Algebraic Geometry

J.S. Milne

Version 5.20
September 14, 2009

A more recent version of these notes is available at www.jmilne.org/math/

These notes are an introduction to the theory of algebraic varieties. In contrast to most such accounts they study abstract algebraic varieties, and not just subvarieties of affine and projective space. This approach leads more naturally into scheme theory.


```
BibTeX information
@misc{milneAG,
  author={Milne, James S.},
  title={Algebraic Geometry (v5.20)},
  year={2009},
  note={Available at www.jmilne.org/math/},
  pages={239+vi}
}
```

v2.01 (August 24, 1996). First version on the web.
v3.01 (June 13, 1998).
v4.00 (October 30, 2003). Fixed errors; many minor revisions; added exercises; added two sections/chapters; 206 pages.
v5.00 (February 20, 2005). Heavily revised; most numbering changed; 227 pages.
v5.10 (March 19, 2008). Minor fixes; TeX style changed, so page numbers changed; 241 pages.
v5.20 (September 14, 2009). Minor corrections; revised Chapters 1, 11, 16; 245 pages.

Available at www.jmilne.org/math/
Please send comments and corrections to me at the address on my web page.

The photograph is of Lake Sylvan, New Zealand.

Contents

Notations

We use the standard (Bourbaki) notations: $\mathbb{N} = \{0, 1, 2, \ldots\}$, $\mathbb{Z}$ = ring of integers, $\mathbb{R}$ = field of real numbers, $\mathbb{C}$ = field of complex numbers, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ = field of p elements, p a prime number. Given an equivalence relation, $[*]$ denotes the equivalence class containing $*$. A family of elements of a set A indexed by a second set I, denoted $(a_i)_{i \in I}$, is a function $i \mapsto a_i : I \to A$.

A field k is said to be separably closed if it has no finite separable extensions of degree > 1. We use k^{sep} and k^{al} to denote separable and algebraic closures of k respectively.

All rings will be commutative with 1, and homomorphisms of rings are required to map 1 to 1. For a ring A, $A^\times$ is the group of units in A:

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

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

$X \overset{\text{def}}{=} Y$	X is defined to be Y, or equals Y by definition;
$X \subset Y$	X is a subset of Y (not necessarily proper, i.e., X may equal Y);
$X \approx Y$	X and Y are isomorphic;
$X \simeq Y$	X and Y are canonically isomorphic (or there is a given or unique isomorphism).

Prerequisites

The reader is assumed to be familiar with the basic objects of algebra, namely, rings, modules, fields, and so on, and with transcendental extensions of fields (FT, Section 8).

References

Atiyah and MacDonald 1969: Introduction to Commutative Algebra, Addison-Wesley.
Cox et al. 1992: Varieties, and Algorithms, Springer.
FT: Milne, J.S., Fields and Galois Theory, v4.20, 2008 (www.jmilne.org/math/).
CA: Milne, J.S., Commutative Algebra, v2.10.
Hartshorne 1977: Algebraic Geometry, Springer.
Mumford 1999: The Red Book of Varieties and Schemes, Springer.
Shafarevich 1994: Basic Algebraic Geometry, Springer.

For other references, see the annotated bibliography at the end.

Acknowledgements

I thank the following for providing corrections and comments on earlier versions of these notes: Sandeep Chellapilla, Umesh V. Dubey, Shalom Feigelstock, B.J. Franklin, Sergei Gelfand, Daniel Gerig, Darij Grinberg, Lucio Guerberoff, Guido Helmers, Christian Hirsch, Jasper Loy Jiabao, Lars Kindler, Sean Rostami, David Rufino, Tom Savage, Nguyen Quoc Thang, Soli Vishkautsan, Dennis Bouke Westra, and others.

Introduction

There is almost nothing left to discover in geometry.
Descartes, March 26, 1619

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

$$\sum_{j=1}^{n} a_{ij} X_j = b_i, \quad i = 1, \ldots, m, \tag{1}$$

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

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

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.

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 topology the study of infinitely differentiable functions and the spaces on which they are defined (differentiable manifolds), and so on:

algebraic geometry	regular (polynomial) functions	algebraic varieties
topology	continuous functions	topological spaces
differential topology	differentiable functions	differentiable manifolds
complex analysis	analytic (power series) functions	complex manifolds.

The approach adopted in this course makes plain the similarities between these different areas of mathematics. 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

$$\frac{d}{dX} \sum a_i X^i = \sum i a_i X^{i-1}.$$

[1] For example, suppose that the system (1) has coefficients $a_{ij} \in k$ and that K is a field containing k. Then (1) 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!)

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

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

$$f(x, y, z) = C \tag{2}$$

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

$$\left(\frac{\partial f}{\partial x}\right)_P (x-a) + \left(\frac{\partial f}{\partial y}\right)_P (y-b) + \left(\frac{\partial f}{\partial z}\right)_P (z-c) = 0. \tag{3}$$

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

Consider a nonzero polynomial $f(x, y, z)$ with coefficients in a field k. In this course, we shall learn that the equation (2) defines a surface in k^3, and we shall use the equation (3) 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 is that $1/X$ is not the derivative of any rational function of X, and nor is X^{np-1} in characteristic $p \neq 0$ — these functions can not be integrated in the ring of polynomial functions.

The first ten chapters of the notes form a basic course on algebraic geometry. In these chapters we generally assume that the ground field is algebraically closed in order to be able to concentrate on the geometry. The remaining chapters treat more advanced topics, and are largely independent of one another except that chapter 11 should be read first.

The approach to algebraic geometry taken in these notes

In differential geometry it is important to define differentiable manifolds abstractly, i.e., not as submanifolds of some Euclidean space. For example, it is difficult even to make sense of a statement such as "the Gauss curvature of a surface is intrinsic to the surface but the principal curvatures are not" without the abstract notion of a surface.

Until the mid 1940s, algebraic geometry was concerned only with algebraic subvarieties of affine or projective space over algebraically closed fields. Then, in order to give substance to his proof of the congruence Riemann hypothesis for curves an abelian varieties, Weil was forced to develop a theory of algebraic geometry for "abstract" algebraic varieties over arbitrary fields,[3] but his "foundations" are unsatisfactory in two major respects:

- Lacking a topology, his method of patching together affine varieties to form abstract varieties is clumsy.
- His definition of a variety over a base field k is not intrinsic; specifically, he fixes some large "universal" algebraically closed field Ω and defines an algebraic variety over k to be an algebraic variety over Ω with a k-structure.

In the ensuing years, several attempts were made to resolve these difficulties. In 1955, Serre resolved the first by borrowing ideas from complex analysis and defining an algebraic

[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 $(\nabla f)_P$ of f at P.

[3] Weil, André. Foundations of algebraic geometry. American Mathematical Society, Providence, R.I. 1946.

variety over an algebraically closed field to be a topological space with a sheaf of functions that is locally affine.[4] Then, in the late 1950s Grothendieck resolved all such difficulties by introducing his theory of schemes.

In these notes, we follow Grothendieck except that, by working only over a base field, we are able to simplify his language by considering only the closed points in the underlying topological spaces. In this way, we hope to provide a bridge between the intuition given by differential geometry and the abstractions of scheme theory.

[4]Serre, Jean-Pierre. Faisceaux algébriques cohérents. Ann. of Math. (2) 61, (1955). 197–278.

Chapter 1

Preliminaries

In this chapter, we review some definitions and basic results in commutative algebra and category theory, and we derive some algorithms for working in polynomial rings.

Rings and algebras

Let A be a ring. A ***subring*** of A is a subset that contains 1_A and is closed under addition, multiplication, and the formation of negatives. 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 $a \in A$.

Elements $x_1, \ldots, x_n$ of an A-algebra B are said to ***generate*** it if every element of B can be expressed as a polynomial in the x_i with coefficients in $i_B(A)$, i.e., if the homomorphism of A-algebras $A[X_1, \ldots, X_n] \to B$ acting as i_A on A and sending X_i to x_i is surjective. We then write $B = (i_B A)[x_1, \ldots, x_n]$.

A ring homomorphism $A \to B$ is said to be of ***finite-type***, and B is a ***finitely generated*** A-algebra if B is generated by a finite set of elements as an A-algebra.

A ring homomorphism $A \to B$ is ***finite***, and B is a ***finite***[1] A-algebra, if B is finitely generated as an A-module.

Let k be a field, and let A be a k-algebra. When $1_A \neq 0$ in A, 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. When $1_A = 0$ in a ring A, then A is the zero ring, i.e., $A = \{0\}$.

Let $A[X]$ be the polynomial ring in the symbol X with coefficients in A. If A is an integral domain, then $\deg(fg) = \deg(f) + \deg(g)$, and it follows that $A[X]$ is also an integral domain; moreover, $A[X]^\times = A^\times$.

Ideals

Let A be a ring. 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) $a \in \mathfrak{a}, r \in A \Rightarrow ra \in \mathfrak{a}$.

The ***ideal generated by a subset*** S of A is the intersection of all ideals $\mathfrak{a}$ containing S — it is easy to verify that this is in fact an ideal, and that it consists of all finite sums of the

[1] The term "module-finite" is also used.

form $\sum r_i s_i$ with $r_i \in A$, $s_i \in S$. The ideal generated by the empty set is the zero ideal $\{0\}$. When $S = \{s_1, s_2, \ldots\}$, we shall write $(s_1, s_2, \ldots)$ 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 $\mathfrak{ab}$. 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 $\mathfrak{a} = (a_1, \ldots, a_m)$ and $\mathfrak{b} = (b_1, \ldots, b_n)$, then $\mathfrak{ab} = (a_1 b_1, \ldots, a_i b_j, \ldots, a_m b_n)$. Note that

$$\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}. \tag{4}$$

The kernel of a homomorphism $A \to B$ is an ideal in A. Conversely, for any ideal $\mathfrak{a}$ in 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 $\varphi\colon A \to A/\mathfrak{a}$ whose kernel is $\mathfrak{a}$. 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 $\mathfrak{p}$ is ***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. Note that if $\mathfrak{p}$ is prime and $a_1 \cdots a_n \in \mathfrak{p}$, then at least one of the $a_i \in \mathfrak{p}$.

An ideal $\mathfrak{m}$ in A is ***maximal*** if it is maximal among the proper ideals of A. Thus $\mathfrak{m}$ is maximal if and only if $A/\mathfrak{m}$ is nonzero and has no proper nonzero ideals, and so is a field. Note that

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

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 $(a, 0) = (1, 0)(a, b) \in \mathfrak{c}$ and $(0, b) = (0, 1)(a, b) \in \mathfrak{c}$. Therefore, $\mathfrak{c} = \mathfrak{a} \times \mathfrak{b}$ with

$$\mathfrak{a} = \{a \mid (a, 0) \in \mathfrak{c}\}, \quad \mathfrak{b} = \{b \mid (0, b) \in \mathfrak{c}\}.$$

THEOREM 1.1 (CHINESE REMAINDER THEOREM). *Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ 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*

$$A \to A/\mathfrak{a}_1 \times \cdots \times A/\mathfrak{a}_n \tag{5}$$

is surjective, with kernel $\prod \mathfrak{a}_i = \bigcap \mathfrak{a}_i$.

PROOF. Suppose first that $n = 2$. As $\mathfrak{a}_1 + \mathfrak{a}_2 = A$, there exist $a_i \in \mathfrak{a}_i$ such that $a_1 + a_2 = 1$. Then $x = a_1 x_2 + a_2 x_1$ maps to $(x_1 \bmod \mathfrak{a}_1, x_2 \bmod \mathfrak{a}_2)$, which shows that (5) is surjective.

For each i, there exist elements $a_i \in \mathfrak{a}_1$ and $b_i \in \mathfrak{a}_i$ such that

$$a_i + b_i = 1, \text{ all } i \geq 2.$$

The product $\prod_{i \geq 2}(a_i + b_i) = 1$, and lies in $\mathfrak{a}_1 + \prod_{i \geq 2} \mathfrak{a}_i$, and so

$$\mathfrak{a}_1 + \prod\nolimits_{i \geq 2} \mathfrak{a}_i = A.$$

We can now apply the theorem in the case $n = 2$ to obtain an element y_1 of A such that

$$y_1 \equiv 1 \bmod \mathfrak{a}_1, \quad y_1 \equiv 0 \bmod \prod\nolimits_{i \geq 2} \mathfrak{a}_i.$$

These conditions imply

$$y_1 \equiv 1 \bmod \mathfrak{a}_1, \quad y_1 \equiv 0 \bmod \mathfrak{a}_j, \text{ all } j > 1.$$

Similarly, there exist elements $y_2, ..., y_n$ such that

$$y_i \equiv 1 \bmod \mathfrak{a}_i, \quad y_i \equiv 0 \bmod \mathfrak{a}_j \text{ for } j \neq i.$$

The element $x = \sum x_i y_i$ maps to $(x_1 \bmod \mathfrak{a}_1, \ldots, x_n \bmod \mathfrak{a}_n)$, which shows that (5) is surjective.

It remains to prove that $\bigcap \mathfrak{a}_i = \prod \mathfrak{a}_i$. Obviously $\bigcap \mathfrak{a}_i \supset \prod \mathfrak{a}_i$. First suppose that $n = 2$, and let $a_1 + a_2 = 1$, as before. For $c \in \mathfrak{a}_1 \cap \mathfrak{a}_2$, we have

$$c = a_1 c + a_2 c \in \mathfrak{a}_1 \cdot \mathfrak{a}_2$$

which proves that $\mathfrak{a}_1 \cap \mathfrak{a}_2 = \mathfrak{a}_1 \mathfrak{a}_2$. We complete the proof by induction. This allows us to assume that $\prod_{i \geq 2} \mathfrak{a}_i = \bigcap_{i \geq 2} \mathfrak{a}_i$. We showed above that $\mathfrak{a}_1$ and $\prod_{i \geq 2} \mathfrak{a}_i$ are relatively prime, and so

$$\mathfrak{a}_1 \cdot (\prod_{i \geq 2} \mathfrak{a}_i) = \mathfrak{a}_1 \cap (\prod_{i \geq 2} \mathfrak{a}_i)$$

by the $n = 2$ case. Now $\mathfrak{a}_1 \cdot (\prod_{i \geq 2} \mathfrak{a}_i) = \prod_{i \geq 1} \mathfrak{a}_i$ and $\mathfrak{a}_1 \cap (\prod_{i \geq 2} \mathfrak{a}_i) = \mathfrak{a}_1 \cap (\bigcap_{i \geq 2} \mathfrak{a}_i) = \bigcap_{i \geq 1} \mathfrak{a}_i$,which completes the proof. □

Noetherian rings

PROPOSITION 1.2. *The following three conditions on a ring A are equivalent:*

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

PROOF. (a) $\implies$ (b): If $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$ is an ascending chain, then $\mathfrak{a} = \bigcup \mathfrak{a}_i$ is an ideal, and hence has a finite set $\{a_1, \ldots, a_n\}$ 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) $\implies$ (c): Let Σ be a nonempty set of ideals in A. The (b) certainly implies that every ascending chain of ideals in Σ has an upper bound in Σ, and so Zorn's lemma shows that Σ has a maximal element.

(c) $\implies$ (a): Let $\mathfrak{a}$ be an ideal, and let Σ be the set of finitely generated ideals contained in $\mathfrak{a}$. Then Σ is nonempty because it contains the zero ideal, and so it contains a maximal element $\mathfrak{c} = (a_1, \ldots, a_r)$. If $\mathfrak{c} \neq \mathfrak{a}$, then there exists an element $a \in \mathfrak{a} \smallsetminus \mathfrak{c}$, and $(a_1, \ldots, a_r, a)$ will be a finitely generated ideal in $\mathfrak{a}$ properly containing $\mathfrak{c}$. This contradicts the definition of $\mathfrak{c}$. □

A ring A is ***noetherian*** if it satisfies the equivalent conditions of the proposition. On applying (c) to the set of all proper ideals containing a fixed proper ideal, we see that every proper ideal in a noetherian ring is contained in a maximal ideal. This is, in fact, true for any ring, but the proof for non-noetherian rings requires Zorn's lemma (CA 2.1).

A ring A is said to be ***local*** if it has exactly one maximal ideal $\mathfrak{m}$. Because every nonunit is contained in a maximal ideal, for a local ring $A^\times = A \smallsetminus \mathfrak{m}$.

PROPOSITION 1.3 (NAKAYAMA'S LEMMA). *Let A be a local ring with maximal ideal $\mathfrak{m}$, and let M be a finitely generated A-module.*

(a) *If $M = \mathfrak{m}M$, then $M = 0$.*
(b) *If N is a submodule of M such that $M = N + \mathfrak{m}M$, then $M = N$.*

PROOF. (a) Suppose that $M \neq 0$. Choose a minimal set of generators $\{e_1, \ldots, e_n\}$, $n \geq 1$, for M, and write

$$e_1 = a_1 e_1 + \cdots + a_n e_n, \quad a_i \in \mathfrak{m}.$$

Then

$$(1 - a_1)e_1 = a_2 e_2 + \cdots + a_n e_n$$

and, as $(1 - a_1)$ is a unit, $e_2, \ldots, e_n$ generate M, contradicting the minimality of the set.

(b) The hypothesis implies that $M/N = \mathfrak{m}(M/N)$, and so $M/N = 0$. □

Now let A be a local noetherian ring with maximal ideal $\mathfrak{m}$. When we regard $\mathfrak{m}$ as an A-module, the action of A on $\mathfrak{m}/\mathfrak{m}^2$ factors through $k = A/\mathfrak{m}$.

COROLLARY 1.4. *The elements $a_1, \ldots, a_n$ 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 $a_1, \ldots, a_n$ 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 $\mathfrak{m} = (a_1, \ldots, a_n) + \mathfrak{m}^2$. Because A is noetherian, $\mathfrak{m}$ is finitely generated, and Nakayama's lemma, applied with $M = \mathfrak{m}$ and $N = (a_1, \ldots, a_n)$, shows that $\mathfrak{m} = (a_1, \ldots, a_n)$. □

DEFINITION 1.5. Let A be a noetherian ring.

(a) The ***height*** $\mathrm{ht}(\mathfrak{p})$ of a prime ideal $\mathfrak{p}$ in A is the greatest length d of a chain of distinct prime ideals
$$\mathfrak{p} = \mathfrak{p}_d \supset \mathfrak{p}_{d-1} \supset \cdots \supset \mathfrak{p}_0. \tag{6}$$
(b) The ***Krull dimension*** of A is $\sup\{\mathrm{ht}(\mathfrak{p}) \mid \mathfrak{p} \subset A, \quad \mathfrak{p} \text{ prime}\}$.

Thus, the Krull dimension of a ring A is the supremum of the lengths of chains of prime ideals in A (the length of a chain is the number of gaps, so the length of (6) is d). For example, a field has Krull dimension 0, and conversely an integral domain of Krull dimension 0 is a field. The height of every nonzero prime ideal in a principal ideal domain is 1, and so such a ring has Krull dimension 1 (provided it is not a field).

The height of any prime ideal in a noetherian ring is finite, but the Krull dimension of the ring may be infinite because it may contain a sequence of prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \ldots$ such that $\mathrm{ht}(\mathfrak{p}_i)$ tends to infinity (see Nagata, Local Rings, 1962, Appendix A.1, p203).

DEFINITION 1.6. A local noetherian ring of Krull dimension d is said to be ***regular*** if its maximal ideal can be generated by d elements.

It follows from Corollary 1.4 that a local noetherian ring is regular if and only if its Krull dimension is equal to the dimension of the vector space $\mathfrak{m}/\mathfrak{m}^2$.

LEMMA 1.7. *In a noetherian ring, every set of generators for an ideal contains a finite generating subset.*

PROOF. Let $\mathfrak{a}$ be an ideal in a noetherian ring A, and let S be a set of generators for $\mathfrak{a}$. An ideal maximal in the set of ideals generated by finite subsets of S must contain every element of S (otherwise it wouldn't be maximal), and so equals $\mathfrak{a}$. $\square$

THEOREM 1.8 (KRULL INTERSECTION THEOREM). *In any noetherian local ring A with maximal ideal $\mathfrak{m}$, $\bigcap_{n\geq 1}\mathfrak{m}^n = \{0\}$.*

PROOF. Let $a_1, \ldots, a_r$ generate $\mathfrak{m}$. Then $\mathfrak{m}^n$ consists of all finite sums

$$\sum_{i_1+\cdots+i_r=n} c_{i_1\cdots i_r} a_1^{i_1}\cdots a_r^{i_r}, \quad c_{i_1\cdots i_r}\in A.$$

In other words, $\mathfrak{m}^n$ consists of the elements of A that equal $g(a_1,\ldots,a_r)$ for some homogeneous polynomial $g(X_1,\ldots,X_r)\in A[X_1,\ldots,X_r]$ of degree n. Let S_m be the set of homogeneous polynomials f of degree m such that $f(a_1,\ldots,a_r)\in\bigcap_{n\geq 1}\mathfrak{m}^n$, and let $\mathfrak{a}$ be the ideal in $A[X_1,\ldots,X_r]$ generated by the set $\bigcup_m S_m$. According to the lemma, there exists a finite set $\{f_1,\ldots,f_s\}$ of elements of $\bigcup_m S_m$ that generates $\mathfrak{a}$. Let $d_i = \deg f_i$, and let $d = \max d_i$. Let $b\in\bigcap_{n\geq 1}\mathfrak{m}^n$; then $b\in\mathfrak{m}^{d+1}$, and so $b = f(a_1,\ldots,a_r)$ for some homogeneous polynomial f of degree $d+1$. By definition, $f\in S_{d+1}\subset\mathfrak{a}$, and so

$$f = g_1 f_1 + \cdots + g_s f_s$$

for some $g_i\in A[X_1,\ldots,X_n]$. As f and the f_i are homogeneous, we can omit from each g_i all terms not of degree $\deg f - \deg f_i$, since these terms cancel out. Thus, we may choose the g_i to be homogeneous of degree $\deg f - \deg f_i = d+1-d_i > 0$. Then $g_i(a_1,\ldots,a_r)\in\mathfrak{m}$, and so

$$b = f(a_1,\ldots,a_r) = \sum\nolimits_i g_i(a_1,\ldots,a_r)\cdot f_i(a_1,\ldots,a_r)\in\mathfrak{m}\cdot\bigcap\nolimits_{n\geq 1}\mathfrak{m}^n.$$

Thus, $\bigcap\mathfrak{m}^n = \mathfrak{m}\cdot\bigcap\mathfrak{m}^n$, and Nakayama's lemma implies that $\bigcap\mathfrak{m}^n = 0$. $\square$

Unique factorization

Let A be an integral domain. An element a of A is ***irreducible*** if it is not zero, not a unit, and admits only trivial factorizations, i.e.,

$$a = bc \implies b \text{ or } c \text{ is a unit.}$$

The element a is said to be ***prime*** if (a) is a prime ideal, i.e.,

$$a|bc \implies a|b \text{ or } a|c.$$

An integral domain A is called a ***unique factorization domain*** if every nonzero nonunit in A can be written as a finite product of irreducible elements in exactly one way up to units and the order of the factors. In such a ring, an irreducible element a can divide a product bc only if it is an irreducible factor of b or c (write $bc = aq$ and express b, c, q as products of irreducible elements).

PROPOSITION 1.9. *Let A be an integral domain, and let a be an element of A that is neither zero nor a unit. If a is prime, then a is irreducible, and the converse holds when A is a unique factorization domain.*

PROOF. Assume that a is prime. If $a = bc$ then a divides bc, and so a divides b or c. Suppose the first, and write $b = aq$. Now $a = bc = aqc$, which implies that $qc = 1$, and that c is a unit. Therefore a is irreducible.

For the converse, assume that a is irreducible. If $a|bc$, then (as we noted above) $a|b$ or $a|c$, and so a is prime. □

PROPOSITION 1.10 (GAUSS'S LEMMA). *Let A be a unique factorization domain with field of fractions F. If $f(X) \in A[X]$ factors into the product of two nonconstant polynomials in $F[X]$, then it factors into the product of two nonconstant polynomials in $A[X]$.*

PROOF. Let $f = gh$ in $F[X]$. For suitable $c, d \in A$, the polynomials $g_1 = cg$ and $h_1 = dh$ have coefficients in A, and so we have a factorization

$$cdf = g_1 h_1 \text{ in } A[X].$$

If an irreducible element p of A divides cd, then, looking modulo (p), we see that

$$0 = \overline{g_1} \cdot \overline{h_1} \text{ in } (A/(p))[X].$$

According to Proposition 1.9, (p) is prime, and so $(A/(p))[X]$ is an integral domain. Therefore, p divides all the coefficients of at least one of the polynomials g_1, h_1, say g_1, so that $g_1 = pg_2$ for some $g_2 \in A[X]$. Thus, we have a factorization

$$(cd/p)f = g_2 h_1 \text{ in } A[X].$$

Continuing in this fashion, we can remove all the irreducible factors of cd, and so obtain a factorization of f in $A[X]$. □

Let A be a unique factorization domain. A nonzero polynomial

$$f = a_0 + a_1 X + \cdots + a_m X^m$$

in $A[X]$ is said to be ***primitive*** if the coefficients a_i have no common factor (other than units). Every polynomial f in $A[X]$ can be written $f = c(f) \cdot f_1$ with $c(f) \in A$ and f_1 primitive. The element $c(f)$, well-defined up to multiplication by a unit, is called the ***content*** of f.

LEMMA 1.11. *The product of two primitive polynomials is primitive.*

PROOF. Let

$$\begin{aligned} f &= a_0 + a_1 X + \cdots + a_m X^m \\ g &= b_0 + b_1 X + \cdots + b_n X^n, \end{aligned}$$

be primitive polynomials, and let p be an irreducible element of A. Let a_{i_0} be the first coefficient of f not divisible by p and b_{j_0} the first coefficient of g not divisible by p. Then all the terms in $\sum_{i+j=i_0+j_0} a_i b_j$ are divisible by p, except $a_{i_0} b_{j_0}$, which is not divisible by p. Therefore, p doesn't divide the $(i_0 + j_0)$th-coefficient of fg. We have shown that no irreducible element of A divides all the coefficients of fg, which must therefore be primitive. □

LEMMA 1.12. *For polynomials $f, g \in A[X]$,*

$$c(fg) = c(f) \cdot c(g);$$

hence every factor in $A[X]$ of a primitive polynomial is primitive.

PROOF. Let $f = c(f) \cdot f_1$ and $g = c(g) \cdot g_1$ with f_1 and g_1 primitive. Then

$$fg = c(f) \cdot c(g) \cdot f_1 g_1$$

with $f_1 g_1$ primitive, and so $c(fg) = c(f)c(g)$. □

PROPOSITION 1.13. *If A is a unique factorization domain, then so also is $A[X]$.*

PROOF. From the factorization $f = c(f)f_1$, we see that the irreducible elements of $A[X]$ are to be found among the constant polynomials and the primitive polynomials, but a constant polynomial is irreducible if and only if a is an irreducible element of A (obvious) and a primitive polynomial is irreducible if and only if it has no primitive factor of lower degree (by 1.12). From this it is clear that every nonzero nonunit f in $A[X]$ is a product of irreducible elements.

From the factorization $f = c(f)f_1$, we see that the irreducible elements of $A[X]$ are to be found among the constant polynomials and the primitive polynomials.

Let

$$f = c_1 \cdots c_m f_1 \cdots f_n = d_1 \cdots d_r g_1 \cdots g_s$$

be two factorizations of an element f of $A[X]$ into irreducible elements with the c_i, d_j constants and the f_i, g_j primitive polynomials. Then

$$c(f) = c_1 \cdots c_m = d_1 \cdots d_r \text{ (up to units in } A),$$

and, on using that A is a unique factorization domain, we see that $m = r$ and the c_i's differ from the d_i's only by units and ordering. Hence,

$$f_1 \cdots f_n = g_1 \cdots g_s \text{ (up to units in } A).$$

Gauss's lemma shows that the f_i, g_j are irreducible polynomials in $F[X]$ and, on using that $F[X]$ is a unique factorization domain, we see that $n = s$ and that the f_i's differ from the g_i's only by units in F and by their ordering. But if $f_i = \frac{a}{b} g_j$ with a and b nonzero elements of A, then $bf_i = ag_j$. As f_i and g_j are primitive, this implies that $b = a$ (up to a unit in A), and hence that $\frac{a}{b}$ is a unit in A. □

Polynomial rings

Let k be a field. A ***monomial*** in $X_1, \ldots, X_n$ 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 denote the monomial by X^α, $\alpha = (a_1, \ldots, a_n) \in \mathbb{N}^n$.

The elements of the polynomial ring $k[X_1,\ldots,X_n]$ 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. In particular, the monomials form a basis for $k[X_1,\ldots,X_n]$ as a k-vector space.

The ***degree***, $\deg(f)$, of a nonzero polynomial f is the largest total degree of a monomial occurring in f with nonzero coefficient. Since $\deg(fg)=\deg(f)+\deg(g)$, $k[X_1,\ldots,X_n]$ is an integral domain and $k[X_1,\ldots,X_n]^\times = k^\times$. An element f of $k[X_1,\ldots,X_n]$ is irreducible if it is nonconstant and $f=gh \implies g$ or h is constant.

THEOREM 1.14. *The ring $k[X_1,\ldots,X_n]$ is a unique factorization domain.*

PROOF. Note that $k[X_1,\ldots,X_{n-1}][X_n] = k[X_1,\ldots,X_n]$; this simply says that every polynomial f in n variables $X_1,\ldots,X_n$ can be expressed uniquely as a polynomial in X_n with coefficients in $k[X_1,\ldots,X_{n-1}]$,

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

Since k itself is a unique factorization domain (trivially), the theorem follows by induction from Proposition 1.13. □

COROLLARY 1.15. *A nonzero proper principal ideal (f) in $k[X_1,\ldots,X_n]$ is prime if and only f is irreducible.*

PROOF. Special case of (1.9). □

Integrality

Let A be an integral domain, and let L be a field containing A. An element α of L is said to be ***integral*** over A if it is a root of a monic[2] polynomial with coefficients in A, i.e., if it satisfies an equation

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

THEOREM 1.16. *The set of elements of L integral over A forms a ring.*

PROOF. Let α and β integral over A. Then there exists a monic polynomial

$$h(X)=X^m+c_1X^{m-1}+\cdots+c_m, \quad c_i\in A,$$

having α and β among its roots (e.g., take h to be the product of the polynomials exhibiting the integrality of α and β). Write

$$h(X)=\prod_{i=1}^m (X-\gamma_i)$$

[2] A polynomial is ***monic*** if its leading coefficient is 1, i.e., $f(X)=X^n+$ terms of degree $<n$.

with the γ_i in an algebraic closure of L. Up to sign, the c_i are the elementary symmetric polynomials in the γ_i (cf. FT §5). I claim that every symmetric polynomial in the γ_i with coefficients in A lies in A: let $p_1, p_2, \ldots$ be the elementary symmetric polynomials in $X_1, \ldots, X_m$; if $P \in A[X_1, \ldots, X_m]$ is symmetric, then the symmetric polynomials theorem (ibid. 5.30) shows that $P(X_1, \ldots, X_m) = Q(p_1, \ldots, p_m)$ for some $Q \in A[X_1, \ldots, X_m]$, and so

$$P(\gamma_1, \ldots, \gamma_m) = Q(-c_1, c_2, \ldots) \in A.$$

The coefficients of the polynomials

$$\prod_{1 \leq i,j \leq m} (X - \gamma_i \gamma_j) \quad \text{and} \quad \prod_{1 \leq i,j \leq m} (X - (\gamma_i \pm \gamma_j))$$

are symmetric polynomials in the γ_i with coefficients in A, and therefore lie in A. As the polynomials are monic and have $\alpha\beta$ and $\alpha \pm \beta$ among their roots, this shows that these elements are integral. □

For a less computational proof, see CA 5.3.

DEFINITION 1.17. The ring of elements of L integral over A is called the ***integral closure*** of A in L.

PROPOSITION 1.18. *Let A be an integral domain with field of fractions F, and let L be a field containing F. If $\alpha \in L$ is algebraic over F, then there exists a $d \in A$ such that $d\alpha$ is integral over A.*

PROOF. By assumption, α satisfies an equation

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

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:

$$d^m \alpha^m + a_1 d^m \alpha^{m-1} + \cdots + a_m d^m = 0.$$

We can rewrite this as

$$(d\alpha)^m + a_1 d (d\alpha)^{m-1} + \cdots + a_m d^m = 0.$$

As $a_1 d, \ldots, a_m d^m \in A$, this shows that $d\alpha$ is integral over A. □

COROLLARY 1.19. *Let A be an integral domain and let L be an algebraic extension of the field of fractions of A. Then L is the field of fractions of the integral closure of A in L.*

PROOF. The proposition shows that every $\alpha \in L$ can be written $\alpha = \beta/d$ with β integral over A and $d \in A$. □

DEFINITION 1.20. An integral domain A is ***integrally closed*** if it is equal to its integral closure in its field of fractions F, i.e., if

$$\alpha \in F, \quad \alpha \text{ integral over } A \implies \alpha \in A.$$

PROPOSITION 1.21. *Every unique factorization domain (e.g. a principal ideal domain) is integrally closed.*

PROOF. Let a/b, $a,b \in A$, be integral over A. If $a/b \notin A$, then there is an irreducible element p of A dividing b but not a. As a/b is integral over A, it satisfies 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

$$a^n + a_1 a^{n-1} b + \cdots + a_n b^n = 0.$$

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 1.22. *Let A be an integrally closed integral domain, and let L be a finite extension of the field of fractions F of A. An element α of L is integral over A if and only if its minimum polynomial over F has coefficients in A.*

PROOF. Let α be integral over A, so that

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

Let α' be a conjugate of α, i.e., a root of the minimum polynomial $f(X)$ of α over F. Then there is an F-isomorphism[3]

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

On applying σ to the above equation we obtain the equation

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

which shows that α' is integral over A. Hence all the conjugates of α are integral over A, and it follows from (1.16) that the coefficients of $f(X)$ are integral over A. They lie in F, 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. □

COROLLARY 1.23. *Let A be an integrally closed integral domain with field of fractions F, and let $f(X)$ be a monic polynomial in $A[X]$. Then every monic factor of $f(X)$ in $F[X]$ has coefficients in A.*

PROOF. It suffices to prove this for an irreducible monic factor g of f in $F[X]$. Let α be a root of g in some extension field of F. Then g is the minimum polynomial α, which, being also a root of f, is integral. Therefore g has coefficients in A. □

[3]Recall (FT §1) that the homomorphism $X \mapsto \alpha\colon F[X] \to F[\alpha]$ defines an isomorphism $F[X]/(f) \to F[\alpha]$, where f is the minimum polynomial of α.

Direct limits (summary)

DEFINITION 1.24. A partial ordering $\leq$ on a set I is said to be ***directed***, and the pair $(I, \leq)$ is called a ***directed set***, if for all $i, j \in I$ there exists a $k \in I$ such that $i, j \leq k$.

DEFINITION 1.25. Let $(I, \leq)$ be a directed set, and let R be a ring.

(a) An ***direct system*** of R-modules indexed by $(I, \leq)$ is a family $(M_i)_{i \in I}$ of R-modules together with a family $(\alpha^i_j\colon M_i \to M_j)_{i \leq j}$ of R-linear maps such that $\alpha^i_i = \mathrm{id}_{M_i}$ and $\alpha^j_k \circ \alpha^i_j = \alpha^i_k$ all $i \leq j \leq k$.

(b) An R-module M together with a family $(\alpha^i\colon M_i \to M)_{i \in I}$ of R-linear maps satisfying $\alpha^i = \alpha^j \circ \alpha^i_j$ all $i \leq j$ is said to be a ***direct limit*** of the system in (a) if it has the following universal property: for any other R-module N and family $(\beta^i\colon M_i \to N)$ of R-linear maps such that $\beta^i = \beta^j \circ \alpha^i_j$ all $i \leq j$, there exists a unique morphism $\alpha\colon M \to N$ such that $\alpha \circ \alpha^i = \beta^i$ for i.

Clearly, the direct limit (if it exists), is uniquely determined by this condition up to a unique isomorphism. We denote it $\varinjlim(M_i, \alpha^j_i)$, or just $\varinjlim M_i$.

Criterion

An R-module M together with R-linear maps $\alpha^i\colon M_i \to M$ is the direct limit of a system (M_i, α^j_i) if and only if

(a) $M = \bigcup_{i \in I} \alpha^i(M_i)$, and

(b) $m_i \in M_i$ maps to zero in M if and only if it maps to zero in M_j for some $j \geq i$.

Construction

Let

$$M = \bigoplus_{i \in I} M_i / M'$$

where M' is the R-submodule generated by the elements

$$m_i - \alpha^i_j(m_i) \quad \text{all } i < j, m_i \in M_i.$$

Let $\alpha^i(m_i) = m_i + M'$. Then certainly $\alpha^i = \alpha^j \circ \alpha^i_j$ for all $i \leq j$. For any R-module N and R-linear maps $\beta^j\colon M_j \to N$, there is a unique map

$$\bigoplus_{i \in I} M_i \to N,$$

namely, $\sum m_i \mapsto \sum \beta^i(m_i)$, sending m_i to $\beta^i(m_i)$, and this map factors through M and is the unique R-linear map with the required properties.

Direct limits of R-algebras, etc., are defined similarly.

Rings of fractions

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

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

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 of equivalence classes in the way suggested by the notation:

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

It is easy to check that these do not depend on the choices of representatives for the equivalence classes, and that we obtain in this way a ring

$$S^{-1}A = \left\{\frac{a}{s} \mid a \in A,\ s \in S\right\}$$

and a ring homomorphism $a \mapsto \frac{a}{1}\colon A \to S^{-1}A$, whose kernel is

$$\{a \in A \mid sa = 0 \text{ for some } s \in S\}.$$

For example, if A is an integral domain an $0 \notin S$, then $a \mapsto \frac{a}{1}$ is injective, but if $0 \in S$, then $S^{-1}A$ is the zero ring.

Write i for the homomorphism $a \mapsto \frac{a}{1}\colon A \to S^{-1}A$.

PROPOSITION 1.26. *The pair $(S^{-1}A, i)$ has the following universal property: every element $s \in S$ maps to a unit in $S^{-1}A$, and any other homomorphism $A \to B$ with this property factors uniquely through i:*

$$\begin{tikzcd} A \arrow[r, "i"] \arrow[dr] & S^{-1}A \arrow[d, dotted, "\exists!"] \\ & B. \end{tikzcd}$$

PROOF. If β exists,

$$s\tfrac{a}{s} = a \implies \beta(s)\beta(\tfrac{a}{s}) = \beta(a) \implies \beta(\tfrac{a}{s}) = \alpha(a)\alpha(s)^{-1},$$

and so β is unique. Define

$$\beta(\tfrac{a}{s}) = \alpha(a)\alpha(s)^{-1}.$$

Then

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

because $\alpha(s)$ is a unit in B, and so β is well-defined. It is obviously a homomorphism. □

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

When A is an integral domain and $S = A \smallsetminus \{0\}$, $F = S^{-1}A$ is the field of fractions of A. In this case, for any other multiplicative subset T of A not containing 0, the ring $T^{-1}A$ can be identified with the subring $\{\frac{a}{t} \in F \mid a \in A, t \in S\}$ of F.

We shall be especially interested in the following examples.

EXAMPLE 1.27. Let $h \in A$. Then $S_h = \{1, h, h^2, \ldots\}$ is a multiplicative subset of A, and we let $A_h = S_h^{-1}A$. Thus every element of A_h can be written in the form a/h^m, $a \in A$, and

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

If h is nilpotent, then $A_h = 0$, and if A is an integral domain with field of fractions F and $h \neq 0$, then A_h is the subring of F of elements of the form a/h^m, $a \in A$, $m \in \mathbb{N}$.

EXAMPLE 1.28. Let $\mathfrak{p}$ be a prime ideal in A. Then $S_\mathfrak{p} = A \smallsetminus \mathfrak{p}$ is a multiplicative subset of A, and we let $A_\mathfrak{p} = S_\mathfrak{p}^{-1}A$. 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 $\mathfrak{m} = \{\frac{a}{s} \mid a \in \mathfrak{p},\ s \notin \mathfrak{p}\}$ is a maximal ideal in $A_\mathfrak{p}$, and it is the only maximal ideal, i.e., $A_\mathfrak{p}$ is a local ring.[4] 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 1.29. *(a) For any ring A and $h \in A$, the map $\sum a_i X^i \mapsto \sum \frac{a_i}{h^i}$ defines an isomorphism*

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

(b) For any multiplicative subset S of A, $S^{-1}A \simeq \varinjlim A_h$, where h runs over the elements of S (partially ordered by division).

PROOF. (a) If $h = 0$, both rings are zero, and so we may assume $h \neq 0$. In the ring $A[x] = A[X]/(1 - hX)$, $1 = hx$, and so h is a unit. Let $\alpha \colon A \to B$ be a homomorphism of rings such that $\alpha(h)$ is a unit in B. The homomorphism $\sum a_i X^i \mapsto \sum \alpha(a_i)\alpha(h)^{-i} \colon A[X] \to B$ factors through $A[x]$ because $1 - hX \mapsto 1 - \alpha(h)\alpha(h)^{-1} = 0$, and, because $\alpha(h)$ is a unit in B, this is the unique extension of α to $A[x]$. Therefore $A[x]$ has the same universal property as A_h, and so the two are (uniquely) isomorphic by an isomorphism that fixes elements of A and makes h^{-1} correspond to x.

(b) When $h|h'$, say, $h' = hg$, there is a canonical homomorphism $\frac{a}{h} \mapsto \frac{ag}{h'} \colon A_h \to A_{h'}$, and so the rings A_h form a direct system indexed by the set S. When $h \in S$, the homomorphism $A \to S^{-1}A$ extends uniquely to a homomorphism $\frac{a}{h} \mapsto \frac{a}{h} \colon A_h \to S^{-1}A$ (1.26), and these homomorphisms are compatible with the maps in the direct system. Now apply the criterion p14 to see that $S^{-1}A$ is the direct limit of the A_h. □

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

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

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 1.30. *Let S be a multiplicative subset of the ring A. The map*

$$\mathfrak{p} \mapsto S^{-1}\mathfrak{p} = (S^{-1}A)\mathfrak{p}$$

is a bijection from the set of prime ideals of A disjoint from S to the set of prime ideals of $S^{-1}A$ with inverse $\mathfrak{q} \mapsto$(inverse image of $\mathfrak{q}$ in A).

PROOF. For an ideal $\mathfrak{b}$ of $S^{-1}A$, let $\mathfrak{b}^c$ be the inverse image of $\mathfrak{b}$ in A, and for an ideal $\mathfrak{a}$ of A, let $\mathfrak{a}^e = (S^{-1}A)\mathfrak{a}$ be the ideal in $S^{-1}A$ generated by the image of $\mathfrak{a}$.

For an ideal $\mathfrak{b}$ of $S^{-1}A$, certainly, $\mathfrak{b} \supset \mathfrak{b}^{ce}$. Conversely, if $\frac{a}{s} \in \mathfrak{b}$, $a \in A$, $s \in S$, then $\frac{a}{1} \in \mathfrak{b}$, and so $a \in \mathfrak{b}^c$. Thus $\frac{a}{s} \in \mathfrak{b}^{ce}$, and so $\mathfrak{b} = \mathfrak{b}^{ce}$.

For an ideal $\mathfrak{a}$ of A, certainly $\mathfrak{a} \subset \mathfrak{a}^{ec}$. Conversely, if $a \in \mathfrak{a}^{ec}$, then $\frac{a}{1} \in \mathfrak{a}^e$, and so $\frac{a}{1} = \frac{a'}{s}$ for some $a' \in \mathfrak{a}$, $s \in S$. Thus, $t(as - a') = 0$ for some $t \in S$, and so $ast \in \mathfrak{a}$. If $\mathfrak{a}$ is a prime ideal disjoint from S, this implies that $a \in \mathfrak{a}$: for such an ideal, $\mathfrak{a} = \mathfrak{a}^{ec}$.

If $\mathfrak{b}$ is prime, then certainly $\mathfrak{b}^c$ is prime. For any ideal $\mathfrak{a}$ of A, $S^{-1}A/\mathfrak{a}^e \simeq \bar{S}^{-1}(A/\mathfrak{a})$ where $\bar{S}$ is the image of S in $A/\mathfrak{a}$. If $\mathfrak{a}$ is a prime ideal disjoint from S, then $\bar{S}^{-1}(A/\mathfrak{a})$ is a subring of the field of fractions of $A/\mathfrak{a}$, and is therefore an integral domain. Thus, $\mathfrak{a}^e$ is prime.

We have shown that $\mathfrak{p} \mapsto \mathfrak{p}^e$ and $\mathfrak{q} \mapsto \mathfrak{q}^c$ are inverse bijections between the prime ideals of A disjoint from S and the prime ideals of $S^{-1}A$. □

LEMMA 1.31. *Let $\mathfrak{m}$ be a maximal ideal of a noetherian 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 ($r < n$):

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathfrak{m}^r/\mathfrak{m}^n & \longrightarrow & A/\mathfrak{m}^n & \longrightarrow & A/\mathfrak{m}^r & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow\simeq & & \downarrow\simeq & & \\
0 & \longrightarrow & \mathfrak{n}^r/\mathfrak{n}^n & \longrightarrow & A_{\mathfrak{m}}/\mathfrak{n}^n & \longrightarrow & A_{\mathfrak{m}}/\mathfrak{n}^r & \longrightarrow & 0.
\end{array}$$

Let $S = A \smallsetminus \mathfrak{m}$, so that $A_{\mathfrak{m}} = S^{-1}A$. Because S contains no zero divisors, the map $a \mapsto \frac{a}{1} \colon A \to A_{\mathfrak{m}}$ is injective, and I'll identify A with its image. 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 $\mathfrak{n}^m = \mathfrak{m}^n A_{\mathfrak{m}} = S^{-1}\mathfrak{m}^m$, 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 $\mathfrak{m}' \supset \mathfrak{m}^m \implies \mathfrak{m}' \supset \mathfrak{m}$), and so the only maximal ideal in $A/\mathfrak{m}^m$ is $\mathfrak{m}/\mathfrak{m}^m$. As s is not in $\mathfrak{m}/\mathfrak{m}^m$, it must be a unit in $A/\mathfrak{m}^m$, and as $sa = 0$ in $A/\mathfrak{m}^m$, a must be 0 in $A/\mathfrak{m}^m$, i.e., $a \in \mathfrak{m}^m$.

We now prove that the map is surjective. Let $\frac{a}{s} \in A_\mathfrak{m}$, $a \in A$, $s \in A \smallsetminus \mathfrak{m}$. The only maximal ideal of A containing $\mathfrak{m}^m$ is $\mathfrak{m}$, and so no maximal ideal contains both s and $\mathfrak{m}^m$; it follows that $(s) + \mathfrak{m}^m = A$. Therefore, there exist $b \in A$ and $q \in \mathfrak{m}^m$ such that $sb + q = 1$. 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 $\frac{a}{s}$. □

PROPOSITION 1.32. *In any noetherian ring, only* 0 *lies in all powers of all maximal ideals.*

PROOF. Let a be an element of a noetherian ring A. If $a \neq 0$, then $\{b \mid ba = 0\}$ is a proper ideal, and so is contained in some maximal ideal $\mathfrak{m}$. Then $\frac{a}{1}$ is nonzero in $A_\mathfrak{m}$, and so $\frac{a}{1} \notin (\mathfrak{m}A_\mathfrak{m})^n$ for some n (by the Krull intersection theorem), which implies that $a \notin \mathfrak{m}^n$. □

NOTES. For more on rings of fractions, see CA §6.

Tensor Products

Tensor products of modules

Let R be a ring. A map $\phi\colon M \times N \to P$ of R-modules is said to be ***R-bilinear*** if

$$\begin{aligned} \phi(x + x', y) &= \phi(x, y) + \phi(x', y), && x, x' \in M, \quad y \in N \\ \phi(x, y + y') &= \phi(x, y) + \phi(x, y'), && x \in M, \quad y, y' \in N \\ \phi(rx, y) &= r\phi(x, y), && r \in R, \quad x \in M, \quad y \in N \\ \phi(x, ry) &= r\phi(x, y), && r \in R, \quad x \in M, \quad y \in N, \end{aligned}$$

i.e., if ϕ is R-linear in each variable. An R-module T together with an R-bilinear map $\phi\colon M \times N \to T$ is called the ***tensor product*** of M and N over R if it has the following universal property: every R-bilinear map $\phi'\colon M \times N \to T'$ factors uniquely through ϕ,

$$\begin{tikzcd} M \times N \arrow[r, "\phi"] \arrow[dr, "\phi'"'] & T \arrow[d, dotted, "\exists!"] \\ & T' \end{tikzcd}$$

As usual, the universal property determines the tensor product uniquely up to a unique isomorphism. We write it $M \otimes_R N$.

Construction Let M and N be R-modules, and let $R^{(M \times N)}$ be the free R-module with basis $M \times N$. Thus each element $R^{(M \times N)}$ can be expressed uniquely as a finite sum

$$\sum r_i(x_i, y_i), \quad r_i \in R, \quad x_i \in M, \quad y_i \in N.$$

Let K be the submodule of $R^{(M \times N)}$ generated by the following elements

$$\begin{aligned}
(x+x',y)-(x,y)-(x',y), &\quad x,x'\in M, \quad y\in N\\
(x,y+y')-(x,y)-(x,y'), &\quad x\in M, \quad y,y'\in N\\
(rx,y)-r(x,y), &\quad r\in R, \quad x\in M, \quad y\in N\\
(x,ry)-r(x,y), &\quad r\in R, \quad x\in M, \quad y\in N,
\end{aligned}$$

and define

$$M\otimes_R N = R^{(M\times N)}/K.$$

Write $x\otimes y$ for the class of (x,y) in $M\otimes_R N$. Then

$$(x,y)\mapsto x\otimes y\colon M\times N\to M\otimes_R N$$

is R-bilinear — we have imposed the fewest relations necessary to ensure this. Every element of $M\otimes_R N$ can be written as a finite sum

$$\sum r_i(x_i\otimes y_i), \quad r_i\in R, \quad x_i\in M, \quad y_i\in N,$$

and all relations among these symbols are generated by the following

$$\begin{aligned}
(x+x')\otimes y &= x\otimes y + x'\otimes y\\
x\otimes(y+y') &= x\otimes y + x\otimes y'\\
r(x\otimes y) &= (rx)\otimes y = x\otimes ry.
\end{aligned}$$

The pair $(M\otimes_R N, (x,y)\mapsto x\otimes y)$ has the following universal property:

Tensor products of algebras

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 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 $\gamma\circ j=\beta$:

$$\begin{tikzcd}
A \arrow[r, "i"] \arrow[dr, "\alpha"'] & C \arrow[d, dotted, "\exists!\ \gamma"] & B \arrow[l, "j"'] \arrow[dl, "\beta"] \\
& R &
\end{tikzcd}$$

If it exists, the tensor product, is uniquely determined up to a unique isomorphism by this property. We write it $A\otimes_k B$.

Construction Regard A and B as k-vector spaces, and form the tensor product $A\otimes_k B$. There is a multiplication map $A\otimes_k B\times A\otimes_k B\to A\otimes_k B$ for which

$$(a\otimes b)(a'\otimes b') = aa'\otimes bb'.$$

This makes $A\otimes_k B$ into a ring, and the homomorphism

$$c\mapsto c(1\otimes 1)=c\otimes 1 = 1\otimes c$$

makes it into a k-algebra. 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 they make $A \otimes_k B$ into the tensor product of A and B in the above sense.

EXAMPLE 1.33. 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 1.34. The ring $k[X_1, \ldots, X_m, X_{m+1}, \ldots, X_{m+n}]$, together with the obvious inclusions

$$k[X_1, \ldots, X_m] \quad \hookrightarrow \quad k[X_1, \ldots, X_{m+n}] \quad \hookleftarrow \quad k[X_{m+1}, \ldots, X_{m+n}]$$

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

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

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

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

is an isomorphism.

REMARK 1.35. (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

$$\Omega \otimes_k k[X_1, \ldots, X_n] \simeq \Omega[1 \otimes X_1, \ldots, 1 \otimes X_n] \simeq \Omega[X_1, \ldots, X_n].$$

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

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

(c) If A and B are algebras of k-valued functions on sets S and T respectively, then $(f \otimes g)(x, y) = f(x)g(y)$ realizes $A \otimes_k B$ as an algebra of k-valued functions on $S \times T$.

For more details on tensor products, see CA §8.

Extension of scalars

Let R be a commutative ring and A an R-algebra (not necessarily commutative) such that the image of $R \to A$ lies in the centre of A. Then we have a functor $M \mapsto A \otimes_R M$ from left R-modules to left A-modules.

Behaviour with respect to direct limits

PROPOSITION 1.36. *Direct limits commute with tensor products:*

$$\varinjlim_{i\in I} M_i \otimes_R \varinjlim_{j\in J} N_j \simeq \varinjlim_{(i,j)\in I\times J} (M_i \otimes_R N_j).$$

PROOF. Using the universal properties of direct limits and tensor products, one sees easily that $\varinjlim(M_i \otimes_R N_j)$ has the universal property to be the tensor product of $\varinjlim M_i$ and $\varinjlim N_j$. □

Flatness

For any R-module M, the functor $N \mapsto M \otimes_R N$ is right exact, i.e.,

$$M \otimes_R N' \to M \otimes_R N \to M \otimes_R N'' \to 0$$

is exact whenever

$$N' \to N \to N'' \to 0$$

is exact. If $M \otimes_R N \to M \otimes_R N'$ is injective whenever $N \to N'$ is injective, then M is said to be ***flat***. Thus M is flat if and only if the functor $N \mapsto M \otimes_R N$ is exact. Similarly, an R-algebra A is flat if $N \mapsto A \otimes_R N$ is flat.

PROPOSITION 1.37. *To be added.*

Categories and functors

A ***category*** C consists of

(a) a class of objects ob(C);
(b) for each pair (a,b) of objects, a set $\mathrm{Mor}(a,b)$, 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***)

$$(\alpha,\beta) \mapsto \beta\circ\alpha\colon \mathrm{Mor}(a,b)\times\mathrm{Mor}(b,c) \to \mathrm{Mor}(a,c).$$

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 $\mathrm{id}_a \in \mathrm{Mor}(a,a)$ such that $\mathrm{id}_a \circ\alpha = \alpha$, $\beta\circ\mathrm{id}_a = \beta$, for all α and β for which these composites are defined. The sets $\mathrm{Mor}(a,b)$ are required to be disjoint (so that a morphism α determines its source and target).

EXAMPLE 1.38. (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 Aff_k of affine k-algebras, whose objects are the affine k-algebras and whose morphisms are the homomorphisms of k-algebras.

(c) In chapter 4 below, we define a category Var_k of algebraic varieties over k, whose objects are the algebraic 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.

Let C and D be categories. A ***covariant functor*** F from C to D consists of

(a) a map $a \mapsto F(a)$ sending each object of C to an object of D, and,

(b) for each pair of objects a, b of C, a map

$$\alpha \mapsto F(\alpha)\colon \mathrm{Mor}(a,b) \to \mathrm{Mor}(F(a), F(b))$$

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

$$\alpha \mapsto F(\alpha)\colon \mathrm{Mor}(a,b) \to \mathrm{Mor}(F(b), F(a))$$

A functor $F\colon \mathsf{C} \to \mathsf{D}$ is ***full*** (resp. ***faithful, fully faithful***) if, for all objects a and b of C, the map

$$\mathrm{Mor}(a,b) \to \mathrm{Mor}(F(a), F(b))$$

is a surjective (resp. injective, bijective).

A covariant functor $F\colon \mathsf{A} \to \mathsf{B}$ of categories is said to be an ***equivalence of categories*** if it is fully faithful and every object of B is isomorphic to an object of the form $F(a)$, $a \in \mathrm{ob}(\mathsf{A})$ (F is ***essentially surjective***). One can show that such a functor F has a ***quasi-inverse***, i.e., that there is a functor $G\colon \mathsf{B} \to \mathsf{A}$, which is also an equivalence, and for which there exist natural isomorphisms $G(F(a)) \approx a$ and $F(G(b)) \approx b$.[5]

Similarly one defines the notion of a contravariant functor being an equivalence of categories.

Any fully faithful functor $F\colon \mathsf{C} \to \mathsf{D}$ defines an equivalence of C with the full subcategory of D whose objects are isomorphic to $F(a)$ for some object a of C. The ***essential image*** of a fully faithful functor $F\colon \mathsf{C} \to \mathsf{D}$ consists of the objects of D isomorphic to an object of the form $F(a)$, $a \in \mathrm{ob}(\mathsf{C})$.

Let F and G be two functors $\mathsf{C} \to \mathsf{D}$. A ***morphism*** (or ***natural transformation***) $\alpha\colon F \to G$ is a collection of morphisms $\alpha(a)\colon F(a) \to G(a)$, one for each object a of C, such that, for every morphism $u\colon a \to b$ in C, the following diagram commutes:

$$\begin{tikzcd} a \arrow[d, "u"] & F(a) \arrow[r, "\alpha(a)"] \arrow[d, "F(u)"] & G(a) \arrow[d, "G(u)"] \\ b & F(b) \arrow[r, "\alpha(b)"] & G(b). \end{tikzcd} \qquad (**)$$

With this notion of morphism, the functors $\mathsf{C} \to \mathsf{D}$ form a category $\mathsf{Fun}(\mathsf{C}, \mathsf{D})$ (provided that we ignore the problem that $\mathrm{Mor}(F, G)$ may not be a set, but only a class).

For any object V of a category C, we have a contravariant functor

$$h_V\colon \mathsf{C} \to \mathsf{Set},$$

[5]For each object b of B, choose an object $G(b)$ of A and an isomorphism $F(G(b)) \to b$. For each morphism $\beta\colon b \to b'$ in B, let $G(\beta)$ be the unique morphism such that

$$\begin{tikzcd} F(G(b)) \arrow[r] \arrow[d, "F(\beta)"] & b \arrow[d, "\beta"] \\ F(G(b')) \arrow[r] & b' \end{tikzcd}$$

commutes. Then G is a quasi-inverse to F.

which sends an object a to the set $\mathrm{Mor}(a, V)$ and sends a morphism $\alpha: a \to b$ to

$$\varphi \mapsto \varphi \circ \alpha: h_V(b) \to h_V(a),$$

i.e., $h_V(*) = \mathrm{Mor}(*, V)$ and $h_V(\alpha) = * \circ \alpha$. Let $\alpha: V \to W$ be a morphism in C. The collection of maps

$$h_\alpha(a): h_V(a) \to h_W(a), \quad \varphi \mapsto \alpha \circ \varphi$$

is a morphism of functors.

PROPOSITION 1.39 (YONEDA LEMMA). *For any functor $F: \mathsf{C} \to \mathsf{Set}$,*

$$\mathrm{Hom}(h_V, F) \simeq F(V).$$

In particular, when $F = h_W$,

$$\mathrm{Hom}(h_V, h_W) \simeq \mathrm{Hom}(W, V)$$

— to give a natural transformation $h_V \to h_W$ is the same as to give a morphism $W \to V$.

PROOF. An element x of $F(V)$ defines a natural transformation $h_V \to F$, namely,

$$\alpha \mapsto F(\alpha)(x): h_V(T) \to F(T), \quad \alpha \in h_V(T) = \mathrm{Hom}(T, V).$$

Conversely, a natural transformation $h_V \to F$ defines an element of $F(V)$, namely, the image of the "universal" element id_V under $h_V(V) \to F(V)$. It is easy to check that these two maps are inverse. □

Algorithms for polynomials

As an introduction to algorithmic algebraic geometry, we derive some algorithms for working with polynomial rings. This section is little more than a summary of the first two chapters of Cox et al.1992 to which I refer the reader for more details. Those not interested in algorithms can skip the remainder of this chapter. Throughout, k is a field (not necessarily algebraically closed).

The two main results will be:

(a) An algorithmic proof of the Hilbert basis theorem: every ideal in $k[X_1, \ldots, X_n]$ has a finite set of generators (in fact, of a special kind).

(b) There exists an algorithm for deciding whether a polynomial belongs to an ideal.

