of k-algebras.

(c) There is a category $\mathbf{Var}_k$ of algebraic varieties over k, whose objects are the algbraic varieties over k and whose morphisms are the regular maps.

The objects in a category need not be sets with structure, and the morphisms need not be maps.

EXERCISE 3.31. List twenty more examples of categories.

Let $\mathbf{C}$ and $\mathbf{D}$ be categories. A *covariant functor* F from $\mathbf{C}$ to $\mathbf{D}$ consists of

(a) a map $A \mapsto F(A)$, sending each object of $\mathbf{C}$ to an object of $\mathbf{D}$, and,
(b) for each pair of objects A, B of $\mathbf{C}$, a map

$$\alpha \mapsto F(\alpha)\colon \operatorname{Mor}(A,B) \to \operatorname{Mor}(F(A),F(B))$$

such that $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$ and $F(\beta\circ\alpha) = F(\beta)\circ F(\alpha)$.

A *contravariant functor* is defined similarly, except that the map on morphisms is

$$\alpha \mapsto F(\alpha)\colon \operatorname{Mor}(A,B) \to \operatorname{Mor}(F(B),F(A))$$

A functor $F\colon \mathbf{C}\to\mathbf{D}$ is *fully faithful* if, for all objects A and B of $\mathbf{C}$, the map

$$\operatorname{Mor}(A,B) \to \operatorname{Mor}(F(A),F(B))$$

is a bijection. Then F defines an equivalence of $\mathbf{C}$ with the full subcategory of $\mathbf{D}$ whose objects are isomorphic to $F(A)$ for some object A of $\mathbf{C}$ (see p42). For example, the functor $A \mapsto \operatorname{Specm} A$ is fully faithful contravariant functor $\mathbf{Aff}_k \to \mathbf{Var}_k$, and defines an equivalence of the first category with the subcategory of the second whose objects are the affine algebraic varieties.

EXAMPLE 3.32. (a) For any object V of a category $\mathbf{C}$, we have a contravariant functor

$$h_V\colon \mathbf{C}\to\mathbf{Sets},$$

which sends an object A to the set $\operatorname{Mor}(A,V)$ and sends a morphism $\alpha\colon A\to B$ to

$$\varphi\mapsto\varphi\circ\alpha\colon h_V(B)\to h_V(A),$$

i.e., $h_V(*) = \operatorname{Mor}(*,V)$ and $h_V(\alpha) = *\circ\alpha$.

(b) We have a contravariant functor

$$V\mapsto\Gamma(V,\mathcal{O}_V)\colon \mathbf{Var}_k\to\mathbf{Aff}_k.$$

Let F and G be two functors $\mathbf{C}\to\mathbf{D}$. A *morphism* $\alpha\colon F\to G$ is a collection of morphisms $\alpha(A)\colon F(A)\to G(A)$, one for each object A of $\mathbf{C}$, such that, for every morphism $u\colon A\to B$ in $\mathbf{C}$, the following diagram commutes:

$$\begin{array}{ccc} A & F(A) & \xrightarrow{\alpha(A)} & G(A) \\ \big\downarrow{\scriptstyle u} & \big\downarrow{\scriptstyle F(u)} & & \big\downarrow{\scriptstyle G(u)} \\ B & F(B) & \xrightarrow{\alpha(B)} & G(B) \end{array} \qquad (**)$$

EXAMPLE 3.33. Let $\alpha\colon V\to W$ be a morphism in $\mathbf{C}$. The collection of maps

$$h_\alpha(A)\colon h_V(A)\to h_W(A),\quad \varphi\mapsto\alpha\circ\varphi$$

is a morphism of functors.

With this notion of morphism, the functors $\mathbf{C}\to\mathbf{D}$ form a category $\mathbf{Fun}(\mathbf{C},\mathbf{D})$ (we ignore the problem that $\operatorname{Mor}(F,G)$ may not be a set — only a class).

PROPOSITION 3.34 (Yoneda Lemma). *The functor*

$$V \mapsto h_V : \mathbf{C} \to \mathbf{Fun}(\mathbf{C}, \mathbf{Sets})$$

is fully faithful.

PROOF. Let A, B be objects of $\mathbf{C}$. We construct an inverse to

$$\alpha \mapsto h_\alpha : \operatorname{Mor}(A, B) \to \operatorname{Mor}(h_A, h_B).$$

For a morphism of functors $\gamma : h_A \to h_B$, define $\beta(\gamma) = \gamma(\mathrm{id}_A)$—it is morphism $A \to B$. Then

$$\beta(h_\alpha) \overset{\text{df}}{=} h_\alpha(\mathrm{id}_A) \overset{\text{df}}{=} \alpha \circ \mathrm{id}_A = \alpha,$$

and

$$h_{\beta(\gamma)}(\alpha) \overset{\text{df}}{=} \beta(\gamma) \circ \alpha \overset{\text{df}}{=} \gamma(\mathrm{id}_A) \circ \alpha = \gamma(\alpha)$$

because of the commutativity of (**):

$$\begin{array}{ccc} A & h_A(A) & \xrightarrow{\gamma} h_B(A) \\ \downarrow{\scriptstyle \alpha} & {\scriptstyle *\circ\alpha}\downarrow & \downarrow{\scriptstyle *\circ\alpha} \\ B & h_B(B) & \xrightarrow{\gamma} h_B(B) \end{array} \qquad (***)$$

Thus $\alpha \to h_\alpha$ and $\gamma \mapsto \beta(\gamma)$ are inverse maps. □

Algebraic varieties as functors (continued). The Yoneda lemma shows that the functor $V \mapsto h_V$ embeds the category of affine algebraic varieties as a full subcategory of the category of covariant functors $\mathbf{Aff}_k \to \mathbf{Sets}$, and it is not difficult to deduce that it embeds the category of all algebraic varieties in to the category of such functors (use 3.12 for example). This proves (3.29).

It is not unusual for a variety to be most naturally defined in terms of its points functor. For example, for any affine k-algebra, let $\mathrm{SL}_n(A)$ be the group of $n \times n$ matrices with coefficients in A having determinant 1. A homomorphism $A \to B$ induces a homomorphism $\mathrm{SL}_n(A) \to \mathrm{SL}_n(B)$, and so $\mathrm{SL}_n(A)$ is a functor. In fact, it is the points functor of the affine variety:

$$\operatorname{Specm} k[X_{11}, \dots, X_{nn}]/(\det(X_{ij}) - 1).$$

Matrix multiplication defines a morphism of functors

$$\mathrm{SL}_n \times \mathrm{SL}_n \to \mathrm{SL}_n$$

which, because of (3.29), arises from a morphism of algebraic varieties. In fact, SL_n is an algebraic group.

Instead of defining varieties to be ringed spaces, it is possible to define them to be functors $\mathbf{Aff}_k \to \mathbf{Sets}$ satisfying certain conditions.

Dominating maps. A regular map $\alpha : V \to W$ is said to be *dominating* if the image of α is dense in W. Suppose V and W are irreducible. If V' and W' are open affine subsets of V and W such that $\varphi(V') \subset W'$, then (2.21) implies that the map $f \mapsto f \circ \varphi : k[W'] \to k[V']$ is injective. Therefore it extends to a map on the fields of fractions, $k(W) \to k(V)$, and this map is independent of the choice of V' and W'.

4. Local Study: Tangent Planes, Tangent Cones, Singularities

In this section, we examine the structure of a variety near a point. I begin with the case of a curve, since the ideas in the general case are the same, but the formulas are more complicated. Throughout, k is an algebraically closed field.

Tangent spaces to plane curves. Consider the curve

$$V : F(X,Y) = 0$$

in the plane $\mathbb{A}^2$ defined by a nonconstant polynomial $F(X,Y)$. We assume that $F(X,Y)$ has no multiple factors, so that $(F(X,Y))$ is a radical ideal and $I(V) = (F(X,Y))$. We can factor F into a product of irreducible polynomials, $F(X,Y) = \prod F_i(X,Y)$, and then $V = \cup V(F_i)$ expresses V as a union of its irreducible components. Each component $V(F_i)$ has dimension 1 (see 1.21) and so V has pure dimension 1. More explicitly, suppose for simplicity that $F(X,Y)$ itself is irreducible, so that $k[V] = k[X,Y]/(F(X,Y)) = k[x,y]$ is an integral domain. If $F \neq X - c$, then x is transcendental over k and y is algebraic over $k(x)$, and so x is a transcendence basis for $k(V)$ over k. Similarly, if $F \neq Y - c$, then y is a transcendence basis for $k(V)$ over k.

Let (a,b) be a point on V. In calculus, the equation of the tangent at $P = (a,b)$ is defined to be

$$\frac{\partial F}{\partial X}(a,b)(X-a) + \frac{\partial F}{\partial Y}(a,b)(Y-b) = 0. \qquad (*)$$

This is the equation of a line unless both $\frac{\partial F}{\partial X}(a,b)$ and $\frac{\partial F}{\partial Y}(a,b)$ are zero, in which case it is the equation of a plane.

Definition 4.1. The *tangent space* $T_P V$ to V at $P = (a,b)$ is the space defined by equation (*).

When $\frac{\partial F}{\partial X}(a,b)$ and $\frac{\partial F}{\partial Y}(a,b)$ are not both zero, $T_P(V)$ is a line, and we say that P is a *nonsingular* or *smooth* point of V. Otherwise, $T_P(V)$ has dimension 2, and we say that P is *singular* or *multiple.* The curve V is said to be *nonsingular* or *smooth* when all its points are nonsingular.

We regard $T_P(V)$ as a subspace of the two-dimensional vector space $T_P(\mathbb{A}^2)$, which is the two-dimensional space of vectors with origin P.

Example 4.2. In each case, the reader is invited to sketch the curve. The characteristic of k is assumed to be $\neq 2, 3$.

(a) $X^m + Y^m = 1$. All points are nonsingular unless the characteristic divides m (in which case $X^m + Y^m - 1$ has multiple factors).
(b) $Y^2 = X^3$. Here only $(0,0)$ is singular.
(c) $Y^2 = X^2(X+1)$. Here again only $(0,0)$ is singular.
(d) $Y^2 = X^3 + aX + b$. In this case, V is singular $\iff$ $Y^2 - X^3 - aX - b$, $2Y$, and $3X^2 + a$ have a common zero $\iff$ $X^3 + aX + b$ and $3X^2 + a$ have a common zero. Since $3X^2 + a$ is the derivative of $X^3 + aX + b$, we see that V is singular if and only if $X^3 + aX + b$ has a multiple root.
(e) $(X^2 + Y^2)^2 + 3X^2Y - Y^3 = 0$. The origin is (very) singular.
(f) $(X^2 + Y^2)^3 - 4X^2Y^2 = 0$. The origin is (even more) singular.

(g) $V = V(FG)$ where FG has no multiple factors and F and G are relatively prime. Then $V = V(F) \cup V(G)$, and a point (a, b) is singular if and only if it is a singular point of $V(F)$, a singular point of $V(G)$, or a point of $V(F) \cap V(G)$. This follows immediately from the equations given by the product rule:

$$\frac{\partial(FG)}{\partial X} = F \cdot \frac{\partial G}{\partial X} + \frac{\partial F}{\partial X} \cdot G, \quad \frac{\partial(FG)}{\partial Y} = F \cdot \frac{\partial G}{\partial Y} + \frac{\partial F}{\partial Y} \cdot G.$$

PROPOSITION 4.3. *Let V be the curve defined by a nonconstant polynomial F without multiple factors. The set of nonsingular points*[13] *is an open dense subset V.*

PROOF. We can assume that F is irreducible. We have to show that the set of singular points is a proper closed subset. Since it is defined by the equations

$$F = 0,\ \frac{\partial F}{\partial X} = 0,\ \frac{\partial F}{\partial Y} = 0,$$

it is obviously closed. It will be proper unless $\partial F/\partial X$ and $\partial F/\partial Y$ are identically zero on V, and are therefore both multiples of F, but, since they have lower degree, this is impossible unless they are both zero. Clearly $\partial F/\partial X = 0$ if and only if F is a polynomial in Y (k of characteristic zero) or is a polynomial in X^p and Y (k of characteristic p). A similar remark applies to $\partial F/\partial Y$. Thus if $\partial F/\partial X$ and $\partial F/\partial Y$ are both zero, then F is constant (characteristic zero) or a polynomial in X^p, Y^p, and hence a p^{th} power (characteristic p). These are contrary to our assumptions. □

The set of singular points of a variety is often called the *singular locus* of the variety.

Tangent cones to plane curves. Note that if $P = (0, 0)$, then the equation defining the tangent space is the linear term of F: since $(0, 0)$ is on V,

$$F = aX + bY + \text{terms of higher degree},$$

and the equation of the tangent space is $F_\ell(X, Y) \stackrel{\text{df}}{=} aX + bY = 0$.

In general a polynomial $F(X, Y)$ can be written (uniquely) as a finite sum

$$F = F_0 + F_1 + F_2 + \cdots + F_m + \cdots$$

where F_m is a homogeneous polynomial of degree m. The first nonzero term on the right (the homogeneous summand of F of least degree) will be written F_* and called the *leading form* of F.

DEFINITION 4.4. Let $F(X, Y)$ be a polynomial without square factors, and let V be the curve defined by F. If $(0, 0) \in V$, then the *geometric tangent cone* to V at $(0, 0)$ is the zero set of F_*. The *tangent cone* is the pair $(V(F_*), F_*)$. To obtain the tangent cone at any other point, translate to the origin, and then translate back.

EXAMPLE 4.5. (a) $Y^2 = X^3$: the geometric tangent cone at $(0, 0)$ is given by $Y^2 = 0$ — it is the X-axis (doubled).

(b) $Y^2 = X^2(X + 1)$: the geometric tangent cone at (0,0) is given by $Y^2 = X^2$ — it is the pair of lines $Y = \pm X$.

[13] In common usage, "singular" means uncommon or extraordinary as in, for example, he spoke with singular shrewdness. Thus the proposition says that singular points (mathematical sense) are singular (usual sense).

(c) $(X^2+Y^2)^2+3X^2Y-Y^3=0$: the geometric tangent cone at $(0,0)$ is given by $3X^2Y-Y^3=0$ — it is the union of the lines $Y=0$, $Y=\pm\sqrt{3X}$.

(d) $(X^2+Y^2)^3-4X^2Y^2=0$: the geometric tangent cone at $(0,0)$ is given by $4X^2Y^2=0$ — it is the union of the x and y axes (each doubled).

In general we can factor F_* as

$$F_*(X,Y)=\prod X^{r_0}(Y-a_iX)^{r_i}.$$

Then $\deg F_*=\sum r_i$ is called the *multiplicity* of the singularity, $\mathrm{mult}_P(V)$. A multiple point is *ordinary* if its tangents are nonmultiple, i.e., $r_i=1$ all i. An ordinary double point is called a *node*, and a nonordinary double point is called a *cusp*. (There are many names for special types of singularities — see any book, especially an old book, on curves.)

The local ring at a point on a curve.

PROPOSITION 4.6. *Let P be a point on a curve V, and let $\mathfrak{m}$ be the corresponding maximal ideal in $k[V]$. If P is nonsingular, then $\dim_k \mathfrak{m}/\mathfrak{m}^2=1$, and otherwise $\dim_k \mathfrak{m}/\mathfrak{m}^2=2$.*

PROOF. Assume first that $P=(0,0)$. Then $\mathfrak{m}=(x,y)$ in $k[V]=k[X,Y]/(F(X,Y))=k[x,y]$. Note that $\mathfrak{m}^2=(x^2,xy,y^2)$, and

$$\mathfrak{m}/\mathfrak{m}^2=(X,Y)/(\mathfrak{m}^2+F(X,Y))=(X,Y)/(X^2,XY,Y^2,F(X,Y)).$$

In this quotient, every element is represented by a linear polynomial $cx+dy$, and the only relation is $F_\ell(x,y)=0$. Clearly $\dim \mathfrak{m}/\mathfrak{m}^2=1$ if $F_\ell\neq 0$, and $\dim\mathfrak{m}/\mathfrak{m}^2=2$ otherwise. Since $F_\ell=0$ is the equation of the tangent space, this proves the proposition in this case.

The same argument works for an arbitrary point (a,b) except that one uses the variables $X'=X-a$ and $Y'=Y-b$ — in essence, one translates the point to the origin. □

We explain what the condition $\dim_k(\mathfrak{m}/\mathfrak{m}^2)=1$ means for the local ring $\mathcal{O}_P=k[V]_{\mathfrak{m}}$ — see later for more details. Let $\mathfrak{n}$ be the maximal ideal $\mathfrak{m}k[V]_{\mathfrak{m}}$ of this local ring. The map $\mathfrak{m}\to\mathfrak{n}$ induces an isomorphism $\mathfrak{m}/\mathfrak{m}^2\to\mathfrak{n}/\mathfrak{n}^2$, and so we have

$$P \text{ nonsingular} \iff \dim_k \mathfrak{m}/\mathfrak{m}^2=1 \iff \dim_k \mathfrak{n}/\mathfrak{n}^2=1.$$

Nakayama's lemma shows that the last condition is equivalent to $\mathfrak{n}$ being a principal ideal. Since $\mathcal{O}_P$ is of dimension 1, $\mathfrak{n}$ being principal means $\mathcal{O}_P$ is a regular local ring of dimension 1, and hence a discrete valuation ring, i.e., a principal ideal domain with exactly one prime element (up to associates). Thus, for a curve,

$$P \text{ nonsingular} \iff \mathcal{O}_P \text{ regular} \iff \mathcal{O}_P \text{ is a discrete valuation ring.}$$

Tangent spaces of subvarieties of $\mathbb{A}^m$. Before defining tangent spaces at points of closed subvarietes of $\mathbb{A}^m$ we review some terminology from linear algebra.

Linear algebra. For a vector space k^m, let X_i be the i^{th} coordinate function $\mathbf{a} \mapsto a_i$. Thus $X_1, \dots, X_m$ is the dual basis to the standard basis for k^m. A linear form $\sum a_i X_i$ can be regarded as an element of the dual vector space $(k^m)^\vee = \text{Hom}(k^m, k)$.

Let $A = (a_{ij})$ be an $n \times m$ matrix. It defines a linear map $\alpha\colon k^m \to k^n$, by

$$\begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} \mapsto A \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix}.$$

Thus, if $\alpha(\mathbf{a}) = \mathbf{b}$, then

$$b_i = \sum_{j=1}^{m} a_{ij} a_j.$$

Write $X_1, \dots, X_m$ for the coordinate functions on k^m and $Y_1, \dots, Y_n$ for the coordinate functions on k^n. Then the last equation can be rewritten as:

$$Y_i \circ \alpha = \sum_{j=1}^{m} a_{ij} X_j.$$

This says that, when we apply α to $\mathbf{a}$, then the i^{th} coordinate of the result is $\sum_{j=1}^m a_{ij}(X_j \mathbf{a}) = \sum_{j=1}^m a_{ij} a_j$.

Tangent spaces. Consider an affine variety $V \subset k^m$, and let $\mathfrak{a} = I(V)$. The *tangent space* $T_{\mathbf{a}}(V)$ to V at $\mathbf{a} = (a_1, \dots, a_m)$ is the subspace of the vector space with origin $\mathbf{a}$ cut out by the linear equations

$$\sum_{i=1}^{m} \left.\frac{\partial F}{\partial X_i}\right|_{\mathbf{a}} (X_i - a_i) = 0, \qquad F \in \mathfrak{a}. \qquad (*).$$

Thus $T_{\mathbf{a}}(\mathbb{A}^m)$ is the vector space of dimension m with origin $\mathbf{a}$, and $T_{\mathbf{a}}(V)$ is the subspace of $T_{\mathbf{a}}(\mathbb{A}^m)$ defined by the equations (*).

Write $(dX_i)_{\mathbf{a}}$ for $(X_i - a_i)$; then the $(dX_i)_{\mathbf{a}}$ form a basis for the dual vector space $T_{\mathbf{a}}(\mathbb{A}^m)^\vee$ to $T_{\mathbf{a}}(\mathbb{A}^m)$—in fact, they are the coordinate functions on $T_{\mathbf{a}}(\mathbb{A}^m)$. As in advanced calculus, for a function $F \in k[X_1, \dots, X_m]$, we define the *differential* of F at $\mathbf{a}$ by the equation:

$$(dF)_{\mathbf{a}} = \sum \left.\frac{\partial F}{\partial X_i}\right|_{\mathbf{a}} (dX_i)_{\mathbf{a}}.$$

It is again a linear form on $T_{\mathbf{a}}(\mathbb{A}^m)$. In terms of differentials, $T_{\mathbf{a}}(V)$ is the subspace of $T_{\mathbf{a}}(\mathbb{A}^m)$ defined by the equations:

$$(dF)_{\mathbf{a}} = 0,\ F \in \mathfrak{a} \qquad (**).$$

I claim that, in (*) and (**), it suffices to take the F in a generating subset for $\mathfrak{a}$. The product rule for differentiation shows that if $G = \sum_j H_j F_j$, then

$$(dG)_{\mathbf{a}} = \sum_j H_j(\mathbf{a}) \cdot (dF_j)_{\mathbf{a}} + F_j(\mathbf{a}) \cdot (dG_j)_{\mathbf{a}}.$$

If $F_1,\dots,F_r$ generate $\mathfrak{a}$ and $\mathbf{a}\in V(\mathfrak{a})$, so that $F_j(\mathbf{a})=0$ for all j, then this equation becomes

$$(dG)_{\mathbf{a}}=\sum_j H_j(\mathbf{a})\cdot(dF_j)_{\mathbf{a}}.$$

Thus $(dG)_{\mathbf{a}}(\mathbf{t})=0$ if $(dF_j)_{\mathbf{a}}(\mathbf{t})=0$ for all j.

When V is irreducible, a point $\mathbf{a}$ on V is said to be *nonsingular (*or *smooth)* if the dimension of the tangent space at $\mathbf{a}$ is equal to the dimension of V; otherwise it is *singular (*or *multiple).* When V is reducible, we say $\mathbf{a}$ is *nonsingular* if $\dim T_{\mathbf{a}}(V)$ is equal to the maximum dimension of an irreducible component of V passing through $\mathbf{a}$. It turns out then that $\mathbf{a}$ is singular precisely when it lies on more than one irreducible component, or when it lies on only one but is a singular point of that component.

Let $\mathfrak{a}=(F_1,\dots,F_r)$, and let

$$J=\operatorname{Jac}(F_1,\dots,F_r)=\left(\frac{\partial F_i}{\partial X_j}\right)=\begin{pmatrix}\frac{\partial F_1}{\partial X_1}, & \dots, & \frac{\partial F_1}{\partial X_m}\\ \vdots & & \vdots\\ \frac{\partial F_r}{\partial X_1}, & \dots, & \frac{\partial F_r}{\partial X_m}\end{pmatrix}.$$

Then the equations defining $T_{\mathbf{a}}(V)$ as a subspace of $T_{\mathbf{a}}(\mathbb{A}^m)$ have matrix $J(\mathbf{a})$. Therefore, from linear algebra,

$$\dim_k T_{\mathbf{a}}(V)=m-\operatorname{rank}J(\mathbf{a}),$$

and so $\mathbf{a}$ is nonsingular if and only if the rank of $\operatorname{Jac}(F_1,\dots,F_r)(\mathbf{a})$ is equal to $m-\dim(V)$. For example, if V is a hypersurface, say $I(V)=(F(X_1,\dots,X_m))$, then

$$\operatorname{Jac}(F)(\mathbf{a})=\left(\frac{\partial F}{\partial X_1}(\mathbf{a}),\dots,\frac{\partial F}{\partial X_m}(\mathbf{a})\right),$$

and $\mathbf{a}$ is nonsingular if and only if not all of the partial derivatives $\frac{\partial F}{\partial X_i}$ vanish at $\mathbf{a}$.

We can regard J as a matrix of regular functions on V. For each r,

$$\{\mathbf{a}\in B\mid \operatorname{rank}J(\mathbf{a})\le r\}$$

is closed in V, because it the set where certain determinants vanish. Therefore, there is an open subset U of V on which $\operatorname{rank}J(\mathbf{a})$ attains its maximum value, and the rank jumps on closed subsets. Later we shall show that the maximum value of $\operatorname{rank}J(\mathbf{a})$ is $m-\dim V$, and so the nonsingular points of V form a nonempty open subset of V.

The differential of a map. Consider a regular map

$$\alpha\colon \mathbb{A}^m\to\mathbb{A}^n,\ a\mapsto(P_1(a_1,\dots,a_m),\dots,P_n(a_1,\dots,a_m)).$$

We think of α as being given by the equations

$$Y_i=P_i(X_1,\dots,X_m),\ i=1,\dots n.$$

It corresponds to the map of rings $\alpha^*\colon k[Y_1,\dots,Y_n]\to k[X_1,\dots,X_m]$ sending Y_i to $P_i(X_1,\dots,X_m)$, $i=1,\dots n$.

Define $(d\alpha)_{\mathbf{a}}\colon T_{\mathbf{a}}(\mathbb{A}^m)\to T_{\mathbf{b}}(\mathbb{A}^n)$ to be the map such that

$$(dY_i)_{\mathbf{b}}\circ(d\alpha)_{\mathbf{a}}=\sum\left.\frac{\partial P_i}{\partial X_j}\right|_{\mathbf{a}}(dX_j)_{\mathbf{a}},$$

i.e., relative to the standard bases, $(d\alpha)_{\mathbf{a}}$ is the map with matrix

$$\operatorname{Jac}(P_1,\dots,P_n)(\mathbf{a}) = \begin{pmatrix} \frac{\partial P_1}{\partial X_1}(\mathbf{a}), & \dots, & \frac{\partial P_1}{\partial X_m}(\mathbf{a}) \\ \vdots & & \vdots \\ \frac{\partial P_n}{\partial X_1}(\mathbf{a}), & \dots, & \frac{\partial P_n}{\partial X_m}(\mathbf{a}) \end{pmatrix}.$$

For example, suppose $\mathbf{a} = (0,\dots,0)$ and $\mathbf{b} = (0,\dots,0)$, so that $T_{\mathbf{a}}(\mathbb{A}^m) = k^m$ and $T_{\mathbf{b}}(\mathbb{A}^n) = k^n$, and

$$P_i = \sum_{j=1}^{m} c_{ij}X_j + (\text{higher terms}),\ i = 1,\dots,n.$$

Then $Y_i \circ (d\alpha)_{\mathbf{a}} = \sum_j c_{ij}X_j$, and the map on tangent spaces is given by the matrix (c_{ij}), i.e., it is simply $\mathbf{t} \mapsto (c_{ij})\mathbf{t}$.

Let $F \in k[X_1,\dots,X_m]$. We can regard F as a regular map $\mathbb{A}^m \to \mathbb{A}^1$, whose differential will be a linear map

$$(dF)_{\mathbf{a}}\colon T_{\mathbf{a}}(\mathbb{A}^m) \to T_{\mathbf{b}}(\mathbb{A}^1), \qquad \mathbf{b} = F(\mathbf{a}).$$

When we identify $T_{\mathbf{b}}(\mathbb{A}^1)$ with k, we obtain an identification of the differential of F (F regarded as a regular map) with the differential of F (F regarded as a regular function).

LEMMA 4.7. *Let $\alpha\colon \mathbb{A}^m \to \mathbb{A}^n$ be as at the start of this subsection. If α maps $V = V(\mathfrak{a}) \subset k^m$ into $W = V(\mathfrak{b}) \subset k^n$, then $(d\alpha)_{\mathbf{a}}$ maps $T_{\mathbf{a}}(V)$ into $T_{\mathbf{b}}(W)$, $\mathbf{b} = \alpha(\mathbf{a})$.*

PROOF. We are given that

$$f \in \mathfrak{b} \Rightarrow f \circ \alpha \in \mathfrak{a},$$

and have to prove that

$$f \in \mathfrak{b} \Rightarrow (df)_{\mathbf{b}} \circ (d\alpha)_{\mathbf{a}} \text{ is zero on } T_{\mathbf{a}}(V).$$

The chain rule holds in our situation:

$$\frac{\partial f}{\partial X_i} = \sum_{i=1}^{n} \frac{\partial f}{\partial Y_j}\frac{\partial Y_j}{\partial X_i}, \quad Y_j = P_j(X_1,\dots,X_m), \quad f = f(Y_1,\dots,Y_n).$$

If α is the map given by the equations

$$Y_j = P_j(X_1,\dots,X_m), \qquad j = 1,\dots,m,$$

then the chain rule implies

$$d(f \circ \alpha)_{\mathbf{a}} = (df)_{\mathbf{b}} \circ (d\alpha)_{\mathbf{a}}, \quad \mathbf{b} = \alpha(\mathbf{a}).$$

Let $\mathbf{t} \in T_{\mathbf{a}}(V)$; then

$$(df)_{\mathbf{b}} \circ (d\alpha)_{\mathbf{a}}(\mathbf{t}) = d(f \circ \alpha)_{\mathbf{a}}(\mathbf{t}),$$

which is zero if $f \in \mathfrak{b}$ because then $f \circ \alpha \in \mathfrak{a}$. Thus $(d\alpha)_{\mathbf{a}}(\mathbf{t}) \in T_{\mathbf{b}}(W)$. □

We therefore get a map $(d\alpha)_{\mathbf{a}}\colon T_{\mathbf{a}}(V) \to T_{\mathbf{b}}(W)$. The usual rules from advanced calculus (alias differential geometry) hold. For example,

$$(d\beta)_{\mathbf{b}} \circ (d\alpha)_{\mathbf{a}} = d(\beta \circ \alpha)_{\mathbf{a}}, \quad \mathbf{b} = \alpha(\mathbf{a}).$$

EXAMPLE 4.8. Let V be the union of the coordinate axes in $\mathbb{A}^3$, and let W be $V(XY(X-Y)) \subset \mathbb{A}^2$ (union of three lines). Then V is not isomorphic to W because $T_o(V)$ has dimension 3, but $T_o(W)$ has dimension 2. (Note that $V = V(XY, YZ, XZ)$, from which it is clear that the origin o is the only singular point on V, and that the tangent space there has dimension 3. An isomorphism $V \to W$ would have to send the singular point to the singular point, i.e., $o \mapsto o$, and map $T_o(V)$ isomorphically onto $T_o(W)$.)

Etale maps. Let V and W be smooth varieties. A regular map $\alpha\colon V \to W$ is *étale* at $\mathbf{a}$ if $(d\alpha)_{\mathbf{a}}\colon T_{\mathbf{a}}(V) \to T_{\mathbf{b}}(W)$ is an isomorphism; α is *étale* if it is étale at all points of V.

EXAMPLE 4.9. (a) A regular map $\alpha = (P_1, \dots, P_n)\colon \mathbb{A}^n \to \mathbb{A}^n$ is étale at $\mathbf{a}$ if and only if $\operatorname{rank} \operatorname{Jac}(P_1, \dots, P_n)(\mathbf{a}) = n$, because the map on the tangent spaces has matrix $\operatorname{Jac}(P_1, \dots, P_n)(\mathbf{a})$. Equivalent condition: $\det\left(\frac{\partial P_i}{\partial X_j}(\mathbf{a})\right) \neq 0$

(b) Let $V = \operatorname{Specm}(A)$ be an affine variety, and let $f = \sum c_i X^i \in A[X]$. Let $W = \operatorname{Specm}(A[X]/(f(X))$ (assuming this is an affine k-algebra), and consider the map $W \to V$ corresponding to the inclusion $A \hookrightarrow A[X]/(f)$. The points of W lying over a point $\mathbf{a} \in V$ correspond to the roots of $\sum c_i(\mathbf{a})X^i$. I claim that the map $W \to V$ is étale at a point $(\mathbf{a}, b)$ if and only if b is a simple root of $\sum c_i(\mathbf{a})X^i$.

To see this, write $A = \operatorname{Specm} k[X_1, \dots, X_n]/\mathfrak{a}$, $\mathfrak{a} = (f_1, \dots, f_r)$, so that $A[X]/(f) = k[X_1, \dots, X_n]/(f_1, \dots, f_r, f)$. The tangent spaces to W and V at $(\mathbf{a}, b)$ and $\mathbf{a}$ respectively are the null spaces of the matrices

$$\begin{pmatrix} \frac{\partial f_1}{\partial X_1}(\mathbf{a}) & \dots & \frac{\partial f_1}{\partial X_m}(\mathbf{a}) & 0 \\ \vdots & & \vdots & \\ \frac{\partial f_n}{\partial X_1}(\mathbf{a}) & \dots & \frac{\partial f_n}{\partial X_m}(\mathbf{a}) & 0 \\ \frac{\partial f}{\partial X_1}(\mathbf{a}) & \dots & \frac{\partial f}{\partial X_m}(\mathbf{a}) & \frac{\partial f}{\partial X}(\mathbf{a}, b) \end{pmatrix} \qquad \begin{pmatrix} \frac{\partial f_1}{\partial X_1}(\mathbf{a}) & \dots & \frac{\partial f_1}{\partial X_m}(\mathbf{a}) \\ \vdots & & \vdots \\ \frac{\partial f_n}{\partial X_1}(\mathbf{a}) & \dots & \frac{\partial f_n}{\partial X_m}(\mathbf{a}) \end{pmatrix}$$

and the map $T_{(\mathbf{a},b)}(W) \to T_{\mathbf{a}}(V)$ is induced by the projection map $k^{n+1} \to k^n$ that omits the last coordinate. This map is an isomorphism if and only if $\frac{\partial f}{\partial X}(\mathbf{a}, b) \neq 0$, because then any solution to the smaller set of equations extends uniquely to a solution of the larger set. But $\frac{\partial f}{\partial X}(\mathbf{a}, b) = \frac{d(\sum_i c_i(\mathbf{a})X^i)}{dX}(b)$, which is zero if and only if b is a multiple root of $\sum_i c_i(\mathbf{a})X^i$.

(c) Consider a dominating map $\alpha\colon W \to V$ of smooth affine varieties, corresponding to a map $A \to B$ of rings. Suppose B can be written $B = A[Y_1, \dots, Y_n]/(P_1, \dots, P_n)$ (same number of polynomials as variables). A similar argument to the above shows that α is étale if and only if $\det\left(\frac{\partial P_i}{\partial X_j}(\mathbf{a})\right) \neq 0$.

(d) The example in (b) is typical; in fact every étale map is locally of this form, provided V is normal (in the sense defined below). More precisely, let $\alpha\colon W \to V$ be étale at $P \in W$, and assume V to normal; then there exist a map $\alpha'\colon W' \to V'$ with $k[W'] = k[V'][X]/(f(X))$, and a commutative diagram

$$\begin{array}{ccccccc} W & \supset & U_1 & \approx & U_1' & \subset & W' \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ V & \supset & U_2 & \approx & U_2' & \subset & V' \end{array}$$

with the U's all open subvarieties and $P \in U_1$.

Warning! In advanced calculus (or differential geometry, or the theory of complex manifolds), the inverse function theorem says that a map α that is étale at a point $\mathbf{a}$ is a local isomorphism there, i.e., there exist open neighbourhoods U and U' of $\mathbf{a}$ and $\alpha(\mathbf{a})$ such that α induces an isomorphism $U \to U'$. **This is not true in algebraic geometry**, at least not for the Zariski topology: a map can be étale at a point without being a local isomorphism. Consider for example the map

$$\alpha\colon \mathbb{A}^1 \setminus \{0\} \to \mathbb{A}^1 \setminus \{0\}, \quad a \mapsto a^2.$$

This is étale if the characteristic is $\neq 2$, because the Jacobian matrix is $(2X)$, which has rank one for all $X \neq 0$ (alternatively, it is of the form (4.9b) with $f(X) = X^2 - T$, where T is the coordinate function on $\mathbb{A}^1$, and $X^2 - c$ has distinct roots for $c \neq 0$). Nevertheless, I claim that there do not exist nonempty open subsets U and U' of $\mathbb{A}^1 - \{0\}$ such that α defines an isomorphism $U \to U'$. If there did, then α would define an isomorphism $k[U'] \to k[U]$ and hence an isomorphism on the fields of fractions $k(\mathbb{A}^1) \to k(\mathbb{A}^1)$. But on the fields of fractions, α defines the map $k(X) \to k(X)$, $X \mapsto X^2$, which is not an isomorphism.

Aside 4.10. There is a conjecture that any étale map $\alpha\colon \mathbb{A}^n \to \mathbb{A}^n$ is an isomorphism. If we write $\alpha = (P_1, \dots, P_n)$, then this becomes the statement

$$\det\left(\frac{\partial P_i}{\partial X_j}(\mathbf{a})\right) \neq 0 \text{ all } \mathbf{a} \Rightarrow \alpha \text{ has a inverse.}$$

The condition, $\det\left(\frac{\partial P_i}{\partial X_j}(\mathbf{a})\right) \neq 0$ all $\mathbf{a}$, implies that $\det\left(\frac{\partial P_i}{\partial X_j}\right)$ is a nonzero constant. This conjecture, which is known as the Jacobian problem, has not been solved in general as far as I know. It has caused many mathematicians a good deal of grief. It is probably harder than it is interesting. See Bass et al., Bull. AMS **7** (1982), 287-330.

Intrinsic definition of the tangent space. The definition we have given of the tangent space at a point requires the variety to be embedded in affine space. In this subsection, we give a more intrinsic definition.

By a *linear form* in $X_1, \dots, X_n$ we mean an expression $\sum c_i X_i$, $c_i \in k$. The linear forms form a vector space of dimension n, which is naturally dual to k^n.

Lemma 4.11. *Let $\mathfrak{c}$ be an ideal in $k[X_1, \dots, X_n]$ generated by linear forms, $\ell_1, \dots, \ell_r$, which we may assume to be linearly independent. Let $X_{i_1}, \dots, X_{i_{n-r}}$ be such that $\{\ell_1, \dots, \ell_r, X_{i_1}, \dots, X_{i_{n-r}}\}$ is a basis for the linear forms in $X_1, \dots, X_n$. Then $k[X_1, \dots, X_n]/\mathfrak{c} \cong k[X_{i_1}, \dots, X_{i_{n-r}}]$.*

Proof. This is obvious if the linear forms $\ell_1, \dots, \ell_r$ are $X_1, \dots, X_r$. In the general case, because $\{X_1, \dots, X_n\}$ and $\{\ell_1, \dots, \ell_r, X_{i_1}, \dots, X_{i_{n-r}}\}$ are both bases for the linear forms, each element of one set can be expressed as a linear combination of the elements of the second set. Therefore

$$k[X_1, \dots, X_n] = k[\ell_1, \dots, \ell_r, X_{i_1}, \dots, X_{i_{n-r}}]$$

and so

$$k[X_1, \dots, X_n]/\mathfrak{c} = k[\ell_1, \dots, \ell_r, X_{i_1}, \dots, X_{i_{n-r}}]/(\ell_1, \dots, \ell_r) \cong k[X_{i_1}, \dots, X_{i_{n-r}}].$$

□

Let $V = V(\mathfrak{a}) \subset k^n$, and assume the origin $P \in V$. Let $\mathfrak{a}_\ell$ be the ideal generated by the linear terms f_ℓ of the $f \in \mathfrak{a}$. By definition, $T_P(V) = V(\mathfrak{a}_\ell)$. Let $A_\ell = k[X_1, \dots, X_n]/\mathfrak{a}_\ell$, and let $\mathfrak{m}$ be the maximal ideal in $k[V]$ corresponding to the origin; thus $\mathfrak{m} = (x_1, \dots, x_n)$.

PROPOSITION 4.12. *There are canonical isomorphisms*

$$\mathrm{Hom}_{k\text{-}linear}(\mathfrak{m}/\mathfrak{m}^2, k) \xrightarrow{\cong} \mathrm{Hom}_{k\text{-}alg}(A_\ell, k) \xrightarrow{\cong} T_P(V).$$

PROOF. First isomorphism. Let $\mathfrak{n} = (X_1, \dots, X_n)$ be the maximal ideal at the origin in $k[X_1, \dots, X_n]$. Then $\mathfrak{m}/\mathfrak{m}^2 = \mathfrak{n}/(\mathfrak{n}^2 + \mathfrak{a})$, and as $f - f_\ell \in \mathfrak{n}^2$ for every $f \in \mathfrak{a}$, we have $\mathfrak{m}/\mathfrak{m}^2 = \mathfrak{n}/(\mathfrak{n}^2 + \mathfrak{a}_\ell)$. Let $f_{1,\ell}, \dots, f_{r,\ell}$ be a basis for the vector space $\mathfrak{a}_\ell$; there are $n - r$ indeterminates $X_{i_1} \dots, X_{i_{n-r}}$ forming with the $f_{i,\ell}$ a basis for the linear forms on k^n. Then $X_{i_1} + \mathfrak{m}^2, \dots, X_{i_{n-r}} + \mathfrak{m}^2$ form a basis for $\mathfrak{m}/\mathfrak{m}^2$ as a k-vector space, and the lemma shows that $A_\ell = k[X_{i_1} \dots, X_{i_{n-r}}]$. Any homomorphism $\alpha\colon A_\ell \to k$ of k-algebras is determined by its values $\alpha(X_{i_1}), \dots, \alpha(X_{i_{n-r}})$, and they can be arbitrarily given. Since the k-linear maps $\mathfrak{m}/\mathfrak{m}^2 \to k$ have a similar description, the first isomorphism is now obvious.

Second isomorphism. To give a k-algebra homomorphism $A_\ell \to k$ is the same as to give an element $(a_1, \dots, a_n) \in k^n$ such that $f(a_1, \dots, a_n) = 0$ for all $f \in A_\ell$, which is the same as to give an element of $T_P(V)$. □

LEMMA 4.13. *Let $\mathfrak{m}$ be a maximal ideal of a ring A, and let $\mathfrak{n} = \mathfrak{m}A_\mathfrak{m}$. For all n, the map*

$$a + \mathfrak{m}^n \mapsto a + \mathfrak{n}^n\colon A/\mathfrak{m}^n \to A_\mathfrak{m}/\mathfrak{n}^n$$

is an isomorphism. Moreover, it induces isomorphisms

$$\mathfrak{m}^r/\mathfrak{m}^n \to \mathfrak{n}^r/\mathfrak{n}^n$$

for all $r < n$.

PROOF. The second statement follows from the first, because of the exact commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathfrak{m}^r/\mathfrak{m}^n & \longrightarrow & A/\mathfrak{m}^n & \longrightarrow & A/\mathfrak{m}^r & \longrightarrow & 0 \\ & & \downarrow & & \downarrow\approx & & \downarrow\approx & & \\ 0 & \longrightarrow & \mathfrak{n}^r/\mathfrak{n}^n & \longrightarrow & A_\mathfrak{m}/\mathfrak{n}^n & \longrightarrow & A_\mathfrak{m}/\mathfrak{n}^r & \longrightarrow & 0. \end{array}$$

To simplify the exposition, in proving that the first map is an isomorphism, I'll assume $A \subset S^{-1}A$. In order to show that the map $A/\mathfrak{m}^n \to A_\mathfrak{n}/\mathfrak{n}^n$ is injective, we have to show that $\mathfrak{n}^m \cap A = \mathfrak{m}^m$. But $\mathfrak{n}^m = S^{-1}\mathfrak{m}^m$, $S = A - \mathfrak{m}$, and so we have to show that $\mathfrak{m}^m = (S^{-1}\mathfrak{m}^m) \cap A$. An element of $(S^{-1}\mathfrak{m}^m) \cap A$ can be written $a = b/s$ with $b \in \mathfrak{m}^m$, $s \in S$, and $a \in A$. Then $sa \in \mathfrak{m}^m$, and so $sa = 0$ in $A/\mathfrak{m}^m$. The only maximal ideal containing $\mathfrak{m}^m$ is $\mathfrak{m}$ (because $\mathfrak{m}' \supset \mathfrak{m}^m \Rightarrow \mathfrak{m}' \supset \mathfrak{m}$), and so the only maximal ideal in $A/\mathfrak{m}^m$ is $\mathfrak{m}/\mathfrak{m}^m$; in particular, $A/\mathfrak{m}^m$ is a local ring. As s is not in $\mathfrak{m}/\mathfrak{m}^m$, it is a unit in $A/\mathfrak{m}^m$, and so $sa = 0$ in $A/\mathfrak{m}^m$ implies $a = 0$ in $A/\mathfrak{m}^m$, i.e., $a \in \mathfrak{m}^m$.