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 $k[X_1, \ldots, X_n]$, 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 ordered by lexicographic (dictionary) order. More precisely, let $\alpha = (a_1, \ldots, a_n)$ and $\beta = (b_1, \ldots, b_n)$ be two elements of $\mathbb{N}^n$; then

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

if, in the vector difference $\alpha - \beta$ (an element of $\mathbb{Z}^n$), 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:

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

Orderings on $k[X_1, \ldots, X_n]$

Fix an ordering on the monomials in $k[X_1, \ldots, X_n]$. Then we can write an element f of $k[X_1, \ldots, X_n]$ 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 $f = \sum a_\alpha X^\alpha \in k[X_1, \ldots, X_n]$. 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 $k[X_1, \ldots, X_n]$

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

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

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

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

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

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 $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)$.

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:

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

(different a_i's).

Continue until you achieve a remainder with the required property. In more detail,[6] after dividing through once by $g_1, \ldots, g_s$, 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 1.40. (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 $2X + 1$.

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

REMARK 1.41. If $r = 0$, then $f \in (g_1, \ldots, g_s)$, but, because the remainder depends on the ordering of the g_i, the converse is false. 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 $g_1, \ldots, g_s$.

Monomial ideals

In general, an ideal $\mathfrak{a}$ can contain a polynomial without containing the individual monomials 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 1.42. An ideal $\mathfrak{a}$ is ***monomial*** if

$$\sum c_\alpha X^\alpha \in \mathfrak{a} \text{ and } c_\alpha \neq 0 \implies X^\alpha \in \mathfrak{a}.$$

PROPOSITION 1.43. *Let $\mathfrak{a}$ be a monomial ideal, and let $A = \{\alpha \mid X^\alpha \in \mathfrak{a}\}$. Then A satisfies the condition*

$$\alpha \in A, \quad \beta \in \mathbb{N}^n \implies \alpha + \beta \in A \tag{*}$$

and $\mathfrak{a}$ is the k-subspace of $k[X_1, \ldots, X_n]$ 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 $k[X_1, \ldots, X_n]$ 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 $k[X_1, \ldots, X_n]$ generated by the set of monomials it contains. If $X^\alpha \in \mathfrak{a}$ and $X^\beta \in k[X_1, \ldots, X_n]$, 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 $k[X_1, \ldots, X_n]$: 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), $n \geq 0$, 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 1.44. *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*

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

In other words, 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 $\mathfrak{a} \subset \langle X^\beta \mid \beta \in A\rangle$. 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 $S = \{\alpha_1, \ldots, \alpha_s\}$ 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, the ideal $\langle X^\alpha \mid \alpha \in A\rangle$ is generated by the monomials X^{α_i}, $\alpha_i \in S$. This suggests the following result.

THEOREM 1.45 (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 1.46. For a nonzero ideal $\mathfrak{a}$ in $k[X_1, \ldots, X_n]$, we let $(\mathrm{LT}(\mathfrak{a}))$ be the ideal generated by $\{\mathrm{LT}(f) \mid f \in \mathfrak{a}\}$.

LEMMA 1.47. *Let $\mathfrak{a}$ be a nonzero ideal in $k[X_1, \ldots, X_n]$; then $(LT(\mathfrak{a}))$ is a monomial ideal, and it equals $(LT(g_1), \ldots, LT(g_n))$ for some $g_1, \ldots, g_n \in \mathfrak{a}$.*

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 1.44 that it is monomial. Now Dickson's Lemma shows that it equals $(\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s))$ for some $g_i \in \mathfrak{a}$. □

THEOREM 1.48 (HILBERT BASIS THEOREM). *Every ideal $\mathfrak{a}$ in $k[X_1, \ldots, X_n]$ is finitely generated; in fact, $\mathfrak{a}$ is generated by any elements of $\mathfrak{a}$ whose leading terms generate $LT(\mathfrak{a})$.*

PROOF. Let $g_1, \ldots, g_n$ be as in the lemma, and let $f \in \mathfrak{a}$. On applying the division algorithm, we find

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

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 $\mathrm{LT}(r) \in \mathrm{LT}(\mathfrak{a}) = (\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s))$, which, according to Lemma 1.44, implies that ***every*** monomial occurring in r is divisible by one in $\mathrm{LT}(g_i)$. Thus $r = 0$, and $g \in (g_1, \ldots, g_s)$. □

Standard (Gröbner) bases

Fix a monomial ordering of $k[X_1, \ldots, X_n]$.

DEFINITION 1.49. A finite subset $S = \{g_1, \ldots, g_s\}$ of an ideal $\mathfrak{a}$ is a ***standard (Grobner, Groebner, Gröbner) basis***[7] for $\mathfrak{a}$ if

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

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 1.50. *Every ideal has a standard basis, and it generates the ideal; if $\{g_1, \ldots, g_s\}$ 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.*

[7] 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.

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 $g_1, \ldots, g_s$ is 0, used only that $\{g_1, \ldots, g_s\}$ is a standard basis for $\mathfrak{a}$. □

REMARK 1.51. The proposition shows that, for $f \in \mathfrak{a}$, the remainder of f on division by $\{g_1, \ldots, g_s\}$ 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 chapter.

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

$$cX^\alpha f_i - dX^\beta f_j, \quad c, d \in k, \tag{**}$$

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 $f \in (f_1, \ldots, f_r)$. First transform $\{f_1, \ldots, f_r\}$ into a standard basis $\{g_1, \ldots, g_s\}$, and then divide f by $g_1, \ldots, g_s$ 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 $\{g_1, \ldots, g_s\}$ 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 $\{g_1, \ldots, g_s\}$ 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 1.52. Consider polynomials $f, g_1, \ldots, g_s \in k[X_1, \ldots, X_n]$. The algorithm that replaces $g_1, \ldots, g_s$ with a standard basis works entirely within $k[X_1, \ldots, X_n]$, 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 $k[X_1, \ldots, X_n]$ or in $K[X_1, \ldots, X_n]$, $K \supset k$, 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.

We conclude this chapter 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]);
```

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

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

```
> 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 symbols 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:

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

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

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

(d) For more information on Maple:

i) There is a brief discussion of the Grobner package in Cox et al. 1992, Appendix C, §1.
ii) 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).
iii) There are many books containing general introductions to Maple syntax.

(e) 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) `http://cocoa.dima.unige.it/`.
Macaulay 2 (Grayson and Stillman) `http://www.math.uiuc.edu/Macaulay2/`.

Exercises

1-1. Let k be an infinite field (not necessarily algebraically closed). Show that an $f \in k[X_1, \ldots, X_n]$ that is identically zero on k^n is the zero polynomial (i.e., has all its coefficients zero).

1-2. Find a minimal set of generators for the ideal

$$(X + 2Y, 3X + 6Y + 3Z, 2X + 4Y + 3Z)$$

in $k[X, Y, Z]$. What standard algorithm in linear algebra will allow you to answer this question for any ideal generated by homogeneous linear polynomials? Find a minimal set of generators for the ideal

$$(X + 2Y + 1, 3X + 6Y + 3X + 2, 2X + 4Y + 3Z + 3).$$

Chapter 2

Algebraic Sets

In this chapter, k is 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 $k[X_1, \ldots, X_n]$:

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

Note that

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

— more equations means fewer solutions.

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

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

Such a sum $\sum f_i g_i$ is zero at any point at which the g_i are all 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 $k[X_1, \ldots, X_n]$.

EXAMPLE 2.1. (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, then $V(S)$ 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 $\mathbb{R}$, although this can be misleading.

(c) For the empty set $\emptyset$, $V(\emptyset) = k^n$.

(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 $k[X_1, \ldots, X_n]$ 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 chapter. Here we give the slick proof.

THEOREM 2.2 (HILBERT BASIS THEOREM). *The ring $k[X_1, \ldots, X_n]$ is noetherian, i.e., every ideal is finitely generated.*

Since k itself is noetherian, and $k[X_1, \ldots, X_{n-1}][X_n] = k[X_1, \ldots, X_n]$, the theorem follows by induction from the next lemma.

LEMMA 2.3. *If A is noetherian, then so also is $A[X]$.*

PROOF. Recall that for a polynomial

$$f(X) = a_0 X^r + a_1 X^{r-1} + \cdots + a_r, \quad a_i \in A, \quad a_0 \neq 0,$$

r is called the degree of f, and a_0 is its leading coefficient.

Let $\mathfrak{a}$ be a proper ideal in $A[X]$, and let $\mathfrak{a}_i$ be the set of elements of A that occur as the leading coefficient of a polynomial in $\mathfrak{a}$ of degree $\leq i$. Then $\mathfrak{a}_i$ is an ideal in A, and

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots \subset \mathfrak{a}_i \subset \cdots.$$

Because A is noetherian, this sequence eventually becomes constant, say $\mathfrak{a}_d = \mathfrak{a}_{d+1} = \ldots$ (and $\mathfrak{a}_d$ consists of the leading coefficients of *all* polynomials in $\mathfrak{a}$).

For each $i \leq d$, choose a finite set $f_{i1}, f_{i2}, \ldots$ of polynomials in $\mathfrak{a}$ of degree i such that the leading coefficients a_{ij} of the f_{ij}'s generate $\mathfrak{a}_i$.

Let $f \in \mathfrak{a}$; we shall prove by induction on the degree of f that it lies in the ideal generated by the f_{ij}. When f has degree 0, it is zero, and so lies in (f_{ij}).

Suppose that f has degree $s \geq d$. Then $f = aX^s + \cdots$ with $a \in \mathfrak{a}_d$, and so

$$a = \sum\nolimits_j b_j a_{dj}, \quad \text{some } b_j \in A.$$

Now

$$f - \sum_j b_j f_{dj} X^{s-d}$$

has degree $< \deg(f)$, and so lies in (f_{ij}) by induction.

Suppose that f has degree $s \leq r$. Then a similar argument shows that

$$f - \sum b_j f_{sj}$$

has degree $< \deg(f)$ for suitable $b_j \in A$, and so lies in (f_{ij}) by induction. □

ASIDE 2.4. One may ask how many elements are needed to generate a given ideal $\mathfrak{a}$ in $k[X_1, \ldots, X_n]$, or, what is not quite the same thing, how many equations are needed to define a given 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 9.7), but often more are required. Determining exactly how many is an area of active research — see (9.14).

The Zariski topology

PROPOSITION 2.5. *There are the following relations:*

(a) $\mathfrak{a} \subset \mathfrak{b} \implies V(\mathfrak{a}) \supset V(\mathfrak{b})$;
(b) $V(0) = k^n$; $V(k[X_1, \ldots, X_n]) = \emptyset$;
(c) $V(\mathfrak{ab}) = V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$;
(d) $V(\sum_{i \in I} \mathfrak{a}_i) = \bigcap_{i \in I} V(\mathfrak{a}_i)$ *for any family of ideals* $(\mathfrak{a}_i)_{i \in I}$.

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

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

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*** on k^n. The induced topology on a subset V of k^n is called the ***Zariski topology*** on V.

The Zariski topology has many strange properties, but it is nevertheless of great importance. For the Zariski topology on k, the closed subsets are just the finite sets and the whole space, and so the topology is not Hausdorff. We shall see in (2.29) below that the proper closed subsets of k^2 are finite unions of (isolated) points and curves (zero sets of irreducible $f \in k[X, Y]$). 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 $k[X_1, \ldots, X_n]$, but first we consider the question of when a set of polynomials has a common zero, i.e., when the equations

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

are "consistent". Obviously, the equations

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

are inconsistent if there exist $f_i \in k[X_1, \ldots, X_n]$ such that $\sum f_i g_i = 1$, i.e., if $1 \in (g_1, \ldots, g_m)$ or, equivalently, $(g_1, \ldots, g_m) = k[X_1, \ldots, X_n]$. The next theorem provides a converse to this.

THEOREM 2.6 (HILBERT NULLSTELLENSATZ). [1] *Every proper ideal $\mathfrak{a}$ in $k[X_1, \ldots, X_n]$ has a zero in k^n.*

A point $P = (a_1, \ldots, a_n)$ in k^n defines a homomorphism "evaluate at P"

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

whose kernel contains $\mathfrak{a}$ if $P \in V(\mathfrak{a})$. Conversely, from a homomorphism $\varphi: k[X_1, \ldots, X_n] \to k$ of k-algebras whose kernel contains $\mathfrak{a}$, we obtain a point P in $V(\mathfrak{a})$, namely,

$$P = (\varphi(X_1), \ldots, \varphi(X_n)).$$

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

Since every proper ideal is contained in a maximal ideal, it suffices to prove this for a maximal ideal $\mathfrak{m}$. Then $K \stackrel{\text{def}}{=} k[X_1, \ldots, X_n]/\mathfrak{m}$ is a field, and it is finitely generated as an algebra over k (with generators $X_1 + \mathfrak{m}, \ldots, X_n + \mathfrak{m}$). 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 2.7 (ZARISKI'S LEMMA). *Let $k \subset K$ be fields (k is 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. The case $r = 0$ being trivial, we may suppose that $K = k[x_1, \ldots, x_r]$ with $r \geq 1$. If K is not algebraic over k, then at least one x_i, say x_1, is not algebraic over k. Then, $k[x_1]$ is a polynomial ring in one symbol over k, and its field of fractions $k(x_1)$ is a subfield of K. Clearly K is generated as a $k(x_1)$-algebra by $x_2, \ldots, x_r$, and so the induction hypothesis implies that $x_2, \ldots, x_r$ are algebraic over $k(x_1)$. According to (1.18), there exists a $d \in k[x_1]$ such that dx_i is integral over $k[x_1]$ for all $i \geq 2$. Let $f \in K = k[x_1, \ldots, x_r]$. For a sufficiently large N, $d^N f \in k[x_1, dx_2, \ldots, dx_r]$, and so

[1] Nullstellensatz = zero-points-theorem.

$d^N f$ is integral over $k[x_1]$ (1.16). When we apply this statement to an element f of $k(x_1)$, (1.21) shows that $d^N f \in k[x_1]$. Therefore, $k(x_1) = \bigcup_N d^{-N}k[x_1]$, but this is absurd, because $k[x_1]$ ($\simeq k[X]$) has infinitely many distinct monic irreducible polynomials[2] 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:

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

Clearly, it is an ideal in $k[X_1, \ldots, X_n]$. There are the following relations:

(a) $V \subset W \implies I(V) \supset I(W)$;
(b) $I(\emptyset) = k[X_1, \ldots, X_n]$; $I(k^n) = 0$;
(c) $I(\bigcup W_i) = \bigcap I(W_i)$.

Only the statement $I(k^n) = 0$ is (perhaps) not obvious. It says that, if a polynomial is nonzero (in the ring $k[X_1, \ldots, X_n]$), then it is nonzero at some point of k^n. This is true with k any infinite field (see Exercise 1-1). Alternatively, it follows from the strong Hilbert Nullstellensatz (cf. 2.14a below).

EXAMPLE 2.8. Let P be the point $(a_1, \ldots, a_n)$. Clearly $I(P) \supset (X_1 - a_1, \ldots, X_n - a_n)$, but $(X_1 - a_1, \ldots, X_n - a_n)$ is a maximal ideal, because "evaluation at $(a_1, \ldots, a_n)$" defines an isomorphism

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

As $I(P)$ is a proper ideal, it must equal $(X_1 - a_1, \ldots, X_n - a_n)$.

PROPOSITION 2.9. *For any subset $W \subset k^n$, $VI(W)$ is the smallest algebraic subset of k^n containing W. In particular, $VI(W) = W$ if W is an algebraic set.*

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

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

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

PROPOSITION 2.10. *Let $\mathfrak{a}$ be an ideal in a ring A.*
(a) The radical of $\mathfrak{a}$ is an ideal.
(b) $\mathrm{rad}(\mathrm{rad}(\mathfrak{a})) = \mathrm{rad}(\mathfrak{a})$.

PROOF. (a) If $a \in \mathrm{rad}(\mathfrak{a})$, then clearly $fa \in \mathrm{rad}(\mathfrak{a})$ for all $f \in A$. Suppose $a, b \in \mathrm{rad}(\mathfrak{a})$, with say $a^r \in \mathfrak{a}$ and $b^s \in \mathfrak{a}$. When we expand $(a + b)^{r+s}$ using the binomial theorem, we find that every term has a factor a^r or b^s, and so lies in $\mathfrak{a}$.
(b) If $a^r \in \mathrm{rad}(\mathfrak{a})$, then $a^{rs} = (a^r)^s \in \mathfrak{a}$ for some s. □

[2] 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.

An ideal is said to be ***radical*** if it equals its radical, i.e., if $f^r \in \mathfrak{a} \implies f \in \mathfrak{a}$. 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 integral domains are reduced, prime ideals (*a fortiori* maximal ideals) are radical.

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 $f^r(P) = f(P)^r$, 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 2.11 (STRONG HILBERT NULLSTELLENSATZ). *For any ideal $\mathfrak{a}$ in $k[X_1, \ldots, X_n]$, $IV(\mathfrak{a})$ is the radical of $\mathfrak{a}$; in particular, $IV(\mathfrak{a}) = \mathfrak{a}$ if $\mathfrak{a}$ is a radical ideal.*

PROOF. We have already noted that $IV(\mathfrak{a}) \supset \operatorname{rad}(\mathfrak{a})$. For the reverse inclusion, we have to show that if h is identically zero on $V(\mathfrak{a})$, then $h^N \in \mathfrak{a}$ for some $N > 0$; here $h \in k[X_1, \ldots, X_n]$. We may assume $h \neq 0$. Let $g_1, \ldots, g_m$ generate $\mathfrak{a}$, and consider the system of $m+1$ equations in $n+1$ variables, $X_1, \ldots, X_n, Y$,

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

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

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

(in the ring $k[X_1, \ldots, X_n, Y]$). On applying the homomorphism

$$\begin{cases} X_i \mapsto X_i \\ Y \mapsto h^{-1} \end{cases} : k[X_1, \ldots, X_n, Y] \to k(X_1, \ldots, X_n)$$

to the above equality, we obtain the identity

$$1 = \sum_{i=1}^{m} f_i(X_1, \ldots, X_n, h^{-1}) \cdot g_i(X_1, \ldots, X_n) \qquad (*)$$

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

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

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

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

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

COROLLARY 2.12. *The map $\mathfrak{a} \mapsto V(\mathfrak{a})$ defines a one-to-one correspondence between the set of radical ideals in $k[X_1, \ldots, X_n]$ 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 (2.11), and that $VI(W) = W$ if W is an algebraic set (2.9). Therefore, I and V are inverse maps. □

COROLLARY 2.13. *The radical of an ideal in $k[X_1, \ldots, X_n]$ is equal to the intersection of the maximal ideals containing it.*

PROOF. Let $\mathfrak{a}$ be an ideal in $k[X_1, \ldots, X_n]$. Because maximal ideals are radical, every maximal ideal containing $\mathfrak{a}$ also contains $\mathrm{rad}(\mathfrak{a})$:

$$\mathrm{rad}(\mathfrak{a}) \subset \bigcap_{\mathfrak{m} \supset \mathfrak{a}} \mathfrak{m}.$$

For each $P = (a_1, \ldots, a_n) \in k^n$, $\mathfrak{m}_P = (X_1 - a_1, \ldots, X_n - a_n)$ is a maximal ideal in $k[X_1, \ldots, X_n]$, and

$$f \in \mathfrak{m}_P \iff f(P) = 0$$

(see 2.8). Thus

$$\mathfrak{m}_P \supset \mathfrak{a} \iff P \in V(\mathfrak{a}).$$

If $f \in \mathfrak{m}_P$ for all $P \in V(\mathfrak{a})$, then f is zero on $V(\mathfrak{a})$, and so $f \in IV(\mathfrak{a}) = \mathrm{rad}(\mathfrak{a})$. We have shown that

$$\mathrm{rad}(\mathfrak{a}) \supset \bigcap_{P \in V(\mathfrak{a})} \mathfrak{m}_P.$$

□

REMARK 2.14. (a) Because $V(0) = k^n$,

$$I(k^n) = IV(0) = \mathrm{rad}(0) = 0;$$

in other words, only the zero polynomial is zero on the whole of k^n.

(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 $k[X_1, \ldots, X_n]$, and the minimal nonempty algebraic sets are the one-point sets. As

$$I((a_1, \ldots, a_n)) = (X_1 - a_1, \ldots, X_n - a_n)$$

(see 2.8), this shows that the maximal ideals of $k[X_1, \ldots, X_n]$ are exactly the ideals of the form $(X_1 - a_1, \ldots, X_n - a_n)$.

(c) The algebraic set $V(\mathfrak{a})$ is empty if and only if $\mathfrak{a} = k[X_1, \ldots, X_n]$, because

$$V(\mathfrak{a}) = \emptyset \Rightarrow \mathrm{rad}(\mathfrak{a}) = k[X_1, \ldots, X_n] \Rightarrow 1 \in \mathrm{rad}(\mathfrak{a}) \Rightarrow 1 \in \mathfrak{a}.$$

(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 $I(W \cap W') = \mathrm{rad}(I(W) + I(W'))$.

For example, let $W = V(X^2 - Y)$ and $W' = V(X^2 + Y)$; then $I(W \cap W') = \mathrm{rad}(X^2, Y) = (X, Y)$ (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.]

ASIDE 2.15. Let P be the set of subsets of k^n and let Q be the set of subsets of $k[X_1, \ldots, X_n]$. Then $I: P \to Q$ and $V: Q \to P$ define a simple Galois correspondence (cf. FT 7.17). Therefore, I and V define a one-to-one correspondence between IP and VQ. But the strong Nullstellensatz shows that IP consists exactly of the radical ideals, and (by definition) VQ consists of the algebraic subsets. Thus we recover Corollary 2.12.

Finding the radical of an ideal

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

PROPOSITION 2.16. *The polynomial $h \in \mathrm{rad}(\mathfrak{a})$ if and only if $1 \in (\mathfrak{a}, 1 - Yh)$ (the ideal in $k[X_1, \ldots, X_n, Y]$ generated by the elements of $\mathfrak{a}$ and $1 - Yh$).*

PROOF. We saw that $1 \in (\mathfrak{a}, 1 - Yh)$ implies $h \in \mathrm{rad}(\mathfrak{a})$ in the course of proving (2.11). Conversely, if $h^N \in \mathfrak{a}$, then

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

□

Since we have an algorithm for deciding whether or not a polynomial belongs to an ideal given a set of generators for the ideal – see Section 1 – we also have an algorithm deciding whether or not a polynomial belongs to the radical of the ideal, but not yet an algorithm for finding a set of generators for the radical. There do exist such algorithms (see Cox et al. 1992, p177 for references), and one has been implemented in the computer algebra system Macaulay 2 (see p29).

The Zariski topology on an algebraic set

We now examine more closely the Zariski topology on k^n and on an algebraic subset of k^n. Proposition 2.9 says that, for each subset W of k^n, $VI(W)$ is the closure of W, and (2.12) says that there is a one-to-one correspondence between the closed subsets of k^n and the radical ideals of $k[X_1, \ldots, X_n]$. Under this correspondence, the closed subsets of an algebraic set V correspond to the radical ideals of $k[X_1, \ldots, X_n]$ containing $I(V)$.

PROPOSITION 2.17. *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 ascending chain of open subsets $U_1 \subset U_2 \subset \cdots$ of V eventually becomes constant, i.e., for some m, $U_m = U_{m+1} = \cdots$; hence every descending chain of closed subsets of V eventually becomes constant.

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

PROOF. (a) Clearly $\{(a_1, \ldots, a_n)\}$ is the algebraic set defined by the ideal $(X_1 - a_1, \ldots, X_n - a_n)$.

(b) A sequence $V_1 \supset V_2 \supset \cdots$ of closed subsets of V gives rise to a sequence of radical ideals $I(V_1) \subset I(V_2) \subset \ldots$, which eventually becomes constant because $k[X_1, \ldots, X_n]$ 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 ***quasicompact*** (by Bourbaki at least; others call it compact, but Bourbaki requires a compact space to be Hausdorff). The proof of (c) shows that every noetherian space is quasicompact. Since an open subspace of a noetherian space is again noetherian, it will also be quasicompact.

The coordinate ring of an algebraic set

Let V be an algebraic subset of k^n, and let $I(V) = \mathfrak{a}$. The ***coordinate ring of*** V is

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

This is a finitely generated reduced k-algebra (because $\mathfrak{a}$ is radical), but it need not be an integral domain.

A function $V \to k$ of the form $P \mapsto f(P)$ for some $f \in k[X_1, \ldots, X_n]$ is said to be ***regular.***[3] Two polynomials $f, g \in k[X_1, \ldots, X_n]$ define the same regular function on V if only if they define the same element of $k[V]$. The coordinate function $x_i\colon V \to k$, $(a_1, \ldots, a_n) \mapsto a_i$ is regular, and $k[V] \simeq k[x_1, \ldots, x_n]$.

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

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

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

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

send a regular function on k^n to its restriction to V, and then to its restriction to W.

Write π for the map $k[X_1, \ldots, X_n] \to k[V]$. 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 $k[X_1, \ldots, X_n]$ 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 $k[X_1, \ldots, X_n]/\pi^{-1}(\mathfrak{b}) \simeq k[V]/\mathfrak{b}$). Clearly

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

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

For $h \in k[V]$, set

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

It is an open subset of V, because it is the complement of $V((h))$, and it is empty if and only if h is zero (2.14a).

[3] In the next chapter, we'll give a more general definition of regular function according to which these are exactly the regular functions on V, and so $k[V]$ will be the ***ring of regular functions on*** V.

PROPOSITION 2.18. *(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 $D(h)$, $h \in k[V]$, are a base for the topology on V, i.e., each $D(h)$ is open, and every 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 $V(\mathfrak{b})$, with $\mathfrak{b}$ an ideal in $k[V]$, and if $f_1, \ldots, f_m$ generate $\mathfrak{b}$, then $U = \bigcup D(f_i)$. □

The $D(h)$ are called the ***basic*** (or ***principal***) ***open subsets*** of V. We sometimes write V_h for $D(h)$. Note that

$$\begin{aligned} D(h) \subset D(h') &\iff V(h) \supset V(h') \\ &\iff \mathrm{rad}((h)) \subset \mathrm{rad}((h')) \\ &\iff h^r \in (h') \text{ some } r \\ &\iff h^r = h'g, \text{ some } g. \end{aligned}$$

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 topological space is said to be ***irreducible*** if it is not the union of two proper closed subsets; equivalently, if any two nonempty open subsets have a nonempty intersection, or if every nonempty open subset is dense.

If an irreducible space W is a finite union of closed subsets, $W = W_1 \cup \ldots \cup W_r$, then $W = W_1$ or $W_2 \cup \ldots \cup W_r$; if the latter, then $W = W_2$ or $W_3 \cup \ldots \cup W_r$, etc.. Continuing in this fashion, we find that $W = W_i$ for some i.

The notion of irreducibility is not useful for Hausdorff topological spaces, because the only irreducible Hausdorff spaces are those consisting of a single point – two points would have disjoint open neighbourhoods contradicting the second condition.

PROPOSITION 2.19. *An algebraic set W is irreducible and only if $I(W)$ is prime.*

PROOF. $\Longrightarrow$: Suppose $fg \in I(W)$. At each point of W, either f is zero 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 $f \in I(W)$. This shows that $I(W)$ 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 (2.5) 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 $f \in \mathfrak{a} \smallsetminus I(W)$. For all $g \in \mathfrak{b}$,

$$fg \in \mathfrak{a} \cap \mathfrak{b} = I(W).$$

Because $I(W)$ 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 $k[X_1, \ldots, X_n]$ 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 those of the form $(x_1 - a_1, \ldots, x_n - a_n)$, $(a_1, \ldots, a_n) \in V$.

EXAMPLE 2.20. Let $f \in k[X_1, \ldots, X_n]$. As we showed in (1.14), $k[X_1, \ldots, X_n]$ is a unique factorization domain, and so (f) is a prime ideal if and only if f is irreducible (1.15). Thus

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

On the other hand, suppose f factors,

$$f = \prod f_i^{m_i}, \quad f_i \text{ distinct irreducible polynomials.}$$

Then

$$\begin{aligned}(f) &= \bigcap (f_i^{m_i}), \quad (f_i^{m_i}) \text{ distinct primary}^4\text{ideals,}\\ \operatorname{rad}((f)) &= \bigcap (f_i), \quad (f_i) \text{ distinct prime ideals,}\\ V(f) &= \bigcup V(f_i), \quad V(f_i) \text{ distinct irreducible algebraic sets.}\end{aligned}$$

PROPOSITION 2.21. *Let V be a noetherian topological space. Then V is a finite union of irreducible closed subsets, $V = V_1 \cup \ldots \cup V_m$. 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 that V can not be written as a *finite* union of irreducible closed subsets. Then, because V is noetherian, there will be a closed subset W of V that is minimal among those that cannot be written in this way. But W itself cannot 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, we deduce 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

$$V = V_1 \cup \ldots \cup V_m = W_1 \cup \ldots \cup W_n$$

are two irredundant decompositions. Then $V_i = \bigcup_j (V_i \cap W_j)$, and so, because V_i is irreducible, $V_i = V_i \cap W_j$ for some j. Consequently, there is a function $f\colon \{1, \ldots, m\} \to \{1, \ldots, n\}$ such that $V_i \subset W_{f(i)}$ for each i. Similarly, there is a function $g\colon \{1, \ldots, n\} \to \{1, \ldots, m\}$ such that $W_j \subset V_{g(j)}$ for each 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 $fg = \mathrm{id}$. Thus f and g are bijections, and the decompositions differ only in the numbering of the sets. □

[3] In a noetherian ring A, a proper ideal $\mathfrak{q}$ is said to ***primary*** if every zero-divisor in $A/\mathfrak{q}$ is nilpotent.

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 2.20, the $V(f_i)$ are the irreducible components of $V(f)$.

COROLLARY 2.22. *A radical ideal $\mathfrak{a}$ in $k[X_1, \ldots, X_n]$ is a finite intersection of prime ideals, $\mathfrak{a} = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_n$; if there are no inclusions among the $\mathfrak{p}_i$, then the $\mathfrak{p}_i$ are uniquely determined up to order.*

PROOF. Write $V(\mathfrak{a})$ as a union of its irreducible components, $V(\mathfrak{a}) = \bigcup V_i$, and take $\mathfrak{p}_i = I(V_i)$. □

REMARK 2.23. (a) An irreducible topological space is connected, but a connected topological space need not be irreducible. For example, $V(X_1X_2)$ is the union of the coordinate axes in k^2, which is connected but not irreducible. An algebraic subset V of k^n is not connected if and only if there exist ideals $\mathfrak{a}$ and $\mathfrak{b}$ such that $\mathfrak{a} \cap \mathfrak{b} = I(V)$ and $\mathfrak{a} + \mathfrak{b} \neq k[X_1, \ldots, X_n]$.

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

(c) 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, $f = f_1 \ldots f_r$, and $(f) = (f_1) \cap \ldots \cap (f_r)$ (a polynomial is divisible by f if and only if it is divisible by each f_i).

(d) In a noetherian ring, every proper ideal $\mathfrak{a}$ has a decomposition into primary ideals: $\mathfrak{a} = \bigcap \mathfrak{q}_i$ (see CA §13). For radical ideals, this becomes a simpler decomposition into prime ideals, as in the corollary. For an ideal (f) with $f = \prod f_i^{m_i}$, it is the decomposition $(f) = \bigcap (f_i^{m_i})$ noted in Example 2.20.

Dimension

We briefly introduce the notion of the dimension of an algebraic set. In chapter 9 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 (see FT §8).[5]

EXAMPLE 2.24. (a) Let $V = k^n$; then $k(V) = k(X_1, \ldots, X_n)$, and so $\dim(V) = n$.

(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 $k[X_{i_1}, \ldots, X_{i_d}]$ where the X_{i_j} are the "free" variables in the system of linear equations defining V — see 5.12).

In linear algebra, we justify saying V has dimension n by proving that its elements are parametrized by n-tuples. 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 exists a finite-to-one map to k^n (see 8.12).

[5] According to CA, 12.8, the transcendence degree of $k(V)$ is equal to the Krull dimension of $k[V]$; cf. 2.30 below.

(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 (2.14b) that this implies that $V(\mathfrak{p})$ is a point.

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

PROPOSITION 2.25. *An irreducible hypersurface in k^n has dimension $n - 1$.*

PROOF. An irreducible hypersurface is the zero set of an irreducible polynomial f (see 2.20). Let

$$k[x_1, \ldots, x_n] = k[X_1, \ldots, X_n]/(f), \quad x_i = X_i + \mathfrak{p},$$

and let $k(x_1, \ldots, x_n)$ be the field of fractions of $k[x_1, \ldots, x_n]$. Since f is not zero, some X_i, say, X_n, occurs in it. Then X_n occurs in every nonzero multiple of f, and so no nonzero polynomial in $X_1, \ldots, X_{n-1}$ belongs to (f). This means that $x_1, \ldots, x_{n-1}$ are algebraically independent. On the other hand, x_n is algebraic over $k(x_1, \ldots, x_{n-1})$, and so $\{x_1, \ldots, x_{n-1}\}$ is a transcendence basis for $k(x_1, \ldots, x_n)$ over k. □

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

PROPOSITION 2.26. *If V is irreducible and Z is a proper algebraic subset 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 $k[Z] = k[V]/\mathfrak{p}$.

Write

$$k[V] = k[X_1, \ldots, X_n]/I(V) = k[x_1, \ldots, x_n].$$

Let $f \in k[V]$. The image $\bar{f}$ of f in $k[V]/\mathfrak{p} = k[Z]$ is the restriction of f to Z. With this notation, $k[Z] = k[\bar{x}_1, \ldots, \bar{x}_n]$. Suppose that $\dim Z = d$ and that the X_i have been numbered so that $\bar{x}_1, \ldots, \bar{x}_d$ are algebraically independent (see FT 8.9 for the proof that this is possible). I will show that, for any nonzero $f \in \mathfrak{p}$, the $d + 1$ elements $x_1, \ldots, x_d, f$ 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

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

with $a_i(x_1, \ldots, x_d) \in k[x_1, \ldots, x_d]$ and not all zero. Because V is irreducible, $k[V]$ is an integral domain, and so we can cancel a power of f if necessary to make $a_m(x_1, \ldots, x_d)$

nonzero. On restricting the functions in the above equality to Z, i.e., applying the homomorphism $k[V] \to k[Z]$, we find that

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

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

PROPOSITION 2.27. *Let V be an irreducible variety such that $k[V]$ is a unique factorization domain (for example, $V = \mathbb{A}^d$). If $W \subset V$ is a closed subvariety of dimension* $\dim V - 1$, *then $I(W) = (f)$ for some $f \in k[V]$.*

PROOF. We know that $I(W) = \bigcap I(W_i)$ where the W_i are the irreducible components of W, and so if we can prove $I(W_i) = (f_i)$ then $I(W) = (f_1 \cdots f_r)$. Thus we may suppose that W is irreducible. Let $\mathfrak{p} = I(W)$; it is a prime ideal, and it is nonzero because otherwise $\dim(W) = \dim(V)$. Therefore it contains an irreducible polynomial f. From (1.15) we know (f) is prime. If $(f) \neq \mathfrak{p}$, then we have

$$W = V(\mathfrak{p}) \subsetneqq V((f)) \subsetneqq V,$$

and $\dim(W) < \dim(V(f)) < \dim V$ (see 2.26), which contradicts the hypothesis. □

EXAMPLE 2.28. Let $F(X, Y)$ and $G(X, Y)$ be nonconstant polynomials with no common factor. Then $V(F(X, Y))$ has dimension 1 by (2.25), and so $V(F(X, Y)) \cap V(G(X, Y))$ must have dimension zero; it is therefore a finite set.

EXAMPLE 2.29. We classify the irreducible closed subsets V of k^2. If V has dimension 2, then (by 2.26) 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 $(X - a, Y - b)$.

ASIDE 2.30. Later (9.4) we shall show that if, in the situation of (2.26), 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,

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

Exercises

2-1. Find $I(W)$, where $V = (X^2, XY^2)$. Check that it is the radical of (X^2, XY^2).

2-2. Identify k^{m^2} with the set of $m \times m$ matrices. Show that, for all r, the set of matrices with rank $\leq r$ is an algebraic subset of k^{m^2}.

2-3. Let $V = \{(t, \ldots, t^n) \mid t \in k\}$. Show that V is an algebraic subset of k^n, and that $k[V] \approx k[X]$ (polynomial ring in one variable). (Assume k has characteristic zero.)

2-4. Using only that $k[X, Y]$ is a unique factorization domain and the results of §§1,2, show that the following is a complete list of prime ideals in $k[X, Y]$:

(a) (0);
(b) $(f(X, Y))$ for f an irreducible polynomial;
(c) $(X - a, Y - b)$ for $a, b \in k$.

2-5. Let A and B be (not necessarily commutative) $\mathbb{Q}$-algebras of finite dimension over $\mathbb{Q}$, and let $\mathbb{Q}^{\mathrm{al}}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. Show that if $\mathrm{Hom}_{\mathbb{C}\text{-algebras}}(A \otimes_{\mathbb{Q}} \mathbb{C}, B \otimes_{\mathbb{Q}} \mathbb{C}) \neq \emptyset$, then $\mathrm{Hom}_{\mathbb{Q}^{\mathrm{al}}\text{-algebras}}(A \otimes_{\mathbb{Q}} \mathbb{Q}^{\mathrm{al}}, B \otimes_{\mathbb{Q}} \mathbb{Q}^{\mathrm{al}}) \neq \emptyset$. (Hint: The proof takes only a few lines.)

Chapter 3

Affine Algebraic Varieties

In this chapter, we define the structure of a ringed space on an algebraic set, 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 §4, 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.

Ringed spaces

Let V be a topological space and k a field.

DEFINITION 3.1. 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 a k-subalgebra of the algebra of all k-valued functions on U, i.e., $\mathcal{O}_V(U)$ contains the constant functions and, if f, g lie in $\mathcal{O}_V(U)$, then so also do $f+g$ 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) A function $f\colon U \to k$ on an open subset U of V is in $\mathcal{O}_V(U)$ if $f|U_i \in \mathcal{O}_V(U_i)$ for all U_i in some open covering of U.

Conditions (b) and (c) require that a function f on U lies in $\mathcal{O}_V(U)$ if and only if each point P of U has a neighborhood U_P such that $f|U_P$ lies in $\mathcal{O}_V(U_P)$; in other words, the condition for f to lie in $\mathcal{O}_V(U)$ is *local*.

EXAMPLE 3.2. (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 ***smooth*** (or ***infinitely differentiable***) if its partial derivatives of all orders exist and are continuous. 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 smooth 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![1] When "constant" is replaced with "locally constant", $\mathcal{O}_V$ 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 open neighbourhood U'' of P contained in U and U'. This is an equivalence relation, and an equivalence class of pairs is called a ***germ*** of a function at P (relative to $\mathcal{O}_V$). 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,

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

A germ of a function at P is defined by a function f on a neigbourhood of P (section of $\mathcal{O}_V$), and two such functions define the same germ if and only if they agree in a possibly smaller neighbourhood of P.

EXAMPLE 3.3. Let $\mathcal{O}_V$ be the sheaf of holomorphic functions on $V = \mathbb{C}$, and let $c \in \mathbb{C}$. A power series $\sum_{n \geq 0} a_n(z-c)^n$, $a_n \in \mathbb{C}$, is called ***convergent*** if it converges on some open neighbourhood of c. The set of such power series is a $\mathbb{C}$-algebra, and I claim that it is canonically isomorphic to the $\mathbb{C}$-algebra of germs of functions $\mathcal{O}_c$.

Let f be a holomorphic function on a neighbourhood U of c. Then f has a unique power series expansion $f = \sum a_n(z-c)^n$ in some (possibly smaller) open neighbourhood of c (Cartan 1963[2], II 2.6). Moreover, another holomorphic function f_1 on a neighbourhood U_1 of c defines the same power series if and only if f_1 and f agree on some neighbourhood of c contained in $U \cap U'$ (ibid. I 4.3). Thus we have a well-defined injective map from the ring of germs of holomorphic functions at c to the ring of convergent power series, which is obviously surjective.

[1] If V is reducible, then it contains disjoint open subsets, say U_1 and U_2. Let f be the function on the union of U_1 and U_2 taking the constant value 1 on U_1 and the constant value 2 on U_2. Then f is not in $\mathcal{O}_V(U_1 \cup U_2)$, and so condition 3.1c fails.

[2] Cartan, Henri. Elementary theory of analytic functions of one or several complex variables. Hermann, Paris; Addison-Wesley; 1963.

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

$$P \mapsto h(P): V \to k, \text{ and } P \mapsto 1/h(P): D(h) \to k.$$

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

$$P \mapsto \frac{g(P)}{h(P)}: D(h) \to k.$$

We say that a function $f: U \to k$ 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 $P \in U$, there exist $g, h \in k[V]$ with $h(P) \neq 0$ such that the functions f and $\frac{g}{h}$ agree in a neighbourhood of P. Write $\mathcal{O}_V(U)$ for the set of regular functions on U.

For example, if $V = k^n$, then a function $f: U \to k$ is regular at a point $P \in U$ if there exist polynomials $g(X_1, \ldots, X_n)$ and $h(X_1, \ldots, X_n)$ with $h(P) \neq 0$ such that $f(Q) = \frac{g(P)}{h(P)}$ for all Q in a neighbourhood of P.

PROPOSITION 3.4. *The map $U \mapsto \mathcal{O}_V(U)$ defines a sheaf of k-algebras on V.*

PROOF. We have to check the conditions (3.1).

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

(b,c) It is clear from the definition that the condition for f to be regular is local. □

Let $g, h \in k[V]$ and $m \in \mathbb{N}$. Then $P \mapsto g(P)/h(P)^m$ is a regular function on $D(h)$, and we'll show that all regular functions on $D(h)$ are of this form, i.e., $\Gamma(D(h), \mathcal{O}_V) \simeq k[V]_h$. In particular, the regular functions on V itself are exactly those defined by elements of $k[V]$.

LEMMA 3.5. *The function $P \mapsto g(P)/h(P)^m$ on $D(h)$ is the zero function if and only 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 $g(P)h(P) = 0$ for all $P \in V$, and so $g(P) = 0$ for all $P \in D(h)$. □

The lemma shows that the canonical map $k[V]_h \to \mathcal{O}_V(D(h))$ is well-defined and injective. The next proposition shows that it is also surjective.

PROPOSITION 3.6. *(a) The canonical map $k[V]_h \to \Gamma(D(h), \mathcal{O}_V)$ is an isomorphism.*

(b) For any $P \in V$, there is a canonical isomorphism $\mathcal{O}_P \to k[V]_{\mathfrak{m}_P}$, where $\mathfrak{m}_P$ is the maximal ideal $I(P)$.

PROOF. (a) 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 $D(h) = \bigcup V_i$ and elements $g_i, h_i \in k[V]$ with h_i nowhere zero on V_i such that $f|V_i = \frac{g_i}{h_i}$. We may assume that each set V_i is basic, say, $V_i = D(a_i)$ for 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 $N \in \mathbb{N}$ and $g_i' \in k[V]$ (see p39). 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 assume that $V_i = D(h_i)$.

We now have that $D(h) = \bigcup D(h_i)$ and that $f|D(h_i) = \frac{g_i}{h_i}$. Because $D(h)$ is quasicompact, 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 Lemma 3.5) that

$$h_i h_j (g_i h_j - g_j h_i) = 0, \text{ i.e., } h_i h_j^2 g_i = h_i^2 h_j g_j. \tag{*}$$

Because $D(h) = \bigcup D(h_i) = \bigcup D(h_i^2)$, the set $V((h)) = V((h_1^2, \ldots, h_m^2))$, and so $h \in \operatorname{rad}(h_1^2, \ldots, h_m^2)$: there exist $a_i \in k[V]$ such that

$$h^N = \sum_{i=1}^{m} a_i h_i^2. \tag{**}$$

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

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

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

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 $D(h_j)$:

$$h_j^2 \sum_{i=1}^{m} a_i g_i h_i = f h_j^2 h^N.$$

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) In the definition of the germs of a sheaf at P, it suffices to consider pairs (f, U) with U lying in a some basis for the neighbourhoods of P, for example, the basis provided by the basic open subsets. Therefore,

$$\mathcal{O}_P = \varinjlim_{h(P)\neq 0} \Gamma(D(h), \mathcal{O}_V) \overset{(a)}{\simeq} \varinjlim_{h \notin \mathfrak{m}_P} k[V]_h \overset{1.29(b)}{\simeq} k[V]_{\mathfrak{m}_P}.$$

□

REMARK 3.7. Let V be an affine variety and P a point on V. Proposition 1.30 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.

REMARK 3.8. (a) Let V be an algebraic subset of k^n, and let $A = k[V]$. The proposition and (2.18) allow us to describe $(V, \mathcal{O}_V)$ purely in terms of A:

- ◇ V is the set of maximal ideals in A; for each $f \in A$, let $D(f) = \{\mathfrak{m} \mid f \notin \mathfrak{m}\}$;
- ◇ the topology on V is that for which the sets $D(f)$ form a base;
- ◇ $\mathcal{O}_V$ is the unique sheaf of k-algebras on V for which $\Gamma(D(f), \mathcal{O}_V) = A_f$.

(b) When V is irreducible, all the rings attached to it are subrings of the field $k(V)$. In this case,

$$\begin{aligned}
\Gamma(D(h), \mathcal{O}_V) &= \left\{g/h^N \in k(V) \mid g \in k[V], \quad N \in \mathbb{N}\right\} \\
\mathcal{O}_P &= \{g/h \in k(V) \mid h(P) \neq 0\} \\
\Gamma(U, \mathcal{O}_V) &= \bigcap\nolimits_{P \in U} \mathcal{O}_P \\
&= \bigcap \Gamma(D(h_i), \mathcal{O}_V) \text{ if } U = \bigcup D(h_i).
\end{aligned}$$

Note that every element of $k(V)$ defines a function on some dense open subset of V. Following tradition, we call the elements of $k(V)$ ***rational functions*** on V.[3] The equalities show that the regular functions on an open $U \subset V$ are the rational functions on V that are defined at each point of U (i.e., lie in $\mathcal{O}_P$ for each $P \in U$).

EXAMPLE 3.9. (a) Let $V = k^n$. Then the ring of regular functions on V, $\Gamma(V, \mathcal{O}_V)$, is $k[X_1, \ldots, X_n]$. For any nonzero polynomial $h(X_1, \ldots, X_n)$, the ring of regular functions on $D(h)$ is

$$\left\{g/h^N \in k(X_1, \ldots, X_n) \mid g \in k[X_1, \ldots, X_n], \quad N \in \mathbb{N}\right\}.$$

For any point $P = (a_1, \ldots, a_n)$, the ring of germs of functions at P is

$$\mathcal{O}_P = \{g/h \in k(X_1, \ldots, X_n) \mid h(P) \neq 0\} = k[X_1, \ldots, X_n]_{(X_1 - a_1, \ldots, X_n - a_n)},$$

and its maximal ideal consists of those g/h with $g(P) = 0$.

(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 2.25). Since $U = D(X) \cup D(Y)$, the ring of regular functions on U is

$$\mathcal{O}_U(U) = k[X, Y]_X \cap k[X, Y]_Y$$

(intersection inside $k(X, Y)$). A regular function f on U can be expressed

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

[3]The terminology is similar to that of "meromorphic function", which also are not functions on the whole space.

where we can assume $X \nmid g$ and $Y \nmid h$. On multiplying through by $X^N Y^M$, 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 hand side either, and so $N = 0$. Similarly, $M = 0$, and so $f \in k[X,Y]$: every regular function on U extends uniquely 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

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

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 3.10. (a) Let V and V' be topological spaces endowed with their sheaves $\mathcal{O}_V$ and $\mathcal{O}_{V'}$ of continuous real valued functions. Every 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, and let x_i be the coordinate function $(a_1, \ldots, a_n) \mapsto a_i$. Recall from advanced calculus that a map

$$\varphi\colon U \to U' \subset \mathbb{R}^m$$

is said to be smooth (infinitely differentiable) if each of its component functions $\varphi_i = x_i \circ \varphi\colon U \to \mathbb{R}$ has continuous partial derivatives of all orders, in which case $f \circ \varphi$ is smooth for all smooth $f\colon U' \to \mathbb{R}$. Therefore, when U and U' are endowed with their sheaves of smooth functions, a continuous map $\varphi\colon U \to U'$ is smooth if and only if it is a morphism of ringed spaces.

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

REMARK 3.11. 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 homomorphism

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

for each $P \in V$, namely, the homomorphism sending the germ represented by (f, U) to the germ represented by $(f \circ \varphi, \varphi^{-1}(U))$.

Affine algebraic varieties

We have just seen that every algebraic set $V \subset k^n$ gives rise to a ringed space $(V, \mathcal{O}_V)$. A ringed space isomorphic to one of this form is called an ***affine algebraic variety over*** k. A map $f\colon V \to W$ of affine varieties is ***regular*** (or a ***morphism of affine algebraic varieties***) if it is a morphism of ringed spaces. With these definitions, the affine algebraic varieties become a category. Since we consider no nonalgebraic affine varieties, we shall sometimes drop "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 $\mathbb{A}^n$. I now explain how to construct "unembedded" affine varieties.

An ***affine k-algebra*** is defined to be a reduced finitely generated k-algebra. For such an algebra A, there exist $x_i \in A$ such that $A = k[x_1, \ldots, x_n]$, and the kernel of the homomorphism

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

is a radical ideal. Therefore (2.13) implies that the intersection of the maximal ideals in A is 0. Moreover, Zariski's lemma 2.7 implies that, for any maximal ideal $\mathfrak{m} \subset A$, 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 attach a ringed space $(V, \mathcal{O}_V)$ to A by letting V be the set of maximal ideals in A. For $f \in A$ let

$$D(f) = \{\mathfrak{m} \mid f(\mathfrak{m}) \neq 0\} = \{\mathfrak{m} \mid f \notin \mathfrak{m}\}.$$

Since $D(fg) = D(f) \cap D(g)$, there is a topology on V for which the $D(f)$ form a base. A pair of elements $g, h \in A$, $h \neq 0$, gives rise to a function

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

and, for U an open subset of V, we define $\mathcal{O}_V(U)$ to be any function $f \colon U \to k$ that is of this form in a neighbourhood of each point of U.

PROPOSITION 3.12. *The pair $(V, \mathcal{O}_V)$ is an affine variety with $\Gamma(V, \mathcal{O}_V) = A$.*

PROOF. Represent A as a quotient $k[X_1, \ldots, X_n]/\mathfrak{a} = k[x_1, \ldots, x_n]$. Then $(V, \mathcal{O}_V)$ is isomorphic to the ringed space attached to $V(\mathfrak{a})$ (see 3.8(a)). □

We write $\operatorname{spm}(A)$ for the topological space V, and $\operatorname{Spm}(A)$ for the ringed space $(V, \mathcal{O}_V)$.

PROPOSITION 3.13. *A ringed space $(V, \mathcal{O}_V)$ is an affine variety if and only if $\Gamma(V, \mathcal{O}_V)$ is an affine k-algebra and the canonical map $V \to \operatorname{spm}(\Gamma(V, \mathcal{O}_V))$ is an isomorphism of ringed spaces.*

PROOF. Let $(V, \mathcal{O}_V)$ be an affine variety, and let $A = \Gamma(V, \mathcal{O}_V)$. For any $P \in V$, $\mathfrak{m}_P =_{\mathrm{df}} \{f \in A \mid f(P) = 0\}$ is a maximal ideal in A, and it is straightforward to check that $P \mapsto \mathfrak{m}_P$ is an isomorphism of ringed spaces. Conversely, if $\Gamma(V, \mathcal{O}_V)$ is an affine k-algebra, then the proposition shows that $\operatorname{Spm}(\Gamma(V, \mathcal{O}_V))$ is an affine variety. □

The category of affine algebraic varieties

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

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, $\mathfrak{m} = \alpha^{-1}(\mathfrak{n})$ is maximal in A because $A/\mathfrak{m} \to B/\mathfrak{n} = k$ is an injective map of k-algebras which implies that $A/\mathfrak{m} = k$. Thus α defines a map

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

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

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

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

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

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 $\operatorname{spm}(A)$ to regular functions on the inverse image of the open subset. Thus α defines a morphism of ringed spaces $\operatorname{Spm}(B) \to \operatorname{Spm}(A)$.

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 3.14. *For any affine algebras A and B,*

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

for any affine varieties V and W,

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

In terms of categories, Proposition 3.14 can now be restated as:

PROPOSITION 3.15. *The functor $A \mapsto \operatorname{Spm} A$ is a (contravariant) equivalence from the category of affine k-algebras to that of affine algebraic varieties with quasi-inverse $(V, \mathcal{O}_V) \mapsto \Gamma(V, \mathcal{O}_V)$.*

Explicit description of morphisms of affine varieties

PROPOSITION 3.16. *Let $V = V(\mathfrak{a}) \subset k^m$, $W = V(\mathfrak{b}) \subset k^n$. The following conditions on a continuous map $\varphi\colon V \to W$ are equivalent:*

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

PROOF. (a) $\implies$ (b). By definition $\varphi_i = y_i \circ \varphi$ where y_i is the coordinate function

$$(b_1, \ldots, b_n) \mapsto b_i\colon W \to k.$$

Hence this implication follows directly from the definition of a regular map.

(b) $\implies$ (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 it sends $k[W]$ into $k[V]$.

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

$$\alpha(f) \in \mathfrak{m}_P \iff f(\varphi(P)) = 0 \iff f(Q) = 0 \iff f \in \mathfrak{m}_Q.$$

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

REMARK 3.17. For $P \in V$, the maximal ideal in $\mathcal{O}_{V,P}$ consists of the germs represented by pairs (f, U) with $f(P) = 0$. Clearly therefore, the map $\mathcal{O}_{W,\varphi(P)} \to \mathcal{O}_{V,P}$ defined by φ (see 3.11) maps $\mathfrak{m}_{\varphi(P)}$ into $\mathfrak{m}_P$, i.e., it is a local homomorphism of local rings.

Now consider equations

$$\begin{aligned} Y_1 &= f_1(X_1, \ldots, X_m) \\ &\ldots \\ Y_n &= f_n(X_1, \ldots, X_m). \end{aligned}$$

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

$$(a_1, \ldots, a_m) \mapsto (f_1(a_1, \ldots, a_m), \ldots, f_n(a_1, \ldots, a_m)).$$

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

$$Y_i \mapsto f_i(X_1, \ldots, X_n).$$

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

$$\alpha(g)(P) = g(\ldots, f_i(P), \ldots) = g(\varphi(P)).$$

Now consider closed subsets $V(\mathfrak{a}) \subset k^m$ and $V(\mathfrak{b}) \subset k^n$ 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 $g \in \mathfrak{b}$; for $Q \in V(\mathfrak{b})$,

$$\alpha(g)(Q) = g(\varphi(Q)) = 0,$$

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

$$f(\varphi(P)) = \alpha(f)(P) = 0,$$

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

Thus, we see that the regular maps

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

are all of the form

$$P \mapsto (f_1(P), \ldots, f_m(P)), \quad f_i \in k[X_1, \ldots, X_n].$$

In particular, they all extend to regular maps $\mathbb{A}^n \to \mathbb{A}^m$.

EXAMPLE 3.18. (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

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

According to (3.14)

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

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, $\mathbb{A}^0 = \mathrm{Spm}\, k$. Then, for any affine variety V,

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

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

(c) Consider $t \mapsto (t^2, t^3)\colon \mathbb{A}^1 \to \mathbb{A}^2$. This is bijective onto its image,

$$V\colon \quad Y^2 = X^3,$$

but it is not an isomorphism onto its image – the inverse map is not regular. Because of (3.15), 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 its 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) Let k have 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 corresponding map on rings,

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

is not surjective.

This is the famous ***Frobenius map.*** Take k to be the algebraic closure of $\mathbb{F}_p$, and write F for the map. Recall that for each $m \geq 1$ there is a unique subfield $\mathbb{F}_{p^m}$ of k of degree m over $\mathbb{F}_p$, and that its elements are the solutions of $X^{p^m} = X$ (FT 4.18). Therefore, the fixed points of F^m are precisely the points of $\mathbb{A}^n$ with coordinates in $\mathbb{F}_{p^m}$. Let $f(X_1, \ldots, X_n)$ be a polynomial with coefficients in $\mathbb{F}_{p^m}$, say,

$$f = \sum c_{i_1 \cdots i_n} X_1^{i_1} \cdots X_n^{i_n}, \quad c_{i_1 \cdots i_n} \in \mathbb{F}_{p^m}.$$

Let $f(a_1, \ldots, a_n) = 0$. 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 $f(a_1^{p^m}, \ldots, a_n^{p^m}) = 0$. Here we have used that the binomial theorem takes the simple form $(X+Y)^{p^m} = X^{p^m} + Y^{p^m}$ in characteristic p. Thus F^m maps $V(f)$ into itself, and its fixed points are the solutions of

$$f(X_1, \ldots, X_n) = 0$$

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

In one of the most beautiful pieces of mathematics of the second half of the twentieth century, Grothendieck defined a cohomology theory (étale cohomology) and proved a fixed point formula that allowed him to express the number of solutions of a system of polynomial equations with coordinates in $\mathbb{F}_{p^n}$ as an alternating sum of traces of operators on finite-dimensional vector spaces, and Deligne used this to obtain very precise estimates for the number of solutions. See my course notes: Lectures on Etale Cohomology.

Subvarieties

Let A be an affine k-algebra. For any ideal $\mathfrak{a}$ in A, we define

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

This is a closed subset of $\operatorname{spm}(A)$, 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

$$\operatorname{Spm}(A/\mathfrak{a}) \to \operatorname{Spm}(A)$$

The image is $V(\mathfrak{a})$, and $\operatorname{spm}(A/\mathfrak{a}) \to V(\mathfrak{a})$ is a homeomorphism. Thus every closed subset of $\operatorname{spm}(A)$ 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 3.19. 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 3.20. *Let $(V, \mathcal{O}_V)$ be an affine variety and let h be a nonzero element of $k[V]$. Then*

$$(D(h), \mathcal{O}_V|D(h)) \simeq \mathrm{Spm}(A_h);$$

in particular, it is an affine variety.

PROOF. The map $A \to A_h$ defines a morphism $\mathrm{spm}(A_h) \to \mathrm{spm}(A)$. The image is $D(h)$, and it is routine (using (1.29)) to verify the rest of the statement. □

If $V = V(\mathfrak{a}) \subset k^n$, then

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

defines an isomorphism of $D(h)$ onto $V(\mathfrak{a}, 1 - hX_{n+1})$. For example, there is an isomorphism of affine varieties

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

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

REMARK 3.21. We have seen that all closed subsets and all basic open subsets of an affine variety V are again affine varieties with their natural ringed structure, but this is not true for all open subsets U. As we saw in (3.13), if U is affine, then the natural map $U \to \mathrm{spm}\, \Gamma(U, \mathcal{O}_U)$ is a bijection. But for $U = \mathbb{A}^2 \smallsetminus (0,0) = D(X) \cup D(Y)$, we know that $\Gamma(U, \mathcal{O}_{\mathbb{A}^2}) = k[X, Y]$ (see 3.9b), but $U \to \mathrm{spm}\, k[X, Y]$ 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 chapter that it is a (nonaffine) algebraic variety.

Properties of the regular map defined by specm(α)

PROPOSITION 3.22. *Let $\alpha \colon A \to B$ be a homomorphism of affine k-algebras, and let*

$$\varphi \colon \mathrm{Spm}(B) \to \mathrm{Spm}(A)$$

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 is injective.*
(b) *φ defines an isomorphism of $\mathrm{Spm}(B)$ onto a closed subvariety of $\mathrm{Spm}(A)$ if and only if α is surjective.*

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

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

On the other hand, if the image of φ is not dense, then the closure of its image will be a proper closed subset of $\mathrm{Spm}(A)$, and so there will be a nonzero function $f \in A$ that is zero on it. Then $f \circ \varphi = 0$.

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

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

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

Affine space without coordinates

Let E be a vector space over k of dimension n. The set $\mathbb{A}(E)$ of points of E has a natural structure of an algebraic variety: the choice of a basis for E defines an bijection $\mathbb{A}(E) \to \mathbb{A}^n$, and the inherited structure of an affine algebraic variety on $\mathbb{A}(E)$ is independent of the choice of the basis (because the bijections defined by two different bases differ by an automorphism of $\mathbb{A}^n$).

We now give an intrinsic definition of the affine variety $\mathbb{A}(E)$. Let V be a finite-dimensional vector space over a field k (not necessarily algebraically closed). The ***tensor algebra*** of V is

$$T^*V = \bigoplus_{i \geq 0} V^{\otimes i}$$

with multiplication defined by

$$(v_1 \otimes \cdots \otimes v_i) \cdot (v_1' \otimes \cdots \otimes v_j') = v_1 \otimes \cdots \otimes v_i \otimes v_1' \otimes \cdots \otimes v_j'.$$

It is noncommutative k-algebra, and the choice of a basis $e_1, \ldots, e_n$ for V defines an isomorphism to T^*V from the k-algebra of noncommuting polynomials in the symbols $e_1, \ldots, e_n$. The ***symmetric algebra*** $S^*(V)$ of V is defined to be the quotient of T^*V by the two-sided ideal generated by the relations

$$v \otimes w - w \otimes v, \quad v, w \in V.$$

This algebra is generated as a k-algebra by commuting elements (namely, the elements of $V = V^{\otimes 1}$), and so is commutative. The choice of a basis $e_1, \ldots, e_n$ for V defines an isomorphism of k-algebras

$$e_1 \cdots e_i \to e_1 \otimes \cdots \otimes e_i : k[e_1, \ldots, e_n] \to S^*(V)$$

(here $k[e_1, \ldots, e_n]$ is the commutative polynomial ring in the symbols $e_1, \ldots, e_n$). In particular, $S^*(V)$ is an affine k-algebra. The pair $(S^*(V), i)$ consisting of $S^*(V)$ and the natural k-linear map $i: V \to S^*(V)$ has the following universal property: any k-linear map $V \to A$ from V into a k-algebra A extends uniquely to a k-algebra homomorphism $S^*(V) \to A$:

$$\begin{tikzcd} V \arrow[r] \arrow[dr, "k-\text{linear}"'] & S^*(V) \arrow[d, dotted, "\exists!"', "k-\text{algebra}"] \\ & A \end{tikzcd} \tag{7}$$

As usual, this universal propery determines the pair $(S^*(V), i)$ uniquely up to a unique isomorphism.

We now define $\mathbb{A}(E)$ to be $\mathrm{Spm}(S^*(E^\vee))$. For an affine k-algebra A,

$$\begin{aligned}
\mathrm{Mor}(\mathrm{Spm}(A), \mathbb{A}(E)) &\simeq \mathrm{Hom}_{k\text{-algebra}}(S^*(E^\vee), A) && (3.14)\\
&\simeq \mathrm{Hom}_{k\text{-linear}}(E^\vee, A) && (7)\\
&\simeq E \otimes_k A && \text{(linear algebra)}.
\end{aligned}$$

In particular,

$$\mathbb{A}(E)(k) \simeq E.$$

Moreover, the choice of a basis $e_1, \ldots, e_n$ for E determines a (dual) basis $f_1, \ldots, f_n$ of $E^\vee$, and hence an isomorphism of k-algebras $k[f_1, \ldots, f_n] \to S^*(E^\vee)$. The map of algebraic varieties defined by this homomorphism is the isomorphism

$$\mathbb{A}(E) \to \mathbb{A}^n$$

whose map on the underlying sets is the isomorphism $E \to k^n$ defined by the basis of E.

NOTES. 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 60 years. Gel'fand and Kolmogorov in 1939[4] proved that if S and T are compact 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 proof begins by showing that, for such a space S, the map

$$P \mapsto \mathfrak{m}_P \overset{\text{def}}{=} \{f: S \to \mathbb{R} \mid f(P) = 0\}$$

is one-to-one correspondence between the points in the space and maximal ideals in the ring.

Exercises

3-1. Show that a map between affine varieties can be continuous for the Zariski topology without being regular.

3-2. Let q be a power of a prime p, and let $\mathbb{F}_q$ be the field with q elements. Let S be a subset of $\mathbb{F}_q[X_1, \ldots, X_n]$, and let V be its zero set in k^n, where k is the algebraic closure of $\mathbb{F}_q$. Show that the map $(a_1, \ldots, a_n) \mapsto (a_1^q, \ldots, a_n^q)$ is a regular map $\varphi: V \to V$ (i.e., $\varphi(V) \subset V$). Verify that the set of fixed points of φ is the set of zeros of the elements of S with coordinates in $\mathbb{F}_q$. (This statement enables one to study the cardinality of the last set using a Lefschetz fixed point formula — see my lecture notes on étale cohomology.)

3-3. Find the image of the regular map

$$(x, y) \mapsto (x, xy): \mathbb{A}^2 \to \mathbb{A}^2$$

and verify that it is neither open nor closed.

---

[4]On rings of continuous functions on topological spaces, Doklady 22, 11-15. See also Allen Shields, Banach Algebras, 1939–1989, Math. Intelligencer, Vol 11, no. 3, p15.

3-4. Show that the circle $X^2+Y^2=1$ is isomorphic (as an affine variety) to the hyperbola $XY=1$, but that neither is isomorphic to $\mathbb{A}^1$.

3-5. Let C be the curve $Y^2=X^2+X^3$, and let φ be the regular map

$$t\mapsto (t^2-1, t(t^2-1))\colon \mathbb{A}^1\to C.$$

Is φ an isomorphism?

Chapter 4

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. Throughout this chapter, k is algebraically closed.

Algebraic prevarieties

As motivation, recall the following definitions.

DEFINITION 4.1. (a) A ***topological manifold of dimension*** n 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. 3.2a)).

(b) A ***differentiable manifold of dimension*** n 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 the ringed space of smooth functions on an open subset of $\mathbb{R}^n$ (cf. 3.2b).

(c) A ***complex manifold of dimension*** n 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 the ringed space holomorphic functions on an open subset of $\mathbb{C}^n$ (cf. 3.2c).

These definitions are easily seen to be equivalent to the more classical definitions in terms of charts and atlases.[1] Often one imposes additional conditions on V, for example, that it be connected or that it have a countable base of open subsets.

DEFINITION 4.2. An ***algebraic prevariety over*** k is a ringed space $(V, \mathcal{O}_V)$ such that V is quasicompact and every point of V has an open neighbourhood U for which $(U, \mathcal{O}_V|U)$ is an affine algebraic variety over k.

Thus, a ringed space $(V, \mathcal{O}_V)$ is an algebraic prevariety over k if there exists a finite open covering $V = \bigcup V_i$ such that $(V_i, \mathcal{O}_V|V_i)$ is an affine algebraic variety over k for all i. An algebraic variety will be defined to be an algebraic prevariety satisfying a certain separation condition.

[1] Provided the latter are stated correctly, which is frequently not the case.

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. Because V is a finite union of open affines, and in each open affine the open affines (in fact the basic open subsets) form a base for the topology, it follows that the open affines form a base for the topology on V.

Let $(V, \mathcal{O}_V)$ be an algebraic prevariety, and let U be an open subset of V. The functions $f: U \to k$ 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 $f: U \to k$ is regular if and only if $f|U_i \cap U$ is regular for all i (by 3.1(c)). 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 4.3. (Projective space). Let $\mathbb{P}^n$ denote $k^{n+1} \smallsetminus \{\text{origin}\}$ modulo the equivalence relation

$$(a_0, \ldots, a_n) \sim (b_0, \ldots, b_n) \iff (a_0, \ldots, a_n) = (cb_0, \ldots, cb_n) \text{ some } c \in k^\times.$$

Thus the equivalence classes are the lines through the origin in k^{n+1} (with the origin omitted). Write $(a_0 : \ldots : a_n)$ 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 $\mathbb{P}^n = \bigcup U_i$, and the map

$$(a_0 : \ldots : a_n) \mapsto (a_0/a_i, \ldots, a_n/a_i) : U_i \xrightarrow{u_i} \mathbb{A}^n$$

(the term a_i/a_i is omitted) is a bijection. In chapter 6 we shall show that there is a unique structure of a (separated) algebraic variety on $\mathbb{P}^n$ for which each U_i is an open affine subvariety of $\mathbb{P}^n$ and each map u_i is an isomorphism of algebraic varieties.

Regular maps

In each of the examples (4.1a,b,c), a morphism of manifolds (continuous map, smooth map, holomorphic 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 $\varphi: V \to W$ 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 three categories:

$$\text{(affine varieties)} \subset \text{(algebraic prevarieties)} \subset \text{(ringed spaces)}.$$

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

PROPOSITION 4.4. *Let $(V, \mathcal{O}_V)$ and $(W, \mathcal{O}_W)$ be prevarieties, and let $\varphi: V \to W$ be a continuous map (of topological spaces). Let $W = \bigcup W_j$ be a covering of W by open affines, and let $\varphi^{-1}(W_j) = \bigcup V_{ji}$ be a covering of $\varphi^{-1}(W_j)$ by open affines. Then φ is regular if and only if its restrictions*

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

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 (sheaf condition 3.1(b)), 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 3.1(c)). Thus φ is regular. The converse is even easier. □

ASIDE 4.5. A differentiable manifold of dimension n is locally isomorphic to an open subset of $\mathbb{R}^n$. 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 chapter 5 below).

(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 chapter) that there does exist a neighbourhood U of P and a regular map $\varphi: U \to \mathbb{A}^d$ such that map $(d\varphi)_P: T_P \to T_{\varphi(P)}$ on the tangent spaces is an isomorphism, but also that there does not always exist a U for which φ itself is an isomorphism onto its image (as the inverse function theorem would assert).

Algebraic varieties

In the study of topological manifolds, the Hausdorff condition eliminates such bizarre possibilities as the line with the origin doubled (see 4.10 below) 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 prevents a sequence in the space having more than one limit. Thus a continuous map into the space should be determined by its values on a dense subset, i.e., if φ_1 and φ_2 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 $\varphi_1, \varphi_2: Z \rightrightarrows U$ agree should be closed. Surprisingly, affine varieties have this property, provided φ_1 and φ_2 are required to be regular maps.

LEMMA 4.6. *Let φ_1 and φ_2 be regular maps of affine algebraic varieties $Z \rightrightarrows V$. The subset of Z on which φ_1 and φ_2 agree is closed.*

PROOF. There are regular functions x_i on V such that $P \mapsto (x_1(P), \ldots, x_n(P))$ 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 $x_i \circ \varphi_1$ and $x_i \circ \varphi_2$ are regular functions on Z, and the set where φ_1 and φ_2 agree is $\bigcap_{i=1}^n V(x_i \circ \varphi_1 - x_i \circ \varphi_2)$, which is closed. □

DEFINITION 4.7. 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 $\varphi_1, \varphi_2: Z \rightrightarrows V$ with Z an affine algebraic variety, the set $\{z \in Z \mid \varphi_1(z) = \varphi_2(z)\}$ is closed in Z.

The terminology is not completely standardized: some authors require a variety to be irreducible, and some call a prevariety a variety.[2]

PROPOSITION 4.8. *Let φ_1 and φ_2 be regular maps $Z \rightrightarrows V$ from an algebraic prevariety Z to a separated prevariety V. The subset of Z on which φ_1 and φ_2 agree is closed.*

PROOF. Let W be the set on which φ_1 and φ_2 agree. For any open affine U of Z, $W \cap U$ is the subset of U on which $\varphi_1|U$ and $\varphi_2|U$ agree, and so $W \cap U$ is closed. This implies that W is closed because Z is a finite union of open affines. □

EXAMPLE 4.9. The open subspace $U = \mathbb{A}^2 \smallsetminus \{(0,0)\}$ of $\mathbb{A}^2$ becomes an algebraic variety when endowed with the sheaf $\mathcal{O}_{\mathbb{A}^2}|U$ (cf. 3.21).

EXAMPLE 4.10. (The affine line with the origin doubled.) Let V_1 and V_2 be copies of $\mathbb{A}^1$. Let $V^* = V_1 \sqcup V_2$ (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 $\mathbb{A}^1$.

Let Var_k denote the category of algebraic varieties over k and regular maps. The functor $A \mapsto \operatorname{Spm} A$ is a fully faithful contravariant functor $\mathsf{Aff}_k \to \mathsf{Var}_k$, and defines an equivalence of the first category with the subcategory of the second whose objects are the affine algebraic varieties.

Maps from varieties to affine varieties

Let $(V, \mathcal{O}_V)$ be an algebraic variety, and let $\alpha\colon A \to \Gamma(V, \mathcal{O}_V)$ be a homomorphism from an affine k-algebra A to the k-algebra of regular functions on V. For any $P \in V$, $f \mapsto \alpha(f)(P)$ is a k-algebra homomorphism $A \to k$, and so its kernel $\varphi(P)$ is a maximal ideal in A. In this way, we get a map

$$\varphi\colon V \to \operatorname{spm}(A)$$

which is easily seen to be regular. Conversely, from a regular map $\varphi\colon V \to \operatorname{Spm}(A)$, we get a k-algebra homomorphism $f \mapsto f \circ \varphi\colon A \to \Gamma(V, \mathcal{O}_V)$. Since these maps are inverse, we have proved the following result.

[2]Our terminology is agrees with that of J-P. Serre, Faisceaux algébriques cohérents. Ann. of Math. 61, (1955). 197–278.

PROPOSITION 4.11. *For an algebraic variety V and an affine k-algebra A, there is a canonical one-to-one correspondence*

$$\mathrm{Mor}(V, \mathrm{Spm}(A)) \simeq \mathrm{Hom}_{k\text{-algebra}}(A, \Gamma(V, \mathcal{O}_V)).$$

Let V be an algebraic variety such that $\Gamma(V, \mathcal{O}_V)$ is an affine k-algebra. Then proposition shows that the regular map $\varphi\colon V \to \mathrm{Spm}(\Gamma(V, \mathcal{O}_V))$ defined by $\mathrm{id}_{\Gamma(V,\mathcal{O}_V)}$ has the following universal property: any regular map from V to an affine algebraic variety U factors uniquely through φ:

$$\begin{tikzcd} V \arrow[r, "\varphi"] \arrow[dr] & \mathrm{Spm}(\Gamma(V, \mathcal{O}_V)) \arrow[d, dotted, "\exists!"] \\ & U. \end{tikzcd}$$

Subvarieties

Let $(V, \mathcal{O}_V)$ be a ringed space, and let W be a subspace. For U open in W, define $\mathcal{O}_W(U)$ to be the set of functions $f\colon U \to k$ such that there exist open subsets U_i of V and $f_i \in \mathcal{O}_V(U_i)$ such that $U = W \cap (\bigcup U_i)$ and $f|W \cap U_i = f_i|W \cap U_i$ for all i. Then $(W, \mathcal{O}_W)$ is again a ringed space.

We now let $(V, \mathcal{O}_V)$ be a prevariety, and examine when $(W, \mathcal{O}_W)$ is also a prevariety.

Open subprevarieties. Because the open affines form a base for the topology on V, for any open subset U of V, $(U, \mathcal{O}_V|U)$ is a prevariety. The inclusion $U \hookrightarrow V$ is regular, and U is called an ***open subprevariety*** of V. 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).

Closed subprevarieties. 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 p56). Such a pair $(Z, \mathcal{O}_Z)$ is called a ***closed subprevariety*** of V. 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).

Subprevarieties. 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. Equivalent conditions: W is the intersection of an open and a closed subset of V; W is open in its closure. 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.

Application.

PROPOSITION 4.12. *A prevariety V is separated if and only if two regular maps from a prevariety to V agree on the whole prevariety whenever they agree on a dense subset of it.*

PROOF. If V is separated, then the set on which a pair of regular maps $\varphi_1, \varphi_2 \colon Z \rightrightarrows V$ agree is closed, and so must be the whole of the Z.

Conversely, consider a pair of maps $\varphi_1, \varphi_2 \colon Z \rightrightarrows V$, and let S be the subset of Z on which they agree. We assume V has the property in the statement of the proposition, 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 $\varphi_1|\bar{S}$ and $\varphi_2|\bar{S}$ 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

PROPOSITION 4.13. *Let $V = \bigcup_{i \in I} V_i$ (finite union), and suppose that each V_i has the structure of a ringed space. Assume the following "patching" condition holds:*

for all i, j, $V_i \cap V_j$ is open in both V_i and V_j and $\mathcal{O}_{V_i}|V_i \cap V_j = \mathcal{O}_{V_j}|V_i \cap V_j$.

Then there is a unique structure of a ringed space on V for which

(a) *each inclusion $V_i \hookrightarrow V$ is a homeomorphism of V_i onto an open set, and*
(b) *for each $i \in I$, $\mathcal{O}_V|V_i = \mathcal{O}_{V_i}$.*

If every V_i is an algebraic prevariety, then so also is V, and to give a regular map from V to a prevariety W amounts to giving a family of regular maps $\varphi_i \colon V_i \to W$ such that $\varphi_i|V_i \cap V_j = \varphi_j|V_i \cap V_j$.

PROOF. One checks easily that the subsets $U \subset V$ such that $U \cap V_i$ is open for all i are the open subsets for a topology on V satisfying (a), and that this is the only topology to satisfy (a). Define $\mathcal{O}_V(U)$ to be the set of functions $f \colon U \to k$ such that $f|U \cap V_i \in \mathcal{O}_{V_i}(U \cap V_i)$ for all i. Again, one checks easily that $\mathcal{O}_V$ is a sheaf of k-algebras satisfying (b), and that it is the only such sheaf.

For the final statement, if each $(V_i, \mathcal{O}_{V_i})$ is a finite union of open affines, so also is $(V, \mathcal{O}_V)$. Moreover, to give a map $\varphi \colon V \to W$ amounts to giving a family of maps $\varphi_i \colon V_i \to W$ such that $\varphi_i|V_i \cap V_j = \varphi_j|V_i \cap V_j$ (obviously), and φ is regular if and only $\varphi|V_i$ is regular for each i. □

Clearly, the V_i may be separated without V being separated (see, for example, 4.10). In (4.27) below, we give a condition on an open affine covering of a prevariety sufficient to ensure that the prevariety is separated.

Products of varieties

Let V and W be objects in a category 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 it has the following universal property: for every pair of morphisms $Z \to V$, $Z \to W$ in C, there exists a unique morphism $Z \to V \times W$ making the diagram

$$\begin{tikzcd} & Z \arrow[dl] \arrow[d, dotted, "\exists!"'] \arrow[dr] & \\ V & V \times W \arrow[l, "p"'] \arrow[r, "q"] & W \end{tikzcd}$$

commute. In other words, it is a product if the map

$$\varphi \mapsto (p \circ \varphi, q \circ \varphi)\colon \mathrm{Hom}(Z, V \times W) \to \mathrm{Hom}(Z, V) \times \mathrm{Hom}(Z, W)$$

is a bijection. The product, if it exists, is uniquely determined up to a unique isomorphism by this universal property.

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) endowed with the product topology.

We shall show that products exist in the category of algebraic varieties. Suppose, for the moment, that $V \times W$ exists. For any prevariety Z, $\mathrm{Mor}(\mathbb{A}^0, Z)$ is the underlying set of Z; more precisely, for any $z \in Z$, the map $\mathbb{A}^0 \to Z$ with image z is regular, and these are all the regular maps (cf. 3.18b). Thus, from the definition of products we have

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

Hence, 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

(a) the projection maps $p, q\colon V \times W \rightrightarrows V, W$ are regular, and
(b) a map $\varphi\colon T \to V \times W$ of sets (with T an algebraic prevariety) is regular 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).

Products of affine varieties

EXAMPLE 4.14. Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals in $k[X_1, \ldots, X_m]$ and $k[X_{m+1}, \ldots, X_{m+n}]$ respectively, and let $(\mathfrak{a}, \mathfrak{b})$ be the ideal in $k[X_1, \ldots, X_{m+n}]$ generated by the elements of $\mathfrak{a}$ and $\mathfrak{b}$. Then there is an isomorphism

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

Again this comes down to checking that the natural map from

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

to

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

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.

The tensor product of two k-algebras A and B has the universal property to be a product in the category of k-algebras, but with the arrows reversed. Because of the category anti-equivalence (3.15), this shows that $\mathrm{Spm}(A\otimes_k B)$ will be the product of $\mathrm{Spm}\, A$ and $\mathrm{Spm}\, B$ in the category of affine algebraic varieties once we have shown that $A\otimes_k B$ is an affine k-algebra.

PROPOSITION 4.15. *Let A and B be k-algebras with A finitely generated.*

(a) *If A and B are reduced, then so also is $A\otimes_k B$.*
(b) *If A and B are integral domains, then so also is $A\otimes_k B$.*

PROOF. 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 assume A and B to be reduced, and suppose that α is nilpotent. Let $\mathfrak{m}$ be a maximal ideal of A. From $a\mapsto \bar{a}\colon A\to A/\mathfrak{m} = k$ we obtain homomorphisms

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

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, the a_i's lie in all maximal ideals $\mathfrak{m}$ of A, and so are zero (see 2.13). Hence $\alpha = 0$, and we have shown that $A\otimes_k B$ is reduced.

Now assume that A and B are integral domains, and let $\alpha,\alpha'\in A\otimes_k B$ 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 $\{b_1, b_2,\ldots\}$ and $\{b_1', b_2',\ldots\}$ 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

$$\mathrm{spm}(A) = V(a_1,\ldots,a_m)\cup V(a_1',\ldots,a_n').$$

As $\mathrm{spm}(A)$ is irreducible (see 2.19), it follows that $\mathrm{spm}(A)$ equals either $V(a_1,\ldots,a_m)$ or $V(a_1',\ldots,a_n')$. In the first case $\alpha = 0$, and in the second $\alpha' = 0$. □

EXAMPLE 4.16. 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, so that there exists an element α in an algebraic closure of k such that $\alpha \notin k$ but $\alpha^p \in k$. Let $k' = k[\alpha]$, and let $\alpha^p = a$. 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

$$\begin{aligned}(\alpha \otimes 1 - 1 \otimes \alpha)^p &= (a \otimes 1 - 1 \otimes a) \\ &= (1 \otimes a - 1 \otimes a) \quad \text{(because } a \in k\text{)} \\ &= 0.\end{aligned}$$

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 second field containing k. By the primitive element theorem (FT 5.1),

$$K = k[\alpha] = k[X]/(f(X)),$$

for some $\alpha \in K$ and its minimal polynomial $f(X)$. Assume that Ω is large enough to split f, say, $f(X) = \prod_i X - \alpha_i$ with $\alpha_i \in \Omega$. Because K/k is separable, the α_i are distinct, and so

$$\begin{aligned}\Omega \otimes_k K &\simeq \Omega[X]/(f(X)) && (1.35(b)) \\ &\simeq \prod \Omega[X]/(X - \alpha_i) && (1.1)\end{aligned}$$

and so it is not an integral domain. For example,

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C}[X]/(X-i) \times \mathbb{C}[X]/(X+i) \simeq \mathbb{C} \times \mathbb{C}.$$

The proposition allows us to make the following definition.

DEFINITION 4.17. The ***product*** of the affine varieties V and W is

$$(V \times W, \mathcal{O}_{V \times W}) = \mathrm{Spm}(k[V] \otimes_k k[W])$$

with the projection maps $p, q \colon V \times W \to V, W$ defined by the homomorphisms $f \mapsto f \otimes 1 \colon k[V] \to k[V] \otimes_k k[W]$ and $g \mapsto 1 \otimes g \colon k[W] \to k[V] \otimes_k k[W]$.

PROPOSITION 4.18. *Let V and W be affine varieties.*

(a) *The variety $(V \times W, \mathcal{O}_{V \times W})$ is the product of $(V, \mathcal{O}_V)$ and $(W, \mathcal{O}_W)$ in the category of affine algebraic varieties; in particular, the set $V \times W$ is the product of the sets V and W and p and q are the projection maps.*
(b) *If V and W are irreducible, then so also is $V \times W$.*

PROOF. (a) As noted at the start of the subsection, the first statement follows from (4.15a), and the second statement then follows by the argument on p66.

(b) This follows from (4.15b) and (2.19). □

COROLLARY 4.19. *Let V and W be affine varieties. For any prevariety T, a map $\varphi \colon T \to V \times W$ is regular if $p \circ \varphi$ and $q \circ \varphi$ are regular.*

PROOF. If $p \circ \varphi$ and $q \circ \varphi$ are regular, then (4.18) implies that φ is regular when restricted to any open affine of T, which implies that it is regular on T. $\square$

The corollary shows that $V \times W$ is the product of V and W in the category of prevarieties (hence also in the categories of varieties).

EXAMPLE 4.20. (a) It follows from (1.34) that $\mathbb{A}^{m+n}$ endowed with the projection maps

$$\mathbb{A}^m \xleftarrow{p} \mathbb{A}^{m+n} \xrightarrow{q} \mathbb{A}^n, \qquad \begin{cases} p(a_1,\ldots,a_{m+n}) = (a_1,\ldots,a_m) \\ q(a_1,\ldots,a_{m+n}) = (a_{m+1},\ldots,a_{m+n}), \end{cases}$$

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

(b) It follows from (1.35c) that

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

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

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 (see 2.29).

Products in general

We now define the product of two algebraic prevarieties V and W.

Write V as a union of open affines $V = \bigcup V_i$, and note that V can be regarded as the variety obtained by patching the $(V_i, \mathcal{O}_{V_i})$; in particular, this covering satisfies the patching condition (4.13). Similarly, write W as a union of open affines $W = \bigcup W_j$. Then

$$V \times W = \bigcup V_i \times W_j$$

and the $(V_i \times W_j, \mathcal{O}_{V_i \times W_j})$ satisfy the patching condition. Therefore, we can define $(V \times W, \mathcal{O}_{V\times W})$ to be the variety obtained by patching the $(V_i \times W_j, \mathcal{O}_{V_i \times W_j})$.

PROPOSITION 4.21. *With the sheaf of k-algebras $\mathcal{O}_{V\times W}$ just defined, $V \times W$ becomes the product of V and W in the category of prevarieties. In particular, the structure of prevariety on $V \times W$ defined by the coverings $V = \bigcup V_i$ and $W = \bigcup W_j$ are independent of the coverings.*

PROOF. Let T be a prevariety, and let $\varphi: T \to V \times W$ be a map of sets such that $p \circ \varphi$ and $q \circ \varphi$ are regular. Then (4.19) implies that the restriction of φ to $\varphi^{-1}(V_i \times W_j)$ is regular. As these open sets cover T, this shows that φ is regular. $\square$

PROPOSITION 4.22. *If V and W are separated, then so also is $V \times W$.*

PROOF. Let φ_1, φ_2 be two regular maps $U \to V \times W$. The set where φ_1, φ_2 agree is the intersection of the sets where $p \circ \varphi_1$, $p \circ \varphi_2$ and $q \circ \varphi_1, q \circ \varphi_2$ agree, which is closed. $\square$

EXAMPLE 4.23. An ***algebraic group*** is a variety G together with regular maps

$$\text{mult}: G \times G \to G, \quad \text{inverse}: G \to G, \quad \mathbb{A}^0 \xrightarrow{e} G$$

that make G into a group in the usual sense. For example,

$$\mathrm{SL}_n = \mathrm{Spm}(k[X_{11}, X_{12}, \ldots, X_{nn}]/(\det(X_{ij}) - 1))$$

and

$$\mathrm{GL}_n = \mathrm{Spm}(k[X_{11}, X_{12}, \ldots, X_{nn}, Y]/(Y \det(X_{ij}) - 1))$$

become algebraic groups when endowed with their usual group structure. The only affine algebraic groups of dimension 1 are

$$\mathbb{G}_m = \mathrm{GL}_1 = \mathrm{Spm}\, k[X, X^{-1}]$$

and

$$\mathbb{G}_a = \mathrm{Spm}\, k[X].$$

Any finite group N can be made into an algebraic group by setting

$$N = \mathrm{Spm}(A)$$

with A the set of all maps $f: N \to k$.

Affine algebraic groups are called ***linear algebraic groups*** because they can all be realized as closed subgroups of GL_n for some n. Connected algebraic groups that can be realized as *closed* algebraic subvarieties of a projective space are called ***abelian varieties*** because they are related to the integrals studied by Abel (happily, they all turn out to be commutative; see 7.15 below).

The connected component G° of an algebraic group G containing the identity component (the ***identity component***) is a closed normal subgroup of G and the quotient G/G° is a finite group. An important theorem of Chevalley says that every connected algebraic group G contains a unique connected linear algebraic group G_1 such that G/G_1 is an abelian variety. Thus, we have the following coarse classification: every algebraic group G contains a sequence of normal subgroups

$$G \supset G^\circ \supset G_1 \supset \{e\}$$

with G/G° a finite group, G°/G_1 an abelian variety, and G_1 a linear algebraic group.

The separation axiom revisited

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 $\Delta \subset V \times V$,

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

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 4.24. *An algebraic prevariety V is separated if and only if Δ_V is closed.*[3]

PROOF. Assume Δ_V is closed. Let φ_1 and φ_2 be regular maps $Z \to V$. The map

$$(\varphi_1, \varphi_2)\colon Z \to V \times V, \quad z \mapsto (\varphi_1(z), \varphi_2(z))$$

is regular because its composites with the projections to V are φ_1 and φ_2. In particular, it is continuous, and so $(\varphi_1, \varphi_2)^{-1}(\Delta)$ is closed. But this is precisely the subset on which φ_1 and φ_2 agree.

Conversely, suppose V is separated. This means that for any affine variety Z and regular maps $\varphi_1, \varphi_2\colon Z \to V$, the set on which φ_1 and φ_2 agree is closed in Z. Apply this with φ_1 and φ_2 the two projection maps $V \times V \to V$, and note that the set on which they agree is Δ_V. □

COROLLARY 4.25. *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 an open 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 (4.6). □

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 the picture suggested by calculus.

COROLLARY 4.26. *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 (as algebraic prevarieties).*

PROOF. The map

$$(v, w) \mapsto (\varphi(v), w)\colon V \times W \to W \times W$$

is regular because its composites with the projections are φ and id_W which are regular. In particular, it is continuous, and as Γ_φ is the inverse image of Δ_W under this map, this proves the first statement. The second statement 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 4.27. *The following three conditions on a prevariety V 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 the map*

$$f \otimes g \mapsto f|_{U \cap U'} \cdot g|_{U \cap U'}\colon k[U] \otimes_k k[U'] \to k[U \cap U']$$

is surjective;

[3] Recall that the topology on $V \times V$ is *not* the product topology. Thus the statement does not contradict the fact that V is not Hausdorff.

(c) *the condition in (b) holds for the sets in some open affine covering of V.*

PROOF. Let U and U' be open affines in V. We shall prove that

(i) if Δ is closed then $U \cap U'$ affine,

(ii) when $U \cap U'$ is affine,

$$(U \times U') \cap \Delta \text{ is closed} \iff k[U] \otimes_k k[U'] \to k[U \cap U'] \text{ is surjective.}$$

Assume (a); then these statements imply (b). Assume that (b) holds for the sets in an open affine covering $(U_i)_{i \in I}$ of V. Then $(U_i \times U_j)_{(i,j) \in I \times I}$ is an open affine covering of $V \times V$, and $\Delta_V \cap (U_i \times U_j)$ is closed in $U_i \times U_j$ for each pair (i, j), which implies (a). Thus, the statements (i) and (ii) imply the theorem.

Proof of (i): The graph of the inclusion $U \cap U' \hookrightarrow V$ is the subset $(U \times U') \cap \Delta$ of $(U \cap U') \times V$. If Δ_V is closed, then $(U \times U') \cap \Delta_V$ is a closed subvariety of an affine variety, and hence is affine (see p56). Now (4.26) implies that $U \cap U'$ is affine.

Proof of (ii): Assume that $U \cap U'$ is affine. Then

$$\begin{aligned} &(U \times U') \cap \Delta_V \text{ is closed in } U \times U' \\ \iff &v \mapsto (v, v) \colon U \cap U' \to U \times U' \text{ is a closed immersion} \\ \iff &k[U \times U'] \to k[U \cap U'] \text{ is surjective (3.22).} \end{aligned}$$

Since $k[U \times U'] = k[U] \otimes_k k[U']$, this completes the proof of (ii). □

In more down-to-earth terms, condition (b) says that $U \cap U'$ is affine and every regular function on $U \cap U'$ is a sum of functions of the form $P \mapsto f(P)g(P)$ with f and g regular functions on U and U'.

EXAMPLE 4.28. (a) Let $V = \mathbb{P}^1$, and let U_0 and U_1 be the standard open subsets (see 4.3). Then $U_0 \cap U_1 = \mathbb{A}^1 \smallsetminus \{0\}$, and the maps on rings corresponding to the inclusions $U_i \hookrightarrow U_0 \cap U_1$ are

$$\begin{aligned} f(X) &\mapsto f(X) \colon k[X] \to k[X, X^{-1}] \\ f(X) &\mapsto f(X^{-1}) \colon k[X] \to k[X, X^{-1}], \end{aligned}$$

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 4.10), and let U and U' be the upper and lower copies of $\mathbb{A}^1$ in V. Then $U \cap U'$ is affine, but the maps on rings corresponding to the inclusions $U_i \hookrightarrow U_0 \cap U_1$ are

$$\begin{aligned} X &\mapsto X \colon k[X] \to k[X, X^{-1}] \\ X &\mapsto X \colon k[X] \to k[X, X^{-1}], \end{aligned}$$

Thus the sets U_0 and U_1 fail the condition in (b).

(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 3.21).

Fibred products

Consider a variety S and two regular maps $\varphi \colon V \to S$ and $\psi \colon W \to S$. Then the set

$$V \times_S W \stackrel{\text{def}}{=} \{(v, w) \in V \times W \mid \varphi(v) = \psi(w)\}$$

is a closed subvariety of $V \times W$ (because it is the set where $\varphi \circ p$ and $\psi \circ q$ agree). It is 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 $(v, w) \mapsto w \colon V \times_S W \to W$ and ψ' for the map $(v, w) \mapsto v \colon V \times_S W \to V$. We then have a commutative diagram:

$$\begin{tikzcd} V \times_S W \arrow[r, "\varphi'"] \arrow[d, "\psi'"] & W \arrow[d, "\psi"] \\ V \arrow[r, "\varphi"] & S. \end{tikzcd}$$

The fibred product has the following universal property: consider a pair of regular maps $\alpha \colon T \to V$, $\beta \colon T \to W$; then

$$t \mapsto (\alpha(t), \beta(t)) \colon T \to V \times W$$

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 $V \times W$);

$$\begin{tikzcd} T \arrow[dr, dotted] \arrow[drr, bend left, "\alpha"] \arrow[ddr, bend right, "\beta"'] & & \\ & V \times_S W \arrow[r] \arrow[d] & W \arrow[d, "\psi"] \\ & V \arrow[r, "\varphi"] & S \end{tikzcd}$$

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 $\varphi \colon V \to S$ with respect to $P \hookrightarrow S$ is the map $\varphi^{-1}(P) \to P$ induced by φ, which is called the ***fibre*** of V over P.

EXAMPLE 4.29. If $f \colon V \to S$ is a regular map and U is an open subvariety of S, then $V \times_S U$ is the inverse image of U in S.

EXAMPLE 4.30. Since a tensor product of rings $A \otimes_R B$ has the opposite universal property to that of a fibred product, one might hope that

$$\mathrm{Spm}(A) \times_{\mathrm{Spm}(R)} \mathrm{Spm}(B) \stackrel{??}{=} \mathrm{Spm}(A \otimes_R B).$$

This is true if $A \otimes_R B$ is an affine k-algebra, but in general it may have nilpotent[4] elements. For example, let $R = k[X]$, let $A = k$ with the R-algebra structure sending X to a, and let $B = k[X]$ with the R-algebra structure sending X to X^p. When k has characteristic $p \neq 0$, then

$$A \otimes_R B \simeq k \otimes_{k[X^p]} k[X] \simeq k[X]/(X^p - a).$$

[4]By this, of course, we mean nonzero nilpotent elements.

The correct statement is

$$\operatorname{Spm}(A) \times_{\operatorname{Spm}(R)} \operatorname{Spm}(B) \simeq \operatorname{Spm}(A \otimes_R B/\mathfrak{N}) \tag{8}$$

where $\mathfrak{N}$ is the ideal of nilpotent elements in $A \otimes_R B$. To prove this, note that for any variety T,

$$\begin{aligned}
\operatorname{Mor}(T, \operatorname{Spm}(A \otimes_R B/\mathfrak{N})) &\simeq \operatorname{Hom}(A \otimes_R B/\mathfrak{N}, \Gamma(T, \mathcal{O}_T)) \\
&\simeq \operatorname{Hom}(A \otimes_R B, \Gamma(T, \mathcal{O}_T)) \\
&\simeq \operatorname{Hom}(A, \Gamma(T, \mathcal{O}_T)) \times_{\operatorname{Hom}(R, \Gamma(T, \mathcal{O}_T))} \operatorname{Hom}(B, \Gamma(T, \mathcal{O}_T)) \\
&\simeq \operatorname{Mor}(V, \operatorname{Spm}(A)) \times_{\operatorname{Mor}(V, \operatorname{Spm}(R))} \operatorname{Mor}(V, \operatorname{Spm}(B)).
\end{aligned}$$

For the first and fourth isomorphisms, we used (4.11); for the second isomorphism, we used that $\Gamma(T, \mathcal{O}_T)$ has no nilpotents; for the third isomorphism, we used the universal property of $A \otimes_R B$.

Dimension

In an irreducible algebraic variety V, every nonempty open subset is dense and irreducible. If U and U' are open affines in V, then so also is $U \cap U'$ and

$$k[U] \subset k[U \cap U'] \subset k(U)$$

where $k(U)$ is the field of fractions of $k[U]$, and so $k(U)$ is also the field of fractions of $k[U \cap U']$ and of $k[U']$. Thus, 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 §2 carry over — for example, if Z is a proper closed subvariety of V, then $\dim(Z) < \dim(V)$.

PROPOSITION 4.31. *Let V and W be irreducible varieties. Then*

$$\dim(V \times W) = \dim(V) + \dim(W).$$

PROOF. We may suppose V and W to be affine. Write

$$\begin{aligned}
k[V] &= k[x_1, \ldots, x_m] \\
k[W] &= k[y_1, \ldots, y_n]
\end{aligned}$$

where the x's and y's have been chosen so that $\{x_1, \ldots, x_d\}$ and $\{y_1, \ldots, y_e\}$ are maximal algebraically independent sets of elements of $k[V]$ and $k[W]$. Then $\{x_1, \ldots, x_d\}$ and $\{y_1, \ldots, y_e\}$ are transcendence bases of $k(V)$ and $k(W)$ (see FT 8.12), and so $\dim(V) = d$ and $\dim(W) = e$. Then[5]

$$k[V \times W] \stackrel{\text{def}}{=} k[V] \otimes_k k[W] \supset k[x_1, \ldots, x_d] \otimes_k k[y_1, \ldots, y_e] \simeq k[x_1, \ldots, x_d, y_1, \ldots, y_e].$$

[5] 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.

Therefore $\{x_1 \otimes 1, \ldots, x_d \otimes 1, 1 \otimes y_1, \ldots, 1 \otimes y_e\}$ 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 $x_i \otimes 1$, $1 \otimes y_j$, $1 \le i \le m$, $1 \le j \le n$, and all of them are algebraic over

$$k[x_1, \ldots, x_d] \otimes_k k[y_1, \ldots, y_e].$$

Thus the transcendence degree of $k(V \times W)$ is $d + e$. □

We extend the definition of dimension to an arbitrary variety V as follows. An algebraic variety is a finite union of noetherian topological spaces, and so is noetherian. Consequently (see 2.21), V is a finite union $V = \bigcup V_i$ of its irreducible components, and we define $\dim(V) = \max \dim(V_i)$. When all the irreducible components of V have dimension n, V is said to be ***pure of dimension*** n (or to be of ***pure dimension*** n).

Birational equivalence

Two irreducible varieties V and W are said to be ***birationally equivalent*** if $k(V) \approx k(W)$.

PROPOSITION 4.32. *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 $B = k[x_1, \ldots, x_n]$. Then $x_i = a_i/b_i$, $a_i, b_i \in A$, and $B \subset A_{b_1 \ldots b_r}$. Since $\operatorname{Spm}(A_{b_1 \ldots b_r})$ is a basic open subvariety of V, we may replace A with $A_{b_1 \ldots b_r}$, 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. □

REMARK 4.33. Proposition 4.32 can be improved as follows: if V and W are irreducible varieties, then every inclusion $k(V) \subset k(W)$ is defined by a regular surjective map $\varphi\colon U \to U'$ from an open subset U of W onto an open subset U' of V.

PROPOSITION 4.34. *Every irreducible algebraic variety of dimension d is birationally equivalent to a hypersurface in $\mathbb{A}^{d+1}$.*

PROOF. Let V be an irreducible variety of dimension d. According to FT 8.21, there exist algebraically independent elements $x_1, \ldots, x_d \in k(V)$ such that $k(V)$ is finite and separable over $k(x_1, \ldots, x_d)$. By the primitive element theorem (FT 5.1), $k(V) = k(x_1, \ldots, x_d, x_{d+1})$ for some x_{d+1}. Let $f \in k[X_1, \ldots, X_{d+1}]$ be an irreducible polynomial satisfied by the x_i, and let H be the hypersurface $f = 0$. Then $k(V) \approx k(H)$. □

REMARK 4.35. 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 (4.33), 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 (cf. FT 8.19) says that every unirational curve is rational. 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 showed that there exist infinitely many surfaces V, no two birationally equivalent, such that $k(X^p, Y^p) \subset k(V) \subset k(X, Y)$.

Dominant maps

As in the affine case, a regular map $\varphi: V \to W$ is said to be ***dominant*** (or ***dominating***) if the image of φ 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 (3.22) 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'.

Algebraic varieties as a functors

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 $\mathrm{Spm}(A) \to V$. For example, if $V = V(\mathfrak{a}) \subset k^n$, then

$$V(A) = \{(a_1, \ldots, a_n) \in A^n \mid f(a_1, \ldots, a_n) = 0 \text{ all } f \in \mathfrak{a}\},$$

which is what you should 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

$$(V \times W)(A) = V(A) \times W(A)$$

(property of a product).

REMARK 4.36. Let V be the union of two subvarieties, $V = V_1 \cup V_2$. If V_1 and V_2 are both open, then $V(A) = V_1(A) \cup V_2(A)$, but not necessarily otherwise. For example, for any polynomial $f(X_1, \ldots, X_n)$,

$$\mathbb{A}^n = D_f \cup V(f)$$

where $D_f \simeq \mathrm{Spm}(k[X_1, \ldots, X_n, T]/(1 - Tf))$ and $V(f)$ is the zero set of f, but

$$A^n \neq \{\mathbf{a} \in A^n \mid f(\mathbf{a}) \in A^\times\} \cup \{\mathbf{a} \in A^n \mid f(\mathbf{a}) = 0\}$$

in general.

THEOREM 4.37. *A regular map $\varphi: V \to W$ of algebraic varieties defines a family of maps of sets, $\varphi(A): V(A) \to W(A)$, one for each affine k-algebra A, such that for every homomorphism $\alpha: A \to B$ of affine k-algebras,*

$$\begin{array}{ccccc} A & & V(A) & \xrightarrow{\varphi(A)} & W(A) \\ \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle V(A)} & & \downarrow{\scriptstyle V(B)} \\ B & & V(B) & \xrightarrow{\varphi(B)} & V(B) \end{array} \qquad (*)$$

commutes. Every family of maps with this property arises from a unique morphism of algebraic varieties.

For a variety V, let h_V^{aff} be the functor sending an affine k-algebra A to $V(A)$. We can restate as Theorem 4.37 follows.

THEOREM 4.38. *The functor*

$$V \mapsto h_V^{\mathrm{aff}} \colon \mathsf{Var}_k \to \mathsf{Fun}(\mathsf{Aff}_k, \mathsf{Sets})$$

if fully faithful.

PROOF. The Yoneda lemma (1.39) shows that the functor

$$V \mapsto h_V \colon \mathsf{Var}_k \to \mathsf{Fun}(\mathsf{Var}_k, \mathsf{Sets})$$

is fully faithful. Let φ be a morphism $h_V^{\mathrm{aff}} \to h_{V'}^{\mathrm{aff}}$, and let T be a variety. Let $(U_i)_{i \in I}$ be a finite affine covering of T. Each intersection $U_i \cap U_j$ is affine (4.27), and so φ gives rise to a commutative diagram

$$\begin{array}{ccccccc}
0 & \to & h_V(T) & \to & \prod_i h_V(U_i) & \rightrightarrows & \prod_{i,j} h_V(U_i \cap U_j) \\
 & & & & \downarrow & & \downarrow \\
0 & \to & h_{V'}(T) & \to & \prod_i h_{V'}(U_i) & \rightrightarrows & \prod_{i,j} h_{V'}(U_i \cap U_j)
\end{array}$$

in which the pairs of maps are defined by the inclusions $U_i \cap U_j \hookrightarrow U_i, U_j$. As the rows are exact (4.13), this shows that φ_V extends uniquely to a functor $h_V \to h_{V'}$, which (by the Yoneda lemma) arises from a unique regular map $V \to V'$. □

COROLLARY 4.39. *To give an affine algebraic group is the same as to give a functor $G \colon \mathsf{Aff}_k \to \mathsf{Gp}$ such that for some n and some finite set S of polynomials in $k[X_1, X_2, \ldots, X_n]$, $G(A)$ is the set of zeros of S in A^n.*

PROOF. Certainly an affine algebraic group defines such a functor. Conversely, the conditions imply that $G = h_V$ for an affine algebraic variety V (unique up to a unique isomorphism). The multiplication maps $G(A) \times G(A) \to G(A)$ give a morphism of functors $h_V \times h_V \to h_V$. As $h_V \times h_V \simeq h_{V \times V}$ (by definition of $V \times V$), we see that they arise from a regular map $V \times V \to V$. Similarly, the inverse map and the identity-element map are regular. □

It is not unusual for a variety to be most naturally defined in terms of its points functor.

REMARK 4.40. The essential image of $h \mapsto h_V \colon \mathsf{Var}_k^{\mathrm{aff}} \to \mathsf{Fun}(\mathsf{Aff}_k, \mathsf{Sets})$ consists of the functors F defined by some (finite) set of polynomials.

We now describe the essential image of $h \mapsto h_V \colon \mathsf{Var}_k \to \mathsf{Fun}(\mathsf{Aff}_k, \mathsf{Sets})$. The ***fibre product*** of two maps $\alpha_1 \colon F_1 \to F_3$, $\alpha_2 \colon F_2 \to F_3$ of sets is the set

$$F_1 \times_{F_3} F_2 = \{(x_1, x_2) \mid \alpha_1(x_1) = \alpha_2(x_2)\}.$$

When F_1, F_2, F_3 are functors and $\alpha_1, \alpha_2, \alpha_3$ are morphisms of functors, there is a functor $F = F_1 \times_{F_3} F_2$ such that

$$(F_1 \times_{F_3} F_2)(A) = F_1(A) \times_{F_3(A)} F_2(A)$$

for all affine k-algebras A.

To simplify the statement of the next proposition, we write U for h_U when U is an affine variety.

PROPOSITION 4.41. *A functor $F\colon \mathsf{Aff}_k \to \mathsf{Sets}$ is in the essential image of Var_k if and only if there exists an affine scheme U and a morphism $U \to F$ such that*

(a) *the functor $R \stackrel{\text{def}}{=} U \times_F U$ is a closed affine subvariety of $U \times U$ and the maps $R \rightrightarrows U$ defined by the projections are open immersions;*
(b) *the set $R(k)$ is an equivalence relation on $U(k)$, and the map $U(k) \to F(k)$ realizes $F(k)$ as the quotient of $U(k)$ by $R(k)$.*

PROOF. Let $F = h_V$ for V an algebraic variety. Choose a finite open affine covering $V = \bigcup U_i$ of V, and let $U = \bigsqcup U_i$. It is again an affine variety (Exercise 4-2). The functor R is $h_{U'}$ where U' is the disjoint union of the varieties $U_i \cap U_j$. These are affine (4.27), and so U' is affine. As U' is the inverse image of Δ_V in $U \times U$, it is closed (4.24). This proves (a), and (b) is obvious.

The converse is omitted for the present. □

REMARK 4.42. A variety V defines a functor $R \mapsto V(R)$ from the category of all k-algebras to Sets. For example, if V is affine,

$$V(R) = \mathrm{Hom}_{k\text{-algebra}}(k[V], R).$$

More explicitly, if $V \subset k^n$ and $I(V) = (f_1, \ldots, f_m)$, then $V(R)$ is the set of solutions in R^n of the system equations

$$f_i(X_1, \ldots, X_n) = 0, \quad i = 1, \ldots, m.$$

Again, we call the elements of $V(R)$ the ***points of V with coordinates in R***.

Note that, when we allow R to have nilpotent elements, it is important to choose the f_i to generate $I(V)$ (i.e., a radical ideal) and not just an ideal $\mathfrak{a}$ such that $V(\mathfrak{a}) = V$.[6]

Exercises

4-1. Show that the only regular functions on $\mathbb{P}^1$ are the constant functions. [Thus $\mathbb{P}^1$ is not affine. When $k = \mathbb{C}$, $\mathbb{P}^1$ is the Riemann sphere (as a set), and one knows from complex analysis that the only holomorphic functions on the Riemann sphere are constant. Since regular functions are holomorphic, this proves the statement in this case. The general case is easier.]

[6] Let $\mathfrak{a}$ be an ideal in $k[X_1, \ldots]$. If A has no nonzero nilpotent elements, then every k-algebra homomorphism $k[X_1, \ldots] \to A$ that is zero on $\mathfrak{a}$ is also zero on $\mathrm{rad}(\mathfrak{a})$, and so

$$\mathrm{Hom}_k(k[X_1, \ldots]/\mathfrak{a}, A) \simeq \mathrm{Hom}_k(k[X_1, \ldots]/\mathrm{rad}(\mathfrak{a}), A).$$

This is not true if A has nonzero nilpotents.

4-2. Let V be the disjoint union of algebraic varieties $V_1, \ldots, V_n$. This set has an obvious topology and ringed space structure for which it is an algebraic variety. Show that V is affine if and only if each V_i is affine.

4-3. Show that every algebraic subgroup of an algebraic group is closed.

Chapter 5

Local Study

In this chapter, we examine the structure of a variety near a point. We 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 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 $V = \bigcup V(F_i)$ expresses V as a union of its irreducible components. Each component $V(F_i)$ has dimension 1 (see 2.25) 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

$$\frac{\partial F}{\partial X}(a,b)(X-a) + \frac{\partial F}{\partial Y}(a,b)(Y-b) = 0. \tag{9}$$

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 5.1. The ***tangent space*** $T_P V$ to V at $P = (a,b)$ is the space defined by equation (9).

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 5.2. For each of the following examples, the reader (or his computer) is invited to sketch the curve.[1] 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,

$$\begin{aligned} V \text{ is singular} &\iff Y^2 - X^3 - aX - b,\ 2Y, \text{ and } 3X^2 + a \text{ have a common zero} \\ &\iff X^3 + aX + b \text{ and } 3X^2 + a \text{ have a common zero.} \end{aligned}$$

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 5.3. *Let V be the curve defined by a nonconstant polynomial F without multiple factors. The set of nonsingular points*[2] *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

$$F = 0, \quad \frac{\partial F}{\partial X} = 0, \quad \frac{\partial F}{\partial Y} = 0,$$

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 called the ***singular locus*** of the variety.

[1] For (b,e,f), see p57 of: Walker, Robert J., Algebraic Curves. Princeton Mathematical Series, vol. 13. Princeton University Press, Princeton, N. J., 1950 (reprinted by Dover 1962).

[2] In common usage, "singular" means uncommon or extraordinary as in "he spoke with singular shrewdness". Thus the proposition says that singular points (mathematical sense) are singular (usual sense).

Tangent cones to plane curves

A polynomial $F(X, Y)$ can be written (uniquely) as a finite sum

$$F = F_0 + F_1 + F_2 + \cdots + F_m + \cdots \tag{10}$$

where F_m is a homogeneous polynomial of degree m. The term F_1 will be denoted F_ℓ and called the ***linear form*** of F, and the first nonzero term on the right of (10) (the homogeneous summand of F of least degree) will be denoted F_* and called the ***leading form*** of F.

If $P = (0,0)$ is on the curve V defined by F, then $F_0 = 0$ and (10) becomes

$$F = aX + bY + \text{higher degree terms;}$$

moreover, the equation of the tangent space is

$$aX + bY = 0.$$

DEFINITION 5.4. 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 5.5. (a) $Y^2 = X^3$: the tangent cone at $(0,0)$ is defined by Y^2 — it is the X-axis (doubled).

(b) $Y^2 = X^2(X+1)$: the tangent cone at (0,0) is defined by $Y^2 - X^2$ — it is the pair of lines $Y = \pm X$.

(c) $(X^2+Y^2)^2 + 3X^2Y - Y^3 = 0$: the tangent cone at $(0,0)$ is defined by $3X^2Y - Y^3$ — it is the union of the lines $Y = 0$, $Y = \pm\sqrt{3}X$.

(d) $(X^2+Y^2)^3 - 4X^2Y^2 = 0$: the tangent cone at $(0,0)$ is defined by $4X^2Y^2 = 0$ — it is the union of the X and Y axes (each doubled).

In general we can factor F_* as

$$F_*(X, Y) = \prod X^{r_0}(Y - a_i X)^{r_i}.$$

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 5.6. *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 $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$ if $F_\ell \neq 0$, and $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 2$ 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 $\mathcal{O}_P = k[V]_\mathfrak{m}$. 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 $\mathfrak{m}/\mathfrak{m}^2 \to \mathfrak{n}/\mathfrak{n}^2$ (see 1.31), 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 (1.3) 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 (1.6), and hence a discrete valuation ring, i.e., a principal ideal domain with exactly one prime element (up to associates) (CA 16.4). 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 $X_1, \ldots, X_m$ 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 $(k^m)^\vee = \mathrm{Hom}(k^m, k)$.

Let $A = (a_{ij})$ be an $n \times m$ matrix. It defines a linear map $\alpha\colon k^m \to k^n$, by

$$\begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} \mapsto A \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^m a_{1j} a_j \\ \vdots \\ \sum_{j=1}^m a_{nj} a_j \end{pmatrix}.$$

Write $X_1, \ldots, X_m$ for the coordinate functions on k^m and $Y_1, \ldots, Y_n$ for the coordinate functions on k^n. Then

$$Y_i \circ \alpha = \sum_{j=1}^m a_{ij} X_j.$$

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 $\mathbf{a} = (a_1, \ldots, a_m)$ is the subspace of the vector space with origin $\mathbf{a}$ cut out by the linear equations

$$\sum_{i=1}^{m} \left.\frac{\partial F}{\partial X_i}\right|_{\mathbf{a}} (X_i - a_i) = 0, \qquad F \in \mathfrak{a}. \tag{11}$$

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 (11).

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 $T_{\mathbf{a}}(\mathbb{A}^m)^\vee$. As in advanced calculus, we define the ***differential*** of a polynomial $F \in k[X_1, \ldots, X_m]$ at $\mathbf{a}$ by the equation:

$$(dF)_{\mathbf{a}} = \sum_{i=1}^{n} \left.\frac{\partial F}{\partial X_i}\right|_{\mathbf{a}} (dX_i)_{\mathbf{a}}.$$

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:

$$(dF)_{\mathbf{a}} = 0, \quad F \in \mathfrak{a}, \tag{12}$$

I claim that, in (11) and (12), 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

$$(dG)_{\mathbf{a}} = \sum_j H_j(\mathbf{a}) \cdot (dF_j)_{\mathbf{a}} + F_j(\mathbf{a}) \cdot (dH_j)_{\mathbf{a}}.$$

If $F_1, \ldots, F_r$ 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 $(dF_1)_{\mathbf{a}}, \ldots, (dF_r)_{\mathbf{a}}$ generate the k-space $\{(dF)_{\mathbf{a}} \mid F \in \mathfrak{a}\}$.

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 component but is a singular point of that component.

Let $\mathfrak{a} = (F_1, \ldots, F_r)$, and let

$$J = \mathrm{Jac}(F_1, \ldots, F_r) = \left(\frac{\partial F_i}{\partial X_j}\right) = \begin{pmatrix} \frac{\partial F_1}{\partial X_1}, & \ldots, & \frac{\partial F_1}{\partial X_m} \\ \vdots & & \vdots \\ \frac{\partial F_r}{\partial X_1}, & \ldots, & \frac{\partial F_r}{\partial X_m} \end{pmatrix}.$$

Then the equations defining $T_{\mathbf{a}}(V)$ as a subspace of $T_{\mathbf{a}}(\mathbb{A}^m)$ have matrix $J(\mathbf{a})$. Therefore, linear algebra shows that

$$\dim_k T_{\mathbf{a}}(V) = m - \mathrm{rank}\, J(\mathbf{a}),$$

and so $\mathbf{a}$ is nonsingular if and only if the rank of $\mathrm{Jac}(F_1, \ldots, F_r)(\mathbf{a})$ is equal to $m-\dim(V)$. For example, if V is a hypersurface, say $I(V) = (F(X_1, \ldots, X_m))$, then

$$\mathrm{Jac}(F)(\mathbf{a}) = \left(\frac{\partial F}{\partial X_1}(\mathbf{a}), \ldots, \frac{\partial F}{\partial X_m}(\mathbf{a})\right),$$

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,

$$\{\mathbf{a} \in V \mid \mathrm{rank}\, J(\mathbf{a}) \leq r\}$$

is closed in V, because it the set where certain determinants vanish. Therefore, there is an open subset U of V on which $\mathrm{rank}\, J(\mathbf{a})$ attains its maximum value, and the rank jumps on closed subsets. Later (5.18) we shall show that the maximum value of $\mathrm{rank}\, J(\mathbf{a})$ is $m - \dim V$, and so the nonsingular points of V form a nonempty open subset of V.

The differential of a regular map

Consider a regular map

$$\varphi\colon \mathbb{A}^m \to \mathbb{A}^n, \quad \mathbf{a} \mapsto (P_1(a_1, \ldots, a_m), \ldots, P_n(a_1, \ldots, a_m)).$$

We think of φ as being given by the equations

$$Y_i = P_i(X_1, \ldots, X_m), i = 1, \ldots n.$$

It corresponds to the map of rings $\varphi^*\colon k[Y_1, \ldots, Y_n] \to k[X_1, \ldots, X_m]$ sending Y_i to $P_i(X_1, \ldots, X_m)$, $i = 1, \ldots n$.