We now prove that the map is surjective. Let $\frac{a}{s} \in A_\mathfrak{m}$. Because $s \notin \mathfrak{m}$ and $\mathfrak{m}$ is maximal, we have that $(s) + \mathfrak{m} = A$, i.e., (s) and $\mathfrak{m}$ are relatively prime. Therefore (s) and $\mathfrak{m}^m$ are relatively prime (no maximal ideal contains both of them), and so there exist $b \in A$ and $q \in \mathfrak{m}^m$ such that $bs + q = 1$. Then b maps to s^{-1} in $A_\mathfrak{m}/\mathfrak{n}^m$ and

so ba maps to $\frac{a}{s}$. More precisely: because s is invertible in $A_{\mathfrak{m}}/\mathfrak{n}^m$, $\frac{a}{s}$ is the *unique* element of this ring such that $s\frac{a}{s} = a$; since $s(ba) = a(1-q)$, the image of ba in $A_{\mathfrak{m}}$ also has this property and therefore equals $\frac{a}{s}$. □

Therefore, we also have a canonical isomorphism

$$T_P(V) \xrightarrow{\approx} \mathrm{Hom}_{k\text{-lin}}(\mathfrak{n}_P/\mathfrak{n}_P^2, k),$$

where $\mathfrak{n}_P$ is now the maximal ideal in $\mathcal{O}_P$ $(= A_{\mathfrak{m}})$.

DEFINITION 4.14. The *tangent space* $T_P(V)$ at a point P of a variety V is $\mathrm{Hom}_{k\text{-lin}}(\mathfrak{n}_P/\mathfrak{n}_P^2, k)$, where $\mathfrak{n}_P$ the maximal ideal in $\mathcal{O}_P$.

When V is embedded in affine space, the above remarks show that this definition agrees with the more explicit definition on p68. The advantage of the present definition is that it depends only on a (small) neighbourhood of P. In particular, it doesn't depend on an affine embedding of V.

A regular map $\alpha\colon V \to W$ sending P to Q defines a local homomorphism $\mathcal{O}_Q \to \mathcal{O}_P$, which induces maps $\mathfrak{m}_Q \to \mathfrak{m}_P$, $\mathfrak{m}_Q/\mathfrak{m}_Q^2 \to \mathfrak{m}_P/\mathfrak{m}_P^2$, and $T_P(V) \to T_Q(W)$. The last map is written $(d\alpha)_P$. When some open neighbourhoods of P and Q are realized as closed subvarieties of affine space, then $(d\alpha)_P$ becomes identified with the map defined earlier.

In particular, if $f \in \mathfrak{m}_P$, then f is represented by a regular map $U \to \mathbb{A}^1$, $P \mapsto 0$, and hence defines a linear map $(df)_P\colon T_P(V) \to k$. This is just the map sending a tangent vector (element of $\mathrm{Hom}_{k\text{-lin}}(\mathfrak{m}_P/\mathfrak{m}_P^2, k)$) to its value at $f \mod \mathfrak{m}_P^2$. Again, in the concrete situation $V \subset \mathbb{A}^m$ this agrees with the previous definition. In general, for $f \in \mathcal{O}_P$, i.e., for f a germ of a function at P, we define

$$(df)_P = f - f(P) \mod \mathfrak{m}^2.$$

The tangent space at P and the space of differentials at P are dual vector spaces—in contrast to the situation in advanced calculus, for us it is easier to define first the space of differentials, and then define the tangent space to be its dual.

Consider for example, $\mathbf{a} \in V(\mathfrak{a}) \subset \mathbb{A}^n$, with $\mathfrak{a}$ a radical ideal. For $f \in k[\mathbb{A}^n] = k[X_1, \dots, X_n]$, we have (trivial Taylor expansion)

$$f = f(P) + \sum c_i(X_i - a_i) + \text{terms of degree } \geq 2 \text{ in the } X_i - a_i,$$

that is,

$$f - f(P) \equiv \sum c_i(X_i - a_i) \mod \mathfrak{m}_P^2.$$

Therefore $(df)_P$ can be identified with

$$\sum c_i(X_i - a_i) = \sum \left.\frac{\partial f}{\partial X_i}\right|_{\mathbf{a}} (X_i - a_i),$$

which is how we originally defined the differential.[14] The tangent space $T_{\mathbf{a}}(V(\mathfrak{a}))$ is the zero set of the equations

$$(df)_P = 0, \qquad f \in \mathfrak{a},$$

[14]The same discussion applies to any $f \in \mathcal{O}_P$. Such an f is of the form $\frac{g}{h}$ with $h(\mathbf{a}) \neq 0$, and has a (not quite so trivial) Taylor expansion of the same form, but with an infinite number of terms, i.e., it lies in the power series ring $k[[X_1 - a_1, \dots, X_n - a_n]]$.

and the set $\{(df)_P|_{T_{\mathfrak{a}}(V)} \mid f \in k[X_1, \dots, X_n]\}$ is the dual space to $T_{\mathfrak{a}}(V)$.

The dimension of the tangent space. In this subsection we show that the dimension of the tangent space is at least that of the variety. First we review some commutative algebra.

Some commutative algebra. Let S be a multiplicative subset of a ring A, and let $S^{-1}A$ be the corresponding ring of fractions. Any ideal $\mathfrak{a}$ in A, generates an ideal $S^{-1}\mathfrak{a}$ in $S^{-1}A$. If $\mathfrak{a}$ contains an element of S, then $S^{-1}\mathfrak{a}$ contains a unit, and so is the whole ring. Thus some of the ideal structure of A is lost in the passage to $S^{-1}A$, but, as the next lemma shows, some is retained.

PROPOSITION 4.15. *Let S be a multiplicative subset of the ring A. The map $\mathfrak{p} \mapsto S^{-1}\mathfrak{p} = \mathfrak{p}(S^{-1}A)$ is a bijection from the set of prime ideals of A disjoint from S to the set of prime ideals of $S^{-1}A$.*

PROOF. It is straightforward to verify that

$$\mathfrak{q} \mapsto (\text{inverse image of } \mathfrak{q} \text{ in } A)$$

provides an inverse to $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$. (See Atiyah and MacDonald 1969, p41–42.) □

For example, let V be an affine variety and P a point on V. The proposition shows that there is a one-to-one correspondence between the prime ideals of $k[V]$ contained in $\mathfrak{m}_P$ and the prime ideals of $\mathcal{O}_P$. In geometric terms, this says that there is a one-to-one correspondence between the prime ideals in $\mathcal{O}_P$ and the irreducible closed subvarieties of V passing through P.

Now let A be a local Noetherian ring with maximal ideal $\mathfrak{m}$. Then $\mathfrak{m}$ is an A-module, and the action of A on $\mathfrak{m}/\mathfrak{m}^2$ factors through $k \overset{\text{df}}{=} A/\mathfrak{m}$.

PROPOSITION 4.16. *The elements $a_1, \dots, a_n$ of $\mathfrak{m}$ generate $\mathfrak{m}$ as an ideal if and only if their residues modulo $\mathfrak{m}^2$ generate $\mathfrak{m}/\mathfrak{m}^2$ as a vector space over k. In particular, the minimum number of generators for the maximal ideal is equal to the dimension of the vector space $\mathfrak{m}/\mathfrak{m}^2$.*

PROOF. If $a_1, \dots, a_n$ generate $\mathfrak{m}$, it is obvious that their residues generate $\mathfrak{m}/\mathfrak{m}^2$. Conversely, suppose that their residues generate $\mathfrak{m}/\mathfrak{m}^2$, so that $\mathfrak{m} = (a_1, \dots, a_n) + \mathfrak{m}^2$. Since A is Noetherian and (hence) $\mathfrak{m}$ is finitely generated, Nakayama's lemma, applied with $M = \mathfrak{m}$ and $N = (a_1, \dots, a_n)$, shows that $\mathfrak{m} = (a_1, \dots, a_n)$. □

LEMMA 4.17 (Nakayama's Lemma). *Let A be a local Noetherian ring, and let M be a finitely generated A-module. If N is a submodule of M such that $M = N + \mathfrak{m}M$, then $M = N$.*

PROOF. After replacing M with the quotient module M/N, we can assume that $N = 0$. Thus we have to show that if $M = \mathfrak{m}M$, then $M = 0$. Let $x_1, \dots, x_n$ generate M, and write

$$x_i = \sum_j a_{ij} x_j$$

for some $a_{ij} \in \mathfrak{m}$. We see that $x_1, \dots, x_n$ can be considered to be solutions to the system of n equations in n variables

$$\sum_j (\delta_{ij} - a_{ij})x_j = 0, \quad \delta_{ij} = \text{Kronecker delta},$$

and so Cramer's rule tells us that $\det(\delta_{ij} - a_{ij}) \cdot x_i = 0$ for all i. But on expanding it out, we find that $\det(\delta_{ij} - a_{ij}) = 1 + m$ with $m \in \mathfrak{m}$. In particular, $\det(\delta_{ij} - a_{ij}) \notin \mathfrak{m}$, and so it is a unit. We deduce that all the x_i are zero, and that $M = 0$. □

A Noetherian local ring A of Krull dimension d is said to be *regular* if its maximal ideal can be generated by d elements. Thus A is regular if and only if its Krull dimension is equal to the dimension of $\mathfrak{m}/\mathfrak{m}^2$.

Two results from Section 7. We shall need to use two results that won't be proved until §7.

4.18. *For any irreducible variety V and regular functions $f_1, \dots, f_r$ on V, the irreducible components of $V(f_1, \dots, f_r)$ have codimension $\leq r$.*

Note that for polynomials of degree 1 on k^n, this is familiar from linear algebra: A system of r linear equations in n variables either has no solutions (the equations are inconsistent) or has a family of solutions of dimension at least $n - r$.

Recall that the Krull dimension of a Noetherian local ring A is the maximum length of a chain of prime ideals:

$$\mathfrak{m} = \mathfrak{p}_0 \supsetneqq \mathfrak{p}_1 \supsetneqq \cdots \supsetneqq \mathfrak{p}_d.$$

In §7, we shall prove:

4.19. *If V is an irreducible variety of dimension d, then the local ring at each point P of V has dimension d.*

The *height* of a prime ideal $\mathfrak{p}$ in a Noetherian ring A, is the maximum length of a chain of prime ideals:

$$\mathfrak{p} = \mathfrak{p}_0 \supsetneqq \mathfrak{p}_1 \supsetneqq \cdots \supsetneqq \mathfrak{p}_d.$$

Because of (4.15), the height of $\mathfrak{p}$ is the Krull dimension of $A_{\mathfrak{p}}$. Thus the above result can be restated as: If V is an irreducible affine variety of dimension d, then every maximal ideal in $k[V]$ has height d.

Sketch of proof of (4.19): If $V = \mathbb{A}^d$, then $A = k[X_1, \dots, X_d]$, and all maximal ideals in this ring have height d, for example,

$$(X_1 - a_1, \dots, X_d - a_d) \supset (X_1 - a_1, \dots, X_{d-1} - a_{d-1}) \supset \dots \supset (X_1 - a_1) \supset 0$$

is a chain of prime ideals of length d that can't be refined. In the general case, the Noether normalization theorem says that $k[V]$ is integral over a polynomial ring $k[x_1, \dots, x_d]$, $x_i \in k[V]$; then clearly $x_1, \dots, x_d$ is a transcendence basis for $k(V)$, and the going up and down theorems (see Atiyah and MacDonald 1969, Chapt 5) show that the local rings of $k[V]$ and $k[x_1, \dots, x_d]$ have the same dimension.

The dimension of the tangent space. Note that (4.16) implies that the dimension of $T_P(V)$ is the minimum number of elements needed to generate $\mathfrak{n}_P \subset \mathcal{O}_P$.

THEOREM 4.20. *Let V be irreducible; then* $\dim T_P(V) \geq \dim(V)$, *and equality holds if and only if $\mathcal{O}_P$ is regular.*

PROOF. Suppose $f_1, \dots, f_r$ generate the maximal ideal $\mathfrak{n}_P$ in $\mathcal{O}_P$. Then $f_1, \dots, f_r$ are all defined on some open affine neighbourhood U of P, and I claim that P is an irreducible component of the zero-set $V(f_1, \dots, f_r)$ of $f_1, \dots, f_r$ in U. If not, there will be some irreducible component $Z \neq P$ of $V(f_1, \dots, f_r)$ passing through P. Write $Z = V(\mathfrak{p})$ with $\mathfrak{p}$ a prime ideal in $k[U]$. Because $V(\mathfrak{p}) \subset V(f_1, \dots, f_r)$ and because Z contains P and is not equal to it, we have

$$(f_1, \dots, f_r) \subset \mathfrak{p} \subsetneqq \mathfrak{m}_P \qquad \text{(ideals in } k[U]\text{)}.$$

On passing to the local ring $\mathcal{O}_P = k[U]_{\mathfrak{m}_P}$, we find (using 4.15) that

$$(f_1, \dots, f_r) \subset \mathfrak{p}\mathcal{O}_P \subsetneqq \mathfrak{n}_P \qquad \text{(ideals in } \mathcal{O}_P\text{)}.$$

This contradicts the assumption that the f_i generate $\mathfrak{m}_P$. Hence P is an irreducible component of $V(f_1, \dots, f_r)$, and (4.18) implies that

$$r \geq \operatorname{codim} P = \dim V.$$

Since the dimension of $T_P(V)$ is the minimum value of r, this implies that $\dim T_P(V) \geq \dim V$. If equality holds, then $\mathfrak{m}_P$ can be generated by $\dim V$ elements, which (because of 4.19) implies that $\mathcal{O}_P$ is regular. Conversely, if $\mathcal{O}_P$ is regular, then the minimum value of r is $\dim V$, and so equality holds. □

As in the affine case, we define a point P to be *nonsingular* if $\dim T_P(V) = \dim V$. Thus a point P is nonsingular if and only if $\mathcal{O}_P$ is a regular local ring. In more geometric terms, we can say that a point P on a variety V of dimension d is nonsingular if and only if it can be defined by d equations in some neighbourhood of the point; more precisely, P is nonsingular if there exists an open neighbourhood U of P and d regular functions $f_1, \dots, f_d$ on U that generate the ideal $\mathfrak{m}_P$.

According to (Atiyah and MacDonald 1969, 11.23), a regular local ring is an integral domain. This provides another explanation of why a point on the intersection of two irreducible components of a variety can't be nonsingular: the local ring at such a point in not an integral domain. (Suppose $P \in Z_1 \cap Z_2$, with $Z_1 \cap Z_2 \neq Z_1, Z_2$. Since $Z_1 \cap Z_2 \neq Z_1$, there is a nonzero regular function f_1 defined on an open neighbourhood U of P in Z_1 that is zero on $U \cap Z_1 \cap Z_2$. Extend f_1 to a neighbourhood of P in $Z_1 \cup Z_2$ by setting $f_1(Q) = 0$ for all $Q \in Z_2$. Then f_1 defines a germ of regular function at P. Similarly construct a function f_2 that is zero on Z_1. Then f_1 and f_2 define nonzero germs of functions at P, but their product is zero.)

An integral domain that is integrally closed in its field of fractions is also called a *normal* ring.

An algebraic variety is *normal* if $\mathcal{O}_P$ is normal for all $P \in V$. Equivalent condition (Atiyah and MacDonald 1969, 5.13): for all open affines $U \subset V$, $k[U]$ is a finite product of normal rings. Since, as we just noted, the local ring at a point lying on two irreducible components can't be an integral domain, a normal variety is a disjoint union of irreducible varieties.

A regular local Noetherian ring is always normal (cf. Atiyah and MacDonald 1969, p123); conversely, a normal local integral domain *of dimension one* is regular (ibid.). Thus nonsingular varieties are normal, and normal curves are nonsingular. However, a normal surface need not be nonsingular: the cone

$$X^2 + Y^2 - Z^2 = 0$$

is normal, but is singular at the origin — the tangent space at the origin is k^3. However, it is true that the singular locus of a normal variety must have codimension ≥ 2. For example, a normal surface can only have isolated singularities — the singular locus can't contain a curve.

Singular points are singular. The set of singular points on a variety is called the *singular locus* of the variety.

THEOREM 4.21. *The nonsingular points of a variety V form a dense open subset.*

PROOF. We have to show that the singular points form a proper closed subset of every irreducible component of V.

Closed: We can assume that V is affine, say $V = V(\mathfrak{a}) \subset \mathbb{A}^n$. Let $P_1, \dots, P_r$ generate $\mathfrak{a}$. Then the set of singular points is the zero set of the ideal generated by the $(n-d) \times (n-d)$ minors of the matrix

$$\mathrm{Jac}(P_1, \dots, P_r)(\mathbf{a}) = \begin{pmatrix} \frac{\partial P_1}{\partial X_1}(\mathbf{a}) & \dots & \frac{\partial P_1}{\partial X_m}(\mathbf{a}) \\ \vdots & & \vdots \\ \frac{\partial P_r}{\partial X_1}(\mathbf{a}) & \dots & \frac{\partial P_r}{\partial X_m}(\mathbf{a}) \end{pmatrix}$$

Proper: Suppose first that V is an irreducible hypersurface in $\mathbb{A}^{d+1}$, i.e., that it is the zero set of a single nonconstant irreducible polynomial $F(X_1, \dots, X_{d+1})$. By (1.21), $\dim V = d$. In this case, the proof is the same as that of (4.3): if $\frac{\partial F}{\partial X_1}$ is identically zero on $V(F)$, then $\frac{\partial F}{\partial X_1}$ must be divisible by F, and hence be zero. Thus F must be a polynomial in $X_2, \dots X_{d+1}$ (characteristic zero) or in $X_1^p, X_2, \dots, X_{d+1}$ (characteristic p). Therefore, if all the points of V are singular, then F is constant (characteristic 0) or a p^{th} power (characteristic p) which contradict the hypothesis.

We shall complete the proof by showing (Lemma 4.21) that there is a nonempty open subset of V that is isomorphic to a nonempty open subset of an irreducible hypersurface in $\mathbb{A}^{d+1}$. □

Two irreducible varieties V and W are said to be *birationally equivalent* if $k(V) \approx k(W)$.

LEMMA 4.22. *Two irreducible varieties V and W are birationally equivalent if and only if there are open subsets U and U' of V and W respectively such that $U \approx U'$.*

PROOF. Assume that V and W are birationally equivalent. We may suppose that V and W are affine, corresponding to the rings A and B say, and that A and B have a common field of fractions K. Write $B = k[x_1, \dots, x_n]$. Then $x_i = a_i/b_i$, $a_i, b_i \in A$, and $B \subset A_{b_1 \dots b_r}$. Since $\mathrm{Specm}(A_{b_1 \dots b_r})$ is a basic open subvariety of V, we may replace

A with $A_{b_1\dots b_r}$, and suppose that $B \subset A$. The same argument shows that there exists a $d \in B \subset A$ such $A \subset B_d$. Now

$$B \subset A \subset B_d \Rightarrow B_d \subset A_d \subset (B_d)_d = B_d,$$

and so $A_d = B_d$. This shows that the open subvarieties $D(b) \subset V$ and $D(b) \subset W$ are isomorphic. This proves the "only if" part, and the "if" part is obvious. □

LEMMA 4.23. *Let V be an irreducible algebraic variety of dimension d; then there is a hypersurface H in $\mathbb{A}^{d+1}$ birationally equivalent to V.*

PROOF. Let $K = k(x_1, \dots, x_n)$, and assume $n > d+1$. After renumbering, we may suppose that $x_1, \dots, x_d$ are algebraically independent. Then $f(x_1, \dots, x_{d+1}) = 0$ for some nonzero irreducible polynomial $f(X_1, \dots, X_{d+1})$ with coefficients in k. Not all $\partial f/\partial X_i$ are zero, for otherwise k will have characteristic $p \neq 0$ and f will be a p^{th} power. After renumbering, we may suppose that $\partial f/\partial X_{d+1} \neq 0$. Then $k(x_1, \dots, x_{d+1}, x_{d+2})$ is algebraic over $k(x_1, \dots, x_d)$ and x_{d+1} is separable over $k(x_1, \dots, x_d)$, and so, by the Primitive Element Theorem (my notes on Fields and Galois Theory 5.1), there is an element y such that $k(x_1, \dots, x_{d+2}) = k(x_1, \dots, x_d, y)$. Thus K is generated by $n-1$ elements (as a field containing k). After repeating the process, possibly several times, we will have $K = k(z_1, \dots, z_{d+1})$ with z_{d+1} separable over $k(z_1, \dots, z_d)$. Now take f to be an irreducible polynomial satisfied by $z_1, \dots, z_{d+1}$ and H to be the hypersurface $f = 0$. □

COROLLARY 4.24. *Any algebraic group G is nonsingular.*

PROOF. From the theorem we know that there is an open dense subset U of G of nonsingular points. For any $g \in G$, $a \mapsto ga$ is an isomorphism $G \to G$, and so gU consists of nonsingular points. Clearly $G = \cup gU$. □

In fact, any variety on which a group acts transitively by regular maps will be nonsingular.

ASIDE 4.25. If V has pure codimension 1 in $\mathbb{A}^{d+1}$, then $I(V) = (f)$ for some polynomial f.

PROOF. We know $I(V) = \cap I(V_i)$ where the V_i are the irreducible components of V, and so if we can prove $I(V_i) = (f_i)$ then $I(V) = (f_1 \cdots f_r)$. Thus we may suppose that V is irreducible. Let $\mathfrak{p} = I(V)$; it is a prime ideal, and it is nonzero because otherwise $\dim(V) = d+1$. Therefore it contains an irreducible polynomial f. From (0.3) we know (f) is prime. If $(f) \neq \mathfrak{p}$, then we have

$$V = V(\mathfrak{p}) \subsetneqq V((f)) \subsetneqq \mathbb{A}^{d+1},$$

and $\dim(V) < \dim(V(f)) < d+1$ (see 1.22), which contradicts the fact that V has dimension d. □

ASIDE 4.26. Lemma 4.22 can be improved as follows: if V and W are irreducible varieties, then every inclusion $k(W) \subset k(V)$ is defined by a regular surjective map $\alpha\colon U \to U'$ from an open subset U of W onto an open subset U' of V.

ASIDE 4.27. An irreducible variety V of dimension d is said to *rational* if it is birationally equivalent to $\mathbb{A}^d$. It is said to be *unirational* if $k(V)$ can be embedded in $k(\mathbb{A}^d)$ — according to the last aside, this means that there is a regular surjective map from

an open subset of $\mathbb{A}^{\dim V}$ onto an open subset of V. Lüroth's theorem (which sometimes used to be included in basic graduate algebra courses) says that a unirational curve is rational, that is, a subfield of $k(X)$ not equal to k is a pure transcendental extension of k. It was proved by Castelnuovo that when k has characteristic zero every unirational surface is rational. Only in the seventies was it shown that this is not true for three dimensional varieties (Artin, Mumford, Clemens, Griffiths, Manin,...). When k has characteristic $p \neq 0$, Zariski showed that there exist nonrational unirational surfaces, and P. Blass (UM thesis 1977) showed that there exist infinitely many surfaces V, no two birationally equivalent, such that $k(X^p, Y^p) \subset k(V) \subset k(X, Y)$.

ASIDE 4.28. Note that, if V is irreducible, then

$$\dim V = \min_P \dim T_P(V)$$

This formula can be useful in computing the dimension of a variety.

Etale neighbourhoods. Recall that a regular map $\alpha\colon W \to V$ is said to be étale at a nonsingular point P of W if the map $(d\alpha)_P\colon T_P(W) \to T_{\alpha(P)}(V)$ is an isomorphism.

Let P be a nonsingular point on a variety V of dimension d. A *local system of parameters* at P is a family $\{f_1, \dots, f_d\}$ of germs of regular functions at P generating the maximal ideal $\mathfrak{n}_P \subset \mathcal{O}_P$. Equivalent conditions: the images of $f_1, \dots, f_d$ in $\mathfrak{n}_P/\mathfrak{n}_P^2$ generate it as a k-vector space (see 4.16); or $(df_1)_P, \dots, (df_d)_P$ is a basis for dual space to $T_P(V)$.

PROPOSITION 4.29. *Let $\{f_1, \dots, f_d\}$ be a local system of parameters at a nonsingular point P of V. Then there is a nonsingular open neighbourhood U of P such that $f_1, f_2, \dots, f_d$ are represented by pairs $(\tilde{f}_1, U), \dots, (\tilde{f}_d, U)$ and the map $(\tilde{f}_1, \dots, \tilde{f}_d)\colon U \to \mathbb{A}^d$ is étale.*

PROOF. Obviously, the f_i are represented by regular functions $\tilde{f}_i$ defined on a single open neighbourhood U' of P, which, because of (4.21), we can choose to be nonsingular. The map $\alpha = (\tilde{f}_1, \dots, \tilde{f}_d)\colon U' \to \mathbb{A}^d$ is étale at P, because the dual map to $(d\alpha)_{\mathbf{a}}$ is $(dX_i)_0 \mapsto (d\tilde{f}_i)_{\mathbf{a}}$. The next lemma then shows that α is étale on an open neighbourhood U of P. □

LEMMA 4.30. *Let W and V be nonsingular varieties. If $\alpha\colon W \to V$ is étale at P, then it is étale at all points in an open neighbourhood of P.*

PROOF. The hypotheses imply that W and V have the same dimension d, and that their tangent spaces all have dimension d. We may assume W and V to be affine, say $W \subset \mathbb{A}^m$ and $V \subset \mathbb{A}^n$, and that α is given by polynomials $P_1(X_1, \dots, X_m), \dots, P_n(X_1, \dots, X_m)$. Then $(d\alpha)_{\mathbf{a}}\colon T_{\mathbf{a}}(\mathbb{A}^m) \to T_{\alpha(\mathbf{a})}(\mathbb{A}^n)$ is a linear map with matrix $\left(\frac{\partial P_i}{\partial X_j}(\mathbf{a})\right)$, and α is not étale at $\mathbf{a}$ if and only if the kernel of this map contains a nonzero vector in the subspace $T_{\mathbf{a}}(V)$ of $T_{\mathbf{a}}(\mathbb{A}^n)$. Let $f_1, \dots, f_r$ generate $I(W)$. Then α is not étale at $\mathbf{a}$ if and only if the matrix

$$\begin{pmatrix} \frac{\partial f_i}{\partial X_j}(\mathbf{a}) \\ \frac{\partial P_i}{\partial X_j}(\mathbf{a}) \end{pmatrix}$$

has rank less than m. This is a polynomial condition on $\mathbf{a}$, and so it fails on a closed subset of W, which doesn't contain P. □

Let V be a nonsingular variety, and let $P \in V$. An *étale neighbourhood* of a point P of V is pair $(Q, \pi\colon U \to V)$ with π an étale map from a nonsingular variety U to V and Q a point of U such that $\pi(Q) = P$.

COROLLARY 4.31. *Let V be a nonsingular variety of dimension d, and let $P \in V$. There is an open Zariski neighbourhood U of P and a map $\pi\colon U \to \mathbb{A}^d$ realizing (P, U) as an étale neighbourhood of $(0, \dots, 0) \in \mathbb{A}^d$.*

PROOF. This is a restatement of the Proposition. □

ASIDE 4.32. Note the analogy with the definition of a differentiable manifold: every point P on nonsingular variety of dimension d has an open neighbourhood that is also a "neighbourhood" of the origin in $\mathbb{A}^d$. There is a "topology" on algebraic varieties for which the "open neighbourhoods" of a point are the étale neighbourhoods. Relative to this "topology", any two nonsingular varieties are locally isomorphic (this is *not* true for the Zariski topology). The "topology" is called the *étale topology* — see my notes Lectures on Etale Cohomology.

Dual numbers and derivations. In general, if A is a k-algebra and M is an A-module, then a *k-derivation* is a map $D\colon A \to M$ such that

(a) $D(c) = 0$ for all $c \in k$;
(b) $D(a + b) = D(a) + D(b)$;
(c) $D(a \cdot b) = a \cdot Db + b \cdot Da$ (Leibniz rule).

Note that the conditions imply that D is k-linear (but not A-linear). We write $\mathrm{Der}_k(A, M)$ for the space of all k-derivations $A \to M$.

For example, the map $f \mapsto (df)_P \stackrel{\text{df}}{=} f - f(P) \bmod \mathfrak{n}_P^2$ is a k-derivation $\mathcal{O}_P \to \mathfrak{n}_P/\mathfrak{n}_P^2$.

PROPOSITION 4.33. *There are canonical isomorphisms*

$$Der_k(\mathcal{O}_P, k) \xrightarrow{\approx} \mathrm{Hom}_{k\text{-}lin}(\mathfrak{n}_P/\mathfrak{n}_P^2, k) \xrightarrow{\approx} T_P(V).$$

PROOF. Note that, as a k-vector space,

$$\mathcal{O}_P = k \oplus \mathfrak{n}_P, \quad f \leftrightarrow (f(P), f - f(P)).$$

A derivation $D\colon \mathcal{O}_P \to k$ is zero on k and on $\mathfrak{n}_P^2$ (Leibniz's rule). It therefore defines a linear map $\mathfrak{n}_P/\mathfrak{n}_P^2 \to k$, and all such linear maps arise in this way, by composition

$$\mathcal{O}_P \stackrel{f \mapsto (df)_P}{\longrightarrow} \mathfrak{n}_P/\mathfrak{n}_P^2 \to k.$$

□

The *ring of dual numbers* is $k[\varepsilon] = k[X]/(X^2)$, $\varepsilon = X \bmod X^2$. As a k-vector space it has a basis $\{1, \varepsilon\}$.

PROPOSITION 4.34. *The tangent space*

$$T_P(V) = \mathrm{Hom}(\mathcal{O}_P, k[\varepsilon]) \quad \textit{(local homomorphisms of local k-algebras).}$$

PROOF. Let $\alpha\colon \mathcal{O}_P \to k[\varepsilon]$ be a local homomorphism of k-algebras, and write $\alpha(a) = a_0 + D_\alpha(a)\varepsilon$. Because α is a homomorphism of k-algebras, $a \mapsto a_0$ is the quotient map $\mathcal{O}_P \to \mathcal{O}_P/\mathfrak{m} = k$. We have

$$\begin{aligned} \alpha(ab) &= (ab)_0 + D_\alpha(ab)\varepsilon, \text{ and} \\ \alpha(a)\alpha(b) &= (a_0 + D_\alpha(a)\varepsilon)(b_0 + D_\alpha(b)\varepsilon) = a_0b_0 + (a_0D_\alpha(b) + b_0D_\alpha(a))\varepsilon. \end{aligned}$$

On comparing these expressions, we see that D_α satisfies Leibniz's rule, and therefore is a k-derivation $\mathcal{O}_P \to k$. All such derivations arise in this way. □

For an affine variety V and a k-algebra A (not necessarily an affine k-algebra), we define $V(A)$, *the set of points of V with coordinates in A*, to be $\mathrm{Hom}_{k\text{-alg}}(k[V], A)$. For example, if $V = V(\mathfrak{a}) \subset \mathbb{A}^n$, then

$$V(A) = \{(a_1, \dots, a_n) \in A^n \mid f(a_1, \dots, a_n) = 0 \text{ all } f \in \mathfrak{a}\}.$$

Consider an $\alpha \in V(k[\varepsilon])$, i.e., a k-algebra homomorphism $\alpha\colon k[V] \to k[\varepsilon]$. The composite $k[V] \to k[\varepsilon] \to k$ is a point P of V, and

$$\mathfrak{m}_P = \mathrm{Ker}(k[V] \to k[\varepsilon] \to k) = \alpha^{-1}((\varepsilon)).$$

Therefore elements of $k[V]$ not in $\mathfrak{m}_P$ map to units in $k[\varepsilon]$, and so α extends to a homomorphism $\alpha'\colon \mathcal{O}_P \to k[\varepsilon]$. By construction, this is a local homomorphism of local k-algebras, and every such homomorphism arises in this way. In this way we get a one-to-one correspondence between the local homomorphisms of k-algebras $\mathcal{O}_P \to k[\varepsilon]$ and the set

$$\{P' \in V(k[\varepsilon]) \mid P' \mapsto P \text{ under the map } V(k[\varepsilon]) \to V(k)\}.$$

This gives us a new interpretation of the tangent space at P.

Consider, for example, $V = V(\mathfrak{a}) \subset \mathbb{A}^n$, $\mathfrak{a}$ a radical ideal in $k[X_1, \dots, X_n]$, and let $\mathbf{a} \in V$. In this case, it is possible to show directly that

$$T_{\mathbf{a}}(V) = \{\mathbf{a}' \in V(k[\varepsilon]) \mid \mathbf{a}' \text{ maps to } \mathbf{a} \text{ under } V(k[\varepsilon]) \to V(k)\}$$

Note that when we write a polynomial $F(X_1, \dots, X_n)$ in terms of the variables $X_i - a_i$, we obtain a formula (trivial Taylor formula)

$$F(X_1, \dots, X_n) = F(a_1, \dots, a_n) + \sum \left.\frac{\partial F}{\partial X_i}\right|_{\mathbf{a}} (X_i - a_i) + R$$

with R a finite sum of products of at least two terms $(X_i - a_i)$. Now let $\mathbf{a} \in k^n$ be a point on V, and consider the condition for $\mathbf{a} + \varepsilon\mathbf{b} \in k[\varepsilon]^n$ to be a point on V. When we substitute $a_i + \varepsilon b_i$ for X_i in the above formula and take $F \in \mathfrak{a}$, we obtain:

$$F(a_1 + \varepsilon b_1, \dots, a_n + \varepsilon b_n) = \varepsilon\Big(\sum \left.\frac{\partial F}{\partial X_i}\right|_{\mathbf{a}} b_i\Big).$$

Consequently, $(a_1 + \varepsilon b_1, \dots, a_n + \varepsilon b_n)$ lies on V if and only if $(b_1, \dots, b_n) \in T_{\mathbf{a}}(V)$ (original definition p68).

Geometrically, we can think of a point of V with coordinates in $k[\varepsilon]$ as being a point of V with coordinates in k (the image of the point under $V(k[\varepsilon]) \to V(k)$) together with a "direction"

REMARK 4.35. The description of the tangent space in terms of dual numbers is particularly convenient when our variety is given to us in terms of its points functor. For example, let M_n be the set of $n \times n$ matrices, and let I be the identity matrix. Write e for I when it is to be regarded as the identity element of GL_n. Then we have

$T_e(\mathrm{GL}_n) = \{I + \varepsilon A \mid A \in M_n\} \approx M_n$;

$T_e(\mathrm{SL}_n) = \{I + \varepsilon A \mid \det(I + \varepsilon A) = I\} = \{I + \varepsilon A \mid \mathrm{trace}(A) = 0\}$.

Assume the characteristic $\neq 2$, and let O_n be orthogonal group:

$$O_n = \{A \in \mathrm{GL}_n \mid AA^{\mathrm{tr}} = I\}.$$

(tr=transpose). This is the group of matrices preserving the quadratic form $X_1^2 + \cdots + X_n^2$. Then $\det\colon O_n \to \{\pm 1\}$ is a homomorphism, and the special orthogonal group SO_n is defined to be the kernel of this map. We have

$$\begin{aligned} T_e(O_n) &= T_e(SO_n) \\ &= \{I + \varepsilon A \in M_n \mid (I + \varepsilon A)(I + \varepsilon A)^{\mathrm{tr}} = I\} \\ &= \{I + \varepsilon A \in M_n \mid A \text{ is skew-symmetric}\}. \end{aligned}$$

Note that, because an algebraic group is nonsingular, $\dim T_e(G) = \dim G$ — this gives a very convenient way of computing the dimension of an algebraic group.

On the tangent space $T_e(\mathrm{GL}_n) = M_n$ of GL_n, there is a bracket operation

$$[M, N] \stackrel{\mathrm{df}}{=} MN - NM$$

which makes $T_e(\mathrm{GL}_n)$ into a Lie algebra. For any closed algbraic subgroup G of GL_n, $T_e(G)$ is stable under the bracket operation on $T_e(\mathrm{GL}_n)$ and is a sub-Lie-algebra of M_n, which we denote $\mathrm{Lie}(G)$. The Lie algebra structure on $\mathrm{Lie}(G)$ is independent of the embedding of G into GL_n (in fact, it has an intrinsic definition), and $G \mapsto \mathrm{Lie}(G)$ is a functor from the category of linear algebraic groups to that of Lie algebras.

This functor is not fully faithful, for example, any étale homomorphism $G \to G'$ will define an isomorphism $\mathrm{Lie}(G) \to \mathrm{Lie}(G')$, but is nevertheless very useful.

Assume k has characteristic zero. A connected algebraic group G is said to be *semisimple* if it has no closed connected solvable normal subgroup (except $\{e\}$). Such a group G may have a finite nontrivial centre $Z(G)$, and we call two semisimple groups G and G' *locally isomorphic* if $G/Z(G) \approx G'/Z(G')$. For example, SL_n is semisimple, with centre μ_n, the set of diagonal matrices $\mathrm{diag}(\zeta, \dots, \zeta)$, $\zeta^n = 1$, and $\mathrm{SL}_n/\mu_n = \mathrm{PSL}_n$. A Lie algebra is *semisimple* if it has no commutative ideal (except $\{0\}$). One can prove that

$$G \text{ is semisimple} \iff \mathrm{Lie}(G) \text{ is semisimple},$$

and the map $G \mapsto \mathrm{Lie}(G)$ defines a one-to-one correspondence between the set of local isomorphism classes of semisimple algebraic groups and the set of isomorphism classes of Lie algebras. The classification of semisimple algebraic groups can be deduced from that of semisimple Lie algebras and a study of the finite coverings of semisimple algebraic groups — this is quite similar to the relation between Lie groups and Lie algebras.

Tangent cones. In this subsection, I assume familiarity with parts of Atiyah and MacDonald 1969, Chapters 11, 12.

Let $V = V(\mathfrak{a}) \subset k^m$, $\mathfrak{a} = \mathrm{rad}(\mathfrak{a})$, and let $P = (0, \dots, 0) \in V$. Define $\mathfrak{a}_*$ to be the ideal generated by the polynomials F_* for $F \in \mathfrak{a}$, where F_* is the leading form of F (see p66). The *geometric tangent cone* at P, $C_P(V)$ is $V(\mathfrak{a}_*)$, and the *tangent cone* is the pair $(V(\mathfrak{a}_*), k[X_1, \dots, X_n]/\mathfrak{a}_*)$. Obviously, $C_P(V) \subset T_P(V)$.

Computing the tangent cone. If $\mathfrak{a}$ is principal, say $\mathfrak{a} = (F)$, then $\mathfrak{a}_* = (F_*)$, but if $\mathfrak{a} = (F_1, \dots, F_r)$, then it need not be true that $\mathfrak{a}_* = (F_{1*}, \dots, F_{r*})$. Consider for example $\mathfrak{a} = (XY, XZ + Z(Y^2 - Z^2))$. One can show that this is a radical ideal either by asking Macaulay (assuming you believe Macaulay), or by following the method suggested in Cox et al. 1992, p474, prob 3 to show that it is an intersection of prime ideals. Since

$$YZ(Y^2 - Z^2) = Y \cdot (XZ + Z(Y^2 - Z^2)) - Z \cdot (XY) \in \mathfrak{a}$$

and is homogeneous, it is in $\mathfrak{a}_*$, but it is not in the ideal generated by XY, XZ. In fact, $\mathfrak{a}_*$ is the ideal generated by

$$XY, \quad XZ, \quad YZ(Y^2 - Z^2).$$

This raises the following question: given a set of generators for an ideal $\mathfrak{a}$, how do you find a set of generators for $\mathfrak{a}_*$? There is an algorithm for this in Cox et al. 1992, p467. Let $\mathfrak{a}$ be an ideal (not necessarily radical) such that $V = V(\mathfrak{a})$, and assume the origin is in V. Introduce an extra variable T such that T"$>$" the remaining variables. Make each generator of $\mathfrak{a}$ homogeneous by multiplying its monomials by appropriate (small) powers of T, and find a Gröbner basis for the ideal generated by these homogeneous polynomials. Remove T from the elements of the basis, and then the polynomials you get generate $\mathfrak{a}_*$.

Intrinsic definition of the tangent cone. Let A be a local ring with maximal ideal $\mathfrak{n}$. The associated graded ring is

$$\mathrm{gr}(A) = \oplus \mathfrak{n}^i/\mathfrak{n}^{i+1}.$$

Note that if $A = B_{\mathfrak{m}}$ and $\mathfrak{n} = \mathfrak{m}A$, then $\mathrm{gr}(A) = \oplus \mathfrak{m}^i/\mathfrak{m}^{i+1}$ (because of (4.13)).

PROPOSITION 4.36. *The map $k[X_1, \dots, X_m]/\mathfrak{a}_* \to gr(\mathcal{O}_P)$ sending the class of X_i in $k[X_1, \dots, X_m]/\mathfrak{a}_*$ to the class of X_i in $gr(\mathcal{O}_P)$ is an isomorphism.*

PROOF. Let $\mathfrak{m}$ be the maximal ideal in $k[X_1, \dots, X_m]/\mathfrak{a}$ corresponding to P. Then

$$\begin{aligned} \mathrm{gr}(\mathcal{O}_P) &= \sum \mathfrak{m}^i/\mathfrak{m}^{i+1} \\ &= \sum (X_1, \dots, X_m)^i/(X_1, \dots, X_m)^{i+1} + \mathfrak{a} \cap (X_1, \dots, X_m)^i \\ &= \sum (X_1, \dots, X_m)^i/(X_1, \dots, X_m)^{i+1} + \mathfrak{a}_i \end{aligned}$$

where $\mathfrak{a}_i$ is the homogeneous piece of $\mathfrak{a}_*$ of degree i (that is, the subspace of $\mathfrak{a}_*$ consisting of homogeneous polynomials of degree i). But

$$(X_1, \dots, X_m)^i/(X_1, \dots, X_m)^{i+1} + \mathfrak{a}_i = i^{\text{th}} \text{ homogeneous piece of } k[X_1, \dots, X_m]/\mathfrak{a}_*.$$

□

For a general variety V and $P \in V$, we define the *geometric tangent cone* $C_P(V)$ of V at P to be $\operatorname{Specm}(\operatorname{gr}(\mathcal{O}_P)_{\text{red}})$, where $\operatorname{gr}(\mathcal{O}_P)_{\text{red}}$ is the quotient of $\operatorname{gr}(\mathcal{O}_P)$ by its nilradical.