Let $\mathbf{a} \in \mathbb{A}^m$, and let $\mathbf{b} = \varphi(\mathbf{a})$. Define $(d\varphi)_{\mathbf{a}}\colon T_{\mathbf{a}}(\mathbb{A}^m) \to T_{\mathbf{b}}(\mathbb{A}^n)$ to be the map such that

$$(dY_i)_{\mathbf{b}} \circ (d\varphi)_{\mathbf{a}} = \sum \left.\frac{\partial P_i}{\partial X_j}\right|_{\mathbf{a}} (dX_j)_{\mathbf{a}},$$

i.e., relative to the standard bases, $(d\varphi)_{\mathbf{a}}$ is the map with matrix

$$\mathrm{Jac}(P_1, \ldots, P_n)(\mathbf{a}) = \begin{pmatrix} \frac{\partial P_1}{\partial X_1}(\mathbf{a}), & \ldots, & \frac{\partial P_1}{\partial X_m}(\mathbf{a}) \\ \vdots & & \vdots \\ \frac{\partial P_n}{\partial X_1}(\mathbf{a}), & \ldots, & \frac{\partial P_n}{\partial X_m}(\mathbf{a}) \end{pmatrix}.$$

For example, suppose $\mathbf{a} = (0, \ldots, 0)$ and $\mathbf{b} = (0, \ldots, 0)$, so that $T_{\mathbf{a}}(\mathbb{A}^m) = k^m$ and $T_{\mathbf{b}}(\mathbb{A}^n) = k^n$, and

$$P_i = \sum_{j=1}^{m} c_{ij} X_j + (\text{higher terms}), i = 1, \ldots, n.$$

Then $Y_i \circ (d\varphi)_{\mathbf{a}} = \sum_j c_{ij} X_j$, 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 $F \in k[X_1, \ldots, X_m]$. 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 5.7. *Let $\varphi\colon \mathbb{A}^m \to \mathbb{A}^n$ be as at the start of this subsection. If φ maps $V = V(\mathfrak{a}) \subset k^m$ into $W = V(\mathfrak{b}) \subset k^n$, then $(d\varphi)_{\mathbf{a}}$ maps $T_{\mathbf{a}}(V)$ into $T_{\mathbf{b}}(W)$, $\mathbf{b} = \varphi(\mathbf{a})$.*

PROOF. We are given that

$$f \in \mathfrak{b} \Rightarrow f \circ \varphi \in \mathfrak{a},$$

and have to prove that

$$f \in \mathfrak{b} \Rightarrow (df)_{\mathbf{b}} \circ (d\varphi)_{\mathbf{a}} \text{ is zero on } T_{\mathbf{a}}(V).$$

The chain rule holds in our situation:

$$\frac{\partial f}{\partial X_i} = \sum_{i=1}^{n} \frac{\partial f}{\partial Y_j}\frac{\partial Y_j}{\partial X_i}, \quad Y_j = P_j(X_1, \ldots, X_m), \quad f = f(Y_1, \ldots, Y_n).$$

If φ is the map given by the equations

$$Y_j = P_j(X_1, \ldots, X_m), \qquad j = 1, \ldots, m,$$

then the chain rule implies

$$d(f \circ \varphi)_{\mathbf{a}} = (df)_{\mathbf{b}} \circ (d\varphi)_{\mathbf{a}}, \quad \mathbf{b} = \varphi(\mathbf{a}).$$

Let $\mathbf{t} \in T_{\mathbf{a}}(V)$; then

$$(df)_{\mathbf{b}} \circ (d\varphi)_{\mathbf{a}}(\mathbf{t}) = d(f \circ \varphi)_{\mathbf{a}}(\mathbf{t}),$$

which is zero if $f \in \mathfrak{b}$ because then $f \circ \varphi \in \mathfrak{a}$. Thus $(d\varphi)_{\mathbf{a}}(\mathbf{t}) \in T_{\mathbf{b}}(W)$. □

We therefore get a map $(d\varphi)_{\mathbf{a}}\colon T_{\mathbf{a}}(V) \to T_{\mathbf{b}}(W)$. The usual rules from advanced calculus hold. For example,

$$(d\psi)_{\mathbf{b}} \circ (d\varphi)_{\mathbf{a}} = d(\psi \circ \varphi)_{\mathbf{a}}, \quad \mathbf{b} = \varphi(\mathbf{a}).$$

The definition we have given of $T_{\mathbf{a}}(V)$ appears to depend on the embedding $V \hookrightarrow \mathbb{A}^n$. Later we shall give an intrinsic of the tangent space, which is independent of any embedding.

EXAMPLE 5.8. Let V be the union of the coordinate axes in $\mathbb{A}^3$, and let W be the zero set of $XY(X - Y)$ in $\mathbb{A}^2$. Each of V and W is a union of three lines meeting at the origin. Are they isomorphic as algebraic varieties? Obviously, the origin o is the only singular point on V or W. 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 $T_o(W)$. But $V = V(XY, YZ, XZ)$, and so $T_o(V)$ has dimension 3, whereas T_oW has dimension 2. Therefore, they are not isomorphic.

Etale maps

DEFINITION 5.9. A regular map $\varphi\colon V \to W$ of smooth varieties is ***étale at a point*** P of V if $(d\varphi)_P\colon T_P(V) \to T_{\varphi(P)}(W)$ is an isomorphism; φ is ***étale*** if it is étale at all points of V.

EXAMPLE 5.10. (a) A regular map

$$\varphi\colon \mathbb{A}^n \to \mathbb{A}^n, \quad a \mapsto (P_1(a_1,\dots,a_n),\dots,P_n(a_1,\dots,a_n))$$

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 $V = \operatorname{Spm}(A)$ be an affine variety, and let $f = \sum c_i X^i \in A[X]$ be such that $A[X]/(f(X))$ is reduced. Let $W = \operatorname{Spm}(A[X]/(f(X))$, and consider the map $W \to V$ corresponding to the inclusion $A \hookrightarrow A[X]/(f)$. Thus

$$\begin{tikzcd} A[X]/(f) & A[X] \arrow[l, two heads] \\ & A \arrow[ul] \arrow[u] \end{tikzcd} \qquad \begin{tikzcd} W \arrow[r, hook] \arrow[dr] & V \times \mathbb{A}^1 \arrow[d] \\ & V. \end{tikzcd}$$

The points of W lying over a point $\mathbf{a} \in V$ are the pairs $(\mathbf{a}, b) \in V \times \mathbb{A}^1$ such that b is a root of $\sum c_i(\mathbf{a})X^i$. I claim that the map $W \to V$ is étale at $(\mathbf{a}, b)$ if and only if b is a *simple* root of $\sum c_i(\mathbf{a})X^i$.

To see this, write $A = \operatorname{Spm} k[X_1,\dots,X_n]/\mathfrak{a}$, $\mathfrak{a} = (f_1,\dots,f_r)$, 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

$$\begin{pmatrix} \frac{\partial f_1}{\partial X_1}(\mathbf{a}) & \cdots & \frac{\partial f_1}{\partial X_m}(\mathbf{a}) & 0 \\ \vdots & & \vdots & \\ \frac{\partial f_n}{\partial X_1}(\mathbf{a}) & \cdots & \frac{\partial f_n}{\partial X_m}(\mathbf{a}) & 0 \\ \frac{\partial f}{\partial X_1}(\mathbf{a}) & \cdots & \frac{\partial f}{\partial X_m}(\mathbf{a}) & \frac{\partial f}{\partial X}(\mathbf{a}, b) \end{pmatrix} \qquad \begin{pmatrix} \frac{\partial f_1}{\partial X_1}(\mathbf{a}) & \cdots & \frac{\partial f_1}{\partial X_m}(\mathbf{a}) \\ \vdots & & \vdots \\ \frac{\partial f_n}{\partial X_1}(\mathbf{a}) & \cdots & \frac{\partial f_n}{\partial X_m}(\mathbf{a}) \end{pmatrix}$$

and the map $T_{(\mathbf{a},b)}(W) \to T_{\mathbf{a}}(V)$ is induced by the projection map $k^{n+1} \to k^n$ omitting 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 of 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 $\sum_i c_i(\mathbf{a})X^i$. The intuitive picture is that $W \to V$ is a finite covering with $\deg(f)$ sheets, which is ramified exactly at the points where two or more sheets cross.

(c) Consider a dominant map $\varphi\colon W \to V$ 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 φ is étale if and only if $\det\left(\frac{\partial P_i}{\partial X_j}(\mathbf{a})\right)$ is never zero.

(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 p94). More precisely, let $\varphi\colon W \to V$ be étale at $P \in W$, and assume V to normal; then there exist a map $\varphi'\colon W' \to V'$ with $k[W'] =$

$k[V'][X]/(f(X))$, and a commutative diagram

$$\begin{array}{ccccccc} W & \supset & U_1 & \approx & U_1' & \subset & W' \\ \downarrow{\scriptstyle\varphi} & & \downarrow & & \downarrow & & \downarrow{\scriptstyle\varphi'} \\ V & \supset & U_2 & \approx & U_2' & \subset & V' \end{array}$$

with the U's all open subvarieties and $P \in U_1$.

In advanced calculus (or differential topology, or complex analysis), the inverse function theorem says that a map φ 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 $\varphi(\mathbf{a})$ such that φ 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

$$\varphi\colon \mathbb{A}^1 \smallsetminus \{0\} \to \mathbb{A}^1 \smallsetminus \{0\}, \quad a \mapsto a^2.$$

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 (5.10b) 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 φ defines an isomorphism $U \to U'$. If there did, then φ 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, φ defines the map $k(X) \to k(X)$, $X \mapsto X^2$, which is not an isomorphism.

ASIDE 5.11. There is an old conjecture that any étale map $\varphi\colon \mathbb{A}^n \to \mathbb{A}^n$ is an isomorphism. If we write $\varphi = (P_1, \ldots, P_n)$, then this becomes the statement:

$$\text{if } \det\left(\frac{\partial P_i}{\partial X_j}(\mathbf{a})\right) \text{ is never zero (for } \mathbf{a} \in k^n\text{), then } \varphi \text{ has a inverse.}$$

The condition, $\det\left(\frac{\partial P_i}{\partial X_j}(\mathbf{a})\right)$ never zero, implies that $\det\left(\frac{\partial P_i}{\partial X_j}\right)$ is a nonzero constant (by the Nullstellensatz 2.6 applied to the ideal generated by $\det\left(\frac{\partial P_i}{\partial X_j}\right)$). This conjecture, which is known as the Jacobian conjecture, has not been settled even for $k = \mathbb{C}$ and $n = 2$, despite the existence of several published proofs and innumerable announced proofs. It has caused many mathematicians a good deal of grief. It is probably harder than it is interesting. See Bass et al. 1982[3].

Intrinsic definition of the tangent space

The definition we have given of the tangent space at a point used an embedding of the variety in affine space. In this section, we give an intrinsic definition that depends only on a small neighbourhood of the point.

[3] Bass, Hyman; Connell, Edwin H.; Wright, David. The Jacobian conjecture: reduction of degree and formal expansion of the inverse. Bull. Amer. Math. Soc. (N.S.) 7 (1982), no. 2, 287–330.

LEMMA 5.12. *Let $\mathfrak{c}$ be an ideal in $k[X_1,\ldots,X_n]$ generated by linear forms $\ell_1,\ldots,\ell_r$, which we may assume to be linearly independent. Let $X_{i_1},\ldots,X_{i_{n-r}}$ be such that*

$$\{\ell_1,\ldots,\ell_r,X_{i_1},\ldots,X_{i_{n-r}}\}$$

is a basis for the linear forms in $X_1,\ldots,X_n$. Then

$$k[X_1,\ldots,X_n]/\mathfrak{c}\simeq k[X_{i_1},\ldots,X_{i_{n-r}}].$$

PROOF. This is obvious if the forms are $X_1,\ldots,X_r$. In the general case, because $\{X_1,\ldots,X_n\}$ and $\{\ell_1,\ldots,\ell_r,X_{i_1},\ldots,X_{i_{n-r}}\}$ are both bases for the linear forms, each element of one set can be expressed as a linear combination of the elements of the other. Therefore,

$$k[X_1,\ldots,X_n]=k[\ell_1,\ldots,\ell_r,X_{i_1},\ldots,X_{i_{n-r}}],$$

and so

$$\begin{aligned}k[X_1,\ldots,X_n]/\mathfrak{c}&=k[\ell_1,\ldots,\ell_r,X_{i_1},\ldots,X_{i_{n-r}}]/\mathfrak{c}\\&\simeq k[X_{i_1},\ldots,X_{i_{n-r}}].\end{aligned}$$

□

Let $V=V(\mathfrak{a})\subset k^n$, and assume that the origin o lies on V. Let $\mathfrak{a}_\ell$ be the ideal generated by the linear terms f_ℓ of the $f\in\mathfrak{a}$. By definition, $T_o(V)=V(\mathfrak{a}_\ell)$. Let $A_\ell=k[X_1,\ldots,X_n]/\mathfrak{a}_\ell$, and let $\mathfrak{m}$ be the maximal ideal in $k[V]$ consisting of the functions zero at o; thus $\mathfrak{m}=(x_1,\ldots,x_n)$.

PROPOSITION 5.13. *There are canonical isomorphisms*

$$\mathrm{Hom}_{k\text{-linear}}(\mathfrak{m}/\mathfrak{m}^2,k)\xrightarrow{\simeq}\mathrm{Hom}_{k\text{-alg}}(A_\ell,k)\xrightarrow{\simeq}T_o(V).$$

PROOF. *First isomorphism:* Let $\mathfrak{n}=(X_1,\ldots,X_n)$ be the maximal ideal at the origin in $k[X_1,\ldots,X_n]$. Then $\mathfrak{m}/\mathfrak{m}^2\simeq\mathfrak{n}/(\mathfrak{n}^2+\mathfrak{a})$, and as $f-f_\ell\in\mathfrak{n}^2$ for every $f\in\mathfrak{a}$, it follows that $\mathfrak{m}/\mathfrak{m}^2\simeq\mathfrak{n}/(\mathfrak{n}^2+\mathfrak{a}_\ell)$. Let $f_{1,\ell},\ldots,f_{r,\ell}$ be a basis for the vector space $\mathfrak{a}_\ell$. From linear algebra we know that there are $n-r$ linear forms $X_{i_1},\ldots,X_{i_{n-r}}$ forming with the $f_{i,\ell}$ a basis for the linear forms on k^n. Then $X_{i_1}+\mathfrak{m}^2,\ldots,X_{i_{n-r}}+\mathfrak{m}^2$ form a basis for $\mathfrak{m}/\mathfrak{m}^2$ as a k-vector space, and the lemma shows that $A_\ell\simeq k[X_{i_1}\ldots,X_{i_{n-r}}]$. A homomorphism $\alpha\colon A_\ell\to k$ of k-algebras is determined by its values $\alpha(X_{i_1}),\ldots,\alpha(X_{i_{n-r}})$, 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 $(a_1,\ldots,a_n)\in k^n$ such that $f(a_1,\ldots,a_n)=0$ for all $f\in\mathfrak{a}_\ell$, which is the same as to give an element of $T_P(V)$. □

Let $\mathfrak{n}$ be the maximal ideal in $\mathcal{O}_o$ $(=A_\mathfrak{m})$. According to (1.31), $\mathfrak{m}/\mathfrak{m}^2\to\mathfrak{n}/\mathfrak{n}^2$, and so there is a canonical isomorphism

$$T_o(V)\xrightarrow{\simeq}\mathrm{Hom}_{k\text{-lin}}(\mathfrak{n}/\mathfrak{n}^2,k).$$

We adopt this as our definition.

DEFINITION 5.14. The ***tangent space*** $T_P(V)$ at a point P of a variety V is defined to be $\mathrm{Hom}_{k\text{-linear}}(\mathfrak{n}_P/\mathfrak{n}_P^2, k)$, where $\mathfrak{n}_P$ the maximal ideal in $\mathcal{O}_P$.

The above discussion shows that this agrees with previous definition[4] for $P = o \in V \subset \mathbb{A}^n$. The advantage of the present definition is that it obviously depends only on a (small) neighbourhood of P. In particular, it doesn't depend on an affine embedding of V.

Note that (1.4) implies that the dimension of $T_P(V)$ is the minimum number of elements needed to generate $\mathfrak{n}_P \subset \mathcal{O}_P$.

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 $\mathfrak{n}_Q \to \mathfrak{n}_P$, $\mathfrak{n}_Q/\mathfrak{n}_Q^2 \to \mathfrak{n}_P/\mathfrak{n}_P^2$, 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, an $f \in \mathfrak{n}_P$ is represented by a regular map $U \to \mathbb{A}^1$ on a neighbourhood U of P sending P to 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 $\mathrm{Hom}_{k\text{-linear}}(\mathfrak{n}_P/\mathfrak{n}_P^2, k)$) to its value at $f \mod \mathfrak{n}_P^2$. 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

$$(df)_P = f - f(P) \mod \mathfrak{n}^2.$$

The tangent space at P and the space of differentials at P are dual vector spaces.

Consider for example, $\mathbf{a} \in V(\mathfrak{a}) \subset \mathbb{A}^n$, with $\mathfrak{a}$ a radical ideal. For $f \in k[\mathbb{A}^n] = k[X_1, \ldots, X_n]$, 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.[5] The tangent space $T_{\mathbf{a}}(V(\mathfrak{a}))$ is the zero set of the equations

$$(df)_P = 0, \qquad f \in \mathfrak{a},$$

and the set $\{(df)_P|_{T_{\mathbf{a}}(V)} \mid f \in k[X_1, \ldots, X_n]\}$ is the dual space to $T_{\mathbf{a}}(V)$.

REMARK 5.15. Let E be a finite dimensional vector space over k. Then

$$T_o(\mathbb{A}(E)) \simeq E.$$

[4]More precisely, define $T_P(V) = \mathrm{Hom}_{k\text{-linear}}(\mathfrak{n}/\mathfrak{n}^2, k)$. For $V = \mathbb{A}^m$, the elements $(dX_i)_o = X_i + \mathfrak{n}^2$ for $1 \leq i \leq m$ form a basis for $\mathfrak{n}/\mathfrak{n}^2$, and hence form a basis for the space of linear forms on $T_P(V)$. A closed immersion $i\colon V \to \mathbb{A}^m$ sending P to o maps $T_P(V)$ isomorphically onto the linear subspace of $T_o(\mathbb{A}^m)$ defined by the equations

$$\sum_{1 \leq i \leq m} \left(\frac{\partial f}{\partial X_i}\right)_o (dX_i)_o = 0, \quad f \in I(iV).$$

[5]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 $k[[X_1 - a_1, \ldots, X_n - a_n]]$.

Nonsingular points

DEFINITION 5.16. (a) A point P on an algebraic variety V is said to be ***nonsingular*** if it lies on a single irreducible component V_i of V, and $\dim_k T_P(V) = \dim V_i$; otherwise the point is said to be ***singular***.

(b) A variety is ***nonsingular*** if all of its points are nonsingular.

(c) The set of singular points of a variety is called its ***singular locus.***

Thus, on an irreducible variety V of dimension d,

$$\begin{aligned} P \text{ is nonsingular} &\iff \dim_k T_P(V) = d \\ &\iff \dim_k(\mathfrak{n}_P/\mathfrak{n}_P^2) = d \\ &\iff \mathfrak{n}_P \text{ can be generated by } d \text{ functions.} \end{aligned}$$

PROPOSITION 5.17. *Let V be an irreducible variety of dimension d. If $P \in V$ is nonsingular, then there exist d regular functions $f_1, \ldots, f_d$ defined in an open neighbourhood U of P such that P is the only common zero of the f_i on U.*

PROOF. Let $f_1, \ldots, f_d$ generate the maximal ideal $\mathfrak{n}_P$ in $\mathcal{O}_P$. Then $f_1, \ldots, f_d$ are all defined on some open affine neighbourhood U of P, and I claim that P is an irreducible component of the zero set $V(f_1, \ldots, f_d)$ of $f_1, \ldots, f_d$ in U. If not, there will be some irreducible component $Z \neq P$ of $V(f_1, \ldots, f_d)$ passing through P. Write $Z = V(\mathfrak{p})$ with $\mathfrak{p}$ a prime ideal in $k[U]$. Because $V(\mathfrak{p}) \subset V(f_1, \ldots, f_d)$ and because Z contains P and is not equal to it, we have

$$(f_1, \ldots, f_d) \subset \mathfrak{p} \subsetneqq \mathfrak{m}_P \qquad \text{(ideals in } k[U]).$$

On passing to the local ring $\mathcal{O}_P = k[U]_{\mathfrak{m}_P}$, we find (using 1.30) that

$$(f_1, \ldots, f_d) \subset \mathfrak{p}\mathcal{O}_P \subsetneqq \mathfrak{n}_P \qquad \text{(ideals in } \mathcal{O}_P).$$

This contradicts the assumption that the f_i generate $\mathfrak{n}_P$. Hence P is an irreducible component of $V(f_1, \ldots, f_d)$. On removing the remaining irreducible components of $V(f_1, \ldots, f_d)$ from U, we obtain an open neighbourhood of P with the required property. □

THEOREM 5.18. *The set of nonsingular points of a variety is dense and open.*

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 $P_1, \ldots, P_r$ 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

$$\mathrm{Jac}(P_1, \ldots, P_r)(\mathbf{a}) = \begin{pmatrix} \frac{\partial P_1}{\partial X_1}(\mathbf{a}) & \ldots & \frac{\partial P_1}{\partial X_m}(\mathbf{a}) \\ \vdots & & \vdots \\ \frac{\partial P_r}{\partial X_1}(\mathbf{a}) & \ldots & \frac{\partial P_r}{\partial X_m}(\mathbf{a}) \end{pmatrix}$$

Proper: According to (4.32) and (4.34) there is a nonempty open subset of V isomorphic to a nonempty open subset of an irreducible hypersurface in $\mathbb{A}^{d+1}$, and so we may suppose 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 $F(X_1, \ldots, X_{d+1})$. By (2.25), $\dim V = d$. Now the proof is the same as that of (5.3): 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 $X_2, \ldots X_{d+1}$ (characteristic zero) or in $X_1^p, X_2, \ldots, X_{d+1}$ (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. $\square$

COROLLARY 5.19. *An irreducible algebraic variety is nonsingular if and only if its tangent spaces $T_P(V)$, $P \in V$, all have the same dimension.*

PROOF. According to the theorem, the constant dimension of the tangent spaces must be the dimension of V, and so all points are nonsingular. $\square$

COROLLARY 5.20. *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 $G = \bigcup gU$. (Alternatively, because G is homogeneous, all tangent spaces have the same dimension.) $\square$

In fact, any variety on which a group acts transitively by regular maps will be nonsingular.

ASIDE 5.21. 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.

Nonsingularity and regularity

In this section we assume two results that won't be proved until §9.

5.22. *For any irreducible variety V and regular functions $f_1, \ldots, f_r$ on V, the irreducible components of $V(f_1, \ldots, f_r)$ have dimension $\geq \dim V - r$ (see 9.7).*

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 its solutions form an affine space of dimension at least $n - r$.

5.23. *If V is an irreducible variety of dimension d, then the local ring at each point P of V has dimension d (see 9.6).*

Because of (1.30), the height of a prime ideal $\mathfrak{p}$ of a ring A is the Krull dimension of $A_{\mathfrak{p}}$. Thus (5.23) 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 (5.23): If $V = \mathbb{A}^d$, then $A = k[X_1, \ldots, X_d]$, and all maximal ideals in this ring have height d, for example,

$$(X_1 - a_1, \ldots, X_d - a_d) \supset (X_1 - a_1, \ldots, X_{d-1} - a_{d-1}) \supset \ldots \supset (X_1 - a_1) \supset 0$$

is a chain of prime ideals of length d that can't be refined, and there is no longer chain. In the general case, the Noether normalization theorem says that $k[V]$ is integral over a polynomial ring $k[x_1, \ldots, x_d]$, $x_i \in k[V]$; then clearly $x_1, \ldots, x_d$ is a transcendence basis for $k(V)$, and the going up and down theorems show that the local rings of $k[V]$ and $k[x_1, \ldots, x_d]$ have the same dimension.

THEOREM 5.24. *Let P be a point on an irreducible variety V. Any generating set for the maximal ideal $\mathfrak{n}_P$ of $\mathcal{O}_P$ has at least d elements, and there exists a generating set with d elements if and only if P is nonsingular.*

PROOF. If $f_1, \ldots, f_r$ generate $\mathfrak{n}_P$, then the proof of (5.17) shows that P is an irreducible component of $V(f_1, \ldots, f_r)$ in some open neighbourhood U of P. Therefore (5.22) shows that $0 \geq d - r$, and so $r \geq d$. The rest of the statement has already been noted. □

COROLLARY 5.25. *A point P on an irreducible variety is nonsingular if and only if $\mathcal{O}_P$ is regular.*

PROOF. This is a restatement of the second part of the theorem. □

According to CA 16.3, a regular local ring is an integral domain. If P lies on two irreducible components of a V, then $\mathcal{O}_P$ is not an integral domain,[6] and so $\mathcal{O}_P$ is not regular. Therefore, the corollary holds also for reducible varieties.

Nonsingularity and normality

An integral domain that is integrally closed in its field of fractions is called a ***normal*** ring.

LEMMA 5.26. *An integral domain A is normal if and only if $A_{\mathfrak{m}}$ is normal 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

$$(sb)^n + (sc_1)(sb)^{n-1} + \cdots + s^n c_n = 0,$$

[6] Suppose that P lies on the intersection $Z_1 \cap Z_2$ of the distinct irreducible components Z_1 and Z_2. Since $Z_1 \cap Z_2$ is a proper closed subset of Z_1, there is an open affine neighbourhood U of P such that $U \cap Z_1 \cap Z_2$ is a proper closed subset of $U \cap Z_1$, and so there is a nonzero regular function f_1 on $U \cap Z_1$ 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 $Q \in Z_2$. Then f_1 defines a nonzero 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.

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 $A = \bigcap A_{\mathfrak{m}}$ (if $c \in \bigcap A_{\mathfrak{m}}$, 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 $V = \bigcup V_i$ 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***. More generally, an algebraic variety V is said to be ***normal*** if $\mathcal{O}_P$ is normal for all $P \in V$. 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 (each of which is normal).

A regular local noetherian ring is always normal (cf. CA 16.3); conversely, a normal local integral domain *of dimension one* is regular. 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 set of singular points on a normal variety V must have dimension $\leq \dim V - 2$. For example, a normal surface can only have isolated singularities — the singular locus can't contain a curve.

Etale neighbourhoods

Recall that a regular map $\alpha: W \to V$ is said to be étale at a nonsingular point P of W if the map $(d\alpha)_P: T_P(W) \to T_{\alpha(P)}(V)$ 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 $\{f_1, \ldots, f_d\}$ of germs of regular functions at P generating the maximal ideal $\mathfrak{n}_P \subset \mathcal{O}_P$. Equivalent conditions: the images of $f_1, \ldots, f_d$ in $\mathfrak{n}_P/\mathfrak{n}_P^2$ generate it as a k-vector space (see 1.4); or $(df_1)_P, \ldots, (df_d)_P$ is a basis for dual space to $T_P(V)$.

PROPOSITION 5.27. *Let $\{f_1, \ldots, f_d\}$ 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 $f_1, f_2, \ldots, f_d$ are represented by pairs $(\tilde{f}_1, U), \ldots, (\tilde{f}_d, U)$ and the map $(\tilde{f}_1, \ldots, \tilde{f}_d): U \to \mathbb{A}^d$ 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 (5.18), we can choose to be nonsingular. The map $\alpha = (\tilde{f}_1, \ldots, \tilde{f}_d): U' \to \mathbb{A}^d$ is étale at P, because the dual map to $(d\alpha)_{\mathfrak{a}}$ is $(dX_i)_o \mapsto (d\tilde{f}_i)_{\mathfrak{a}}$. The next lemma then shows that α is étale on an open neighbourhood U of P. □

LEMMA 5.28. *Let W and V be nonsingular varieties. If $\alpha: W \to V$ 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 $P_1(X_1,\ldots,X_m),\ldots,P_n(X_1,\ldots,X_m)$. 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 $f_1,\ldots,f_r$ 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 5.29. *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* $(0,\ldots,0) \in \mathbb{A}^d$.

PROOF. This is a restatement of the Proposition. □

ASIDE 5.30. 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.

The inverse function theorem

THEOREM 5.31 (INVERSE FUNCTION THEOREM). *If a regular map of nonsingular varieties $\varphi\colon V \to W$ is étale at $P \in V$, then there exists a commutative diagram*

$$\begin{tikzcd} V \arrow[d, "\varphi"] & U_P \arrow[l, "\text{open}"'] \arrow[d, "\varphi'", "\approx"'] \\ W & U_{\varphi(P)} \arrow[l, "\text{étale}"'] \end{tikzcd}$$

with U_P an open neighbourhood U of P, $U_{f(P)}$ an étale neighbourhood $\varphi(P)$, and φ' an isomorphism.

PROOF. According to (5.38), there exists an open neighbourhood U of P such that the restriction $\varphi|U$ of φ to U is étale. To get the above diagram, we can take $U_P = U$, $U_{\varphi(P)}$ to be the étale neighbourhood $\varphi|U\colon U \to W$ of $\varphi(P)$, and φ' to be the identity map. □

The rank theorem

For vector spaces, the rank theorem says the following: let $\alpha\colon V \to W$ be a linear map of k-vector spaces of rank r; then there exist bases for V and W relative to which α has matrix $\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$. In other words, there is a commutative diagram

$$\begin{tikzcd} V \arrow[r, "\alpha"] \arrow[d, "\approx"] & W \arrow[d, "\approx"] \\ k^m \arrow[r, "(x_1,\ldots,x_m)\mapsto(x_1,\ldots,x_r,0,\ldots)"] & k^n \end{tikzcd}$$

A similar result holds locally for differentiable manifolds. In algebraic geometry, there is the following weaker analogue.

THEOREM 5.32 (RANK THEOREM). *Let $\varphi\colon V \to W$ be a regular map of nonsingular varieties of dimensions m and n respectively, and let $P \in V$. If $\operatorname{rank}(T_P(\varphi)) = n$, then there exists a commutative diagram*

$$\begin{tikzcd} U_P \arrow[r, "\varphi|U_P"] \arrow[d, "\text{étale}"] & U_{\varphi(P)} \arrow[d, "\text{étale}"] \\ \mathbb{A}^m \arrow[r, "(x_1,\ldots,x_m)\mapsto(x_1,\ldots,x_n)"] & \mathbb{A}^n \end{tikzcd}$$

in which U_P and $U_{\varphi(P)}$ are open neighbourhoods of P and $\varphi(P)$ respectively and the vertical maps are étale.

PROOF. Choose a local system of parameters $g_1, \ldots, g_n$ at $\varphi(P)$, and let $f_1 = g_1 \circ \varphi, \ldots, f_n = g_n \circ \varphi$. Then $df_1, \ldots, df_n$ are linearly independent forms on $T_P(V)$, and there exist $f_{n+1}, \ldots, f_m$ such $df_1, \ldots, df_m$ is a basis for $T_P(V)^\vee$. Then $f_1, \ldots, f_m$ is a local system of parameters at P. According to (5.28), there exist open neighbourhoods U_P of P and $U_{\varphi(P)}$ of $\varphi(P)$ such that the maps

$$(f_1, \ldots, f_m)\colon U_P \to \mathbb{A}^m$$
$$(g_1, \ldots, g_n)\colon U_{\varphi(P)} \to \mathbb{A}^n$$

are étale. They give the vertical maps in the above diagram. □

Smooth maps

DEFINITION 5.33. A regular map $\varphi\colon V \to W$ of nonsingular varieties is ***smooth at a point*** P of V if $(d\varphi)_P\colon T_P(V) \to T_{\varphi(P)}(W)$ is surjective; φ is ***smooth*** if it is smooth at all points of V.

THEOREM 5.34. *A map $\varphi\colon V \to W$ is smooth at $P \in V$ if and only if there exist open neighbourhoods U_P and $U_{\varphi(P)}$ of P and $\varphi(P)$ respectively such that $\varphi|U_P$ factors into*

$$U_P \xrightarrow{\text{étale}} \mathbb{A}^{\dim V - \dim W} \times U_{\varphi(P)} \xrightarrow{q} U_{\varphi(P)}.$$

PROOF. Certainly, if $\varphi|U_P$ factors in this way, it is smooth. Conversely, if φ is smooth at P, then we get a diagram as in the rank theorem. From it we get maps

$$U_P \to \mathbb{A}^m \times_{\mathbb{A}^n} U_{\varphi(P)} \to U_{\varphi(P)}.$$

The first is étale, and the second is the projection of $\mathbb{A}^{m-n} \times U_{\varphi(P)}$ onto $U_{\varphi(P)}$. □

COROLLARY 5.35. *Let V and W be nonsingular varieties. If $\varphi: V \to W$ is smooth at P, then it is smooth on an open neighbourhood of V.*

PROOF. In fact, it is smooth on the neighbourhood U_P in the theorem. □

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 $D: A \to M$ such that

(a) $D(c) = 0$ for all $c \in k$;
(b) $D(f + g) = D(f) + D(g)$;
(c) $D(fg) = f \cdot Dg + f \cdot Dg$ (Leibniz's 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 $f \mapsto (df)_P \overset{\text{def}}{=} f - f(P) \bmod \mathfrak{n}_P^2$ is a k-derivation $\mathcal{O}_P \to \mathfrak{n}_P/\mathfrak{n}_P^2$.

PROPOSITION 5.36. *There are canonical isomorphisms*

$$\mathrm{Der}_k(\mathcal{O}_P, k) \xrightarrow{\simeq} \mathrm{Hom}_{k\text{-linear}}(\mathfrak{n}_P/\mathfrak{n}_P^2, k) \xrightarrow{\simeq} T_P(V).$$

PROOF. The composite $k \xrightarrow{c \mapsto c} \mathcal{O}_P \xrightarrow{f \mapsto f(P)} k$ is the identity map, and so, when regarded as k-vector space, $\mathcal{O}_P$ decomposes into

$$\mathcal{O}_P = k \oplus \mathfrak{n}_P, \quad f \leftrightarrow (f(P), f - f(P)).$$

A derivation $D: \mathcal{O}_P \to k$ is zero on k and on $\mathfrak{n}_P^2$ (by Leibniz's rule). It therefore defines a k-linear map $\mathfrak{n}_P/\mathfrak{n}_P^2 \to k$. Conversely, a k-linear map $\mathfrak{n}_P/\mathfrak{n}_P^2 \to k$ defines a derivation by composition

$$\mathcal{O}_P \xrightarrow{f \mapsto (df)_P} \mathfrak{n}_P/\mathfrak{n}_P^2 \to k.$$ □

The ***ring of dual numbers*** is $k[\varepsilon] = k[X]/(X^2)$ where $\varepsilon = X + (X^2)$. As a k-vector space it has a basis $\{1, \varepsilon\}$, and $(a + b\varepsilon)(a' + b'\varepsilon) = aa' + (ab' + a'b)\varepsilon$.

PROPOSITION 5.37. *The tangent space to V at P is canonically isomorphic to the space of local homomorphisms of local k-algebras $\mathcal{O}_P \to k[\varepsilon]$:*

$$T_P(V) \simeq \mathrm{Hom}(\mathcal{O}_P, k[\varepsilon]).$$

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 $\mathcal{O}_P \to k$. Conversely, all such derivations D arise in this way. □

Recall (4.42) that for an affine variety V and a k-algebra R (not necessarily an affine k-algebra), we define $V(R)$ to be $\mathrm{Hom}_{k\text{-alg}}(k[V], A)$. For example, if $V = V(\mathfrak{a}) \subset \mathbb{A}^n$ with $\mathfrak{a}$ radical, then

$$V(A) = \{(a_1, \ldots, a_n) \in A^n \mid f(a_1, \ldots, a_n) = 0 \text{ all } f \in \mathfrak{a}\}.$$

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 $k[X_1, \ldots, X_n]$, 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 $F(X_1, \ldots, X_n)$ in terms of the variables $X_i - a_i$, we obtain a formula (trivial Taylor formula)

$$F(X_1, \ldots, X_n) = F(a_1, \ldots, a_n) + \sum \left.\frac{\partial F}{\partial X_i}\right|_{\mathbf{a}} (X_i - a_i) + R$$

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:

$$F(a_1 + \varepsilon b_1, \ldots, a_n + \varepsilon b_n) = \varepsilon\left(\sum \left.\frac{\partial F}{\partial X_i}\right|_{\mathbf{a}} b_i\right).$$

Consequently, $(a_1 + \varepsilon b_1, \ldots, a_n + \varepsilon b_n)$ lies on V if and only if $(b_1, \ldots, b_n) \in T_{\mathbf{a}}(V)$ (original definition p84).

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 "tangent direction"

REMARK 5.38. 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.

(a) A matrix $I+\varepsilon A$ has inverse $I-\varepsilon A$ in $M_n(k[\varepsilon])$, and so lies in $\mathrm{GL}_n(k[\varepsilon])$. Therefore,

$$\begin{aligned} T_e(\mathrm{GL}_n) &= \{I + \varepsilon A \mid A \in M_n\} \\ &\simeq M_n(k). \end{aligned}$$

(b) Since

$$\det(I + \varepsilon A) = I + \varepsilon \operatorname{trace}(A)$$

(using that $\varepsilon^2 = 0$),

$$\begin{aligned} T_e(\mathrm{SL}_n) &= \{I + \varepsilon A \mid \operatorname{trace}(A) = 0\} \\ &\simeq \{A \in M_n(k) \mid \operatorname{trace}(A) = 0\}. \end{aligned}$$

(c) Assume the characteristic $\neq 2$, and let O_n be orthogonal group:

$$\mathrm{O}_n = \{A \in \mathrm{GL}_n \mid A^{\mathrm{tr}} \cdot A = I\}.$$

(A^{tr} denotes the transpose of A). This is the group of matrices preserving the quadratic form $X_1^2 + \cdots + X_n^2$. The determinant defines a surjective regular homomorphism $\det\colon O_n \to \{\pm 1\}$, whose kernel is defined to be the special orthogonal group SO_n. For $I + \varepsilon A \in M_n(k[\varepsilon])$,

$$(I + \varepsilon A)^{\mathrm{tr}} \cdot (I + \varepsilon A) = I + \varepsilon A^{\mathrm{tr}} + \varepsilon A,$$

and so

$$\begin{aligned} T_e(\mathrm{O}_n) = T_e(\mathrm{SO}_n) &= \{I + \varepsilon A \in M_n(k[\varepsilon]) \mid A \text{ is skew-symmetric}\} \\ &\simeq \{A \in M_n(k) \mid A \text{ is skew-symmetric}\}. \end{aligned}$$

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.

ASIDE 5.39. On the tangent space $T_e(\mathrm{GL}_n) \simeq M_n$ of GL_n, there is a bracket operation

$$[M, N] \stackrel{\text{def}}{=} MN - NM$$

which makes $T_e(\mathrm{GL}_n)$ into a Lie algebra. For any closed algebraic 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 in terms of left invariant derivations), 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 it 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 $\mathrm{diag}(\zeta, \ldots, \zeta)$, $\zeta^n = 1$, 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 section, 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 $P = (0, \ldots, 0) \in V$. 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 p82). The ***geometric tangent cone*** at P, $C_P(V)$ is $V(\mathfrak{a}_*)$, and the ***tangent cone*** is the pair $(V(\mathfrak{a}_*), k[X_1, \ldots, X_n]/\mathfrak{a}_*)$. 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 $\mathfrak{a} = (F_1, \ldots, F_r)$, then it need not be true that $\mathfrak{a}_* = (F_{1*}, \ldots, F_{r*})$. 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, problem 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

$$\mathrm{gr}(A) = \bigoplus\nolimits_{i \geq 0} \mathfrak{n}^i/\mathfrak{n}^{i+1}.$$

Note that if $A = B_\mathfrak{m}$ and $\mathfrak{n} = \mathfrak{m}A$, then $\mathrm{gr}(A) = \bigoplus \mathfrak{m}^i/\mathfrak{m}^{i+1}$ (because of (1.31)).

PROPOSITION 5.40. *The map $k[X_1,\dots,X_n]/\mathfrak{a}_* \to gr(\mathcal{O}_P)$ sending the class of X_i in $k[X_1,\dots,X_n]/\mathfrak{a}_*$ to the class of X_i in $gr(\mathcal{O}_P)$ is an isomorphism.*

PROOF. Let $\mathfrak{m}$ be the maximal ideal in $k[X_1,\dots,X_n]/\mathfrak{a}$ corresponding to P. Then

$$\begin{aligned}\mathrm{gr}(\mathcal{O}_P) &= \sum \mathfrak{m}^i/\mathfrak{m}^{i+1}\\ &= \sum (X_1,\dots,X_n)^i/(X_1,\dots,X_n)^{i+1} + \mathfrak{a}\cap(X_1,\dots,X_n)^i\\ &= \sum (X_1,\dots,X_n)^i/(X_1,\dots,X_n)^{i+1} + \mathfrak{a}_i\end{aligned}$$

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

$$(X_1,\dots,X_n)^i/(X_1,\dots,X_n)^{i+1} + \mathfrak{a}_i = i^{\text{th}} \text{ homogeneous piece of } k[X_1,\dots,X_n]/\mathfrak{a}_*.$$

□

For a general variety V and $P \in V$, we define the ***geometric tangent cone*** $C_P(V)$ of V at P to be $\mathrm{Spm}(\mathrm{gr}(\mathcal{O}_P)_{\mathrm{red}})$, where $\mathrm{gr}(\mathcal{O}_P)_{\mathrm{red}}$ is the quotient of $\mathrm{gr}(\mathcal{O}_P)$ by its nilradical, and we define the ***tangent cone*** to be $(C_P(V), \mathrm{gr}(\mathcal{O}_P))$.

Recall (Atiyah and MacDonald 1969, 11.21) that $\dim(A) = \dim(\mathrm{gr}(A))$. 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 $\mathrm{gr}(\mathcal{O}_P)$ 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 $\mathrm{gr}(\mathcal{O}_P)$ 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 $\mathrm{gr}(\mathcal{O}_{\alpha(P)}) \to \mathrm{gr}(\mathcal{O}_P)$.

The map on the rings $k[X_1,\dots,X_n]/\mathfrak{a}^*$ defined by a map of algebraic varieties is not the obvious one, i.e., it is not necessarily induced by the same map on polynomial rings as the original map. To see what it is, it is necessary to use Proposition 5.40, i.e., it is necessary to work with the rings $\mathrm{gr}(\mathcal{O}_P)$.

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 (ibid., 10.23). Thus $\alpha\colon V \to W$ is étale at P if and only if the map $\hat{\mathcal{O}}_{\alpha(P)} \to \hat{\mathcal{O}}_P$ is an isomorphism. Hence (5.27) 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: $a_n = f^{(n)}(a)/n!$.

Exercises

5-1. Find the singular points, and the tangent cones at the singular points, for each of

(a) $Y^3 - Y^2 + X^3 - X^2 + 3Y^2X + 3X^2Y + 2XY$;
(b) $X^4 + Y^4 - X^2Y^2$ (assume the characteristic is not 2).

5-2. Let $V \subset \mathbb{A}^n$ be an irreducible affine variety, and let P be a nonsingular point on V. Let H be a hyperplane in $\mathbb{A}^n$ (i.e., the subvariety defined by a linear equation $\sum a_i X_i = d$ with not all a_i zero) passing through P but not containing $T_P(V)$. Show that P is a nonsingular point on each irreducible component of $V \cap H$ on which it lies. (Each irreducible component has codimension 1 in V — you may assume this.) Give an example with $H \supset T_P(V)$ and P singular on $V \cap H$. Must P be singular on $V \cap H$ if $H \supset T_P(V)$?

5-3. Let P and Q be points on varieties V and W. Show that

$$T_{(P,Q)}(V \times W) = T_P(V) \oplus T_Q(W).$$

5-4. For each n, show that there is a curve C and a point P on C such that the tangent space to C at P has dimension n (hence C can't be embedded in $\mathbb{A}^{n-1}$).

5-5. Let I be the $n \times n$ identity matrix, and let J be the matrix $\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$. The ***symplectic group*** Sp_n is the group of $2n \times 2n$ matrices A with determinant 1 such that $A^{\mathrm{tr}} \cdot J \cdot A = J$. (It is the group of matrices fixing a nondegenerate skew-symmetric form.) Find the tangent space to Sp_n at its identity element, and also the dimension of Sp_n.

5-6. Find a regular map $\alpha\colon V \to W$ which induces an isomorphism on the geometric tangent cones $C_P(V) \to C_{\alpha(P)}(W)$ but is not étale at P.

5-7. Show that the cone $X^2 + Y^2 = Z^2$ is a normal variety, even though the origin is singular (characteristic $\neq 2$). See p94.

5-8. Let $V = V(\mathfrak{a}) \subset \mathbb{A}^n$. Suppose that $\mathfrak{a} \neq I(V)$, and for $\mathbf{a} \in V$, let $T'_{\mathbf{a}}$ be the subspace of $T_{\mathbf{a}}(\mathbb{A}^n)$ defined by the equations $(df)_{\mathbf{a}} = 0$, $f \in \mathfrak{a}$. Clearly, $T'_{\mathbf{a}} \supset T_{\mathbf{a}}(V)$, but need they always be different?

Chapter 6

Projective Varieties

Throughout this chapter, k will be an algebraically closed field. Recall (4.3) that we defined $\mathbb{P}^n$ to be the set of equivalence classes in $k^{n+1} \smallsetminus \{\text{origin}\}$ for the relation

$$(a_0, \ldots, a_n) \sim (b_0, \ldots, b_n) \iff (a_0, \ldots, a_n) = c(b_0, \ldots, b_n) \text{ for some } c \in k^\times.$$

Write $(a_0 : \ldots : a_n)$ for the equivalence class of $(a_0, \ldots, a_n)$, and π for the map

$$k^{n+1} \smallsetminus \{\text{origin}\}/{\sim} \to \mathbb{P}^n.$$

Let U_i be the set of $(a_0 : \ldots : a_n) \in \mathbb{P}^n$ such that $a_i \neq 0$, and let u_i be the bijection

$$(a_0 : \ldots : a_n) \mapsto \left(\frac{a_0}{a_i}, \ldots, \frac{a_n}{a_i}\right) : U_i \mapsto \mathbb{A}^n \quad (\tfrac{a_i}{a_i} \text{ omitted}).$$

In this chapter, we shall define on $\mathbb{P}^n$ a (unique) structure of an algebraic variety for which these maps become isomorphisms of affine algebraic varieties. A variety isomorphic to a closed subvariety of $\mathbb{P}^n$ is called a ***projective variety***, and a variety isomorphic to a locally closed subvariety of $\mathbb{P}^n$ is called a ***quasi-projective variety***.[1] Every affine variety is quasiprojective, but there are many varieties that are not quasiprojective. We study morphisms between quasiprojective varieties.

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 (see 6.34 below) says that a curve of degree m in the projective plane 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 $F(X_0, \ldots, X_n)$ is said to be ***homogeneous of degree*** d if it is a sum of terms $a_{i_0,\ldots,i_n} X_0^{i_0} \cdots X_n^{i_n}$ with $i_0 + \cdots + i_n = d$; equivalently,

$$F(tX_0, \ldots, tX_n) = t^d F(X_0, \ldots, X_n)$$

[1]A subvariety of an affine variety is said to be ***quasi-affine***. For example, $\mathbb{A}^2 \smallsetminus \{(0,0)\}$ is quasi-affine but not affine.

for all $t \in k$. Write $k[X_0, \ldots, X_n]_d$ for the subspace of $k[X_0, \ldots, X_n]$ of polynomials of degree d. Then

$$k[X_0, \ldots, X_n] = \bigoplus_{d \geq 0} k[X_0, \ldots, X_n]_d;$$

that is, each polynomial F can be written uniquely as a sum $F = \sum F_d$ with F_d homogeneous of degree d.

Let $P = (a_0 : \ldots : a_n) \in \mathbb{P}^n$. Then P also equals $(ca_0 : \ldots : ca_n)$ for any $c \in k^\times$, and so we can't speak of the value of a polynomial $F(X_0, \ldots, X_n)$ at P. However, if F is homogeneous, then $F(ca_0, \ldots, ca_n) = c^d F(a_0, \ldots, a_n)$, and so it does make sense to say that F is zero or not zero at P. An ***algebraic set in*** $\mathbb{P}^n$ (or ***projective algebraic set***) is the set of common zeros in $\mathbb{P}^n$ of some set of homogeneous polynomials.

EXAMPLE 6.1. Consider the projective algebraic subset E of $\mathbb{P}^2$ defined by the homogeneous equation

$$Y^2 Z = X^3 + aXZ^2 + bZ^3 \tag{13}$$

where $X^3 + aX + b$ is assumed not to have multiple roots. It consists of the points $(x : y : 1)$ on the affine curve $E \cap U_2$

$$Y^2 = X^3 + aX + b,$$

together with the point "at infinity" $(0 : 1 : 0)$.

Curves defined by equations of the form (13) are called ***elliptic curves***. They can also be described as the curves of genus one, or as the abelian varieties of dimension one. Such a curve becomes 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. (Without the point at infinity, it is not possible to make E into an algebraic group.)

When $a, b \in \mathbb{Q}$, 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 book on Elliptic Curves for all of this.)

An ideal $\mathfrak{a} \subset k[X_0, \ldots, X_n]$ is said to be ***homogeneous*** if it contains with any polynomial F all the homogeneous components of F, i.e., if

$$F \in \mathfrak{a} \implies F_d \in \mathfrak{a}, \text{ all } d.$$

It is straightforward to check that

◇ an ideal is homogeneous if and only if it is generated by (a finite set of) homogeneous polynomials;
◇ the radical of a homogeneous ideal is homogeneous;
◇ an intersection, product, or 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 $\mathfrak{a}$. If $F_1, \ldots, F_r$ are homogeneous generators for $\mathfrak{a}$, then $V(\mathfrak{a})$ is the set of common zeros of the F_i. Clearly every polynomial in $\mathfrak{a}$ is zero on every representative of a point in $V(\mathfrak{a})$. We write $V^{\text{aff}}(\mathfrak{a})$ for the set of common zeros of $\mathfrak{a}$ in k^{n+1}. It is ***cone*** in k^{n+1}, i.e., together with any point P it contains the line through P and the origin, and

$$V(\mathfrak{a}) = (V^{\text{aff}}(\mathfrak{a}) \smallsetminus (0,\ldots,0))/\!\sim .$$

The sets $V(\mathfrak{a})$ have similar properties to their namesakes in $\mathbb{A}^n$.

PROPOSITION 6.2. *There are the following relations:*

(a) $\mathfrak{a} \subset \mathfrak{b} \Rightarrow V(\mathfrak{a}) \supset V(\mathfrak{b})$;
(b) $V(0) = \mathbb{P}^n$; $\quad V(\mathfrak{a}) = \varnothing \iff \mathit{rad}(\mathfrak{a}) \supset (X_0,\ldots,X_n)$;
(c) $V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$;
(d) $V(\sum \mathfrak{a}_i) = \bigcap V(\mathfrak{a}_i)$.

PROOF. Statement (a) is obvious. For the second part of (b), note that

$$V(\mathfrak{a}) = \emptyset \iff V^{\text{aff}}(\mathfrak{a}) \subset \{(0,\ldots,0)\} \iff \operatorname{rad}(\mathfrak{a}) \supset (X_0,\ldots,X_n),$$

by the strong Nullstellensatz (2.11). The remaining statements can be proved directly, or by using the relation between $V(\mathfrak{a})$ and $V^{\text{aff}}(\mathfrak{a})$. □

If C is a cone in k^{n+1}, then $I(C)$ is a homogeneous ideal in $k[X_0,\ldots,X_n]$: if $F(ca_0,\ldots,ca_n) = 0$ for all $c \in k^{\times}$, then

$$\sum_d F_d(a_0,\ldots,a_n)\cdot c^d = F(ca_0,\ldots,ca_n) = 0,$$

for infinitely many c, and so $\sum F_d(a_0,\ldots,a_n)X^d$ is the zero polynomial. For a subset S of $\mathbb{P}^n$, we define the ***affine cone over*** S in k^{n+1} to be

$$C = \pi^{-1}(S) \cup \{\text{origin}\}$$

and we set

$$I(S) = I(C).$$

Note that if S is nonempty and closed, then C is the closure of $\pi^{-1}(S) = \emptyset$, and that $I(S)$ is spanned by the homogeneous polynomials in $k[X_0,\ldots,X_n]$ that are zero on S.

PROPOSITION 6.3. *The maps V and I define inverse bijections between the set of algebraic subsets of $\mathbb{P}^n$ and the set of proper homogeneous radical ideals of $k[X_0,\ldots,X_n]$. 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

$$\begin{tikzcd}
\{\text{algebraic subsets of } \mathbb{P}^n\} \arrow[rr, "S\mapsto C"] & & \{\text{nonempty closed cones in } k^{n+1}\} \arrow[dl, "I"] \\
& \{\text{proper homogeneous radical ideals in } k[X_0,\ldots,X_n]\} \arrow[ul, "V"] &
\end{tikzcd}$$

Here the top map sends S to the affine cone over S, and the maps V and I are in the sense of projective geometry and affine geometry respectively. The composite of any three of these maps is the identity map, which proves the first statement because the composite of the top map with I is I in the sense of projective geometry. 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. □

Note that $(X_0, \ldots, X_n)$ and $k[X_0, \ldots, X_n]$ are both radical homogeneous ideals, but

$$V(X_0, \ldots, X_n) = \emptyset = V(k[X_0, \ldots, X_n])$$

and so the correspondence between irreducible subsets of $\mathbb{P}^n$ and radical homogeneous ideals is not quite one-to-one.

The Zariski topology on $\mathbb{P}^n$

Proposition 6.2 shows that the projective algebraic sets are the closed sets for a topology on $\mathbb{P}^n$. In this section, we verify that it agrees with that defined in the first paragraph of this chapter. 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 base for the topology of $\mathbb{P}^n$.

To each polynomial $f(X_1, \ldots, X_n)$, we attach the homogeneous polynomial of the same degree

$$f^*(X_0, \ldots, X_n) = X_0^{\deg(f)} f\left(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}\right),$$

and to each homogeneous polynomial $F(X_0, \ldots, X_n)$, we attach the polynomial

$$F_*(X_1, \ldots, X_n) = F(1, X_1, \ldots, X_n).$$

PROPOSITION 6.4. *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 6.5. 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 p39). 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 $\mathbb{P}^n$.

Closed subsets of $\mathbb{A}^n$ and $\mathbb{P}^n$

We identify $\mathbb{A}^n$ with U_0, and examine the closures in $\mathbb{P}^n$ of closed subsets of $\mathbb{A}^n$. Note that

$$\mathbb{P}^n = \mathbb{A}^n \sqcup H_\infty, \quad H_\infty = V(X_0).$$

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 6.6. *(a) Let V be a closed subset of $\mathbb{A}^n$. Then V^* is the closure of V in $\mathbb{P}^n$, and $(V^*)_* = V$. If $V = \bigcup V_i$ is the decomposition of V into its irreducible components, then $V^* = \bigcup V_i^*$ is the decomposition of V^* into its irreducible components.*

(b) Let V be a closed subset of $\mathbb{P}^n$. Then $V_* = V \cap \mathbb{A}^n$, and 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. □

EXAMPLE 6.7. (a) For

$$V\colon Y^2 = X^3 + aX + b,$$

we have

$$V^*\colon Y^2 Z = X^3 + aXZ^2 + bZ^3,$$

and $(V^*)_* = V$.

(b) Let $V = V(f_1, \ldots, f_m)$; then the closure of V in $\mathbb{P}^n$ is the union of the irreducible components of $V(f_1^*, \ldots, f_m^*)$ not contained in H_∞. For example, let $V = V(X_1, X_1^2 + X_2) = \{(0,0)\}$; then $V(X_0 X_1, X_1^2 + X_0 X_2)$ consists of the two points $(1\colon 0\colon 0)$ (the closure of V) and $(0\colon 0\colon 1)$ (which is contained in H_∞).[2]

(b) For $V = H_\infty = V(X_0)$, $V_* = \emptyset = V(1)$ and $(V_*)^* = \emptyset \neq V$.

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

$$H_\infty = \{(0 : a_1 : \ldots : a_n) \subset \mathbb{P}^n\},$$

[2] Of course, in this case $\mathfrak{a} = (X_1, X_2)$, $\mathfrak{a}^* = (X_1, X_2)$, and $V^* = \{(1\colon 0\colon 0)\}$, and so this example doesn't contradict the proposition.

which can be identified with $\mathbb{P}^{n-1}$.

For example, $\mathbb{P}^1 = \mathbb{A}^1 \sqcup H_\infty$ (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

$$1 + aX_1 + bX_2 = 0$$

in $\mathbb{A}^2$. Its closure in $\mathbb{P}^2$ is the line

$$X_0 + aX_1 + bX_2 = 0.$$

This line intersects the line $H_\infty = V(X_0)$ at the point $(0 : -b : a)$, which equals $(0 : 1 : -a/b)$ when $b \neq 0$. Note that $-a/b$ is the slope of the line $1 + aX_1 + bX_2 = 0$, 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.

We can also identify $\mathbb{A}^n$ with U_n, as in Example 6.1. Note that in this case 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 $U_i \subset \mathbb{P}^n$ defined by the homeomorphism $u_i \colon U_i \to \mathbb{A}^n$.

LEMMA 6.8. *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 $k(X_0, X_1, \ldots, X_n)$.

Recall that

$$U_0 = \{(a_0 : a_1 : \ldots : a_n) \mid a_0 \neq 0\}; \; (a_0 : a_1 : \ldots : a_n) \leftrightarrow (\tfrac{a_1}{a_0}, \tfrac{a_2}{a_0}, \ldots, \tfrac{a_n}{a_0}) \in \mathbb{A}^n.$$

Let $k[\frac{X_1}{X_0}, \frac{X_2}{X_0}, \ldots, \frac{X_n}{X_0}]$ be the subring of $k(X_0, X_1, \ldots, X_n)$ generated by the quotients $\frac{X_i}{X_0}$ — it is the polynomial ring in the n symbols $\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}$. An element $f(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}) \in k[\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}]$ defines a map

$$(a_0 : a_1 : \ldots : a_n) \mapsto f(\tfrac{a_1}{a_0}, \ldots, \tfrac{a_n}{a_0}) \colon U_0 \to k,$$

and in this way $k[\frac{X_1}{X_0}, \frac{X_2}{X_0}, \ldots, \frac{X_n}{X_0}]$ becomes identified with the ring of regular functions on U_0, and U_0 with $\operatorname{Spm}\left(k[\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}]\right)$.

Next consider the open subset of U_0,

$$U_{01} = \{(a_0 : \ldots : a_n) \mid a_0 \neq 0, a_1 \neq 0\}.$$

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 $k[\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}] \hookrightarrow k[\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}, \frac{X_0}{X_1}]$. An element $f(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}, \frac{X_0}{X_1})$ of $k[\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}, \frac{X_0}{X_1}]$ defines the function $(a_0 : \ldots : a_n) \mapsto f(\frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}, \frac{a_0}{a_1})$ on U_{01}.

Similarly,

$$U_1 = \{(a_0 : a_1 : \ldots : a_n) \mid a_1 \neq 0\}; (a_0 : a_1 : \ldots : a_n) \leftrightarrow (\tfrac{a_0}{a_1}, \ldots, \tfrac{a_n}{a_1}) \in \mathbb{A}^n,$$

and we identify U_1 with $\operatorname{Spm}\left(k[\frac{X_0}{X_1}, \frac{X_2}{X_0}, \ldots, \frac{X_n}{X_1}]\right)$. A polynomial $f(\frac{X_0}{X_1}, \ldots, \frac{X_n}{X_1})$ in $k[\frac{X_0}{X_1}, \ldots, \frac{X_n}{X_1}]$ defines the map $(a_0 : \ldots : a_n) \mapsto f(\frac{a_0}{a_1}, \ldots, \frac{a_n}{a_1})\colon U_1 \to k$.

When regarded as an open subset of U_1, $U_{01} = D(\frac{X_0}{X_1})$, 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 $f(\frac{X_0}{X_1}, \ldots, \frac{X_n}{X_1}, \frac{X_1}{X_0})$ 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 subrings $k[\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}, \frac{X_0}{X_1}]$ and $k[\frac{X_0}{X_1}, \ldots, \frac{X_n}{X_1}, \frac{X_1}{X_0}]$ of $k(X_0, X_1, \ldots, X_n)$ are equal, 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 (3.8a). 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 $k[\frac{X_0}{X_1}, \frac{X_2}{X_1}, \ldots, \frac{X_n}{X_1}]$. □

PROPOSITION 6.9. *There is a unique structure of a (separated) algebraic variety on $\mathbb{P}^n$ for which each U_i is an open affine subvariety of $\mathbb{P}^n$ and each map u_i is an isomorphism of algebraic varieties.*

PROOF. Endow each U_i with the structure of an affine algebraic variety for which u_i is an isomorphism. Then $\mathbb{P}^n = \bigcup U_i$, and the lemma shows that this covering satisfies the patching condition (4.13), and so $\mathbb{P}^n$ has a unique structure of a ringed space for which $U_i \hookrightarrow \mathbb{P}^n$ is a homeomorphism onto an open subset of $\mathbb{P}^n$ and $\mathcal{O}_{\mathbb{P}^n}|U_i = \mathcal{O}_{U_i}$. Moreover, because each U_i is an algebraic variety, this structure makes $\mathbb{P}^n$ into an algebraic prevariety. Finally, the lemma shows that $\mathbb{P}^n$ satisfies the condition (4.27c) to be separated. □

EXAMPLE 6.10. Let C be the plane projective curve

$$C\colon Y^2Z = X^3$$

and assume $\operatorname{char}(k) \neq 2$. For each $a \in k^\times$, there is an automorphism

$$(x : y : z) \mapsto (ax : y : a^3 z)\colon C \xrightarrow{\varphi_a} C.$$

Patch two copies of $C \times \mathbb{A}^1$ together along $C \times (\mathbb{A}^1 - \{0\})$ by identifying (P, u) with $(\varphi_a(P), a^{-1})$, $P \in C$, $a \in \mathbb{A}^1 \smallsetminus \{0\}$. One obtains in this way a singular 2-dimensional variety that is not quasiprojective (see Hartshorne 1977, Exercise 7.13). It is even complete — see below — and so if it were quasiprojective, it would be projective. It is known that every irreducible separated curve is quasiprojective, 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 homogeneous coordinate ring of a subvariety of $\mathbb{P}^n$

Recall (page 41) 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 $k[U_0] = k[\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}]$. We regard this as a subring of $k(X_0, \ldots, X_n)$, and wish to identify the field of fractions of $k[U_0]$ as a subfield of $k(X_0, \ldots, X_n)$. Any nonzero $F \in k[U_0]$ can be written

$$F(\tfrac{X_1}{X_0}, \ldots, \tfrac{X_n}{X_0}) = \frac{F^*(X_0, \ldots, X_n)}{X_0^{\deg(F)}}$$

with F^* homogeneous of degree $\deg(F)$, and it follows that the field of fractions of $k[U_0]$ is

$$k(U_0) = \left\{ \frac{G(X_0, \ldots, X_n)}{H(X_0, \ldots, X_n)} \;\middle|\; G, H \text{ homogeneous of the same degree} \right\} \cup \{0\}.$$

Write $k(X_0, \ldots, X_n)_0$ for this field (the subscript 0 is short for "subfield of elements of degree 0"), so that $k(\mathbb{P}^n) = k(X_0, \ldots, X_n)_0$. Note that for $F = \frac{G}{H}$ in $k(X_0, \ldots, X_n)_0$,

$$(a_0 : \ldots : a_n) \mapsto \frac{G(a_0, \ldots, a_n)}{H(a_0, \ldots, a_n)} : D(H) \to k,$$

is a well-defined function, 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 $V = V(\mathfrak{p})$ with $\mathfrak{p}$ a homogeneous radical ideal in $k[X_0, \ldots, X_n]$, and we define the ***homogeneous coordinate ring*** of V (with its given embedding) to be

$$k_{\mathrm{hom}}[V] = k[X_0, \ldots, X_n]/\mathfrak{p}.$$

Note that $k_{\mathrm{hom}}[V]$ 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 $\mathbb{P}^n$, i.e., it is not intrinsic to V (see 6.19 below). We say that a nonzero $f \in k_{\mathrm{hom}}[V]$ is ***homogeneous of degree*** d if it can be represented by a homogeneous polynomial F of degree d in $k[X_0, \ldots, X_n]$ (we say that 0 is homogeneous of degree 0).

LEMMA 6.11. *Each element of $k_{\mathrm{hom}}[V]$ 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 $k_{\mathrm{hom}}[V]$ is an integral domain, we can form its field of fractions $k_{\mathrm{hom}}(V)$. Define

$$k_{\mathrm{hom}}(V)_0 = \left\{ \frac{g}{h} \in k_{\mathrm{hom}}(V) \;\middle|\; g \text{ and } h \text{ homogeneous of the same degree} \right\} \cup \{0\}.$$

PROPOSITION 6.12. *The field of rational functions on V is $k(V) \stackrel{\text{def}}{=} k_{\text{hom}}(V)_0$.*

PROOF. Consider $V_0 \stackrel{\text{def}}{=} U_0 \cap V$. As in the case of $\mathbb{P}^n$, we can identify $k[V_0]$ with a subring of $k_{\text{hom}}[V]$, and then the field of fractions of $k[V_0]$ becomes identified with $k_{\text{hom}}(V)_0$. □

Regular functions on a projective variety

Let V be an irreducible projective variety, and let $f \in k(V)$. By definition, we can write $f = \frac{g}{h}$ with g and h homogeneous of the same degree in $k_{\text{hom}}[V]$ and $h \neq 0$. For any $P = (a_0 : \ldots : a_n)$ with $h(P) \neq 0$,

$$f(P) =_{\text{df}} \frac{g(a_0, \ldots, a_n)}{h(a_0, \ldots, a_n)}$$

is well-defined: if $(a_0, \ldots, a_n)$ is replaced by $(ca_0, \ldots, ca_n)$, then both the numerator and denominator are multiplied by $c^{\deg(g)} = c^{\deg(h)}$.

We can write f in the form $\frac{g}{h}$ in many different ways,[3] but if

$$f = \frac{g}{h} = \frac{g'}{h'} \quad (\text{in } k(V)_0),$$

then

$$gh' - g'h \quad (\text{in } k_{\text{hom}}[V])$$

and so

$$g(a_0, \ldots, a_n) \cdot h'(a_0, \ldots, a_n) = g'(a_0, \ldots, a_n) \cdot h(a_0, \ldots, a_n).$$

Thus, of $h'(P) \neq 0$, the two representions give the same value for $f(P)$.

PROPOSITION 6.13. *For each $f \in k(V) =_{\text{df}} k_{\text{hom}}(V)_0$, 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 on an open subset of V arises from a unique element of $k(V)$.*

PROOF. From the above discussion, we see that f defines a regular function on $U = \bigcup D(h)$ where h runs over the denominators of expressions $f = \frac{g}{h}$ with g and h homogeneous of the same degree in $k_{\text{hom}}[V]$.

Conversely, let f be a regular function on an open subset U of V, and let $P \in U$. Then P lies in the open affine subvariety $V \cap U_i$ for some i, and so f coincides with the function defined by some $f_P \in k(V \cap U_i) = k(V)$ on an open neighbourhood of P. If f coincides with the function defined by $f_Q \in k(V)$ in a neighbourhood of a second point Q of U, then f_P and f_Q define the same function on some open affine U', and so $f_P = f_Q$ as elements of $k[U'] \subset k(V)$. This shows that f is the function defined by f_P on the whole of U. □

REMARK 6.14. (a) The elements of $k(V) = k_{\text{hom}}(V)_0$ should be regarded as the algebraic 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

[3] Unless $k_{\text{hom}}[V]$ is a unique factorization domain, there will be no preferred representation $f = \frac{g}{h}$.

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 (6.21) that, for any nonzero homogeneous $h \in k_{\mathrm{hom}}[V]$, $D(h)$ 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 6.15. *The map*

$$\pi\colon \mathbb{A}^{n+1} \smallsetminus \{\text{origin}\} \to \mathbb{P}^n,\ (a_0, \ldots, a_n) \mapsto (a_0 : \ldots : a_n)$$

is an open morphism of algebraic varieties. A map $\alpha\colon \mathbb{P}^n \to V$ 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

$$(a_0, \ldots, a_n) \mapsto (\tfrac{a_0}{a_i} : \ldots : \tfrac{a_n}{a_i})\colon k^{n+1} \smallsetminus V(X_i) \to U_i,$$

which is the regular map of affine varieties corresponding to the map of k-algebras

$$k\left[\tfrac{X_0}{X_i}, \ldots, \tfrac{X_n}{X_i}\right] \to k[X_0, \ldots, X_n][X_i^{-1}].$$

(In the first algebra $\frac{X_j}{X_i}$ is to be thought of as a single symbol.) It now follows from (4.4) that π is regular.

Let U be an open subset of $k^{n+1} \smallsetminus \{\text{origin}\}$, 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 $k^{n+1} \smallsetminus \{\text{origin}\}$, because $U' = \bigcup cU$, $c \in k^{\times}$, 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 (6.3) 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 6.16. Consider polynomials $F_0(X_0, \ldots, X_m), \ldots, F_n(X_0, \ldots, X_m)$ of the same degree. The map

$$(a_0 : \ldots : a_m) \mapsto (F_0(a_0, \ldots, a_m) : \ldots : F_n(a_0, \ldots, a_m))$$

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 $\bigcup D(F_i) = \mathbb{P}^n \smallsetminus V(F_1, \ldots, F_n)$. 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 6.17. *Let $V = V(\mathfrak{a}) \subset \mathbb{P}^m$ and $W = V(\mathfrak{b}) \subset \mathbb{P}^n$. A map $\varphi\colon V \to W$ is regular if and only if, for every $P \in V$, there exist polynomials*

$$F_0(X_0, \ldots, X_m), \ldots, F_n(X_0, \ldots, X_m),$$

homogeneous of the same degree, such that

$$\varphi\left((b_0 : \ldots : b_n)\right) = (F_0(b_0, \ldots, b_m) : \ldots : F_n(b_0, \ldots, b_m))$$

for all points $(b_0 : \ldots : b_m)$ in some neighbourhood of P in $V(\mathfrak{a})$.

PROOF. Straightforward. □

EXAMPLE 6.18. We prove that the circle $X^2 + Y^2 = Z^2$ is isomorphic to $\mathbb{P}^1$. This equation can be rewritten $(X + iY)(X - iY) = Z^2$, and so, after a change of variables, the equation of the circle becomes $C : XZ = Y^2$. Define

$$\varphi\colon \mathbb{P}^1 \to C,\ (a : b) \mapsto (a^2 : ab : b^2).$$

For the inverse, define

$$\psi\colon C \to \mathbb{P}^1 \quad \text{by} \begin{cases} (a : b : c) \mapsto (a : b) & \text{if } a \neq 0 \\ (a : b : c) \mapsto (b : c) & \text{if } b \neq 0 \end{cases}.$$

Note that,

$$a \neq 0 \neq b, \quad ac = b^2 \implies \frac{c}{b} = \frac{b}{a}$$

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 6.19. Let $L = \sum c_i X_i$ be a nonzero linear form in $n + 1$ variables. Then the map

$$(a_0 : \ldots : a_n) \mapsto \left(\frac{a_0}{L(\mathbf{a})}, \ldots, \frac{a_n}{L(\mathbf{a})}\right)$$

is a bijection of $D(L) \subset \mathbb{P}^n$ onto the hyperplane $L(X_0, X_1, \ldots, X_n) = 1$ 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 $k[\frac{X_0}{\sum c_i X_i}, \ldots, \frac{X_n}{\sum c_i X_i}]$. In this ring, each quotient $\frac{X_j}{\sum c_i X_i}$ is to be thought of as a single symbol, and $\sum c_j \frac{X_j}{\sum c_i X_i} = 1$; thus it is a polynomial ring in n symbols; any one symbol $\frac{X_j}{\sum c_i X_i}$ for which $c_j \neq 0$ can be omitted (see Lemma 5.12).

For a fixed $P = (a_0 : \ldots : a_n) \in \mathbb{P}^n$, the set of $\mathbf{c} = (c_0 : \ldots : c_n)$ such that

$$L_{\mathbf{c}}(P) \stackrel{\text{def}}{=} \sum c_i a_i \neq 0$$

is a nonempty open subset of $\mathbb{P}^n$ ($n > 0$). Therefore, for any finite set S of points of $\mathbb{P}^n$,

$$\{\mathbf{c} \in \mathbb{P}^n \mid S \subset D(L_{\mathbf{c}})\}$$

is a nonempty open subset of $\mathbb{P}^n$ (because $\mathbb{P}^n$ is irreducible). In particular, S is contained in an open affine subset $D(L_{\mathbf{c}})$ of $\mathbb{P}^n$. Moreover, if $S \subset V$ where V is a closed subvariety of $\mathbb{P}^n$, then $S \subset V \cap D(L_{\mathbf{c}})$: any finite set of points of a projective variety is contained in an open affine subvariety.

EXAMPLE 6.20. (The Veronese map.) 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[4]. 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

$$v\colon \mathbb{P}^n \to \mathbb{P}^{\nu_{n,m}},\ (a_0 : \ldots : a_n) \mapsto (\ldots : b_{i_0 \ldots i_n} : \ldots), \quad b_{i_0 \ldots i_n} = a_0^{i_0} \ldots a_n^{i_n}.$$

In other words, the Veronese mapping sends an $n+1$-tuple $(a_0 : \ldots : a_n)$ to the set of monomials in the a_i of degree m. 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

$$(b_{2,0} : b_{1,1} : b_{0,2}) \mapsto \begin{cases} (b_{2,0} : b_{1,1}) \text{ if } b_{2,0} \neq 1 \\ (b_{1,1} : b_{0,2}) \text{ if } b_{0,2} \neq 0. \end{cases}$$

is an inverse $\nu(\mathbb{P}^1) \to \mathbb{P}^1$. (Cf. Example 6.19.) [5]

[4]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 the induction.

[5]Note that, although $\mathbb{P}^1$ and $\nu(\mathbb{P}^1)$ are isomorphic, their homogeneous coordinate rings are not. In fact $k_{\text{hom}}[\mathbb{P}^1] = k[X_0, X_1]$, which is the affine coordinate ring of the smooth variety $\mathbb{A}^2$, whereas $k_{\text{hom}}[\nu(\mathbb{P}^1)] = k[X_0, X_1, X_2]/(X_0 X_2 - X_1^2)$ which is the affine coordinate ring of the singular variety $X_0 X_2 - X_1^2$.

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 $\nu\colon \mathbb{P}^n \to \nu(\mathbb{P}^n)$.

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 chapter 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 $\nu(\mathbb{P}^n) \subset \bigcup V_i$.

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 6.21. 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

$$\sum a_{i_0 \ldots i_n} X_{i_0 \ldots i_n}.$$

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 (6.14b).

EXAMPLE 6.22. 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. We sketch a proof that it is surjective.[6] Consider a hypersurface

$$H\colon F(X_0, \ldots, X_n) = 0$$

in $\mathbb{P}^n$ and a line

$$L = \{(ta_0 : \ldots : ta_n) \mid t \in k\}$$

in $\mathbb{P}^n$. The points of $H \cap L$ are given by the solutions of

$$F(ta_0, \ldots, ta_n) = 0,$$

which is a polynomial of degree $\leq \deg(F)$ in t unless $L \subset H$. Therefore, $H \cap L$ contains $\leq \deg(F)$ points, and it is not hard to show that for a fixed H and most L it will contain exactly $\deg(F)$ points. Thus, the hyperplanes are exactly the closed subvarieties H of $\mathbb{P}^n$ such that

(a) $\dim(H) = n - 1$,
(b) $\#(H \cap L) = 1$ for all lines L not contained in H.

These are geometric conditions, and so any automorphism of $\mathbb{P}^n$ must map hyperplanes to hyperplanes. But on an open subset of $\mathbb{P}^n$, such an automorphism takes the form

$$(b_0 : \ldots : b_n) \mapsto (F_0(b_0, \ldots, b_n) : \ldots : F_n(b_0, \ldots, b_n))$$

where the F_i are homogeneous of the same degree d (see 6.17). Such a map will take hyperplanes to hyperplanes if only if $d = 1$.

[6] This is related to the fundamental theorem of projective geometry — see E. Artin, Geometric Algebra, Interscience, 1957, Theorem 2.26.

EXAMPLE 6.23. (The Segre map.) This is the mapping

$$((a_0 : \ldots : a_m), (b_0 : \ldots : b_n)) \mapsto ((\ldots : a_i b_j : \ldots)) \colon \mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^{mn+m+n}.$$

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 interpret the tuples on the left as being the coefficients of two linear forms $L_1 = \sum a_i X_i$ and $L_2 = \sum b_j Y_j$, then the image of the pair is the set of coefficients of the homogeneous form of degree 2, $L_1 L_2$. From this observation, it is obvious that the map is defined on the whole of $\mathbb{P}^m \times \mathbb{P}^n$ ($L_1 \neq 0 \neq L_2 \Rightarrow L_1 L_2 \neq 0$) 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 1994, I 5.1. For example, the map

$$((a_0 : a_1), (b_0 : b_1)) \mapsto (a_0 b_0 : a_0 b_1 : a_1 b_0 : a_1 b_1) \colon \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$$

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

$$F(X_0, \ldots, X_m; Y_0, \ldots, Y_n) = 0$$

with F separately homogeneous in the X's and in the Y's.

EXAMPLE 6.24. Let $L_1, \ldots, L_{n-d}$ 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 $\pi \colon \mathbb{P}^n - E \to \mathbb{P}^{n-d-1}$ by $\pi(a) = (L_1(a) : \ldots : L_{n-d}(a))$; 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 $F_1, \ldots, F_r$ are homogeneous forms of the same degree, and $Z = V(F_1, \ldots, F_r)$, then $a \mapsto (F_1(a) : \ldots : F_r(a))$ is a morphism $\mathbb{P}^n - Z \to \mathbb{P}^{r-1}$.

By carefully choosing the centre E, it is possible to linearly 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.[7] For example, suppose we have

[7] 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 $\mathbb{P}^2$.

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 P_0 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 6.25. *Every finite set S of points of a quasiprojective variety V is contained in an open affine subset of V.*

PROOF. Regard V as a subvariety of $\mathbb{P}^n$, let $\bar{V}$ be the closure of V in $\mathbb{P}^n$, and let $Z = \bar{V} \smallsetminus V$. Because $S \cap Z = \emptyset$, for each $P \in S$ there exists a homogeneous polynomial $F_P \in I(Z)$ such that $F_P(P) \neq 0$. We may suppose that the F_P's have the same degree. An elementary argument shows that some linear combination F of the F_P, $P \in S$, is nonzero at each P. Then F is zero on Z, and so $\bar{V} \cap D(F)$ is an open affine of V, but F is nonzero at each P, and so $\bar{V} \cap D(F)$ contains S. □

Projective space without coordinates

Let E be a vector space over k of dimension n. 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 (because the bijections defined by two different bases differ by an automorphism of $\mathbb{P}^n$). Note that in contrast to $\mathbb{P}^n$, which has $n+1$ distinguished hyperplanes, namely, $X_0 = 0, \ldots, X_n = 0$, no hyperplane in $\mathbb{P}(E)$ is distinguished.

Grassmann varieties

Let E be a vector space over k of dimension n, and let $G_d(E)$ be the set of d-dimensional subspaces of E. When $d = 0$ or n, $G_d(E)$ has a single element, and so from now on we assume that $0 < d < n$. Fix a basis for E, and let $S \in G_d(E)$. The choice of a basis for S then determines a $d \times n$ matrix $A(S)$ whose rows are the coordinates of the basis elements. Changing the basis for S multiplies $A(S)$ on the left by an invertible $d \times d$ matrix. Thus, the family of $d \times d$ minors of $A(S)$ is determined up to multiplication by a nonzero constant, and so defines a point $P(S)$ in $\mathbb{P}^{\binom{n}{d}-1}$.

PROPOSITION 6.26. *The map $S \mapsto P(S)\colon G_d(E) \to \mathbb{P}^{\binom{n}{d}-1}$ is injective, with image a closed subset of $\mathbb{P}^{\binom{n}{d}-1}$.*

We give the proof below. The maps P defined by different bases of E differ by an automorphism of $\mathbb{P}^{\binom{n}{d}-1}$, and so the statement is independent of the choice of the basis — later (6.31) we shall give a "coordinate-free description" of the map. The map realizes $G_d(E)$ as a projective algebraic variety called the ***Grassmann variety*** of d-dimensional subspaces of E.

EXAMPLE 6.27. The affine cone over a line in $\mathbb{P}^3$ is a two-dimensional subspace of k^4. Thus, $G_2(k^4)$ can be identified with the set of lines in $\mathbb{P}^3$. 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

$$P(L) = (p_{01} : p_{02} : p_{03} : p_{12} : p_{13} : p_{23}) \in \mathbb{P}^5, \quad p_{ij} \stackrel{\text{def}}{=} \begin{vmatrix} x_i & x_j \\ y_i & y_j \end{vmatrix},$$

depends only on L. The map $L \mapsto P(L)$ is a bijection from $G_2(k^4)$ onto the quadric

$$\Pi : X_{01}X_{23} - X_{02}X_{13} + X_{03}X_{12} = 0$$

in $\mathbb{P}^5$. For a direct elementary proof of this, see (10.20, 10.21) below.

REMARK 6.28. Let S' be a subspace of E of complementary dimension $n-d$, and let $G_d(E)_{S'}$ be the set of $S \in G_d(V)$ such that $S \cap S' = \{0\}$. Fix an $S_0 \in G_d(E)_{S'}$, so that $E = S_0 \oplus S'$. For any $S \in G_d(V)_{S'}$, the projection $S \to S_0$ given by this decomposition is an isomorphism, and so S is the graph of a homomorphism $S_0 \to S'$:

$$s \mapsto s' \iff (s, s') \in S.$$

Conversely, the graph of any homomorphism $S_0 \to S'$ lies in $G_d(V)_{S'}$. Thus,

$$G_d(V)_{S'} \approx \mathrm{Hom}(S_0, S') \approx \mathrm{Hom}(E/S', S'). \tag{14}$$

The isomorphism $G_d(V)_{S'} \approx \mathrm{Hom}(E/S', S')$ depends on the choice of S_0 — it is the element of $G_d(V)_{S'}$ corresponding to $0 \in \mathrm{Hom}(E/S', S')$. The decomposition $E = S_0 \oplus S'$ gives a decomposition $\mathrm{End}(E) = \left(\begin{smallmatrix} \mathrm{End}(S_0) & \mathrm{Hom}(S',S_0) \\ \mathrm{Hom}(S_0,S') & \mathrm{End}(S') \end{smallmatrix}\right)$, and the bijections (14) show that the group $\left(\begin{smallmatrix} 1 & 0 \\ \mathrm{Hom}(S_0,S') & 1 \end{smallmatrix}\right)$ acts simply transitively on $G_d(E)_{S'}$.

REMARK 6.29. The bijection (14) identifies $G_d(E)_{S'}$ with the affine variety $\mathbb{A}(\mathrm{Hom}(S_0, S'))$ defined by the vector space $\mathrm{Hom}(S_0, S')$ (cf. p57). Therefore, the tangent space to $G_d(E)$ at S_0,

$$T_{S_0}(G_d(E)) \simeq \mathrm{Hom}(S_0, S') \simeq \mathrm{Hom}(S_0, E/S_0). \tag{15}$$

Since the dimension of this space doesn't depend on the choice of S_0, this shows that $G_d(E)$ is nonsingular (5.19).

REMARK 6.30. Let B be the set of all bases of E. The choice of a basis for E identifies B with GL_n, which is the principal open subset of $\mathbb{A}^{n^2}$ where $\det \neq 0$. In particular, B has a natural structure as an irreducible algebraic variety. The map $(e_1, \ldots, e_n) \mapsto \langle e_1, \ldots, e_d \rangle : B \to G_d(E)$ is a surjective regular map, and so $G_d(E)$ is also irreducible.

REMARK 6.31. The exterior algebra $\bigwedge E = \bigoplus_{d \geq 0} \bigwedge^d E$ of E is the quotient of the tensor algebra by the ideal generated by all vectors $e \otimes e$, $e \in E$. The elements of $\bigwedge^d E$ are called ***(exterior)*** d***-vectors***.The exterior algebra of E is a finite-dimensional graded algebra over k with $\bigwedge^0 E = k$, $\bigwedge^1 E = E$; if $e_1, \ldots, e_n$ form an ordered basis for V, then the $\binom{n}{d}$ wedge products $e_{i_1} \wedge \ldots \wedge e_{i_d}$ $(i_1 < \cdots < i_d)$ form an ordered basis for $\bigwedge^d E$. In particular, $\bigwedge^n E$ has dimension 1. For a subspace S of E of dimension d, $\bigwedge^d S$ is the one-dimensional subspace of $\bigwedge^d E$ spanned by $e_1 \wedge \ldots \wedge e_d$ for any basis $e_1, \ldots, e_d$ of S. Thus, there is a well-defined map

$$S \mapsto \bigwedge^d S\colon G_d(E) \to \mathbb{P}(\bigwedge^d E) \tag{16}$$

which the choice of a basis for E identifies with $S \mapsto P(S)$. Note that the subspace spanned by $e_1, \ldots, e_n$ can be recovered from the line through $e_1 \wedge \ldots \wedge e_d$ as the space of vectors v such that $v \wedge e_1 \wedge \ldots \wedge e_d = 0$ (cf. 6.32 below).

First proof of Proposition 6.26. Fix a basis $e_1, \ldots, e_n$ of E, and let $S_0 = \langle e_1, \ldots, e_d \rangle$ and $S' = \langle e_{d+1}, \ldots, e_n \rangle$. Order the coordinates in $\mathbb{P}^{\binom{n}{d}-1}$ so that

$$P(S) = (a_0\colon \ldots : a_{ij}\colon \ldots \colon \ldots)$$

where a_0 is the left-most $d \times d$ minor of $A(S)$, and a_{ij}, $1 \leq i \leq d$, $d < j \leq n$, is the minor obtained from the left-most $d \times d$ minor by replacing the i^{th} column with the j^{th} column. Let U_0 be the ("typical") standard open subset of $\mathbb{P}^{\binom{n}{d}-1}$ consisting of the points with nonzero zero$^{\text{th}}$ coordinate. Clearly,[8] $P(S) \in U_0$ if and only if $S \in G_d(E)_{S'}$. We shall prove the proposition by showing that $P\colon G_d(E)_{S'} \to U_0$ is injective with closed image.

For $S \in G_d(E)_{S'}$, the projection $S \to S_0$ is bijective. For each i, $1 \leq i \leq d$, let

$$e_i' = e_i + \textstyle\sum_{d<j\leq n} a_{ij} e_j \tag{17}$$

denote the unique element of S projecting to e_i. Then $e_1', \ldots, e_d'$ is a basis for S. Conversely, for any $(a_{ij}) \in k^{d(n-d)}$, the e_i''s defined by (17) span an $S \in G_d(E)_{S'}$ and project to the e_i's. Therefore, $S \leftrightarrow (a_{ij})$ gives a one-to-one correspondence $G_d(E)_{S'} \leftrightarrow k^{d(n-d)}$ (this is a restatement of (14) in terms of matrices).

Now, if $S \leftrightarrow (a_{ij})$, then

$$P(S) = (1 : \ldots : a_{ij}\colon \ldots \colon \ldots : f_k(a_{ij})\colon \ldots)$$

where $f_k(a_{ij})$ is a polynomial in the a_{ij} whose coefficients are independent of S. Thus, $P(S)$ determines (a_{ij}) and hence also S. Moreover, the image of $P\colon G_d(E)_{S'} \to U_0$ is the graph of the regular map

$$(\ldots, a_{ij}, \ldots) \mapsto (\ldots, f_k(a_{ij}), \ldots)\colon \mathbb{A}^{d(n-d)} \to \mathbb{A}^{\binom{n}{d}-d(n-d)-1},$$

which is closed (4.26).

Second proof of Proposition 6.26. An exterior d-vector v is said to be ***pure*** (or ***decomposable***) if there exist vectors $e_1, \ldots, e_d \in V$ such that $v = e_1 \wedge \ldots \wedge e_d$. According to (6.31), the image of $G_d(E)$ in $\mathbb{P}(\bigwedge^d E)$ consists of the lines through the pure d-vectors.

[8] If $e \in S' \cap S$ is nonzero, we may choose it to be part of the basis for S, and then the left-most $d \times d$ submatrix of $A(S)$ has a row of zeros. Conversely, if the left-most $d \times d$ submatrix is singular, we can change the basis for S so that it has a row of zeros; then the basis element corresponding to the zero row lies in $S' \cap S$.

LEMMA 6.32. *Let w be a nonzero d-vector and let*

$$M(w) = \{v \in E \mid v \wedge w = 0\};$$

then $\dim_k M(w) \leq d$, *with equality if and only if w is pure.*

PROOF. Let $e_1, \ldots, e_m$ be a basis of $M(w)$, and extend it to a basis $e_1, \ldots, e_m, \ldots, e_n$ of V. Write

$$w = \sum_{1 \leq i_1 < \ldots < i_d} a_{i_1 \ldots i_d} e_{i_1} \wedge \ldots \wedge e_{i_d}, \quad a_{i_1 \ldots i_d} \in k.$$

If there is a nonzero term in this sum in which e_j does not occur, then $e_j \wedge w \neq 0$. Therefore, each nonzero term in the sum is of the form $ae_1 \wedge \ldots \wedge e_m \wedge \ldots$. It follows that $m \leq d$, and $m = d$ if and only if $w = ae_1 \wedge \ldots \wedge e_d$ with $a \neq 0$. □

For a nonzero d-vector w, let $[w]$ denote the line through w. The lemma shows that $[w] \in G_d(E)$ if and only if the linear map $v \mapsto v \wedge w \colon E \mapsto \bigwedge^{d+1} E$ has rank $\leq n - d$ (in which case the rank is $n - d$). Thus $G_d(E)$ is defined by the vanishing of the minors of order $n - d + 1$ of this map. [9]

Flag varieties

The discussion in the last subsection extends easily to chains of subspaces. Let $\mathbf{d} = (d_1, \ldots, d_r)$ be a sequence of integers with $0 < d_1 < \cdots < d_r < n$, and let $G_{\mathbf{d}}(E)$ be the set of flags

$$F: \quad E \supset E^1 \supset \cdots \supset E^r \supset 0 \tag{18}$$

with E^i a subspace of E of dimension d_i. The map

$$G_{\mathbf{d}}(E) \xrightarrow{F \mapsto (V^i)} \textstyle\prod_i G_{d_i}(E) \subset \prod_i \mathbb{P}(\bigwedge^{d_i} E)$$

realizes $G_{\mathbf{d}}(E)$ as a closed subset[10] $\prod_i G_{d_i}(E)$, and so it is a projective variety, called a ***flag variety***. The tangent space to $G_{\mathbf{d}}(E)$ at the flag F consists of the families of homomorphisms

$$\varphi^i \colon E^i \to V/E^i, \quad 1 \leq i \leq r, \tag{19}$$

[9] In more detail, the map

$$w \mapsto (v \mapsto v \wedge w) \colon \bigwedge^d E \to \operatorname{Hom}_k(E, \bigwedge^{d+1} E)$$

is injective and linear, and so defines an injective regular map

$$\mathbb{P}(\bigwedge^d E) \hookrightarrow \mathbb{P}(\operatorname{Hom}_k(E, \bigwedge^{d+1} E)).$$

The condition rank $\leq n-d$ defines a closed subset W of $\mathbb{P}(\operatorname{Hom}_k(E, \bigwedge^{d+1} E))$ (once a basis has been chosen for E, the condition becomes the vanishing of the minors of order $n - d + 1$ of a linear map $E \to \bigwedge^{d+1} E$), and

$$G_d(E) = \mathbb{P}(\bigwedge^d E) \cap W.$$

[10] For example, if u_i is a pure d_i-vector and u_{i+1} is a pure d_{i+1}-vector, then it follows from (6.32) that $M(u_i) \subset M(u_{i+1})$ if and only if the map

$$v \mapsto (v \wedge u_i, v \wedge u_{i+1}) \colon V \to \bigwedge^{d_i+1} V \oplus \bigwedge^{d_{i+1}+1} V$$

has rank $\leq n - d_i$ (in which case it has rank $n - d_i$). Thus, $G_{\mathbf{d}}(V)$ is defined by the vanishing of many minors.

that are compatible in the sense that

$$\varphi^i | E^{i+1} \equiv \varphi^{i+1} \bmod E^{i+1}.$$

ASIDE 6.33. A basis $e_1, \ldots, e_n$ for E is ***adapted to*** the flag F if it contains a basis $e_1, \ldots, e_{j_i}$ for each E^i. Clearly, every flag admits such a basis, and the basis then determines the flag. As in (6.30), this implies that $G_{\mathbf{d}}(E)$ is irreducible. Because $\mathrm{GL}(E)$ acts transitively on the set of bases for E, it acts transitively on $G_{\mathbf{d}}(E)$. For a flag F, the subgroup $P(F)$ stabilizing F is an algebraic subgroup of $\mathrm{GL}(E)$, and the map

$$g \mapsto gF_0 \colon \mathrm{GL}(E)/P(F_0) \to G_{\mathbf{d}}(E)$$

is an isomorphism of algebraic varieties. Because $G_{\mathbf{d}}(E)$ is projective, this shows that $P(F_0)$ is a parabolic subgroup of $\mathrm{GL}(V)$.

Bezout's theorem

Let V be a hypersurface in $\mathbb{P}^n$ (that is, a closed subvariety of dimension $n-1$). For such a variety, $I(V) = (F(X_0, \ldots, X_n))$ 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 6.34. *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 (2.26) 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 $\alpha_1, \ldots, \alpha_{mn}$ 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 (7.12) 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 6.35. 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 $\mathrm{rad}(f,g) = \mathfrak{m}$, 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 motivated much of the most interesting work in commutative algebra in the second half of the twentieth century.

Hilbert polynomials (sketch)

Recall that for a projective variety $V \subset \mathbb{P}^n$,

$$k_{\mathrm{hom}}[V] = k[X_0,\ldots,X_n]/\mathfrak{b} = k[x_0,\ldots,x_n],$$

where $\mathfrak{b} = I(V)$. We observed that $\mathfrak{b}$ is homogeneous, and therefore $k_{\mathrm{hom}}[V]$ is a graded ring:

$$k_{\mathrm{hom}}[V] = \bigoplus\nolimits_{m\geq 0} k_{\mathrm{hom}}[V]_m,$$

where $k_{\mathrm{hom}}[V]_m$ is the subspace generated by the monomials in the x_i of degree m. Clearly $k_{\mathrm{hom}}[V]_m$ is a finite-dimensional k-vector space.

THEOREM 6.36. *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 6.37. For $V = \mathbb{P}^n$, $k_{\mathrm{hom}}[V] = k[X_0,\ldots,X_n]$, and (see the footnote on page 114), $\dim k_{\mathrm{hom}}[V]_m = \binom{m+n}{n} = \frac{(m+n)\cdots(m+1)}{n!}$, 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 6.38. *Let V be a projective variety of dimension d and degree δ; then*

$$P(V,T) = \frac{\delta}{d!}T^d + \text{terms of lower degree.}$$

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 6.39. Let V be the image of the Veronese map

$$(a_0 : a_1) \mapsto (a_0^d : a_0^{d-1}a_1 : \ldots : a_1^d) \colon \mathbb{P}^1 \to \mathbb{P}^d.$$

Then $k_{\mathrm{hom}}[V]_m$ 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.

Exercises

6-1. Show that a point P on a projective curve $F(X,Y,Z) = 0$ is singular if and only if $\partial F/\partial X$, $\partial F/\partial Y$, and $\partial F/\partial Z$ are all zero at P. If P is nonsingular, show that the tangent line at P has the (homogeneous) equation

$$(\partial F/\partial X)_P X + (\partial F/\partial Y)_P Y + (\partial F/\partial Z)_P Z = 0.$$

Verify that $Y^2 Z = X^3 + aXZ^2 + bZ^3$ is nonsingular if $X^3 + aX + b$ has no repeated root, and find the tangent line at the point at infinity on the curve.

6-2. Let L be a line in $\mathbb{P}^2$ and let C be a nonsingular conic in $\mathbb{P}^2$ (i.e., a curve in $\mathbb{P}^2$ defined by a homogeneous polynomial of degree 2). Show that either

(a) L intersects C in exactly 2 points, or
(b) L intersects C in exactly 1 point, and it is the tangent at that point.

6-3. Let $V = V(Y - X^2, Z - X^3) \subset \mathbb{A}^3$. Prove

(a) $I(V) = (Y - X^2, Z - X^3)$,
(b) $ZW - XY \in I(V)^* \subset k[W,X,Y,Z]$, but $ZW - XY \notin ((Y - X^2)^*, (Z - X^3)^*)$. (Thus, if $F_1, \ldots, F_r$ generate $\mathfrak{a}$, it does not follow that $F_1^*, \ldots, F_r^*$ generate $\mathfrak{a}^*$, even if $\mathfrak{a}^*$is radical.)

6-4. Let $P_0, \ldots, P_r$ be points in $\mathbb{P}^n$. Show that there is a hyperplane H in $\mathbb{P}^n$ passing through P_0 but *not* passing through any of $P_1, \ldots, P_r$.

6-5. Is the subset

$$\{(a : b : c) \mid a \neq 0, \quad b \neq 0\} \cup \{(1 : 0 : 0)\}$$

of $\mathbb{P}^2$ locally closed?

6-6. Show that the image of the Segre map $\mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^{mn+m+n}$ (see 6.23) is not contained in any hyperplane of $\mathbb{P}^{mn+m+n}$.

Chapter 7

Complete varieties

Throughout this chapter, k is an algebraically closed field.

Definition and basic properties

Complete varieties are the analogues in the category of algebraic 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 compact if and only if, for all topological spaces W, the projection $q\colon V \times W \to W$ is closed, i.e., maps closed sets to closed sets (see Bourbaki, N., General Topology, I, 10.2, Corollary 1 to Theorem 1).

DEFINITION 7.1. 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 7.2. Consider the projection

$$(x, y) \mapsto y\colon \mathbb{A}^1 \times \mathbb{A}^1 \to \mathbb{A}^1$$

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 7.3. *Let V be a complete variety.*

(a) *A closed subvariety of V is complete.*
(b) *If V' is complete, so also is $V \times V'$.*
(c) *For any morphism $\varphi\colon V \to W$, $\varphi(V)$ 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 $\varphi\colon V \to \mathbb{P}^1$ 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 $\Gamma_\varphi = \{(v, \varphi(v))\} \subset V \times W$ be the graph of φ. It is a closed subset of $V \times W$ (because W is a variety, see 4.26), and $\varphi(V)$ is the projection of Γ_φ into W. Since V is complete, the projection is closed, and so $\varphi(V)$ is closed, and hence is a subvariety of W (see p65). Consider

$$\Gamma_\varphi \times W \to \varphi(V) \times W \to W.$$

The variety Γ_φ, being isomorphic to V (see 4.26), is complete, and so the mapping $\Gamma_\varphi \times W \to W$ is closed. As $\Gamma_\varphi \to \varphi(V)$ is surjective, it follows that $\varphi(V) \times W \to W$ 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 $\varphi(V)$ is connected and closed, it must either be a single point (and φ is constant) or $\mathbb{P}^1$ (and φ is onto).

(e) A regular function on V is a regular map $f: V \to \mathbb{A}^1 \subset \mathbb{P}^1$, which (d) shows to be constant. □

COROLLARY 7.4. *A variety is complete if and only if its irreducible components are complete.*

PROOF. It follows from (a) that the irreducible components of a complete variety are complete. Conversely, let V be a variety whose irreducible components V_i are complete. If Z is closed in $V \times W$, then $Z_i =_{\mathrm{df}} Z \cap (V_i \times W)$ is closed in $V_i \times W$. Therefore, $q(Z_i)$ is closed in W, and so $q(Z) = \bigcup q(Z_i)$ is also closed. □

COROLLARY 7.5. *A regular map $\varphi: V \to W$ from a complete connected variety to an affine variety has image equal to a point. In particular, any complete connected affine variety is a point.*

PROOF. Embed W as a closed subvariety of $\mathbb{A}^n$, and write $\varphi = (\varphi_1, \ldots, \varphi_n)$ where φ_i is the composite of φ with the coordinate function $\mathbb{A}^n \to \mathbb{A}^1$. Then each φ_i is a regular function on V, and hence is constant. (Alternatively, apply the remark following 4.11.) This proves the first statement, and the second follows from the first applied to the identity map. □

REMARK 7.6. (a) 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 $\mathbb{A}^n \subset \mathbb{P}^n$.

(b) Here is another criterion: a variety V is complete if and only if every regular map $C \smallsetminus \{P\} \to V$ extends to a regular map $C \to V$; here P is a nonsingular point on a curve C. Intuitively, this says that Cauchy sequences have limits in V.

Projective varieties are complete

THEOREM 7.7. *A projective variety is complete.*

Before giving the proof, we shall need two lemmas.

LEMMA 7.8. *A variety V is complete if $q: V \times W \to W$ is a closed mapping for all irreducible affine varieties W (or even all affine spaces $\mathbb{A}^n$).*

PROOF. Write W as a finite union of open subvarieties $W = \bigcup W_i$. If Z is closed in $V \times W$, then $Z_i =_{\text{df}} Z \cap (V \times W_i)$ is closed in $V \times W_i$. Therefore, $q(Z_i)$ is closed in W_i for all i. As $q(Z_i) = q(Z) \cap W_i$, this shows that $q(Z)$ is closed. □

After (7.3a), it suffices to prove the Theorem for projective space $\mathbb{P}^n$ itself; thus we have to prove that the projection $\mathbb{P}^n \times W \to W$ is a closed mapping in the case that W is an irreducible affine variety. We shall need to understand the topology on $W \times \mathbb{P}^n$ in terms of ideals. Let $A = k[W]$, and let $B = A[X_0, \ldots, X_n]$. Note that $B = A \otimes_k k[X_0, \ldots, X_n]$, and so we can view it as the ring of regular functions on $W \times \mathbb{A}^{n+1}$: for $f \in A$ and $g \in k[X_0, \ldots, X_n]$, $f \otimes g$ is the function

$$(w, \mathbf{a}) \mapsto f(w) \cdot g(\mathbf{a}): W \times \mathbb{A}^{n+1} \to k.$$

The ring B has an obvious grading — a monomial $aX_0^{i_0} \ldots X_n^{i_n}$, $a \in A$, 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 7.9. *(a) 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.*

(b) The set $V(\mathfrak{b})$ is empty if and only if $\operatorname{rad}(\mathfrak{b}) \supset (X_0, \ldots, X_n)$.

(c) 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 this in (6.1) and (6.2), and similar arguments apply in the present more general situation. For example, to see that $V(\mathfrak{b})$ is closed, cover $\mathbb{P}^n$ with the standard open affines U_i and show that $V(\mathfrak{b}) \cap U_i$ is closed for all i.

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

$$\sum a_{i_0 \ldots i_n} X_0^{i_0} \ldots X_n^{i_n}, \quad a_{i_0 \ldots i_n} \in k[W],$$

is zero on $W \times \{\text{origin}\}$ if and only if its constant term is zero, and so

$$I^{\text{aff}}(W \times \{\text{origin}\}) = (X_0, X_1, \ldots, X_n).$$

Thus, the Nullstellensatz shows that $V(\mathfrak{b}) = \emptyset \Rightarrow \operatorname{rad}(\mathfrak{b}) = (X_0, \ldots, X_n)$. Conversely, if $X_i^N \in \mathfrak{b}$ for all i, then obviously $V(\mathfrak{b})$ is empty.

For (c), 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 $IV(\mathfrak{b})$ is prime. □

PROOF (OF 7.7). 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 homogeneous prime ideal in $B=A[X_0,\ldots,X_n]$.

If $p(Z)$ is contained in some closed subvariety W' of W, then Z is contained in $W'\times\mathbb{P}^n$, and we can 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 $V^{\mathrm{aff}}(\mathfrak{b})$ under the projection $W\times\mathbb{A}^{n+1}\to W$ is also dense in W, and so (see 3.22a) 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 $\mathfrak{m}B+\mathfrak{b}\supset(X_0,\ldots,X_n)^N$ for some N (by 7.9b), 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,

$$B_N\subset\mathfrak{m}B+\mathfrak{b}\implies B_N=\mathfrak{m}B_N+B_N\cap\mathfrak{b}.$$

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 $g=\sum m_ib_i$, $m_i\in\mathfrak{m}$, $b_i\in B$, then $g_N=\sum m_ib_{iN}$; 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 (1.3) 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. □

REMARK 7.10. In Example 6.19 above, we showed that every finite set of points in a projective variety is contained in an open affine subvariety. There is a partial converse to this statement: let V be a nonsingular complete 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.[1])

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[2] 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.

[1] Kleiman, Steven L., Toward a numerical theory of ampleness. Ann. of Math. (2) 84 1966 293–344.
See also,
Hartshorne, Robin, Ample subvarieties of algebraic varieties. Lecture Notes in Mathematics, Vol. 156 Springer, 1970, I §9 p45.

[2] Elimination theory became unfashionable several decades ago—one prominent algebraic geometer went so far as to announce that Theorem 7.7 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.

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

$$\begin{vmatrix} s_0 & s_1 & \ldots & s_m & & \\ & s_0 & \ldots & & s_m & \\ & & \ldots & & & \ldots \\ t_0 & t_1 & \ldots & t_n & & \\ & t_0 & \ldots & & t_n & \\ & & \ldots & & & \ldots \end{vmatrix} \begin{array}{l} n \text{ rows} \\ \\ \\ \\ \\ m \text{ rows} \end{array}$$

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 7.11. *The resultant* $\mathrm{Res}(P, Q) = 0$ *if and only if*

(a) *both s_0 and t_0 are zero; or*
(b) *the two polynomials have a common root.*

PROOF. If (a) holds, then $\mathrm{Res}(P, Q) = 0$ because the first column is zero. 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

$$P(X) = (X-\alpha)P_1(X), \qquad Q(X) = (X-\alpha)Q_1(X).$$

Using these equalities, we find that

$$P(X)Q_1(X) - Q(X)P_1(X) = 0. \tag{20}$$

On equating the coefficients of $X^{m+n-1}, \ldots, X, 1$ in (20) 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

$$\begin{pmatrix} s_0 & s_1 & \ldots & s_m & & \\ & s_0 & \ldots & & s_m & \\ & & \ldots & & & \ldots \\ t_0 & t_1 & \ldots & t_n & & \\ & t_0 & \ldots & & t_n & \\ & & \ldots & & & \ldots \end{pmatrix}$$

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 (20). A root α of P must be also be a root of P_1 or of Q. If the former, cancel $X-\alpha$ from the left hand side of (20), and consider a root β of $P_1/(X-\alpha)$. As $\deg P_1 < \deg P$, this argument eventually leads to 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 7.12. *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) $(1 : 0)$ in the case that $s_0 = 0$;
(b) $(a : 1)$ with a a root of $P(X, 1)$.

Since a similar statement is true for $Q(X, Y)$, (7.12) is a restatement of (7.11). □

Now regard the coefficients of P and Q as indeterminates. 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 $\mathrm{Res}(P, Q) = 0$. 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

$$P_i(T_1, \ldots, T_m; X_0, \ldots, X_n),$$

homogeneous in the X_i, elimination theory gives an algorithm for finding polynomials $R_j(T_1, \ldots, T_n)$ such that the $P_i(a_1, \ldots, a_m; X_0, \ldots, X_n)$ have a common zero if and only if $R_j(a_1, \ldots, a_n) = 0$ for all j. (Theorem 7.7 shows only 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 complete 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 $v \mapsto (v, w)\colon V \to V \times W$ (this map is regular because its components are).

THEOREM 7.13 (RIGIDITY THEOREM). *Let* $\varphi\colon V \times W \to Z$ *be a regular map, and assume that* V *is complete, that* V *and* W *are irreducible, and that* Z *is separated. If there exist points* $v_0 \in V$, $w_0 \in W$, $z_0 \in Z$ *such that*

$$\varphi(V \times \{w_0\}) = \{z_0\} = \varphi(\{v_0\} \times W),$$

then $\varphi(V \times W) = \{z_0\}$.

PROOF. Because V is complete, the projection map $q\colon V \times W \to W$ is closed. Therefore, for any open affine neighbourhood U of z_0,

$$T = q(\varphi^{-1}(Z \smallsetminus U))$$

is closed in W. Note that

$$W \smallsetminus T = \{w \in W \mid \varphi(V, w) \subset U\},$$

and so $w_0 \in W \smallsetminus T$. In particular, $W \smallsetminus T$ is nonempty, and so it is dense in W. As $V \times \{w\}$ is complete and U is affine, $\varphi(V \times \{w\})$ must be a point whenever $w \in W \smallsetminus T$: in fact,

$$\varphi(V, w) = \varphi(v_0, w) = \{z_0\}.$$

We have shown that φ takes the constant value z_0 on the dense subset $V \times (W - T)$ of $V \times W$, and therefore on the whole of $V \times W$. □

In more colloquial terms, the theorem says that if φ collapses a vertical and a horizontal slice to a point, then it collapses the whole of $V \times W$ to a point, which must therefore be "rigid".

An ***abelian variety*** is a complete connected group variety.

COROLLARY 7.14. *Every regular map $\alpha\colon A \to B$ of abelian varieties is the composite of a homomorphism with a translation; in particular, a regular map $\alpha\colon A \to B$ such that $\alpha(0) = 0$ is a homomorphism.*

PROOF. After composing α with a translation, we may suppose that $\alpha(0) = 0$. Consider the map

$$\varphi\colon A \times A \to B, \qquad \varphi(a, a') = \alpha(a + a') - \alpha(a) - \alpha(a').$$

Then $\varphi(A \times 0) = 0 = \varphi(0 \times A)$ and so $\varphi = 0$. This means that α is a homomorphism. □

COROLLARY 7.15. *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, $a \mapsto -a\colon A \to A$, takes the identity element to itself, the preceding corollary shows that it is a homomorphism. □

Theorems of Chow

THEOREM 7.16. *For every algebraic variety V, there exists a projective algebraic variety W and a regular map φ from an open dense subset U of W to V whose graph is closed in $V \times W$; the set $U = W$ if and only if V is complete.*

PROOF. To be added. □

See:

Chow, W-L., On the projective embedding of homogeneous varieties, Lefschetz's volume, Princeton 1956.

Serre, Jean-Pierre. Géométrie algébrique et géométrie analytique. Ann. Inst. Fourier, Grenoble 6 (1955–1956), 1–42 (p12).

THEOREM 7.17. *For any complete algebraic variety V, there exists a projective algebraic variety W and a surjective birational map $W \to V$.*

PROOF. To be added. (See Mumford 1999, p60.) □

Theorem 7.17 is usually known as Chow's Lemma.

Nagata's Embedding Theorem

A necessary condition for a prevariety to be an open subvariety of a complete variety is that it be separated. A theorem of Nagata says that this condition is also sufficient.

THEOREM 7.18. *For every variety V, there exists an open immersion $V \to W$ with W complete.*

PROOF. To be added. □

See:

Nagata, Masayoshi. Imbedding of an abstract variety in a complete variety. J. Math. Kyoto Univ. 2 1962 1–10.

Nagata, Masayoshi. A generalization of the imbedding problem of an abstract variety in a complete variety. J. Math. Kyoto Univ. 3 1963 89–102.

Lütkebohmert, W. On compactification of schemes. Manuscripta Math. 80 (1993), no. 1, 95–111.

Deligne, P., Le théorème de plongement de Nagata, personal notes.

Conrad, B., Deligne's notes on Nagata compactifications, 1997, 26pp, `http://www.math.lsa.umich.edu/~bdconrad/`.

Exercises

7-1. Identify the set of homogeneous polynomials $F(X,Y) = \sum a_{ij} X^i Y^j$, $0 \le i, j \le m$, with an affine space. Show that the subset of reducible polynomials is closed.

7-2. Let V and W be complete irreducible varieties, and let A be an abelian variety. Let P and Q be points of V and W. Show that any regular map $h\colon V \times W \to A$ such that $h(P,Q) = 0$ can be written $h = f \circ p + g \circ q$ where $f\colon V \to A$ and $g\colon W \to A$ are regular maps carrying P and Q to 0 and p and q are the projections $V \times W \to V, W$.

Chapter 8

Finite Maps

Throughout this chapter, k is an algebraically closed field.

Definition and basic properties

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. Recall also that a variety V is affine if and only if $\Gamma(V, \mathcal{O}_V)$ is an affine k-algebra and the canonical map $(V, \mathcal{O}_V) \to \mathrm{Spm}(\Gamma(V, \mathcal{O}_V))$ is an isomorphism (3.13).

DEFINITION 8.1. A regular map $\varphi\colon W \to V$ 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.

For example, suppose W and V are affine and $k[W]$ is a finite $k[V]$-algebra. Then φ is finite because, for any open affine U in V, $\varphi^{-1}(U)$ is affine with

$$k[\varphi^{-1}(U)] \simeq k[W] \otimes_{k[V]} k[U] \tag{21}$$

(see 4.29, 4.30); in particular, the canonical map

$$\varphi^{-1}(U) \to \mathrm{Spm}(\Gamma(\varphi^{-1}(U), \mathcal{O}_W) \tag{22}$$

is an isomorphism.

PROPOSITION 8.2. *It suffices to check the condition in the definition for all subsets in one open affine covering of V.*

Unfortunately, this is not as obvious as it looks. We first need a lemma.

LEMMA 8.3. *Let $\varphi\colon W \to V$ be a regular map with V affine, and let U be an open affine in V. There is a canonical isomorphism of k-algebras*

$$\Gamma(W, \mathcal{O}_W) \otimes_{k[V]} k[U] \to \Gamma(\varphi^{-1}(U), \mathcal{O}_W).$$

PROOF. Let $U' = \varphi^{-1}(U)$. The map is defined by the $k[V]$-bilinear pairing

$$(f, g) \mapsto (f|_{U'}, g \circ \varphi|_{U'})\colon \Gamma(W, \mathcal{O}_W) \times k[U] \to \Gamma(U', \mathcal{O}_W).$$

When W is also affine, it is the isomorphism (21).

Let $W = \bigcup W_i$ be a finite open affine covering of W, and consider the commutative diagram:

$$\begin{array}{ccccccc} 0 \to & \Gamma(W,\mathcal{O}_W)\otimes_{k[V]}k[U] & \to & \prod_i \Gamma(W_i,\mathcal{O}_W)\otimes_{k[V]}k[U] & \rightrightarrows & \prod_{i,j}\Gamma(W_{ij},\mathcal{O}_W)\otimes_{k[V]}k[U] \\ & \downarrow & & \downarrow & & \downarrow \\ 0 \to & \Gamma(U',\mathcal{O}_W) & \to & \prod_i \Gamma(U'\cap W_i,\mathcal{O}_W) & \rightrightarrows & \prod_{i,j}\Gamma(U\cap W_{ij},\mathcal{O}_W) \end{array}$$

Here $W_{ij} = W_i \cap W_j$. The bottom row is exact because $\mathcal{O}_W$ is a sheaf, and the top row is exact because $\mathcal{O}_W$ is a sheaf and $k[U]$ is flat over $k[V]$ (see Section 1)[1]. The varieties W_i and $W_i \cap W_j$ are all affine, and so the two vertical arrows at right are products of isomorphisms (21). This implies that the first is also an isomorphism. □

PROOF (OF THE PROPOSITION). Let V_i be an open affine covering of V (which we may suppose to be finite) such that $W_i =_{\text{def}} \varphi^{-1}(V_i)$ is an affine subvariety of W for all i and $k[W_i]$ is a finite $k[V_i]$-algebra. Let U be an open affine in V, and let $U' = \varphi^{-1}(U)$. Then $\Gamma(U',\mathcal{O}_W)$ is a subalgebra of $\prod_i \Gamma(U'\cap W_i,\mathcal{O}_W)$, and so it is an affine k-algebra finite over $k[U]$.[2] We have a morphism of varieties over V

$$\begin{tikzcd} U' \arrow[rr, "\text{can}"] \arrow[dr] & & \operatorname{Spm}(\Gamma(U',\mathcal{O}_W)) \arrow[dl] \\ & V & \end{tikzcd} \tag{23}$$

which we shall show to be an isomorphism. We know (see (22)) that each of the maps

$$U'\cap W_i \to \operatorname{Spm}(\Gamma(U'\cap W_i,\mathcal{O}_W))$$

is an isomorphism. But (8.2) shows that $\operatorname{Spm}(\Gamma(U'\cap W_i,\mathcal{O}_W))$ is the inverse image of V_i in $\operatorname{Spm}(\Gamma(U',\mathcal{O}_W))$. Therefore can is an isomorphism over each V_i, and so it is an isomorphism. □

PROPOSITION 8.4. (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.

[1] A sequence $0 \to M' \to M \to M''$ is exact if and only if $0 \to A_\mathfrak{m}\otimes_A M' \to A_\mathfrak{m}\otimes_A M \to A_\mathfrak{m}\otimes_A M''$ is exact for all maximal ideals $\mathfrak{m}$ of A. This implies the claim because $k[U]_{\mathfrak{m}_P} \simeq \mathcal{O}_{U,P} \simeq \mathcal{O}_{V,P} \simeq k[V]_{\mathfrak{m}_P}$ for all $P \in U$.

[2] Recall that a module over a noetherian ring is noetherian if and only if it is finitely generated, and that a submodule of a noetherian module is noetherian. Therefore, a submodule of a finitely generated module is finitely generated.

(b) If B is a finite A-algebra and C is a finite B-algebra, then C is a finite A-algebra. To see this, note that 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. To see this, note that 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 finitely generated $k[T]$-submodule of $k[T, T^{-1}]$ is contained in $T^{-n}k[T]$ for some n).

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 8.5. *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 $\mathfrak{m}_Q \supset \alpha(\mathfrak{m}_P)$, and so the points of W mapping to P are in one-to-one correspondence 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 8.6. *A finite k-algebra A has only finitely many maximal ideals.*

PROOF. Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ be maximal ideals in A. They are obviously coprime in pairs, and so the Chinese Remainder Theorem (1.1) shows that the map

$$A \to A/\mathfrak{m}_1 \times \cdots \times A/\mathfrak{m}_n, \qquad a \mapsto (\ldots, a_i \bmod \mathfrak{m}_i, \ldots),$$

is surjective. It follows that $\dim_k A \geq \sum \dim_k(A/\mathfrak{m}_i) \geq n$ (dimensions as k-vector spaces). □

THEOREM 8.7. *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 8.4a and b), and so we can replace W with Z; we then have to show that $\mathrm{Im}(\varphi)$ is closed. The map corresponds to a finite map of rings $A \to B$. This will factors as $A \to A/\mathfrak{a} \hookrightarrow B$, from which we obtain maps

$$\mathrm{Spm}(B) \to \mathrm{Spm}(A/\mathfrak{a}) \hookrightarrow \mathrm{Spm}(A).$$

The second map identifies $\mathrm{Spm}(A/\mathfrak{a})$ with the closed subvariety $V(\mathfrak{a})$ of $\mathrm{Spm}(A)$, and so it remains to show that the first map is surjective. This is a consequence of the next lemma. □

LEMMA 8.8 (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 1.30). 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. This follows from Lemma 8.9 below.

(b) The ring $B/\mathfrak{q}$ contains $A/\mathfrak{p}$, and it is integral over $A/\mathfrak{p}$. If $\mathfrak{q}$ is maximal, then Lemma 8.9 shows that $\mathfrak{p}$ is also. For the converse, note that any integral domain integral over a field is a field because it is a union of integral domains finite over the field, which are automatically fields (left multiplication by an element is injective, and hence surjective, being a linear map of a finite-dimensional vector space). □

LEMMA 8.9. *Let* A *be a subring of a field* K*. If* K *is integral over* A*, then* A *is also a field.*

PROOF. Let a be a nonzero element of A. Then $a^{-1} \in K$, and it is integral over A:

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

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 $a^{-1} \in A$. □

COROLLARY 8.10. *Let* $\varphi \colon W \to V$ *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 8.4c), 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 8.11. (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 (3.21).

(c) Let

$$V = V(X^n + T_1 X^{n-1} + \cdots + T_n) \subset \mathbb{A}^{n+1},$$

and consider the projection map

$$(a_1, \ldots, a_n, x) \mapsto (a_1, \ldots, a_n) \colon V \to \mathbb{A}^n.$$

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

$$(a_0,\ldots,a_n,x) \mapsto (a_1,\ldots,a_n)\colon V \xrightarrow{\varphi} \mathbb{A}^{n+1}$$

has finite fibres except for the fibre above $o = (0,\ldots,0)$, which is $\mathbb{A}^1$. The restriction $\varphi|V \smallsetminus \varphi^{-1}(o)$ 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

$$P(X,Y) = T_0X^n + T_1X^{n-1}Y + ... + T_nY^n,$$

and let V be its zero set in $\mathbb{P}^1\times(\mathbb{A}^{n+1}\smallsetminus\{o\})$. In this case, the projection map $V\to\mathbb{A}^{n+1}\smallsetminus\{o\}$ is finite. (Prove this directly, or apply 8.24 below.)

(f) The morphism $\mathbb{A}^1 \longrightarrow \mathbb{A}^2$, $t\mapsto(t^2,t^3)$ 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 $\mathbb{A}^1 \longrightarrow \mathbb{A}^1$, $a\mapsto a^m$ 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).

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 3.18c) 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 8.12. *For any irreducible affine algebraic variety V of a variety of dimension d, there is a finite surjective map $\varphi\colon V\to\mathbb{A}^d$.*

PROOF. This is a geometric re-statement of the following theorem. □

THEOREM 8.13 (NOETHER NORMALIZATION THEOREM). *Let A be a finitely generated k-algebra, and assume that A is an integral domain. Then there exist elements $y_1,\ldots,y_d\in A$ that are algebraically independent over k and such that A is integral over $k[y_1,\ldots,y_d]$.*

PROOF. Let $x_1, \ldots, x_n$ generate A as a k-algebra. We can renumber the x_i so that $x_1, \ldots, x_d$ are algebraically independent and $x_{d+1}, \ldots, x_n$ are algebraically dependent on $x_1, \ldots, x_d$ (FT, 8.12).