Recall (Atiyah and MacDonald 1969, 11.21) that $\dim(A) = \dim(\operatorname{gr}(A))$. Therefore the dimension of the geometric tangent cone at P is the same as the dimension of V (in contrast to the dimension of the tangent space).

Recall (ibid., 11.22) that $\operatorname{gr}(\mathcal{O}_P)$ is a polynomial ring in d variables ($d = \dim V$) if and only if $\mathcal{O}_P$ is regular. Therefore, P is nonsingular if and only if $\operatorname{gr}(\mathcal{O}_P)$ is a polynomial ring in d variables, in which case $C_P(V) = T_P(V)$.

Using tangent cones, we can extend the notion of an étale morphism to singular varieties. Obviously, a regular map $\alpha\colon V \to W$ induces a homomorphism $\operatorname{gr}(\mathcal{O}_{\alpha(P)}) \to \operatorname{gr}(\mathcal{O}_P)$. We say that α is *étale* at P if this is an isomorphism. Note that then there is an isomorphism of the geometric tangent cones $C_P(V) \to C_{\alpha(P)}(W)$, but this map may be an isomorphism without α being étale at P. Roughly speaking, to be étale at P, we need the map on geometric tangent cones to be an isomorphism and to preserve the "multiplicities" of the components.

It is a fairly elementary result that a local homomorphism of local rings $\alpha\colon A \to B$ induces an isomorphism on the graded rings if and only if it induces an isomorphism on the completions. Thus $\alpha\colon V \to W$ is étale at P if and only if the map is $\hat{\mathcal{O}}_{\alpha(P)} \to \hat{\mathcal{O}}_P$ an isomorphism. Hence (4.29) shows that the choice of a local system of parameters $f_1, \dots, f_d$ at a nonsingular point P determines an isomorphism $\hat{\mathcal{O}}_P \to k[[X_1, \dots, X_d]]$.

We can rewrite this as follows: let $t_1, \dots, t_d$ be a local system of parameters at a nonsingular point P; then there is a canonical isomorphism $\hat{\mathcal{O}}_P \to k[[t_1, \dots, t_d]]$. For $f \in \hat{\mathcal{O}}_P$, the image of $f \in k[[t_1, \dots, t_d]]$ can be regarded as the Taylor series of f.

For example, let $V = \mathbb{A}^1$, and let P be the point a. Then $t = X - a$ is a local parameter at a, $\mathcal{O}_P$ consists of quotients $f(X) = g(X)/h(X)$ with $h(a) \neq 0$, and the coefficients of the Taylor expansion $\sum_{n\geq 0} a_n(X-a)^n$ of $f(X)$ can be computed as in elementary calculus courses: $a_n = f^{(n)}(a)/n!$.

5. Projective Varieties and Complete Varieties

Throughout this section, k will be an algebraically closed field. Recall that we defined

$$\mathbb{P}^n = k^{n+1} \setminus \{\text{origin}\}/\!\sim,$$

where $(a_0, \dots, a_n) \sim (b_0, \dots, b_n)$ if and only if there exists a $c \neq 0$ in k such that $(a_0, \dots, a_n) = c(b_0, \dots, b_n)$. Write $(a_0 : \dots : a_n)$ for the equivalence class of $(a_0, \dots, a_n)$, and π for the map $k^{n+1} \setminus \{\text{origin}\}/\!\sim \to \mathbb{P}^n$. Let U_i be the set of $(a_0 : \dots : a_n) \in \mathbb{P}^n$ such that $a_i \neq 0$. Then $(a_0 : \dots : a_n) \mapsto (\frac{a_0}{a_i}, \dots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, \dots, \frac{a_n}{a_i})$ is a bijection $v_i \colon U_i \to k^n$, and we used these bijections to define the structure of a ringed space on $\mathbb{P}^n$; specifically, we said that $U \subset \mathbb{P}^n$ is open if and only if $v_i(U \cap U_i)$ is open for all i, and that a function $f \colon U \to k$ is regular if and only if $(f|U \cap U_i) \circ v_i^{-1}$ is regular on $v_i(U \cap U_i)$ for all i.

In this chapter, we shall first derive another description of the topology on $\mathbb{P}^n$, and then we shall show that the ringed space structure makes $\mathbb{P}^n$ into a separated algebraic variety. A closed subvariety of $\mathbb{P}^n$ (or any variety isomorphic to such a variety) is called a *projective variety*, and a locally closed subvariety of $\mathbb{P}^n$ (or any variety isomorphic to such a variety) is called a *quasi-projective variety*. Note that every affine variety is quasi-projective, but there are many varieties that are not quasi-projective. We study morphisms between (quasi-) projective varieties. Finally, we show that a projective variety is "complete", that is, it has the analogue of a property that distinguishes compact topological spaces among locally compact spaces.

Projective varieties are important for the same reason compact manifolds are important: results are often simpler when stated for projective varieties, and the "part at infinity" often plays a role, even when we would like to ignore it. For example, a famous theorem of Bezout says that a curve of degree m in the projective plane[15] intersects a curve of degree n in exactly mn points (counting multiplicities). For affine curves, one has only an inequality.

Algebraic subsets of $\mathbb{P}^n$. A polynomial $F(X_0, \dots, X_n)$ is said to be *homogeneous of degree d* if it is a sum of terms $a_{i_0,\dots,i_n} X_0^{i_0} \cdots X_n^{i_n}$ with $i_0 + \cdots + i_n = d$; equivalently,

$$F(tX_0, \dots, tX_n) = t^d F(X_0, \dots, X_n)$$

for all $t \in k$. Write $k[X_0, \dots, X_n]_d$ for the subspace of $k[X_0, \dots, X_n]$ of polynomials of degree d. Then

$$k[X_0, \dots, X_n] = \bigoplus_{d \geq 0} k[X_0, \dots, X_n]_d;$$

that is, each polynomial F can be written uniquely as a sum $F = \sum F_d$ with F_d of degree d.

Let $P = (a_0 : \dots : a_n) \in \mathbb{P}^n$. Then P can also be written $(ca_0 : \dots : ca_n)$ for any $c \in k^\times$, and so we can't speak of the value of a polynomial $F(X_0, \dots, X_n)$ at P. However, if F is homogeneous, then $F(ca_0, \dots, ca_n) = c^d F(a_0, \dots, a_n)$, and so it does make sense to say that F is zero or not zero at P. We define a *projective algebraic set* to be the set of common zeros in $\mathbb{P}^n$ of a collection of homogeneous polynomials.

[15] This means that it is defined by a homogeneous polynomial $F(X, Y, Z)$ of degree m.

EXAMPLE 5.1. Consider the projective algebraic subset E of $\mathbb{P}^2$ defined by the homogeneous equation

$$Y^2Z = X^3 + aXZ^2 + bZ^3 \qquad (*)$$

where $X^3 + aX + b$ is assumed not to have multiple roots. It consists of the points $(x : y : 1)$ on the affine curve E_{aff}

$$Y^2 = X^3 + aX + b,$$

together with the point "at infinity" (0:1:0).

Poincaré is usually credited (incorrectly!) with showing that E is an algebraic group, with the group law such that $P + Q + R = 0$ if and only if P, Q, and R lie on a straight line. The zero for the group is the point at infinity.

Curves defined by equations of the form (*) are called *elliptic curves*. They can also be described as the curves of genus one, or as the abelian varieties of dimension one.

In the case $k = \mathbb{C}$, for each equation (*), there is a lattice $L \subset \mathbb{C}$ and a function $\wp$ (the Weierstrass $\wp$-function) that is analytic on $\mathbb{C} - L$ and doubly periodic for L (i.e., such that $\wp(z + \lambda) = \wp(z)$ for all $\lambda \in L$) such that

$$\wp'^2 = \wp^3 + a\wp + b.$$

The map $z \mapsto (\wp(z) : \wp'(z) : 1) : \mathbb{C}/L - \{0\} \to \mathbb{P}^2$ is a bijection from $\mathbb{C}/L - \{0\}$ onto E_{aff}. This map can be extended to an isomorphism $\mathbb{C}/L \xrightarrow{\approx} E$ by sending 0 to $(0 : 1 : 0)$.

In the case that $a, b \in \mathbb{Q}$, we can speak of the zeros of (*) with coordinates in $\mathbb{Q}$. They also form a group $E(\mathbb{Q})$, which Mordell showed to be finitely generated. It is easy to compute the torsion subgroup of $E(\mathbb{Q})$, but there is at present no known algorithm for computing the rank of $E(\mathbb{Q})$. More precisely, there is an "algorithm" which always works, but which has not been proved to terminate after a finite amount of time, at least not in general. There is a very beautiful theory surrounding elliptic curves over $\mathbb{Q}$ and other number fields, whose origins can be traced back 1,800 years to Diophantus. (See my notes on Elliptic Curves for all of this.)

An ideal $\mathfrak{a} \subset k[X_0, \dots, X_n]$ is said to be *homogeneous* if it contains with any polynomial F all the homogeneous components of F, i.e., if $F \in \mathfrak{a} \Rightarrow F_d \in \mathfrak{a}$, all d. Such an ideal is generated by homogeneous polynomials (obviously), and conversely, an ideal generated by a set of homogeneous polynomials is homogeneous. The radical of a homogeneous ideal is homogeneous, the intersection of two homogeneous ideals is homogeneous, and a sum of homogeneous ideals is homogeneous.

For a homogeneous ideal $\mathfrak{a}$, we write $V(\mathfrak{a})$ for the set of common zeros of the homogeneous polynomials in $\mathfrak{a}$ — clearly every polynomial in $\mathfrak{a}$ will then be zero on $V(\mathfrak{a})$. If $F_1, \dots, F_r$ are homogeneous generators for $\mathfrak{a}$, then $V(\mathfrak{a})$ is the set of common zeros of the F_i. The sets $V(\mathfrak{a})$ have similar properties to their namesakes in $\mathbb{A}^n$:

$\mathfrak{a} \subset \mathfrak{b} \Rightarrow V(\mathfrak{a}) \supset V(\mathfrak{b})$;

$V(0) = \mathbb{P}^n$; $V(\mathfrak{a}) = \varnothing \iff \text{rad}(\mathfrak{a}) \supset (X_0, \dots, X_n)$;

$V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$;

$V(\sum \mathfrak{a}_i) = \cap V(\mathfrak{a}_i)$.

The first statement is obvious. For the second, let $V^{\mathrm{aff}}(\mathfrak{a})$ be the zero set of $\mathfrak{a}$ in k^{n+1}. It is a cone — it contains together with any point P the line through P and the origin — and

$$V(\mathfrak{a}) = (V^{\mathrm{aff}}(\mathfrak{a}) \setminus (0,\dots,0))/\sim .$$

We have $V(\mathfrak{a}) = \emptyset \iff V^{\mathrm{aff}}(\mathfrak{a}) \subset \{(0,\dots,0)\} \iff \mathrm{rad}(\mathfrak{a}) \supset (X_0,\dots,X_n)$, by the Hilbert Nullstellensatz. The remaining statements can be proved directly, or by using the relation between $V(\mathfrak{a})$ and $V^{\mathrm{aff}}(\mathfrak{a})$.

Let C be a cone in k^{n+1}; then $I(C)$ is a homogeneous ideal in $k[X_0,\dots,X_n]$, because

$$F(ca_0,\dots,ca_n) = \sum c^d F_d(a_0,\dots,a_n),$$

and so, if $F(ca_0,\dots,ca_n) = 0$ for all $c \in k^\times$, we must also have $F_d(a_0,\dots,a_n) = 0$. For any $S \subset \mathbb{P}^n$, $C = \pi^{-1}(S) \cup \{\text{origin}\}$ is a cone in k^{n+1}, and we define $I(S) = I(C)$.

PROPOSITION 5.2. *The maps V and I define a bijection between the set of algebraic subsets of $\mathbb{P}^n$ and the set of homogeneous radical ideals of $k[X_0,\dots,X_n]$, except that V maps both the ideals $(X_0,\dots,X_n)$ and $k[X_0,\dots,X_n]$ to the empty set. An algebraic set V in $\mathbb{P}^n$ is irreducible if and only if $I(V)$ is prime; in particular, $\mathbb{P}^n$ is irreducible.*

PROOF. Note that we have bijections

$$\{\text{algebraic subsets of } \mathbb{P}^n, \neq \varnothing\} \xrightarrow{\pi^{-1}}$$
$$\{\text{closed cones in } k^{n+1}, \neq \{(0,\dots,0),\varnothing\} \xrightarrow{I}$$
$$\{\text{homogeneous radical ideals in } k[X_0,\dots,X_n], \neq (X_0,\dots,X_n), k[X_0,\dots,X_n]\} \xrightarrow{V}$$
$$\{\text{algebraic subsets of } \mathbb{P}^n, \ \neq \varnothing\}.$$

Here the first map sends V to $\pi^{-1}(V) \cup \{\text{origin}\}$, which is also the closure of $\pi^{-1}(V)$, and the third map is V in the sense of projective geometry. The composite of any three of these maps is the identity map. Obviously, V is irreducible if and only if the closure of $\pi^{-1}(V)$ is irreducible, which is true if and only if $I(V)$ is a prime ideal. □

The Zariski topology on $\mathbb{P}^n$. The statements above show that projective algebraic sets are the closed sets for a topology on $\mathbb{P}^n$. In this subsection, we verify that it agrees with that defined in the first paragraph of this section. For a homogeneous polynomial F, let

$$D(F) = \{P \in \mathbb{P}^n \mid F(P) \neq 0\}.$$

Then, just as in the affine case, $D(F)$ is open and the sets of this type form a basis for the topology of $\mathbb{P}^n$.

With each polynomial $f(X_1,\dots,X_n)$, we associate the homogeneous polynomial of the same degree

$$f^*(X_0,\dots,X_n) = X_0^{\deg(f)} f\left(\frac{X_1}{X_0},\dots,\frac{X_n}{X_0}\right),$$

and with each homogeneous polynomial $F(X_0,\dots,X_n)$ we associate the polynomial

$$F_*(X_1,\dots,X_n) = F(1,X_1,\dots,X_n).$$

PROPOSITION 5.3. *For the topology on $\mathbb{P}^n$ just defined, each U_i is open, and when we endow it with the induced topology, the bijection*

$$U_i \leftrightarrow \mathbb{A}^n,\ (a_0 : \ldots : 1 : \ldots : a_n) \leftrightarrow (a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)$$

becomes a homeomorphism.

PROOF. It suffices to prove this with $i = 0$. The set $U_0 = D(X_0)$, and so it is a basic open subset in $\mathbb{P}^n$. Clearly, for any homogeneous polynomial $F \in k[X_0, \ldots, X_n]$,

$$D(F(X_0, \ldots, X_n)) \cap U_0 = D(F(1, X_1, \ldots, X_n)) = D(F_*)$$

and, for any polynomial $f \in k[X_1, \ldots, X_n]$,

$$D(f) = D(f^*) \cap U_0.$$

Thus, under $U_0 \leftrightarrow \mathbb{A}^n$, the basic open subsets of $\mathbb{A}^n$ correspond to the intersections with U_i of the basic open subsets of $\mathbb{P}^n$, which proves that the bijection is a homeomorphism. □

REMARK 5.4. It is possible to use this to give a different proof that $\mathbb{P}^n$ is irreducible. We apply the criterion that a space is irreducible if and only if every nonempty open subset is dense (see p22). Note that each U_i is irreducible, and that $U_i \cap U_j$ is open and dense in each of U_i and U_j (as a subset of U_i, it is the set of points $(a_0 : \ldots : 1 : \ldots : a_j : \ldots : a_n)$ with $a_j \neq 0$). Let U be a nonempty open subset of $\mathbb{P}^n$; then $U \cap U_i$ is open in U_i. For some i, $U \cap U_i$ is nonempty, and so must meet $U_i \cap U_j$. Therefore U meets every U_j, and so is dense in every U_j. It follows that its closure is all of $\mathbb{P}^n$.

We identify $\mathbb{A}^n$ with U_0, and examine the closures in $\mathbb{P}^n$ of closed subsets of $\mathbb{A}^n$.

With each ideal $\mathfrak{a}$ in $k[X_1, \ldots, X_n]$, we associate the homogeneous ideal $\mathfrak{a}^*$ in $k[X_0, \ldots, X_n]$ generated by $\{f^* \mid f \in \mathfrak{a}\}$. For a closed subset V of $\mathbb{A}^n$, set $V^* = V(\mathfrak{a}^*)$ with $\mathfrak{a} = I(V)$.

With each homogeneous ideal $\mathfrak{a}$ in $k[X_0, X_1, \ldots, X_n]$, we associate the ideal $\mathfrak{a}_*$ in $k[X_1, \ldots, X_n]$ generated by $\{F_* \mid F \in \mathfrak{a}\}$. When V is a closed subset of $\mathbb{P}^n$, we set $V_* = V(\mathfrak{a}_*)$ with $\mathfrak{a} = I(V)$.

PROPOSITION 5.5. *(a) For V a closed algebraic subset of $\mathbb{A}^n$, V^* is the closure of V in $\mathbb{P}^n$, and $(V^*)_* = V$. If $V = \cup V_i$ is the decomposition of V into its irreducible components, then $V^* = \cup V_i^*$ is the decomposition of V^* into its irreducible components.*

(b) For V a closed algebraic subset of $\mathbb{P}^n$, $V_* = V \cap \mathbb{A}^n$. If no irreducible component of V lies in H_∞ or contains H_∞, then V_* is a proper subset of $\mathbb{A}^n$, and $(V_*)^* = V$.

PROOF. Straightforward. □

The hyperplane at infinity. It is often convenient to think of $\mathbb{P}^n$ as being $\mathbb{A}^n = U_0$ with a hyperplane added "at infinity". More precisely, identify the U_0 with $\mathbb{A}^n$. The complement of U_0 in $\mathbb{P}^n$ is $H_\infty = \{(0 : a_1 : \ldots : a_n) \subset \mathbb{P}^n\}$, which can be identified with $\mathbb{P}^{n-1}$.

For example, $\mathbb{P}^1 = \mathbb{A}^1 \cup H_\infty$ (disjoint union), with H_∞ consisting of a single point, and $\mathbb{P}^2 = \mathbb{A}^2 \cup H_\infty$ with H_∞ a projective line. Consider the line

$$aX + bY + 1 = 0$$

in $\mathbb{A}^2$. Its closure in $\mathbb{P}^2$ is the line

$$aX + bY + Z = 0.$$

It intersects the hyperplane $H_\infty = V(Z)$ at the point $(-b : a : 0)$, which equals $(1 : -a/b : 0)$ when $b \neq 0$. Note that $-a/b$ is the slope of the line $aX + bY + 1 = 0$, and so the point at which a line intersects H_∞ depends only on the slope of the line: parallel lines meet in one point at infinity. We can think of the projective plane $\mathbb{P}^2$ as being the affine plane $\mathbb{A}^2$ with one point added at infinity for each direction in $\mathbb{A}^2$.

Similarly, we can think of $\mathbb{P}^n$ as being $\mathbb{A}^n$ with one point added at infinity for each direction in $\mathbb{A}^n$ — being parallel is an equivalence relation on the lines in $\mathbb{A}^n$, and there is one point at infinity for each equivalence class of lines.

Note that the point at infinity on the elliptic curve $Y^2 = X^3 + aX + b$ is the intersection of the closure of any vertical line with H_∞.

$\mathbb{P}^n$ is an algebraic variety. For each i, write $\mathcal{O}_i$ for the sheaf on U_i defined by the bijection $\mathbb{A}^n \leftrightarrow U_i \subset \mathbb{P}^n$.

LEMMA 5.6. *Write $U_{ij} = U_i \cap U_j$; then $\mathcal{O}_i|U_{ij} = \mathcal{O}_j|U_{ij}$. When endowed with this sheaf U_{ij} is an affine variety; moreover, $\Gamma(U_{ij}, \mathcal{O}_i)$ is generated as a k-algebra by the functions $(f|U_{ij})(g|U_{ij})$ with $f \in \Gamma(U_i, \mathcal{O}_i)$, $g \in \Gamma(U_j, \mathcal{O}_j)$.*

PROOF. It suffices to prove this for $(i, j) = (0, 1)$. All rings occurring in the proof will be identified with subrings of the field $k(X_0, X_1, \dots, X_n)$.

Recall that

$$U_0 = \{(a_0 : a_1 : \dots : a_n) \mid a_0 \neq 0\};\ (a_0 : a_1 : \dots : a_n) \leftrightarrow (\frac{a_1}{a_0}, \frac{a_2}{a_0}, \dots, \frac{a_n}{a_0}) \in \mathbb{A}^n.$$

Let $k[\frac{X_1}{X_0}, \frac{X_2}{X_0}, \dots, \frac{X_n}{X_0}]$ be the subring of $k(X_0, X_1, \dots, X_n)$ generated by the quotients $\frac{X_i}{X_0}$—it is the polynomial ring in the n variables $\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0}$. An element $f(\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0}) \in k[\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0}]$ defines the map

$$(a_0 : a_1 : \dots : a_n) \mapsto f(\frac{a_1}{a_0}, \dots, \frac{a_n}{a_0}) : U_0 \to k,$$

and in this way $k[\frac{X_1}{X_0}, \frac{X_2}{X_0}, \dots, \frac{X_n}{X_0}]$ becomes identified with the ring of regular functions on U_0, and U_0 with $\operatorname{Specm} k[\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0}]$.

Next consider the open subset of U_0,

$$U_{01} = \{(a_0 : \dots : a_n) \mid a_0 \neq 0,\ a_1 \neq 0\}.$$

It is $D(\frac{X_1}{X_0})$, and is therefore an affine subvariety of $(U_0, \mathcal{O}_0)$. The inclusion $U_{01} \hookrightarrow U_0$ corresponds to the inclusion of rings $k[\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0}] \hookrightarrow k[\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0}, \frac{X_0}{X_1}]$. An element $f(\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0}, \frac{X_0}{X_1})$ of $k[\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0}, \frac{X_0}{X_1}]$ defines the function $(a_0 : \dots : a_n) \mapsto f(\frac{a_1}{a_0}, \dots, \frac{a_n}{a_0}, \frac{a_0}{a_1})$ on U_{01}.

Similarly,

$$U_1 = \{(a_0 : a_1 : \ldots : a_n) \mid a_1 \neq 0\};\ (a_0 : a_1 : \ldots : a_n) \leftrightarrow (\frac{a_0}{a_1}, \ldots, \frac{a_n}{a_1}) \in \mathbb{A}^n,$$

and we identify U_1 with $\operatorname{Specm} k[\frac{X_0}{X_1}, \frac{X_2}{X_0}, \ldots, \frac{X_n}{X_1}]$. An element $f(\frac{X_0}{X_1}, \ldots, \frac{X_n}{X_1}) \in k[\frac{X_0}{X_1}, \ldots, \frac{X_n}{X_1}]$ defines the map $(a_0 : \ldots : a_n) \mapsto f(\frac{a_0}{a_1}, \ldots, \frac{a_n}{a_1}) : U_1 \to k$.

When regarded as an open subset of U_1,

$$U_{01} = \{(a_0 : \ldots : a_n) \mid a_0 \neq 0,\ a_1 \neq 0\},$$

is $D(\frac{X_0}{X_1})$, and is therefore an affine subvariety of $(U_1, \mathcal{O}_1)$, and the inclusion $U_{01} \hookrightarrow U_1$ corresponds to the inclusion of rings $k[\frac{X_0}{X_1}, \ldots, \frac{X_n}{X_1}] \hookrightarrow k[\frac{X_0}{X_1}, \ldots, \frac{X_n}{X_1}, \frac{X_1}{X_0}]$. An element $f(\frac{X_0}{X_1}, \ldots, \frac{X_n}{X_1})$ of $k[\frac{X_0}{X_1}, \ldots, \frac{X_n}{X_1}, \frac{X_1}{X_0}]$ defines the function $(a_0 : \ldots : a_n) \mapsto f(\frac{a_0}{a_1}, \ldots, \frac{a_n}{a_1}, \frac{a_1}{a_0})$ on U_{01}.

The two rings $k[\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}, \frac{X_0}{X_1}]$, $k[\frac{X_0}{X_1}, \ldots, \frac{X_n}{X_1}, \frac{X_1}{X_0}]$ are equal as subrings of $k(X_0, X_1, \ldots, X_n)$, and an element of this ring defines the same function on U_{01} regardless of which of the two rings it is considered an element. Therefore, whether we regard U_{01} as a subvariety of U_0 or of U_1 it inherits the same structure as an affine algebraic variety. This proves the first two assertions, and the third is obvious: $k[\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}, \frac{X_0}{X_1}]$ is generated by its subrings $k[\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}]$ and $k[\frac{X_0}{X_1}, \frac{X_2}{X_1}, \ldots, \frac{X_n}{X_1}]$. □

Write u_i for the map $\mathbb{A}^n \to U_i \subset \mathbb{P}^n$. For any open subset U of $\mathbb{P}^n$, we define $f : U \to k$ to be regular if and only if $f \circ u_i$ is a regular function on $u_i^{-1}(U)$ for all i. This obviously defines a sheaf $\mathcal{O}$ of k-algebras on $\mathbb{P}^n$.

PROPOSITION 5.7. *For each i, the bijection $\mathbb{A}^n \to U_i$ is an isomorphism of ringed spaces, $\mathbb{A}^n \to (U_i, \mathcal{O}|U_i)$; therefore $(\mathbb{P}^n, \mathcal{O})$ is a prevariety. It is in fact a variety.*

PROOF. Let U be an open subset of U_i. Then $f : U \to k$ is regular if and only if

(a) it is regular on $U \cap U_i$, and
(b) it is regular on $U \cap U_j$ for all $j \neq i$.

But the last lemma shows that (a) implies (b) because $U \cap U_j \subset U_{ij}$. To prove that $\mathbb{P}^n$ is separated, apply the criterion (3.26c) to the covering $\{U_i\}$ of $\mathbb{P}^n$. □

EXAMPLE 5.8. Assume k does not have characteristic 2, and let C be the plane projective curve: $Y^2Z = X^3$. For each $a \in k^\times$, there is an automorphism

$$\varphi_a : C \to C,\ (x : y : z) \mapsto (ax : y : a^3z).$$

Patch two copies of $C \times \mathbb{A}^1$ together along $C \times (\mathbb{A}^1 - \{0\})$ by identifying (P, u) with $(\varphi_u(P), u^{-1})$, $P \in C$, $u \in \mathbb{A}^1 - \{0\}$. One obtains in this way a singular 2-dimensional variety that is not quasi-projective (see Hartshorne 1977, p171). (It is even complete (see below), and so if it were quasi-projective, it would be projective. It is known that every irreducible separated curve is quasi-projective, and every nonsingular complete surface is projective, and so this is an example of minimum dimension. In Shafarevich 1994, VI.2.3 there is an example of a nonsingular complete variety of dimension 3 that is not projective.)

The field of rational functions of a projective variety. Recall (page 24) that we attached to each irreducible variety V a field $k(V)$ with the property that $k(V)$ is the field of fractions of $k[U]$ for any open affine $U \subset V$. We now describe this field in the case that $V = \mathbb{P}^n$. Recall that $k[U_0] = k[\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0}]$. We regard this as a subring of $k(X_0, \dots, X_n)$, and wish to identify the field of fractions of $k[U_0]$ as a subfield of $k(X_0, \dots, X_n)$. Any nonzero $F \in k[U_0]$ can be written

$$F(\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0}) = \frac{F^*(X_0, \dots, X_n)}{X_0^{\deg(F)}},$$

and it follows that the field of fractions of $k[U_0]$ is

$$k(U_0) = \left\{ \frac{G(X_0, \dots, X_n)}{H(X_0, \dots, X_n)} \mid G,\ H \text{ homogeneous of the same degree} \right\} \cup \{0\}.$$

Write $k(X_0, \dots, X_n)_0$ for this field (the subscript 0 is short for "subfield of elements of degree 0"), so that $k(\mathbb{P}^n) = k(X_0, \dots, X_n)_0$. Note that an element $F = \frac{G}{H}$ in $k(X_0, \dots, X_n)_0$ defines a well-defined function

$$D(H) \to k,\ (a_0 : \dots : a_n) \mapsto \frac{G(a_0, \dots, a_n)}{H(a_0, \dots, a_n)},$$

which is obviously regular (look at its restriction to U_i).

We now extend this discussion to any irreducible projective variety V. Such a V can be written $V = V(\mathfrak{p})$, where $\mathfrak{p}$ is a homogeneous ideal in $k[X_0, \dots, X_n]$. Let $k_h[V] = k[X_0, \dots, X_n]/\mathfrak{p}$—it is called the *homogeneous coordinate ring* of V. (Note that $k_h[V]$ is the ring of regular functions on the affine cone over V; therefore its dimension is $\dim(V) + 1$. It depends, not only on V, but on the embedding of V into $\mathbb{P}^n$—it is not intrinsic to V (see 5.17 below).) We say that a nonzero $f \in k_h[V]$ is *homogeneous of degree d* if it can be represented by a homogeneous polynomial F of degree d in $k[X_0, \dots, X_n]$. We give 0 degree 0.

LEMMA 5.9. *Each element of $k_h[V]$ can be written uniquely in the form*

$$f = f_0 + \cdots + f_d$$

with f_i homogeneous of degree i.

PROOF. Let F represent f; then F can be written $F = F_0 + \cdots + F_d$ with F_i homogeneous of degree i, and when reduced modulo $\mathfrak{p}$, this gives a decomposition of f of the required type. Suppose f also has a decomposition $f = \sum g_i$, with g_i represented by the homogeneous polynomial G_i of degree i. Then $F - G \in \mathfrak{p}$, and the homogeneity of $\mathfrak{p}$ implies that $F_i - G_i = (F - G)_i \in \mathfrak{p}$. Therefore $f_i = g_i$. □

It therefore makes sense to speak of homogeneous elements of $k[V]$. For such an element h, we define $D(h) = \{P \in V \mid h(P) \neq 0\}$.

Since $k_h[V]$ is an integral domain, we can form its field of fractions $k_h(V)$. Define

$$k_h(V)_0 = \{\frac{g}{h} \in k_h(V) \mid g \text{ and } h \text{ homogeneous of the same degree}\} \cup \{0\}.$$

PROPOSITION 5.10. *The field of rational functions on V is $k_h(V)_0$.*

PROOF. Consider $V_0 \stackrel{\text{df}}{=} U_0 \cap V$. As in the case of $\mathbb{P}^n$, we can identify $k[V_0]$ with a subring of $k_h[V]$, and then the field of fractions of $k[V_0]$ becomes identified with $k_h(V)_0$. □

Regular functions on a projective variety. Again, let V be an irreducible projective variety. Let $f \in k(V)_0$, and let $P \in V$. If we can write $f = \frac{g}{h}$ with g and h homogeneous of the same degree and $h(P) \neq 0$, then we define $f(P) = \frac{g(P)}{h(P)}$. By $g(P)$ we mean the following: let $P = (a_0 : \ldots : a_n)$; represent g by a homogeneous $G \in k[X_0, \ldots, X_n]$, and write $g(P) = G(a_0, \ldots, a_n)$; this is independent of the choice of G, and if $(a_0, \ldots, a_n)$ is replaced by $(ca_0, \ldots, ca_n)$, then $g(P)$ is multiplied by $c^{\deg(g)} = c^{\deg(h)}$. Thus the quotient $\frac{g(P)}{h(P)}$ is well-defined.

Note that we may be able to write f as $\frac{g}{h}$ with g and h homogeneous polynomials of the same degree in many essentially different ways (because $k_h[V]$ need not be a unique factorization domain), and we define the value of f at P if there is one such representation with $h(P) \neq 0$. The value $f(P)$ is independent of the representation $f = \frac{g}{h}$ (write $P = (a_0 : \ldots : a_n) = \mathbf{a}$; if $\frac{g}{h} = \frac{g'}{h'}$ in $k_h(V)_0$, then $gh' = g'h$ in $k_h[V]$, which is the ring of regular functions on the affine cone over V; hence $g(\mathbf{a})h'(\mathbf{a}) = g'(\mathbf{a})h(\mathbf{a})$, which proves the claim).

PROPOSITION 5.11. *For each $f \in k(V) \stackrel{df}{=} k_h(V)_0$, there is an open subset U of V where $f(P)$ is defined, and $P \mapsto f(P)$ is a regular function on U. Every regular function φ on an open subset of V is defined by some $f \in k(V)$.*

PROOF. Straightforward from the above discussion. Note that if the functions defined by f_1 and f_2 agree on an open subset of V, then $f_1 = f_2$ in $k(V)$. □

REMARK 5.12. (a) The elements of $k(V) = k_h(V)_0$ should be thought of as the analogues of meromorphic functions on a complex manifold; the regular functions on an open subset U of V are the "meromorphic functions without poles" on U. [In fact, when $k = \mathbb{C}$, this is more than an analogy: a nonsingular projective algebraic variety over $\mathbb{C}$ defines a complex manifold, and the meromorphic functions on the manifold are precisely the rational functions on the variety. For example, the meromorphic functions on the Riemann sphere are the rational functions in z.]

(b) We shall see presently (5.19) that, for any nonzero homogeneous $h \in k_h[V]$, $D(h)$ is an open affine subset of V. The ring of regular functions on it is

$$k[D(h)] = \{g/h^m \mid g \text{ homogeneous of degree } m\deg(h)\} \cup \{0\}.$$

We shall also see that the ring of regular functions on V itself is just k, i.e., any regular function on an irreducible (connected will do) projective variety is constant. However, if U is an open nonaffine subset of V, then the ring $\Gamma(U, \mathcal{O}_V)$ of regular functions can be almost anything—it needn't even be a finitely generated k-algebra!

Morphisms from projective varieties. We describe the morphisms from a projective variety to another variety.

PROPOSITION 5.13. *The map*

$$\pi : \mathbb{A}^{n+1} \setminus \{\textit{origin}\} \to \mathbb{P}^n,\ (a_0, \ldots, a_n) \mapsto (a_0 : \ldots : a_n)$$

is an open morphism of algebraic varieties. A map $\alpha : \mathbb{P}^n \to V$ with V a prevariety is regular if and only if $\alpha \circ \pi$ is regular.

PROOF. The restriction of π to $D(X_i)$ is the projection

$$(a_0, \dots, a_n) \mapsto (\frac{a_0}{a_i} : \dots : \frac{a_n}{a_i}) : k^{n+1} \setminus V(X_i) \to U_i,$$

which is the regular map of affine varieties corresponding to the map of k-algebras

$$k\left[\frac{X_0}{X_i}, \dots, \frac{X_n}{X_i}\right] \to k[X_0, \dots, X_n][X_i^{-1}].$$

(In the first algebra $\frac{X_j}{X_i}$ is to be thought of as a single variable.) It now follows from (3.5) that π is regular.

Let U be an open subset of $k^{n+1} \setminus \{\text{origin}\}$, and let U' be the union of all the lines through the origin that meet U, that is, $U' = \pi^{-1}\pi(U)$. Then U' is again open in $k^{n+1} \setminus \{\text{origin}\}$, because $U' = \cup cU$, $c \in k^\times$, and $x \mapsto cx$ is an automorphism of $k^{n+1} \smallsetminus \{\text{origin}\}$. The complement Z of U' in $k^{n+1} \smallsetminus \{\text{origin}\}$ is a closed cone, and the proof of (5.2) shows that its image is closed in $\mathbb{P}^n$; but $\pi(U)$ is the complement of $\pi(Z)$. Thus π sends open sets to open sets.

The rest of the proof is straightforward. □

Thus, the regular maps $\mathbb{P}^n \to V$ are just the regular maps $\mathbb{A}^{n+1} \smallsetminus \{\text{origin}\} \to V$ factoring through $\mathbb{P}^n$ (as maps of sets).

REMARK 5.14. Consider polynomials $F_0(X_0, \dots, X_m), \dots, F_n(X_0, \dots, X_m)$ of the same degree. The map

$$(a_0 : \dots : a_m) \mapsto (F_0(a_0, \dots, a_m) : \dots : F_n(a_0, \dots, a_m))$$

obviously defines a regular map to $\mathbb{P}^n$ on the open subset of $\mathbb{P}^m$ where not all F_i vanish, that is, on the set $\cup D(F_i) = \mathbb{P}^n \setminus V(F_1, \dots, F_n)$. Its restriction to any subvariety V of $\mathbb{P}^m$ will also be regular. It may be possible to extend the map to a larger set by representing it by different polynomials. Conversely, every such map arises in this way, at least locally. More precisely, there is the following result.

PROPOSITION 5.15. *Let $V = V(\mathfrak{a}) \subset \mathbb{P}^m$, $W = V(\mathfrak{b}) \subset \mathbb{P}^n$. A map $\varphi\colon V \to W$ is regular if and only if, for every $P \in V$, there exist polynomials $F_0(X_0, \dots, X_m), \dots, F_n(X_0, \dots, X_m)$, homogeneous of the same degree, such that*

$$Q = (b_0 : \dots : b_n) \mapsto (F_0(b_0, \dots, b_m) : \dots : F_n(b_0, \dots, b_m))$$

for all points $Q = (b_0 : \dots : b_m)$ in some neighbourhood of P in $V(\mathfrak{a})$.

PROOF. Straightforward. □

EXAMPLE 5.16. We prove that the circle $X^2 + Y^2 = Z^2$ is isomorphic to $\mathbb{P}^1$. After an obvious change of variables, the equation of the circle becomes $C : XZ = Y^2$. Define

$$\varphi : \mathbb{P}^1 \to C,\ (a : b) \mapsto (a^2 : ab : b^2).$$

For the inverse, define

$$\psi : C \to \mathbb{P}^1 \quad \text{by} \quad \begin{cases} (a : b : c) \mapsto (a : b) & \text{if } a \neq 0 \\ (a : b : c) \mapsto (b : c) & \text{if } b \neq 0 \end{cases}.$$

Note that,

$$a \neq 0 \neq b,\ ac = b^2 \Rightarrow \frac{c}{b} = \frac{b}{a}$$

and so the two maps agree on the set where they are both defined. Clearly, both φ and ψ are regular, and one checks directly that they are inverse.

Examples of regular maps of projective varieties. We list some of the classic maps.

EXAMPLE 5.17. Let $L = \sum c_i X_i$ be a nonzero linear form in $n+1$ variables. Then the map

$$(a_0 : \ldots : a_n) \mapsto (\frac{a_0}{L(\mathbf{a})}, \ldots, \frac{a_n}{L(\mathbf{a})})$$

is a bijection of $D(L) \subset \mathbb{P}^n$ onto the hyperplane $L(X_1, \ldots, X_n) = 1$ of $\mathbb{A}^{n+1}$, with inverse

$$(a_0, \ldots, a_n) \mapsto (a_0 : \ldots : a_n).$$

Both maps are regular — for example, the components of the first map are the regular functions $\frac{X_j}{\sum c_i X_i}$. As $V(L-1)$ is affine, so also is $D(L)$, and its ring of regular functions is $k[\frac{X_0}{\sum c_i X_i}, \ldots, \frac{X_n}{\sum c_i X_i}]$. (This is really a polynomial ring in n variables—any one variable $X_j / \sum c_i X_i$ for which $c_j \neq 0$ can be omitted—see lemma 4.11.)

EXAMPLE 5.18. (The Veronese mapping.) Let

$$I = \{(i_0, \ldots, i_n) \in \mathbb{N}^{n+1} \mid \sum i_j = m\}.$$

Note that I indexes the monomials of degree m in $n+1$ variables. It has $\binom{m+n}{m}$ elements[16]. Write $\nu_{n,m} = \binom{m+n}{m} - 1$, and consider the projective space $\mathbb{P}^{\nu_{n,m}}$ whose coordinates are indexed by I; thus a point of $\mathbb{P}^{\nu_{n,m}}$ can be written $(\ldots : b_{i_0 \ldots i_n} : \ldots)$. The Veronese mapping is defined to be

$$v\colon \mathbb{P}^n \to \mathbb{P}^{\nu_{n,m}},\ (a_0 : \ldots : a_n) \mapsto (\ldots : b_{i_0 \ldots i_n} : \ldots),\ b_{i_0 \ldots i_n} = a_0^{i_0} \ldots a_n^{i_n}.$$

For example, when $n = 1$ and $m = 2$, the Veronese map is

$$\mathbb{P}^1 \to \mathbb{P}^2,\ (a_0 : a_1) \mapsto (a_0^2 : a_0 a_1 : a_1^2).$$

Its image is the curve $\nu(\mathbb{P}^1) : X_0 X_2 = X_1^2$, and the map

$$(b_{2,0} : b_{1,1} : b_{0,2}) \mapsto \begin{cases} (b_{2,0} : b_{1,1}) \text{ if } b_{2,0} \neq 1 \\ (b_{1,1} : b_{0,2}) \text{ if } b_{0,2} \neq 0. \end{cases}$$

[16]This can be proved by induction on $m+n$. If $m = 0 = n$, then $\binom{0}{0} = 1$, which is correct. A general homogeneous polynomial of degree m can be written uniquely as

$$F(X_0, X_1, \ldots, X_n) = F_1(X_1, \ldots, X_n) + X_0 F_2(X_0, X_1, \ldots, X_n)$$

with F_1 homogeneous of degree m and F_2 homogeneous of degree $m-1$. But

$$\binom{m+n}{n} = \binom{m+n-1}{m} + \binom{m+n-1}{m-1}$$

because they are the coefficients of X^m in

$$(X+1)^{m+n} = (X+1)(X+1)^{m+n-1},$$

and this proves what we want.

is an inverse $\nu(\mathbb{P}^1) \to \mathbb{P}^1$. (Cf. Example 5.17.) [17]

When $n = 1$ and m is general, the Veronese map is

$$\mathbb{P}^1 \to \mathbb{P}^m,\ (a_0 : a_1) \mapsto (a_0^m : a_0^{m-1}a_1 : \ldots : a_1^m).$$

I claim that, in the general case, the image of ν is a closed subset of $\mathbb{P}^{\nu_{n,m}}$ and that ν defines an isomorphism of projective varieties $\nu : \mathbb{P}^n \to \nu(\mathbb{P}^n)$.

First note that the map has the following interpretation: if we regard the coordinates a_i of a point P of $\mathbb{P}^n$ as being the coefficients of a linear form $L = \sum a_i X_i$ (well-defined up to multiplication by nonzero scalar), then the coordinates of $\nu(P)$ are the coefficients of the homogeneous polynomial L^m with the binomial coefficients omitted.

As $L \neq 0 \Rightarrow L^m \neq 0$, the map ν is defined on the whole of $\mathbb{P}^n$, that is,

$$(a_0, \ldots, a_n) \neq (0, \ldots, 0) \Rightarrow (\ldots, b_{i_0 \ldots i_n}, \ldots) \neq (0, \ldots, 0).$$

Moreover, $L_1 \neq cL_2 \Rightarrow L_1^m \neq cL_2^m$, because $k[X_0, \ldots, X_n]$ is a unique factorization domain, and so ν is injective. It is clear from its definition that ν is regular.

We shall see later in this section that the image of any projective variety under a regular map is closed, but in this case we can prove directly that $\nu(\mathbb{P}^n)$ is defined by the system of equations:

$$b_{i_0 \ldots i_n} b_{j_0 \ldots j_n} = b_{k_0 \ldots k_n} b_{\ell_0 \ldots \ell_n}, \qquad i_h + j_h = k_h + \ell_h, \text{ all } h \qquad (*).$$

Obviously $\mathbb{P}^n$ maps into the algebraic set defined by these equations. Conversely, let

$$V_i = \{(\ldots : b_{i_0 \ldots i_n} : \ldots) \mid b_{0 \ldots 0 m 0 \ldots 0} \neq 0\}.$$

Then $\nu(U_i) \subset V_i$ and $\nu^{-1}(V_i) = U_i$. It is possible to write down a regular map $V_i \to U_i$ inverse to $\nu | U_i$: for example, define $V_0 \to \mathbb{P}^n$ to be

$$(\ldots : b_{i_0 \ldots i_n} : \ldots) \mapsto (b_{m,0,\ldots,0} : b_{m-1,1,0,\ldots,0} : b_{m-1,0,1,0,\ldots,0} : \ldots : b_{m-1,0,\ldots,0,1}).$$

Finally, one checks that $\nu(\mathbb{P}^n) \subset \cup V_i$.

For any closed variety $W \subset \mathbb{P}^n$, $\nu | W$ is an isomorphism of W onto a closed subvariety $\nu(W)$ of $\nu(\mathbb{P}^n) \subset \mathbb{P}^{\nu_{n,m}}$.

Remark 5.19. The Veronese mapping has a very important property. If F is a nonzero homogeneous form of degree $m \geq 1$, then $V(F) \subset \mathbb{P}^n$ is called a *hypersurface of degree* m and $V(F) \cap W$ is called a *hypersurface section* of the projective variety W. When $m = 1$, "surface" is replaced by "plane".

Now let H be the hypersurface in $\mathbb{P}^n$ of degree m

$$\sum a_{i_0 \ldots i_n} X_0^{i_0} \cdots X_n^{i_n} = 0,$$

and let L be the hyperplane in $\mathbb{P}^{\nu_{n,m}}$ defined by

$$\sum a_{i_0 \ldots i_n} X_{i_0 \ldots i_n}.$$

[17] Note that, although $\mathbb{P}^1$ and $\nu(\mathbb{P}^1)$ are isomorphic, their homogeneous coordinate rings are not. In fact $k_h[\mathbb{P}^1] = k[X_0, X_1]$, which is the affine coordinate ring of the smooth variety $\mathbb{A}^2$, whereas $k_h[\nu(\mathbb{P}^1)] = k[X_0, X_1, X_2]/(X_0X_2 - X_1^2)$ which is the affine coordinate ring of the singular variety $X_0X_2 - X_1^2$.

Then $\nu(H) = \nu(\mathbb{P}^n) \cap L$, i.e.,

$$H(\mathbf{a}) = 0 \iff L(\nu(\mathbf{a})) = 0.$$

Thus for any closed subvariety W of $\mathbb{P}^n$, ν defines an isomorphism of the hypersurface section $W \cap H$ of V onto the hyperplane section $\nu(W) \cap L$ of $\nu(W)$. This observation often allows one to reduce questions about hypersurface sections to questions about hyperplane sections.

As one example of this, note that ν maps the complement of a hypersurface section of W isomorphically onto the complement of a hyperplane section of $\nu(W)$, which we know to be affine. Thus the complement of any hypersurface section of a projective variety is an affine variety—we have proved the statement in (5.12b).

EXAMPLE 5.20. An element $A = (a_{ij})$ of GL_{n+1} defines an automorphism of $\mathbb{P}^n$:

$$(x_0 : \ldots : x_n) \mapsto (\ldots : \sum a_{ij}x_j : \ldots);$$

clearly it is a regular map, and the inverse matrix gives the inverse map. Scalar matrices act as the identity map.

Let $\mathrm{PGL}_{n+1} = \mathrm{GL}_{n+1}/k^\times I$, where I is the identity matrix, that is, PGL_{n+1} is the quotient of GL_{n+1} by its centre. Then PGL_{n+1} is the complement in $\mathbb{P}^{(n+1)^2-1}$ of the hypersurface $\det(X_{ij}) = 0$, and so it is an affine variety with ring of regular functions

$$k[\mathrm{PGL}_{n+1}] = \{F(\ldots, X_{ij}, \ldots)/\det(X_{ij})^m \mid \deg(F) = m \cdot (n+1)\} \cup \{0\}.$$

It is an affine algebraic group.

The homomorphism $\mathrm{PGL}_{n+1} \to \mathrm{Aut}(\mathbb{P}^n)$ is obviously injective. It is also surjective — see Mumford, Geometric Invariant Theory, Springer, 1965, p20.

EXAMPLE 5.21. (The Segre mapping.) This is the mapping

$$((a_0 : \ldots : a_m), (b_0 : \ldots : b_n)) \mapsto ((\ldots : a_ib_j : \ldots)) : \mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^{mn+m+n}.$$

The index set for $\mathbb{P}^{mn+m+n}$ is $\{(i,j) \mid 0 \le i \le m, \quad 0 \le j \le n\}$. Note that if we interprete the tuples on the left as being the coefficients of two linear forms $L_1 = \sum a_iX_i$ and $L_2 = \sum b_jY_j$, then the image of the pair is the set of coefficients of the homogeneous form of degree 2, L_1L_2. From this observation, it is obvious that the map is defined on the whole of $\mathbb{P}^m \times \mathbb{P}^n$ ($L_1 \ne 0 \ne L_2 \Rightarrow L_1L_2 \ne 0$) and is injective. On any subset of the form $U_i \times U_j$ it is defined by polynomials, and so it is regular. Again one can show that it is an isomorphism onto its image, which is the closed subset of $\mathbb{P}^{mn+m+n}$ defined by the equations

$$w_{ij}w_{kl} - w_{il}w_{kj} = 0.$$

(See Shafarevich 1988, I.5.1) For example, the map

$$((a_0 : a_1), (b_0 : b_1)) \mapsto (a_0b_0 : a_0b_1 : a_1b_0 : a_1b_1) : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$$

has image the hypersurface

$$H : \quad WZ = XY.$$

The map

$$(w : x : y : z) \mapsto ((w : y), (w : x))$$

is an inverse on the set where it is defined. [Incidentally, $\mathbb{P}^1 \times \mathbb{P}^1$ is not isomorphic to $\mathbb{P}^2$, because in the first variety there are closed curves, e.g., two vertical lines, that don't intersect.]

If V and W are closed subvarieties of $\mathbb{P}^m$ and $\mathbb{P}^n$, then the Segre map sends $V \times W$ isomorphically onto a closed subvariety of $\mathbb{P}^{mn+m+n}$. Thus products of projective varieties are projective.

There is an explicit description of the topology on $\mathbb{P}^m \times \mathbb{P}^n$: the closed sets are the sets of common solutions of families of equations

$$F(X_0, \dots, X_m; Y_0, \dots, Y_n) = 0$$

with F separately homogeneous in the X's and in the Y's.

EXAMPLE 5.22. Let $L_1, \dots, L_{n-d}$ be linearly independent linear forms in $n+1$ variables; their zero set E in k^{n+1} has dimension $d+1$, and so their zero set in $\mathbb{P}^n$ is a d-dimensional linear space. Define $\pi : \mathbb{P}^n - E \to \mathbb{P}^{n-d-1}$ by $\pi(a) = (L_1(a) : \dots : L_{n-d}(a))$; such a map is called a *projection with centre* E. If V is a closed subvariety disjoint from E, then π defines a regular map $V \to \mathbb{P}^{n-d-1}$. More generally, if $F_1, \dots, F_r$ are homogeneous forms of the same degree, and $Z = V(F_1, \dots, F_r)$, then $a \mapsto (F_1(a) : \dots : F_r(a))$ is a morphism $\mathbb{P}^n - Z \to \mathbb{P}^{r-1}$.

By carefully choosing the centre E, it is possible to project any smooth curve in $\mathbb{P}^n$ isomorphically onto a curve in $\mathbb{P}^3$, and nonisomorphically (but bijectively on an open subset) onto a curve in $\mathbb{P}^2$ with only nodes as singularities.[18] For example, suppose we have a nonsingular curve C in $\mathbb{P}^3$. To project to $\mathbb{P}^2$ we need three linear forms L_0, L_1, L_2 and the centre of the projection is the point where all forms are zero. We can think of the map as projecting from the centre P_0 onto some (projective) plane by sending the point P to the point where P_0P intersects the plane. To project C to a curve with only ordinary nodes as singularities, one needs to choose P_0 so that it doesn't lie on any tangent to C, any trisecant (line crossing the curve in 3 points), or any chord at whose extremities the tangents are coplanar. See for example Samuel, P., Lectures on Old and New Results on Algebraic Curves, Tata Notes, 1966.

PROPOSITION 5.23. *Let V be a projective variety, and let S be a finite set of points of V. Then S is contained in an open affine subset of V.*

PROOF. Find a hyperplane passing through at least one point of V but missing the elements of S, and apply 5.19. (See the exercises.) □

REMARK 5.24. There is a converse: let V be a nonsingular complete (see below) irreducible variety; if every finite set of points in V is contained in an open affine subset of V then V is projective. (Conjecture of Chevalley; proved by Kleiman about 1966.)

Complete varieties. Complete varieties are the analogues in the category of varieties of compact topological spaces in the category of Hausdorff topological spaces. Recall that the image of a compact space under a continuous map is compact, and hence is closed if the image space is Hausdorff. Moreover, a Hausdorff space V is

[18] A nonsingular curve of degree d in $\mathbb{P}^2$ has genus $\frac{(d-1)(d-2)}{2}$. Thus, if g is not of this form, a curve of genus g can't be realized as a nonsingular curve in $\mathbb{P}^2$.

compact if and only if, for all topological spaces W, the projection $q : V \times W \to W$ is closed, i.e., maps closed sets to closed sets (see Bourbaki, Topologie Générale, I, §10).

DEFINITION 5.25. An algebraic variety V is said to be *complete* if for all algebraic varieties W, the projection $q\colon V \times W \to W$ is closed.

Note that a complete variety is required to be separated — we really mean it to be a variety and not a prevariety.

EXAMPLE 5.26. Consider the projection

$$(x, y) \mapsto y : \mathbb{A}^1 \times \mathbb{A}^1 \to \mathbb{A}^1$$

This is not closed; for example, the variety $V : XY = 1$ is closed in $\mathbb{A}^2$ but its image in $\mathbb{A}^1$ omits the origin. However, if we replace V with its closure in $\mathbb{P}^1 \times \mathbb{A}^1$, then its projection is the whole of $\mathbb{A}^1$.

PROPOSITION 5.27. *Let V be complete.*

(a) *A closed subvariety of V is complete.*
(b) *If V' is complete, so also is $V \times V'$.*
(c) *For any morphism $\alpha : V \to W$, $\alpha(V)$ is closed and complete; in particular, if V is a subvariety of W, then it is closed in W.*
(d) *If V is connected, then any regular map $\alpha : V \to \mathbb{P}^1$ is either constant or onto.*
(e) *If V is connected, then any regular function on V is constant.*

PROOF. (a) Let Z be a closed subvariety of a complete variety V. Then for any variety W, $Z \times W$ is closed in $V \times W$, and so the restriction of the closed map $q : V \times W \to W$ to $Z \times W$ is also closed.

(b) The projection $V \times V' \times W \to W$ is the composite of the projections

$$V \times V' \times W \to V' \times W \to W,$$

both of which are closed.

(c) Let $\Gamma_\alpha = \{(v, \alpha(v))\} \subset V \times W$ be the graph of α. It is a closed subset of $V \times W$ (because W is a variety, see 3.25), and $\alpha(V)$ is the projection of Γ_α onto W. Since V is complete, the projection is closed, and so $\alpha(V)$ is closed, and hence is a subvariety of W. Consider

$$\Gamma_\alpha \times W \to \alpha(V) \times W \to W.$$

We have that Γ_α is complete (because it is isomorphic to V, see 3.25), and so the mapping $\Gamma_\alpha \times W \to W$ is closed. As $\Gamma_\alpha \to \alpha(V)$ is surjective, it follows that $\alpha(V) \times W \to W$ is also closed.

(d) Recall that the only proper closed subsets of $\mathbb{P}^1$ are the finite sets, and such a set is connected if and only if it consists of a single point. Because $\alpha(V)$ is connected and closed, it must either be a single point (and α is constant) or $\mathbb{P}^1$ (and α is onto).

(e) A regular function on V is a regular map $f : V \to \mathbb{A}^1 \subset \mathbb{P}^1$. Regard it as a map into $\mathbb{P}^1$. If it isn't constant, it must be onto, which contradicts the fact that it maps into $\mathbb{A}^1$. □

COROLLARY 5.28. *Consider a regular map $\alpha\colon V \to W$; if V is complete and connected and W is affine, then the image of α is a point.*

PROOF. Embed W as a closed subvariety of $\mathbb{A}^n$, and write $\alpha = (\alpha_1, \dots, \alpha_n)$ where each α_i is a regular map $W \to \mathbb{A}^1$. Then each α_i is a regular function on V, and hence is constant. □

REMARK 5.29. The statement that a complete variety V is closed in any larger variety W perhaps explains the name: if V is complete, W is irreducible, and $\dim V = \dim W$, then $V = W$. (Contrast $\mathbb{A}^n \subset \mathbb{P}^n$.)

THEOREM 5.30. *A projective variety is complete.*

LEMMA 5.31. *A variety V is complete if and only if $q : V \times W \to W$ is a closed mapping for all irreducible affine varieties W.*

PROOF. Straightforward. □

After (5.27a), it suffices to prove the Theorem for projective space $\mathbb{P}^n$ itself; thus we have to prove that the projection $W \times \mathbb{P}^n \to W$ is a closed mapping in the case that W is an affine variety. Note that $W \times \mathbb{P}^n$ is covered by the open affines $W \times U_i$, $0 \le i \le n$, and that a subset U of $W \times \mathbb{P}^n$ is closed if and only if its intersection with each $W \times U_i$ is closed. We shall need another more explicit description of the topology on $W \times \mathbb{P}^n$.

Let $A = k[W]$, and let $B = A[X_0, \dots, X_n]$. Note that $B = A \otimes_k k[X_0, \dots, X_n]$, and so we can view it as the ring of regular functions on $W \times \mathbb{A}^{n+1}$: $f \otimes g$ takes the value $f(w) \cdot g(\mathbf{a})$ at the point $(w, \mathbf{a}) \in W \times \mathbb{A}^{n+1}$. The ring B has an obvious grading—a monomial $aX_0^{i_0} \dots X_n^{i_n}$, $a \in A$, has degree $\sum i_j$—and so we have the notion of a homogeneous ideal $\mathfrak{b} \subset B$. It makes sense to speak of the zero set $V(\mathfrak{b}) \subset W \times \mathbb{P}^n$ of such an ideal. For any ideal $\mathfrak{a} \subset A$, $\mathfrak{a}B$ is homogeneous, and $V(\mathfrak{a}B) = V(\mathfrak{a}) \times \mathbb{P}^n$.

LEMMA 5.32. *(i) For each homogeneous ideal $\mathfrak{b} \subset B$, the set $V(\mathfrak{b})$ is closed, and every closed subset of $W \times \mathbb{P}^n$ is of this form.*

(ii) The set $V(\mathfrak{b})$ is empty if and only if $\operatorname{rad}(\mathfrak{b}) \supset (X_0, \dots, X_n)$.

(iii) If W is irreducible, then $W = V(\mathfrak{b})$ for some homogeneous prime ideal $\mathfrak{b}$.

PROOF. In the case that $A = k$, we proved all this on pp 90–92, and the same arguments apply in the present more general situation. For example, to see that $V(\mathfrak{b})$ is closed, apply the criterion stated above.

The set $V(\mathfrak{b})$ is empty if and only if the cone $V^{\text{aff}}(\mathfrak{b}) \subset W \times \mathbb{A}^{n+1}$ defined by $\mathfrak{b}$ is contained in $W \times \{\text{origin}\}$. But $\sum a_{i_0 \dots i_n} X_0^{i_0} \dots X_n^{i_n}$, $a_{i_0 \dots i_n} \in k[W]$, is zero on $W \times \{\text{origin}\}$ if an only if its constant term is zero, and so

$$I^{\text{aff}}(W \times \{\text{origin}\}) = (X_0, X_1, \dots, X_n).$$

Thus, the Nullstellensatz shows that $V(\mathfrak{b}) = \emptyset \Rightarrow \operatorname{rad}(\mathfrak{b}) = (X_0, \dots, X_n)$. Conversely, if $X_i^N \in \mathfrak{b}$ for all i, then obviously $V(\mathfrak{b})$ is empty.

For the final statement, note that if $V(\mathfrak{b})$ is irreducible, then the closure of its inverse image in $W \times \mathbb{A}^{n+1}$ is also irreducible, and so the ideal of functions zero on it prime. □

PROOF OF 5.30. Write p for the projection $W \times \mathbb{P}^n \to W$. We have to show that Z closed in $W \times \mathbb{P}^n$ implies $p(Z)$ closed in W. If Z is empty, this is true, and so we can assume it to be nonempty. Then Z is a finite union of irreducible closed subsets

Z_i of $W \times \mathbb{P}^n$, and it suffices to show that each $p(Z_i)$ is closed. Thus we may assume that Z is irreducible, and hence that $Z = V(\mathfrak{b})$ with $\mathfrak{b}$ a prime homogeneous ideal in $B = A[X_0, \dots, X_n]$.

Note that if $p(Z) \subset W'$, W' a closed subvariety of W, then $Z \subset W' \times \mathbb{P}^n$—we can then replace W with W'. This allows us to assume that $p(Z)$ is dense in W, and we now have to show that $p(Z) = W$.

Because $p(Z)$ is dense in W, the image of the cone $V^{\text{aff}}(\mathfrak{b})$ under the projection $W \times \mathbb{A}^{n+1} \to W$ is also dense in W, and so (see 2.21a) the map $A \to B/\mathfrak{b}$ is injective.

Let $w \in W$: we shall show that if $w \notin p(Z)$, i.e., if there does not exist a $P \in \mathbb{P}^n$ such that $(w, P) \in Z$, then $p(Z)$ is empty, which is a contradiction.

Let $\mathfrak{m} \subset A$ be the maximal ideal corresponding to w. Then $\mathfrak{m}B+\mathfrak{b}$ is a homogeneous ideal, and $V(\mathfrak{m}B+\mathfrak{b}) = V(\mathfrak{m}B) \cap V(\mathfrak{b}) = (w \times \mathbb{P}^n) \cap V(\mathfrak{b})$, and so w will be in the image of Z unless $V(\mathfrak{m}B+\mathfrak{b}) \neq \emptyset$. But if $V(\mathfrak{m}B+\mathfrak{b}) = \emptyset$, then $\mathfrak{m}B+\mathfrak{b} \supset (X_0, \dots, X_n)^N$ for some N (by 5.33b), and so $\mathfrak{m}B + \mathfrak{b}$ contains the set B_N of homogeneous polynomials of degree N. Because $\mathfrak{m}B$ and $\mathfrak{b}$ are homogeneous ideals,

$$B_N \subset \mathfrak{m}B + \mathfrak{b} \Rightarrow B_N = \mathfrak{m}B_N + B_N \cap \mathfrak{b}.$$

In detail: the first inclusion says that an $f \in B_N$ can be written $f = g+h$ with $g \in \mathfrak{m}B$ and $h \in \mathfrak{b}$. On equating homogeneous components, we find that $f_N = g_N + h_N$. Moreover: $f_N = f$; if $g = \sum m_i b_i$, $m_i \in \mathfrak{m}$, $b_i \in B$, then $g_N = \sum m_i b_{iN}$; and $h_N \in \mathfrak{b}$ because $\mathfrak{b}$ is homogeneous. Together these show $f \in \mathfrak{m}B_N + B_N \cap \mathfrak{b}$.

Let $M = B_N/B_N \cap \mathfrak{b}$, regarded as an A-module. The displayed equation says that $M = \mathfrak{m}M$. The argument in the proof of Nakayama's lemma (4.17) shows that $(1+m)M = 0$ for some $m \in \mathfrak{m}$. Because $A \to B/\mathfrak{b}$ is injective, the image of $1+m$ in $B/\mathfrak{b}$ is nonzero. But $M = B_N/B_N \cap \mathfrak{b} \subset B/\mathfrak{b}$, which is an integral domain, and so the equation $(1+m)M = 0$ implies that $M = 0$. Hence $B_N \subset \mathfrak{b}$, and so $X_i^N \in \mathfrak{b}$ for all i, which contradicts the assumption that $Z = V(\mathfrak{b})$ is nonempty. □

Elimination theory. We have shown that, for any closed subset Z of $\mathbb{P}^m \times W$, the projection $q(Z)$ of Z in W is closed. Elimination theory [19] is concerned with providing an algorithm for passing from the equations defining Z to the equations defining $q(Z)$. We illustrate this in one case.

Let $P = s_0X^m+s_1X^{m-1}+\cdots+s_m$ and $Q = t_0X^n+t_1X^{n-1}+\cdots+t_n$ be polynomials. The *resultant* of P and Q is defined to be the determinant

$$\begin{vmatrix} s_0 & s_1 & \dots & s_m & & \\ & s_0 & \dots & & s_m & \\ & & \dots & & & \dots \\ t_0 & t_1 & \dots & t_n & & \\ & t_0 & \dots & & t_n & \\ & & \dots & & & \dots \end{vmatrix} \quad \begin{matrix} \\ n\text{-rows} \\ \\ \\ m\text{-rows} \\ \\ \end{matrix}$$

[19] Elimination theory became unfashionable several decades ago—one prominent algebraic geometer went so far as to announce that Theorem 5.30 eliminated elimination theory from mathematics, provoking Abhyankar, who prefers equations to abstractions, to start the chant "eliminate the eliminators of elimination theory". With the rise of computers, it has become fashionable again.

There are n rows of s's and m rows of t's, so that the matrix is $(m+n)\times(m+n)$; all blank spaces are to be filled with zeros. The resultant is a polynomial in the coefficients of P and Q.

PROPOSITION 5.33. *The resultant $Res(P,Q)=0$ if and only if*

(a) *both s_0 and t_0 are zero; or*
(b) *the two polyomials have a common root.*

PROOF. If (a) holds, then certainly $\mathrm{Res}(P,Q)=0$. Suppose that α is a common root of P and Q, so that there exist polynomials P_1 and Q_1 of degrees $m-1$ and $n-1$ respectively such that

$$P(X)=(X-\alpha)P_1(X),\qquad Q(X)=(X-\alpha)Q_1(X).$$

From these equations we find that

$$P(X)Q_1(X)-Q(X)P_1(X)=0.\qquad (*)$$

On equating the coefficients of $X^{m+n-1},\dots,X,1$ in (*) to zero, we find that the coefficients of P_1 and Q_1 are the solutions of a system of $m+n$ linear equations in $m+n$ unknowns. The matrix of coefficients of the system is the transpose of the matrix

$$\begin{pmatrix} s_0 & s_1 & \dots & s_m & & \\ & s_0 & \dots & & s_m & \\ & & \dots & & & \dots \\ t_0 & t_1 & \dots & t_n & & \\ & t_0 & \dots & & t_n & \\ & & \dots & & & \dots \end{pmatrix}$$

The existence of the solution shows that this matrix has determinant zero, which implies that $\mathrm{Res}(P,Q)=0$.

Conversely, suppose that $\mathrm{Res}(P,Q)=0$ but neither s_0 nor t_0 is zero. Because the above matrix has determinant zero, we can solve the linear equations to find polynomials P_1 and Q_1 satisfying (*). If α is a root of P, then it must also be a root of P_1 or Q. If the former, cancel $X-\alpha$ from the left hand side of (*) and continue. As $\deg P_1<\deg P$, we eventually find a root of P that is not a root of P_1, and so must be a root of Q. □

The proposition can be restated in projective terms. We define the resultant of two homogeneous polynomials

$$P(X,Y)=s_0X^m+s_1X^{m-1}Y+\cdots+s_mY^m,\quad Q(X,Y)=t_0X^n+\cdots+t_nY^n,$$

exactly as in the nonhomogeneous case.

PROPOSITION 5.34. *The resultant $\mathrm{Res}(P,Q)=0$ if and only if P and Q have a common zero in $\mathbb{P}^1$.*

PROOF. The zeros of $P(X,Y)$ in $\mathbb{P}^1$ are of the form:

(a) $(a:1)$ with a a root of $P(X,1)$, or
(b) $(1:0)$ in the case that $s_0=0$.

Thus (5.34) is a restatement of (5.33). □

Now regard the coefficients of P and Q as indeterminants. The pairs of polynomials (P,Q) are parametrized by the space $\mathbb{A}^{m+1}\times\mathbb{A}^{n+1}=\mathbb{A}^{m+n+2}$. Consider the closed subset $V(P,Q)$ in $\mathbb{A}^{m+n+2}\times\mathbb{P}^1$. The proposition shows that its projection on $\mathbb{A}^{m+n+2}$ is the set defined by $\operatorname{Res}(P,Q)=0$. Thus, not only have we shown that the projection of $V(P,Q)$ is closed, but we have given an algorithm for passing from the polynomials defining the closed set to those defining its projection.

Elimination theory does this in general. Given a family of polynomials $P_i(T_1,\dots,T_m;X_0,\dots,X_n)$, homogeneous in the X_i, elimination theory gives an algorithm for finding polynomials $R_j(T_1,\dots,T_n)$ such that the $P_i(a_1,\dots,a_m;X_0,\dots,X_n)$ have a common zero if and only if $R_j(a_1,\dots,a_n)=0$ for all j. (Our theorem only shows that the R_j exist.) See Cox et al. 1992, Chapter 8, Section 5..

Maple can find the resultant of two polynomials in one variable: for example, entering "resultant$((x+a)^5,(x+b)^5,x)$" gives the answer $(-a+b)^{25}$. Explanation: the polynomials have a common root if and only if $a=b$, and this can happen in 25 ways. Macaulay doesn't seem to know how to do more.

The rigidity theorem. The paucity of maps between projective varieties has some interesting consequences. First an observation: for any point $w\in W$, the projection map $V\times W\to V$ defines an isomorphism $V\times\{w\}\to V$ with inverse $v\mapsto(v,w):V\to V\times W$ (this map is regular because its components are).

THEOREM 5.35. *Let $\alpha:V\times W\to U$ be a regular map, and assume that V is complete, that V and W are irreducible, and that U is separated. If there are points $u_0\in U$, $v_0\in V$, and $w_0\in W$ such that*

$$\alpha(V\times\{w_0\})=\{u_0\}=\alpha(\{v_0\}\times W)$$

then $\alpha(V\times W)=\{u_0\}$.

PROOF. Let U_0 be an open affine neighbourhood of u_0. Because the projection map $q:V\times W\to W$ is closed, $Z\stackrel{\text{df}}{=}q(\alpha^{-1}(U-U_0))$ is closed in W. Note that a point w of W lies outside Z if and only $\alpha(V\times\{w\})\subset U_0$. In particular $w_0\in W-Z$, and so $W-Z$ is dense in W. As $V\times\{w\}$ is complete and U_0 is affine, $\alpha(V\times\{w\})$ must be a point whenever $w\in W-Z$: in fact, $\alpha(V\times\{w\})=\alpha(v_0,w)=\{u_0\}$. Thus α is constant on the dense subset $V\times(W-Z)$ of $V\times W$, and so is constant. □

An *abelian variety* is a complete connected group variety.

COROLLARY 5.36. *Every regular map $\alpha:A\to B$ of abelian varieties is the composite of a homomorphism with a translation; in particular, a regular map $\alpha:A\to B$ such that $\alpha(0)=0$ is a homomorphism.*

PROOF. After composing α with a translation, we may assume that $\alpha(0)=0$. Consider the map

$$\varphi:A\times A\to B,\qquad \varphi(a,a')=\alpha(a+a')-\alpha(a)-\alpha(a').$$

Then $\varphi(A\times 0)=0=\varphi(0\times A)$ and so $\varphi=0$. This means that α is a homomorphism. □

COROLLARY 5.37. *The group law on an abelian variety is commutative.*

PROOF. Commutative groups are distinguished among all groups by the fact that the map taking an element to its inverse is a homomorphism: if $(gh)^{-1} = g^{-1}h^{-1}$, then, on taking inverses, we find that $gh = hg$. Since the negative map, $a \mapsto -a : A \to A$, takes the identity element to itself, the preceding corollary shows that it is a homomorphism. □

Projective space without coordinates. Let E be a vector space over k of dimension $n+1$. The set $\mathbb{P}(E)$ of lines through zero in E has a natural structure of an algebraic variety: the choice of a basis for E defines an bijection $\mathbb{P}(E) \to \mathbb{P}^n$, and the inherited structure of an algebraic variety on $\mathbb{P}(E)$ is independent of the choice of the basis. Note that in contrast to $\mathbb{P}^n$, which has $n+1$ distinguished hyperplanes, namely, $X_0 = 0, \dots, X_n = 0$, no hyperplane in $\mathbb{P}(E)$ is distinguished.

One can also define the structure of an algebraic variety on the set $G_{n+1,r}(E)$ of r-dimensional subspaces in E. The resulting varieties are called *Grassmanians*. They are projective.

Bezout's theorem. Let V be a hypersurface in $\mathbb{P}^n$ (that is, a closed subvariety of codimension 1). For such a variety, $I(V) = (F(X_0, \dots, X_n))$ with F a homogenous polynomial without repeated factors. We define the *degree* of V to be the degree of F.

The next theorem is one of the oldest, and most famous, in algebraic geometry.

THEOREM 5.38 (Bezout). *Let C and D be curves in $\mathbb{P}^2$ of degrees m and n respectively. If C and D have no irreducible component in common, then they intersect in exactly mn points, counted with appropriate multiplicities.*

PROOF. Decompose C and D into their irreducible components. Clearly it suffices to prove the theorem for each irreducible component of C and each irreducible component of D. We can therefore assume that C and D are themselves irreducible.

We know from (1.22) that $C \cap D$ is of dimension zero, and so is finite. After a change of variables, we can assume that $a \neq 0$ for all points $(a : b : c) \in C \cap D$.

Let $F(X, Y, Z)$ and $G(X, Y, Z)$ be the polynomials defining C and D, and write

$$F = s_0 Z^m + s_1 Z^{m-1} + \cdots + s_m, \qquad G = t_0 Z^n + t_1 Z^{n-1} + \cdots + t_n$$

with s_i and t_j polynomials in X and Y of degrees i and j respectively. Clearly $s_m \neq 0 \neq t_n$, for otherwise F and G would have Z as a common factor. Let R be the resultant of F and G, regarded as polynomials in Z. It is a homogeneous polynomial of degree mn in X and Y, or else it is identically zero. If the latter occurs, then for every $(a, b) \in k^2$, $F(a, b, Z)$ and $G(a, b, Z)$ have a common zero, which contradicts the finiteness of $C \cap D$. Thus R is a nonzero polynomial of degree mn. Write $R(X, Y) = X^{mn} R_*(\frac{Y}{X})$ where $R_*(T)$ is a polynomial of degree $\leq mn$ in $T = \frac{Y}{X}$.

Suppose first that $\deg R_* = mn$, and let $\alpha_1, \dots, \alpha_{mn}$ be the roots of R_* (some of them may be multiple). Each such root can be written $\alpha_i = \frac{b_i}{a_i}$, and $R(a_i, b_i) = 0$. According to (5.34) this means that the polynomials $F(a_i, b_i, Z)$ and $G(a_i, b_i, Z)$ have a common root c_i. Thus $(a_i : b_i : c_i)$ is a point on $C \cap D$, and conversely, if $(a : b : c)$ is a point on $C \cap D$ (so $a \neq 0$), then $\frac{b}{a}$ is a root of $R_*(T)$. Thus we see in this case,

that $C \cap D$ has precisely mn points, provided we take the multiplicity of $(a : b : c)$ to be the multiplicity of $\frac{b}{a}$ as a root of R_*.

Now suppose that R_* has degree $r < mn$. Then $R(X,Y) = X^{mn-r}P(X,Y)$ where $P(X,Y)$ is a homogeneous polynomial of degree r not divisible by X. Obviously $R(0,1) = 0$, and so there is a point $(0 : 1 : c)$ in $C \cap D$, in contradiction with our assumption. □

REMARK 5.39. The above proof has the defect that the notion of multiplicity has been too obviously chosen to make the theorem come out right. It is possible to show that the theorem holds with the following more natural definition of multiplicity. Let P be an isolated point of $C \cap D$. There will be an affine neighbourhood U of P and regular functions f and g on U such that $C \cap U = V(f)$ and $D \cap U = V(g)$. We can regard f and g as elements of the local ring $\mathcal{O}_P$, and clearly $\operatorname{rad}(f,g) = \mathfrak{m}$, the maximal ideal in $\mathcal{O}_P$. It follows that $\mathcal{O}_P/(f,g)$ is finite-dimensional over k, and we define the multiplicity of P in $C \cap D$ to be $\dim_k(\mathcal{O}_P/(f,g))$. For example, if C and D cross transversely at P, then f and g will form a system of local parameters at P — $(f,g) = \mathfrak{m}$ — and so the multiplicity is one.

The attempt to find good notions of multiplicities in very general situations has motivated much of the most interesting work in commutative algebra over the last 20 years.

Hilbert polynomials (sketch). Recall that for a projective variety $V \subset \mathbb{P}^n$,

$$k_h[V] = k[X_0, \dots, X_n]/\mathfrak{b} = k[x_0, \dots, x_n],$$

where $\mathfrak{b} = I(V)$. We observed that $\mathfrak{b}$ is homogeneous, and therefore $k_h[V]$ is a graded ring:

$$k_h[V] = \oplus_{m \geq 0} k_h[V]_m,$$

where $k_h[V]_m$ is the subspace generated by the monomials in the x_i of degree m. Clearly $k_h[V]_m$ is a finite-dimensional k-vector space.

THEOREM 5.40. *There is a unique polynomial $P(V,T)$ such that $P(V,m) = \dim_k k[V]_m$ for all m sufficiently large.*

PROOF. Omitted. □

EXAMPLE 5.41. For $V = \mathbb{P}^n$, $k_h[V] = k[X_0, \dots, X_n]$, and (see the footnote on page 89), $\dim k_h[V]_m = \binom{m+n}{n} = \frac{(m+n)\cdots(m+1)}{n!}$, and so

$$P(\mathbb{P}^n, T) = \binom{T+n}{n} = \frac{(T+n)\cdots(T+1)}{n!}.$$

The polynomial $P(V,T)$ in the theorem is called the *Hilbert polynomial* of V. Despite the notation, it depends not just on V but also on its embedding in projective space.

THEOREM 5.42. *Let V be a projective variety of dimension d and degree δ; then*

$$P(V,T) = \frac{\delta}{d!}T^d + \textit{terms of lower degree.}$$

PROOF. Omitted. □

The *degree* of a projective variety is the number of points in the intersection of the variety and of a general linear variety of complementary dimension (see later).

EXAMPLE 5.43. Let V be the image of the Veronese map

$$(a_0 : a_1) \mapsto (a_0^d : a_0^{d-1}a_1 : \ldots : a_1^d) : \mathbb{P}^1 \to \mathbb{P}^d.$$

Then $k_h[V]_m$ can be identified with the set of homogeneous polynomials of degree $m \cdot d$ in two variables (look at the map $\mathbb{A}^2 \to \mathbb{A}^{d+1}$ given by the same equations), which is a space of dimension $dm + 1$, and so

$$P(V, T) = dT + 1.$$

Thus V has dimension 1 (which we certainly knew) and degree d.

Macaulay knows how to compute Hilbert polynomials.

References: Hartshorne 1977, I.7; Atiyah and Macdonald 1969, Chapter 11; Harris 1992, Lecture 13.

6. Finite Maps

Throughout this section, k is an algebraically closed field.

Recall that an A-algebra B is said to be *finite* if it is finitely generated as an A-module. This is equivalent to B being finitely generated as an A-algebra and integral over A.

Definition 6.1. A regular map $\varphi : W \to V$ is said to be *finite* if for all open affine subsets U of V, $\varphi^{-1}(U)$ is an affine variety, and $k[\varphi^{-1}(U)]$ is a finite $k[U]$-algebra.

Proposition 6.2. *It suffices to check the condition in the definition for all subsets in one open affine covering (U_i) of V.*

Proof. Omitted. (See Mumford 1966, III.1, proposition 5). □

Hence a map $\varphi : \mathrm{Specm}(B) \to \mathrm{Specm}(A)$ of affine varieties is finite if and only if B is a finite A-algebra.

Proposition 6.3. (a) *For any closed subvariety Z of V, the inclusion $Z \hookrightarrow V$ is finite.*
(b) *The composite of two finite morphisms is finite.*
(c) *The product of two finite morphisms is finite.*

Proof. (a) Let U be an open affine subvariety of V. Then $Z \cap U$ is a closed subvariety of U. It is therefore affine, and the map $Z \cap U \to U$ corresponds to a map $A \to A/\mathfrak{a}$ of rings, which is obviously finite.

(b) If B is a finite A-algebra and C is a finite B-algebra, then C is a finite A-algebra: indeed, if $\{b_i\}$ is a set of generators for B as an A-module, and $\{c_j\}$ is a set of generators for C as a B-module, then $\{b_i c_j\}$ is a set of generators for C as an A-module.

(c) If B and B' are respectively finite A and A'-algebras, then $B \otimes_k B'$ is a finite $A \otimes_k A'$-algebra: indeed, if $\{b_i\}$ is a set of generators for B as an A-module, and $\{b'_j\}$ is a set of generators for B' as an A-module, the $\{b_i \otimes b'_j\}$ is a set of generators for $B \otimes_A B'$ as an A-module. □

By way of contrast, an open immersion is rarely finite. For example, the inclusion $\mathbb{A}^1 - \{0\} \hookrightarrow \mathbb{A}^1$ is not finite because the ring $k[T, T^{-1}]$ is not finitely generated as a $k[T]$-module. (Any finite set of elements in $k[T, T^{-1}]$ has a fixed power of T as a common denominator.)

The fibres of a regular map $\varphi : W \to V$ are the subvarieties $\varphi^{-1}(P)$ of W for $P \in V$. When the fibres are all finite, φ is said to be *quasi-finite*.

Proposition 6.4. *A finite map $\varphi : W \to V$ is quasi-finite.*

Proof. Let $P \in V$; we wish to show $\varphi^{-1}(P)$ is finite. After replacing V with an affine neighbourhood of P, we can suppose that it is affine, and then W will be affine also. The map φ then corresponds to a map $\alpha : A \to B$ of affine k-algebras, and a point Q of W maps to P if and only $\alpha^{-1}(\mathfrak{m}_Q) = \mathfrak{m}_P$. But this holds if and only if[20] $\mathfrak{m}_Q \supset \alpha(\mathfrak{m}_P)$, and so the points of W mapping to P are in one-to-one correspondence

[20] Clearly then $\alpha^{-1}(\mathfrak{m}_Q) \supset \mathfrak{m}_P$, and we know it is a maximal ideal.

with the maximal ideals of $B/\alpha(\mathfrak{m})B$. Clearly $B/\alpha(\mathfrak{m})B$ is generated as a k-vector space by the image of any generating set for B as an A-module, and the next lemma shows that it has only finitely many maximal ideals. □

LEMMA 6.5. *A finite k-algebra A has only finitely many maximal ideals.*

PROOF. Let $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ be maximal ideals in A. They are obviously coprime in pairs, and so the Chinese Remainder Theorem (see below) shows that the map

$$A \to A/\mathfrak{m}_1 \times \cdots \times A/\mathfrak{m}_n, \qquad a \mapsto (\dots, a_i \mod \mathfrak{m}_i, \dots),$$

is surjective. It follows that $\dim_k A \geq \sum \dim_k(A/\mathfrak{m}_i) \geq n$ (dimensions as k-vector spaces). □

LEMMA 6.6 (Chinese Remainder Theorem). *Let $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ be ideals in a ring A. If $\mathfrak{a}_i$ is coprime to $\mathfrak{a}_j$ (i.e., $\mathfrak{a}_i + \mathfrak{a}_j = A$) whenever $i \neq j$, then the map*

$$A \to A/\mathfrak{a}_1 \times \cdots \times A/\mathfrak{a}_m$$

is surjective, with kernel $\prod \mathfrak{a}_i = \cap \mathfrak{a}_i$.

PROOF. The proof is elementary (see Atiyah and MacDonald 1969, 1.10). □

THEOREM 6.7. *A finite map $\varphi : W \to V$ is closed.*

PROOF. Again we can assume V and W to be affine. Let Z be a closed subset of W. The restriction of φ to Z is finite (by 6.3a and b), and so we can replace W with Z; we then we have to show that $\mathrm{Im}(\varphi)$ is closed. The map corresponds to a finite map of rings $A \to B$. This will factor, $A \to A/\mathfrak{a} \hookrightarrow B$, from which we obtain maps

$$\mathrm{Specm}(B) \to \mathrm{Specm}(A/\mathfrak{a}) \hookrightarrow \mathrm{Specm}(A).$$

The second map identifies $\mathrm{Specm}(A/\mathfrak{a})$ with the closed subvariety $V(\mathfrak{a})$ of $\mathrm{Specm}(A)$, and so it remains to show that the first map is surjective. This is a consequence of the next lemma. □

LEMMA 6.8 (Going-Up Theorem). *Let $A \subset B$ be rings with B integral over A.*

(a) *For every prime ideal $\mathfrak{p}$ of A, there is a prime ideal $\mathfrak{q}$ of B such that $\mathfrak{q} \cap A = \mathfrak{p}$.*
(b) *Let $\mathfrak{p} = \mathfrak{q} \cap A$; then $\mathfrak{p}$ is maximal if and only if $\mathfrak{q}$ is maximal.*

PROOF. (a) If S is a multiplicative subset of a ring A, then the prime ideals of $S^{-1}A$ are in one-to-one correspondence with the prime ideals of A not meeting S (see 4.15). It therefore suffices to prove (a) after A and B have been replaced by $S^{-1}A$ and $S^{-1}B$, where $S = A - \mathfrak{p}$. Thus we may assume that A is local, and that $\mathfrak{p}$ is its unique maximal ideal. In this case, for all proper ideals $\mathfrak{b}$ of B, $\mathfrak{b} \cap A \subset \mathfrak{p}$ (otherwise $\mathfrak{b} \supset A \ni 1$). To complete the proof of (a), I shall show that for all maximal ideals $\mathfrak{n}$ of B, $\mathfrak{n} \cap A = \mathfrak{p}$.

Consider $B/\mathfrak{n} \supset A/(\mathfrak{n} \cap A)$. Here $B/\mathfrak{n}$ is a field, which is integral over its subring $A/(\mathfrak{n} \cap A)$, and $\mathfrak{n} \cap A$ will be equal to $\mathfrak{p}$ if and only if $A/(\mathfrak{n} \cap A)$ is a field. Thus the claim follows from the next lemma. □

LEMMA 6.9. *Let A be a subring of a field K. If K is integral over A, then A also is a field.*

PROOF. Let $a \in A$, $a \neq 0$. Then $a^{-1} \in K$, and it is integral over A:

$$(a^{-1})^n + a_1(a^{-1})^{n-1} + \cdots + a_n = 0,\ a_i \in A.$$

On multiplying through by a^{n-1}, we find that

$$a^{-1} + a_1 + \cdots + a_n a^{n-1} = 0,$$

from which it follows that $a^{-1} \in A$. □

PROOF. (of 6.8b)The ring $B/\mathfrak{q}$ contains $A/\mathfrak{p}$, and it is integral over $A/\mathfrak{p}$. If $\mathfrak{q}$ is maximal, then (6.9) shows that $\mathfrak{p}$ is also. For the converse, note that any integral domain algebraic over a field is a field — it is a union of integral domains finite over k, and multiplication by any nonzero element of an integral domain finite over a field is an isomorphism (it is injective by definition, and an injective endomorphism of a finite-dimensional vector space is also surjective). □

COROLLARY 6.10. *Let $\varphi : W \to V$ be finite; if V is complete, then so also is W.*

PROOF. Consider

$$W \times T \to V \times T \to T, \quad (w,t) \mapsto (\varphi(w),t) \mapsto t.$$

Because $W \times T \to V \times T$ is finite (see 6.3c), it is closed, and because V is complete, $V \times T \to T$ is closed. A composite of closed maps is closed, and therefore the projection $W \times T \to T$ is closed. □

EXAMPLE 6.11. labelFM11 (a) Project $XY = 1$ onto the X axis. This map is quasi-finite but not finite, because $k[X, X^{-1}]$ is not finite over $k[X]$.