Because x_n is algebraically dependent on $x_1, \ldots, x_d$, there exists a nonzero polynomial $f(X_1, \ldots, X_d, T)$ such that $f(x_1, \ldots, x_d, x_n) = 0$. Write

$$f(X_1, \ldots, X_d, T) = a_0 T^m + a_1 T^{m-1} + \cdots + a_m$$

with $a_i \in k[X_1, \ldots, X_d]$ ($\approx k[x_1, \ldots, x_d]$). 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 $k[x_1, \ldots, x_d]$, that is, x_n will be integral (not merely algebraic) over $k[x_1, \ldots, x_d]$. The next lemma suggest how we might achieve this happy state by making a linear change of variables.

LEMMA 8.14. *If $F(X_1, \ldots, X_d, T)$ is a homogeneous polynomial of degree r, then*

$$F(X_1 + \lambda_1 T, \ldots, X_d + \lambda_d T, T) = F(\lambda_1, \ldots, \lambda_d, 1) T^r + \text{terms of degree} < r \text{ in } T.$$

PROOF. The polynomial $F(X_1 + \lambda_1 T, \ldots, X_d + \lambda_d T, T)$ is still homogeneous of degree r (in $X_1, \ldots, X_d, T$), 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 NORMALIZATION THEOREM (CONTINUED)). Note that unless $F(X_1, \ldots, X_d, T)$ is the zero polynomial, it will always be possible to choose $(\lambda_1, \ldots, \lambda_d)$ so that $F(\lambda_1, \ldots, \lambda_d, 1) \neq 0$ — 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 (Exercise 1-1).

Let F be the homogeneous part of highest degree of f, and choose $(\lambda_1, \ldots, \lambda_d)$ so that $F(\lambda_1, \ldots, \lambda_d, 1) \neq 0$. The lemma then shows that

$$f(X_1 + \lambda_1 T, \ldots, X_d + \lambda_d T, T) = c T^r + b_1 T^{r-1} + \cdots + b_0,$$

with $c = F(\lambda_1, \ldots, \lambda_d, 1) \in k^\times$, $b_i \in k[X_1, \ldots, X_d]$, $\deg b_i < r$. 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 $k[x_1 - \lambda_1 x_n, \ldots, x_d - \lambda_d x_n]$. Put $x_i' = x_i - \lambda_i x_n$, $1 \leq i \leq d$. Then x_n is integral over the ring $k[x_1', \ldots, x_d']$, and it follows that A is integral over $A' = k[x_1', \ldots, x_d', x_{d+1}, \ldots, x_{n-1}]$. Repeat the process for A', and continue until the theorem is proved. □

REMARK 8.15. 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 CA 5.11), but the above proof is simpler and 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 shows that, when W and V are separated, every quasi-finite map arises in this way.

THEOREM 8.16 (ZARISKI'S MAIN THEOREM). *Any quasi-finite map of varieties* $\varphi\colon W \to V$ *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 (140). □

REMARK 8.17. 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 $\varphi\colon W \to V$ 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 8.18. One may ask how a birational regular map $\varphi\colon W \to V$ 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 $\varphi\colon V' \to V$ 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 8.19. *Let* $\varphi\colon W \to V$ *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 $W' = V$. □

COROLLARY 8.20. *Any quasi-finite regular map* $\varphi\colon W \to V$ *with* W *complete is finite.*

PROOF. In this case, $\iota\colon W \hookrightarrow W'$ must be an isomorphism (7.3). □

REMARK 8.21. Let W and V be irreducible varieties, and let $\varphi\colon W \to V$ be a dominant 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 (a) and the preceding discussion, we find that φ is birational, and from (b) 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 $\varphi\colon W \to V$ satisfying the conditions (a) and (b) is an isomorphism.

NOTES. The full name of Theorem 8.16 is "the main theorem of Zariski's paper Transactions AMS, 53 (1943), 490-532". Zariski's original statement is that in (8.19). Grothendieck proved it in the stronger form (8.16) for all schemes. There is a good discussion of the theorem in Mumford 1999, III.9. For a proof see Musili, C., Algebraic geometry for beginners. Texts and Readings in Mathematics, 20. Hindustan Book Agency, New Delhi, 2001, §65.

The base change of a finite map

Recall that the base change of a regular map $\varphi\colon V \to S$ is the map φ' in the diagram:

$$\begin{array}{ccc} V \times_S W & \xrightarrow{\psi'} & V \\ \downarrow{\scriptstyle\varphi'} & & \downarrow{\scriptstyle\varphi} \\ W & \xrightarrow{\psi} & S. \end{array}$$

PROPOSITION 8.22. *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 $A \otimes_R B/\mathfrak{N}$ is a finite B-algebra, which is obvious. □

Proper maps

A regular map $\varphi\colon V \to S$ of varieties is said to be proper if it is "universally closed", that is, if for all maps $T \to S$, the base change $\varphi'\colon V \times_S T \to T$ 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 $\varphi\colon V \to S$ is proper, then $\varphi^{-1}(P)$ is a complete variety for all $P \in S$.

PROPOSITION 8.23. *If $W \to V$ is proper and V is complete, then W is complete.*

PROOF. Let T be a variety, and consider

$$\begin{array}{ccc}
W & \longleftarrow & W \times T \\
\downarrow & & \downarrow{\scriptstyle \text{closed}} \\
V & \longleftarrow & V \times T \\
\downarrow & & \downarrow{\scriptstyle \text{closed}} \\
\{\text{point}\} & \longleftarrow & T
\end{array}$$

As $W \times T \simeq W \times_V (V \times T)$ and $W \to V$ is proper, $W \times T \to V \times T$ is closed, and as V is complete, $V \times T \to T$ is closed. Therefore, $W \times T \to T$ is closed. □

PROPOSITION 8.24. *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 8.25. *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

$$W \xrightarrow{w \mapsto (w, \iota w)} W \times_V W' \xrightarrow{(w, w') \mapsto w'} W'.$$

The image of the first map is Γ_ι, which is closed because W' is a variety (see 4.26; 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

$$a \mapsto a^n \colon \mathbb{A}^1 \smallsetminus \{0\} \to \mathbb{A}^1,$$

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.

Exercises

8-1. Prove that a finite map is an isomorphism if and only if it is bijective and étale. (Cf. Harris 1992, 14.9.)

8-2. Give an example of a surjective quasi-finite regular map that is not finite (different from any in the notes).

8-3. Let $\varphi\colon V \to W$ be a regular map with the property that $\varphi^{-1}(U)$ is an open affine subset of W whenever U is an open affine subset of V. Show that if V is separated, then so also is W.

8-4. For every $n \geq 1$, find a finite map $\varphi\colon W \to V$ with the following property: for all $1 \leq i \leq n$,

$$V_i \stackrel{\text{def}}{=} \{P \in V \mid \varphi^{-1}(P) \text{ has } \leq i \text{ points}\}$$

is a closed subvariety of dimension i.

Chapter 9

Dimension Theory

Throughout this chapter, k is an algebraically closed field. 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.

Let W be a subvariety of a variety V. The ***codimension*** of W in V is

$$\operatorname{codim}_V W = \dim V - \dim W.$$

In §3 and §6 we proved the following results:

9.1. (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 2.24b, 5.12). 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 2.25 and 2.27)*[1].

(c) *If* V *is irreducible and* Z *is a proper closed subset of* V, *then* $\dim Z < \dim V$ *(see 2.26).*

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 9.2. *Let* V *be an irreducible affine variety, and let* f *a nonzero regular function. If* f *has a zero on* V, *then its zero set is pure of dimension* $\dim(V) - 1$.

[1] The careful reader will check that we didn't use 5.22 or 5.23 in the proof of 2.27.

In other words: let V be a closed subvariety of $\mathbb{A}^n$ and let $F \in k[X_1, \ldots, X_n]$; 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 pure 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

$$\operatorname{tr}\deg_k A/\mathfrak{p} = \operatorname{tr}\deg_k A - 1.$$

LEMMA 9.3. *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 $\mathrm{Nm}_{L/K}\alpha$. Hence, if A is integrally closed (e.g., if A is a unique factorization domain), then $\mathrm{Nm}_{L/K}\alpha \in A$. 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,

$$g(X) = X^r + a_{r-1}X^{r-1} + \cdots + a_0.$$

In some extension field E of L, $g(X)$ will split

$$g(X) = \textstyle\prod_{i=1}^r (X - \alpha_i), \quad \alpha_1 = \alpha, \quad \prod_{i=1}^r \alpha_i = \pm a_0.$$

Because α is integral over A, each α_i is integral over A (see the proof of 1.22), and it follows that $\mathrm{Nm}_{L/K}\,\alpha \overset{\text{FT 5.38}}{=} (\prod_{i=1}^r \alpha_i)^{[L:K(\alpha)]}$ is integral over A (see 1.16).

Now suppose A is integrally closed, so that $\mathrm{Nm}\,\alpha \in A$. 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 $\mathrm{Nm}\,\alpha = \pm a_0^{\frac{n}{r}}$. □

PROOF (OF THEOREM 9.2). We first show that it suffices to prove the theorem in the case that $V(f)$ is irreducible. Suppose $Z_0, \ldots, Z_n$ are the irreducible components of $V(f)$. There exists a point $P \in Z_0$ that does not lie on any other Z_i (otherwise the decomposition $V(f) = \bigcup Z_i$ would be redundant). As $Z_1, \ldots, Z_n$ 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 (8.13), there is a finite surjective map $\pi\colon V \to \mathbb{A}^d$, which realizes $k(V)$ as a finite extension of the field $k(\mathbb{A}^d)$. We shall show that $\mathfrak{p} \cap k[\mathbb{A}^d] = \mathrm{rad}(f_0)$ where $f_0 = \mathrm{Nm}_{k(V)/k(\mathbb{A}^d)}\, f$. Hence

$$k[\mathbb{A}^d]/\mathrm{rad}(f_0) \to k[V]/\mathfrak{p}$$

is injective. As it is also finite, this shows that $\dim V(f) = \dim V(f_0)$, and we already know the theorem for $\mathbb{A}^d$ (9.1b).

By assumption $k[V]$ is finite (hence integral) over its subring $k[\mathbb{A}^d]$. 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 $(f_0) \subset \mathfrak{p} \cap k[\mathbb{A}^d]$, which implies

$$\mathrm{rad}(f_0) \subset \mathfrak{p} \cap k[\mathbb{A}^d]$$

because $\mathfrak{p}$ is radical. For the reverse inclusion, let $g \in \mathfrak{p} \cap k[\mathbb{A}^d]$. 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 $k[\mathbb{A}^d] \hookrightarrow k[V]$ 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 (9.1b). □

COROLLARY 9.4. *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 Theorem 9.2 implies that $\dim Z = \dim V - 1$. □

COROLLARY 9.5 (TOPOLOGICAL CHARACTERIZATION OF DIMENSION). *Suppose V is irreducible and that*

$$V \supset V_1 \supset \cdots \supset V_d \neq \emptyset$$

is a maximal chain of distinct closed irreducible subsets of V. Then $\dim(V) = d$. *(Maximal means that the chain can't be refined.)*

PROOF. From (9.4) we find that

$$\dim V = \dim V_1 + 1 = \dim V_2 + 2 = \cdots = \dim V_d + d = d. \qquad \square$$

REMARK 9.6. (a) The corollary shows that, when V is affine, $\dim V =$ 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 5.23). Moreover, if $\mathfrak{p}$ is an ideal in $k[V]$ with height i, then there is a maximal (i.e., nonrefinable) chain of distinct prime ideals

$$(0) \subset \mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \cdots \subset \mathfrak{p}_d \neq k[V]$$

with $\mathfrak{p}_i = \mathfrak{p}$.

(b) Now that we know that the two notions of dimension coincide, we can restate (9.2) 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 (CA 15.3), and is called Krull's principal ideal theorem.

COROLLARY 9.7. *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*

$$\operatorname{codim}(Z) \leq r, \textit{ i.e., } \dim(Z) \geq \dim V - r.$$

PROOF. As in the proof of (9.4), 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, $\operatorname{codim}(Z') \leq r-1$. 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 $\operatorname{codim}(Z) = \operatorname{codim}(Z') \leq r-1$; otherwise, the theorem shows that Z has codimension 1 in Z', and $\operatorname{codim}(Z) = \operatorname{codim}(Z') + 1 \leq r$. □

PROPOSITION 9.8. *Let V and W be closed subvarieties of $\mathbb{A}^n$; for any (nonempty) irreducible component Z of $V \cap W$,*

$$\dim(Z) \geq \dim(V) + \dim(W) - n;$$

that is,

$$\operatorname{codim}(Z) \leq \operatorname{codim}(V) + \operatorname{codim}(W).$$

PROOF. In the course of the proof of (4.27), 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 (9.7). □

REMARK 9.9. (a) The example (in $\mathbb{A}^3$)

$$\begin{cases} X^2 + Y^2 & = Z^2 \\ \quad\quad Z & = 0 \end{cases}$$

shows that Proposition 9.8 becomes false if one only looks at real points. Also, that the pictures we draw can mislead.

(b) The statement of (9.8) 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 (9.8) fails because the diagonal in $V \times V$ cannot be defined by 3 equations (it takes the same 4 that define the diagonal in $\mathbb{A}^4$) — the diagonal is not a set-theoretic complete intersection.

REMARK 9.10. In (9.7), the components of $V(f_1, \ldots, f_r)$ 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 (9.2)). 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 9.11. *Let Z be a closed irreducible subvariety of codimension r in an affine variety V. Then there exist regular functions $f_1, \ldots, f_r$ on V such that Z is an irreducible component of $V(f_1, \ldots, f_r)$ and all irreducible components of $V(f_1, \ldots, f_r)$ 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 $\operatorname{codim} Z_i = i$. We shall show that there exist $f_1, \ldots, f_r \in k[V]$ such that, for all $s \leq r$, Z_s is an irreducible component of $V(f_1, \ldots, f_s)$ and all irreducible components of $V(f_1, \ldots, f_s)$ 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 9.2. Suppose $f_1, \ldots, f_{s-1}$ have been chosen, and let $Y_1 = Z_{s-1}, \ldots, Y_m$, be the irreducible components of $V(f_1, \ldots, f_{s-1})$. 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 9.12 (PRIME AVOIDANCE LEMMA). *If an ideal $\mathfrak{a}$ of a ring A is not contained in any of the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$, 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 $h_{i_0} \stackrel{\text{def}}{=} \prod f_i$ 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 $\sum_{i=1}^{r} h_i$ is therefore in $\mathfrak{a}$ but not in any $\mathfrak{p}_i$. □

REMARK 9.13. 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 $f_1, \ldots, f_r \in A$ such that $\mathfrak{p}$ is minimal among the prime ideals containing $(f_1, \ldots, f_r)$. This statement is true for all noetherian local rings.

REMARK 9.14. 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 $f_i \in k[X_1, \ldots, X_n]$ (resp. homogeneous polynomials $f_i \in k[X_0, \ldots, X_n]$) such that

$$V = V(f_1, \ldots, f_r).$$

Such a variety is said to be an ***ideal-theoretic complete intersection*** if the f_i can be chosen so that $I(V) = (f_1, \ldots, f_r)$. 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 (9.11) shows that there is a neighbourhood U of P in $\mathbb{A}^n$ and functions $f_1, \ldots, f_r$ on U such that $U \cap V = V(f_1, \ldots, f_r)$ (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

ideal-theoretic complete intersection $\Rightarrow$ 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 (cf. 5.17).

PROPOSITION 9.15. *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 $f_1, \ldots, f_r$ on U such that $Z \cap U = V(f_1, \ldots, f_r)$.*

PROOF. By assumption

$$\dim_k T_P(Z) = \dim Z = \dim V - r = \dim_k T_P(V) - r.$$

There exist functions $f_1, \ldots, f_r$ 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

$$(df_1)_P = 0, \ldots, (df_r)_P = 0.$$

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 $Z' \stackrel{\text{def}}{=} V(f_1, \ldots, f_r)$ (zero set in U) passing through P. After replacing U by a smaller neighbourhood, we can assume that Z' is irreducible. As $f_1, \ldots, f_r \in I(Z')$, 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 9.16. *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 (2.27) 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 9.17. 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 $V(f|Z') = \{(0, \ldots, 0)\}$, which is impossible (because it has codimension 2, which violates 9.2). 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 9.18. *Let $V = V(\mathfrak{a}) \subset \mathbb{P}^n$ be a projective variety of dimension ≥ 1, and let $f \in k[X_0, \ldots, X_n]$ 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 (9.2) is the fact that $V \cap V(f)$ is nonempty. Let $V^{\text{aff}}(\mathfrak{a})$ be the zero set of $\mathfrak{a}$ in $\mathbb{A}^{n+1}$ (that is, the affine cone over V). Then $V^{\text{aff}}(\mathfrak{a}) \cap V^{\text{aff}}(f)$ is nonempty (it contains $(0, \ldots, 0)$), and so it has codimension 1 in $V^{\text{aff}}(\mathfrak{a})$. Clearly $V^{\text{aff}}(\mathfrak{a})$ has dimension ≥ 2, and so $V^{\text{aff}}(\mathfrak{a}) \cap V^{\text{aff}}(f)$ has dimension ≥ 1. This implies that the polynomials in $\mathfrak{a}$ have a zero in common with f other than the origin, and so $V(\mathfrak{a}) \cap V(f) \neq \emptyset$. $\square$

COROLLARY 9.19. *Let $f_1, \cdots, f_r$ be homogeneous nonconstant elements of $k[X_0, \ldots, X_n]$; and let Z be an irreducible component of $V \cap V(f_1, \ldots f_r)$. Then codim$(Z) \leq r$, and if $\dim(V) \geq r$, then $V \cap V(f_1, \ldots f_r)$ is nonempty.*

PROOF. Induction on r, as before. $\square$

COROLLARY 9.20. *Let $\alpha \colon \mathbb{P}^n \to \mathbb{P}^m$ be regular; if $m < n$, then α is constant.*

PROOF. [2]Let $\pi \colon \mathbb{A}^{n+1} - \{\text{origin}\} \to \mathbb{P}^n$ be the map $(a_0, \ldots, a_n) \mapsto (a_0 : \ldots : a_n)$. Then $\alpha \circ \pi$ is regular, and there exist polynomials $F_0, \ldots, F_m \in k[X_0, \ldots, X_n]$ such that $\alpha \circ \pi$ is the map

$$(a_0, \ldots, a_n) \mapsto (F_0(a) : \ldots : F_m(a)).$$

As $\alpha \circ \pi$ factors through $\mathbb{P}^n$, the F_i must be homogeneous of the same degree. Note that

$$\alpha(a_0 : \ldots : a_n) = (F_0(a) : \ldots : F_m(a)).$$

If $m < n$ and the F_i are nonconstant, then (9.18) 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. $\square$

PROPOSITION 9.21. *Let Z be a closed irreducible subvariety of V; if codim$(Z) = r$, then there exist homogeneous polynomials $f_1, \ldots, f_r$ in $k[X_0, \ldots, X_n]$ such that Z is an irreducible component of $V \cap V(f_1, \ldots, f_r)$.*

PROOF. Use the same argument as in the proof (9.11). $\square$

[2]Lars Kindler points out that, in this proof, it is not obvious that the map $\alpha \circ \pi$ is given globally by a system of polynomials (rather than just locally). It is in fact given globally, and this is not too difficult to prove: a regular map from a variety V to $\mathbb{P}^n$ corresponds to a line bundle on V and a set of global sections, and all line bundles on $\mathbb{A}^n$ are trivial (see, for example, Hartshorne II 7.1 and II 6.2). I should fix this in a future version.

PROPOSITION 9.22. *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 $k[X_0, \ldots, X_n]$.*

PROOF. Follows from the affine case. □

COROLLARY 9.23. *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 codim(Z) $\leq$codim(V)+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 9.24. *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 9.25. *Let W be a vector space of dimension d over an infinite field k, and let $E_1, \ldots, E_r$ 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 (Exercise 1-1).

Suppose $r > 0$, and let $V_1, \ldots, V_s$ 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 $L_0, \ldots, L_r$ 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.

Chapter 10

Regular Maps and Their Fibres

Throughout this chapter, k is an algebraically closed field.

Consider again the regular map $\varphi\colon \mathbb{A}^2 \to \mathbb{A}^2$, $(x,y) \mapsto (x,xy)$ (Exercise 3-3). The image of φ is

$$\begin{aligned} C &= \{(a,b) \in \mathbb{A}^2 \mid a \neq 0 \text{ or } a = 0 = b\} \\ &= (\mathbb{A}^2 \smallsetminus \{y\text{-axis}\}) \cup \{(0,0)\}, \end{aligned}$$

which is neither open nor closed, and, in fact, is not even locally closed. The fibre

$$\varphi^{-1}(a,b) = \begin{cases} \{(a,b/a)\} & \text{if } a \neq 0 \\ Y\text{-axis} & \text{if } (a,b) = (0,0) \\ \emptyset & \text{if } a = 0,\, b \neq 0. \end{cases}$$

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 over 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 10.1. *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 $C = \bigcup(U_i \cap Z_i)$ 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 $\bar{C} \subset \bigcup Z_i$, 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 10.2. *A regular map $\varphi: W \to V$ 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 10.3. *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 $\alpha: A \to \Omega$ from A into an algebraically closed field Ω such that $\alpha(a) \neq 0$ can be extended to a homomorphism $\beta: B \to \Omega$ such that $\beta(b) \neq 0$.*

Consider, for example, the rings $k[X] \subset k[X, X^{-1}]$. A homomorphism $\alpha: k[X] \to k$ 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 10.3, we only really need the case $b = 1$, but the more general statement is needed so that we can prove it by induction.

LEMMA 10.4. *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 $\alpha: A \to \Omega$ 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 $\tilde{\alpha}: A[T] \to \Omega[T]$ 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 $h(T) = c_r T^r + c_{r-1}T^{r-1} + \cdots + c_0 \in \mathfrak{a}$,

$$h'(c) = \alpha(c_r) + \alpha(c_{r-1})c + \cdots + c_0 c^r = 0.$$

On taking $h = g$, we see that $c = 0$, and on taking $h = f$, we obtain the contradiction $\alpha(a_m) = 0$. □

PROOF (OF 10.3) Suppose that we know the proposition in the case that B is generated by a single element, and write $B = A[x_1, \ldots, x_n]$. Then there exists an element b_{n-1} such that any homomorphism $\alpha: A[x_1, \ldots, x_{n-1}] \to \Omega$ such that $\alpha(b_{n-1}) \neq 0$ extends to a homomorphism $\beta: B \to \Omega$ 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

$$b = f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n, \quad a_i \in A,$$

and take $a = a_0$. If $\alpha: A \to \Omega$ 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 $\sum d_i x^i \mapsto \sum \alpha(d_i)c^i$.

Case (ii). The ideal $\mathfrak{a} \neq (0)$. Let $f(T) = a_m T^m + \cdots$, $a_m \neq 0$, 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 $\beta: B \to \Omega$ by the previous lemma, and $\beta(u(x) \cdot b) = \beta(c) \neq 0$, and so $\beta(b) \neq 0$. □

ASIDE 10.5. In case (ii) of the above proof, both b and b^{-1} are algebraic over A, and so there exist equations

$$a_0 b^m + \cdots + a_m = 0, \quad a_i \in A, \quad a_0 \neq 0;$$

$$a_0' b^{-n} + \cdots + a_n' = 0, \quad a_i' \in A, \quad a_0' \neq 0.$$

One can show that $a = a_0 a_0'$ has the property required by the Proposition—see Atiyah and MacDonald, 5.23.

PROOF (OF 10.2) 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 $W_1, \ldots, W_r$ 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 dominant). 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. □

Orbits of group actions

Let G be an algebraic group. An ***action*** of G on a variety V is a regular map

$$(g, P) \mapsto gP\colon G \times V \to V$$

such that

(a) $1_G P = P$, all $P \in V$;
(b) $g(g'P) = (gg')P$, all $g, g' \in G$, $P \in V$.

PROPOSITION 10.6. *Let $G \times V \to V$ be an action of an algebraic group G on a variety V.*

(a) *Each orbit of G in X is open in its closure.*
(b) *There exist closed orbits.*

PROOF. (a) Let O be an orbit of G in V and let $P \in O$. Then $g \mapsto gP : G \to V$ is a regular map with image O, and so O contains a nonempty set U open in $\bar{O}$ (10.2). As $O = \bigcup_{g \in G(k)} gU$, it is open in $\bar{O}$.

(b) Let $S = \bar{O}$ be minimal among the closures of orbits. From (a), we know that O is open in S. Therefore, if $S \smallsetminus O$ were nonempty, it would contain the closure of an orbit, contradicting the minimality of S. Hence $S = O$. □

Let G be an algebraic group acting on a variety V. Let $G\backslash V$ denote the quotient topological space with the sheaf $\mathcal{O}_{G\backslash V}$ such that $\Gamma(U, \mathcal{O}_{G\backslash V}) = \Gamma(\pi^{-1}U, \mathcal{O}_V)^G$, where $\pi : G \to G/V$ is the quotient map. When $(G\backslash V, \mathcal{O}_{G\backslash V})$ is a variety, we call it the ***geometric quotient*** of V under the action of G.

PROPOSITION 10.7. *Let N be a normal algebraic subgroup of an affine algebraic group G. Then the geometric quotient of G by N exists, and is an affine algebraic group.*

PROOF. Omitted for the present. □

A connected affine algebraic group G is ***solvable*** if there exist connected algebraic subgroups

$$G = G_d \supset G_{d-1} \supset \cdots \supset G_0 = \{1\}$$

such that G_i is normal in G_{i+1}, and G_i/G_{i+1} is commutative.

THEOREM 10.8 (BOREL FIXED POINT THEOREM). *A connected solvable affine algebraic group G acting on a complete algebraic variety V has at least one fixed point.*

PROOF. We prove this by induction on the $\dim G$. Assume first that G is commutative, and let $O = Gx$ be a closed orbit of G in V (see 10.6). Let N be the stabilizer of x. Because G is commutative, N is normal, and we get a bijection $G/N \to O$. As G acts transitively on G/N and O, the map $G/N \to O$ is proper (see Exercise 10-4); as O is complete (7.3a), so also is G/N (see 8.23), and as it is affine and connected, it consists of a single point (7.5). Therefore, O consists of a single point, which is a fixed point for the action.

By assumption, there exists a closed normal subgroup H of G such that G/H is a commutative. The set X^H of fixed points of H in X is nonempty (by induction) and closed (because it is the intersection of the sets

$$X^h = \{x \in X \mid hx = x\}$$

for $h \in H$). Because H is normal, X^H is stable under G, and the action of G on it factors through G/H. Every fixed point of G/H in X^H is a fixed point for G acting on X. □

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 dominant.

THEOREM 10.9. *Let $\varphi\colon W \to V$ be a dominant 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 10.10. Consider the subvariety $W \subset V \times \mathbb{A}^m$ defined by r linear equations

$$\sum_{j=1}^{m} a_{ij} X_j = 0, \quad a_{ij} \in k[V], \quad i = 1, \ldots, r,$$

and let φ be the projection $W \to V$. For $P \in V$, $\varphi^{-1}(P)$ is the set of solutions of

$$\sum_{j=1}^{m} a_{ij}(P) X_j = 0, \quad a_{ij}(P) \in k, \quad i = 1, \ldots, r,$$

and so its dimension is $m - \mathrm{rank}(a_{ij}(P))$. 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 dominant, there is a homomorphism $k(V) \hookrightarrow k(W)$, and obviously $\mathrm{tr\,deg}_k k(V) \leq \mathrm{tr\,deg}_k k(W)$ (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 (9.11) we know that there exist regular functions $f_1, \ldots, f_m$ such that P is an irreducible component of $V(f_1, \ldots, f_m)$. After replacing V by a smaller neighbourhood of P, we can suppose that $P = V(f_1, \ldots, f_m)$. Then $\varphi^{-1}(P)$ is the zero set of the regular functions $f_1 \circ \varphi, \ldots, f_m \circ \varphi$, and so (if nonempty) has codimension $\leq m$ in W (see 9.7). 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 dominant, $k[V] \to k[W]$ 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 $k[V] = k[x_1, \ldots, x_M]$ and $k[W] = k[y_1, \ldots, y_N]$, 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 $y_1, \ldots, y_{n-m}$ are algebraically independent over $k[x_1, \ldots, x_m]$, and that the remaining y_i are algebraic over $k[x_1, \ldots, x_m, y_1, \ldots, y_{n-m}]$. There are therefore relations

$$F_i(x_1, \ldots, x_m, y_1, \ldots, y_{n-m}, y_i) = 0, \quad i = n-m+1, \ldots, N. \tag{24}$$

with $F_i(X_1,\ldots,X_m,Y_1,\ldots,Y_{n-m},Y_i)$ a nonzero polynomial. We write $\bar{y}_i$ for the restriction of y_i to $\varphi^{-1}(P)$. Then

$$k[\varphi^{-1}(P)] = k[\bar{y}_1,\ldots,\bar{y}_N].$$

The equations (24) give an algebraic relation among the functions $x_1,\ldots,y_i$ on W. When we restrict them to $\varphi^{-1}(P)$, they become equations:

$$F_i(x_1(P),\ldots,x_m(P),\bar{y}_1,\ldots,\bar{y}_{n-m},\bar{y}_i) = 0, \quad i = n-m+1,\ldots,N.$$

If these are nontrivial algebraic relations, i.e., if none of the polynomials

$$F_i(x_1(P),\ldots,x_m(P),Y_1,\ldots,Y_{n-m},Y_i)$$

is identically zero, then the transcendence degree of $k(\bar{y}_1,\ldots,\bar{y}_N)$ over k will be $\leq n-m$.

Thus, regard $F_i(x_1,\ldots,x_m,Y_1,\ldots,Y_{n-m},Y_i)$ 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 $U = V - \bigcup V_i$—it is a nonempty open subset of V. If $P \in U$, then none of the polynomials $F_i(x_1(P),\ldots,x_m(P),Y_1,\ldots,Y_{n-m},Y_i)$ 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 $Z_1,\ldots,Z_r$ 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 10.11. *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 (10.9) 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 $P \in U$, $\varphi^{-1}(P) \nsubseteq Z$.

(c) $\varphi(Z) = V$, $\dim(Z) \geq n+\dim(V)$. Then (b) of (10.9) 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 $Z_1,\ldots,Z_r$ 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, $\varphi^{-1}(P) \nsubseteq Z_i$ for any i, but $\varphi^{-1}(P)$ is irreducible and $\varphi^{-1}(P) = \bigcup(\varphi^{-1}(P) \cap Z_i)$, and so this is impossible. □

The fibres of finite maps

Let $\varphi: W \to V$ be a finite dominant 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.

THEOREM 10.12. *Let $\varphi: W \to V$ 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 10.13. (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 consider the map

$$t \mapsto (t^2 - 1, t(t^2 - 1)): \mathbb{A}^1 \to C.$$

It is one-to-one except that the points $t = \pm 1$ both map to 0. On coordinate rings, it corresponds to the inclusion

$$k[x, y] \hookrightarrow k[T],\, x \mapsto T^2 - 1,\, y \mapsto t(t^2 - 1),$$

and so is of degree one. 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 $\varphi: \mathbb{A}^n \to \mathbb{A}^n$, $(a_1, \ldots, a_n) \mapsto (a_1^p, \ldots, a_n^p)$, 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

$$k(X_1, \ldots, X_n) \supset k(X_1^p, \ldots, X_n^p)$$

which is purely inseparable.

LEMMA 10.14. *Let $Q_1, \ldots, Q_r$ 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 10.12). 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 $\varphi^{-1}(P) = \{Q_1, \ldots, Q_r\}$. 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 1.22). 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 $r \leq m \leq \deg(\varphi)$.

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

$$k[V] \to k[V][T]/(F) \stackrel{T \mapsto f}{\to} k[W]$$

gives a factorization

$$W \to \operatorname{Spm}(k[V][T]/(F)) \to V.$$

Each point $P' \in U$ has exactly m inverse images under the second map, and the first map is finite and dominant, 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

$$W \longrightarrow \operatorname{Spm}(A[T]/(F)) \to V$$

shows that $\#\varphi^{-1}(P) \geq \deg(\varphi)$ 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 10.15. Let $\varphi \colon W \to V$ be as in the theorem, and let $V_i = \{P \in V \mid \#\varphi^{-1}(P) \leq i\}$. 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.

Flat maps

A regular map $\varphi \colon V \to W$ is ***flat*** if for all $P \in V$, the homomorphism $\mathcal{O}_{\varphi(P)} \to \mathcal{O}_P$ defined by φ is flat. If φ is flat, then for every pair U and U' of open affines of V and W such that $\varphi(U) \subset U'$ the map $\Gamma(U', \mathcal{O}_W) \to \Gamma(U, \mathcal{O}_V)$ is flat; conversely, if this condition holds for sufficiently many pairs that the U's cover V and the U''s cover W, then φ is flat.

PROPOSITION 10.16. *(a) An open immersion is flat.*

(b) The composite of two flat maps is flat.

(c) Any base extension of a flat map is flat.

PROOF. To be added. □

THEOREM 10.17. *A finite map $\varphi\colon V \to W$ is flat if and only if*

$$\sum_{Q \mapsto P} \dim_k \mathcal{O}_Q/\mathfrak{m}_P \mathcal{O}_Q$$

is independent of $P \in W$.

PROOF. To be added. □

THEOREM 10.18. *Let V and W be irreducible varieties. If $\varphi\colon V \to W$ is flat, then*

$$\dim \varphi^{-1}(Q) = \dim V - \dim W \tag{25}$$

for all $Q \in W$. Conversely, if V and W are nonsingular and (25) holds for all $Q \in W$, then φ is flat.

PROOF. To be added. □

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

$$p(L) = (p_{01} : p_{02} : p_{03} : p_{12} : p_{13} : p_{23}) \in \mathbb{P}^5, \quad p_{ij} \stackrel{\text{def}}{=} \begin{vmatrix} x_i & x_j \\ y_i & y_j \end{vmatrix},$$

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 10.19. *The line L can be recovered from $p(L)$ as follows:*

$$L = \{(\textstyle\sum_j a_j p_{0j} : \sum_j a_j p_{1j} : \sum_j a_j p_{2j} : \sum_j a_j p_{3j}) \mid (a_0 : a_1 : a_2 : a_3) \in \mathbb{P}^3\}.$$

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

$$f(\mathbf{y})\mathbf{x} - f(\mathbf{x})\mathbf{y} = (\textstyle\sum a_j p_{0j}, \sum a_j p_{1j}, \sum a_j p_{2j}, \sum a_j p_{3j}).$$

□

LEMMA 10.20. *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 10.21. *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

$$\begin{aligned}(-p_{01}p_{03} : -p_{02}p_{03} : -p_{03}^2 : \underbrace{p_{01}p_{23} - p_{02}p_{13}}_{-p_{03}p_{12}} : -p_{03}p_{13} : -p_{03}p_{23}) \\ = (p_{01} : p_{02} : p_{03} : p_{12} : p_{13} : p_{23}).\end{aligned}$$

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 Grassmannians discussed in §6.)

We next consider the set of homogeneous polynomials of degree m in 4 variables,

$$F(X_0, X_1, X_2, X_3) = \sum_{i_0+i_1+i_2+i_3=m} a_{i_0i_1i_2i_3} X_0^{i_0} \dots X_3^{i_3}.$$

LEMMA 10.22. *The set of homogeneous polynomials of degree m in 4 variables is a vector space of dimension $\binom{3+m}{m}$*

PROOF. See the footnote p114. □

Let $\nu = \binom{3+m}{m} - 1 = \frac{(m+1)(m+2)(m+3)}{6} - 1$, and regard $\mathbb{P}^\nu$ as the projective space attached to the vector space of homogeneous polynomials of degree m in 4 variables (p118). Then we have a surjective map

$$\mathbb{P}^\nu \to \{\text{surfaces of degree } m \text{ in } \mathbb{P}^3\},$$

$$(\ldots : a_{i_0 i_1 i_2 i_3} : \ldots) \mapsto V(F), \qquad F = \sum a_{i_0 i_1 i_2 i_3} X_0^{i_0} X_1^{i_1} X_2^{i_2} X_3^{i_3}.$$

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 (possibly 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 10.23. *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 10.24. 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

$$p(L) = (p_{01} : p_{02} : \ldots) \qquad F = \sum a_{i_0 i_1 i_2 i_3} X_0^{i_0} \cdots X_3^{i_3}.$$

From (10.19) we see that L lies on the surface $F(X_0, X_1, X_2, X_3) = 0$ if and only if

$$F(\textstyle\sum b_j p_{0j} : \sum b_j p_{1j} : \sum b_j p_{2j} : \sum b_j p_{3j}) = 0, \text{ all } (b_0, \ldots, b_3) \in k^4.$$

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 $F(...) = 0$ 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

$$P(\ldots, a_{i_0 i_1 i_2 i_3}, \ldots ; p_{01}, p_{02} : \ldots)$$

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 7.9).

It remains to compute the dimension of Γ_m. We shall apply Proposition 10.11 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 homogeneous 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 (10.11) 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 By definition

$$\psi^{-1}(F) = \{L \mid L \text{ lies on } V(F)\}.$$

EXAMPLE 10.25. 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 (10.9) 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 10.26. *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 6.23)

$$(a_0 : a_1), (b_0 : b_1) \mapsto (a_0 b_0 : a_0 b_1 : a_1 b_0 : a_1 b_1) : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3.$$

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:

$$\begin{cases} t_0 X = t_1 Z \\ t_0 Y = t_1 W \end{cases} \text{and} \begin{cases} t_0 X = t_1 Y \\ t_0 Z = t_1 W. \end{cases}$$

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 $\psi : \Gamma_2 \to \mathbb{P}^9$ is surjective. Thus (10.9) 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 (this was a homework problem in the original course).

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:

$$\begin{array}{ccl} \Gamma_2 - \psi^{-1}(S) & = & \text{pairs, } (F, L) \text{ with } L \text{ on } F; \\ \downarrow & & \\ R & = & \text{set of reguli;} \\ \downarrow & & \\ \mathbb{P}^9 - S & = & \text{set of nondegenerate quadrics.} \end{array}$$

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 (10.30) below).

We now look at the case $m = 3$. Here $\dim \Gamma_3 = 19$; $\nu = 19$: we have a map

$$\psi : \Gamma_3 \to \mathbb{P}^{19}.$$

THEOREM 10.27. *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 10.28. (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, $0 \leq i, j \leq 2$:

$$\begin{cases} X_0 + \zeta^i X_1 = 0 \\ X_2 + \zeta^j X_3 = 0 \end{cases} \quad \begin{cases} X_0 + \zeta^i X_2 = 0 \\ X_1 + \zeta^j X_3 = 0 \end{cases} \quad \begin{cases} X_0 + \zeta^i X_3 = 0 \\ X_1 + \zeta^j X_2 = 0 \end{cases}$$

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 10.27). 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 10.9), which contradicts two of the above examples. Therefore the map is surjective[1], 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 (8.24), the restriction of ψ to $\psi^{-1}(U)$ is finite, and so we can apply (10.12) to see that all cubics in $U - U'$ have fewer than 27 lines.

REMARK 10.29. 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 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 $\mathbb{P}^2$.

[1] According to Miles Reid (1988, p126) every adult algebraic geometer knows the proof that every cubic contains a line.

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 10.30. *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 $k(W)$). □

Exercises

10-1. Let G be a connected algebraic group, and consider an action of G on a variety V, i.e., a regular map $G \times V \to V$ such that $(gg')v = g(g'v)$ for all $g, g' \in G$ and $v \in V$. Show that each orbit $O = Gv$ of G is nonsingular and open in its closure $\bar{O}$, and that $\bar{O} \smallsetminus O$ is a union of orbits of strictly lower dimension. Deduce that there is at least one closed orbit.

10-2. Let $G = \mathrm{GL}_2 = V$, and let G act on V by conjugation. According to the theory of Jordan canonical forms, the orbits are of three types:

(a) Characteristic polynomial $X^2 + aX + b$; distinct roots.
(b) Characteristic polynomial $X^2 + aX + b$; minimal polynomial the same; repeated roots.
(c) Characteristic polynomial $X^2 + aX + b = (X - \alpha)^2$; minimal polynomial $X - \alpha$.

For each type, find the dimension of the orbit, the equations defining it (as a subvariety of V), the closure of the orbit, and which other orbits are contained in the closure.

(You may assume, if you wish, that the characteristic is zero. Also, you may assume the following (fairly difficult) result: for any closed subgroup H of an algebraic group G, G/H has a natural structure of an algebraic variety with the following properties: $G \to G/H$ is regular, and a map $G/H \to V$ is regular if the composite $G \to G/H \to V$ is regular; $\dim G/H = \dim G - \dim H$.)

[The enthusiasts may wish to carry out the analysis for GL_n.]

10-3. Find $3d^2$ lines on the Fermat projective surface

$$X_0^d + X_1^d + X_2^d + X_3^d = 0, \quad d \geq 3, \quad (p, d) = 1, \quad p \text{ the characteristic.}$$

10-4. (a) Let $\varphi\colon W \to V$ be a quasi-finite dominant regular map of irreducible varieties. Show that there are open subsets U' and U of W and V such that $\varphi(U') \subset U$ and $\varphi\colon U' \to U$ is finite.

(b) Let G be an algebraic group acting transitively on irreducible varieties W and V, and let $\varphi\colon W \to V$ be G-equivariant regular map satisfying the hypotheses in (a). Then φ is finite, and hence proper.

Chapter 11

Algebraic spaces; geometry over an arbitrary field

In this chapter, we explain how to extend the theory of the preceding chapters to a nonalgebraically closed base field. One major difference is that we need to consider ringed spaces in which the sheaf of rings is no longer a sheaf of functions on the base space. Once we allow that degree of extra generality, it is natural to allow the rings to have nilpotents. In this way we obtain the notion of an algebraic space, which even over an algebraically closed field is more general than that of an algebraic variety.

Throughout this chapter, k is a field and k^{al} is an algebraic closure of k.

Preliminaries

Sheaves

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 $U' \subset U$ a "restriction" map

$$a \mapsto a|U' \colon \mathcal{F}(U) \to \mathcal{F}(U');$$

when $U = U'$ the restriction map is required to be the identity map, and if

$$U'' \subset U' \subset U,$$

then the composite of the restriction maps

$$\mathcal{F}(U) \to \mathcal{F}(U') \to \mathcal{F}(U'')$$

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, i.e., a morphism of functors.

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

$$\mathcal{F}_v = \varinjlim \mathcal{F}(U) \quad \text{(limit over open neighbourhoods of } v).$$

In other words, it is the set of equivalence classes of pairs (U, s) with U an open neighbourhood of v and $s \in \mathcal{F}(U)$; two pairs (U, s) and (U', s') are equivalent if $s|U'' = s|U''$ for some open neighbourhood U'' of v contained in $U \cap U'$.

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

$$\psi(U'): \mathcal{O}'(U') \to \mathcal{O}(\varphi^{-1}(U')), \quad U' \text{ open in } V',$$

commuting with the restriction maps. Such a pair defines homomorphism of rings $\psi_v: \mathcal{O}'_{\varphi(v)} \to \mathcal{O}_v$ 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.

In the remainder of this chapter, a ringed space will be a topological space V together with a sheaf of k-algebras, and morphisms of ringed spaces will be required to preserve the k-algebra structures.

Extending scalars (extending the base field)

Nilpotents

Recall that a ring A is reduced if it has no nilpotents. The ring A may be reduced without $A \otimes_k k^{\mathrm{al}}$ being reduced. Consider for example the algebra $A = k[X, Y]/(X^p + Y^p + a)$ where $p = \mathrm{char}(k)$ and a is not a p^{th}-power in k. Then A is reduced (even an integral domain) because $X^p + Y^p + a$ is irreducible in $k[X, Y]$, but

$$\begin{aligned} A \otimes_k k^{\mathrm{al}} &\simeq k^{\mathrm{al}}[X, Y]/(X^p + Y^p + a) \\ &= k^{\mathrm{al}}[X, Y]/((X + Y + \alpha)^p), \quad \alpha^p = a, \end{aligned}$$

which is not reduced because $x + y + \alpha \neq 0$ but $(x + y + \alpha)^p = 0$.

In this subsection, we show that problems of this kind arise only because of inseparability. In particular, they don't occur if k is perfect.

Now assume k has characteristic $p \neq 0$, and let Ω be some (large) field containing k^{al}. 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.

DEFINITION 11.1. Subfields K, K' of Ω containing k are said to be ***linearly disjoint*** over k if the map $K \otimes_k K' \to \Omega$ is injective.

Equivalent conditions:

- ◇ if $e_1, \ldots, e_m \in K$ are linearly independent over k and $e'_1, \ldots, e'_{m'} \in K'$ are linearly independent over k, then the elements $e_1e'_1, e_1e'_2, \ldots, e_me'_{m'}$ of Ω are linearly independent over k;
- ◇ if $e_1, \ldots, e_m \in K$ are linearly independent over k, then they are also linearly independent over K'.

(*) The following statements are easy to prove.

(a) Every purely transcendental extension of k is linearly disjoint from every algebraic extension of k.
(b) Every separable algebraic extension of k is linearly disjoint from every purely inseparable algebraic extension of k.
(c) Let $K \supset k$ and $L \supset E \supset k$ be subfields of Ω. Then K and L are linearly disjoint over k if and only if K and E are linearly disjoint over k and KE and L are linearly disjoint over k.

LEMMA 11.2. *Let $K = k(x_1, \ldots, x_{d+1}) \subset \Omega$ with $x_1, \ldots, x_d$ algebraically independent over F, and let $f \in k[X_1, \ldots, X_{d+1}]$ be an irreducible polynomial such that $f(x_1, \ldots, x_{d+1}) = 0$. If k is linearly disjoint from $k^{\frac{1}{p}}$, then $f \notin k[X_1^p, \ldots, X_{d+1}^p]$.*

PROOF. Suppose otherwise, say, $f = g(X_1^p, \ldots, X_{d+1}^p)$. Let $M_1, \ldots, M_r$ be the monomials in $X_1, \ldots, X_{d+1}$ that actually occur in $g(X_1, \ldots, X_{d+1})$, and let $m_i = M_i(x_1, \ldots, x_{d+1})$. Then $m_1, \ldots, m_r$ are linearly independent over k (because each has degree less than that of f). However, $m_1^p, \ldots, m_r^p$ are linearly dependent over k, because $g(x_1^p, \ldots, x_{d+1}^p) = 0$. But

$$\sum a_i m_i^p = 0 \quad (a_i \in k) \implies \sum a_i^{\frac{1}{p}} m_i = 0 \quad (a_i^{\frac{1}{p}} \in k^{\frac{1}{p}})$$

and we have a contradiction. □

A ***separating transcendence basis*** for $K \supset k$ is a transcendence basis $\{x_1, \ldots, x_d\}$ such that K is separable over $k(x_1, \ldots, x_d)$. The next proposition is improves Theorem 8.21 of FT.

PROPOSITION 11.3. *Let K be a finitely generated field extension k, and let Ω be an algebraically closed field containing K^{al}. The following statements are equivalent:*

(a) *K/k admits a separating transcendence basis;*
(b) *for any purely inseparable extension L of k in K, the fields K and L are linearly disjoint over k;*
(c) *the fields K and $k^{\frac{1}{p}}$ are linearly disjoint over k.*

PROOF. (a)⇒(b). This follows easily from (*).

(b)⇒(c). Trivial.

(c)⇒(a). Let $K = k(x_1, \ldots, x_n)$, and let d be the transcendence degree of K/k. After renumbering, we may suppose that $x_1, \ldots, x_d$ are algebraically independent (FT 8.12). We proceed by induction on n. If $n = d$ there is nothing to prove, and so we may assume that $n \geq d + 1$. Then $f(x_1, \ldots, x_{d+1}) = 0$ for some nonzero irreducible polynomial $f(X_1, \ldots, X_{d+1})$ with coefficients in k. Not all $\partial f/\partial X_i$ are zero, for otherwise f would be a polynomial in $X_1^p, \ldots, X_{d+1}^p$, which contradicts the lemma. After renumbering again, we may suppose that $\partial f/\partial X_{d+1} \neq 0$, and so $\{x_1, \ldots, x_d\}$ is a separating transcendence basis for $k(x_1, \ldots, x_{d+1})$ over k, which proves the proposition when $n = d + 1$. In the general case, $k(x_1, \ldots, x_{d+1}, x_{d+2})$ is algebraic over $k(x_1, \ldots, x_d)$ and x_{d+1} is separable over $k(x_1, \ldots, x_d)$, and so, by the primitive element theorem (FT 5.1) there is an element y such that $k(x_1, \ldots, x_{d+2}) = k(x_1, \ldots, x_d, y)$. Thus K is generated by the $n-1$ elements $x_1, \ldots x_d, y, x_{d+3}, \ldots, x_n$, and we apply induction. □

A finitely generated field extension $K \supset k$ is said to be ***regular*** if it satisfies the equivalent conditions of the proposition.

PROPOSITION 11.4. *Let A be a reduced finitely generated k-algebra. The following statements are equivalent:*

(a) $k^{\frac{1}{p}} \otimes_k A$ *is reduced;*
(b) $k^{\mathrm{al}} \otimes_k A$ *is reduced;*
(c) $K \otimes_k A$ *is reduced for all fields $K \supset k$.*

When A is an integral domain, they are also equivalent to A and $k^{\frac{1}{p}}$ being linearly disjoint over k.

PROOF. The implications c$\Longrightarrow$b$\Longrightarrow$a are obvious, and so we only have to prove a $\Longrightarrow$c. After localizing A at a minimal prime, we may suppose that it is a field. Let $e_1, \ldots, e_n$ be elements of A linearly independent over k. If they become linearly dependent over $k^{\frac{1}{p}}$, then $e_1^p, \ldots, e_n^p$ are linearly dependent over k, say, $\sum a_i e_i^p = 0$, $a_i \in k$. Now $\sum a_i^{\frac{1}{p}} \otimes e_i$ is a nonzero element of $k^{\frac{1}{p}} \otimes_k A$, but

$$\left(\sum a_i^{\frac{1}{p}} \otimes e_i\right)^p = \sum a_i \otimes e_i^p = \sum 1 \otimes a_i e_i^p = 1 \otimes \sum a_i e_i^p = 0.$$

This shows that A and $k^{\frac{1}{p}}$ are linearly disjoint over k, and so A has a separating transcendence basis over k. From this it follows that $K \otimes_k A$ is reduced for all fields $K \supset k$. □

Idempotents

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 $A \approx k[X]/(f(X))$ for some irreducible separable polynomial $f(X)$, and so

$$A \otimes_k k^{\mathrm{al}} \approx k^{\mathrm{al}}[X]/(f(X)) = k^{\mathrm{al}}/(\prod(X - a_i)) \simeq \prod k^{\mathrm{al}}/(X - a_i)$$

(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 provides a converse.

PROPOSITION 11.5. *Let A be a finitely generated k-algebra, and assume that A is an integral domain, and that $A \otimes_k k^{\mathrm{al}}$ is reduced. Then $A \otimes_k k^{\mathrm{al}}$ 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 $a \in k$).*

LEMMA: Let k be algebraically closed in an extension field K, and let a be an element of K^{al} that is algebraic over k. Then K and $k[a]$ are linearly disjoint over k, and $[K[a]:K] = [k[a]:k]$.

PROOF: Let $f(X)$ be the minimum polynomial of a over k. Then $f(X)$ is irreducible over K, because the coefficients of any factor of $f(X)$ in $K[X]$ are algebraic over k, and hence lie in k. It follows that the map

$$K \otimes_k k[a] \to K[a]$$

is an isomorphism, because both rings are isomorphic to $K[X]/(f(X))$.

PROOF (OF THE PROPOSITION) Let K be the field of fractions of A — it suffices to show that K is linearly disjoint from L where L is any finite algebraic extension of k in K^{al} (because then $K \otimes_k L \simeq KL$, which is an integral domain). If L is separable over k, then it can be generated by a single element, and so this follows from the lemma. In the general case, we let E be the largest subfield of L separable over k. From (*)(c), we see that it suffices to show that KE and L are linearly disjoint over E. From (11.4), we see that K and $k^{1/p}$ are linearly disjoint over k, and so K is a regular extension of k (see 11.3). It follows easily that KE is a regular extension of E, and KE is linearly disjoint from L by (*)(b). □

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 spaces

For a finitely generated k-algebra A, we define $\mathrm{spm}(A)$ to be the set of maximal ideals in A endowed 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 $\mathrm{spm}(A)$ such that $\Gamma(D(f), \mathcal{O})) = A_f$ for all $f \in A$ (recall that A_f is the ring obtained from A by inverting f), and we denote the resulting ringed space by $\mathrm{Spm}(A)$. The stalk at $\mathfrak{m} \in V$ is $\varinjlim_f A_f \simeq A_{\mathfrak{m}}$.

Let $\mathfrak{m}$ be a maximal ideal of A. Then $k(\mathfrak{m}) =_{\mathrm{df}} A/\mathfrak{m}$ is field that is finitely generated as a k-algebra, and is therefore of finite degree over k (Zariski's lemma, 2.7).

The sections of $\mathcal{O}$ are no longer functions on $V = \mathrm{spm}\, A$. For $\mathfrak{m} \in \mathrm{spm}(A)$ and $f \in A$ we set $f(\mathfrak{m})$ equal to the image of f in $k(\mathfrak{m})$. It does make sense to speak of the zero set of f in V, and $D(f) = \{\mathfrak{m} \mid f(\mathfrak{m}) \neq 0\}$. For $f, g \in A$,

$$f(\mathfrak{m}) = g(\mathfrak{m}) \text{ for all } \mathfrak{m} \in A \iff f - g \text{ is nilpotent.}$$

When k is algebraically closed and A is an affine k-algebra, $k(\mathfrak{m}) \simeq k$ and we recover the definition of $\mathrm{Spm}\, A$ in §3.

An ***affine algebraic space***[1] over k is a ringed space $(V, \mathcal{O}_V)$ such that

◇ $\Gamma(V, \mathcal{O}_V)$ is a finitely generated k-algebra,

◇ for each $P \in V$, $I(P) =_{\mathrm{df}} \{f \in \Gamma(V, \mathcal{O}_V) \mid f(P) = 0\}$ is a maximal ideal in $\Gamma(V, \mathcal{O}_V)$, and

[1]Not to be confused with the algebraic spaces of, for example, of J-P. Serre, Espaces Fibrés Algébriques, 1958, which are simply algebraic varieties in the sense of these notes, or with the algebraic spaces of M. Artin, Algebraic Spaces, 1969, which generalize (!) schemes.

◇ the map $P \mapsto I(P)\colon V \to \mathrm{Spm}(\Gamma(V, \mathcal{O}_V))$ is an isomorphism of ringed spaces.

For an affine algebraic space, we sometimes denote $\Gamma(V, \mathcal{O}_V)$ by $k[V]$. A ***morphism of algebraic spaces over*** k is a morphism of ringed spaces — it is automatically a morphism of locally ringed spaces. An affine algebraic space $(V, \mathcal{O}_V)$ is ***reduced*** if $\Gamma(V, \mathcal{O}_V)$ is reduced.

Let $\alpha\colon A \to B$ be a homomorphism of finitely generated k-algebras. For any maximal ideal $\mathfrak{m}$ of B, there is an injection of k-algebras $A/\alpha^{-1}(\mathfrak{m}) \hookrightarrow B/\mathfrak{m}$. As $B/\mathfrak{m}$ is a field of finite degree over k, this shows that $\alpha^{-1}(\mathfrak{m})$ is a maximal ideal of A. Therefore α defines a map $\mathrm{spm}\, B \to \mathrm{spm}\, A$, which one shows easily defines a morphism of affine algebraic k-spaces

$$\mathrm{Spm}\, B \to \mathrm{Spm}\ A,$$

and this gives a bijection

$$\mathrm{Hom}_{k\text{-alg}}(A, B) \simeq \mathrm{Hom}_k(\mathrm{Spm}\, B, \mathrm{Spm}\, A).$$

Therefore $A \mapsto \mathrm{Spm}(A)$ is an equivalence of from the category of finitely generated k-algebras to that of affine algebraic spaces over k; its quasi-inverse is $V \mapsto k[V] \stackrel{\text{def}}{=} \Gamma(V, \mathcal{O}_V)$. Under this correspondence, reduced algebraic spaces correspond to reduced algebras.

Let V be an affine algebraic space over k. For an ideal $\mathfrak{a}$ in $k[V]$,

$$\mathrm{spm}(A/\mathfrak{a}) \simeq V(\mathfrak{a}) \stackrel{\text{def}}{=} \{P \in V \mid f(P) = 0 \text{ for all } f \in \mathfrak{a}\}.$$

We call $V(\mathfrak{a})$ endowed with the ring structure provided by this isomorphism a ***closed algebraic subspace*** of V. Thus, there is a one-to-one correspondence between the closed algebraic subspaces of V and the ideals in $k[V]$. Note that if $\mathrm{rad}(\mathfrak{a}) = \mathrm{rad}(\mathfrak{b})$, then $V(\mathfrak{a}) = V(\mathfrak{b})$ as topological spaces (but not as algebraic spaces).

Let $\varphi\colon \mathrm{Spm}(B) \to \mathrm{Spm}(A)$ be the map defined by a homomorphism $\alpha\colon A \to B$.

◇ The image of φ is dense if and only if the kernel of α is nilpotent.
◇ The map φ defines an isomorphism of $\mathrm{Spm}(B)$ with a closed subvariety of $\mathrm{Spm}(A)$ if and only if α is surjective.

Affine algebraic varieties.

An ***affine*** k***-algebra*** 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 11.4 has the following consequences: if A is an affine k-algebra, then $A \otimes_k K$ is reduced for all fields K containing k; when k is perfect, every reduced finitely generated k-algebra is affine.

Let A be a finitely generated k-algebra. The choice of a set $\{x_1, ..., x_n\}$ of generators for A, determines isomorphisms

$$A \to k[x_1, ..., x_n] \to k[X_1, ..., X_n]/(f_1, ..., f_m),$$

and

$$A \otimes_k k^{\mathrm{al}} \to k^{\mathrm{al}}[X_1, ..., X_n]/(f_1, ..., f_m).$$

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.

An affine algebraic space $(V, \mathcal{O}_V)$ such that $\Gamma(V, \mathcal{O}_V)$ is an affine k-algebra is called an ***affine algebraic variety over*** k. Thus, a ringed space $(V, \mathcal{O}_V)$ is an affine algebraic variety if $\Gamma(V, \mathcal{O}_V)$ is an affine k-algebra, $I(P)$ is a maximal ideal in $\Gamma(V, \mathcal{O}_V)$ for each $P \in V$, and $P \mapsto I(P)\colon V \to \mathrm{spm}(\Gamma(V, \mathcal{O}_V))$ is an isomorphism of ringed spaces.

Let

$$\begin{aligned} A &= k[X_1, ..., X_m]/\mathfrak{a}, \\ B &= k[Y_1, ..., Y_n]/\mathfrak{b}. \end{aligned}$$

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 a finitely generated k-algebra, and let $V = \mathrm{Spm}\, A$. For any field $K \supset k$, $K \otimes_k A$ is a finitely generated K-algebra, and hence we get a variety $V_K =_{\mathrm{df}} \mathrm{Spm}(K \otimes_k A)$ over K. We say that V_K has been obtained from V by ***extension of scalars*** or ***extension of the base field***. 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 $V_0 = \mathrm{Spm}(A_0)$ be an affine variety over k, and let $W = V(\mathfrak{b})$ be a closed subvariety of $V \stackrel{\text{def}}{=} V_{0,k^{\mathrm{al}}}$. 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 $A_0 \otimes_k k^{\mathrm{al}}$ 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.

The definition of the affine space $\mathbb{A}(E)$ attached to a vector space E works over any field.

Algebraic spaces; algebraic varieties.

An ***algebraic space over*** k is a ringed space $(V, \mathcal{O})$ for which there exists a finite covering (U_i) of V by open subsets such that $(U_i, \mathcal{O}|U_i)$ is an affine algebraic space over k for all i. A ***morphism of algebraic spaces*** (also called a ***regular map***) over k is a morphism of locally ringed spaces of k-algebras. An algebraic space is ***separated*** if for all pairs of morphisms of k-spaces $\alpha, \beta\colon Z \to V$, the subset of Z on which α and β agree is closed.

Similarly, an ***algebraic prevariety over*** k is a ringed space $(V, \mathcal{O})$ for which there exists a finite covering (U_i) of V by open subsets such that $(U_i, \mathcal{O}|U_i)$ is an affine algebraic variety over k for all i. A separated prevariety is called a ***variety***.

With any algebraic space V over k we can associate a reduced algebraic space V_{red} such that

- ◇ $V_{\mathrm{red}} = V$ as a topological space,
- ◇ for all open affines $U \subset V$, $\Gamma(U, \mathcal{O}_{V_{\mathrm{red}}})$ is the quotient of $\Gamma(U, \mathcal{O}_V)$ by its nilradical.

For example, if $V = \mathrm{Spm}\, k[X_1, \ldots, X_n]/\mathfrak{a}$, then $V_{\mathrm{red}} = \mathrm{Spm}\, k[X_1, \ldots, X_n]/\mathrm{rad}(\mathfrak{a})$. The identity map $V_{\mathrm{red}} \to V$ is a regular map. Any closed subset of V can be given a unique structure of a reduced algebraic space.

Products.

If A and B are finitely generated k-algebras, then $A \otimes_k B$ is a finitely generated k-algebra, and $\mathrm{Spm}(A \otimes_k B)$ is the product of $\mathrm{Spm}(A)$ and $\mathrm{Spm}(B)$ in the category of algebraic k-spaces, i.e., it has the correct universal property. This definition of product extends in a natural way to all algebraic spaces.

The tensor product of two reduced k-algebras may 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), $A \otimes_k k^{\mathrm{al}}$ and $B \otimes_k k^{\mathrm{al}}$ are affine k-algebras, and therefore so also is their tensor product over k^{al} (4.15); but

$$(A \otimes_k k^{\mathrm{al}}) \otimes_{k^{\mathrm{al}}} (k^{\mathrm{al}} \otimes_k B) \simeq ((A \otimes_k k^{\mathrm{al}}) \otimes_{k^{\mathrm{al}}} k^{\mathrm{al}}) \otimes_k B \simeq (A \otimes_k B) \otimes_k k^{\mathrm{al}}.$$

Thus, if V and W are algebraic (pre)varieties over k, then so also is their product.

Just as in (4.24, 4.25), the diagonal Δ is locally closed in $V \times V$, and it is closed if and only if V is separated.

Extension of scalars (extension of the base field).

Let V be an algebraic space over k, and let K be a field containing k. There is a natural way of defining an algebraic space V_K over K, said to be obtained from V by ***extension of scalars*** (or ***extension of the base field***): if V is a union of open affines, $V = \bigcup U_i$, then $V_K = \bigcup U_{i,K}$ and the $U_{i,K}$ are patched together the same way as the U_i. If K is algebraic over k, there is a morphism $(V_K, \mathcal{O}_{V_K}) \to (V, \mathcal{O}_V)$ that is universal: for any algebraic K-space W and morphism $(W, \mathcal{O}_W) \to (V, \mathcal{O}_V)$, there exists a unique regular map $W \to V_K$ giving a commutative diagram,

$$\begin{tikzcd} W \arrow[r, dotted, "\exists!"] \arrow[dr] & V_K \arrow[d] & K \arrow[d, dash] \\ & V & k. \end{tikzcd}$$

The dimension of an algebraic space or variety doesn't change under extension of scalars.

When V is an algebraic space (or variety) over k^{al} obtained from an algebraic space (or 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 an algebraic space (or variety) V_0 over k together with an isomorphism $\varphi\colon V \to V_{0,k^{\mathrm{al}}}$.

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 $j(E) \stackrel{\mathrm{def}}{=} \frac{1728(4a)^3}{-16(4a^3+27b^2)}$ 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).

Let V be an algebraic space over k. When k is perfect, V_{red} is an algebraic prevariety over k, but not necessarily otherwise, i.e., $(V_{\mathrm{red}})_{k^{\mathrm{al}}}$ need not be reduced. This shows that when k is not perfect, passage to the associated reduced algebraic space does not commute with extension of the base field: we may have

$$(V_{\mathrm{red}})_K \neq (V_K)_{\mathrm{red}}.$$

PROPOSITION 11.6. *Let V be an algebraic space over a field k. Then V is an algebraic prevariety if and only if $V_{k^{\frac{1}{p}}}$ is reduced, in which case V_K is reduced for all fields $K \supset k$.*

PROOF. Apply 11.4. □

Connectedness

A variety V over a field k is said to be ***geometrically connected*** if $V_{k^{\mathrm{al}}}$ is connected, in which case, V_Ω is connected for every field Ω containing k.

We first examine zero-dimensional varieties. Over $\mathbb{C}$, a zero-dimensional variety is nothing more than a finite set (finite disjoint union of copies $\mathbb{A}^0$). Over $\mathbb{R}$, a connected zero-dimensional variety V is either geometrically connected (e.g., $\mathbb{A}^0_{\mathbb{R}}$) or geometrically nonconnected (e.g., $V : X^2 + 1$; subvariety of $\mathbb{A}^1$), in which case $V(\mathbb{C})$ is a conjugate pair of complex points. Thus, one sees that to give a zero-dimensional variety over $\mathbb{R}$ is to give a finite set with an action of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$.

Similarly, a connected variety V over $\mathbb{R}$ may be geometrically connected, or it may decompose over $\mathbb{C}$ into a pair of conjugate varieties. Consider, for example, the following subvarieties of $\mathbb{A}^2$:

$L : Y + 1$ is a geometrically connected line over $\mathbb{R}$;

$L' : Y^2 + 1$ is connected over $\mathbb{R}$, but over $\mathbb{C}$ it decomposes as the pair of conjugate lines $Y = \pm i$.

Note that $\mathbb{R}$ is algebraically closed[2] in

$$\mathbb{R}[L] = \mathbb{R}[X, Y]/(Y + 1) \cong \mathbb{R}[X]$$

but not in

$$\mathbb{R}[L'] = \mathbb{R}[X, Y]/(Y^2 + 1) \cong \left(\mathbb{R}[Y]/(Y^2 + 1)\right)[X] \cong \mathbb{C}[X].$$

PROPOSITION 11.7. *A connected variety V over a field k is geometrically connected if and only if k is algebraically closed in $k(V)$.*

PROOF. This follows from the statement: let A be a finitely generated k-algebra such that A is an integral domain and $A \otimes_k k^{\mathrm{al}}$ is reduced; then $A \otimes k^{\mathrm{al}}$ is an integral domain if and only if k is algebraically closed in A (11.5). □

[2] A field k is algebraically closed in a k-algebra A if every $a \in A$ algebraic over k lies in k.

PROPOSITION 11.8. *To give a zero-dimensional variety V over a field k is to give (equivalently)*

(a) *a finite set E plus, for each $e \in E$, a finite separable field extension $\mathbb{Q}(e)$ of $\mathbb{Q}$, or*
(b) *a finite set S with a continuous[3] (left) action of $\Sigma \overset{\text{def}}{=} \mathrm{Gal}(k^{\mathrm{sep}}/k)$.[4]*

PROOF. Because each point of a variety is closed, the underlying topological space V of a zero-dimensional variety $(V, \mathcal{O}_V)$ is finite and discrete. For U an open affine in V, $A = \Gamma(U, \mathcal{O}_V)$ is a finite affine k-algebra. In particular, it is reduced, and so the intersection of its maximal ideals $\bigcap \mathfrak{m} = 0$. The Chinese remainder theorem shows that $A \simeq \prod A/\mathfrak{m}$. Each $A/\mathfrak{m}$ is a finite field extension of k, and it is separable because otherwise $(A/\mathfrak{m}) \otimes_k k^{\mathrm{al}}$ would not be reduced. The proves (a).

The set S in (b) is $V(k^{\mathrm{sep}})$ with the natural action of Σ. We can recover $(V, \mathcal{O}_V)$ from S as follows: let V be the set $\Sigma\backslash S$ of orbits endowed with the discrete topology, and, for $e = \Sigma s \in \Sigma\backslash S$, let $k(e) = (k^{\mathrm{sep}})^{\Sigma_s}$ where Σ_s is the stabilizer of s in Σ; then, for $U \subset V$, $\Gamma(U, \mathcal{O}_V) = \prod_{e \in U} k(e)$. □

PROPOSITION 11.9. *Given a variety V over k, there exists a map $f: V \to \pi$ from V to a zero-dimensional variety π such that, for all $e \in \pi$, the fibre V_e is a geometrically connected variety over $k(e)$.*

PROOF. Let π be the zero-dimensional variety whose underlying set is the set of connected components of V over $\mathbb{Q}$ and such that, for each $e = V_i \in \pi$, $k(e)$ is the algebraic closure of k in $\mathbb{Q}(V_i)$. Apply (11.7) to see that the obvious map $f: V \to \pi$ has the desired property. □

EXAMPLE 11.10. Let V be a connected variety over a k, and let k' be the algebraic closure of k in $k(V)$. The map $f: V \to \mathrm{Spm}\, k$ realizes V as a geometrically connected variety over k. Conversely, for a geometrically connected variety $f: V \to \mathrm{Spm}\, k'$ over a finite extension of k, the composite of f with $\mathrm{Spm}\, k' \to \mathrm{Spm}\, k$ realizes V as a variety over k (connected, but not geometrically connected if $k' \neq k$).

EXAMPLE 11.11. Let $f: V \to \pi$ be as in (11.9). When we regard π as a set with an action of Σ, then its points are in natural one-to-one correspondence with the connected components of $V_{k^{\mathrm{sep}}}$ and its Σ-orbits are in natural one-to-one correspondence with the connected components of V. Let $e \in \pi$ and let $V' = f_{k^{\mathrm{sep}}}^{-1}(e)$ — it is a connected component of $V_{k^{\mathrm{sep}}}$. Let Σ_e be the stabilizer of e; then V' arises from a geometrically connected variety over $k(e) \overset{\text{def}}{=} (k^{\mathrm{sep}})^{\Sigma_e}$.

ASIDE 11.12. Proposition 11.9 is a special case of Stein factorization (10.30).

[3]This means that the action factors through the quotient of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ by an open subgroup (all open subgroups of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ are of finite index, but not all subgroups of finite index are open).

[4]The cognoscente will recognize this as Grothendieck's way of expressing Galois theory over $\mathbb{Q}$.

Fibred products

Fibred products exist in the category of algebraic spaces. For example, if $R \to A$ and $R \to B$ are homomorphisms of finitely generated k-algebras, then $A \otimes_R B$ is a finitely generated k-algebras and

$$\mathrm{Spm}(A) \times_{\mathrm{Spm}(R)} \mathrm{Spm}(B) = \mathrm{Spm}(A \otimes_R B).$$

For algebraic prevarieties, the situation is less satisfactory. Consider a variety S and two regular maps $V \to S$ and $W \to S$. Then $(V \times_S W)_{\mathrm{red}}$ is the fibred product of V and W over S in the category of reduced algebraic k-spaces. When k is perfect, this is a variety, but not necessarily otherwise. Even when the fibred product exists in the category of algebraic prevarieties, it is anomolous. The correct object is the fibred product in the category of algebraic spaces which, as we have observed, may no longer be an algebraic variety. This is one reason for introducing algebraic spaces.

Consider the fibred product:

$$\begin{tikzcd}
\mathbb{A}^1 \arrow[d, "x\mapsto x^p"'] & \mathbb{A}^1 \times_{\mathbb{A}^1} \{a\} \arrow[l] \arrow[d] \\
\mathbb{A}^1 & \{a\} \arrow[l]
\end{tikzcd}$$

In the category of algebraic varieties, $\mathbb{A}^1 \times_{\mathbb{A}^1} \{a\}$ is a single point if a is a pth power in k and is empty otherwise; in the category of algebraic spaces, $\mathbb{A}^1 \times_{\mathbb{A}^1} \{a\} = \mathrm{Spm}\, k[T]/(T^p - a)$, which can be thought of as a p-fold point (point with multiplicity p).

The points on an algebraic space

Let V be an algebraic space over k. A ***point of V with coordinates in k*** (or a ***point of V rational over k***, or a ***k-point of V***) is a morphism $\mathrm{Spm}\, k \to V$. For example, if V is affine, say $V = \mathrm{Spm}(A)$, 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, if V is the affine algebraic space 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 $V = \mathrm{Spm}(A)$, we set

$$V(R) = \mathrm{Hom}_{k\text{-alg}}(A, R).$$

Again, if

$$A = k[X_1, ..., X_n]/(f_1, ..., f_m),$$

then

$$V(R) = \{(a_1, ..., a_n) \in R^n \mid f_i(a_1, ..., a_n) = 0, \quad i = 1, 2, ..., m\}.$$

What is the relation between the elements of V and the elements of $V(k)$? Suppose V is affine, say $V = \mathrm{Spm}(A)$. 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 $k(v)$ for the residue field $\mathcal{O}_v/\mathfrak{m}_v$. Then $k(v)$ is a finite extension of k, and we call the degree of $k(v)$ 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.

Now assume k to be perfect. The k^{al}-rational points of V with image $v \in V$ are in one-to-one correspondence with the k-homomorphisms $k(v) \to k^{\mathrm{al}}$ — therefore, there are exactly $\deg(v)$ of them, and they form a single orbit under the action of $\mathrm{Gal}(k^{\mathrm{al}}/k)$. The natural map $V_{k^{\mathrm{al}}} \to V$ realizes V (as a topological space) as the quotient of $V_{k^{\mathrm{al}}}$ by the action of $\mathrm{Gal}(k^{\mathrm{al}}/k)$ — there is a one-to-one correspondence between the set of points of V and 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 $\mathfrak{a} = (f_1, \ldots, f_r)$. Let $d = \dim V$. The ***singular locus*** V_{sing} of V is defined by the vanishing of the $(n-d) \times (n-d)$ minors of the matrix

$$\mathrm{Jac}(f_1, f_2, \ldots, f_r) = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} & \cdots & \frac{\partial f_1}{\partial x_r} \\ \frac{\partial f_2}{\partial x_1} & & & \\ \vdots & & & \\ \frac{\partial f_r}{\partial x_1} & & & \frac{\partial f_r}{\partial x_r} \end{pmatrix}.$$

We say that v is ***nonsingular*** if some $(n-d) \times (n-d)$ minor doesn't vanish at v. We say V is ***nonsingular*** if its singular locus is empty (i.e., V_{sing} is the empty variety or, equivalently, $V_{\mathrm{sing}}(k^{\mathrm{al}})$ is empty) . Obviously V is nonsingular $\iff$ $V_{k^{\mathrm{al}}}$ is nonsingular; also the formation of V_{sing} commutes with extension of scalars. Therefore, if V is a variety, V_{sing} is a proper closed subvariety of V (Theorem 5.18).

THEOREM 11.13. *Let V be an algebraic space over k.*

(a) *If $P \in V$ is nonsingular, then $\mathcal{O}_P$ is regular.*
(b) *If all points of V are nonsingular, then V is a nonsingular algebraic variety.*

PROOF. (a) Similar arguments to those in chapter 5 show that $\mathfrak{m}_P$ can be generated by $\dim V$ elements, and $\dim V$ is the Krull dimension of $\mathcal{O}_P$.

(b) It suffices to show that V is geometrically reduced, and so we may replace k with its algebraic closure. From (a), each local ring $\mathcal{O}_P$ is regular, but regular local rings are integral domains (CA 16.3).[5] □

[5]One shows that if R is regular, then the associated graded ring $\bigoplus \mathfrak{m}^i/\mathfrak{m}^{i+1}$ is a polynomial ring in $\dim R$ symbols. Using this, one see that if $xy = 0$ in R, then one of x or y lies in $\bigcap_n \mathfrak{m}^n$, which is zero by the Krull intersection theorem (1.8).

THEOREM 11.14. *The converse to (a) of the theorem fails. For example, let k be a field of characteristic $p \neq 0, 2$, and let a be a nonzero element of k that is not a p^{th} power. Then $f(X, Y) = Y^2 + X^p - a$ is irreducible, and remains irreducible over k^{al}. Therefore,*

$$A = k[X, Y]/(f(X, Y)) = k[x, y]$$

is an affine k-algebra, and we let V be the curve $\operatorname{Spm} A$. One checks that V is normal, and hence is regular by Atiyah and MacDonald 1969, 9.2. However,

$$\frac{\partial f}{\partial X} = 0, \quad \frac{\partial f}{\partial Y} = 2Y,$$

and so $(a^{\frac{1}{p}}, 0) \in V_{\text{sing}}(k^{\text{al}})$: the point P in V corresponding to the maximal ideal (y) of A is singular even though $\mathcal{O}_P$ is regular.

The relation between "nonsingular" and "regular" is examined in detail in: Zariski, O., The Concept of a Simple Point of an Abstract Algebraic Variety, Transactions of the American Mathematical Society, Vol. 62, No. 1. (Jul., 1947), pp. 1-52.

Separable points

Let V be an algebraic variety over k. Call a point $P \in V$ ***separable*** if $k(P)$ is a separable extension of k.

PROPOSITION 11.15. *The separable points are dense in V; in particular, $V(k)$ is dense in V if k is separably closed.*

PROOF. It suffices to prove this for each irreducible component of V, and we may replace an irreducible component of V by any variety birationally equivalent with it (4.32). Therefore, it suffices to prove it for a hypersurface H in $\mathbb{A}^{d+1}$ defined by a polynomial $f(X_1, \ldots, X_{d+1})$ that is separable when regarded as a polynomial in X_{d+1} with coefficients in $k(X_1, \ldots, X_d)$ (4.34, 11.3). Then $\frac{\partial f}{\partial X_{d+1}} \neq 0$ (as a polynomial in $X_1, \ldots, X_d$), and on the nonempty open subset $D(\frac{\partial f}{\partial X_{d+1}})$ of $\mathbb{A}^d$, $f(a_1, \ldots, a_d, X_{d+1})$ will be a separable polynomial. The points of H lying over points of U are separable. □

Tangent cones

DEFINITION 11.16. The ***tangent cone*** at a point P on an algebraic space V is $\operatorname{Spm}(\operatorname{gr}(\mathcal{O}_P))$.

When V is a variety over an algebraically closed field, this agrees with the definition in chapter 5, except that there we didn't have the correct language to describe it — even in that case, the tangent cone may be an algebraic space (not an algebraic variety).

Projective varieties.

Everything in this chapter holds, essentially unchanged, when k is allowed to be an arbitrary field.

If $V_{k^{\text{al}}}$ is a projective variety, then so also is V. The idea of the proof is the following: to say that V is projective means that it has an ample divisor; but a divisor D on V is ample if $D_{k^{\mathrm{al}}}$ is ample on $V_{k^{\mathrm{al}}}$; by assumption, there is a divisor D on $V_{k^{\mathrm{al}}}$ that is ample; any multiple of the sum of the Galois conjugates of D will also be ample, but some such divisor will arise from a divisor on V.

Complete varieties.

Everything in this chapter holds unchanged when k is allowed to be an arbitrary field.

Normal varieties; Finite maps.

As noted in (8.15), the Noether normalization theorem requires a different proof when the field is finite. Also, as noted earlier in this chapter, one needs to be careful with the definition of fibre. For example, one should define a regular map $\varphi\colon V \to W$ to be quasifinite if the fibres of the map of sets $V(k^{\mathrm{al}}) \to W(k^{\mathrm{al}})$ are finite.

Otherwise, k can be allowed to be arbitrary.

Dimension theory

The dimension of a variety V over an arbitrary field k can be defined as in the case that k is algebraically closed. The dimension of V is unchanged by extension of the base field. Most of the results of this chapter hold for arbitrary base fields.

Regular maps and their fibres

Again, the results of this chapter hold for arbitrary fields provided one is careful with the notion of a fibre.

Algebraic groups

We now define an ***algebraic group*** to be an algebraic *space* G together with regular maps

$$\mathrm{mult}\colon G \times G, \quad \mathrm{inverse}\colon G \to G, \quad e\colon \mathbb{A}^0 \to G$$

making $G(R)$ into a group in the usual sense for all k-algebras R.

THEOREM 11.17. *Let G be an algebraic group over k.*

(a) *If G is connected, then it is geometrically connected.*
(b) *If G is geometrically reduced (i.e., a variety), then it is nonsingular.*
(c) *If k is perfect and G is reduced, then it is geometrically reduced.*
(d) *If k has characteristic zero, then G is geometrically reduced (hence nonsingular).*

PROOF. (a) The existence of e shows that k is algebraically closed in $k(G)$. Therefore (a) follows from (11.7).

(b) It suffices to show that $G_{k^{\mathrm{al}}}$ is nonsingular, but this we did in (5.20).

(c) As $k = k^{\frac{1}{p}}$, this follows from (11.6).

(d) See my notes, Algebraic Groups and Arithmetic Groups, Theorem 2.31. □

Exercises

11-1. Show directly that, up to isomorphism, the curve $X^2 + Y^2 = 1$ over $\mathbb{C}$ has exactly two models over $\mathbb{R}$.

Chapter 12

Divisors and Intersection Theory

In this chapter, k is an arbitrary field.

Divisors

Recall that a normal ring is an integral domain that is integrally closed in its field of fractions, and that 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 12.1. Let V be a projective variety, say, defined by a homogeneous ring R. When R is normal, V is said to be ***projectively normal***. If V is projectively normal, then it 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 $\mathrm{Div}(V)$ 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 by 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 $V = \mathrm{Spm}(R)$. 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, $V = \bigcup Z_i$ (see 9.2) and $\mathrm{ord}_Z(f) = 0$ unless Z is one of the Z_i.

The map
$$f \mapsto \mathrm{div}(f) \colon k(V)^\times \to \mathrm{Div}(V)$$
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*** $\mathrm{Pic}(V)$ of V is defined to be the group of divisors on V modulo principal divisors. (Later, we shall define $\mathrm{Pic}(V)$ 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 12.2. 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 prime 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 9.13).

If $D|_U = \mathrm{div}(f)$, 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 $D_1, \ldots, D_n$ be effective divisors on V. We say that $D_1, \ldots, D_n$ ***intersect properly*** at $P \in |D_1| \cap \ldots \cap |D_n|$ if P is an isolated point of the intersection. In this case, we define

$$(D_1 \cdot \ldots \cdot D_n)_P = \dim_k \mathcal{O}_P/(f_1, \ldots, f_n)$$

where f_i is a local equation for D_i near P. The hypothesis on P implies that this is finite.

EXAMPLE 12.3. 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 $D_1, \ldots, D_n$ ***intersect properly*** if they do so at every point of intersection of their supports; equivalently, if $|D_1| \cap \ldots \cap |D_n|$ is a finite set. We then define the intersection number

$$(D_1 \cdot \ldots \cdot D_n) = \sum_{P \in |D_1| \cap \ldots \cap |D_n|} (D_1 \cdot \ldots \cdot D_n)_P.$$

EXAMPLE 12.4. 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 9.2 to see that this does define a divisor on W; if the image of α is disjoint from $|D|$, then $\alpha^* D = 0$.)

EXAMPLE 12.5. 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 12.6 (ADDITIVITY). *Let $D_1, \ldots, D_n, D$ be divisors on V. If $(D_1 \cdot \ldots \cdot D_n)_P$ and $(D_1 \cdot \ldots \cdot D)_P$ are both defined, then so also is $(D_1 \cdot \ldots \cdot D_n + D)_P$, and*

$$(D_1 \cdot \ldots \cdot D_n + D)_P = (D_1 \cdot \ldots \cdot D_n)_P + (D_1 \cdot \ldots \cdot D)_P.$$

PROOF. One writes some exact sequences. See Shafarevich 1994, IV.1.2. □

Note that in intersection theory, unlike every other branch of mathematics, we add first, and then multiply.

Since every divisor is the difference of two effective divisors, Lemma 12.1 allows us to extend the definition of $(D_1 \cdot \ldots \cdot D_n)$ to all divisors intersecting properly (not just effective divisors).

LEMMA 12.7 (INVARIANCE UNDER LINEAR EQUIVALENCE). *Assume V is complete. If $D_n \sim D_n'$, then*

$$(D_1 \cdot \ldots \cdot D_n) = (D_1 \cdot \ldots \cdot D_n').$$

PROOF. By additivity, it suffices to show that $(D_1 \cdot \ldots \cdot D_n) = 0$ 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 12.5 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 12.8. *For any n divisors $D_1, \ldots, D_n$ on an n-dimensional variety, there exists n divisors $D_1', \ldots, D_n'$ 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 $D_1', \ldots, D_n'$ as in the lemma, and set

$$(D_1 \cdot \ldots \cdot D_n) = (D_1' \cdot \ldots \cdot D_n').$$

EXAMPLE 12.9. 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

$$(\Delta \cdot \Gamma_\alpha) = \mathrm{Tr}(\alpha|H^0(C,\mathbb{Q}) - \mathrm{Tr}(\alpha|H^1(C,\mathbb{Q}) + \mathrm{Tr}(\alpha|H^2(C,\mathbb{Q}).$$

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 12.10. *Let $\alpha \colon W \to V$ be a finite map between nonsingular varieties. For any divisors $D_1, \ldots, D_n$ 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 $D_1, \ldots, D_n$ are principal with equations $f_1, \ldots, f_n$ 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 $\mathfrak{a} = (f_1, \ldots, f_n)$. Set $S = A \smallsetminus \mathfrak{m}_P$; then

$$S^{-1}A/S^{-1}\mathfrak{a} = S^{-1}(A/\mathfrak{a}) = A/\mathfrak{a}$$

because $A/\mathfrak{a}$ is already local. Hence

$$(D_1 \cdot \ldots \cdot D_n)_P = \dim A/(f_1, \ldots, f_n).$$

Similarly,

$$(\alpha^* D_1 \cdot \ldots \cdot \alpha^* D_n)_P = \dim B/(f_1 \circ \alpha, \ldots, f_n \circ \alpha).$$

But B is a free A-module of rank d, and

$$A/(f_1, \ldots, f_n) \otimes_A B = B/(f_1 \circ \alpha, \ldots, f_n \circ \alpha).$$

Therefore, as A-modules, and hence as k-vector spaces,

$$B/(f_1 \circ \alpha, \ldots, f_n \circ \alpha) \approx (A/(f_1, \ldots, f_n))^d$$

which proves the formula. □

EXAMPLE 12.11. 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 $Z_1 \cap Z_2$. Then

$$\dim\ Z_1 + \dim\ Z_2 \leq \dim\ V + \dim\ W,$$

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

$$\chi^{\mathcal{O}}(\mathcal{O}/\mathfrak{p}_1, \mathcal{O}/\mathfrak{p}_2) = \sum_{i=0}^{\dim V} (-1)^i \dim_k(\mathrm{Tor}_i^{\mathcal{O}}(\mathcal{O}/\mathfrak{p}_1, \mathcal{O}/\mathfrak{p}_2))$$

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

$$(Z_1 \cdot Z_2)_W = mW, \quad m = \chi^{\mathcal{O}}(\mathcal{O}/\mathfrak{p}_1, \mathcal{O}/\mathfrak{p}_2).$$

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 $\mathrm{div}(f)$ is a cycle of codimension r on V (since W may not be normal, the definition of $\mathrm{div}(f)$ 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 finding algebraic cycles on varieties other than the obvious ones (divisors, intersections of divisors,...). However, there are many deep conjectures concerning them, due to Beilinson, Bloch, Murre, and others.

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 12.12. (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.

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.

Exercises

You may assume the characteristic is zero if you wish.

12-1. Let $V = V(F) \subset \mathbb{P}^n$, where F is a homogeneous polynomial of degree δ without multiple factors. Show that V has degree δ according to the definition in the notes.

12-2. Let C be a curve in $\mathbb{A}^2$ defined by an irreducible polynomial $F(X, Y)$, and assume C passes through the origin. Then $F = F_m + F_{m+1} + \cdots$, $m \geq 1$, with F_m the homogeneous part of F of degree m. Let $\sigma: W \to \mathbb{A}^2$ be the blow-up of $\mathbb{A}^2$ at $(0, 0)$, and let C' be the closure of $\sigma^{-1}(C \smallsetminus (0, 0))$. Let $Z = \sigma^{-1}(0, 0)$. Write $F_m = \prod_{i=1}^{s}(a_i X + b_i Y)^{r_i}$, with the $(a_i : b_i)$ being distinct points of $\mathbb{P}^1$, and show that $C' \cap Z$ consists of exactly s distinct points.

12-3. Find the intersection number of $D_1: Y^2 = X^r$ and $D_2: Y^2 = X^s$, $r > s > 2$, at the origin.

12-4. Find $\mathrm{Pic}(V)$ when V is the curve $Y^2 = X^3$.

Chapter 13

Coherent Sheaves; Invertible Sheaves

In this chapter, k is an arbitrary field.

Coherent sheaves

Let $V = \operatorname{Spm} A$ 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 $f \in A$,

$$\Gamma(D(f), \mathcal{M}) = M_f \quad (= A_f \otimes_A M).$$

Such an $\mathcal{O}_V$-module $\mathcal{M}$ 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 of rank n 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 $V = \operatorname{Spm}(A)$, 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 (1.3) shows that

$$\mathcal{M}(v) = 0 \Rightarrow \mathcal{M}_v = 0.$$

The ***support*** of a coherent sheaf $\mathcal{M}$ is

$$\operatorname{Supp}(\mathcal{M}) = \{v \in V \mid \mathcal{M}(v) \neq 0\} = \{v \in V \mid \mathcal{M}_v \neq 0\}.$$

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

$$\operatorname{Supp}(\mathcal{M}) = V(\mathfrak{a}).$$

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 13.1. *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 $x_1, \ldots, x_n$ be elements of M whose images in $M/\mathfrak{m}M$ form a basis for it over $\kappa(v)$. Consider the map

$$\gamma\colon A^n \to M, \quad (a_1, \ldots, a_n) \mapsto \sum a_i x_i.$$

Its 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 13.2. *Let A be an affine k-algebra. Then*

$$\bigcap \mathfrak{m} = 0 \text{ (intersection of all maximal ideals in } A\text{).}$$

PROOF. When k is algebraically closed, we showed (4.13) that this follows from the strong Nullstellensatz. In the general case, consider a maximal ideal $\mathfrak{m}$ of $A \otimes_k k^{\mathrm{al}}$. Then

$$A/(\mathfrak{m} \cap A) \hookrightarrow (A \otimes_k k^{\mathrm{al}})/\mathfrak{m} = k^{\mathrm{al}},$$

and so $A/\mathfrak{m} \cap A$ 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 $A \otimes k^{\mathrm{al}}$ is in all maximal ideals of A, 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 13.4 below). For a such a U, one writes $U = \bigcup U_i$ 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:

$$[\mathcal{L}]\cdot[\mathcal{L}'] \stackrel{\text{def}}{=} [\mathcal{L}\otimes\mathcal{L}'].$$

The product structure is associative and commutative (because tensor products are associative and commutative, up to 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 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***, $\mathrm{Pic}(V)$, 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 $\mathrm{Pic}(V)$.

PROPOSITION 13.3. *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 7.5 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

$$s_1 \colon \mathcal{O}_V \to \mathcal{L}, \quad s_2 \colon \mathcal{O}_V \to \mathcal{L}^\vee.$$

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 and irreducible. 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

$$\operatorname{Div}(V) \to \operatorname{Pic}(V), \quad D \mapsto [\mathcal{L}(D)],$$

which is zero on the principal divisors.

EXAMPLE 13.4. 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, $\Gamma(V, \mathcal{L}(D) \otimes \mathcal{L}(D)) \neq \Gamma(V, \mathcal{L}(D)) \otimes \Gamma(V, \mathcal{L}(D))$.

PROPOSITION 13.5. *For an irreducible nonsingular variety, the map $D \mapsto [\mathcal{L}(D)]$ defines an isomorphism*

$$\mathrm{Div}(V)/\mathrm{PrinDiv}(V) \to \mathrm{Pic}(V).$$

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) $\mathrm{div}(g) + D \geq 0$ (on the whole of V);
(b) if $\mathrm{div}(f) + D \geq 0$ 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 $D \geq \mathrm{div}(-g)$ (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 $\mathrm{div}(-f) \leq \mathrm{div}(g)$ on U, so that $D|U + \mathrm{div}(g) \geq 0$. Since the U's cover V, together with (a) this implies that $D = \mathrm{div}(-g)$.

(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 13.6. Suppose V is affine, say $V = \mathrm{Spm}\, A$. 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, Algèbre Commutative, 1961–83, 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 13.7. Quite a lot is known about $\mathrm{Pic}(V)$, 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

$$0 \to P(k) \to \mathrm{Pic}(V) \to \mathrm{NS}(V) \to 0$$

where $\mathrm{NS}(V)$ 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 homomorphism $A \to B$ 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 13.8. (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 $\mathcal{L}$, $\alpha^*(\mathcal{L}^{-1}) \simeq (\alpha^*\mathcal{L})^{-1}$.*

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. □

See Kleiman.

Principal bundles

To be added.

Chapter 14

Differentials (Outline)

In this subsection, 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 §5) that a k-derivation is a k-linear map $D: A \to M$ satisfying Leibniz's rule:

$$D(fg) = f \circ Dg + g \circ Df, \quad \text{all } f, g \in A.$$

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 has the following universal property: for any k-derivation $D: A \to M$, there is a unique k-linear map $\alpha: \Omega^1_{A/k} \to M$ such that $D = \alpha \circ d$,

$$\begin{tikzcd} A \arrow[r, "d"] \arrow[dr, "D"'] & \Omega^1 \arrow[d, dotted, "\exists!\ k\text{-linear}"] \\ & M \end{tikzcd}$$

EXAMPLE 14.1. 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

$$df = \sum \frac{\partial f}{\partial X_i} dX_i.$$

EXAMPLE 14.2. 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:

$$df = 0 \text{ for all } f \in \mathfrak{a}.$$

PROPOSITION 14.3. *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 $\Omega^n_{V/k}(U) = \bigwedge^n \Omega^1_{A/k}$ whenever $U = \operatorname{Spm} A$ 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 14.4. 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 $D(y) \cap D(3x^2 + a)$. Since $E = D(y) \cup D(3x^2 + a)$, 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. 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.

In general, 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.

PROPOSITION 14.5. *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 14.6 (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 1999, III.4.

Chapter 15

Algebraic Varieties over the Complex Numbers

This is only an outline.

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 topology;
(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 two propositions are a little surprising.

PROPOSITION 15.1. *If a nonsingular variety is connected for the Zariski topology, then it is connected for the complex topology.*

Consider, for example, $\mathbb{A}^1$. Then, certainly, it is connected for both the Zariski topology (that for which the nonempty open subsets are those that omit only finitely many points) and the complex topology (that for which X is homeomorphic to $\mathbb{R}^2$). When we remove a circle from X, it becomes disconnected for the complex topology, but remains connected for the Zariski topology. This doesn't contradict the theorem, because $\mathbb{A}^1_{\mathbb{C}}$ with a circle removed is not an algebraic variety.

Let X be a connected nonsingular (hence irreducible) curve. We prove that it is connected for the complex topology. Removing or adding a finite number of points to X will not change whether it is connected for the complex topology, and so we can assume that X is projective. Suppose X is the disjoint union of two nonempty open (hence closed) sets X_1 and X_2. According to the Riemann-Roch theorem (14.6), there exists a nonconstant rational function f on X having poles only in X_1. Therefore, its restriction to X_2 is holomorphic. Because X_2 is compact, f is constant on each connected component of X_2 (Cartan 1963[1],

[1] Cartan, H., Elementary Theory of Analytic Functions of One or Several Variables, Addison-Wesley, 1963.

VI.4.5) say, $f(z) = a$ on some infinite connected component. Then $f(z) - a$ has infinitely many zeros, which contradicts the fact that it is a rational function.

The general case can be proved by induction on the dimension (Shafarevich 1994, VII.2).

PROPOSITION 15.2. *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. Mumford 1999, I 10, Corollary 1, p60. □

For example, if U is an open dense subset of a closed subset Z of V (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 15.3. *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. Mumford 1999, I 10, Theorem 2, p60. □

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 15.4. *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. Shafarevich 1994, VIII 3.1, Theorem 1. □

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 $g > 1$, 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 in the sense of Artin***.[2] 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.[3]

One way to show that a complex manifold is algebraic is to embed it into projective space.

[2]Perhaps these should be called ***algebraic orbispaces*** (in analogy with manifolds and orbifolds).

[3]Artin, Michael. Algebraic spaces. Whittemore Lectures given at Yale University, 1969. Yale Mathematical Monographs, 3. Yale University Press, New Haven, Conn.-London, 1971. vii+39 pp.

Knutson, Donald. Algebraic spaces. Lecture Notes in Mathematics, Vol. 203. Springer-Verlag, Berlin-New York, 1971. vi+261 pp.

THEOREM 15.5. *Any closed analytic submanifold of* $\mathbb{P}^n$ *is algebraic.*

PROOF. See Shafarevich 1994, VIII 3.1, in the nonsingular case. □

COROLLARY 15.6. *Any holomorphic map from one projective algebraic variety to a second projective algebraic variety is algebraic.*

PROOF. Let $\varphi: V \to W$ 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 lattice 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 1999, I.10.

Shafarevich 1994, Book 3.

Chapter 16

Descent Theory

Consider fields $k \subset \Omega$. A variety V over k defines a variety V_Ω over Ω by extension of the base field (§11). Descent theory attempts to answer the following question: what additional structure do you need to place on a variety over Ω, or regular map of varieties over Ω, to ensure that it comes from k?

In this chapter, we shall make free use of the axiom of choice (usually in the form of Zorn's lemma).

Models

Let $\Omega \supset k$ be fields, and let V be a variety over Ω. Recall (p175) that a model of V over k (or a ***k-structure*** on V) is a variety V_0 over k together with an isomorphism $\varphi\colon V \to V_{0\Omega}$. Recall also that a variety over Ω need not have a model over k, and when it does it typically will have many nonisomorphic models.

Consider an affine variety. An embedding $V \hookrightarrow \mathbb{A}^n_\Omega$ defines a model of V over k if $I(V)$ is generated by polynomials in $k[X_1,\ldots,X_n]$, because then $I_0 \overset{\text{def}}{=} I(V) \cap k[X_1,\ldots,X_n]$ is a radical ideal, $k[X_1,\ldots,X_n]/I_0$ is an affine k-algebra, and $V(I_0) \subset \mathbb{A}^n_k$ is a model of V. Moreover, every model (V_0,φ) arises in this way, because every model of an affine variety is affine. However, different embeddings in affine space will usually give rise to different models. Similar remarks apply to projective varieties.

Note that the condition that $I(V)$ be generated by polynomials in $k[X_1,\ldots,X_n]$ is stronger than asking that V be the zero set of some polynomials in $k[X_1,\ldots,X_n]$. For example, let $V = V(X+Y+\alpha)$ where α is an element of Ω such that $\alpha^p \in k$ but $\alpha \notin k$. Then V is the zero set of the polynomial $X^p + Y^p + \alpha^p$, which has coefficients in k, but $I(V) = (X+Y+\alpha)$ is not generated by polynomials in $k[X,Y]$.

Fixed fields

Let $\Omega \supset k$ be fields, and let Γ be the group $\mathrm{Aut}(\Omega/k)$ of automomorphisms of Ω (as an abstract field) fixing the elements of k. Define the ***fixed field*** Ω^Γ of Γ to be

$$\{a \in \Omega \mid \sigma a = a \text{ for all } \sigma \in \Gamma\}.$$

PROPOSITION 16.1. *The fixed field of Γ equals k in each of the following two cases:*

(a) *Ω is a Galois extension of k (possibly infinite);*

(b) *Ω is a separably closed field and k is perfect.*

PROOF. (a) See FT 7.8.

(b) See FT 8.23. □

REMARK 16.2. (a) The proof of Proposition 16.1 definitely requires the axiom of choice. For example, it is known that every measurable homomorphism of Lie groups is continuous, and so any measurable automorphism of $\mathbb{C}$ is equal to the identity map or to complex conjugation. Therefore, without the axiom of choice, $\Gamma \overset{\text{def}}{=} \mathrm{Aut}(\mathbb{C}/\mathbb{Q})$ has only two elements, and $\mathbb{C}^{\Gamma} = \mathbb{R}$.

(b) Suppose that Ω is algebraically closed and k is not perfect. Then k has characteristic $p \neq 0$ and Ω contains an element α such that $\alpha \notin k$ but $\alpha^p = a \in k$. As α is the unique root of $X^p - a$, every automorphism of Ω fixing k also fixes α, and so $\Omega^{\Gamma} \neq k$.

The ***perfect closure*** of k in Ω is the subfield

$$k^{p^{-\infty}} = \{\alpha \in \Omega \mid \alpha^{p^n} \in k \text{ for some } n\}$$

of Ω. Then $k^{p^{-\infty}}$ is purely inseparable over k, and when Ω is algebraically closed, it is the smallest perfect subfield of Ω containing k.

COROLLARY 16.3. *If Ω is separably closed, then Ω^{Γ} is a purely inseparable algebraic extension of k.*

PROOF. When k has characteristic zero, $\Omega^{\Gamma} = k$, and there is nothing to prove. Thus, we may suppose that k has characteristic $p \neq 0$. Choose an algebraic closure Ω^{al} of Ω, and let $k^{p^{-\infty}}$ be the perfect closure of k in Ω^{al}. As Ω^{al} is purely inseparable over Ω, every element σ of Γ extends uniquely to an automorphism $\tilde{\sigma}$ of Ω^{al}: let $\alpha \in \Omega^{\mathrm{al}}$ and let $\alpha^{p^n} \in \Omega$; then $\tilde{\sigma}(\alpha)$ is the unique root of $X^{p^n} - \sigma(\alpha^{p^n})$ in Ω. The action of Γ on Ω^{al} identifies it with $\mathrm{Aut}(\Omega^{\mathrm{al}}/k^{p^{-\infty}})$. According to the proposition, $(\Omega^{\mathrm{al}})^{\Gamma} = k^{p^{-\infty}}$, and so

$$k^{p^{-\infty}} \supset \Omega^{\Gamma} \supset k.$$ □

Descending subspaces of vector spaces

In this subsection, $\Omega \supset k$ are fields such that k is the fixed field of $\Gamma = \mathrm{Aut}(\Omega/k)$.

Let V be a k-subspace of an Ω-vector space $V(\Omega)$ such that the map

$$c \otimes v \mapsto cv \colon \Omega \otimes_k V \to V(\Omega)$$

is an isomorphism. Equivalent conditions: V is the k-span of an Ω-basis for $V(\Omega)$; every k-basis for V is an Ω-basis for $V(\Omega)$. The group Γ acts on $\Omega \otimes_k V$ through its action on Ω:

$$\sigma(\textstyle\sum c_i \otimes v_i) = \sum \sigma c_i \otimes v_i, \quad \sigma \in \Gamma, \quad c_i \in \Omega, \quad v_i \in V. \tag{26}$$

Correspondingly, there is a unique action of Γ on $V(\Omega)$ fixing the elements of V and such that each $\sigma \in \Gamma$ acts σ-linearly:

$$\sigma(cv) = \sigma(c)\sigma(v) \text{ all } \sigma \in \Gamma, c \in \Omega, v \in V(\Omega). \tag{27}$$

LEMMA 16.4. *The following conditions on a subspace W of $V(\Omega)$ are equivalent:*

(a) *$W \cap V$ spans W;*
(b) *$W \cap V$ contains an Ω-basis for W;*
(c) *the map $\Omega \otimes_k (W \cap V) \to W$, $c \otimes v \mapsto cv$, is an isomorphism.*

PROOF. (a) $\implies$ (b,c) A k-linearly independent subset of V is Ω-linearly independent in $V(\Omega)$. Therefore, if $W \cap V$ spans W, then any k-basis $(e_i)_{i\in I}$ for $W \cap V$ will be an Ω-basis for W. Moreover, $(1 \otimes e_i)_{i\in I}$ will be an Ω-basis for $\Omega \otimes_k (W \cap V)$, and since the map $\Omega \otimes_k (W \cap V) \to W$ sends $1 \otimes e_i$ to e_i, it is an isomorphism.

(c) $\implies$ (a), (b) $\implies$ (a). Obvious. □

LEMMA 16.5. *For any k-vector space V, $V = V(\Omega)^\Gamma$.*

PROOF. Let $(e_i)_{i\in I}$ be a k-basis for V. Then $(1 \otimes e_i)_{i\in I}$ is an Ω-basis for $\Omega \otimes_k V$, and $\sigma \in \Gamma$ acts on $v = \sum c_i \otimes e_i$ according to the rule (26). Thus, v is fixed by Γ if and only if each c_i is fixed by Γ and so lies in k. □

LEMMA 16.6. *Let V be a k-vector space, and let W be a subspace of $V(\Omega)$ stable under the action of Γ. If $W^\Gamma = 0$, then $W = 0$.*

PROOF. Suppose $W \neq 0$. As V contains an Ω-basis for $V(\Omega)$, every nonzero element w of W can be expressed in the form

$$w = c_1 e_1 + \cdots + c_n e_n, \quad c_i \in \Omega \smallsetminus \{0\}, \quad e_i \in V, \quad n \geq 1.$$

Choose w to be a nonzero element for which n takes its smallest value. After scaling, we may suppose that $c_1 = 1$. For $\sigma \in \Gamma$, the element

$$\sigma w - w = (\sigma c_2 - c_2)e_2 + \cdots + (\sigma c_n - c_n)e_n$$

lies in W and has at most $n-1$ nonzero coefficients, and so is zero. Thus, $w \in W^\Gamma = \{0\}$, which is a contradiction. □

PROPOSITION 16.7. *A subspace W of $V(\Omega)$ is of the form $W = \Omega W_0$ for some k-subspace W_0 of V if and only if it is stable under the action of Γ.*

PROOF. Certainly, if $W = \Omega W_0$, then it is stable under Γ (and $W = \Omega(W \cap V)$). Conversely, assume that W is stable under Γ, and let W' be a complement to $W \cap V$ in V, so that

$$V = (W \cap V) \oplus W'.$$

Then

$$(W \cap \Omega W')^\Gamma = W^\Gamma \cap \left(\Omega W'\right)^\Gamma = (W \cap V) \cap W' = 0,$$

and so, by (16.6),

$$W \cap \Omega W' = 0. \tag{28}$$

As $W \supset \Omega(W \cap V)$ and

$$V(\Omega) = \Omega(W \cap V) \oplus \Omega W',$$

this implies that $W = \Omega(W \cap V)$. □

Descending subvarieties and morphisms

In this subsection, $\Omega \supset k$ are fields such that k is the fixed field of $\Gamma = \mathrm{Aut}(\Omega/k)$ and Ω is separably closed. Recall (11.15) that for any variety V over Ω, $V(\Omega)$ is Zariski dense in V. In particular, two regular maps $V \to V'$ coincide if they agree on $V(\Omega)$.

For any variety V over k, Γ acts on $V(\Omega)$. For example, if V is embedded in $\mathbb{A}^n$ or $\mathbb{P}^n$ over k, then Γ acts on the coordinates of a point. If $V = \mathrm{Spm}A$, then

$$V(\Omega) = \mathrm{Hom}_{k\text{-algebra}}(A, \Omega),$$

and Γ acts through its action on Ω.

PROPOSITION 16.8. *Let V be a variety over k, and let W be a closed subvariety of V_Ω such that $W(\Omega)$ is stable under the action of Γ on $V(\Omega)$. Then there is a closed subvariety W_0 of V such that $W = W_{0\Omega}$.*

PROOF. Suppose first that V is affine, and let $I(W) \subset \Omega[V_\Omega]$ be the ideal of regular functions zero on W. Recall that $\Omega[V_\Omega] = \Omega \otimes_k k[V]$ (see §11). Because $W(\Omega)$ is stable under Γ, so also is $I(W)$, and Proposition 16.7 shows that $I(W)$ is spanned by $I_0 = I(W) \cap k[V]$. Therefore, the zero set of I_0 is a closed subvariety W_0 of V with the property that $W = W_{0\Omega}$.

To deduce the general case, cover V with open affines $V = \bigcup V_i$. Then $W_i \stackrel{\text{def}}{=} V_{i\Omega} \cap W$ is stable under Γ, and so it arises from a closed subvariety W_{i0} of V_i; a similar statement holds for $W_{ij} \stackrel{\text{def}}{=} W_i \cap W_j$. Define W_0 to be the variety obtained by patching the varieties W_{i0} along the open subvarieties W_{ij0}. □

PROPOSITION 16.9. *Let V and W be varieties over k, and let $f\colon V_\Omega \to W_\Omega$ be a regular map. If f commutes with the actions of Γ on $V(\Omega)$ and $W(\Omega)$, then f arises from a (unique) regular map $V \to W$ over k.*

PROOF. Apply Proposition 16.8 to the graph of f, $\Gamma_f \subset (V \times W)_\Omega$. □

COROLLARY 16.10. *A variety V over k is uniquely determined (up to a unique isomorphism) by the variety V_Ω together with action of Γ on $V(\Omega)$.*

PROOF. More precisely, we have shown that the functor

$$V \rightsquigarrow (V_\Omega,\ \text{action of } \Gamma \text{ on } V(\Omega)) \tag{29}$$

is fully faithful. □

REMARK 16.11. In Theorems 16.42 and 16.43 below, we obtain sufficient conditions for a pair to lie in the essential image of the functor (29).

Galois descent of vector spaces

Let Γ be a group acting on a field Ω, and let k be a subfield of Ω^{Γ}. By an ***action*** of Γ on an Ω-vector space V we mean a homomorphism $\Gamma \to \mathrm{Aut}_k(V)$ satisfying (27), i.e., such that each $\sigma \in \Gamma$ acts σ-linearly.

LEMMA 16.12. *Let S be the standard $M_n(k)$-module (i.e., $S = k^n$ with $M_n(k)$ acting by left multiplication). The functor $V \mapsto S \otimes_k V$ from k-vector spaces to left $M_n(k)$-modules is an equivalence of categories.*

PROOF. Let V and W be k-vector spaces. The choice of bases $(e_i)_{i\in I}$ and $(f_j)_{j\in J}$ for V and W identifies $\mathrm{Hom}_k(V, W)$ with the set of matrices $(a_{ji})_{(j,i)\in J\times I}$, $a_{ji} \in k$, such that, for a fixed i, all but finitely many a_{ji} are zero. Because S is a simple $M_n(k)$-module and $\mathrm{End}_{M_n(k)}(S) = k$, the set $\mathrm{Hom}_{M_n(k)}(S \otimes_k V, S \otimes_k W)$ has the same description, and so the functor $V \mapsto S \otimes_k V$ is fully faithful.

The functor $V \mapsto S \otimes_k V$ sends a vector space V with basis $(e_i)_{i\in I}$ to a direct sum of copies of S indexed by I. Therefore, to show that the functor is essentially surjective, we have prove that every left $M_n(k)$-module is a direct sum of copies of S.

We first prove this for $M_n(k)$ regarded as a left $M_n(k)$-module. For $1 \le i \le n$, let $L(i)$ be the set of matrices in $M_n(k)$ whose entries are zero except for those in the i^{th} column. Then $L(i)$ is a left ideal in $M_n(k)$, and $L(i)$ is isomorphic to S as an $M_n(k)$-module. Hence,

$$M_n(k) = \bigoplus_i L(i) \simeq S^n \qquad \text{(as a left } M_n(k)\text{-module)}.$$

We now prove it for an arbitrary left $M_n(k)$-module M, which we may suppose to be nonzero. The choice of a set of generators for M realizes it as a quotient of a sum of copies of $M_n(k)$, and so M is a sum of copies of S. It remains to show that the sum can be made direct. Let I be the set of submodules of M isomorphic to S, and let Ξ be the set of subsets J of I such that the sum $N(J) \stackrel{\text{def}}{=} \sum_{N\in J} N$ is direct, i.e., such that for any $N_0 \in J$ and finite subset J_0 of J not containing N_0, $N_0 \cap \sum_{N\in J_0} N = 0$. If $J_1 \subset J_2 \subset \ldots$ is a chain of sets in Ξ, then $\bigcup J_i \in \Xi$, and so Zorn's lemma implies that Ξ has maximal elements. For any maximal J, $M = N(J)$ because otherwise, there exists an element S' of I not contained in $N(J)$; because S' is simple, $S' \cap N(J) = 0$, and it follows that $J \cup \{S'\} \in \Xi$, contradicting the maximality of J. □

ASIDE 16.13. Let A and B be rings (not necessarily commutative), and let S be A-B-bimodule (this means that A acts on S on the left, B acts on S on the right, and the actions commute). When the functor $M \mapsto S \otimes_B M\colon \mathsf{Mod}_B \to \mathsf{Mod}_A$ is an equivalence of categories, A and B are said to be ***Morita equivalent through*** S. In this terminology, the lemma says that $M_n(k)$ and k are Morita equivalent through S.

PROPOSITION 16.14. *Let Ω be a finite Galois extension of k with Galois group Γ. The functor $V \rightsquigarrow \Omega \otimes_k V$ from k-vector spaces to Ω-vector spaces endowed with an action of Γ is an equivalence of categories.*

PROOF. Let $\Omega[\Gamma]$ be the Ω-vector space with basis $\{\sigma \in \Gamma\}$, and make $\Omega[\Gamma]$ into a k-algebra by setting

$$\left(\sum_{\sigma\in\Gamma} a_\sigma \sigma\right)\left(\sum_{\tau\in\Gamma} b_\tau \tau\right) = \sum_{\sigma,\tau} (a_\sigma \cdot \sigma b_\tau)\sigma\tau.$$

Then $\Omega[\Gamma]$ acts k-linearly on Ω by the rule

$$(\textstyle\sum_{\sigma\in\Gamma} a_\sigma\sigma)c = \sum_{\sigma\in\Gamma} a_\sigma(\sigma c),$$

and Dedekind's theorem on the independence of characters (FT 5.14) implies that the homomorphism

$$\Omega[\Gamma] \to \mathrm{End}_k(\Omega)$$

defined by this action is injective. By counting dimensions over k, one sees that it is an isomorphism. Therefore, Lemma 16.12 shows that $\Omega[\Gamma]$ and k are Morita equivalent through Ω, i.e., the functor $V \mapsto \Omega \otimes_k V$ from k-vector spaces to left $\Omega[\Gamma]$-modules is an equivalence of categories. This is precisely the statement of the lemma. □

When Ω is an infinite Galois extension of k, we endow Γ with the Krull topology, and we say that an action of Γ on an Ω-vector space V is ***continuous*** if every element of V is fixed by an open subgroup of Γ, i.e., if

$$V = \bigcup\nolimits_\Delta V^\Delta \qquad \text{(union over the open subgroups } \Delta \text{ of } \Gamma\text{)}.$$

For example, the action of Γ on Ω is obviously continuous, and it follows that, for any k-vector space V, the action of Γ on $\Omega \otimes_k V$ is continuous.

PROPOSITION 16.15. *Let Ω be a Galois extension of k (possibly infinite) with Galois group Γ. For any Ω-vector space V equipped with a continuous action of Γ, the map*

$$\textstyle\sum c_i \otimes v_i \mapsto \sum c_i v_i \colon \Omega \otimes_k V^\Gamma \to V$$

is an isomorphism.

PROOF. Suppose first that Γ is finite. Proposition 16.14 allows us to assume $V = \Omega \otimes_k W$ for some k-subspace W of V. Then $V^\Gamma = (\Omega \otimes_k W)^\Gamma = W$, and so the statement is true.

When Γ is infinite, the finite case shows that $\Omega \otimes_k (V^\Delta)^{\Gamma/\Delta} \simeq V^\Delta$ for every open normal subgroup Δ of Γ. Now pass to the direct limit over Δ, recalling that tensor products commute with direct limits (CA 8.1). □

Descent data

For a homomorphism of fields $\sigma\colon F \to L$, we sometimes write σV for V_L (the variety over L obtained by base change). For example, if V is embedded in affine or projective space, then σV is the affine or projective variety obtained by applying σ to the coefficients of the equations defining V.

A regular map $\varphi\colon V \to W$ defines a regular map $\varphi_L\colon V_L \to W_L$ which we also denote $\sigma\varphi\colon \sigma V \to \sigma W$. Note that $(\sigma\varphi)(\sigma Z) = \sigma(\varphi(Z))$ for any subvariety Z of V. The map $\sigma\varphi$ is obtained from φ by applying σ to the coefficients of the polynomials defining φ.

Let $\Omega \supset k$ be fields, and let $\Gamma = \mathrm{Aut}(\Omega/k)$. An Ω/k***-descent system*** on a variety V over Ω is a family $(\varphi_\sigma)_{\sigma\in\Gamma}$ of isomorphisms $\varphi_\sigma\colon \sigma V \to V$ satisfying the following cocycle condition:

$$\begin{tikzcd} \sigma\tau V \arrow[r, "\sigma\varphi_\tau"'] \arrow[rr, bend left, "\varphi_{\sigma\tau}"] & \sigma V \arrow[r, "\varphi_\sigma"'] & V \end{tikzcd}$$

$$\varphi_\sigma \circ (\sigma\varphi_\tau) = \varphi_{\sigma\tau} \text{ for all } \sigma, \tau \in \Gamma.$$

A model (V_0, φ) of V over a subfield K of Ω containing k ***splits*** $(\varphi_\sigma)_{\sigma\in\Gamma}$ if

$$\varphi_\sigma = \varphi^{-1} \circ \sigma\varphi \qquad\qquad \begin{tikzcd} \sigma V \arrow[r, "\sigma\varphi"'] \arrow[rr, bend left, "\varphi_\sigma"] & \sigma(V_{0\Omega}) = V_{0\Omega} & V \arrow[l, "\varphi"'] \end{tikzcd}.$$

for all σ fixing K.

A descent system $(\varphi_\sigma)_{\sigma\in\Gamma}$ is said to be ***continuous*** if it is split by some model over a subfield K of Ω that is *finitely generated* over k. A ***descent datum*** is a continuous descent system. A descent datum is ***effective*** if it is split by some model over k. In a given situation, we say that ***descent is effective*** or that ***it is possible to descend the base field*** if every descent datum is effective.

Let V_0 be a variety over k, and let $V = V_{0\Omega}$. Then $V = \sigma V$ because the two varieties are obtained from V_0 by extension of scalars with respect to the maps $k \to L$ and $k \to L \xrightarrow{\sigma} L$, which are equal. Write φ_σ for the identity map $\sigma V \to V$; then $(\varphi_\sigma)_{\sigma\in\Gamma}$ is a descent datum on V.

Let $(\varphi_\sigma)_{\sigma\in\Gamma}$ be an Ω/k descent system on a variety V, and let $\Gamma' = \mathrm{Aut}(\Omega^{\mathrm{sep}}/k)$. Every k-automorphism of Ω extends to a k-automorphism of Ω^{sep}, and $(\varphi_\sigma)_{\sigma\in\Gamma}$ extends to the Ω^{sep}/k descent system $(\varphi'_\sigma)_{\sigma\in\Gamma'}$ on $V_{\Omega^{\mathrm{sep}}}$ with $\varphi'_\sigma = \left(\varphi_{\sigma|\Omega}\right)_{\Omega^{\mathrm{sep}}}$. A model of V over a subfield K of Ω splits $(\varphi_\sigma)_{\sigma\in\Gamma}$ if and only if it splits $(\varphi'_\sigma)_{\sigma\in\Gamma'}$. This observation sometimes allows us to assume that Ω is separably closed.

PROPOSITION 16.16. *Assume that k is the fixed field of $\Gamma = \mathrm{Aut}(\Omega/k)$, and that (V_0, φ) and (V'_0, φ') split descent data $(\varphi_\sigma)_{\sigma\in\Gamma}$ and $(\varphi'_\sigma)_{\sigma\in\Gamma}$ on varieties V and V' over Ω. To give a regular map $\psi_0\colon V_0 \to V'_0$ amounts to giving a regular map $\psi\colon V \to V'$ such that $\psi \circ \varphi_\sigma = \varphi'_\sigma \circ \sigma\psi$ for all $\sigma \in \Gamma$, i.e., such that*

$$\begin{tikzcd} \sigma V \arrow[r, "\varphi_\sigma"] \arrow[d, "\sigma\psi"] & V \arrow[d, "\psi"] \\ \sigma V' \arrow[r, "\varphi'_\sigma"] & V' \end{tikzcd} \qquad (30)$$

commutes for all $\sigma \in \Gamma$.