(b) The map $\mathbb{A}^2 - \{\text{origin}\} \hookrightarrow \mathbb{A}^2$ is quasi-finite but not finite, because the inverse image of $\mathbb{A}^2$ is not affine (2.20).

(c) Let $V = V(X^n + T_1X^{n-1} + \cdots + T_n) \subset \mathbb{A}^{n+1}$, and consider the projection map

$$(a_1, \ldots, a_n, x) \mapsto (a_1, \ldots, a_n) : V \to \mathbb{A}^n.$$

The fibre over any point $(a_1, \ldots, a_n) \in \mathbb{A}^n$ is the set of solutions of

$$X^n + a_1X^{n-1} + \cdots + a_n = 0,$$

and so it has exactly n points, counted with multiplicities. The map is certainly quasi-finite; it is also finite because it corresponds to the finite map of k-algebras,

$$k[T_1, \ldots, T_n] \to k[T_1, \ldots, T_n, X]/(X^n + T_1X^{n-1} + \cdots + T_n).$$

(d) Let $V = V(T_0X^n + T_1X^{n-1} + \cdots + T_n) \subset \mathbb{A}^{n+2}$. The projection $\varphi : V \to \mathbb{A}^{n+1}$ has finite fibres except for the fibre above $(0, \ldots, 0)$, which is $\mathbb{A}^1$. The restriction $\varphi|V \smallsetminus \varphi^{-1}(\text{origin})$ is quasi-finite, but not finite. Above points of the form $(0, \ldots, 0, *, \ldots, *)$ some of the roots "vanish off to ∞". (Example (a) is a special case of this.)

(e) Let $P(X,Y) = T_0X^n + T_1X^{n-1}Y + \ldots + T_nY^n$, and let V be its zero set in $\mathbb{P}^1 \times (\mathbb{A}^{n+1} - \{\text{origin}\})$. In this case, the projection map $V \to \mathbb{A}^{n+1} - \{\text{origin}\}$ is finite. (Prove this directly, or apply 6.24 below.)

(f) The morphism $\mathbb{A}^1 \to \mathbb{A}^2$, $t \mapsto (t^2, t^3)$ is finite because the image of $k[X,Y]$ in $k[T]$ is $k[T^2, T^3]$, and $\{1, T\}$ is a set of generators for $k[T]$ over this subring.

(g) The morphism $\mathbb{A}^1 \to \mathbb{A}^1$, $a \mapsto a^m$ is finite (special case of (c)).

(h) The obvious map

$$(\mathbb{A}^1 \text{ with the origin doubled }) \to \mathbb{A}^1$$

is quasi-finite but not finite (the inverse image of $\mathbb{A}^1$ is not affine).

EXERCISE 6.12. Prove that a finite map is an isomorphism if and only if it is bijective and étale. (Cf. Harris 1992, 14.9.)

The Frobenius map $t \mapsto t^p\colon \mathbb{A}^1 \to \mathbb{A}^1$ in characteristic $p \neq 0$ and the map $t \mapsto (t^2, t^3)\colon \mathbb{A}^1 \to V(Y^2 - X^3) \subset \mathbb{A}^2$ from the line to the cuspidal cubic (see 2.17c) are examples of finite bijective regular maps that are not isomorphisms.

Noether Normalization Theorem. This theorem sometimes allows us to reduce the proofs of statements about affine varieties to the case of $\mathbb{A}^n$.

THEOREM 6.13. *For any irreducible affine algebraic variety V of a variety of dimension d, there is a finite surjective map $\varphi : V \to \mathbb{A}^d$.*

PROOF. This is a geometric re-statement of the original theorem. □

THEOREM 6.14 (Noether Normalization Theorem). *Let A be a finitely generated k-algebra, and assume that A is an integral domain. Then there exist elements $y_1, \dots, y_d \in A$ that are algebraically independent over k and such that A is integral over $k[y_1, \dots, y_d]$.*

PROOF. Let $x_1, \dots, x_n$ generate A as a k-algebra. We can renumber the x_i so that $x_1, \dots, x_d$ are algebraically independent and $x_{d+1}, \dots, x_n$ are algebraically dependent on $x_1, \dots, x_d$ (see 6.12 of my notes on Fields and Galois Theory).

Because x_n is algebraically dependent on $x_1, \dots, x_d$, there exists a nonzero polynomial $f(X_1, \dots, X_d, T)$ such that $f(x_1, \dots, x_d, x_n) = 0$. Write

$$f(X_1, \dots, X_d, T) = a_0T^m + a_1T^{m-1} + \cdots + a_m$$

with $a_i \in k[X_1, \dots, X_d]$ ($\approx k[x_1, \dots, x_d]$). If a_0 is a nonzero constant, we can divide through by it, and then x_n will satisfy a monic polynomial with coefficients in $k[x_1, \dots, x_d]$, that is, x_n will be integral (not merely algebraic) over $k[x_1, \dots, x_d]$. The next lemma suggest how we might achieve this happy state by making a linear change of variables. □

LEMMA 6.15. *If $F(X_1, \dots, X_d, T)$ is a homogeneous polynomial of degree r, then*

$$F(X_1 + \lambda_1T, \dots, X_d + \lambda_dT, T) = F(\lambda_1, \dots, \lambda_d, 1)T^r + \text{terms of degree} < r \text{ in } T.$$

PROOF. The polynomial $F(X_1 + \lambda_1T, \dots, X_d + \lambda_dT, T)$ is still homogeneous of degree r (in $X_1, \dots, X_d, T$), and the coefficient of the monomial T^r in it can be obtained by substituting 0 for each X_i and 1 for T. □

PROOF. (of the Noether Normalization Theorem, continued). Note that unless $F(X_1, \dots, X_d, T)$ is the zero polynomial, it will always be possible to choose $(\lambda_1, \dots, \lambda_d)$ so that $F(\lambda_1, \dots, \lambda_d, 1) \neq 0$ —substituting $T = 1$ merely dehomogenizes the polynomial (no cancellation of terms occurs), and a nonzero polynomial can't be zero on all of k^n (this can be proved by induction on the number of variables; it uses only that k is infinite).

Let F be the homogeneous part of highest degree of f, and choose $(\lambda_1, \dots, \lambda_d)$ so that $F(\lambda_1, \dots, \lambda_d, 1) \neq 0$. The lemma then shows that

$$f(X_1 + \lambda_1 T, \dots, X_d + \lambda_d T, T) = cT^r + b_1 T^{r-1} + \cdots + b_0,$$

with $c = F(\lambda_1, \dots, \lambda_d, 1) \in k^\times$, $b_i \in k[X_1, \dots, X_d]$, $\deg b_i < r$. On substituting x_n for T and $x_i - \lambda_i x_n$ for X_i we obtain an equation demonstrating that x_n is integral over $k[x_1 - \lambda_1 x_n, \dots, x_d - \lambda_d x_n]$. Put $x_i' = x_i - \lambda_i x_n$, $1 \leq i \leq d$. Then x_n is integral over the ring $k[x_1', \dots, x_d']$, and it follows that A is integral over $A' = k[x_1', \dots, x_d', x_{d+1}, \dots, x_{n-1}]$. Repeat the process for A', and continue until the theorem is proved. □

Remark 6.16. The above proof uses only that k is infinite, not that it is algebraically closed (that's all one needs for a nonzero polynomial not to be zero on all of k^n). There are other proofs that work also for finite fields (see Mumford 1966, p4-6), but the above proof gives us the additional information that the y_i's can be chosen to be linear combinations of the x_i. This has the following geometric interpretation:

let V be a closed subvariety of $\mathbb{A}^n$ of dimension d; then there exists a linear map $\mathbb{A}^n \to \mathbb{A}^d$ whose restriction to V is a finite map $V \twoheadrightarrow \mathbb{A}^d$.

Zariski's main theorem. An obvious way to construct a nonfinite quasi-finite map $W \to V$ is to take a finite map $W' \to V$ and remove a closed subset of W'. Zariski's Main Theorem show that, when W and V are separated, every quasi-finite map arises in this way.

Theorem 6.17 (Zariski's Main Theorem). *Any quasi-finite map of varieties $\varphi : W \to V$ factors into $W \overset{\iota}{\hookrightarrow} W' \overset{\varphi'}{\to} V$ with φ' finite and ι an open immersion.*

Proof. Omitted — see the references below. □

Remark 6.18. Assume (for simplicity) that V and W are irreducible and affine. The proof of the theorem provides the following description of the factorization: it corresponds to the maps

$$k[V] \to k[W'] \to k[W]$$

with $k[W']$ the integral closure of $k[V]$ in $k[W]$.

A regular map $\varphi : W \to V$ of irreducible varieties is said to be *birational* if it induces an isomorphism $k(V) \to k(W)$ on the fields of rational functions (that is, if it demonstrates that W and V are birationally equivalent).

Remark 6.19. One may ask how a birational regular map $\varphi : W \to V$ can fail to be an isomorphism. Here are three examples.

(a) The inclusion of an open subset into a variety is birational.
(b) The map $\mathbb{A}^1 \to C$, $t \mapsto (t^2, t^3)$, is birational. Here C is the cubic $Y^2 = X^3$, and the map $k[C] \to k[\mathbb{A}^1] = k[T]$ identifies $k[C]$ with the subring $k[T^2, T^3]$ of $k[T]$. Both rings have $k(T)$ as their fields of fractions.
(c) For any smooth variety V and point $P \in V$, there is a regular birational map $\varphi : V' \to V$ such that the restriction of φ to $V' - \varphi^{-1}(P)$ is an isomorphism onto $V - P$, but $\varphi^{-1}(P)$ is the projective space attached to the vector space $T_P(V)$.

The next result says that, if we require the target variety to be normal (thereby excluding example (b)), and we require the map to be quasi-finite (thereby excluding example (c)), then we are left with (a).

COROLLARY 6.20. *Let $\varphi : W \to V$ be a birational regular map of irreducible varieties. Assume*

(a) *V is normal, and*
(b) *φ is quasi-finite.*

Then φ is an isomorphism of W onto an open subset of V.

PROOF. Factor φ as in the theorem. For each open affine subset U of V, $k[\varphi'^{-1}(U)]$ is the integral closure of $k[U]$ in $k(W)$. But $k(W) = k(V)$ (because φ is birational), and $k[U]$ is integrally closed in $k(V)$ (because V is normal), and so $U = \varphi'^{-1}(U)$ (as varieties). It follows that $W' = V$. □

REMARK 6.21. Let W and V be irreducible varieties, and let $\varphi : W \to V$ be a dominating map. It induces a map $k(V) \hookrightarrow k(W)$, and if $\dim W = \dim V$, then $k(W)$ is a finite extension of $k(V)$. We shall see later that, if n is the separable degree of $k(V)$ over $k(W)$, then there is an open subset U of W such that φ is $n:1$ on U, i.e., for $P \in \varphi(U)$, $\varphi^{-1}(P)$ has exactly n points.

Now suppose that φ is a bijective regular map $W \to V$. We shall see later that this implies that W and V have the same dimension. Assume:

(a) $k(W)$ is separable over $k(V)$;
(b) V is normal.

From (i) and the preceding remark, we find that φ is birational, and from (ii) and the corollary, we find that φ is an isomorphism of W onto an open subset of V; as it is surjective, it must be an isomorphism of W onto V. We conclude: a bijective regular map $\varphi : W \to V$ satisfying the conditions (i) and (ii) is an isomorphism.

REMARK 6.22. The full name of Theorem 6.17 is "the main theorem of Zariski's paper Trans. AMS, 53 (1943), 490-532". Zariski's original statement is that in (6.20). Grothendieck proved it in the stronger form (6.17) for all schemes. There is a good discussion of the theorem in Mumford 1966, III.9. See also: Nowak, Krzysztof Jan, A simple algebraic proof of Zariski's main theorem on birational transformations, Univ. Iagel. Acta Math. No. 33 (1996), 115–118; MR 97m:14016.

Fibre products. Consider a variety S and two regular maps $\varphi : V \to S$ and $\psi : W \to S$. Then the set

$$V \times_S W \stackrel{\text{df}}{=} \{(v, w) \in V \times W \mid \varphi(v) = \psi(w)\}$$

is a closed subvariety of $V \times W$, called the *fibred product* of V and W over S. Note that if S consists of a single point, then $V \times_S W = V \times W$.

Write φ' for the map $(v,w)\mapsto w : V\times_S W\to W$ and ψ' for the map $(v,w)\mapsto v : V\times_S W\to V$. We then have a commutative diagram:

$$\begin{array}{ccc} V\times_S W & \xrightarrow{\psi'} & W \\ \big\downarrow{\scriptstyle \varphi'} & & \big\downarrow{\scriptstyle \varphi} \\ W & \xrightarrow{\psi} & S. \end{array}$$

The fibred product has the following universal property: consider a pair of regular maps $\alpha : T\to V$, $\beta : T\to W$; then

$$(\alpha,\beta) = t\mapsto (\alpha(t),\,\beta(t)) : T\to V\times W$$

factors through $V\times_S W$ (as a map of sets) if and only if $\varphi\alpha = \psi\beta$, in which case (α,β) is regular (because it is regular as a map into $V\times W$).

Suppose V, W, and S are affine, and let A, B, and R be their rings of regular functions. Then $A\otimes_R B$ has the same universal property as $V\times_S W$, except with the directions of the arrows reversed. Since both objects are uniquely determined by their universal properties, this shows that $k[V\times_S W] = A\otimes_R B/\ N$, where N is the nilradical of $A\otimes_R B$ (that is, the set of nilpotent elements of $A\otimes_R B$).

The map φ' in the above diagram is called the base change of φ with respect to ψ. For any point $P\in S$, the base change of $\varphi : V\to S$ with respect to $P\hookrightarrow S$ is the map $\varphi^{-1}(P)\to P$ induced by φ.

Proposition 6.23. *The base change of a finite map is finite.*

Proof. We may assume that all the varieties concerned are affine. Then the statement becomes: if A is a finite R-algebra, then $A\otimes_R B/\ N$ is a finite B-algebra, which is obvious. □

Proper maps. A regular map $\varphi : V\to S$ of varieties is said to be proper if it is "universally closed", that is, if for all maps $T\to S$, the base change $\varphi' : V\times_S T\to T$ of φ is closed. Note that a variety V is complete if and only if the map $V\to\{\text{point}\}$ is proper. From its very definition, it is clear that the base change of a proper map is proper. In particular, if $\varphi : V\to S$ is proper, then $\varphi^{-1}(P)$ is a complete variety for all $P\in S$.

Proposition 6.24. *A finite map of varieties is proper.*

Proof. The base change of a finite map is finite, and hence closed. □

The next result (whose proof requires Zariski's Main Theorem) gives a purely geometric criterion for a regular map to be finite.

Proposition 6.25. *A proper quasi-finite map $\varphi\colon W\to V$ of varieties is finite.*

Proof. Factor φ into $W\overset{\iota}{\hookrightarrow} W'\overset{\alpha}{\to} W$ with α finite and ι an open immersion. Factor ι into

$$W\overset{w\mapsto(w,\iota w)}{\to} W\times_V W'\overset{(w,w')\mapsto w'}{\to} W'.$$

The image of the first map is Γ_ι, which is closed because W' is a variety (see 3.25; W' is separated because it is finite over a variety — exercise). Because φ is proper,

the second map is closed. Hence ι is an open immersion with closed image. It follows that its image is a connected component of W', and that W is isomorphic to that connected component. □

If W and V are curves, then any surjective map $W \to V$ is closed. Thus it is easy to give examples of closed surjective quasi-finite nonfinite maps. For example, the map

$$a \mapsto a^n : \mathbb{A}^1 \smallsetminus \{0\} \to \mathbb{A}^1,$$

which corresponds to the map on rings

$$k[T] \to k[T, T^{-1}], \quad T \mapsto T^n,$$

is such a map. This doesn't violate the theorem, because the map is only closed, not universally closed.

7. Dimension Theory

Recall that to an irreducible variety V, we attach a field $k(V)$ — it is the field of fractions of $k[U]$ for any open affine subvariety U of V, and also the field of fractions of $\mathcal{O}_P$ for any point P in V. We defined the dimension of V to be the transcendence degree of $k(V)$ over k. Note that, directly from this definition, $\dim V = \dim U$ for any open subvariety U of V. Also, that if $W \to V$ is a finite surjective map, then $\dim W = \dim V$ (because $k(W)$ is a finite field extension of $k(V)$).

When V is not irreducible, we defined the dimension of V to be the maximum dimension of an irreducible component of V, and we said that V is pure of dimension d if the dimensions of the irreducible components are all equal to d.

In §1 and §3 we proved the following results:

7.1. (a) *The dimension of a linear subvariety of $\mathbb{A}^n$ (that is, a subvariety defined by linear equations) has the value predicted by linear algebra (see 1.20b, 4.11). In particular,* $\dim \mathbb{A}^n = n$. *As a consequence,* $\dim \mathbb{P}^n = n$.

(b) *Let Z be a proper closed subset of $\mathbb{A}^n$; then Z has pure codimension one in $\mathbb{A}^n$ if and only if $I(Z)$ is generated by a single nonconstant polynomial. Such a variety is called an affine hypersurface (see 1.21 and 4.25)*[21].

(c) *If V is irreducible and Z is a proper closed subset of V, then* $\dim Z < \dim V$ *(see 1.22).*

Affine varieties. The fundamental additional result that we need is that, when we impose additional polynomial conditions on an algebraic set, the dimension doesn't go down by more than linear algebra would suggest.

Theorem 7.2. *Let V be an irreducible affine variety, and let $f \in k[V]$. If f is not zero or a unit in $k[V]$, then $V(f)$ is pure of dimension* $\dim(V) - 1$.

Alternatively we can state this as follows: let V be a closed subvariety of $\mathbb{A}^n$ and let $F \in k[X_1, \dots, X_n]$; then

$$V \cap V(f) = \begin{cases} V & \text{if } F \text{ is identically zero on } V \\ \emptyset & \text{if } F \text{ has no zeros on } V \\ \text{hypersurface} & \text{otherwise.} \end{cases}$$

where by hypersurface we mean a closed subvariety of codimension 1.

We can also state it in terms of the algebras: let A be an affine k-algebra; let $f \in A$ be neither zero nor a unit, and let $\mathfrak{p}$ be a prime ideal that is minimal among those containing (f); then

$$\text{tr deg}_k A/\mathfrak{p} = \text{tr deg}_k A - 1.$$

Proof. We begin the proof of Theorem 7.2. Note that we know it already in the case that $V = \mathbb{A}^n$ (see 7.1b).

We first show that it suffices to prove the theorem in the case that $V(f)$ is irreducible.

Suppose $Z_0, \dots, Z_n$ are the irreducible components of $V(f)$. We can choose a point $P \in Z_0$ that does not lie on any other Z_i (otherwise the decomposition $V(f) = \cup Z_i$

[21] The cautious reader will check that we didn't use 4.18 or 4.19 in the proof of 4.25.

would be redundant). As $Z_1, \dots, Z_n$ are closed, there is an open neighbourhood U of P, which we can take to be affine, that does not meet any Z_i except Z_0. Now $V(f|U) = Z_0 \cap U$, which is irreducible.

As $V(f)$ is irreducible, $\mathrm{rad}(f)$ is a prime ideal $\mathfrak{p} \subset k[V]$. According to the Noether normalization theorem (6.14), there is a finite surjective map $\pi : V \to \mathbb{A}^d$, which realizes $k(V)$ is a finite extension of the field $k(\mathbb{A}^d)$. The idea of the proof is to show that $\pi(V)$ is the zero set of a single element $f_0 \in k[\mathbb{A}^d]$, and to use that we already know the theorem for $\mathbb{A}^d$. □

LEMMA 7.3. *Let A be an integral domain, and let L be a finite extension of the field of fractions K of A. If $\alpha \in L$ is integral over A, then so also is $Nm_{L/K}\alpha$. Hence, if A is integrally closed (e.g., if A is a unique factorization domain), then $Nm_{L/K}\alpha \in A$. In this last case, α divides $\mathrm{Nm}_{L/K}\,\alpha$ in the ring $A[\alpha]$.*

PROOF. Let $g(X)$ be the minimum polynomial of α over K,

$$g(X) = X^r + a_{r-1}X^{r-1} + \cdots + a_0.$$

Then $\mathrm{Nm}\alpha = \pm a_0^{\frac{n}{r}} = a_0^{\frac{n}{r}}$, where $n = [L : K]$. In some extension field E of L, $g(X)$ will split

$$g(X) = \prod(X - \alpha_i), \quad \alpha_1 = \alpha, \quad \prod \alpha_i = \pm a_0.$$

Because α is integral over A, $g(X)$ has coefficients in A (see 1.33), and so each α_i is integral over A. Since the elements of E integral over A form a subring of E, it follows that $\mathrm{Nm}\,\alpha$ is integral over A.

Now suppose A is integrally closed, so that $a = \mathrm{Nm}\,\alpha \in A$. From the equation

$$0 = \alpha(\alpha^{r-1} + a_{r-1}\alpha^{r-2} + \cdots + a_1) + a_0$$

we see that α divides a_0 in $A[\alpha]$, and therefore it also divides $a = a_0^{\frac{n}{r}}$. □

PROOF. (of 7.2 continued) Let $f_0 = \mathrm{Nm}_{k(V)/k(\mathbb{A}^d)}\, f$. According to the lemma, f_0 lies in $k[\mathbb{A}^d]$, and I claim that $\mathfrak{p} \cap k[\mathbb{A}^d] = \mathrm{rad}(f_0)$. The lemma shows that f divides f_0 in $k[V]$, and so $f_0 \in (f) \subset \mathfrak{p}$. Hence $\mathrm{rad}(f_0) \subset \mathfrak{p} \cap k[\mathbb{A}^d]$. For the reverse inclusion, suppose that $g \in \mathfrak{p} \cap k[\mathbb{A}^d]$. Then $g \in \mathrm{rad}(f)$, and so $g^m = fh$ for some $h \in k[V]$, $m \in \mathbb{N}$. Taking norms, we find that $g^{me} = \mathrm{Nm}(fh) = f_0 \cdot \mathrm{Nm}(h) \in (f_0)$, where $e = [k(V) : k(\mathbb{A}^n)]$, which proves the claim.

The inclusion $k[V] \hookrightarrow k[\mathbb{A}^d]$ therefore induces an inclusion

$$k[\mathbb{A}^d]/\mathrm{rad}(f_0) = k[\mathbb{A}^d]/\mathfrak{p} \cap k[\mathbb{A}^d] \hookrightarrow k[V]/\mathfrak{p},$$

which makes $k[V]/\mathfrak{p}$ into a finite algebra over $k[\mathbb{A}^d]/\mathrm{rad}(f_0)$. Hence

$$\dim V(\mathfrak{p}) = \dim V(f_0).$$

Clearly $f \neq 0 \Rightarrow f_0 \neq 0$, and $f_0 \in \mathfrak{p} \Rightarrow f_0$ is not a nonzero constant. Therefore $\dim V(f_0) = d - 1$ by (7.1b). □

COROLLARY 7.4. *Let V be an irreducible variety, and let Z be a maximal proper closed irreducible subset of V. Then* $\dim(Z) = \dim(V) - 1$.

PROOF. For any open affine subset U of V meeting Z, $\dim U = \dim V$ and $\dim U \cap Z = \dim Z$. We may therefore assume that V itself is affine. Let f be a nonzero regular function on V vanishing on Z, and let $V(f)$ be the set of zeros of f (in V). Then $Z \subset V(f) \subset V$, and Z must be an irreducible component of $V(f)$ for otherwise it wouldn't be maximal in V. Thus we can apply the theorem to obtain that $\dim Z = \dim V - 1$. □

COROLLARY 7.5 (Topological Characterization of Dimension). *Suppose V is irreducible and that*

$$V \supsetneqq V_1 \supsetneqq \cdots \supsetneqq V_d \neq \emptyset$$

is a maximal chain of closed irreducible subsets of V. Then $\dim(V) = d$. (Maximal means that the chain can't be refined.)

PROOF. From (7.4) we know that

$$\dim V = \dim V_1 + 1 = \dim V_2 + 2 = \cdots = \dim V_d + d = d.$$

□

REMARK 7.6. (a) Recall that the Krull dimension of a ring A is the sup of the lengths of chains of prime ideals in A. It may be infinite, even when A is Noetherian (for an example of this, see Nagata, Local Rings, 1962, Appendix A.1). However a local Noetherian ring has finite Krull dimension, and so

$$\text{Krull dim } A = \sup_{\mathfrak{m} \text{ maximal}} \text{Krull dim } A_{\mathfrak{m}}.$$

In Nagata's nasty example, there is a sequence of maximal ideals $\mathfrak{m}_1$, $\mathfrak{m}_2$, $\mathfrak{m}_3$, ... in A such that the Krull dimension of $A_{\mathfrak{m}_i}$ tends to infinity.

The corollary shows that, when V is affine, $\dim V = \text{Krull dim } k[V]$, but it shows much more. Note that each V_i in a maximal chain (as above) has dimension $d - i$, and that any closed irreducible subset of V of dimension $d - i$ occurs as a V_i in a maximal chain. These facts translate into statements about ideals in affine k-algebras that do not hold for all Noetherian rings. For example, if A is an affine k-algebra that is an integral domain, then Krull dim $A_{\mathfrak{m}}$ is the same for all maximal ideals of A — all maximal ideals in A have the same height (we have proved 4.19). Moreover, if $\mathfrak{p}$ is an ideal in $k[V]$ with height i, then there is a maximal (i.e., nonrefinable) chain of prime ideals

$$(0) \subsetneqq \mathfrak{p}_1 \subsetneqq \mathfrak{p}_2 \subsetneqq \cdots \subsetneqq \mathfrak{p}_d \subsetneqq k[V]$$

with $\mathfrak{p}_i = \mathfrak{p}$.

(b) Now that we know that the two notions of dimension coincide, we can restate (7.2) as follows: let A be an affine k-algebra; let $f \in A$ be neither zero nor a unit, and let $\mathfrak{p}$ be a prime ideal that is minimal among those containing (f); then

$$\text{Krull dim } A/\mathfrak{p} = \text{Krull dim } A - 1.$$

This statement does hold for all Noetherian local rings (see Atiyah and MacDonald 1969, 11.18), and is called Krull's principal ideal theorem.

COROLLARY 7.7. *Let V be an irreducible variety, and let Z be an irreducible component of $V(f_1, \dots f_r)$, where the f_i are regular functions on V. Then codim$(Z) \leq r$.*

PROOF. As in the proof of (7.4), we can assume V to be affine. We use induction on r. Because Z is a closed irreducible subset of $V(f_1,\dots f_{r-1})$, it is contained in some irreducible component Z' of $V(f_1,\dots f_{r-1})$. By induction, $\operatorname{codim}(Z') \le r-1$. Also Z is an irreducible component of $Z' \cap V(f_r)$ because

$$Z \subset Z' \cap V(f_r) \subset V(f_1,\dots,f_r)$$

and Z is a maximal closed irreducible subset of $V(f_1,\dots,f_r)$. If f_r vanishes identically on Z', then $Z = Z'$ and $\operatorname{codim}(Z) = \operatorname{codim}(Z') \le r-1$; otherwise, the theorem shows that Z has codimension 1 in Z', and $\operatorname{codim}(Z) = \operatorname{codim}(Z') + 1 \le r$. □

PROPOSITION 7.8. *Let V and W be closed subvarieties of $\mathbb{A}^n$; for any (nonempty) irreducible component Z of $V \cap W$,*

$$\dim(Z) \ge \dim(V) + \dim(W) - n;$$

that is,

$$\operatorname{codim}(Z) \le \operatorname{codim}(V) + \operatorname{codim}(W).$$

PROOF. In the course of the proof of (3.26), we showed that $V \cap W$ is isomorphic to $\Delta \cap (V \times W)$, and this is defined by the n equations $X_i = Y_i$ in $V \times W$. Thus the statement follows from (7.7). □

REMARK 7.9. (a) The example

$$\begin{cases} X^2 + Y^2 &= Z^2 \\ Z &= 0 \end{cases}$$

shows that Proposition 7.8 becomes false if one only looks at real points. Also, that the pictures we draw can mislead.

(b) The statement of (7.8) is false if $\mathbb{A}^n$ is replaced by an arbitrary affine variety. Consider for example the affine cone V

$$X_1X_4 - X_2X_3 = 0.$$

It contains the planes,

$$Z : X_2 = 0 = X_4; \qquad Z = \{(*,0,*,0)\}$$

$$Z' : X_1 = 0 = X_3; \qquad Z' = \{(0,*,0,*)\}$$

and $Z \cap Z' = \{(0,0,0,0)\}$. Because V is a hypersurface in $\mathbb{A}^4$, it has dimension 3, and each of Z and Z' has dimension 2. Thus

$$\operatorname{codim} Z \cap Z' = 3 \nleq 1 + 1 = \operatorname{codim} Z + \operatorname{codim} Z'.$$

The proof of (7.8) fails because the diagonal in $V \times V$ cannot be defined by 3 equations (it takes the same 4 that define the diagonal in $\mathbb{A}^4$)—thus the diagonal is not a set-theoretic complete intersection.

REMARK 7.10. In (7.7), the components of $V(f_1,\dots,f_r)$ need not all have the same dimension, and it is possible for all of them to have codimension $< r$ without any of the f_i being redundant.

For example, let V be the same affine cone as in the above remark. Note that $V(X_1) \cap V$ is a union of the planes:

$$V(X_1) \cap V = \{(0,0,*,*)\} \cup \{(0,*,0,*)\}.$$

Both of these have codimension 1 in V (as required by (7.2)). Similarly, $V(X_2) \cap V$ is the union of two planes,

$$V(X_2) \cap V = \{(0,0,*,*)\} \cup \{(*,0,*,0)\},$$

but $V(X_1, X_2) \cap V$ consists of a single plane $\{(0,0,*,*)\}$: it is still of codimension 1 in V, but if we drop one of two equations from its defining set, we get a larger set.

PROPOSITION 7.11. *Let Z be a closed irreducible subvariety of codimension r in an affine variety V. Then there exist regular functions $f_1, \dots, f_r$ on V such that Z is an irreducible component of $V(f_1, \dots, f_r)$ and all irreducible components of $V(f_1, \dots, f_r)$ have codimension r.*

PROOF. We know that there exists a chain of closed irreducible subsets

$$V \supset Z_1 \supset \cdots \supset Z_r = Z$$

with codim $Z_i = i$. We shall show that there exist $f_1, \dots, f_r \in k[V]$ such that, for all $s \leq r$, Z_s is an irreducible component of $V(f_1, \dots, f_s)$ and all irreducible components of $V(f_1, \dots, f_s)$ have codimension s.

We prove this by induction on s. For $s = 1$, take any $f_1 \in I(Z_1)$, $f_1 \neq 0$, and apply Theorem 7.2. Suppose $f_1, \dots, f_{s-1}$ have been chosen, and let $Y_1 = Z_{s-1}, \dots, Y_m$, be the irreducible components of $V(f_1, \dots, f_{s-1})$. We seek an element f_s that is identically zero on Z_s but is not identically zero on any Y_i—for such an f_s, all irreducible components of $Y_i \cap V(f_s)$ will have codimension s, and Z_s will be an irreducible component of $Y_1 \cap V(f_s)$. But $Y_i \not\subseteq Z_s$ for any i (Z_s has smaller dimension than Y_i), and so $I(Z_s) \not\subseteq I(Y_i)$. Now the prime avoidance lemma (see below) tells us that there is an element $f_s \in I(Z_s)$ such that $f_s \notin I(Y_i)$ for any i, and this is the function we want. □

LEMMA 7.12 (Prime Avoidance Lemma). *If an ideal $\mathfrak{a}$ of a ring A is not contained in any of the prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$, then it is not contained in their union.*

PROOF. We may assume that none of the prime ideals is contained in a second, because then we could omit it. Fix an i_0 and, for each $i \neq i_0$, choose an $f_i \in \mathfrak{p}_i, \quad f_i \notin \mathfrak{p}_{i_0}$, and choose $f_{i_0} \in \mathfrak{a}$, $f_{i_0} \notin \mathfrak{p}_{i_0}$. Then $h_{i_0} \stackrel{\text{df}}{=} \prod f_i$ lies in each $\mathfrak{p}_i$ with $i \neq i_0$ and $\mathfrak{a}$, but not in $\mathfrak{p}_{i_0}$ (here we use that $\mathfrak{p}_{i_0}$ is prime). The element $\sum h_i$ is therefore in $\mathfrak{a}$ but not in any $\mathfrak{p}_i$. □

REMARK 7.13. The proposition shows that for a prime ideal $\mathfrak{p}$ in an affine k-algebra, if $\mathfrak{p}$ has height r, then there exist elements $f_1, \dots, f_r \in A$ such that $\mathfrak{p}$ is minimal among the prime ideals containing $(f_1, \dots, f_r)$. This statement is true for all Noetherian local rings.

REMARK 7.14. The last proposition shows that a curve C in $\mathbb{A}^3$ is an irreducible component of $V(f_1, f_2)$ for some $f_1,\ f_2 \in k[X, Y, Z]$. In fact $C = V(f_1, f_2, f_3)$ for suitable polynomials f_1, f_2, and f_3 — this is an exercise in Shafarevich 1994 (I.6, Exercise 8); see also Hartshorne 1977, I, Exercise 2.17. Apparently, it is not known whether two polynomials always suffice to define a curve in $\mathbb{A}^3$ — see Kunz 1985, p136. The union of two skew lines in $\mathbb{P}^3$ can't be defined by two polynomials (ibid. p140), but it is unknown whether all connected curves in $\mathbb{P}^3$ can be defined by two polynomials. Macaulay (the man, not the program) showed that for every $r \geq 1$,

there is a curve C in $\mathbb{A}^3$ such that $I(C)$ requires at least r generators (see the same exercise in Hartshorne for a curve whose ideal can't be generated by 2 elements).

In general, a closed variety V of codimension r in $\mathbb{A}^n$ (resp. $\mathbb{P}^n$) is said to be a *set-theoretic complete intersection* if there exist r polynomials $f_i \in k[X_1, \dots, X_n]$ (resp. homogeneous polynomials $f_i \in k[X_0, \dots, X_n]$) such that

$$V = V(f_1, \dots, f_r).$$

Such a variety is said to be an *ideal-theoretic complete intersection* if the f_i can be chosen so that $I(V) = (f_1, \dots, f_r)$. Chapter V of Kunz's book is concerned with the question of when a variety is a complete intersection. Obviously there are many ideal-theoretic complete intersections, but most of the varieties one happens to be interested in turn out not to be. For example, no abelian variety of dimension > 1 is an ideal-theoretic complete intersection (being an ideal-theoretic complete intersection imposes constraints on the cohomology of the variety, which are not fulfilled in the case of abelian varieties).

Let P be a point on an irreducible variety $V \subset \mathbb{A}^n$. Then (7.11) shows that there is a neighbourhood U of P in $\mathbb{A}^n$ and functions $f_1, \dots, f_r$ on U such that $U \cap V = V(f_1, \dots, f_r)$ (zero set in U). Thus $U \cap V$ is a set-theoretic complete intersection in U. One says that V is a *local complete intersection* at $P \in V$ if there is an open affine neighbourhood U of P in $\mathbb{A}^n$ such that $I(V \cap U)$ can be generated by r regular functions on U. Note that

$$\text{ideal-theoretic complete intersection} \Rightarrow \text{local complete intersection at all } \mathfrak{p}.$$

It is not difficult to show that a variety is a local complete intersection at every nonsingular point.

PROPOSITION 7.15. *Let Z be a closed subvariety of codimension r in variety V, and let P be a point of Z that is nonsingular when regarded both as a point on Z and as a point on V. Then there is an open affine neighbourhood U of P and regular functions $f_1, \dots, f_r$ on U such that $Z \cap U = V(f_1, \dots, f_r)$.*

PROOF. By assumption

$$\dim_k T_P(Z) = \dim Z = \dim V - r = \dim_k T_P(V) - r.$$

There exist functions $f_1, \dots, f_r$ contained in the ideal of $\mathcal{O}_P$ corresponding to Z such that $T_P(Z)$ is the subspace of $T_P(V)$ defined by the equations

$$(df_1)_P = 0, \dots, (df_r)_P = 0.$$

All the f_i will be defined on some open affine neighbourhood U of P (in V), and clearly Z is the only component of $Z' \stackrel{\text{df}}{=} V(f_1, \dots, f_r)$ (zero set in U) passing through P. After replacing U by a smaller neighbourhood, we can assume that Z' is irreducible. As $f_1, \dots, f_r \in I(Z')$, we must have $T_P(Z') \subset T_P(Z)$, and therefore $\dim Z' \leq \dim Z$. But $I(Z') \subset I(Z \cap U)$, and so $Z' \supset Z \cap U$. These two facts imply that $Z' = Z \cap U$. □

PROPOSITION 7.16. *Let V be an affine variety such that $k[V]$ is a unique factorization domain. Then every pure closed subvariety Z of V of codimension one is principal, i.e., $I(Z) = (f)$ for some $f \in k[V]$.*

PROOF. In (4.25) we proved this in the case that $V = \mathbb{A}^n$, but the argument only used that $k[\mathbb{A}^n]$ is a unique factorization domain. □

EXAMPLE 7.17. The condition that $k[V]$ is a unique factorization domain is definitely needed. Again let V be the cone

$$X_1X_4 - X_2X_3 = 0$$

in $\mathbb{A}^4$ and let Z and Z' be the planes

$$Z = \{(*, 0, *, 0)\} \qquad Z' = \{(0, *, 0, *)\}.$$

Then $Z \cap Z' = \{(0,0,0,0)\}$, which has codimension 2 in Z'. If $Z = V(f)$ for some regular function f on V, then $V(f|Z') = \{(0, \dots, 0)\}$, which is impossible (because it has codimension 2, which violates 7.2). Thus Z is not principal, and so

$$k[X_1, X_2, X_3, X_4]/(X_1X_4 - X_2X_3)$$

is not a unique factorization domain.

Projective varieties. The results for affine varieties extend to projective varieties with one important simplification: if V and W are projective varieties of dimensions r and s in $\mathbb{P}^n$ and $r + s \geq n$, then $V \cap W \neq \emptyset$.

THEOREM 7.18. *Let $V = V(\mathfrak{a}) \subset \mathbb{P}^n$ be a projective variety of dimension ≥ 1, and let $f \in k[X_0, \dots, X_n]$ be homogeneous, nonconstant, and $\notin \mathfrak{a}$; then $V \cap V(f)$ is nonempty and of pure codimension* 1.

PROOF. Since the dimension of a variety is equal to the dimension of any dense open affine subset, the only part that doesn't follow immediately from (7.2) is the fact that $V \cap V(f)$ is nonempty. Let $V^{aff}(\mathfrak{a})$ be the zero set of $\mathfrak{a}$ in $\mathbb{A}^{n+1}$ (that is, the affine cone over V). Then $V^{aff}(\mathfrak{a}) \cap V^{aff}(f)$ is nonempty (it contains $(0, \dots, 0)$), and so it has codimension 1 in $V^{aff}(\mathfrak{a})$. Clearly $V^{aff}(\mathfrak{a})$ has dimension ≥ 2, and so $V^{aff}(\mathfrak{a}) \cap V^{aff}(f)$ has dimension ≥ 1. This implies that the polynomials in $\mathfrak{a}$ have a zero in common with f other than the origin, and so $V(\mathfrak{a}) \cap V(f) \neq \emptyset$. □

COROLLARY 7.19. *Let $f_1, \cdots, f_r$ be homogeneous nonconstant elements of $k[X_0, \dots, X_n]$; and let Z be an irreducible component of $V \cap V(f_1, \dots f_r)$. Then codim$(Z) \leq r$, and if* $\dim(V) \geq r$, *then $V \cap V(f_1, \dots f_r)$ is nonempty.*

PROOF. Induction on r, as before. □

COROLLARY 7.20. *Let $\alpha\colon \mathbb{P}^n \to \mathbb{P}^m$ be regular; if $m < n$, then α is constant.*

PROOF. Let $\pi\colon \mathbb{A}^{n+1} - \{\text{origin}\} \to \mathbb{P}^n$ be the map $(a_0, \dots, a_n) \mapsto (a_0 : \dots : a_n)$. Then $\alpha \circ \pi$ is regular, and there exist polynomials $F_0, \dots, F_m \in k[X_0, \dots, X_n]$ such that $\alpha \circ \pi$ is the map

$$(a_0, \dots, a_n) \mapsto (F_0(a) : \dots : F_m(a)).$$

As $\alpha \circ \pi$ factors through $\mathbb{P}^n$, the F_i must be homogeneous of the same degree. Note that

$$\alpha(a_0 : \dots : a_n) = (F_0(a) : \dots : F_m(a)).$$

If $m < n$ and the F_i are nonconstant, then (7.18) shows they have a common zero and so α is not defined on all of $\mathbb{P}^n$. Hence the F_i's must be constant. □

PROPOSITION 7.21. *Let Z be a closed irreducible subvariety of V; if $\operatorname{codim}(Z) = r$, then there exist homogeneous polynomials $f_1, \dots, f_r$ in $k[X_0, \dots, X_n]$ such that Z is an irreducible component of $V \cap V(f_1, \dots, f_r)$.*

PROOF. Use the same argument as in the proof (7.11). □

PROPOSITION 7.22. *Every pure closed subvariety Z of $\mathbb{P}^n$ of codimension one is principal, i.e., $I(Z) = (f)$ for some f homogeneous element of $k[X_0, \dots, X_n]$.*

PROOF. Follows from the affine case. □

COROLLARY 7.23. *Let V and W be closed subvarieties of $\mathbb{P}^n$; if $\dim(V) + \dim(W) \geq n$, then $V \cap W \neq \emptyset$, and every irreducible component of it has $\operatorname{codim}(Z) \leq \operatorname{codim}(V) + \operatorname{codim}(W)$.*

PROOF. Write $V = V(\mathfrak{a})$ and $W = V(\mathfrak{b})$, and consider the affine cones $V' = V(\mathfrak{a})$ and $W' = W(\mathfrak{b})$ over them. Then

$$\dim(V') + \dim(W') = \dim(V) + 1 + \dim(W) + 1 \geq n + 2.$$

As $V' \cap W' \neq \emptyset$, $V' \cap W'$ has dimension ≥ 1, and so it contains a point other than the origin. Therefore $V \cap W \neq \emptyset$. The rest of the statement follows from the affine case. □

PROPOSITION 7.24. *Let V be a closed subvariety of $\mathbb{P}^n$ of dimension $r < n$; then there is a linear projective variety E of dimension $n - r - 1$ (that is, E is defined by $r + 1$ independent linear forms) such that $E \cap V = \emptyset$.*

PROOF. Induction on r. If $r = 0$, then V is a finite set, and the next lemma shows that there is a hyperplane in k^{n+1} not meeting V. □

LEMMA 7.25. *Let W be a vector space of dimension d over an infinite field k, and let $E_1, \dots, E_r$ be a finite set of nonzero subspaces of W. Then there is a hyperplane H in W containing none of the E_i.*

PROOF. Pass to the dual space V of W. The problem becomes that of showing V is not a finite union of proper subspaces $E_i^\vee$. Replace each $E_i^\vee$ by a hyperplane H_i containing it. Then H_i is defined by a nonzero linear form L_i. We have to show that $\prod L_j$ is not identically zero on V. But this follows from the statement that a polynomial in n variables, with coefficients not all zero, can not be identically zero on k^n. (See the first homework exercise.)

Suppose $r > 0$, and let $V_1, \dots, V_s$ be the irreducible components of V. By assumption, they all have dimension $\leq r$. The intersection E_i of all the linear projective varieties containing V_i is the smallest such variety. The lemma shows that there is a hyperplane H containing none of the nonzero E_i; consequently, H contains none of the irreducible components V_i of V, and so each $V_i \cap H$ is a pure variety of dimension $\leq r - 1$ (or is empty). By induction, there is an linear subvariety E' not meeting $V \cap H$. Take $E = E' \cap H$. □

Let V and E be as in the theorem. If E is defined by the linear forms $L_0, \dots, L_r$ then the projection $a \mapsto (L_0(a) : \cdots : L_r(a))$ defines a map $V \to \mathbb{P}^r$. We shall see later that this map is finite, and so it can be regarded as a projective version of the Noether normalization theorem.

8. Regular Maps and Their Fibres.

Throughout this section, k is an algebraically closed field. Consider again the regular map $\varphi\colon \mathbb{A}^2 \to \mathbb{A}^2$, $(x, y) \mapsto (x, xy)$. We have seen that its image

$$C = (\mathbb{A}^2 \smallsetminus \{y\text{-axis}\}) \cup \{(0,0)\}$$

is neither open nor closed, and, in fact, is not even locally closed. The fibre

$$\varphi^{-1}(x, y) = (\mathbb{A}^2 \smallsetminus \{y\text{-axis}\}) \cup \{(0,0)\}.$$

From this unpromising example, it would appear that it is not possible to say anything about the image of a regular map, nor about the dimension or number of elements in its fibres. However, it turns out that (almost) everything that can go wrong already goes wrong for this map. We shall show:

(a) the image of a regular map is a finite union of locally closed sets;
(b) the dimensions of the fibres can jump only on closed subsets;
(c) the number of elements (if finite) in the fibres can drop only on closed subsets, provided the map is finite, the target variety is normal, and k has characteristic zero.

Constructible sets. Let W be a topological space. A subset C of W is said to *constructible* if it is a finite union of sets of the form $U \cap Z$ with U open and Z closed. Obviously, if C is constructible and $V \subset W$, then $C \cap V$ is constructible. A constructible set in $\mathbb{A}^n$ is definable by a finite number of polynomials; more precisely, it is defined by a finite number of statements of the form

$$f(X_1, \cdots, X_n) = 0, \qquad g(X_1, \cdots, X_n) \neq 0$$

combined using only "and" and "or" (or, better, statements of the form $f = 0$ combined using "and", "or", and "not"). The next proposition shows that a constructible set C that is dense in an irreducible variety V must contain a nonempty open subset of V. Contrast $\mathbb{Q}$, which is dense in $\mathbb{R}$ (real topology), but does not contain an open subset of $\mathbb{R}$, or any infinite subset of $\mathbb{A}^1$ that omits an infinite set.

Proposition 8.1. *Let C be a constructible set whose closure $\bar{C}$ is irreducible. Then C contains a nonempty open subset of $\bar{C}$.*

Proof. We are given that $C = \cup(U_i \cap Z_i)$ with each U_i open and each Z_i closed. We may assume that each set $U_i \cap Z_i$ in this decomposition is nonempty. Clearly $\bar{C} \subset \cup Z_i$, and as $\bar{C}$ is irreducible, it must be contained in one of the Z_i. For this i

$$C \supset U_i \cap Z_i \supset U_i \cap \bar{C} \supset U_i \cap C \supset U_i \cap (U_i \cap Z_i) = U_i \cap Z_i.$$

Thus $U_i \cap Z_i = U_i \cap \bar{C}$ is a nonempty open subset of $\bar{C}$ contained in C. □

Theorem 8.2. *A regular map $\varphi\colon W \to V$ sends constructible sets to constructible sets. In particular, if U is a nonempty open subset of W, then $\varphi(U)$ contains a nonempty open subset of its closure in V.*

The key result we shall need from commutative algebra is the following. (In the next two results, A and B are arbitrary commutative rings—they need not be k-algebras.)

PROPOSITION 8.3. *Let $A \subset B$ be integral domains with B finitely generated as an algebra over A, and let b be a nonzero element of B. Then there exists an element $a \neq 0$ in A with the following property: every homomorphism $\alpha\colon A \to \Omega$ from A into an algebraically closed field Ω such that $\alpha(a) \neq 0$ can be extended to a homomorphism $\beta\colon B \to \Omega$ such that $\beta(b) \neq 0$.*

Consider, for example, the rings $k[X] \subset k[X, X^{-1}]$. A homomorphism $\alpha\colon k[X] \to k$ extends to a homomorphism $k[X, X^{-1}] \to k$ if and only if $\alpha(X) \neq 0$. Therefore, for $b = 1$, we can take $a = X$. In the application we make of Proposition 8.3, we only really need the case $b = 1$, but the more general statement is needed so that we can prove it by induction.

LEMMA 8.4. *Let $B \supset A$ be integral domains, and assume $B = A[t] \approx A[T]/\mathfrak{a}$. Let $\mathfrak{c} \subset A$ be the set of leading coefficients of the polynomials in $\mathfrak{a}$. Then every homomorphism $\alpha\colon A \to \Omega$ from A into an algebraically closed field Ω such that $\alpha(\mathfrak{c}) \neq 0$ can be extended to a homomorphism of B into Ω.*

PROOF. Note that $\mathfrak{c}$ is an ideal in A. If $\mathfrak{a} = 0$, then $\mathfrak{c} = 0$, and there is nothing to prove (in fact, every α extends). Thus we may assume $\mathfrak{a} \neq 0$. Let $f = a_m T^m + \cdots + a_0$ be a nonzero polynomial of minimum degree in $\mathfrak{a}$ such that $\alpha(a_m) \neq 0$. Because $B \neq 0$, we have that $m \geq 1$.

Extend α to a homomorphism $\tilde{\alpha}\colon A[T] \to \Omega[T]$ by sending T to T. The Ω-submodule of $\Omega[T]$ generated by $\tilde{\alpha}(\mathfrak{a})$ is an ideal (because $T \cdot \sum c_i \tilde{\alpha}(g_i) = \sum c_i \tilde{\alpha}(g_i T)$). Therefore, unless $\tilde{\alpha}(\mathfrak{a})$ contains a nonzero constant, it generates a proper ideal in $\Omega[T]$, which will have a zero c in Ω. The homomorphism

$$A[T] \xrightarrow{\tilde{\alpha}} \Omega[T] \to \Omega, \qquad T \mapsto T \mapsto c$$

then factors through $A[T]/\mathfrak{a} = B$ and extends α.

In the contrary case, $\mathfrak{a}$ contains a polynomial

$$g(T) = b_n T^n + \cdots + b_0, \quad \alpha(b_i) = 0 \quad (i > 0), \quad \alpha(b_0) \neq 0.$$

On dividing $f(T)$ into $g(T)$ we find that

$$a_m^d g(T) = q(T) f(T) + r(T), \quad d \in \mathbb{N}, \quad q, r \in A[T], \quad \deg r < m.$$

On applying $\tilde{\alpha}$ to this equation, we obtain

$$\alpha(a_m)^d \alpha(b_0) = \tilde{\alpha}(q)\tilde{\alpha}(f) + \tilde{\alpha}(r).$$

Because $\tilde{\alpha}(f)$ has degree $m > 0$, we must have $\tilde{\alpha}(q) = 0$, and so $\tilde{\alpha}(r)$ is a nonzero constant. After replacing $g(T)$ with $r(T)$, we may assume $n < m$. If $m = 1$, such a $g(T)$ can't exist, and so we may suppose $m > 1$ and (by induction) that the lemma holds for smaller values of m.

For $h(T) = c_r T^r + c_{r-1} T^{r-1} + \cdots + c_0$, let $h'(T) = c_r + \cdots + c_0 T^r$. Then the A-module generated by the polynomials $T^s h'(T)$, $s \geq 0$, $h \in \mathfrak{a}$, is an ideal $\mathfrak{a}'$ in $A[T]$. Moreover, $\mathfrak{a}'$ contains a nonzero constant if and only if $\mathfrak{a}$ contains a nonzero polynomial cT^r, which implies $t = 0$ and $A = B$ (since B is an integral domain).

If $\mathfrak{a}'$ does not contain nonzero constants, then set $B' = A[T]/\mathfrak{a}' = A[t']$. Then $\mathfrak{a}'$ contains the polynomial $g' = b_n + \cdots + b_0 T^n$, and $\alpha(b_0) \neq 0$. Because $\deg g' < m$, the

induction hypothesis implies that α extends to a homomorphism $B' \to \Omega$. Therefore, there is a $c \in \Omega$ such that, for all $h(T) = c_rT^r + c_{r-1}T^{r-1} + \cdots + c_0 \in \mathfrak{a}$,

$$h'(c) = \alpha(c_r) + \alpha(c_{r-1})c + \cdots + c_0c^r = 0.$$

On taking $h = g$, we see that $c = 0$, and on taking $h = f$, we obtain the contradiction $\alpha(a_m) = 0$. □

PROOF. (of 8.3) Suppose that we know the proposition in the case that B is generated by a single element, and write $B = A[x_1, \dots, x_n]$. Then there exists an element b_{n-1} such that any homomorphism $\alpha\colon A[x_1, \dots, x_{n-1}] \to \Omega$ such that $\alpha(b_{n-1}) \neq 0$ extends to a homomorphism $\beta\colon B \to \Omega$ such that $\beta(b) \neq 0$. Continuing in this fashion, we obtain an element $a \in A$ with the required property.

Thus we may assume $B = A[x]$. Let $\mathfrak{a}$ be the kernel of the homomorphism $X \mapsto x$, $A[X] \to A[x]$.

Case (i). The ideal $\mathfrak{a} = (0)$. Write

$$b = f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n, \quad a_i \in A,$$

and take $a = a_0$. If $\alpha\colon A \to \Omega$ is such that $\alpha(a_0) \neq 0$, then there exists a $c \in \Omega$ such that $f(c) \neq 0$, and we can take β to be the homomorphism $\sum d_ix^i \mapsto \sum \alpha(d_i)c^i$.

Case (ii). The ideal $\mathfrak{a} \neq (0)$. Let $f(T) = a_mT^m + \cdots$, $a_m \neq 0$, be an element of $\mathfrak{a}$ of minimum degree. Let $h(T) \in A[T]$ represent b. Since $b \neq 0$, $h \notin \mathfrak{a}$. Because f is irreducible over the field of fractions of A, it and h are coprime over that field. Hence there exist $u, v \in A[T]$ and $c \in A - \{0\}$ such that

$$uh + vf = c.$$

It follows now that ca_m satisfies our requirements, for if $\alpha(ca_m) \neq 0$, then α can be extended to $\beta\colon B \to \Omega$ by the previous lemma, and $\beta(u(x) \cdot b) = \beta(c) \neq 0$, and so $\beta(b) \neq 0$. □

ASIDE 8.5. In case (ii) of the above proof, both b and b^{-1} are algebraic over A, and so there exist equations

$$a_0b^m + \cdots + a_m = 0, \quad a_i \in A, \quad a_0 \neq 0;$$

$$a_0'b^{-n} + \cdots + a_n' = 0, \quad a_i' \in A, \quad a_0' \neq 0.$$

One can show that $a = a_0a_0'$ has the property required by the Proposition—see Atiyah and MacDonald, 5.23.

PROOF. (of 8.2) We first prove the "in particular" statement of the Theorem. By considering suitable open affine coverings of W and V, one sees that it suffices to prove this in the case that both W and V are affine. If $W_1, \dots, W_r$ are the irreducible components of W, then the closure of $\varphi(W)$ in V, $\varphi(W)^- = \varphi(W_1)^- \cup \ldots \cup \varphi(W_r)^-$, and so it suffices to prove the statement in the case that W is irreducible. We may also replace V with $\varphi(W)^-$, and so assume that both W and V are irreducible. Then φ corresponds to an injective homomorphism $A \to B$ of affine k-algebras. For some $b \neq 0$, $D(b) \subset U$. Choose a as in the lemma. Then for any point $P \in D(a)$, the homomorphism $f \mapsto f(P)\colon A \to k$ extends to a homomorphism $\beta\colon B \to k$ such that $\beta(b) \neq 0$. The kernel of β is a maximal ideal corresponding to a point $Q \in D(b)$ lying over P.

We now prove the theorem. Let W_i be the irreducible components of W. Then $C \cap W_i$ is constructible in W_i, and $\varphi(W)$ is the union of the $\varphi(C \cap W_i)$; it is therefore constructible if the $\varphi(C \cap W_i)$ are. Hence we may assume that W is irreducible. Moreover, C is a finite union of its irreducible components, and these are closed in C; they are therefore constructible. We may therefore assume that C also is irreducible; $\bar{C}$ is then an irreducible closed subvariety of W.

We shall prove the theorem by induction on the dimension of W. If $\dim(W) = 0$, then the statement is obvious because W is a point. If $\bar{C} \neq W$, then $\dim(\bar{C}) < \dim(W)$, and because C is constructible in $\bar{C}$, we see that $\varphi(C)$ is constructible (by induction). We may therefore assume that $\bar{C} = W$. But then $\bar{C}$ contains a nonempty open subset of W, and so the case just proved shows that $\varphi(C)$ contains an nonempty open subset U of its closure. Replace V be the closure of $\varphi(C)$, and write

$$\varphi(C) = U \cup \varphi(C \cap \varphi^{-1}(V - U)).$$

Then $\varphi^{-1}(V - U)$ is a proper closed subset of W (the complement of $V - U$ is dense in V and φ is dominating). As $C \cap \varphi^{-1}(V - U)$ is constructible in $\varphi^{-1}(V - U)$, the set $\varphi(C \cap \varphi^{-1}(V - U))$ is constructible in V by induction, which completes the proof. □

The fibres of morphisms. We wish to examine the fibres of a regular map $\varphi\colon W \to V$. Clearly, we can replace V by the closure of $\varphi(W)$ in V and so assume φ to be dominating.

THEOREM 8.6. *Let $\varphi\colon W \to V$ be a dominating regular map of irreducible varieties. Then*

(a) $\dim(W) \geq \dim(V)$*;*
(b) *if $P \in \varphi(W)$, then*

$$\dim(\varphi^{-1}(P)) \geq \dim(W) - \dim(V)$$

for every $P \in V$, with equality holding exactly on a nonempty open subset U of V.
(c) *The sets*

$$V_i = \{P \in V \mid \dim(\varphi^{-1}(P)) \geq i\}$$

are closed $\varphi(W)$.

EXAMPLE 8.7. Consider the subvariety $W \subset V \times \mathbb{A}^m$ defined by r linear equations

$$\sum_{j=1}^{m} a_{ij} X_j = 0, \quad a_{ij} \in k[V], \quad i = 1, \dots, r,$$

and let φ be the projection $W \to V$. For $P \in V$, $\varphi^{-1}(P)$ is the set of solutions of

$$\sum_{j=1}^{m} a_{ij}(P) X_j = 0, \quad a_{ij}(P) \in k, \quad i = 1, \dots, r,$$

and so its dimension is $m - \operatorname{rank}(a_{ij}(P))$. Since the rank of the matrix $(a_{ij}(P))$ drops on closed subsets, the dimension of the fibre jumps on closed subsets.

PROOF. (a) Because the map is dominating, there is a homomorphism $k(V) \hookrightarrow k(W)$, and obviously $\operatorname{tr deg}_k k(V) \leq \operatorname{tr deg}_k k(W)$ (an algebraically independent subset of $k(V)$ remains algebraically independent in $k(W)$).

(b) In proving the first part of (b), we may replace V by any open neighbourhood of P. In particular, we can assume V to be affine. Let m be the dimension of V. From (7.11) we know that there exist regular functions $f_1, \dots, f_m$ such that P is an irreducible component of $V(f_1, \dots, f_m)$. After replacing V by a smaller neighbourhood of P, we can suppose that $P = V(f_1, \dots, f_m)$. Then $\varphi^{-1}(P)$ is the zero set of the regular functions $f_1 \circ \varphi, \dots, f_m \circ \varphi$, and so (if nonempty) has codimension $\leq m$ in W (see 7.7). Hence

$$\dim \varphi^{-1}(P) \geq \dim W - m = \dim(W) - \dim(V).$$

In proving the second part of (b), we can replace both W and V with open affine subsets. Since φ is dominating, $k[V] \to k[W]$ is injective, and we may regard it as an inclusion (we identify a function x on V with $x \circ \varphi$ on W). Then $k(V) \subset k(W)$. Write $k[V] = k[x_1, \dots, x_M]$ and $k[W] = k[y_1, \dots, y_N]$, and suppose V and W have dimensions m and n respectively. Then $k(W)$ has transcendence degree $n-m$ over $k(V)$, and we may suppose that $y_1, \dots, y_{n-m}$ are algebraically independent over $k[x_1, \dots, x_m]$, and that the remaining y_i are algebraic over $k[x_1, \dots, x_m, y_1, \dots, y_{n-m}]$. There are therefore relations

$$F_i(x_1, \dots, x_m, y_1, \dots, y_{n-m}, y_i) = 0, \quad i = n - m + 1, \dots, N. \qquad (*)$$

with $F_i(X_1, \dots, X_m, Y_1, \dots, Y_{n-m}, Y_i)$ a nonzero polynomial. We write $\bar{y}_i$ for the restriction of y_i to $\varphi^{-1}(P)$. Then

$$k[\varphi^{-1}(P)] = k[\bar{y}_1, \dots, \bar{y}_N].$$

The equations (*) give an algebraic relation among the functions $x_1, \dots, y_i$ on W. When we restrict them to $\varphi^{-1}(P)$, they become equations:

$$F_i(x_1(P), \dots, x_m(P), \bar{y}_1, \dots, \bar{y}_{n-m}, \bar{y}_i) = 0, \quad i = n - m + 1, \dots, N. \qquad (**).$$

If these are nontrivial algebraic relations, i.e., if none of the polynomials

$$F_i(x_1(P), \dots, x_m(P), Y_1, \dots, Y_{n-m}, Y_i)$$

is identically zero, then the transcendence degree of $k(\bar{y}_1, \dots, \bar{y}_N)$ over k will be $\leq n - m$.

Thus, regard $F_i(x_1, \dots, x_m, Y_1, \dots, Y_{n-m}, Y_i)$ as a polynomial in the Y's with coefficients polynomials in the x's. Let V_i be the closed subvariety of V defined by the simultaneous vanishing of the coefficients of this polynomial—it is a proper closed subset of V. Let $U = V - \cup V_i$—it is a nonempty open subset of V. If $P \in U$, then none of the polynomials $F_i(x_1(P), \dots, x_m(P), Y_1, \dots, Y_{n-m}, Y_i)$ is identically zero, and so for $P \in U$, the dimension of $\varphi^{-1}(P)$ is $\leq n - m$, and hence $= n - m$ by (a).

Finally, if for a particular point P, $\dim \varphi^{-1}(P) = n - m$, then one can modify the above argument to show that the same is true for all points in an open neighbourhood of P.

(c) We prove this by induction on the dimension of V—it is obviously true if $\dim V = 0$. We know from (b) that there is an open subset U of V such that

$$\dim \varphi^{-1}(P) = n - m \iff P \in U.$$

Let Z be the complement of U in V; thus $Z = V_{n-m+1}$. Let $Z_1, \dots, Z_r$ be the irreducible components of Z. On applying the induction to the restriction of φ to the map $\varphi^{-1}(Z_j) \to Z_j$ for each j, we obtain the result. □

PROPOSITION 8.8. *Let $\varphi\colon W \to V$ be a regular surjective closed mapping of varieties (e.g., W complete or φ finite). If V is irreducible and all the fibres $\varphi^{-1}(P)$ are irreducible of dimension n, then W is irreducible of dimension* $\dim(V) + n$.

PROOF. Let Z be a closed irreducible subset of W, and consider the map $\varphi|Z\colon Z \to V$; it has fibres $(\varphi|Z)^{-1}(P) = \varphi^{-1}(P) \cap Z$. There are three possibilities.

(a) $\varphi(Z) \neq V$. Then $\varphi(Z)$ is a proper closed subset of V.
(b) $\varphi(Z) = V$, $\dim(Z) < n + \dim(V)$. Then (b) of (8.6) shows that there is a nonempty open subset U of V such that for $P \in U$,
$$\dim(\varphi^{-1}(P) \cap Z) = \dim(Z) - \dim(V) < n;$$
thus for $P \in U$, $\varphi^{-1}(P) \not\subseteq Z$.
(c) $\varphi(Z) = V$, $\dim(Z) \geq n + \dim(V)$. Then (b) of (8.6) shows that
$$\dim(\varphi^{-1}(P) \cap Z) \geq \dim(Z) - \dim(V) \geq n$$
for all P; thus $\varphi^{-1}(P) \subset Z$ for all $P \in V$, and so $Z = W$; moreover $\dim Z = n$.

Now let $Z_1, \dots, Z_r$ be the irreducible components of W. I claim that (iii) holds for at least one of the Z_i. Otherwise, there will be an open subset U of V such that for P in U, $\varphi^{-1}(P) \not\subseteq Z_i$ for any i, but $\varphi^{-1}(P)$ is irreducible and $\varphi^{-1}(P) = \cup(\varphi^{-1}(P) \cup Z_i)$, and so this is impossible. □

The fibres of finite maps. Let $\varphi\colon W \to V$ be a finite dominating morphism of irreducible varieties. Then $\dim(W) = \dim(V)$, and so $k(W)$ is a finite field extension of $k(V)$. Its degree is called the *degree* of the map φ.

LEMMA 8.9. *An integral domain A is integrally closed if and only if $A_{\mathfrak{m}}$ is integrally closed for all maximal ideals $\mathfrak{m}$ of A.*

PROOF. $\Rightarrow$: If A is integrally closed, then so is $S^{-1}A$ for any multiplicative subset S (not containing 0), because if

$$b^n + c_1 b^{n-1} + \cdots + c_n = 0, \quad c_i \in S^{-1}A,$$

then there is an $s \in S$ such that $sc_i \in A$ for all i, and then

$$(sb)^n + (sc_1)(sb)^{n-1} + \cdots + s^n c_n = 0,$$

demonstrates that $sb \in A$, whence $b \in S^{-1}A$.

$\Leftarrow$: If c is integral over A, it is integral over each $A_{\mathfrak{m}}$, hence in each $A_{\mathfrak{m}}$, and $A = \cap A_{\mathfrak{m}}$ (if $c \in \cap A_{\mathfrak{m}}$, then the set of $a \in A$ such that $ac \in A$ is an ideal in A, not contained in any maximal ideal, and therefore equal to A itself). □

Thus the following conditions on an irreducible variety V are equivalent:

(a) for all $P \in V$, $\mathcal{O}_P$ is integrally closed;

(b) for all irreducible open affines U of V, $k[U]$ is integrally closed;
(c) there is a covering $V = \cup V_i$ of V by open affines such that $k[V_i]$ is integrally closed for all i.

An irreducible variety V satisfying these conditions is said to be *normal*. We also call a disjoint union of such varieties normal. Thus a variety V is normal if and only if $\mathcal{O}_P$ is an integrally closed integral domain for all $P \in V$.

THEOREM 8.10. *Let $\varphi\colon W \to V$ be a finite surjective regular map of irreducible varieties, and assume that V is normal.*

(a) *For all $P \in V$, $\#\varphi^{-1}(P) \leq \deg(\varphi)$.*
(b) *The set of points P of V such that $\#\varphi^{-1}(P) = \deg(\varphi)$ is an open subset of V, and it is nonempty if $k(W)$ is separable over $k(V)$.*

Before proving the theorem, we give examples to show that we need W to be separated and V to be normal in (a), and that we need $k(W)$ to be separable over $k(V)$ for the second part of (b).

EXAMPLE 8.11. (a) Consider the map

$$\{\mathbb{A}^1 \text{ with origin doubled }\} \to \mathbb{A}^1.$$

The degree is one and that map is one-to-one except at the origin where it is two-to-one.

(b) Let C be the curve $Y^2 = X^3 + X^2$, and let $\varphi\colon \mathbb{A}^1 \to C$ be the map $t \mapsto (t^2 - 1, t(t^2 - 1))$. The map corresponds to the inclusion $k[x, y] \hookrightarrow k[T]$ and is of degree one. The map is one-to-one except that the points $t = \pm 1$ both map to 0. The ring $k[x, y]$ is not integrally closed; in fact $k[T]$ is its integral closure in its field of fractions.

(c) Consider the Frobenius map $\varphi\colon \mathbb{A}^n \to \mathbb{A}^n$, $(a_1, \dots, a_n) \mapsto (a_1^p, \dots, a_n^p)$, where $p = \mathrm{char}k$. This map has degree p^n but it is one-to-one. The field extension corresponding to the map is

$$k(X_1, \dots, X_n) \supset k(X_1^p, \dots, X_n^p)$$

which is purely inseparable.

LEMMA 8.12. *Let $Q_1, \dots, Q_r$ be distinct points on an affine variety V. Then there is a regular function f on V taking distinct values at the Q_i.*

PROOF. We can embed V as closed subvariety of $\mathbb{A}^n$, and then it suffices to prove the statement with $V = \mathbb{A}^n$ — almost any linear form will do. □

PROOF. (of Theorem 8.10). In proving (a) of the theorem, we may assume that V and W are affine, and so the map corresponds to a finite map of k-algebras, $k[V] \to k[W]$. Let $\varphi^{-1}(P) = \{Q_1, \dots, Q_r\}$. According to the lemma, there exists an $f \in k[W]$ taking distinct values at the Q_i. Let

$$F(T) = T^m + a_1 T^{m-1} + \cdots + a_m$$

be the minimum polynomial of f over $k(V)$. It has degree $m \leq [k(W) : k(V)] = \deg \varphi$, and it has coefficients in $k[V]$ because V is normal (see 1.33). Now $F(f) = 0$ implies

$F(f(Q_i)) = 0$, i.e.,

$$f(Q_i)^m + a_1(P) \cdot f(Q_i)^{m-1} + \cdots + a_m(P) = 0.$$

Therefore the $f(Q_i)$ are all roots of a single polynomial of degree m, and so $r \le m \le \deg(\varphi)$.

In order to prove the first part of (b), we show that, if there is a point $P \in V$ such that $\varphi^{-1}(P)$ has $\deg(\varphi)$ elements, then the same is true for all points in an open neighbourhood of P. Choose f as in the last paragraph corresponding to such a P. Then the polynomial

$$T^m + a_1(P) \cdot T^{m-1} + \cdots + a_m(P) = 0 \qquad (*)$$

has $r = \deg \varphi$ distinct roots, and so $m = r$. Consider the discriminant $\operatorname{disc} F$ of F. Because (*) has distinct roots, $\operatorname{disc}(F)(P) \neq 0$, and so $\operatorname{disc}(F)$ is nonzero on an open neighbourhood U of P. The factorization

$$k[V] \to k[V][T]/(F) \overset{T \mapsto f}{\to} k[W]$$

gives a factorization

$$W \to \operatorname{Specm}(k[V][T]/(F)) \to V.$$

Each point $P' \in U$ has exactly m inverse images under the second map, and the first map is finite and dominating, and therefore surjective (recall that a finite map is closed). This proves that $\varphi^{-1}(P')$ has at least $\deg(\varphi)$ points for $P' \in U$, and part (a) of the theorem then implies that it has exactly $\deg(\varphi)$ points.

We now show that if the field extension is separable, then there exists a point such that $\#\varphi^{-1}(P)$ has $\deg \varphi$ elements. Because $k(W)$ is separable over $k(V)$, there exists a $f \in k[W]$ such that $k(V)[f] = k(W)$. Its minimum polynomial F has degree $\deg(\varphi)$ and its discriminant is a nonzero element of $k[V]$. The diagram

$$W \to \operatorname{Specm}(A[T]/(F)) \to V$$

shows that $\#\varphi^{-1}(P) \ge \deg(\varphi)$ for P a point such that $\operatorname{disc}(f)(P) \neq 0$. □

When $k(W)$ is separable over $k(V)$, then φ is said to be *separable*.

REMARK 8.13. Let $\varphi\colon W \to V$ be as in the theorem, and let $V_i = \{P \in V \mid \#\varphi^{-1}(P) \le i\}$. Let $d = \deg \varphi$. Part (b) of the theorem states that V_{d-1} is closed, and is a proper subset when φ is separable. I don't know under what hypotheses all the sets V_i will closed (and V_i will be a proper subset of V_{i-1}). The obvious induction argument fails because V_{i-1}may not be normal.

Lines on surfaces. As an application of some of the above results, we consider the problem of describing the set of lines on a surface of degree m in $\mathbb{P}^3$. To avoid possible problems, we assume for the rest of this chapter that k has characteristic zero.

We first need a way of describing lines in $\mathbb{P}^3$. Recall that we can associate with each projective variety $V \subset \mathbb{P}^n$ an affine cone over $\tilde{V}$ in k^{n+1}. This allows us to think of points in $\mathbb{P}^3$ as being one-dimensional subspaces in k^4, and lines in $\mathbb{P}^3$ as being two-dimensional subspaces in k^4. To such a subspace $W \subset k^4$, we can attach a one-dimensional subspace $\bigwedge^2 W$ in $\bigwedge^2 k^4 \approx k^6$, that is, to each line L in $\mathbb{P}^3$, we can attach point $p(L)$ in $\mathbb{P}^5$. Not every point in $\mathbb{P}^5$ should be of the form $p(L)$—heuristically, the lines in $\mathbb{P}^3$ should form a four-dimensional set. (Fix two planes in $\mathbb{P}^3$; giving a

line in $\mathbb{P}^3$ corresponds to choosing a point on each of the planes.) We shall show that there is natural one-to-one correspondence between the set of lines in $\mathbb{P}^3$ and the set of points on a certain hyperspace $\Pi \subset \mathbb{P}^5$. Rather than using exterior algebras, I shall usually give the old-fashioned proofs.

Let L be a line in $\mathbb{P}^3$ and let $\mathbf{x} = (x_0 : x_1 : x_2 : x_3)$ and $\mathbf{y} = (y_0 : y_1 : y_2 : y_3)$ be distinct points on L. Then

$$p(L) = (p_{01} : p_{02} : p_{03} : p_{12} : p_{13} : p_{23}) \in \mathbb{P}^5, \quad p_{ij} \stackrel{\text{df}}{=} \begin{vmatrix} x_i & x_j \\ y_i & y_j \end{vmatrix},$$

depends only on L. The p_{ij} are called the Plücker coordinates of L, after Plücker (1801-1868).

In terms of exterior algebras, write e_0, e_1, e_2, e_3 for the canonical basis for k^4, so that $\mathbf{x}$, regarded as a point of k^4 is $\sum x_i e_i$, and $\mathbf{y} = \sum y_i e_i$; then $\bigwedge^2 k^4$ is a 6-dimensional vector space with basis $e_i \wedge e_j$, $0 \le i < j \le 3$, and $x \wedge y = \sum p_{ij} e_i \wedge e_j$ with p_{ij} given by the above formula.

We define p_{ij} for all i, j, $0 \le i, j \le 3$ by the same formula — thus $p_{ij} = -p_{ji}$.

LEMMA 8.14. *The line L can be recovered from $p(L)$ as follows:*

$$L = \{(\sum_j a_j p_{0j} : \sum_j a_j p_{1j} : \sum_j a_j p_{2j} : \sum_j a_j p_{3j}) \mid (a_0 : a_1 : a_2 : a_3) \in \mathbb{P}^3\}.$$

PROOF. Let $\tilde{L}$ be the cone over L in k^4—it is a two-dimensional subspace of k^4—and let $\mathbf{x} = (x_0, x_1, x_2, x_3)$ and $\mathbf{y} = (y_0, y_1, y_2, y_3)$ be two linearly independent vectors in $\tilde{L}$. Then

$$\tilde{L} = \{f(\mathbf{y})\mathbf{x} - f(\mathbf{x})\mathbf{y} \mid f : k^4 \to k \text{ linear}\}.$$

Write $f = \sum a_j X_j$; then

$$f(\mathbf{y})\mathbf{x} - f(\mathbf{x})\mathbf{y} = (\sum a_j p_{0j}, \sum a_j p_{1j}, \sum a_j p_{2j}, \sum a_j p_{3j}).$$

□

LEMMA 8.15. *The point $p(L)$ lies on the quadric $\Pi \subset \mathbb{P}^5$ defined by the equation*

$$X_{01}X_{23} - X_{02}X_{13} + X_{03}X_{12} = 0.$$

PROOF. This can be verified by direct calculation, or by using that

$$0 = \begin{vmatrix} x_0 & x_1 & x_2 & x_3 \\ y_0 & y_1 & y_2 & y_3 \\ x_0 & x_1 & x_2 & x_3 \\ y_0 & y_1 & y_2 & y_3 \end{vmatrix} = 2(p_{01}p_{23} - p_{02}p_{13} + p_{03}p_{12})$$

(expansion in terms of 2×2 minors). □

LEMMA 8.16. *Every point of Π is of the form $p(L)$ for a unique line L.*

PROOF. Assume $p_{03} \neq 0$; then the line through the points $(0 : p_{01} : p_{02} : p_{03})$ and $(p_{03} : p_{13} : p_{23} : 0)$ has Plücker coordinates

$$\begin{aligned} (-p_{01}p_{03} \quad &: \quad -p_{02}p_{03} : -p_{03}^2 : \underbrace{p_{01}p_{23} - p_{02}p_{13}}_{-p_{03}p_{12}} : -p_{03}p_{13} : -p_{03}p_{23}) \\ &= \quad (p_{01} : p_{02} : p_{03} : p_{12} : p_{13} : p_{23}). \end{aligned}$$

A similar construction works when one of the other coordinates is nonzero, and this way we get inverse maps. □

Thus we have a canonical one-to-one correspondence

$$\{\text{lines in } \mathbb{P}^3\} \leftrightarrow \{\text{points on } \Pi\};$$

that is, we have identified the set of lines in $\mathbb{P}^3$ with the points of an algebraic variety. We may now use the methods of algebraic geometry to study the set. [This is a special case of the Grassmanians mentioned on p108.]

We next consider the set of homogeneous polynomials of degree m in 4 variables,

$$F(X_0, X_1, X_2, X_3) = \sum_{i_0+i_1+i_2+i_3=m} a_{i_0 i_1 i_2 i_3} X_0^{i_0} \dots X_3^{i_3}.$$

We don't distinguish two polynomials if one is a nonzero multiple of the other.

LEMMA 8.17. *The set of homogeneous polynomials of degree m in 4 variables is a vector space of dimension $\binom{3+m}{m}$*

PROOF. See a previous footnote page 89. □

Let $\nu = \binom{3+m}{m} = \frac{(m+1)(m+2)(m+3)}{6} - 1$; then we have a surjective map

$$\mathbb{P}^\nu \to \{\text{surfaces of degree } m \text{ in } \mathbb{P}^3\},$$

$$(\dots : a_{i_0 i_1 i_2 i_3} : \dots) \mapsto V(F), \qquad F = \sum a_{i_0 i_1 i_2 i_3} X_0^{i_0} X_1^{i_1} X_2^{i_2} X_3^{i_3}.$$

The map is not quite injective—for example, X^2Y and XY^2 define the same surface—but nevertheless, we can (somewhat loosely) think of the points of $\mathbb{P}^\nu$ as being (possible degenerate) surfaces of degree m in $\mathbb{P}^3$.

Let $\Gamma_m \subset \Pi \times \mathbb{P}^\nu \subset \mathbb{P}^5 \times \mathbb{P}^\nu$ be the set of pairs (L, F) consisting of a line L in $\mathbb{P}^3$ lying on the surface $F(X_0, X_1, X_2, X_3) = 0$.

THEOREM 8.18. *The set Γ_m is a closed irreducible subset of $\Pi \times \mathbb{P}^\nu$; it is therefore a projective variety. The dimension of Γ_m is $\frac{m(m+1)(m+5)}{6} + 3$.*

EXAMPLE 8.19. For $m = 1$, Γ_m is the set of pairs consisting of a plane in $\mathbb{P}^3$ and a line on the plane. The theorem says that the dimension of Γ_1 is 5. Since there are ∞^3 planes in $\mathbb{P}^3$, and each has ∞^2 lines on it, this seems to be correct.

PROOF. We first show that Γ_m is closed. Let

$$p(L) = (p_{01} : p_{02} : \dots) \qquad F = \sum a_{i_0 i_1 i_2 i_3} X_0^{i_0} \cdots X_3^{i_3}.$$

From (8.14) we see that L lies on the surface $F(X_0, X_1, X_2, X_3) = 0$ if and only if

$$F(\sum b_j p_{0j} : \sum b_j p_{1j} : \sum b_j p_{2j} : \sum b_j p_{3j}) = 0, \text{ all } (b_0, \dots, b_3) \in k^4.$$

Expand this out as a polynomial in the b_j's with coefficients polynomials in the $a_{i_0 i_1 i_2 i_3}$ and p_{ij}'s. Then $F(\dots) = 0$ for all $\mathbf{b} \in k^4$ if and only if the coefficients of the polynomial are all zero. But each coefficient is of the form

$$P(\dots, a_{i_0 i_1 i_2 i_3}, \dots ; p_{01}, p_{02} : \dots)$$

with P homogeneous separately in the a's and p's, and so the set is closed in $\Pi \times \mathbb{P}^\nu$ (cf. the discussion in 5.32).

It remains to compute the dimension of Γ_m. We shall apply Proposition 8.8 to the projection map

$$\begin{array}{ccc} (L,F) & \Gamma_m & \subset \Pi \times \mathbb{P}^\nu \\ \downarrow & \downarrow \varphi & \\ L & \Pi & \end{array}$$

For $L \in \Pi$, $\varphi^{-1}(L)$ consists of the homomogeneous polynomials of degree m such that $L \subset V(F)$ (taken up to nonzero scalars). After a change of coordinates, we can assume that L is the line

$$\begin{cases} X_0 = 0 \\ X_1 = 0, \end{cases}$$

i.e., $L = \{(0,0,*,*)\}$. Then L lies on $F(X_0,X_1,X_2,X_3) = 0$ if and only if X_0 or X_1 occurs in each nonzero monomial term in F, i.e.,

$$F \in \varphi^{-1}(L) \iff a_{i_0 i_1 i_2 i_3} = 0 \text{ whenever } i_0 = 0 = i_1.$$

Thus $\varphi^{-1}(L)$ is a linear subspace of $\mathbb{P}^\nu$; in particular, it is irreducible. We now compute its dimension. Recall that F has $\nu+1$ coefficients altogether; the number with $i_0 = 0 = i_1$ is $m+1$, and so $\varphi^{-1}(L)$ has dimension

$$\frac{(m+1)(m+2)(m+3)}{6} - 1 - (m+1) = \frac{m(m+1)(m+5)}{6} - 1.$$

We can now deduce from (8.8) that Γ_m is irreducible and that

$$\dim(\Gamma_m) = \dim(\Pi) + \dim(\varphi^{-1}(L)) = \frac{m(m+1)(m+5)}{6} + 3,$$

as claimed. □

Now consider the other projection

$$\begin{array}{ccc} (L,F) & \Gamma_m & \subset \Pi \times \mathbb{P}^\nu \\ \downarrow & \downarrow \psi & \\ F & \mathbb{P}^\nu & \end{array}$$

By definition

$$\psi^{-1}(F) = \{L \mid L \text{ lies on } V(F)\}.$$

EXAMPLE 8.20. Let $m = 1$. Then $\nu = 3$ and $\dim \Gamma_1 = 5$. The projection $\psi\colon \Gamma_1 \to \mathbb{P}^3$ is surjective (every plane contains at least one line), and (8.6) tells us that $\dim \psi^{-1}(F) \geq 2$. In fact of course, the lines on any plane form a 2-dimensional family, and so $\psi^{-1}(F) = 2$ for all F.

THEOREM 8.21. *When $m > 3$, the surfaces of degree m containing no line correspond to an open subset of $\mathbb{P}^\nu$.*

PROOF. We have

$$\dim \Gamma_m - \dim \mathbb{P}^\nu = \frac{m(m+1)(m+5)}{6} + 3 - \frac{(m+1)(m+2)(m+3)}{6} + 1 = 4 - (m+1).$$

Therefore, if $m > 3$, then $\dim \Gamma_m < \dim \mathbb{P}^\nu$, and so $\psi(\Gamma_m)$ is a proper closed subvariety of $\mathbb{P}^\nu$. This proves the claim. □

We now look at the case $m = 2$. Here $\dim \Gamma_m = 10$, and $\nu = 9$, which suggests that ψ should be surjective and that its fibres should all have dimension ≥ 1. We shall see that this is correct.

A quadric is said to be *nondegenerate* if it is defined by an irreducible polynomial of degree 2. After a change of variables, any nondegenerate quadric will be defined by an equation

$$XW = YZ.$$

This is just the image of the Segre mapping (see 5.21)

$$(a_0 : a_1), (b_0 : b_1) \mapsto (a_0b_0 : a_0b_1 : a_1b_0 : a_1b_1) : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3.$$

There are two obvious families of lines on $\mathbb{P}^1 \times \mathbb{P}^1$, namely, the horizontal family and the vertical family; each is parametrized by $\mathbb{P}^1$, and so is called a *pencil of lines*. They map to two families of lines on the quadric:

$$\begin{cases} t_0X = t_1X \\ t_0Y = t_1W \end{cases} \quad \text{and} \quad \begin{cases} t_0X = t_1Y \\ t_0Z = t_1W. \end{cases}$$

Since a degenerate quadric is a surface or a union of two surfaces, we see that every quadric surface contains a line, that is, that $\psi\colon \Gamma_2 \to \mathbb{P}^9$ is surjective. Thus (8.6) tells us that all the fibres have dimension ≥ 1, and the set where the dimension is > 1 is a proper closed subset. In fact the dimension of the fibre is > 1 exactly on the set of reducible F's, which we know to be closed (see the solution to Homework 9, Problem 1).

It follows from the above discussion that if F is nondegenerate, then $\psi^{-1}(F)$ is isomorphic to the disjoint union of two lines, $\psi^{-1}(F) \approx \mathbb{P}^1 \cup \mathbb{P}^1$. Classically, one defines a *regulus* to be a nondegenerate quadric surface together with a choice of a pencil of lines. One can show that the set of reguli is, in a natural way, an algebraic variety R, and that, over the set of nondegenerate quadrics, ψ factors into the composite of two regular maps:

$$\begin{array}{rcl} \Gamma_2 - \psi^{-1}(S) & = & \text{pairs, } (F, L) \text{ with } L \text{ on } F; \\ \downarrow & & \\ R & = & \text{set of reguli;} \\ \downarrow & & \\ \mathbb{P}^9 - S & = & \text{set of nondegenerate quadrics.} \end{array}$$

The fibres of the top map are connected, and of dimension 1 (they are all isomorphic to $\mathbb{P}^1$), and the second map is finite and two-to-one. Factorizations of this type occur quite generally (see the Stein factorization theorem (8.25) below).

We now look at the case $m = 3$. Here $\dim \Gamma_3 = 19$; $\nu = 19$: we have a map

$$\psi\colon \Gamma_3 \to \mathbb{P}^{19}.$$

THEOREM 8.22. *The set of cubic surfaces containing exactly* 27 *lines corresponds to an open subset of* $\mathbb{P}^{19}$*; the remaining surfaces either contain an infinite number of lines or a nonzero finite number* ≤ 27.

EXAMPLE 8.23. (a) Consider the Fermat surface

$$X_0^3 + X_1^3 + X_2^3 + X_3^3 = 0.$$

Let ζ be a primitive cube root of one. There are the following lines on the surface, $0 \le i, j \le 2$:

$$\begin{cases} X_0 + \zeta^i X_1 = 0 \\ X_2 + \zeta^j X_3 = 0 \end{cases} \qquad \begin{cases} X_0 + \zeta^i X_2 = 0 \\ X_1 + \zeta^j X_3 = 0 \end{cases} \qquad \begin{cases} X_0 + \zeta^i X_3 = 0 \\ X_1 + \zeta^j X_2 = 0 \end{cases}$$

There are three sets, each with nine lines, for a total of 27 lines.

(b) Consider the surface

$$X_1X_2X_3 = X_0^3.$$

In this case, there are exactly three lines. To see this, look first in the affine space where $X_0 \neq 0$—here we can take the equation to be $X_1X_2X_3 = 1$. A line in $\mathbb{A}^3$ can be written in parametric form $X_i = a_it + b_i$, but a direct inspection shows that no such line lies on the surface. Now look where $X_0 = 0$, that is, in the plane at infinity. The intersection of the surface with this plane is given by $X_1X_2X_3 = 0$ (homogeneous coordinates), which is the union of three lines, namely,

$$X_1 = 0;\ X_2 = 0;\ X_3 = 0.$$

Therefore, the surface contains exactly three lines.

(c) Consider the surface

$$X_1^3 + X_2^3 = 0.$$

Here there is a pencil of lines:

$$\begin{cases} t_0X_1 = t_1X_0 \\ t_0X_2 = -t_1X_0. \end{cases}$$

(In the affine space where $X_0 \neq 0$, the equation is $X^3 + Y^3 = 0$, which contains the line $X = t$, $Y = -t$, all t.)

We now discuss the proof of Theorem 8.22). If $\psi\colon \Gamma_3 \to \mathbb{P}^{19}$ were not surjective, then $\psi(\Gamma_3)$ would be a proper closed subvariety of $\mathbb{P}^{19}$, and the nonempty fibres would *all* have dimension ≥ 1 (by 8.6), which contradicts two of the above examples. Therefore the map is surjective[22], and there is an open subset U of $\mathbb{P}^{19}$ where the fibres have dimension 0; outside U, the fibres have dimension > 0.

Given that every cubic surface has at least one line, it is not hard to show that there is an open subset U' where the cubics have exactly 27 lines (see Reid, 1988, pp106–110); in fact, U' can be taken to be the set of nonsingular cubics. According to (6.24), the restriction of ψ to $\psi^{-1}(U)$ is finite, and so we can apply (8.10) to see that all cubics in $U - U'$ have fewer than 27 lines.

Remark 8.24. The twenty-seven lines on a cubic surface were discovered in 1849 by Salmon and Cayley, and have been much studied—see A. Henderson, The Twenty-Seven Lines Upon the Cubic Surface, Cambridge University Press, 1911. For example, it is known that the group of permutations of the set of 27 lines preserving intersections (that is, such that $L \cap L' \neq \emptyset \iff \sigma(L) \cap \sigma(L') \neq \emptyset$) is isomorphic to the Weyl group of the root system of a simple Lie algebra of type E_6, and hence has 25920 elements.

It is known that there is a set of 6 skew lines on a nonsingular cubic surface V. Let L and L' be two skew lines. Then "in general" a line joining a point on L to a point

[22]According to Miles Reid (1988, p126) every adult algebraic geometer knows this proof that every cubic contains a line.

on L' will meet the surface in exactly one further point. In this way one obtains an invertible regular map from an open subset of $\mathbb{P}^1 \times \mathbb{P}^1$ to an open subset of V, and hence V is birationally equivalent to $\mathbb{P}^2$.

Stein factorization. The following important theorem shows that the fibres of a proper map are disconnected only because the fibres of finite maps are disconnected.

THEOREM 8.25. *Let $\varphi\colon W \to V$ be a proper morphism of varieties. It is possible to factor φ into $W \xrightarrow{\varphi_1} W' \xrightarrow{\varphi_2} V$ with φ_1 proper with connected fibres and φ_2 finite.*

PROOF. This is usually proved at the same time as Zariski's main theorem (if W and V are irreducible, and V is affine, then W' is the affine variety with $k[W']$ the integral closure of $k[V]$ in $k(W)$). □

9. Algebraic Geometry over an Arbitrary Field

We now explain how to extend the theory in the preceding sections to a nonalgebraically closed base field. Fix a field k, and let k^{al} be an algebraic closure of k.

Sheaves. We shall need a more abstract notion of a ringed space and of a sheaf.

A *presheaf* $\mathcal{F}$ on a topological space V is a map assigning to each open subset U of V a set $\mathcal{F}(U)$ and to each inclusion $U \supset U'$ a "restriction" map

$$a \mapsto a|U' \colon \mathcal{F}(U) \to \mathcal{F}(U');$$

the restriction map $\mathcal{F}(U) \to \mathcal{F}(U)$ is required to be the identity map, and if $U'' \supset U' \supset U$, then the composite of the restriction maps $\mathcal{F}(U) \to \mathcal{F}(U')$ and $\mathcal{F}(U') \to \mathcal{F}(U'')$ is required to be the restriction map $\mathcal{F}(U) \to \mathcal{F}(U'')$. In other words, a presheaf is a contravariant functor to the category of sets from the category whose objects are the open subsets of V and whose morphisms are the inclusions . A *homomorphism* of presheaves $\alpha \colon \mathcal{F} \to \mathcal{F}'$ is a family of maps

$$\alpha(U) \colon \mathcal{F}(U) \to \mathcal{F}'(U)$$

commuting with the restriction maps.

A presheaf $\mathcal{F}$ is a *sheaf* if for every open covering $\{U_i\}$ of an open subset U of V and family of elements $a_i \in \mathcal{F}(U_i)$ agreeing on overlaps (that is, such that $a_i|U_i \cap U_j = a_j|U_i \cap U_j$ for all i, j), there is a unique element $a \in \mathcal{F}(U)$ such that $a_i = a|U_i$ for all i. A *homomorphism* of sheaves on V is a homomorphism of presheaves.

If the sets $\mathcal{F}(U)$ are abelian groups and the restriction maps are homomorphisms, then the sheaf is a *sheaf of abelian groups*. Similarly one defines a *sheaf of rings,* a sheaf of k-algebras, and a *sheaf of modules* over a sheaf of rings.

For $v \in V$, the *stalk* of a sheaf $\mathcal{F}$ (or presheaf) at v is

$$\mathcal{F}_v = \varinjlim \mathcal{F}(U) \quad \text{(limit over open neighbourhoods of } v\text{)}.$$

A *ringed space* is a pair $(V, \mathcal{O})$ consisting of topological space V together with a sheaf of rings. If the stalk $\mathcal{O}_v$ of $\mathcal{O}$ at v is a local ring for all $v \in V$, then $(V, \mathcal{O})$ is called a *locally ringed space.* A *morphism* $(V, O) \to (V', O')$ *of ringed spaces* is a pair (φ, ψ) with φ a continuous map $V \to V'$ and ψ a family of maps

$$\psi(U') \colon \mathcal{O}'(U') \to \mathcal{O}(\varphi^{-1}(U')),\ U' \text{ open in } V',$$

commuting with the restriction maps. Such a pair defines homomorphism of rings $\psi_v \colon \mathcal{O}'_{\varphi(v)} \to \mathcal{O}_v$ for all $v \in V$. A *morphism of locally ringed spaces* is a morphism of ringed space such that ψ_v is a local homomorphism for all v.

Extending scalars. Recall that a ring A is *reduced* if it has no nonzero nilpotents. If A is reduced, then $A \otimes_k k^{\mathrm{al}}$ need not be reduced. Consider for example the algebra $A = k[X, Y]/(X^p + Y^p + a)$ where $p = char(k)$ and $a \notin k^p$. Then A is reduced (even an integral domain) because $X^p + Y^p + a$ is irreducible in $k[X, Y]$, but

$$A \otimes_k k^{\mathrm{al}} = k^{\mathrm{al}}[X, Y]/(X^p + Y^p + a) = k^{\mathrm{al}}[X, Y]/((X + Y + \alpha)^p),\ \alpha^p = a,$$

which is not reduced because $x + y + \alpha \neq 0$ but $(x + y + \alpha)^p = 0$.

The next proposition shows that problems of this kind arise only because of inseparability; in particular, they don't occur if k is perfect.

Recall that the *characteristic exponent* of a field is p if k has characteristic $p \neq 0$, and it is 1 is k has characteristic zero. For p equal to the characteristic exponent of k, let

$$k^{\frac{1}{p}} = \{\alpha \in k^{\mathrm{al}} \mid \alpha^p \in k\}.$$

It is a subfield of k^{al}, and $k^{\frac{1}{p}} = k$ if and only if k is perfect.

PROPOSITION 9.1. *Let A be a reduced finitely generated k-algebra. The following statements are equivalent:*

(a) *$A \otimes_k k^{\frac{1}{p}}$ is reduced;*
(b) *$A \otimes_k k^{al}$ is reduced;*
(c) *$A \otimes_k K$ is reduced for all fields $K \supset k$.*

PROOF. Clearly c$\Longrightarrow$b$\Longrightarrow$a. The implication a $\Longrightarrow$c follows from Zariski and Samuel 1958, III.15, Theorem 39 (localize A at a minimal prime to get a field). □

Even when A is an integral domain and $A \otimes_k k^{\mathrm{al}}$ is reduced, the latter need not be an integral domain. Suppose, for example, that A is a finite separable field extension of k. Then $A \approx k[X]/(f(X))$ with $f(X)$ an irreducible separable polynomial. Hence

$$A \otimes_k k^{\mathrm{al}} \approx k^{\mathrm{al}}[X]/(f(X)) = k^{\mathrm{al}}/(\Pi(X - a_i)) \approx \Pi\ k^{\mathrm{al}}/(X - a_i)$$

(by the Chinese remainder theorem). This shows that if A contains a finite separable field extension of k, then $A \otimes_k k^{\mathrm{al}}$ can't be an integral domain. The next proposition gives a converse.

PROPOSITION 9.2. *Let A be a finitely generated k-algebra, and assume that A is an integral domain, and that $A \otimes_k k^{al}$ is reduced. Then $A \otimes_k k^{al}$ is an integral domain if and only if k is algebraically closed in A (i.e., if $a \in A$ is algebraic over k, then $a \in k$).*

PROOF. Ibid. III.15. □

After these preliminaries, it is possible rewrite all of the preceding sections with k not necessarily algebraically closed. I indicate briefly how this is done.

Affine algebraic varieties. An *affine k-algebra* A is a finitely generated k-algebra A such that $A \otimes_k k^{\mathrm{al}}$ is reduced. Since $A \subset A \otimes_k k^{\mathrm{al}}$, A itself is then reduced. Proposition 9.1 has the following consequence.

COROLLARY 9.3. *Let A be a reduced finitely generated k-algebra.*

(a) *If k is perfect, then A is an affine k-algebra.*
(b) *If A is an affine k-algebra, then $A \otimes_k K$ is reduced for all fields K containing k.*

Let A be a finitely generated k-algebra. The choice of a set $\{x_1, ..., x_n\}$ of generators for A, determines isomorphisms

$$A \cong k[x_1, ..., x_n] \cong k[X_1, ..., X_n]/(f_1, ..., f_m),$$

and

$$A \otimes_k k^{\mathrm{al}} \cong k^{\mathrm{al}}[X_1, ..., X_n]/(f_1, ..., f_m).$$

Thus A is an affine algebra if the elements $f_1, ..., f_m$ of $k[X_1, ..., X_n]$ generate a *radical* ideal when regarded as elements of $k^{\mathrm{al}}[X_1, ..., X_n]$. From the above remarks, we see that this condition implies that they generate a radical ideal in $k[X_1, ..., X_n]$, and the converse implication holds when k is perfect.

Let A be an affine k-algebra. Define $\mathrm{specm}(A)$ to be the set of maximal ideals in A, and endow it with the topology having as basis the sets $D(f)$, $D(f) = \{\mathfrak{m} \mid f \notin m\}$. There is a unique sheaf of k-algebras $\mathcal{O}$ on $\mathrm{specm}(A)$ such that $\mathcal{O}(D(f)) = A_f$ for all f (recall that A_f is the ring obtained from A by inverting f). Here $\mathcal{O}$ is a sheaf in the above abstract sense — the elements of $\mathcal{O}(U)$ are not functions on U with values in k, although we may wish to think of them as if they were. If $f \in A$ and $\mathfrak{m}_v \in \mathrm{specm}(A)$, then we can define $f(v)$ to be the image of f in the $\kappa(v) \stackrel{\mathrm{df}}{=} A/\mathfrak{m}_v$, and it does make sense to speak of the zero set of f in V. The ringed space

$$\mathrm{Specm}(A) = (\mathrm{specm}(A), \mathcal{O})$$

is called an *affine variety* over k. The stalk at $\mathfrak{m} \in V$ is the local ring $A_{\mathfrak{m}}$, and so $\mathrm{Specm}(A)$ is a locally ringed space.

If $k = k^{\mathrm{al}}$, and

$$A = k[x_1, ..., x_n] = k[X_1, ..., X_n]/(f_1, ..., f_m),$$

then the Nullstellensatz allows us to identify $\mathrm{specm}(A)$ with the set $V(f_1, ..., f_m)$ of common zeros of the f_i, via

$$(x_1 - a_1, ..., x_n - a_n) \longmapsto (a_1, ..., a_n).$$

Moreover, in this case, the elements of $\mathcal{O}(U)$ can be identified with k-valued functions on U.

A *morphism* of affine algebraic varieties over k is defined to be a morphism $(V, \mathcal{O}_V) \to (W, \mathcal{O}_W)$ of ringed spaces of k-algebras — it is automatically a morphism of locally ringed spaces.

A homomorphism of k-algebras $A \to B$ defines a morphism of affine k-varieties,

$$\mathrm{Specm}\, B \to \mathrm{Specm}\ \ A$$

in a natural way, and this gives a bijection:

$$Hom_{k-alg}(A, B) \cong \mathrm{Hom}_k(W, V), \quad V = \mathrm{Specm}\, A, \quad W = \mathrm{Specm}\ \ B.$$

Therefore $A \mapsto \mathrm{Specm}(A)$ is an equivalence of from the category of affine k-algebras to that of affine algebraic varieties over k; its quasi-inverse is $V \mapsto k[V] \stackrel{\mathrm{df}}{=} \Gamma(V, \mathcal{O}_V)$.

If $A = k[X_1, ..., X_m]/\mathfrak{a}$ and $B = k[Y_1, ..., Y_n]/\mathfrak{b}$, a homomorphism $A \to B$ is determined by a family of polynomials, $P_i(Y_1, ..., Y_n)$, $i = 1, ..., m$; the homomorphism sends x_i to $P_i(y_1, ..., y_n)$; in order to define a homomorphism, the P_i must be such that

$$F \in \mathfrak{a} \Longrightarrow F(P_1, ..., P_n) \in \mathfrak{b};$$

two families $P_1, ..., P_m$ and $Q_1, ..., Q_m$ determine the same map if and only if $P_i \equiv Q_i \mod \mathfrak{b}$ for all i.

Let A be an affine k-algebra, and let $V = \operatorname{Specm} A$. For any field $K \supset k$, $A \otimes_k K$ is an affine algebra over K, and hence we get a variety $V_K \stackrel{\text{df}}{=} \operatorname{Specm}(A \otimes_k K)$ over K. We say that V_K has been obtained from V by *extension of scalars*. Note that if $A = k[X_1, ..., X_n]/(f_1, ..., f_m)$ then $A \otimes_k K = K[X_1, ..., X_n]/(f_1, ..., f_m)$. The map $V \mapsto V_K$ is a functor from affine varieties over k to affine varieties over K.

Let $V_0 = \operatorname{Specm}(A_0)$ be an affine variety over k, and let $W = V(\mathfrak{b})$ be a closed subvariety of $V \stackrel{\text{df}}{=} V_{0,k^{\text{al}}}$. Then W arises by extension of scalars from a closed subvariety W_0 of V_0 if and only if the ideal $\mathfrak{b}$ of $A_0 \otimes_k k^{\text{al}}$ is generated by elements A_0. Except when k is perfect, this is stronger than saying W is the zero set of a family of elements of A.

Algebraic varieties. A ringed space $(V, \mathcal{O})$ is a *prevariety* over k if there is a finite covering (U_i) of V by open subsets such that $(U_i, \mathcal{O}|U_i)$ is an affine variety over k for all i. A *morphism of prevarieties* over k is a morphism of ringed spaces of k-algebras.

A prevariety V over k is *separated* if for all pairs of morphisms of k-varieties $\alpha, \beta : Z \to V$, the subset of Z on which α and β agree is closed. A *variety* is a separated prevariety.

Products: Let A and B be finitely generated k-algebras. It is possible for A and B to be reduced but for $A \otimes_k B$ fail to be reduced — consider for example,

$$A = k[X, Y]/(X^p + Y^p + a), \quad B = k[Z]/(Z^p - a), \quad a \notin k^p.$$

However, if A and B are affine k-algebras, then $A \otimes_k B$ is again an affine k-algebra. To see this, note that (by definition), $A \otimes_k k^{\text{al}}$ and $B \otimes_k k^{\text{al}}$ are affine k-algebras, and therefore so also is their tensor product over k^{al} (3.16); but

$$(A \otimes_k k^{\text{al}}) \otimes_{k^{\text{al}}} (k^{\text{al}} \otimes_k B) = ((A \otimes_k k^{\text{al}}) \otimes_{k^{\text{al}}} k^{\text{al}}) \otimes_k B = (A \otimes_k B) \otimes_k k^{\text{al}}.$$

Thus we can define the product of two affine algebraic varieties, $V = \operatorname{Specm} A$ and $W = \operatorname{Specm} B$, over k by

$$V \times_k W = \operatorname{Specm}(A \otimes_k B).$$

It has the universal property expected of products, and the definition extends in a natural way to (pre)varieties.

Just as in (3.18), the diagonal Δ is locally closed in $V \times V$, and it is closed if and only if V is separated.

Extension of scalars: Let V be a variety over k, and let K be a field containing k. There is a natural way of defining a variety V_K, said to be obtained from V by *extension of scalars*: if V is a union of open affines, $V = \cup U_i$, then $V_K = \cup U_{i,K}$ and the $U_{i,K}$ are patched together the same way as the U_i. The dimension of a variety doesn't change under extension of scalars.

When V is a variety over k^{al} obtained from a variety V_0 over k by extension of scalars, we sometimes call V_0 a *model* for V over k. More precisely, a model of V over k is a variety V_0 over k together with an isomorphism $\varphi\colon V_{0,k^{\text{al}}} \to V$.

Of course, V need not have a model over k — for example, an elliptic curve

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3$$

over k^{al} will have a model over $k \subset k^{\mathrm{al}}$ if and only if its j-invariant $j(E) \stackrel{\mathrm{df}}{=} \frac{1728(4a)^3}{-16(4a^3+27b^2)}$ lies in k. Moreover, when V has a model over k, it will usually have a large number of them, no two of which are isomorphic over k. Consider, for example, the quadric surface in $\mathbb{P}^3$over $\mathbb{Q}^{\mathrm{al}}$,

$$V : X^2 + Y^2 + Z^2 + W^2 = 0.$$

The models over V over $\mathbb{Q}$ are defined by equations

$$aX^2 + bY^2 + cZ^2 + dW^2 = 0,\ a,\ b,\ c,\ d \in \mathbb{Q}.$$

Classifying the models of V over $\mathbb{Q}$ is equivalent to classifying quadratic forms over $\mathbb{Q}$ in 4 variables. This has been done, but it requires serious number theory. In particular, there are infinitely many (see Chapter VIII of my notes on Class Field Theory).

Exercise 9.4. Show directly that, up to isomorphism, the curve $X^2 + Y^2 = 1$ over $\mathbb{C}$ has exactly two models over $\mathbb{R}$.

The points on a variety. Let V be a variety over k. A *point* of V *with coordinates* in k, or a *point* of V *rational* over k, is a morphism $\operatorname{Specm} k \to V$. For example, if V is affine, say $V = \operatorname{Specm}(A)$, then a point of V with coordinates in k is a k-homomorphism $A \to k$. If $A = k[X_1, ..., X_n]/(f_1, ..., f_m)$, then to give a k-homomorphism $A \to k$ is the same as to give an n-tuple $(a_1, ..., a_n)$ such that

$$f_i(a_1, ..., a_n) = 0, \quad i = 1, ..., m.$$

In other words, of V is the affine variety over k defined by the equations

$$f_i(X_1, \dots, X_n) = 0, \quad i = 1, \dots, m$$

then a point of V with coordinates in k is a solution to this system of equations in k. We write $V(k)$ for the points of V with coordinates in k.

We extend this notion to obtain the set of points $V(R)$ of a variety V with coordinates in *any* k-algebra R. For example, when $V = \operatorname{Specm}(A)$, we set

$$V(R) = Hom_{k-alg}(A, R).$$

Again, if

$$A = k[X_1, ..., X_n]/(f_1, ..., f_m),$$

then

$$V(R) = \{(a_1, ..., a_n) \in R^n \ \mid \ f_i(a_1, ..., a_n) = 0, i = 1, 2, ..., m\}.$$

What is the relation between the elements of V and the elements of $V(k)$? Suppose V is affine, say $V = \operatorname{Specm}(A)$. Let $v \in V$. Then v corresponds to a maximal ideal $\mathfrak{m}_v$ in A (actually, it *is* a maximal ideal), and we write $\kappa(v)$ for the residue field $\mathcal{O}_v/\mathfrak{m}_v$. Then $\kappa(v)$ is a finite extension of k, and we call the degree of $\kappa(v)$ over k the *degree* of v. Let K be a field algebraic over k. To give a point of V with coordinates in K is to give a homomorphism of k-algebras $A \to K$. The kernel of such a homomorphism is a maximal ideal $\mathfrak{m}_v$ in A, and the homomorphisms $A \to k$ with kernel $\mathfrak{m}_v$ are in one-to-one correspondence with the k-homomorphisms $\kappa(v) \to K$. In particular, we see that there is a natural one-to-one correspondence between the points of V with

coordinates in k and the points v of V with $\kappa(v) = k$, i.e., with the points v of V of degree 1. This statement holds also for nonaffine algebraic varieties.

Assume now that k is perfect. The k^{al}-rational points of V with image $v \in V$ are in one-to-one correspondence with the k-homomorphisms $\kappa(v) \to k^{\mathrm{al}}$ — therefore, there are exactly $\deg(v)$ of them, and they form a single orbit under the action of $\mathrm{Gal}(k^{\mathrm{al}}/k)$. Thus there is a natural bijection from V to the set of orbits for $\mathrm{Gal}(k^{\mathrm{al}}/k)$ acting on $V(k^{\mathrm{al}})$.

Local Study. Let $V = V(\mathfrak{a}) \subset \mathbb{A}^n$, and let $\mathfrak{a} = (f_1, ..., f_r)$. The *singular locus* V_{sing} of V is defined by the vanishing of the $(n-d) \times (n-d)$ minors of the matrix

$$Jac(f_1, f_2, \dots, f_r) = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} & \cdots & \frac{\partial f_1}{\partial x_r} \\ \frac{\partial f_2}{\partial x_1} & & & \\ \vdots & & & \\ \frac{\partial f_r}{\partial x_1} & & & \frac{\partial f_r}{\partial x_r} \end{pmatrix}.$$

We say that v is *nonsingular* if some $(n-d) \times (n-d)$ minor doesn't vanish at v. We say V is nonsingular all its singular locus is empty. If V is nonsingular, then it is regular, but not conversely. Obviously V is nonsingular $\iff V_{k^{\mathrm{al}}}$ is nonsingular.

Note that V_{sing} is compatible with extension of scalars. Therefore (Theorem 4.21) it is a proper subvariety of V.

Projective varieties; complete varieties. It is possible to associate projective varieties to certain graded rings over k. An algebraic variety over k is *complete* if for all varieties W, the projection map $V \times W \to W$ is closed, and this property persists under extension of scalars to k^{al}. A projective variety is complete.

Finite maps. The Noether normalization theorem needs a different proof when the field is finite.

10. Divisors and Intersection Theory

In this section, k is an arbitrary field.

Divisors. Recall that a normal ring is an integral domain that is integrally closed in its field of fractions. A variety V is *normal* if $\mathcal{O}_v$ is a normal ring for all $v \in V$. Equivalent condition: for every open connected affine subset U of V, $\Gamma(U, \mathcal{O}_V)$ is a normal ring.

Remark 10.1. Let V be a projective variety, say defined by a homogeneous ring R. If R is normal, then V is said to be *projectively normal*. A projectively normal variety is normal, but the converse statement is false.

Assume now that V is normal and irreducible.

A *prime divisor* on V is an irreducible subvariety of V of codimension 1. A *divisor* on V is an element of the free abelian group $Div(V)$ generated by the prime divisors. Thus a divisor D can be written uniquely as a finite (formal) sum

$$D = \sum n_i Z_i, \quad n_i \in \mathbb{Z}, \quad Z_i \text{ a prime divisor on } V.$$

The *support* $|D|$ of D is the union of the Z_i corresponding to nonzero n_i's. A divisor is said to be *effective* (or *positive*) if $n_i \geq 0$ for all i. We get a partial ordering on the divisors defining $D \geq D'$ to mean $D - D' \geq 0$.

Because V is normal, there is associated with every prime divisor Z on V a discrete valuation ring $\mathcal{O}_Z$. This can be defined, for example, by choosing an open affine subvariety U of V such that $U \cap Z \neq \emptyset$; then $U \cap Z$ is a maximal proper closed subset of U, and so the ideal $\mathfrak{p}$ corresponding to it is minimal among the nonzero ideals of $R = \Gamma(U, \mathcal{O})$; so $R_{\mathfrak{p}}$ is a normal ring with exactly one nonzero prime ideal $\mathfrak{p}R$ — it is therefore a discrete valuation ring (Atiyah and MacDonald 9.2), which is defined to be $\mathcal{O}_Z$. More intrinsically we can define $\mathcal{O}_Z$ to be the set of rational functions on V that are defined an open subset U of V with $U \cap Z \neq \emptyset$.

Let ord_Z be the valuation of $k(V)^\times \twoheadrightarrow \mathbb{Z}$ with valuation ring $\mathcal{O}_Z$. The divisor of a nonzero element f of $k(V)$ is defined to be

$$\mathrm{div}(f) = \sum \mathrm{ord}_Z(f) \cdot Z.$$

The sum is over all the prime divisors of V, but in fact $\mathrm{ord}_Z(f) = 0$ for all but finitely many Z's. In proving this, we can assume that V is affine (because it is a finite union of affines), say $V = \mathrm{Specm}(R)$. Then $k(V)$ is the field of fractions of R, and so we can write $f = g/h$ with $g, h \in R$, and $\mathrm{div}(f) = \mathrm{div}(g) - \mathrm{div}(h)$. Therefore, we can assume $f \in R$. The zero set of f, $V(f)$ either is empty or is a finite union of prime divisors, $V = \cup Z_i$ (see 7.2) and $\mathrm{ord}_Z(f) = 0$ unless Z is one of the Z_i.

The map

$$f \mapsto \mathrm{div}(f) \colon k(V)^\times \to Div(V)$$

is a homomorphism. A divisor of the form $\mathrm{div}(f)$ is said to be *principal*, and two divisors are said to be *linearly equivalent*, denoted $D \sim D'$, if they differ by a principal divisor.

When V is nonsingular, the *Picard group* $Pic(V)$ of V is defined to be the group of divisors on V modulo principal divisors. (Later, we shall define $Pic(V)$ for an

arbitrary variety; when V is singular it will differ from the group of divisors modulo principal divisors, even when V is normal.)

EXAMPLE 10.2. Let C be a nonsingular affine curve corresponding to the affine k-algebra R. Because C is nonsingular, R is a Dedekind domain. A prime divisor on C can be identified with a nonzero prime divisor in R, a divisor on C with a fractional ideal, and $Pic(C)$ with the ideal class group of R.

Let U be an open subset of V, and let Z be a prime divisor of V. Then $Z \cap U$ is either empty or is a prime divisor of U. We define the *restriction* of a divisor $D = \sum n_Z Z$ on V to U to be

$$D|_U = \sum_{Z \cap U \neq \emptyset} n_Z \cdot Z \cap U.$$

When V is nonsingular, every divisor D is *locally principal*, i.e., every point P has an open neighbourhood U such that the restriction of D to U is principal. It suffices to prove this for a divisor Z. If P is not in the support of D, we can take $f = 1$. The prime divisors passing through P are in one-to-one correspondence with the prime ideals $\mathfrak{p}$ of height 1 in $\mathcal{O}_P$, i.e., the minimal nonzero prime ideals. Our assumption implies that $\mathcal{O}_P$ is a regular local ring. It is a (fairly hard) theorem in commutative algebra that a regular local ring is a unique factorization domain. It is a (fairly easy) theorem that a Noetherian integral domain is a unique factorization domain if every prime ideal of height 1 is principal (Nagata 1962, 13.1). Thus $\mathfrak{p}$ is principal in $\mathcal{O}_\mathfrak{p}$, and this implies that it is principal in $\Gamma(U, \mathcal{O}_V)$ for some open affine set U containing P (see also 7.13).

If $D|_U = \operatorname{div}(f)$, then we call f a *local equation* for D on U.

Intersection theory. Fix a nonsingular variety V of dimension n over a field k, assumed to be perfect. Let W_1 and W_2 be irreducible closed subsets of V, and let Z be an irreducible component of $W_1 \cap W_2$. Then intersection theory attaches a multiplicity to Z. We shall only do this in an easy case.

Divisors. Let V be a nonsingular variety of dimension n, and let $D_1, \dots, D_n$ be effective divisors on V. We say that $D_1, \dots, D_n$ *intersect properly* at $P \in |D_1| \cap \dots \cap |D_n|$ if P is an isolated point of the intersection. In this case, we define

$$(D_1 \cdot \dots \cdot D_n)_P = \dim_k \mathcal{O}_P/(f_1, \dots, f_n)$$

where f_i is a local equation for D_i near P. The hypothesis on P implies that this is finite.

EXAMPLE 10.3. In all the examples, the ambient variety is a surface.

(a) Let Z_1 be the affine plane curve $Y^2 - X^3$, let Z_2 be the curve $Y = X^2$, and let $P = (0, 0)$. Then

$$(Z_1 \cdot Z_2)_P = \dim k[X, Y]_{(X,Y)}/(Y - X^3, Y^2 - X^3) = \dim k[X]/(X^4 - X^3) = 3.$$

(b) If Z_1 and Z_2 are prime divisors, then $(Z_1 \cdot Z_2)_P = 1$ if and only if f_1, f_2 are local uniformizing parameters at P. Equivalently, $(Z_1 \cdot Z_2)_P = 1$ if and only if Z_1 and Z_2 are *transversal* at P, that is, $T_{Z_1}(P) \cap T_{Z_2}(P) = \{0\}$.

(c) Let D_1 be the x-axis, and let D_2 be the cuspidal cubic $Y^2 - X^3$. For $P = (0,0)$, $(D_1 \cdot D_2)_P = 3$.

(d) In general, $(Z_1 \cdot Z_2)_P$ is the "order of contact" of the curves Z_1 and Z_2.

We say that $D_1, \dots, D_n$ *intersect properly* if they do so at every point of intersection of their supports; equivalently, if $|D_1| \cap \dots \cap |D_n|$ is a finite set. We then define the intersection number

$$(D_1 \cdot \dots \cdot D_n) = \sum_{P \in |D_1| \cap \dots \cap |D_n|} (D_1 \cdot \dots \cdot D_n)_P.$$

EXAMPLE 10.4. Let C be a curve. If $D = \sum n_i P_i$, then the intersection number

$$(D) = \sum n_i [k(P_i) : k].$$

By definition, this is the degree of D.

Consider a regular map $\alpha\colon W \to V$ of connected nonsingular varieties, and let D be a divisor on V whose support does not contain the image of W. There is then a unique divisor $\alpha^* D$ on W with the following property: if D has local equation f on the open subset U of V, then $\alpha^* D$ has local equation $f \circ \alpha$ on $\alpha^{-1}U$. (Use 7.2 to see that this does define a divisor on W; if the image of α is disjoint from $|D|$, then $\alpha^* D = 0$.)

EXAMPLE 10.5. Let C be a curve on a surface V, and let $\alpha\colon C' \to C$ be the normalization of C. For any divisor D on V,

$$(C \cdot D) = \deg \alpha^* D.$$

LEMMA 10.6 (Additivity). *Let $D_1, \dots, D_n, D$ be divisors on V. If $(D_1 \cdot \dots \cdot D_n)_P$ and $(D_1 \cdot \dots \cdot D)_P$ are both defined, then so also is $(D_1 \cdot \dots \cdot D_n + D)_P$, and*

$$(D_1 \cdot \dots \cdot D_n + D)_P = (D_1 \cdot \dots \cdot D_n)_P + (D_1 \cdot \dots \cdot D)_P.$$

PROOF. One writes some exact sequences. See Shafarevich 1994, IV.1.2. □

Note that in intersection theory, unlike every other part of mathematics, we add first, and then multiply.

Since every divisor is the difference of two effective divisors, Lemma 10.1 allows us to extend the definition of $(D_1 \cdot \dots \cdot D_n)$ to all divisors intersecting properly (not just effective divisors).

LEMMA 10.7 (Invariance under linear equivalence). *Assume V is complete. If $D_n \sim D_n'$, then*

$$(D_1 \cdot \dots \cdot D_n) = (D_1 \cdot \dots \cdot D_n').$$

PROOF. By additivity, it suffices to show that $(D_1 \cdot \dots \cdot D_n) = 0$ if D_n is a principal divisor. For $n = 1$, this is just the statement that a function has as many poles as zeros (counted with multiplicities). Suppose $n = 2$. By additivity, we may assume that D_1 is a curve, and then the assertion follows from Example 10.5 because

$$D \text{ principal } \Rightarrow \alpha^* D \text{ principal.}$$

The general case may be reduced to this last case (with some difficulty). See Shafarevich 1994, IV.1.3. □

LEMMA 10.8. *For any n divisors $D_1, \dots, D_n$ on an n-dimensional variety, there exists n divisors $D_1', \dots, D_n'$ intersect properly.*

PROOF. See Shafarevich 1994, IV.1.4. □

We can use the last two lemmas to define $(D_1 \cdot \ldots \cdot D_n)$ for any divisors on a complete nonsingular variety V: choose $D_1', \dots, D_n'$ as in the lemma, and set

$$(D_1 \cdot \ldots \cdot D_n) = (D_1' \cdot \ldots \cdot D_n').$$

EXAMPLE 10.9. Let C be a smooth complete curve over $\mathbb{C}$, and let $\alpha\colon C \to C$ be a regular map. Then the Lefschetz trace formula states that

$$(\Delta \cdot \Gamma_\alpha) = \operatorname{Tr}(\alpha|H^0(C,\mathbb{Q}) - \operatorname{Tr}(\alpha|H^1(C,\mathbb{Q}) + \operatorname{Tr}(\alpha|H^2(C,\mathbb{Q}).$$

In particular, we see that $(\Delta \cdot \Delta) = 2 - 2g$, which may be negative, even though Δ is an effective divisor.

Let $\alpha\colon W \to V$ be a finite map of irreducible varieties. Then $k(W)$ is a finite extension of $k(V)$, and the degree of this extension is called the *degree* of α. If $k(W)$ is separable over $k(V)$ and k is algebraically closed, then there is an open subset U of V such that $\alpha^{-1}(u)$ consists exactly $d = \deg\alpha$ points for all $u \in U$. In fact, $\alpha^{-1}(u)$ always consists of exactly $\deg\alpha$ points if one counts multiplicities. Number theorists will recognize this as the formula $\sum e_i f_i = d$. Here the f_i are 1 (if we take k to be algebraically closed), and e_i is the multiplicity of the i^{th} point lying over the given point.

A finite map $\alpha\colon W \to V$ is *flat* if every point P of V has an open neighbourhood U such that $\Gamma(\alpha^{-1}U, \mathcal{O}_W)$ is a free $\Gamma(U, \mathcal{O}_V)$-module — it is then free of rank $\deg\alpha$.

THEOREM 10.10. *Let $\alpha\colon W \to V$ be a finite map between nonsingular varieties. For any divisors $D_1, \dots, D_n$ on V intersecting properly at a point P of V,*

$$\sum_{\alpha(Q)=P} (\alpha^* D_1 \cdot \ldots \cdot \alpha^* D_n) = \deg\alpha \cdot (D_1 \cdot \ldots \cdot D_n)_P.$$

PROOF. After replacing V by a sufficiently small open affine neighbourhood of P, we may assume that α corresponds to a map of rings $A \to B$ and that B is free of rank $d = \deg\alpha$ as an A-module. Moreover, we may assume that $D_1, \dots, D_n$ are principal with equations $f_1, \dots, f_n$ on V, and that P is the only point in $|D_1| \cap \ldots \cap |D_n|$. Then $\mathfrak{m}_P$ is the only ideal of A containing $\mathfrak{a} = (f_1, \dots, f_n)$. Set $S = A \setminus \mathfrak{m}_P$; then

$$S^{-1}A/S^{-1}\mathfrak{a} = S^{-1}(A/\mathfrak{a}) = A/\mathfrak{a}$$

because $A/\mathfrak{a}$ is already local. Hence

$$(D_1 \cdot \ldots \cdot D_n)_P = \dim A/(f_1, \dots, f_n).$$

Similarly,

$$(\alpha^* D_1 \cdot \ldots \cdot \alpha^* D_n)_P = \dim B/(f_1 \circ \alpha, \dots, f_n \circ \alpha).$$

But B is a free A-module of rank d, and

$$A/(f_1, \dots, f_n) \otimes_A B = B/(f_1 \circ \alpha, \dots, f_n \circ \alpha).$$

Therefore, as A-modules, and hence as k-vector spaces,

$$B/(f_1 \circ \alpha, \dots, f_n \circ \alpha) \approx (A/(f_1, \dots, f_n))^d$$

which proves the formula. □

EXAMPLE 10.11. Assume k is algebraically closed of characteristic $p \neq 0$. Let $\alpha\colon \mathbb{A}^1 \to \mathbb{A}^1$ be the Frobenius map $c \mapsto c^p$. It corresponds to the map $k[X] \to k[X]$, $X \mapsto X^p$, on rings. Let D be the divisor c. It has equation $X - c$ on $\mathbb{A}^1$, and $\alpha^* D$ has the equation $X^p - c = (X - \gamma)^p$. Thus $\alpha^* D = p(\gamma)$, and so

$$\deg(\alpha^* D) = p = p \cdot \deg(D).$$

The general case. Let V be a nonsingular connected variety. A *cycle of codimension* r on V is an element of the free abelian group $C^r(V)$ generated by the prime cycles of codimension r.

Let Z_1 and Z_2 be prime cycles on any nonsingular variety V, and let W be an irreducible component of $Z_1 \cap Z_2$. We know that

$$\dim\ Z_1 + \dim\ Z_2 \leq \dim\ V + \dim\ W,$$

and we say Z_1 and Z_2 *intersect properly* at W if equality holds.

Define $\mathcal{O}_{V,W}$ to be the set of rational functions on V that are defined on some open subset U of V with $U \cap W \neq \emptyset$ — it is a local ring. Assume that Z_1 and Z_2 intersect properly at W, and let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be the ideals in $\mathcal{O}_{V,W}$ corresponding to Z_1 and Z_2 (so $\mathfrak{p}_i = (f_1, f_2, ..., f_r)$ if the f_j define Z_i in some open subset of V meeting W). The example of divisors on a surface suggests that we should set

$$(Z_1 \cdot Z_2)_W = \dim_k \mathcal{O}_{V,W}/(\mathfrak{p}_1, \mathfrak{p}_2),$$

but examples show this is not a good definition. Note that

$$\mathcal{O}_{V,W}/(\mathfrak{p}_1, \mathfrak{p}_2) = \mathcal{O}_{V,W}/\mathfrak{p}_1 \otimes_{\mathcal{O}_{V,W}} \mathcal{O}_{V,W}/\mathfrak{p}_2.$$

It turns out that we also need to consider the higher Tor terms. Set

$$\chi^{\mathcal{O}}(\mathcal{O}/\mathfrak{p}_1, \mathcal{O}/\mathfrak{p}_2) = \sum_{i=0}^{\dim V} (-1)^i \dim_k(Tor_i^{\mathcal{O}}(\mathcal{O}/\mathfrak{p}_1, \mathcal{O}/\mathfrak{p}_2)$$

where $\mathcal{O} = \mathcal{O}_{V,W}$. It is an integer ≥ 0, and $= 0$ if Z_1 and Z_2 do not intersect properly at W. When they do intersect properly, we define $(Z_1 \cdot Z_2)_W = mW$, $m = \chi^{\mathcal{O}}(\mathcal{O}/\mathfrak{p}_1, \mathcal{O}/\mathfrak{p}_2)$. When Z_1 and Z_2 are divisors on a surface, the higher Tor's vanish, and so this definition agrees with the previous one.

Now assume that V is projective. It is possible to define a notion of rational equivalence for cycles of codimension r: let W be an irreducible subvariety of codimension $r-1$, and let $f \in k(W)^\times$; then $div(f)$ is a cycle of codimension r on V (since W may not be normal, the definition of $div(f)$ requires care), and we let $C^r(V)'$ be the subgroup of $C^r(V)$ generated by such cycles as W ranges over all irreducible subvarieties of codimension $r-1$ and f ranges over all elements of $k(W)^\times$. Two cycles are said to be *rationally equivalent* if they differ by an element of $C^r(V)'$, and the quotient of $C^r(V)$ by $C^r(V)'$ is called the *Chow group* $CH^r(V)$. A discussion similar to that in the case of a surface leads to well-defined pairings

$$CH^r(V) \times CH^s(V) \to CH^{r+s}(V).$$

In general, we know very little about the Chow groups of varieties — for example, there has been little success at algebraic cycles on varieties other than the obvious one (divisors, intersections of divisors,...).

We can restate our definition of the degree of a variety in $\mathbb{P}^n$ as follows: a closed subvariety V of $\mathbb{P}^n$ of dimension d has degree $(V \cdot H)$ for any linear subspace of $\mathbb{P}^n$ of codimension d. (All linear subspaces of $\mathbb{P}^n$of codimension r are rationally equivalent, and so $(V \cdot H)$ is independent of the choice of H.)

REMARK 10.12. (Bezout's theorem). A divisor D on $\mathbb{P}^n$ is linearly equivalent of δH, where δ is the degree of D and H is any hyperplane. Therefore

$$(D_1 \cdot \cdots \cdot D_n) = \delta_1 \cdots \delta_n$$

where δ_j is the degree of D_j. For example, if C_1 and C_2 are curves in $\mathbb{P}^2$ defined by irreducible polynomials F_1 and F_2 of degrees δ_1 and δ_2 respectively, then C_1 and C_2 intersect in $\delta_1\delta_2$ points (counting multiplicities).

References:

Shafarevich 1994, IV.1, IV.2.

Fulton, W., Introduction to Intersection Theory in Algebraic Geometry, (AMS Publication; CBMS regional conference series #54.) This is a pleasant introduction.

Fulton, W., Intersection Theory. Springer, 1984. The ultimate source for everything to do with intersection theory.

Serre: Algèbre Locale, Multiplicités, Springer Lecture Notes, 11, 1957/58 (third edition 1975). This is where the definition in terms of Tor's was first suggested.

11. Coherent Sheaves; Invertible Sheaves.

Coherent Sheaves. Let $V = \operatorname{Specm} A$ be an affine variety over k, and let M be a finitely generated A-module. There is a unique sheaf of $\mathcal{O}_V$-modules $\mathcal{M}$ on V such that, for all $f \in A$,

$$\Gamma(D(f), \mathcal{M}) = M_f \quad (= A_f \otimes_A M).$$

The sheaf $\mathcal{M}$ is said to be *coherent*. A homomorphism $M \to N$ of A-modules defines a homomorphism $\mathcal{M} \to \mathcal{N}$ of $\mathcal{O}_V$-modules, and $M \mapsto \mathcal{M}$ is a fully faithful functor from the category of finitely generated A-modules to the category of coherent $\mathcal{O}_V$-modules, with quasi-inverse $\mathcal{M} \mapsto \Gamma(V, \mathcal{M})$.

Now consider a variety V. An $\mathcal{O}_V$-module $\mathcal{M}$ is said to be *coherent* if, for every open affine subset U of V, $\mathcal{M}|U$ is coherent. It suffices to check this condition for the sets in an open affine covering of V.

For example, $\mathcal{O}_V^n$ is a coherent $\mathcal{O}_V$-module. An $\mathcal{O}_V$-module $\mathcal{M}$ is said to be *locally free of rank n* if it is locally isomorphic to $\mathcal{O}_V^n$, i.e., if every point $P \in V$ has an open neighbourhood such that $\mathcal{M}|U \approx \mathcal{O}_V^n$. A locally free $\mathcal{O}_V$-module is coherent.

Let $v \in V$, and let $\mathcal{M}$ be a coherent $\mathcal{O}_V$-module. We define a $\kappa(v)$-module $\mathcal{M}(v)$ as follows: after replacing V with an open neighbourhood of v, we can assume that it is affine; hence we may suppose that $V = \operatorname{Specm}(A)$, that v corresponds to a maximal ideal $\mathfrak{m}$ in A (so that $\kappa(v) = A/\mathfrak{m}$), and $\mathcal{M}$ corresponds to the A-module M; we then define

$$\mathcal{M}(v) = M \otimes_A \kappa(v) = M/\mathfrak{m}M.$$

It is a finitely generated vector space over $\kappa(v)$. Don't confuse $\mathcal{M}(v)$ with the stalk $\mathcal{M}_v$ of $\mathcal{M}$ which, with the above notations, is $M_{\mathfrak{m}} = M \otimes_A A_{\mathfrak{m}}$. Thus $\mathcal{M}(v) = \mathcal{M}_v/\mathfrak{m}\mathcal{M}_v = \kappa(v) \otimes_{A_{\mathfrak{m}}} \mathcal{M}_{\mathfrak{m}}$. Nakayama's Lemma shows that

$$\mathcal{M}(v) = 0 \Rightarrow \mathcal{M}_v = 0.$$

The *support* of a coherent sheaf $\mathcal{M}$ is

$$Supp(\mathcal{M}) = \{v \in V \mid \mathcal{M}(v) \neq 0\} = \{v \in V \mid \mathcal{M}_v \neq 0\}.$$

Suppose V is affine, and that $\mathcal{M}$ corresponds to the A-module M. Let $\mathfrak{a}$ be the annihilator of M:

$$\mathfrak{a} = \{f \in A \mid fM = 0\}.$$

Then $M/\mathfrak{m}M \neq 0 \iff \mathfrak{m} \supset \mathfrak{a}$ (for otherwise $A/\mathfrak{m}A$ contains a nonzero element annihilating $M/\mathfrak{m}M$), and so

$$Supp(\mathcal{M}) = V(\mathfrak{a}).$$

Thus the support of a coherent module is a closed subset of V.

Note that if $\mathcal{M}$ is locally free of rank n, then $\mathcal{M}(v)$ is a vector space of dimension n for all v. There is a converse of this.

Proposition 11.1. *If $\mathcal{M}$ is a coherent $\mathcal{O}_V$-module such that $\mathcal{M}(v)$ has constant dimension n for all $v \in V$, then $\mathcal{M}$ is a locally free of rank n.*

PROOF. We may assume that V is affine, and that $\mathcal{M}$ corresponds to the finitely generated A-module M. Fix a maximal ideal $\mathfrak{m}$ of A, and let $x_1, \dots, x_n$be elements of M whose images in $M/\mathfrak{m}M$ form a basis for it over $\kappa(v)$. Consider the map

$$\gamma\colon A^n \to M, \quad (a_1, \dots, a_n) \mapsto \sum a_i x_i.$$

The cokernel is a finitely generated A-module whose support does not contain v. Therefore there is an element $f \in A$, $f \notin \mathfrak{m}$, such that γ defines a surjection $A_f^n \to M_f$. After replacing A with A_f we may assume that γ itself is surjective. For every maximal ideal $\mathfrak{n}$ of A, the map $(A/\mathfrak{n})^n \to M/\mathfrak{n}M$ is surjective, and hence (because of the condition on the dimension of $\mathcal{M}(v)$) bijective. Therefore, the kernel of γ is contained in $\mathfrak{n}^n$ (meaning $\mathfrak{n} \times \cdots \times \mathfrak{n}$) for all maximal ideals $\mathfrak{n}$ in A, and the next lemma shows that this implies that the kernel is zero. □

LEMMA 11.2. *Let A be an affine k-algebra. Then*

$$\cap \mathfrak{m} = 0 \text{ } \textit{(intersection of all maximal ideals in } A\textit{)}.$$

PROOF. Suppose first that k is algebraically closed. Recall (1.9) that if $\mathfrak{a}$ is a radical ideal in $k[X_1, \dots, X_n]$, then $IV(\mathfrak{a}) = \mathfrak{a}$. When we use the one-to-one correspondence between points of $V(\mathfrak{a})$ and the maximal ideals of $k[X_1, \dots, X_n]$ containing $\mathfrak{a}$, we see that this says that a function that is in every maximal ideal containing $\mathfrak{a}$ is, in fact, in $\mathfrak{a}$. On applying this statement to the ring $A = k[X_1, \dots, X_n]/\mathfrak{a}$, we obtain the lemma.

Now drop the assumption that k is algebraically closed, and consider a maximal ideal $\mathfrak{m}$ of $A \otimes_k k^{\text{al}}$. Then

$$A/\mathfrak{m} \cap A \hookrightarrow A \otimes_k k^{\text{al}} = k^{\text{al}}.$$

Therefore $A/\mathfrak{m} \cap A$ is an integral domain. Since it is finite-dimensional over k, it is a field, and so $\mathfrak{m} \cap A$ is a maximal ideal in A. Thus if $f \in A$ is in all maximal ideals of A, then its image in $A \otimes k^{\text{al}}$ is in all maximal ideals of A, then its image in $A \otimes k^{\text{al}}$ is in all maximal ideals of $A \otimes k^{\text{al}}$, and so is zero. □

For two coherent $\mathcal{O}_V$-modules $\mathcal{M}$ and $\mathcal{N}$, there is a unique coherent $\mathcal{O}_V$-module $\mathcal{M} \otimes_{\mathcal{O}_V} \mathcal{N}$ such that

$$\Gamma(U, \mathcal{M} \otimes_{\mathcal{O}_V} \mathcal{N}) = \Gamma(U, \mathcal{M}) \otimes_{\Gamma(U, \mathcal{O}_V)} \Gamma(U, \mathcal{N})$$

for all open affines $U \subset V$. The reader should be careful not to assume that this formula holds for nonaffine open subsets U (see example 11.4 below). For a such a U, one writes $U = \cup U_i$ with the U_i open affines, and defines $\Gamma(U, \mathcal{M} \otimes_{\mathcal{O}_V} \mathcal{N})$ to be the kernel of

$$\prod_i \Gamma(U_i, \mathcal{M} \otimes_{\mathcal{O}_V} \mathcal{N}) \rightrightarrows \prod_{i,j} \Gamma(U_{ij}, \mathcal{M} \otimes_{\mathcal{O}_V} \mathcal{N}).$$

Define $\mathcal{H}om(\mathcal{M}, \mathcal{N})$ to be the sheaf on V such that

$$\Gamma(U, \mathcal{H}om(\mathcal{M}, \mathcal{N})) = \mathcal{H}om_{\mathcal{O}_U}(\mathcal{M}, \mathcal{N})$$

(homomorphisms of $\mathcal{O}_U$-modules) for all open U in V. It is easy to see that this is a sheaf. If the restrictions of $\mathcal{M}$ and $\mathcal{N}$ to some open affine U correspond to A-modules

M and N, then

$$\Gamma(U, \mathcal{H}om(\mathcal{M}, \mathcal{N})) = \mathrm{Hom}_A(M, N),$$

and so $\mathcal{H}om(\mathcal{M}, \mathcal{N})$ is again a coherent $\mathcal{O}_V$-module.

Invertible sheaves. An *invertible sheaf* on V is a locally free $\mathcal{O}_V$-module $\mathcal{L}$ of rank 1. The tensor product of two invertible sheaves is again an invertible sheaf. In this way, we get a product structure on the set of isomorphism classes of invertible sheaves:

$$[\mathcal{L}] \cdot [\mathcal{L}'] = [\mathcal{L} \otimes \mathcal{L}'].$$

The product structure is associative and commutative (because tensor products are associative and commutative, up to a canonical isomorphism), and $[\mathcal{O}_V]$ is an identity element. Define

$$\mathcal{L}^\vee = \mathcal{H}om(\mathcal{L}, \mathcal{O}_V).$$

Clearly, $\mathcal{L}^\vee$ is free of rank 1 over any open set where $\mathcal{L}$ is free of rank 1, and so $\mathcal{L}^\vee$ is again an invertible sheaf. Moreover, the canonical map

$$\mathcal{L}^\vee \otimes \mathcal{L} \to \mathcal{O}_V, \quad (f, x) \mapsto f(x)$$

is an isomorphism (because it is obviously an isomorphism over any open subset where $\mathcal{L}$ is free). Thus

$$[\mathcal{L}^\vee][\mathcal{L}] = [\mathcal{O}_V].$$

For this reason, we often write $\mathcal{L}^{-1}$ for $\mathcal{L}^\vee$.

From these remarks, we see that the set of isomorphism classes of invertible sheaves on V is a group — it is called the *Picard group*, $Pic(V)$, of V.

We say that an invertible sheaf $\mathcal{L}$ is *trivial* if it is isomorphic to $\mathcal{O}_V$ — then $\mathcal{L}$ represents the zero element in $Pic(V)$.

PROPOSITION 11.3. *An invertible sheaf $\mathcal{L}$ on a complete variety V is trivial if and only if both it and its dual have nonzero global sections, i.e.,*

$$\Gamma(V, \mathcal{L}) \neq 0 \neq \Gamma(V, \mathcal{L}^\vee).$$

PROOF. We may assume that V is irreducible. Note first that, for any $\mathcal{O}_V$-module $\mathcal{M}$ on any variety V, the map

$$\mathrm{Hom}(\mathcal{O}_V, \mathcal{M}) \to \Gamma(V, \mathcal{M}), \quad \alpha \mapsto \alpha(1)$$

is an isomorphism.

Next recall that the only regular functions on a complete variety are the constant functions (see 5.28 in the case that k is algebraically closed), i.e., $\Gamma(V, \mathcal{O}_V) = k'$ where k' is the algebraic closure of k in $k(V)$. Hence $\mathcal{H}om(\mathcal{O}_V, \mathcal{O}_V) = k'$, and so a homomorphism $\mathcal{O}_V \to \mathcal{O}_V$ is either 0 or an isomorphism.

We now prove the proposition. The sections define nonzero homomorphisms

$$s_1 \colon \mathcal{O}_V \to \mathcal{L}, \quad s_2 : \mathcal{O}_V \to \mathcal{L}^\vee.$$

We can take the dual of the second homomorphism, and so obtain nonzero homomorphisms

$$\mathcal{O}_V \xrightarrow{s_1} \mathcal{L} \xrightarrow{s_2^\vee} \mathcal{O}_V.$$

The composite is nonzero, and hence an isomorphism, which shows that $s_2^\vee$ is surjective, and this implies that it is an isomorphism (for any ring A, a surjective homomorphism of A-modules $A \to A$ is bijective because 1 must map to a unit). □

Invertible sheaves and divisors. Now assume that V is nonsingular. For a divisor D on V, the vector space $L(D)$ is defined to be

$$L(D) = \{f \in k(V)^\times \mid \operatorname{div}(f) + D \geq 0\}.$$

We make this definition local: define $\mathcal{L}(D)$ to be the sheaf on V such that, for any open set U,

$$\Gamma(U, \mathcal{L}(D)) = \{f \in k(V)^\times \mid \operatorname{div}(f) + D \geq 0 \text{ on } U\} \cup \{0\}.$$

The condition "$\operatorname{div}(f)+D \geq 0$ on U" means that, if $D = \sum n_Z Z$, then $\operatorname{ord}_Z(f)+n_Z \geq 0$ for all Z with $Z \cap U \neq \emptyset$. Thus, $\Gamma(U, \mathcal{L}(D))$ is a $\Gamma(U, \mathcal{O}_V)$-module, and if $U \subset U'$, then $\Gamma(U', \mathcal{L}(D)) \subset \Gamma(U, \mathcal{L}(D))$. We define the restriction map to be this inclusion. In this way, $\mathcal{L}(D)$ becomes a sheaf of $\mathcal{O}_V$-modules.

Suppose D is principal on an open subset U, say $D|U = \operatorname{div}(g)$, $g \in k(V)^\times$. Then

$$\Gamma(U, \mathcal{L}(D)) = \{f \in k(V)^\times \mid \operatorname{div}(fg) \geq 0 \text{ on } U\} \cup \{0\}.$$

Therefore,

$$\Gamma(U, \mathcal{L}(D)) \to \Gamma(U, \mathcal{O}_V), \quad f \mapsto fg,$$

is an isomorphism. These isomorphisms clearly commute with the restriction maps for $U' \subset U$, and so we obtain an isomorphism $\mathcal{L}(D)|U \to \mathcal{O}_U$. Since every D is locally principal, this shows that $\mathcal{L}(D)$ is locally isomorphic to $\mathcal{O}_V$, i.e., that it is an invertible sheaf. If D itself is principal, then $\mathcal{L}(D)$ is trivial.

Next we note that the canonical map

$$\mathcal{L}(D) \otimes \mathcal{L}(D') \to \mathcal{L}(D + D'), \quad f \otimes g \mapsto fg$$

is an isomorphism on any open set where D and $D'$are principal, and hence it is an isomorphism globally. Therefore, we have a homomorphism

$$Div(V) \to Pic(V), \quad D \mapsto [\mathcal{L}(D)],$$

which is zero on the principal divisors.

Example 11.4. Let V be an elliptic curve, and let P be the point at infinity. Let D be the divisor $D = P$. Then $\Gamma(V, \mathcal{L}(D)) = k$, the ring of constant functions, but $\Gamma(V, \mathcal{L}(2D))$ contains a nonconstant function x. Therefore,

$$\Gamma(V, \mathcal{L}(2D)) \neq \Gamma(V, \mathcal{L}(D)) \otimes \Gamma(V, \mathcal{L}(D)),$$

— in other words, $\Gamma(V, \mathcal{L}(D) \otimes \mathcal{L}(D)) \neq \Gamma(U, \mathcal{L}(D) \otimes \mathcal{L}(D))$.

Proposition 11.5. *For an irreducible nonsingular variety, the map $D \mapsto [\mathcal{L}(D)]$ defines an isomorphism*

$$Div(V)/PrinDiv(V) \to Pic(V).$$

Proof. (Injectivity). If s is an isomorphism $\mathcal{O}_V \to \mathcal{L}(D)$, then $g = s(1)$ is an element of $k(V)^\times$ such that

(a) $\operatorname{div}(g) + D \geq 0$ (on the whole of V);

(b) if $\operatorname{div}(f) + D \geq 0$ on U, that is, if $f \in \Gamma(U, \mathcal{L}(D))$, then $f = h(g|U)$ for some $h \in \Gamma(U, \mathcal{O}_V)$.

Statement (a) says that $D \geq \operatorname{div}(-g)$ (on the whole of V). Suppose U is such that $D|U$ admits a local equation $f = 0$. When we apply (b) to $-f$, then we see that $\operatorname{div}(-f) \leq \operatorname{div}(g)$ on U, so that $D|U + \operatorname{div}(g) \geq 0$. Since the U's cover V, together with (a) this implies that $D = \operatorname{div}(-g)$.

(Surjectivity). Define

$$\Gamma(U, \mathcal{K}) = \begin{cases} k(V)^\times \text{ if } U \text{ is open an nonempty} \\ 0 \text{ if } U \text{ is empty.} \end{cases}$$

Because V is irreducible, $\mathcal{K}$ becomes a sheaf with the obvious restriction maps. On any open subset U where $\mathcal{L}|U \approx \mathcal{O}_U$, we have $\mathcal{L}|U \otimes \mathcal{K} \approx \mathcal{K}$. Since these open sets form a covering of V, V is irreducible, and the restriction maps are all the identity map, this implies that $\mathcal{L} \otimes \mathcal{K} \approx \mathcal{K}$ on the whole of V. Choose such an isomorphism, and identify $\mathcal{L}$ with a subsheaf of $\mathcal{K}$. On any U where $\mathcal{L} \approx \mathcal{O}_U$, $\mathcal{L}|U = g\mathcal{O}_U$ as a subsheaf of $\mathcal{K}$, where g is the image of $1 \in \Gamma(U, \mathcal{O}_V)$. Define D to be the divisor such that, on a U, g^{-1} is a local equation for D. □

Example 11.6. Suppose V is affine, say $V = \operatorname{Specm} A$. We know that coherent $\mathcal{O}_V$-modules correspond to finitely generated A-modules, but what do the locally free sheaves of rank n correspond to? They correspond to finitely generated *projective* A-modules (Bourbaki, Commutative Algebra, II.5.2). The invertible sheaves correspond to finitely generated projective A-modules of rank 1. Suppose for example that V is a curve, so that A is a Dedekind domain. This gives a new interpretation of the ideal class group: it is the group of isomorphism classes of finitely generated projective A-modules of rank one (i.e., such that $M \otimes_A K$ is a vector space of dimension one).

This can be proved directly. First show that every (fractional) ideal is a projective A-module — it is obviously finitely generated of rank one; then show that two ideals are isomorphic as A-modules if and only if they differ by a principal divisor; finally, show that every finitely generated projective A-module of rank 1 is isomorphic to a fractional ideal (by assumption $M \otimes_A K \approx K$; when we choose an identification $M \otimes_A K = K$, then $M \subset M \otimes_A K$ becomes identified with a fractional ideal). [Exercise: Prove the statements in this last paragraph.]

Remark 11.7. Quite a lot is known about $Pic(V)$, the group of divisors modulo linear equivalence, or of invertible sheaves up to isomorphism. For example, for any complete nonsingular variety V, there is an abelian variety P canonically attached to V, called the *Picard variety* of V, and an exact sequence

$$0 \to P(k) \to Pic(V) \to NS(V) \to 0$$

where $NS(V)$ is a finitely generated group called the Néron-Severi group.

Much less is known about algebraic cycles of codimension > 1, and about locally free sheaves of rank > 1 (and the two don't correspond exactly, although the Chern classes of locally free sheaves are algebraic cycles).

Direct images and inverse images of coherent sheaves. Consider a homomomorphism $A \to B$ of rings. From an A-module M, we get an B-module $B \otimes_A M$, which is finitely generated if M is finitely generated. Conversely, an B-module M

can also be considered an A-module, but it usually won't be finitely generated (unless B is finitely generated as an A-module). Both these operations extend to maps of varieties.

Consider a regular map $\alpha\colon W \to V$, and let $\mathcal{F}$ be a coherent sheaf of $\mathcal{O}_V$-modules. There is a unique coherent sheaf of $\mathcal{O}_W$-modules $\alpha^*\mathcal{F}$ with the following property: for any open affine subsets U' and U of W and V respectively such that $\alpha(U') \subset U$, $\alpha^*\mathcal{F}|U'$ is the sheaf corresponding to the $\Gamma(U', \mathcal{O}_W)$-module $\Gamma(U', \mathcal{O}_W) \otimes_{\Gamma(U,\mathcal{O}_V)} \Gamma(U, \mathcal{F})$.

Let $\mathcal{F}$ be a sheaf of $\mathcal{O}_V$-modules. For any open subset U of V, we define $\Gamma(U, \alpha_*\mathcal{F}) = \Gamma(\alpha^{-1}U, \mathcal{F})$, regarded as a $\Gamma(U, \mathcal{O}_V)$-module via the map $\Gamma(U, \mathcal{O}_V) \to \Gamma(\alpha^{-1}U, \mathcal{O}_W)$. Then $U \mapsto \Gamma(U, \alpha_*\mathcal{F})$ is a sheaf of $\mathcal{O}_V$-modules. In general, $\alpha_*\mathcal{F}$ will not be coherent, even when $\mathcal{F}$ is.

LEMMA 11.8. (a) *For any regular maps $U \xrightarrow{\alpha} V \xrightarrow{\beta} W$ and coherent $\mathcal{O}_W$-module $\mathcal{F}$ on W, there is a canonical isomorphism*

$$(\beta\alpha)^*\mathcal{F} \xrightarrow{\approx} \alpha^*(\beta^*\mathcal{F}).$$

(b) *For any regular map $\alpha\colon V \to W$, α^* maps locally free sheaves of rank n to locally free sheaves of rank n (hence also invertible sheaves to invertible sheaves). It preserves tensor products, and, for an invertible sheaf $\mathcal{L}$, $\alpha^*(\mathcal{L}^{-1}) \cong (\alpha^*\mathcal{L})^{-1}$.*

PROOF. (a) This follows from the fact that, given homomorphisms of rings $A \to B \to T$, $T \otimes_B (B \otimes_A M) = T \otimes_A M$.

(b) This again follows from well-known facts about tensor products of rings. □

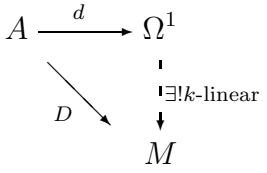
12. Differentials

In this section, we sketch the theory of differentials. We allow k to be an arbitrary field.

Let A be a k-algebra, and let M be an A-module. Recall (from §4) that a k-derivation is a k-linear map $D : A \to M$ such that

$$D(fg) = f \circ Dg + g \circ Df \text{ (Leibniz's rule).}$$

A pair $(\Omega^1_{A/k}, d)$ comprising an A-module $\Omega^1_{A/k}$ and a k-derivation $d : A \to \Omega^1_{A/k}$ is called the *module of differential one-forms* for A over k^{al} if it is universal:



Example 12.1. Let $A = k[X_1, ..., X_n]$; then $\Omega^1_{A/k}$ is the free A-module with basis the symbols $dX_1, ..., dX_n$, and $df = \sum \partial f/\partial X_i \cdot dX_i$.

Example 12.2. Let $A = k[X_1, ..., X_n]/\mathfrak{a}$; then $\Omega^1_{A/k}$ is the free A-module with basis the symbols $dX_1, ..., dX_n$ modulo the relations: $df = 0$ for all $f \in \mathfrak{a}$.

Proposition 12.3. *Let V be a variety. For each $n \geq 0$, there is a unique sheaf of $\mathcal{O}_V$-modules $\Omega^n_{V/k}$ on V such that $\Omega^n_{V/k}(U) = \Lambda^n \Omega^1_{A/k}$ whenever $U = \operatorname{Specm} A$ is an open affine of V.*

Proof. Omitted. □

The sheaf $\Omega^n_{V/k}$ is called the *sheaf of differential n-forms* on V.

Example 12.4. Let E be the affine curve

$$Y^2 = X^3 + aX + b,$$

and assume $X^3 + aX + b$ has no repeated roots (so that E is nonsingular). Write x and y for regular functions on E defined by X and Y. On the open set $D(y)$ where $y \neq 0$, let $\omega_1 = dx/y$, and on the open set $D(3x^2 + a)$, let $\omega_2 = 2dy/(3x^2 + a)$. Since $y^2 = x^3 + ax + b$,

$$2ydy = (3x^2 + a)dx.$$

and so ω_1 and ω_2 agree on . Since $E = D(y) \cap D(3x^2 + a)$, we see that there is a differential ω on E whose restrictions to $D(y)$ and $D(3x^2 + a)$ are ω_1 and ω_2 respectively. It is an easy exercise in working with projective coordinates to show that ω extends to a differential one-form on the whole projective curve

$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

In fact, $\Omega^1_{C/k}(C)$ is a one-dimensional vector space over k, with ω as basis. More generally, if C is a complete nonsingular absolutely irreducible curve of genus g, then $\Omega^1_{C/k}C)$ is a vector space of dimension g over k. Note that $\omega = dx/y = dx/(x^3 + ax + b)^{\frac{1}{2}}$, which can't be integrated in terms of elementary functions. Its integral is called an elliptic integral (integrals of this form arise when one tries to find the arc length

of an ellipse). The study of elliptic integrals was one of the starting points for the study of algebraic curves.

PROPOSITION 12.5. *If V is nonsingular, then $\Omega^1_{V/k}$ is a locally free sheaf of rank* $\dim(V)$ *(that is, every point P of V has a neighbourhood U such that $\Omega^1_{V/k}|U \approx (\mathcal{O}_V|U)^{\dim(V)}$).*

PROOF. Omitted. □

Let C be a complete nonsingular absolutely irreducible curve, and let ω be a nonzero element of $\Omega^1_{k(C)/k}$. We define the divisor (ω) of ω as follows: let $P \in C$; if t is a uniformizing parameter at P, then dt is a basis for $\Omega^1_{k(C)/k}$ as a $k(C)$-vector space, and so we can write $\omega = fdt$, $f \in k(V)^\times$; define $ord_P(\omega) = ord_P(f)$, and $(\omega) = \sum ord_P(\omega)P$. Because $k(C)$ has transcendence degree 1 over k, $\Omega^1_{k(C)/k}$ is a $k(C)$-vector space of dimension one, and so the divisor (ω) is independent of the choice of ω up to linear equivalence. By an abuse of language, one calls (ω) for any nonzero element of $\Omega^1_{k(C)/k}$ a *canonical class* K on C. For a divisor D on C, let $\ell(D) = \dim_k(L(D))$.

THEOREM 12.6 (Riemann-Roch). *Let C be a complete nonsingular absolutely irreducible curve over k.*

(a) *The degree of a canonical divisor is* $2g - 2$.
(b) *For any divisor D on C,*

$$\ell(D) - \ell(K - D) = 1 + g - \deg(D).$$

More generally, if V is a smooth complete variety of dimension d, it is possible to associate with the sheaf of differential d-forms on V a canonical linear equivalence class of divisors K. This divisor class determines a rational map to projective space, called the *canonical map.*

References

Shafarevich, 1994, III.5.

Mumford 1966, III.4.

13. Algebraic Varieties over the Complex Numbers

It is not hard to show that there is a unique way to endow all algebraic varieties over $\mathbb{C}$ with a topology such that:

(a) on $\mathbb{A}^n = \mathbb{C}^n$ it is just the usual complex topology;
(b) on closed subsets of $\mathbb{A}^n$ it is the induced toplogy;
(c) all morphisms of algebraic varieties are continuous;
(d) it is finer than the Zariski topology.

We call this new topology the *complex topology* on V. Note that (a), (b), and (c) determine the topology uniquely for affine algebraic varieties ((c) implies that an isomorphism of algebraic varieties will be a homeomorphism for the complex topology), and (d) then determines it for all varieties.

Of course, the complex topology is *much* finer than the Zariski topology — this can be seen even on $\mathbb{A}^1$. In view of this, the next proposition is little surprising.

Proposition 13.1. *Let V be an algebraic variety over $\mathbb{C}$, and let C be a constructible subset of V (in the Zariski topology); then the closure of C in the Zariski topology equals its closure in the complex topology.*

Proof. Omitted. □

For example, if U is an open dense subset of a closed subset Z of V (both for the Zariski topology), then U is also dense in Z for the complex topology.

The next result helps explain why completeness is the analogue of compactness for topological spaces.

Proposition 13.2. *Let V be an algebraic variety over $\mathbb{C}$; then V is complete (as an algebraic variety) if and only if it is compact for the complex topology.*

Proof. Omitted. □

In general, there are many more holomorphic (complex analytic) functions than there are polynomial functions on a variety over $\mathbb{C}$. For example, by using the exponential function it is possible to construct many holomorphic functions on $\mathbb{C}$ that are not polynomials in z, but all these functions have nasty singularities at the point at infinity on the Riemann sphere. In fact, the only meromorphic functions on the Riemann sphere are the rational functions. This generalizes.

Theorem 13.3. *Let V be a complete nonsingular variety over $\mathbb{C}$. Then V is, in a natural way, a complex manifold, and the field of meromorphic functions on V (as a complex manifold) is equal to the field of rational functions on V.*

Proof. Omitted. □

This provides one way of constructing compact complex manifolds that are not algebraic varieties: find such a manifold M of dimension n such that the transcendence degree of the field of meromorphic functions on M is $< n$. For a torus $\mathbb{C}^g/\Lambda$ of dimension $g \geq 1$, this is typically the case. However, when the transcendence degree of the field of meromorphic functions is equal to the dimension of manifold, then M can be given the structure, not necessarily of an algebraic variety, but of something

more general, namely, that of an *algebraic space*. Roughly speaking, an algebraic space is an object that is locally an affine algebraic variety, where locally means for the étale "topology" rather than the Zariski topology.

One way to show that a complex manifold is algebraic is to embed it into projective space.

THEOREM 13.4. *Any closed analytic submanifold of $\mathbb{P}^n$ is algebraic.*

PROOF. Omitted. □

COROLLARY 13.5. *Any holomorphic map from one projective algebraic variety to a second projective algebraic variety is algebraic.*

PROOF. Let $\varphi\colon V \to W$ be the map. Then the graph Γ_φ of φ is a closed subset of $V \times W$, and hence is algebraic according to the theorem. Since φ is the composite of the isomorphism $V \to \Gamma_\varphi$ with the projection $\Gamma_\varphi \to W$, and both are algebraic, φ itself is algebraic. □

Since, in general, it is hopeless to write down a set of equations for a variety (it is a fairly hopeless task even for an abelian variety of dimension 3), the most powerful way we have for constructing varieties is to first construct a complex manifold and then prove that it has a natural structure as a algebraic variety. Sometimes one can then show that it has a canonical model over some number field, and then it is possible to reduce the equations defining it modulo a prime of the number field, and obtain a variety in characteristic p.

For example, it is known that $\mathbb{C}^g/\Lambda$ (Λ a lattic in $\mathbb{C}^g$) has the structure of an algebraic variety if and only if there is a skew-symmetric form ψ on $\mathbb{C}^g$ having certain simple properties relative to Λ. The variety is then an abelian variety, and all abelian varieties over $\mathbb{C}$ are of this form.

References

Mumford 1966, I.10.

Shafarevich 1994, Book 3.

14. Further Reading

In this course, we have associated an affine algebraic variety to any affine algebra over a field k. For many reasons, for example, in order to be able to study the reduction of varieties to characteristic $p \neq 0$, Grothendieck realized that it is important to attach a geometric object to *every* commutative ring. Unfortunately, $A \mapsto \operatorname{specm} A$ is not functorial in this generality: if $\alpha\colon A \to B$ is a homomorphism of rings, then $\alpha^{-1}(\mathfrak{m})$ for $\mathfrak{m}$ maximal need not be maximal — consider for example the inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$. Thus he was forced to replace $\operatorname{specm}(A)$ with $\operatorname{spec}(A)$, the set of all prime ideals in A. He then attaches an affine *scheme* $\operatorname{Spec}(A)$ to each ring A, and defines a scheme to be a locally ringed space that admits an open covering by affine schemes.

There is a natural functor $V \mapsto V^*$ from the category of varieties over k to the category of absolutely reduced schemes of finite-type over k, which is an equivalence of categories. To construct V^* from V, one only has to add one point for each irreducible closed subvariety of V. Then $U \mapsto U^*$ is a bijection from the set of open subsets of V to the set of open subsets of V^*. Moreover, $\Gamma(U^*, \mathcal{O}_{V^*}) = \Gamma(U, \mathcal{O}_V)$ for each open subset U of V. Therefore the topologies and sheaves on V and V^* are the same — only the underlying sets differ.

Every aspiring algebraic and (especially) arithmetic geometer needs to learn the basic theory of schemes, and for this I recommend reading Chapters II and III of Hartshorne 1997.

Among the books listed below, I especially recommend Shafarevich 1994 — it is very easy to read, and is generally more elementary than these notes, but covers more ground (being much longer).

Commutative Algebra

Atiyah, M.F and MacDonald, I.G., Introduction to Commutative Algebra, Addison-Wesley 1969. This is the most useful short text. It extracts the essence of a good part of Bourbaki 1961–83.

Bourbaki, N., Algèbre Commutative, Chap. 1–7, Hermann, 1961–65; Chap 8–9, Masson, 1983. Very clearly written, but it is a reference book, not a text book.

Eisenbud, D., Commutative Algebra, Springer, 1995. The emphasis is on motivation.

Nagata, M., Local Rings, Wiley, 1962. Contains much important material, but it is concise to the point of being almost unreadable.

Reid, M., Undergraduate Commutative Algebra, Cambridge 1995. According to the author, it covers roughly the same material as Chapters 1–8 of Atiyah and MacDonald 1969, but is cheaper, has more pictures, and is considerably more opinionated. (However, Chapters 10 and 11 of Atiyah and MacDonald 1969 contain crucial material.)

Serre: Algèbre Locale, Multiplicités, Lecture Notes in Math. 11, Springer, 1957/58 (third edition 1975).

Zariski, O., and Samuel, P., Commutative Algebra, Vol. I 1958, Vol II 1960, van Nostrand. Very detailed and well organized.

Elementary Algebraic Geometry

Reid, M., Undergraduate Algebraic Geometry. A brief, elementary introduction. The final section contains an interesting, but idiosyncratic, account of algebraic geometry in the twentieth century.

Abhyankar, S., Algebraic Geometry for Scientists and Engineers, AMS, 1990. Mainly curves, from a very explicit and down-to-earth point of view.

Computational Algebraic Geometry

Cox, D., Little, J., O'Shea, D., Ideals, Varieties, and Algorithms, Springer, 1992. This gives an algorithmic approach to algebraic geometry, which makes everything very down-to-earth and computational, but the cost is that the book doesn't get very far in 500pp.

Subvarieties of Projective Space

Shafarevich, I., Basic Algebraic Geometry, Book 1, Springer, 1994. Very easy to read.

Harris, Joe: Algebraic Geometry: A first course, Springer, 1992. The emphasis is on examples.

Algebraic Geometry over the Complex Numbers

Griffiths, P., and Harris, J., Principles of Algebraic Geometry, Wiley, 1978. A comprehensive study of subvarieties of complex projective space using heavily analytic methods.

Mumford, D., Algebraic Geometry I: Complex Projective Varieties. The approach is mainly algebraic, but the complex topology is exploited at crucial points.

Shafarevich, I., Basic Algebraic Geometry, Book 3, Springer, 1994.

Abstract Algebraic Varieties

Dieudonné, J., Cours de Géometrie Algébrique, 2, PUF, 1974. A brief introduction to abstract algebraic varieties over algebraically closed fields.

Kempf, G., Algebraic Varieties, Cambridge, 1993. Similar approach to these notes, but is more concisely written, and includes two sections on the cohomology of coherent sheaves.

Kunz, E., Introduction to Commutative Algebra and Algebraic Geometry, Birkhaüser, 1985. Similar approach to these notes, but includes more commutative algebra and has a long chapter discussing how many equations it takes to describe an algebraic variety.

Mumford, D. Introduction to Algebraic Geometry, Harvard notes, 1966. Notes of a course written (as I recall) by W. Waterhouse. Apart from the original treatise (Grothendieck and Dieudonné 1960–67), this was the first place one could learn the new approach to algebraic geometry. The first chapter is on varieties, and last two on schemes.

Mumford, David: The Red Book of Varieties and Schemes, Lecture Notes in Math. 1358, Springer, 1988. Reprint of Mumford 1966.

Schemes

Eisenbud, D., and Harris, J., Schemes: the language of modern algebraic geometry, Wadsworth, 1992. A brief elementary introduction to scheme theory.

Grothendieck, A., and Dieudonné, J., Eléments de Géométrie Algébrique. Publ. Math. IHES 1960–1967. This was intended to cover everything in algebraic geometry in 13 massive books, that is, it was supposed to do for algebraic geometry what Euclid's "Elements" did for geometry. Unlike the earlier Elements, it was abandoned after 4 books. It is an extremely useful reference.

Hartshorne, R., Algebraic Geometry, Springer 1977. Chapters II and III give an excellent account of scheme theory and cohomology, so good in fact, that no one seems willing to write a competitor. The first chapter on varieties is very sketchy.

Iitaka, S. Algebraic Geometry: an introduction to birational geometry of algebraic varieties, Springer, 1982. Not as well-written as Hartshorne 1977, but it is more elementary, and it covers some topics that Hartshorne doesn't.

Shafarevich, I., Basic Algebraic Geometry, Book 2, Springer, 1994. A brief introduction to schemes and abstract varieties.

History

Dieudonné, J., History of Algebraic Geometry, Wadsworth, 1985.

Of Historical Interest

Hodge, W., and Pedoe, D., Methods of Algebraic Geometry, Cambridge, 1947–54.

Lang, S., Introduction to Algebraic Geometry, Interscience, 1958. An introduction to Weil 1946.

Weil, A., Foundations of Algebraic Geometry, AMS, 1946; Revised edition 1962. This is where Weil laid the foundations for his work on abelian varieties and jacobian varieties over arbitrary fields, and his proof of the analogue of the Riemann hypothesis for curves and abelian varieties. Unfortunately, not only does its language differ from the current language of algebraic geometry, but it is incompatible with it.

There is also a recent book by Kenji Ueno, which I haven't seen.

J.S. Milne, Mathematics Department, University of Michigan, Ann Arbor, MI 48109.

affine algebra, 36, 132
affine subvariety, 44
algebra
  finite, 5
  finite-type, 5
algebraic group, 53
algebraic prevariety, 44
algebraic set, 14
algebraic space, 152

basic open subset, 22
Bezout's Theorem, 98, 142
birationally equivalent, 72

category, 56
characteristic exponent, 132
Chinese Remainder Theorem, 102
Chow group, 141
complete intersection
  ideal-theoretic, 114
  local, 114
  set-theoretic, 114
complex topology, 151
constructible set, 117
cusp, 61
cycle
  algebraic, 141

degree
  of a map, 122, 140
  of a point, 135
  total, 5
derivation, 75
Dickson's Lemma, 10
differential, 62
dimension, 24, 25, 55
division algorithm, 7
divisor, 137
  effective, 137
  local equation for, 138
  locally principal, 138
  positive, 137
  prime, 137
  principal, 137
  restriction of, 138
  support of, 137
dominating map, 58

elliptic curve, 14, 81, 134
equivalence of categories, 38
etale, 65, 79
etale neighbourhood, 75

fibred product, 106
field
  algebraically closed, 3
field of rational functions, 24, 55
finite map, 101
Frobenius map, 41
functor, 57

Groebner basis, *see also* standard basis

Hilbert Basis Theorem, 10, 15
Hilbert Nullstellensatz, 17
  strong, 19
Hilbert polynomial, 99
homogeneous coordinate ring, 86
homomorphism
  of algebras, 5
  of sheaves, 131
hypersurface, 24, 90
hypersurface section, 90

ideal, 4
  homogeneous, 81
  maximal, 4
  monomial, 9
  prime, 4
immersion, 47
  closed, 47
  open, 47
integral, 26
integral closure, 27
integrally closed, 28
intersect properly, 138, 139, 141
irreducible components, 23
irreducible topological space, 22

Krull dimension, 26

leading coefficient, 7
leading monomial, 7
leading term, 7
linearly equivalent, 137
local system of parameters, 74

manifold
  complex, 44
  differentiable, 44
  topological, 44
monomial, 5
morphism
  of affine algebraic varieties, 36
  of ringed spaces, 35
multidegree, 7
multiplicative subset, 31
multiplicity
  of a point, 61

Nakayama's Lemma, 69
node, 61
Noether Normalization Theorem, 104, 136
Noetherian, 21
nondegenerate quadric, 128
nonsingular, 59, 63, 71, 136
normal, 71

ordering
  grevlex, 7
  lex, 6

pencil of lines, 128
Picard group, 137, 145
Picard variety, 147
point
  with coordinates in a ring, 56
point with coordinates in a ring, 76
polynomial
  elementary symmetric, 26
  homogeneous, 80
  irreducible, 6
  symmetric, 26
presheaf, 131
prevariety, 134
Prime Avoidance Lemma, 113
principal open subset, 22
product
  of affine varieties, 52
  of algebraic varieties, 52
projection with centre, 92
projective algebraic set, 80
projectively normal, 137
pure dimension, 25

quasi-compact, 21
quasi-inverse, 38

rational function, 35
rational variety, 73
rationally equivalent, 141
regular function, 33, 37, 44
regular map, 36, 45
resultant, 95
Riemann-Roch Theorem, 150
ring
  coordinate, 21
  Noetherian, 5
  of regular functions, 21
ring of dual numbers, 75
ringed space, 30, 131
  locally, 131

section of a sheaf, 30
Segre mapping, 91
semisimple
  group, 77
  Lie algebra, 77
separable map, 124
separated, 46, 134
sheaf, 131
  coherent, 143
  invertible, 145
  locally free, 143
  of algebras, 30
  support of, 143
singular locus, 72, 136
smooth, 59, 63
stalk, 131
standard basis, 10
  minimal, 11
Stein factorization, 130

tangent cone, 60, 78
  geometric, 60, 78, 79
tangent space, 59, 62, 68
tensor product, 49

unirational variety, 73

variety, 134
  abelian, 53, 97
  affine algebraic, 36
  algebraic, 46
  complete, 93, 136
  degree of,, 98
  Grassmanian, 98
  normal, 123, 137
  projective, 80
  quasi-projective, 80
Veronese mapping, 89

Yoneda Lemma, 58

Zariski topology, 16
Zariski's Lemma, 17
Zariski's Main Theorem, 105