PROOF. Given ψ_0, define ψ to make the right hand square in

$$\begin{tikzcd} \sigma V \arrow[r, "\sigma\varphi"] \arrow[d, "\sigma\psi"] & V_{0\Omega} \arrow[d, "\psi_{0\Omega}"] & V \arrow[l, "\varphi"'] \arrow[d, "\psi"] \\ \sigma V' \arrow[r, "\sigma\varphi'"] & V'_{0\Omega} \arrow[r, "\varphi'"] & V' \end{tikzcd}$$

commute. The left hand square is obtained from the right hand square by applying σ, and so it also commutes. The outer square is (30).

In proving the converse, we may assume that Ω is separably closed. Given ψ, use φ and φ' to transfer ψ to a regular map $\psi'\colon V_{0\Omega} \to V'_{0\Omega}$. Then the hypothesis implies that ψ' commutes with the actions of Γ on $V_0(\Omega)$ and $V'_0(\Omega)$, and so is defined over k (16.9). $\square$

COROLLARY 16.17. *Assume that k is the fixed field of $\Gamma = \mathrm{Aut}(\Omega/k)$, and that (V_0, φ) splits the descent datum $(\varphi_\sigma)_{\sigma\in\Gamma}$. Let W be a variety over k. To give a regular map $W \to$*

V_0 (resp. $V_0 \to W$) amounts to giving a regular map $\psi\colon W_\Omega \to V$ (resp. $\psi\colon V \to W_\Omega$) compatible with the descent datum, i.e., such that

$$\begin{tikzcd} & \sigma V \arrow[d, "\varphi_\sigma"] \\ W_\Omega \arrow[ur, "\sigma\psi"] \arrow[r, "\psi"'] & V \end{tikzcd} \qquad \text{(resp.} \begin{tikzcd} \sigma V \arrow[d, "\varphi_\sigma"'] \arrow[dr, "\sigma\psi"] & \\ V \arrow[r, "\psi"'] & W_\Omega \end{tikzcd} \text{)}$$

commutes.

PROOF. Special case of the proposition in which W_Ω is endowed with its natural descent datum. □

REMARK 16.18. Proposition 16.16 implies that the functor taking a variety V over k to V_Ω over Ω endowed with its natural descent datum is fully faithful.

Let $(\varphi_\sigma)_{\sigma\in\Gamma}$ be an Ω/k-descent system on V. For a subvariety W of V, we set ${}^\sigma W = \varphi_\sigma(\sigma W)$. Then the following diagram commutes:

$$\begin{tikzcd} \sigma V \arrow[r, "\varphi_\sigma", "\simeq"'] & V \\ \sigma W \arrow[u, "\cup"'] \arrow[r, "\varphi_\sigma|\sigma W", "\simeq"'] & {}^\sigma W \arrow[u, "\cup"'] \end{tikzcd}$$

LEMMA 16.19. *The following hold.*

(a) *For all $\sigma, \tau \in \Gamma$ and $W \subset V$, ${}^\sigma({}^\tau W) = {}^{\sigma\tau}W$.*

(b) *Suppose that $(\varphi_\sigma)_{\sigma\in\Gamma}$ is split by a model (V_0, φ) of V over k_0, and let W be a subvariety of V. If $W = \varphi^{-1}(W_{0\Omega})$ for some subvariety W_0 of V_0, then ${}^\sigma W = W$ for all $\sigma \in \Gamma$; the converse is true if $\Omega^\Gamma = k$.*

PROOF. (a) By definition

$${}^\sigma({}^\tau W) = \varphi_\sigma(\sigma(\varphi_\tau(\tau W)) = (\varphi_\sigma \circ \sigma\varphi_\tau)(\sigma\tau W) = \varphi_{\sigma\tau}(\sigma\tau W) = {}^{\sigma\tau}W.$$

In the second equality, we used that $(\sigma\varphi)(\sigma W) = \sigma(\varphi W)$.

(b) Let $W = \varphi^{-1}(W_{0\Omega})$. By hypothesis $\varphi_\sigma = \varphi^{-1} \circ \sigma\varphi$, and so

$${}^\sigma W = (\varphi^{-1} \circ \sigma\varphi)(\sigma W) = \varphi^{-1}(\sigma(\varphi W)) = \varphi^{-1}(\sigma W_{0\Omega}) = \varphi^{-1}(W_{0\Omega}) = W.$$

Conversely, suppose ${}^\sigma W = W$ for all $\sigma \in \Gamma$. Then

$$\varphi(W) = \varphi({}^\sigma W) = (\sigma\varphi)(\sigma W) = \sigma(\varphi(W)).$$

Therefore, $\varphi(W)$ is stable under the action of Γ on $V_{0\Omega}$, and so is defined over k (see 16.8). □

For a descent system $(\varphi_\sigma)_{\sigma\in\Gamma}$ on V and a regular function f on an open subset U of V, we define ${}^\sigma f$ to be the function $(\sigma f)\circ\varphi_\sigma^{-1}$ on ${}^\sigma U$, so that ${}^\sigma f({}^\sigma P)=\sigma(f(P))$ for all $P\in U$. Then ${}^\sigma({}^\tau f)={}^{\sigma\tau}f$, and so this defines an action of Γ on the regular functions.

The ***Krull topology*** on Γ is that for which the subgroups of Γ fixing a subfield of Ω finitely generated over k form a basis of open neighbourhoods of 1 (see FT §8). An action of Γ on an Ω-vector space V is ***continuous*** if

$$V=\bigcup_{\Delta}V^{\Delta}\qquad\text{(union over the open subgroups Δ of Γ).}$$

For a subfield L of Ω containing k, let $\Delta_L=\mathrm{Aut}(\Omega/L)$.

PROPOSITION 16.20. *Assume that Ω is separably closed. A descent system $(\varphi_\sigma)_{\sigma\in\Gamma}$ on an affine variety V is continuous if and only if the action of Γ on $\Omega[V]$ is continuous.*

PROOF. If $(\varphi_\sigma)_{\sigma\in\Gamma}$ is continuous, it is split by a model of V over a subfield K of Ω finitely generated over k. By definition, Δ_K is open, and $\Omega[V]^{\Delta_K}$ contains a set $\{f_1,\ldots,f_n\}$ of generators for $\Omega[V]$ as an Ω-algebra. Now $\Omega[V]=\bigcup L[f_1,\ldots,f_n]$ where L runs over the subfields of Ω containing K and finitely generated over k. As $L[f_1,\ldots,f_n]=\Omega[V]^{\Delta_L}$, this shows that $\Omega[V]=\bigcup\Omega[V]^{\Delta_L}$.

Conversely, if the action of Γ on $\Omega[V]$ is continuous, then for some subfield L of Ω finitely generated over k, $\Omega[V]^{\Delta_L}$ will contain a set of generators $f_1,\ldots,f_n$ for $\Omega[V]$ as an Ω-algebra. According to (16.3), Ω^{Δ_L} is a purely inseparable algebraic extension of L, and so, after replacing L with a finite extension, the embedding $V\hookrightarrow\mathbb{A}^n$ defined by the f_i will determine a model of V over L. This model splits $(\varphi_\sigma)_{\sigma\in\Gamma}$, which is therefore continuous. □

PROPOSITION 16.21. *A descent system $(\varphi_\sigma)_{\sigma\in\Gamma}$ on a variety V over Ω is continuous if there exists a finite set S of points in $V(\Omega)$ such that*

(a) *any automorphism of V fixing all $P\in S$ is the identity map, and*
(b) *there exists a subfield K of Ω finitely generated over k such that ${}^\sigma P=P$ for all $\sigma\in\Gamma$ fixing K.*

PROOF. Let (V_0,φ) be a model of V over a subfield K of Ω finitely generated over k. After possibly replacing K by a larger finitely generated field, we may suppose (i) that ${}^\sigma P=P$ for all $\sigma\in\Gamma$ fixing K and all $P\in S$ (because of (b)) and (ii) that $\varphi(P)\in V_0(K)$ for all $P\in S$ (because S is finite). Then, for $P\in S$ and every σ fixing K,

$$\varphi_\sigma(\sigma P)\overset{\text{def}}{=}{}^\sigma P\overset{\text{(i)}}{=}P$$
$$(\sigma\varphi)(\sigma P)=\sigma(\varphi P)\overset{\text{(ii)}}{=}\varphi P,$$

and so φ_σ and $\varphi^{-1}\circ\sigma\varphi$ are isomorphisms $\sigma V\to V$ sending σP to P. Therefore, φ_σ and $\varphi^{-1}\circ\sigma\varphi$ differ by an automorphism of V fixing the $P\in S$, which implies that they are equal. This says that (V_0,φ) splits $(\varphi_\sigma)_{\sigma\in\Gamma}$. □

PROPOSITION 16.22. *Let V be a variety over Ω whose only automorphism is the identity map. A descent datum on V is effective if V has a model over k.*

PROOF. Let (V, φ) be a model of V over k. For $\sigma \in \Gamma$, the maps φ_σ and $\varphi^{-1} \circ \sigma\varphi$ are both isomorphisms $\sigma V \to V$, and so differ by an automorphism of V. Therefore they are equal, which says that (V, φ) splits $(\varphi_\sigma)_{\sigma \in \Gamma}$. □

Of course, in Proposition 16.21, S doesn't have to be a finite set of points. The proposition will hold with S any additional structure on V that rigidifies V (i.e., is such that $\mathrm{Aut}(V, S) = 1$) and is such that (V, S) has a model over a finitely generated extension of k.

Galois descent of varieties

In this subsection, Ω is a Galois extension of k with Galois group Γ.

THEOREM 16.23. *A descent datum $(\varphi_\sigma)_{\sigma \in \Gamma}$ on a variety V is effective if V is covered by open affines U with the property that ${}^\sigma U = U$ for all $\sigma \in \Gamma$.*

PROOF. Assume first that V is affine, and let $A = k[V]$. A descent datum $(\varphi_\sigma)_{\sigma \in \Gamma}$ defines a continuous action of Γ on A (see 16.20). From (16.15), we know that

$$c \otimes a \mapsto ca \colon \Omega \otimes_k A^\Gamma \to A \tag{31}$$

is an isomorphism. Let $V_0 = \mathrm{Spm} A^\Gamma$, and let φ be the isomorphism $V \to V_{0\Omega}$ defined by (31). Then (V_0, φ) splits the descent datum.

In the general case, write V as a finite union of open affines U_i such that ${}^\sigma U_i = U_i$ for all $\sigma \in \Gamma$. Then V is the variety over Ω obtained by patching the U_i by means of the maps

$$U_i \hookleftarrow U_i \cap U_j \hookrightarrow U_j. \tag{32}$$

Each intersection $U_i \cap U_j$ is again affine (4.27), and so the system (32) descends to k. The variety over k obtained by patching the descended system is a model of V over k splitting the descent datum. □

COROLLARY 16.24. *If each finite set of points of $V(\Omega^{\mathrm{sep}})$ is contained in an open affine subvariety of $V_{\Omega^{\mathrm{sep}}}$, then every descent datum on V is effective.*

PROOF. As we noted before, an Ω/k-descent datum for V extends in a natural way to an Ω^{sep}/k-descent datum for $V_{\Omega^{\mathrm{sep}}}$, and if a model (V_0, φ) over k splits the second descent datum, then it also splits the first. Thus, we may suppose that Ω is separably closed.

Let $(\varphi_\sigma)_{\sigma \in \Gamma}$ be a descent datum on V, and let U be a subvariety of V. By definition, (φ_σ) is split by a model (V_1, φ) of V over some finite extension k_1 of k. After possibly replacing k_1 with a larger finite extension, there will exist a subvariety U_1 of V_1 such that $\varphi(U) = U_{1\Omega}$. Now (16.19b) shows that ${}^\sigma U$ depends only on the coset $\sigma\Delta$ where $\Delta = \mathrm{Gal}(\Omega/k_1)$. In particular, $\{{}^\sigma U \mid \sigma \in \Gamma\}$ is finite. The subvariety $\bigcap_{\sigma \in \Gamma} {}^\sigma U$ is stable under Γ, and so (see 16.8, 16.19) ${}^\tau(\bigcap_{\sigma \in \Gamma} {}^\sigma U) = (\bigcap_{\sigma \in \Gamma} {}^\sigma U)$ for all $\tau \in \Gamma$.

Let $P \in V$. Because $\{{}^\sigma P \mid \sigma \in \Gamma\}$ is finite, it is contained in an open affine U of V. Now $U' = \bigcap_{\sigma \in \Gamma} {}^\sigma U$ is an open affine in V containing P and such that ${}^\sigma U' = U'$ for all $\sigma \in \Gamma$. It follows that the variety V satisfies the hypothesis of Theorem 16.23. □

COROLLARY 16.25. *Descent is effective in each of the following two cases:*

(a) *V is quasiprojective, or*
(b) *an affine algebraic group G acts transitively on V.*

PROOF. (a) Apply (6.25) (whose proof applies unchanged over any infinite base field).

(b) We may assume Ω to be separably closed. Let S be a finite set of points of $V(\Omega)$, and let U be an open affine in V. For each $P \in S$, there is a nonempty open subvariety G_P of G such that $G_P \cdot P \subset U$. Because Ω is separably closed, there exists a $g \in (\bigcap_{P \in S} G_P \cdot P)(\Omega)$ (see 11.15). Now $g^{-1}U$ is an open affine containing S. $\square$

Weil restriction

Let K/k be a finite extension of fields, and let V be a variety over K. A pair (V_*, φ) consisting of a variety V_* over k and a regular map $\varphi \colon V_{*K} \to V$ is called the K/k-***Weil restriction*** of V if it has the following universal property: for any variety T over k and regular map $\varphi' \colon T_K \to V$, there exists a unique regular map $\psi \colon T \to V$ (of k-varieties) such that $\varphi \circ \psi_K = \varphi'$, i.e.,

$$\text{given} \quad \begin{tikzcd} T_K \arrow[dr, "\varphi'"] & \\ V_{*K} \arrow[r, "\varphi"] & V \end{tikzcd} \qquad \begin{tikzcd} T \arrow[d, dashed, "\exists!\ \psi"] \\ V_* \end{tikzcd} \quad \text{such that} \quad \begin{tikzcd} T_K \arrow[d, "\psi_K"'] \arrow[dr, "\varphi'"] & \\ V_{*K} \arrow[r, "\varphi"] & V \end{tikzcd} \quad \text{commutes.}$$

In other words, (V_*, φ) is the K/k-Weil restriction of V if φ defines an isomorphism

$$\mathrm{Mor}_k(T, V_*) \to \mathrm{Mor}_K(T_K, V)$$

(natural in the k-variety T); in particular,

$$V_*(A) \simeq V(K \otimes_k A)$$

(natural in the affine k-algebra A). If it exists, the K/k-Weil restriction of V is uniquely determined by its universal property (up to a unique isomorphism).

When (V_*, φ) is the K/k-Weil restriction of V, the variety V_* is said to have been obtained from V ***by (Weil) restriction of scalars*** or ***by restriction of the base field***.

PROPOSITION 16.26. *If V satisfies the hypothesis of (16.24) (for example, if V is quasiprojective) and K/k is separable, then the K/k-Weil restriction exists.*

PROOF. Let Ω be a Galois extension of k large enough to contain all conjugates of K, i.e., such that $\Omega \otimes_k K \simeq \prod_{\tau: K \to \Omega} \tau K$. Let $V' = \prod \tau V$ — this is a variety over Ω. For $\sigma \in \mathrm{Gal}(\Omega/k)$, define $\varphi_\sigma \colon \sigma V' \to V'$ to be the regular map that acts on the factor $\sigma(\tau V)$ as the canonical isomorphism $\sigma(\tau V) \simeq (\sigma\tau)V$. Then $(\varphi_\sigma)_{\sigma \in \mathrm{Gal}(\Omega/k)}$ is a descent datum, and so defines a model (V_*, φ_*) of V' over k.

Choose a $\tau_0 \colon K \to \Omega$. The projection map $V' \to \tau_0 V$ is invariant under the action of $\mathrm{Gal}(\Omega/\tau_0 K)$, and so defines a regular map $(V_*)_{\tau_0 K} \to \tau_0 V$ (16.9), and hence a regular map $\varphi \colon V_{*K} \to V$. It is easy to check that this has the correct universal property. $\square$

Generic fibres and specialization

In this subsection, k is an algebraically closed field.

Let $\varphi: V \to U$ be a dominant map with U irreducible, and let $K = k(U)$. Then there is a regular map $\varphi_K: V_K \to \mathrm{Spm} K$, called the ***generic fibre*** of φ. For example, if V and U are affine, so that φ corresponds to an injective homomorphism of rings $f: A \to B$, then φ_K corresponds to $A \otimes_k K \to B \otimes_k K$. In the general case, we replace U with any open affine and write V as a finite union of affines $V = \bigcup_i V_i$; then $V_K = \bigcup_i V_{iK}$.

Let K be a field finitely generated over k, and let V be a variety over K. For any irreducible k-variety U with $k(U) = K$, there will exist a dominant map $\varphi: V \to U$ with generic fibre V. For example, we can take $U = \mathrm{Spm}(A)$ where A is any finitely generated k-subalgebra of K containing a set of generators for K and containing the coefficients of some set of polynomials defining V. Let P be a point in the image of φ. Then the fibre of V over P is a variety $V(P)$ over k, called the ***specialization*** of V at P.

Similar statements are true for morphisms of varieties.

Rigid descent

LEMMA 16.27. *Let V and W be varieties over an algebraically closed field k. If V and W become isomorphic over some field containing k, then they are already isomorphic over k.*

PROOF. The hypothesis implies that, for some field K finitely generated over k, there exists an isomorphism $\varphi: V_K \to W_K$. Let U be an affine k-variety such that $k(U) = K$. After possibly replacing U with an open subset, we can φ extend to an isomorphism $\varphi_U: U \times V \to U \times W$. The fibre of φ_U at any point of U is an isomorphism $V \to W$. □

Consider fields $\Omega \supset K_1, K_2 \supset k$. Recall (11.1) that K_1 and K_2 are said to be linearly disjoint over k if the homomorphism

$$\textstyle\sum a_i \otimes b_i \mapsto \sum a_i b_i : K_1 \otimes_k K_2 \to K_1 \cdot K_2$$

is injective.

LEMMA 16.28. *Let $\Omega \supset k$ be algebraically closed fields, and let V be a variety over Ω. If there exist models of V over subfields K_1, K_2 of Ω finitely generated over k and linearly disjoint over k, then there exists a model of V over k.*

PROOF. The model of V over K_1 extends to a model over an irreducible affine variety U_1 with $k(U_1) = K_1$, i.e., there exists a surjective map $V_1 \to U_1$ of k-varieties whose generic fibre is a model of V over K_1. A similar statement applies to the model over K_2. Because K_1 and K_2 are linearly disjoint, $K_1 \otimes_k K_2$ is an integral domain with field of fractions $k(U_1 \times U_2)$. From the map $V_1 \to U_1$, we get a map $V_1 \times U_2 \to U_1 \times U_2$, and similarly for V_2.

Assume initially that $V_1 \times U_2$ and $U_1 \times V_2$ are isomorphic over $U_1 \times U_2$, so that we have a commutative diagram:

$$\begin{tikzcd}
V_1 \arrow[d] & V_1 \times U_2 \arrow[l] \arrow[r, "\approx"] \arrow[dr] & U_1 \times V_2 \arrow[r] \arrow[d] & V_2 \arrow[d] \\
U_1 & & U_1 \times U_2 \arrow[ll] & U_2 \arrow[l]
\end{tikzcd}$$

Let P be a point of U_1. When we pull back the triangle to the subvariety $P \times U_2$ of $U_1 \times U_2$, we get the diagram at left below. Note that $P \times U_2 \simeq U_2$ and that $P \simeq \operatorname{Spm} k$ (because k is algebraically closed).

$$\begin{tikzcd} V(P) \times U_2 \arrow[rr, "\approx"] \arrow[dr] & & P \times V_2 \arrow[dl] \\ & P \times U_2 & \end{tikzcd} \qquad \begin{tikzcd} V(P)_{K_2} \arrow[rr, "\approx"] \arrow[dr] & & V_{2K_2} \arrow[dl] \\ & \operatorname{Spm} K_2 & \end{tikzcd}$$

The generic fibre of this diagram is the diagram at right. Here $V_1(P)_{K_2}$ is the variety over K_2 obtained from $V_1(P)$ by extension of scalars $k \to K_2$. As V_{2K_2} is a model V over K_2, it follows that $V_1(P)$ is a model of V over k.

We now prove the general case. The varieties $(V_1 \times U_2)_{k(U_1 \times U_2)}$ and $(U_1 \times V_2)_{k(U_1 \times U_2)}$ become isomorphic over some finite field extension L of $k(U_1 \times U_2)$. Let $\bar{U}$ be the normalization[1] of $U_1 \times U_2$ in L, and let U be a dense open subset of $\bar{U}$ such that some isomorphism of $(V_1 \times U_2)_L$ with $(U_1 \times V_2)_L$ extends to an isomorphism over U. The going-up theorem (8.8) shows that $\bar{U} \to U_1 \times U_2$ is surjective, and so the image U' of U in $U_1 \times U_2$ contains a nonempty (hence dense) open subset of $U_1 \times U_2$ (see 10.2). In particular, U' contains a subset $P \times U_2'$ with U_2' a nonempty open subset of U_2. Now the previous argument gives us varieties $V_1(P)_{K_2}$ and V_{2K_2} over K_2 that become isomorphic over $k(U'')$ where U'' is the inverse image of $P \times U_2'$ in $\bar{U}$. As $k(U'')$ is a finite extension of K_2, this again shows that $V_1(P)$ is a model of V over k. □

EXAMPLE 16.29. Let E be an elliptic curve over Ω with j-invariant $j(E)$. There exists a model of E over a subfield K of Ω if and only if $j(E) \in K$. If $j(E)$ is transcendental, then any two such fields contain $k(j(E))$, and so can't be linearly disjoint. Therefore, the hypothesis in the proposition implies $j(E) \in k$, and so E has a model over k.

LEMMA 16.30. *Let Ω be algebraically closed of infinite transcendence degree over k, and assume that k is algebraically closed in Ω. For any $K \subset \Omega$ finitely generated over k, there exists a $\sigma \in \operatorname{Aut}(\Omega/k)$ such that K and σK are linearly disjoint over k.*

PROOF. Let $a_1, \ldots, a_n$ be a transcendence basis for K/k, and extend it to a transcendence basis $a_1, \ldots, a_n, b_1, \ldots, b_n, \ldots$ of Ω/k. Let σ be any permutation of the transcendence basis such that $\sigma(a_i) = b_i$ for all i. Then σ defines a k-automorphism of $k(a_1, \ldots a_n, b_1, \ldots, b_n, \ldots)$, which we extend to an automorphism of Ω.

Let $K_1 = k(a_1, \ldots, a_n)$. Then $\sigma K_1 = k(b_1, \ldots, b_n)$, and certainly K_1 and σK_1 are linearly disjoint. In particular, $K_1 \otimes_k \sigma K_1$ is an integral domain. Because k is algebraically closed in K, $K \otimes_k \sigma K$ is an integral domain (cf. 11.5). This implies that K and σK are linearly disjoint. □

LEMMA 16.31. *Let $\Omega \supset k$ be algebraically closed fields such that Ω is of infinite transcendence degree over k, and let V be a variety over Ω. If V is isomorphic to σV for every $\sigma \in \operatorname{Aut}(\Omega/k)$, then V has a model over k.*

[1] Let $U_1 \times U_2 = \operatorname{Spm} C$; then $\bar{U} = \operatorname{Spm} \bar{C}$, where $\bar{C}$ is the integral closure of C in L.

PROOF. There will exist a model V_0 of V over a subfield K of Ω finitely generated over k. According to Lemma 16.30, there exists a $\sigma \in \mathrm{Aut}(\Omega/k)$ such that K and σK are linearly disjoint. Because $V \approx \sigma V$, σV_0 is a model of V over σK, and we can apply Lemma 16.28. □

In the next two theorems, $\Omega \supset k$ are fields such that the fixed field of $\Gamma = \mathrm{Aut}(\Omega/k)$ is k and Ω is algebraically closed

THEOREM 16.32. *Let V be a quasiprojective variety over Ω, and let $(\varphi_\sigma)_{\sigma\in\Gamma}$ be a descent system for V. If the only automorphism of V is the identity map, then V has a model over k splitting (φ_σ).*

PROOF. According to Lemma 16.31, V has a model (V_0, φ) over the algebraic closure k^{al} of k in Ω, which (see the proof of 16.22) splits $(\varphi_\sigma)_{\sigma\in\mathrm{Aut}(\Omega/k^{\mathrm{al}})}$.

Now $\varphi'_\sigma \stackrel{\text{def}}{=} \varphi^{-1} \circ \varphi_\sigma \circ \sigma\varphi$ is stable under $\mathrm{Aut}(\Omega/k^{\mathrm{al}})$, and hence is defined over k^{al} (16.9). Moreover, φ'_σ depends only on the restriction of σ to k^{al}, and $(\varphi'_\sigma)_{\sigma\in\mathrm{Gal}(k^{\mathrm{al}}/k)}$ is a descent system for V_0. It is continuous by (16.21), and so V_0 has a model (V_{00}, φ') over k splitting $(\varphi'_\sigma)_{\sigma\in\mathrm{Gal}(k^{\mathrm{al}}/k)}$. Now $(V_{00}, \varphi \circ \varphi'_\Omega)$ splits $(\varphi_\sigma)_{\sigma\in\mathrm{Aut}(\Omega/k)}$. □

We now consider pairs (V, S) where V is a variety over Ω and S is a family of points $S = (P_i)_{1\le i\le n}$ of V indexed by $[1, n]$. A morphism $(V, (P_i)_{1\le i\le n}) \to (W, (Q_i)_{1\le i\le n})$ is a regular map $\varphi\colon V \to W$ such that $\varphi(P_i) = Q_i$ for all i.

THEOREM 16.33. *Let V be a quasiprojective variety over Ω, and let $(\varphi_\sigma)_{\sigma\in\mathrm{Aut}(\Omega/k)}$ be a descent system for V. Let $S = (P_i)_{1\le i\le n}$ be a finite set of points of V such that*

(a) *the only automorphism of V fixing each P_i is the identity map, and*
(b) *there exists a subfield K of Ω finitely generated over k such that ${}^\sigma P = P$ for all $\sigma \in \Gamma$ fixing K.*

Then V has a model over k splitting (φ_σ).

PROOF. Lemmas 16.27–16.31 all hold for pairs (V, S) (with the same proofs), and so the proof of Theorem 16.32 applies. □

EXAMPLE 16.34. Theorem 16.33 can be used to prove that certain abelian varieties attached to algebraic varieties in characteristic zero, for example, the generalized Jacobian varieties, are defined over the same field as the variety.[2] We illustrate this with the usual Jacobian variety J of a complete nonsingular curve C. For such a curve C over $\mathbb{C}$, there is a principally polarized abelian variety $J(C)$ such that, as a complex manifold,

$$J(C)(\mathbb{C}) = \Gamma(C, \Omega^1)^\vee / H_1(C, \mathbb{Z}).$$

The association $C \mapsto J(C)$ is a functorial, and so a descent datum $(\varphi_\sigma)_{\sigma\in\mathrm{Aut}(\Omega/k)}$ on C defines a descent system on $J(C)$. It is known that if we take S to be the set of points of order 3 on $J(C)$, then condition (a) of the theorem is satisfied (see, for example, Milne 1986[3], 17.5), and condition (b) can be seen to be satisfied by regarding $J(C)$ as the Picard variety of C.

[2]This was pointed out to me by Niranjan Ramachandran.

[3]Milne, J.S., Abelian varieties, in Arithmetic Geometry, Springer, 1986.

Weil's descent theorems

THEOREM 16.35. *Let k be a finite separable extension of a field k_0, and let I be the set of k-homomorphisms $k \to k_0^{\mathrm{al}}$. Let V be a quasiprojective variety over k; for each pair (σ, τ) of elements of I, let $\varphi_{\tau,\sigma}$ be an isomorphism $\sigma V \to \tau V$ (of varieties over k_0^{al}). Then there exists a variety V_0 over k_0 and an isomorphism $\varphi\colon V_{0k} \to V$ such that $\varphi_{\tau,\sigma} = \tau\varphi \circ (\sigma\varphi)^{-1}$ for all $\sigma, \tau \in I$ if and only if the $\varphi_{\tau,\sigma}$ are defined over k_0^{sep} and satisfy the following conditions:*

(a) $\varphi_{\tau,\rho} = \varphi_{\tau,\sigma} \circ \varphi_{\sigma,\rho}$ *for all* $\rho, \sigma, \tau \in I$;
(b) $\varphi_{\tau\omega,\sigma\omega} = \omega\varphi_{\tau,\sigma}$ *for all* $\sigma, \tau \in I$ *and all* k_0*-automorphisms* ω *of* k_0^{al} *over* k_0.

Moreover, when this is so, the pair (V_0, φ) is unique up to isomorphism over k_0, and V_0 is quasiprojective or quasi-affine if V is.

PROOF. This is Theorem 3 of Weil 1956,[4] p515. It is essentially a restatement of (a) of Corollary 16.25 (and (V_0, φ) is unique up to a *unique* isomorphism over k_0). □

An extension K of a field k is said to be ***regular*** if it is finitely generated, admits a separating transcendence basis, and k is algebraically closed in K. These are precisely the fields that arise as the field of rational functions on geometrically irreducible algebraic variety over k.

Let k be a field, and let $k(t)$, $t = (t_1, \ldots, t_n)$, be a regular extension of k (in Weil's terminology, t is a *generic point* of a variety over k). By $k(t')$ we shall mean a field isomorphic to $k(t)$ by $t \mapsto t'$, and we write $k(t,t')$ for the field of fractions of $k(t) \otimes_k k(t')$.[5] When V_t is a variety over $k(t)$, we shall write $V_{t'}$ for the variety over $k(t')$ obtained from V_t by base change with respect to $t \mapsto t'\colon k(t) \to k(t')$. Similarly, if f_t denotes a regular map of varieties over $k(t)$, then $f_{t'}$ denotes the regular map over $k(t')$ obtained by base change. Similarly, $k(t'')$ is a second field isomorphic to $k(t)$ by $t \mapsto t''$ and $k(t, t', t'')$ is the field of fractions of $k(t) \otimes_k k(t') \otimes_k k(t'')$.

THEOREM 16.36. *With the above notations, let V_t be a quasiprojective variety over $k(t)$; for each pair (t, t'), let $\varphi_{t',t}$ be an isomorphism $V_t \to V_{t'}$ defined over $k(t,t')$. Then there exists a variety V defined over k and an isomorphism $\varphi_t\colon V_{k(t)} \to V_t$ (of varieties over $k(t)$) such that $\varphi_{t',t} = \varphi_{t'} \circ \varphi_t^{-1}$ if and only if $\varphi_{t',t}$ satisfies the following condition:*

$$\varphi_{t'',t} = \varphi_{t'',t'} \circ \varphi_{t',t} \quad \text{(isomorphism of varieties over } k(t,t',t'')\text{)}.$$

Moreover, when this is so, the pair (V, φ_t) is unique up to an isomorphism over k, and V is quasiprojective or quasi-affine if V is.

PROOF. This is Theorem 6 and Theorem 7 of Weil 1956, p522. □

THEOREM 16.37. *Let Ω be an algebraically closed field of infinite transcendence degree over a perfect field k. Then descent is effective for quasiprojective varieties over Ω.*

[4] Weil, André, The field of definition of a variety. Amer. J. Math. 78 (1956), 509–524.

[5] If $k(t)$ and $k(t')$ are linearly disjoint subfields of some large field Ω, then $k(t,t')$ is the subfield of Ω generated over k by t and t'.

PROOF. Let (φ_σ) be a descent datum on a variety V over Ω. Because (φ_σ) is continuous, it is split by a model of V over some subfield K of Ω finitely generated over k. Let k' be the algebraic closure of k in K; then k' is a finite extension of k and K is a regular extension of k. Write $K = k(t)$, and let (V_t, φ') be a model of V over $k(t)$ splitting (φ_σ). According to Lemma 16.30, there exists a $\sigma \in \mathrm{Aut}(\Omega/k)$ such that $\sigma k(t) = k(t')$ and $k(t)$ are linearly disjoint over k. The isomorphism

$$V_{t\Omega} \xrightarrow{\varphi'} V \xrightarrow{\varphi_\sigma^{-1}} \sigma V \xrightarrow{(\sigma\varphi')^{-1}} V_{t',\Omega}$$

is defined over $k(t,t')$ and satisfies the conditions of Theorem 16.36. Therefore, there exists a model (W, φ) of V over k' splitting $(\varphi_\sigma)_{\sigma\in\mathrm{Aut}(\Omega/k(t)}$.

For $\sigma, \tau \in \mathrm{Aut}(\Omega/k)$, let $\varphi_{\tau,\sigma}$ be the composite of the isomorphisms

$$\sigma W \xrightarrow{\sigma\varphi} \sigma V \xrightarrow{\varphi_\sigma} V \xrightarrow{\varphi_\tau^{-1}} \tau V \xrightarrow{\tau\varphi} \tau W.$$

Then $\varphi_{\tau,\sigma}$ is defined over the algebraic closure of k in Ω and satisfies the conditions of Theorem 16.35, which gives a model of W over k splitting $(\varphi_\sigma)_{\sigma\in\mathrm{Aut}(\Omega/k)}$. □

Restatement in terms of group actions

In this subsection, $\Omega \supset k$ are fields such that $k = \Omega^\Gamma$ and Ω is algebraically closed. Recall that for any variety V over k, there is a natural action of Γ on $V(\Omega)$. In this subsection, we describe the essential image of the functor

$$\{\text{quasiprojective varieties over } k\} \to \{\text{quasiprojective varieties over } \Omega + \text{action of } \Gamma\}.$$

In other words, we determine which pairs $(V, *)$, with V a quasiprojective variety over Ω and $*$ an action of Γ on $V(\Omega)$,

$$(\sigma, P) \mapsto \sigma * P : \Gamma \times V(\Omega) \to V(\Omega),$$

arise from a variety over k. There are two obvious necessary conditions for this.

Regularity condition

Obviously, the action should recognize that $V(\Omega)$ is not just a set, but rather the set of points of an algebraic variety. For $\sigma \in \Gamma$, let σV be the variety obtained by applying σ to the coefficients of the equations defining V, and for $P \in V(\Omega)$ let σP be the point on σV obtained by applying σ to the coordinates of P.

DEFINITION 16.38. We say that the action $*$ is ***regular*** if the map

$$\sigma P \mapsto \sigma * P : (\sigma V)(\Omega) \to V(\Omega)$$

is regular isomorphism for all σ.

A priori, this is only a map of sets. The condition requires that it be induced by a regular map $\varphi_\sigma : \sigma V \to V$. If $V = V_{0\Omega}$ for some variety V_0 defined over k, then $\sigma V = V$, and φ_σ is the identity map, and so the condition is clearly necessary.

REMARK 16.39. The maps φ_σ satisfy the cocycle condition $\varphi_\sigma \circ \sigma\varphi_\tau = \varphi_{\sigma\tau}$. In particular, $\varphi_\sigma \circ \sigma\varphi_{\sigma^{-1}} = \mathrm{id}$, and so if $*$ is regular, then each φ_σ is an isomorphism, and the family $(\varphi_\sigma)_{\sigma\in\Gamma}$ is a descent system. Conversely, if $(\varphi_\sigma)_{\sigma\in\Gamma}$ is a descent system, then

$$\sigma * P = \varphi_\sigma(\sigma P)$$

defines a regular action of Γ on $V(\Omega)$. Note that if $* \leftrightarrow (\varphi_\sigma)$, then $\sigma * P =^\sigma P$.

Continuity condition

DEFINITION 16.40. We say that the action $*$ is ***continuous*** if there exists a subfield L of Ω finitely generated over k and a model V_0 of V over L such that the action of $\Gamma(\Omega/L)$ is that defined by V_0.

For an affine variety V, an action of Γ on V gives an action of Γ on $\Omega[V]$, and one action is continuous if and only if the other is.

Continuity is obviously necessary. It is easy to write down regular actions that fail it, and hence don't arise from varieties over k.

EXAMPLE 16.41. The following are examples of actions that fail the continuity condition ((b) and (c) are regular).

(a) Let $V = \mathbb{A}^1$ and let $*$ be the trivial action.
(b) Let $\Omega/k = \mathbb{Q}^{\mathrm{al}}/\mathbb{Q}$, and let N be a normal subgroup of finite index in $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ that is not open,[6] i.e., that fixes no extension of $\mathbb{Q}$ of finite degree. Let V be the zero-dimensional variety over $\mathbb{Q}^{\mathrm{al}}$ with $V(\mathbb{Q}^{\mathrm{al}}) = \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})/N$ with its natural action.
(c) Let k be a finite extension of $\mathbb{Q}_p$, and let $V = \mathbb{A}^1$. The homomorphism $k^\times \to \mathrm{Gal}(k^{\mathrm{ab}}/k)$ can be used to twist the natural action of Γ on $V(\Omega)$.

Restatement of the main theorems

Let $\Omega \supset k$ be fields such that k is the fixed field of $\Gamma = \mathrm{Aut}(\Omega/k)$ and Ω is algebraically closed.

THEOREM 16.42. *Let V be a quasiprojective variety over Ω, and let $*$ be a regular action of Γ on $V(\Omega)$. Let $S = (P_i)_{1\le i\le n}$ be a finite set of points of V such that*

(a) *the only automorphism of V fixing each P_i is the identity map, and*
(b) *there exists a subfield K of Ω finitely generated over k such that $\sigma * P = P$ for all $\sigma \in \Gamma$ fixing K.*

Then $*$ arises from a model of V over k.

PROOF. This a restatement of Theorem 16.33. □

THEOREM 16.43. *Let V be a quasiprojective variety over Ω with an action $*$ of Γ. If $*$ is regular and continuous, then $*$ arises from a model of V over k in each of the following cases:*

[6]For a proof that such subgroups exist, see FT 7.25.

(a) *Ω is algebraic over k, or*
(b) *Ω is has infinite transcendence degree over k.*

PROOF. Restatements of (16.23, 16.25) and of (16.37). □

The condition "quasiprojective" is necessary, because otherwise the action may not stabilize enough open affine subsets to cover V.

Faithfully flat descent

Recall that a homomorphism $f\colon A \to B$ of rings is flat if the functor "extension of scalars" $M \mapsto B \otimes_A M$ is exact. It is ***faithfully flat*** if a sequence

$$0 \to M' \to M \to M'' \to 0$$

of A-modules is exact if and only if

$$0 \to B \otimes_A M' \to B \otimes_A M \to B \otimes_A M'' \to 0$$

is exact. For a field k, a homomorphism $k \to A$ is always flat (because exact sequences of k-vector spaces are split-exact), and it is faithfully flat if $A \neq 0$.

The next theorem and its proof are quintessential Grothendieck.

THEOREM 16.44. *If $f\colon A \to B$ is faithfully flat, then the sequence*

$$0 \to A \xrightarrow{f} B \xrightarrow{d^0} B^{\otimes 2} \to \cdots \to B^{\otimes r} \xrightarrow{d^{r-1}} B^{\otimes r+1} \to \cdots$$

is exact, where

$$\begin{aligned} B^{\otimes r} &= B \otimes_A B \otimes_A \cdots \otimes_A B \qquad (r \text{ times}) \\ d^{r-1} &= \sum (-1)^i e_i \\ e_i(b_0 \otimes \cdots \otimes b_{r-1}) &= b_0 \otimes \cdots \otimes b_{i-1} \otimes 1 \otimes b_i \otimes \cdots \otimes b_{r-1}. \end{aligned}$$

PROOF. It is easily checked that $d^r \circ d^{r-1} = 0$. We assume first that f admits a section, i.e., that there is a homomorphism $g\colon B \to A$ such that $g \circ f = 1$, and we construct a contracting homotopy $k_r\colon B^{\otimes r+2} \to B^{\otimes r+1}$. Define

$$k_r(b_0 \otimes \cdots \otimes b_{r+1}) = g(b_0)b_1 \otimes \cdots \otimes b_{r+1}, \qquad r \geq -1.$$

It is easily checked that

$$k_{r+1} \circ d^{r+1} + d^r \circ k_r = 1, \quad r \geq -1,$$

and this shows that the sequence is exact.

Now let A' be an A-algebra. Let $B' = A' \otimes_A B$ and let $f' = 1 \otimes f\colon A' \to B'$. The sequence corresponding to f' is obtained from the sequence for f by tensoring with A' (because $B^{\otimes r} \otimes A' \cong B'^{\otimes f}$ etc.). Thus, if A' is a faithfully flat A-algebra, it suffices to prove the theorem for f'. Take $A' = B$, and then $b \overset{f}{\mapsto} b \otimes 1\colon B \to B \otimes_A B$ has a section, namely, $g(b \otimes b') = bb'$, and so the sequence is exact. □

THEOREM 16.45. *If $f: A \to B$ is faithfully flat and M is an A-module, then the sequence*

$$0 \to M \xrightarrow{1\otimes f} M \otimes_A B \xrightarrow{1\otimes d^0} M \otimes_A B^{\otimes 2} \to \cdots \to M \otimes_B B^{\otimes r} \xrightarrow{1\otimes d^{r-1}} B^{\otimes r+1} \to \cdots$$

is exact.

PROOF. As in the above proof, one may assume that f has a section, and use it to construct a contracting homotopy. □

REMARK 16.46. Let $f: A \to B$ be a faithfully flat homomorphism, and let M be an A-module. Write M' for the B-module $f_*M = B \otimes_A M$. The module $e_{0*}M' = (B \otimes_A B) \otimes_B M'$ may be identified with $B \otimes_A M'$ where $B \otimes_A B$ acts by $(b_1 \otimes b_2)(b \otimes m) = b_1 b \otimes b_2 m$, and $e_{1*}M'$ may be identified with $M' \otimes_A B$ where $B \otimes_A B$ acts by $(b_1 \otimes b_2)(m \otimes b) = b_1 m \otimes b_2 b$. There is a canonical isomorphism $\phi: e_{1*}M' \to e_{0*}M'$ arising from

$$e_{1*}M' = (e_1 f)_*M = (e_0 f)_*M = e_{0*}M';$$

explicitly, it is the map

$$(b \otimes m) \otimes b' \mapsto b \otimes (b' \otimes m): M' \otimes_A B \to B \otimes_A M.$$

Moreover, M can be recovered from the pair (M', ϕ) because

$$M = \{m \in M' \mid 1 \otimes m = \phi(m \otimes 1)\}.$$

Conversely, every pair (M', ϕ) satisfying certain obvious conditions does arise in this way from an A-module. Given $\phi: M' \otimes_A B \to B \otimes_A M'$, define

$$\begin{aligned} \phi_1&: B \otimes_A M' \otimes_A B \to B \otimes_A B \otimes_A M' \\ \phi_2&: M' \otimes_A B \otimes_A B \to B \otimes_A B \otimes_A M', \\ \phi_3&: M' \otimes_A B \otimes_A B \to B \otimes_A M' \otimes_A B \end{aligned}$$

by tensoring ϕ with id_B in the first, second, and third positions respectively. Then a pair (M', ϕ) arises from an A-module M as above if and only if $\phi_2 = \phi_1 \circ \phi_3$. The necessity is easy to check. For the sufficiency, define

$$M = \{m \in M' \mid 1 \otimes m = \phi(m \otimes 1)\}.$$

There is a canonical map $b \otimes m \mapsto bm: B \otimes_A M \to M'$, and it suffices to show that this is an isomorphism (and that the map arising from M is ϕ). Consider the diagram

$$\begin{array}{ccc} M' \otimes_A B & \overset{\alpha\otimes 1}{\underset{\beta\otimes 1}{\rightrightarrows}} & B \otimes_A M' \otimes_A B \\ \downarrow \phi & & \downarrow \phi_1 \\ B \otimes_A M' & \overset{e_0\otimes 1}{\underset{e_1\otimes 1}{\rightrightarrows}} & B \otimes_A B \otimes_A M' \end{array}$$

in which $\alpha(m) = 1 \otimes m$ and $\beta(m) = \phi(m \otimes 1)$. As the diagram commutes with either the upper of the lower horizontal maps (for the lower maps, this uses the relation $\phi_2 = \phi_1 \circ \phi_3$), ϕ induces an isomorphism on the kernels. But, by defintion of M, the kernel of the pair $(\alpha \otimes 1, \beta \otimes 1)$ is $M \otimes_A B$, and, according to (16.45), the kernel of the pair $(e_0 \otimes 1, e_1 \otimes 1)$ is M'. This essentially completes the proof.

A regular map $\varphi\colon W \to V$ of algebraic spaces is ***faithfully flat*** if it is surjective on the underlying sets and $\mathcal{O}_{\varphi(P)} \to \mathcal{O}_P$ is flat for all $P \in W$, and it is ***affine*** if the inverse images of open affines in V are open affines in W.

THEOREM 16.47. *Let $\varphi\colon W \to V$ be a faithfully flat map of algebraic spaces. To give an algebraic space U affine over V is the same as to give an algebraic space U' affine over V together with an isomorphism $\phi\colon p_1^*U' \to p_2^*U'$ satisfying*

$$p_{31}^*(\phi) = p_{32}^*(\phi) \circ p_{21}^*(\phi).$$

Here p_{ji} denotes the projection $W \times W \times W \to W \times W$ such that $p_{ji}(w_1, w_2, w_3) = (w_j, w_i)$.

PROOF. When W and V are affine, (16.46) gives a similar statement for modules, hence for algebras, and hence for algebraic spaces. $\square$

EXAMPLE 16.48. Let Γ be a finite group, and regard it as an algebraic group of dimension 0. Let V be an algebraic space over k. An algebraic space ***Galois over V with Galois group Γ*** is a finite map $W \to V$ to algebraic space together with a regular map $W \times \Gamma \to W$ such that

(a) for all k-algebras R, $W(R) \times \Gamma(R) \to W(R)$ is an action of the group $\Gamma(R)$ on the set $W(R)$ in the usual sense, and the map $W(R) \to V(R)$ is compatible with the action of $\Gamma(R)$ on $W(R)$ and its trivial action on $V(R)$, and
(b) the map $(w, \sigma) \mapsto (w, w\sigma)\colon W \times \Gamma \to W \times_V W$ is an isomorphism.

Then there is a commutative diagram[7]

$$\begin{array}{ccccccc}
V & \leftarrow & W & \leftleftarrows & W \times \Gamma & \substack{\leftarrow \\ \leftarrow \\ \leftarrow} & W \times \Gamma^2 \\
\| & & \| & & \downarrow \simeq & & \downarrow \simeq \\
V & \leftarrow & W & \leftleftarrows & W \times_V W & \substack{\leftarrow \\ \leftarrow \\ \leftarrow} & W \times_V W \times_V W
\end{array}$$

The vertical isomorphisms are

$$(w, \sigma) \mapsto (w, w\sigma)$$
$$(w, \sigma_1, \sigma_2) \mapsto (w, w\sigma_1, w\sigma_1\sigma_2).$$

Therefore, in this case, Theorem 16.47 says that to give an algebraic space affine over V is the same as to give an algebraic space affine over W together with an action of Γ on it compatible with that on W. When we take W and V to be the spectra of fields, then this becomes affine case of Theorem 16.23.

EXAMPLE 16.49. In Theorem 16.47, let φ be the map corresponding to a regular extension of fields $k \to k(t)$. This case of Theorem 16.47 coincides with the affine case of Theorem 16.36 except that the field $k(t, t')$ has been replaced by the ring $k(t) \otimes_k k(t')$.

[7] See Milne, J. S., Etale cohomology. Princeton, 1980, p100.

NOTES. The paper of Weil cited in subsection on Weil's descent theorems is the first important paper in descent theory. Its results haven't been superseded by the many results of Grothendieck on descent. In Milne 1999[8], Theorem 16.33 was deduced from Weil's theorems. The present more elementary proof was suggested by Wolfart's elementary proof of the 'obvious' part of Belyi's theorem (Wolfart 1997[9]; see also Derome 2003[10]).

[8]Milne, J. S., Descent for Shimura varieties. Michigan Math. J. 46 (1999), no. 1, 203–208.

[9]Wolfart, Jürgen. The "obvious" part of Belyi's theorem and Riemann surfaces with many automorphisms. Geometric Galois actions, 1, 97–112, London Math. Soc. Lecture Note Ser., 242, Cambridge Univ. Press, Cambridge, 1997.

[10]Derome, G., Descente algébriquement close, J. Algebra, 266 (2003), 418–426.

Chapter 17

Lefschetz Pencils (Outline)

In this chapter, we see how to fibre a variety over $\mathbb{P}^1$ in such a way that the fibres have only very simple singularities. This result sometimes allows one to prove theorems by induction on the dimension of the variety. For example, Lefschetz initiated this approach in order to study the cohomology of varieties over $\mathbb{C}$.

Throughout this chapter, k is an algebraically closed field.

Definition

A linear form $H = \sum_{i=0}^{m} a_i T_i$ defines a hyperplane in $\mathbb{P}^m$, and two linear forms define the same hyperplane if and only if one is a nonzero multiple of the other. Thus the hyperplanes in $\mathbb{P}^m$ form a projective space, called the ***dual projective space*** $\check{\mathbb{P}}^m$.

A line D in $\check{\mathbb{P}}^m$ is called a ***pencil*** of hyperplanes in $\mathbb{P}^m$. If H_0 and H_∞ are any two distinct hyperplanes in D, then the pencil consists of all hyperplanes of the form $\alpha H_0 + \beta H_\infty$ with $(\alpha{:}\,\beta) \in \mathbb{P}^1(k)$. If $P \in H_0 \cap H_\infty$, then it lies on every hyperplane in the pencil — the ***axis*** A of the pencil is defined to be the set of such P. Thus

$$A = H_0 \cap H_\infty = \cap_{t \in D} H_t.$$

The axis of the pencil is a linear subvariety of codimension 2 in $\mathbb{P}^m$, and the hyperplanes of the pencil are exactly those containing the axis. Through any point in $\mathbb{P}^m$ not on A, there passes exactly one hyperplane in the pencil. Thus, one should imagine the hyperplanes in the pencil as sweeping out $\mathbb{P}^m$ as they rotate about the axis.

Let V be a nonsingular projective variety of dimension $d \geq 2$, and embed V in some projective space $\mathbb{P}^m$. By the square of an embedding, we mean the composite of $V \hookrightarrow \mathbb{P}^m$ with the Veronese mapping (6.20)

$$(x_0{:}\ldots{:}x_m) \mapsto (x_0^2{:}\ldots{:}x_i x_j{:}\ldots{:}x_m^2){:}\, \mathbb{P}^m \to \mathbb{P}^{\frac{(m+2)(m+1)}{2}}.$$

DEFINITION 17.1. A line D in $\check{\mathbb{P}}^m$ is said to be a ***Lefschetz pencil*** for $V \subset \mathbb{P}^m$ if

(a) the axis A of the pencil $(H_t)_{t \in D}$ cuts V transversally;
(b) the hyperplane sections $V_t \overset{\text{def}}{=} V \cap H_t$ of V are nonsingular for all t in some open dense subset U of D;
(c) for $t \notin U$, V_t has only a single singularity, and the singularity is an ordinary double point.

Condition (a) means that, for every point $P \in A \cap V$, $\mathrm{Tgt}_P(A) \cap \mathrm{Tgt}_P(V)$ has codimension 2 in $\mathrm{Tgt}_P(V)$.

Condition (b) means that, except for a finite number of t, H_t cuts V transversally, i.e., for every point $P \in H_t \cap V$, $\mathrm{Tgt}_P(H_t) \cap \mathrm{Tgt}_P(V)$ has codimension 1 in $\mathrm{Tgt}_P(V)$.

A point P on a variety V of dimension d is an ***ordinary double point*** if the tangent cone at P is isomorphic to the subvariety of $\mathbb{A}^{d+1}$ defined by a nondegenerate quadratic form $Q(T_1, \ldots, T_{d+1})$, or, equivalently, if

$$\hat{\mathcal{O}}_{V,P} \approx k[[T_1, \ldots, T_{d+1}]]/(Q(T_1, \ldots, T_{d+1})).$$

THEOREM 17.2. *There exists a Lefschetz pencil for V (after possibly replacing the projective embedding of V by its square).*

PROOF. (Sketch). Let $W \subset V \times \check{\mathbb{P}}^m$ be the closed variety whose points are the pairs (x, H) such that H contains the tangent space to V at x. For example, if V has codimension 1 in $\mathbb{P}^m$, then $(x, H) \in Y$ if and only if H is the tangent space at x. In general,

$$(x, H) \in W \iff x \in H \text{ and } H \text{ does not cut } V \text{ transversally at } x.$$

The image of W in $\check{\mathbb{P}}^m$ under the projection $V \times \check{\mathbb{P}}^m \to \check{\mathbb{P}}^m$ is called the ***dual variety*** $\check{V}$ of V. The fibre of $W \to V$ over x consists of the hyperplanes containing the tangent space at x, and these hyperplanes form an irreducible subvariety of $\check{\mathbb{P}}^m$ of dimension $m - (\dim V + 1)$; it follows that W is irreducible, complete, and of dimension $m - 1$ (see 10.11) and that $\check{V}$ is irreducible, complete, and of codimension ≥ 1 in $\check{\mathbb{P}}^m$ (unless $V = \mathbb{P}^m$, in which case it is empty). The map φ: $W \to \check{V}$ is unramified at (x, H) if and only if x is an ordinary double point on $V \cap H$ (see SGA 7, XVII 3.7[1]). Either φ is generically unramified, or it becomes so when the embedding is replaced by its square (so, instead of hyperplanes, we are working with quadric hypersurfaces) (ibid. 3.7). We may assume this, and then (ibid. 3.5), one can show that for $H \in \check{V} \smallsetminus \check{V}_{\mathrm{sing}}$, $V \cap H$ has only a single singularity and the singularity is an ordinary double point. Here $\check{V}_{\mathrm{sing}}$ is the singular locus of $\check{V}$.

By Bertini's theorem (Hartshorne 1977, II 8.18) there exists a hyperplane H_0 such that $H_0 \cap V$ is irreducible and nonsingular. Since there is an $(m-1)$-dimensional space of lines through H_0, and at most an $(m-2)$-dimensional family will meet V_{sing}, we can choose H_∞ so that the line D joining H_0 and H_∞ does not meet $\check{V}_{\mathrm{sing}}$. Then D is a Lefschetz pencil for V. □

THEOREM 17.3. *Let $D = (H_t)$ be a Lefschetz pencil for V with axis $A = \cap H_t$. Then there exists a variety V^* and maps*

$$V \leftarrow V^* \xrightarrow{\pi} D.$$

such that:

(a) *the map $V^* \to V$ is the blowing up of V along $A \cap V$;*

[1] Groupes de monodromie en géométrie algébrique. Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7). Dirigé par A. Grothendieck. Lecture Notes in Mathematics, Vol. 288, 340. Springer-Verlag, Berlin-New York, 1972, 1973.

(b) *the fibre of* $V^* \to D$ *over* t *is* $V_t = V \cap H_t$.

Moreover, π *is proper, flat, and has a section.*

PROOF. (Sketch) Through each point x of $V \smallsetminus A \cap V$, there will be exactly one H_x in D. The map

$$\varphi\colon V \smallsetminus A \cap V \to D,\, x \mapsto H_x,$$

is regular. Take the closure of its graph Γ_φ in $V \times D$; this will be the graph of π. □

REMARK 17.4. The singular V_t may be reducible. For example, if V is a quadric surface in $\mathbb{P}^3$, then V_t is curve of degree 2 in $\mathbb{P}^2$ for all t, and such a curve is singular if and only if it is reducible (look at the formula for the genus). However, if the embedding $V \hookrightarrow \mathbb{P}^m$ is replaced by its cube, this problem will never occur.

References

The only modern reference I know of is SGA 7, Exposé XVII.

Chapter 18

Algebraic Schemes and Algebraic Spaces

In this course, we have attached an affine algebraic variety to any algebra finitely generated 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, $A \mapsto \operatorname{spm} A$ is not functorial in this generality: if $\varphi\colon A \to B$ is a homomorphism of rings, then $\varphi^{-1}(\mathfrak{m})$ for $\mathfrak{m}$ maximal need not be maximal — consider for example the inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$. Thus he was forced to replace $\operatorname{spm}(A)$ 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 algebraic spaces over k to the category of schemes of finite-type over k, which is an equivalence of categories. The algebraic varieties correspond to geometrically reduced schemes. To construct V^* from V, one only has to add one point p_Z for each irreducible closed subvariety Z of V. For any open subset U of V, let U^* be the subset of V^* containing the points of U together with the points p_Z such that $U \cap Z$ is nonempty. Thus, $U \mapsto U^*$ 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. For a closed irreducible subset Z of V, the local ring $\mathcal{O}_{V^*,p_Z} = \varinjlim_{U \cap Z \neq \emptyset} \Gamma(U, \mathcal{O}_U)$. The reverse functor is even easier: simply omit the nonclosed points from the base space.[1]

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.

[1] Some authors call a geometrically reduced scheme of finite-type over a field a variety. Despite their similarity, it is important to distinguish such schemes from varieties (in the sense of these notes). For example, if W and W' are subvarieties of a variety, their intersection in the sense of schemes need not be reduced, and so may differ from their intersection in the sense of varieties. For example, if $W = V(\mathfrak{a}) \subset \mathbb{A}^n$ and $W' = V(\mathfrak{a}') \subset \mathbb{A}^{n'}$ with $\mathfrak{a}$ and $\mathfrak{a}'$ radical, then the intersection W and W' in the sense of schemes is $\operatorname{Spec} k[X_1, \ldots, X_{n+n'}]/(\mathfrak{a}, \mathfrak{a}')$ while their intersection in the sense of varieties is $\operatorname{Spec} k[X_1, \ldots, X_{n+n'}]/\operatorname{rad}(\mathfrak{a}, \mathfrak{a}')$ (and their intersection in the sense of algebraic spaces is $\operatorname{Spm} k[X_1, \ldots, X_{n+n'}]/(\mathfrak{a}, \mathfrak{a}')$).

Appendix A

Solutions to the exercises

1-1 Use induction on n. For $n = 1$, use that a nonzero polynomial in one variable has only finitely many roots (which follows from unique factorization, for example). Now suppose $n > 1$ and write $f = \sum g_i X_n^i$ with each $g_i \in k[X_1, \ldots, X_{n-1}]$. If f is not the zero polynomial, then some g_i is not the zero polynomial. Therefore, by induction, there exist $(a_1, \ldots, a_{n-1}) \in k^{n-1}$ such that $f(a_1, \ldots, a_{n-1}, X_n)$ is not the zero polynomial. Now, by the degree-one case, there exists a b such that $f(a_1, \ldots, a_{n-1}, b) \neq 0$.

1-2 $(X + 2Y, Z)$; Gaussian elimination (to reduce the matrix of coefficients to row echelon form); (1), unless the characteristic of k is 2, in which case the ideal is $(X + 1, Z + 1)$.

2-1 $W = Y$-axis, and so $I(W) = (X)$. Clearly,

$$(X^2, XY^2) \subset (X) \subset \mathrm{rad}(X^2, XY^2)$$

and $\mathrm{rad}((X)) = (X)$. On taking radicals, we find that $(X) = \mathrm{rad}(X^2, XY^2)$.

2-2 The $d \times d$ minors of a matrix are polynomials in the entries of the matrix, and the set of matrices with rank $\leq r$ is the set where all $(r + 1) \times (r + 1)$ minors are zero.

2-3 Clearly $V = V(X_n - X_1^n, \ldots, X_2 - X_1^2)$. The map

$$X_i \mapsto T^i : k[X_1, \ldots, X_n] \to k[T]$$

induces an isomorphism $k[V] \to \mathbb{A}^1$. [Hence $t \mapsto (t, \ldots, t^n)$ is an isomorphism of affine varieties $\mathbb{A}^1 \to V$.]

2-4 We use that the prime ideals are in one-to-one correspondence with the closed irreducible subsets Z of $\mathbb{A}^2$. For such a set, $0 \leq \dim Z \leq 2$.

Case $\dim Z = 2$. Then $Z = \mathbb{A}^2$, and the corresponding ideal is (0).

Case $\dim Z = 1$. Then $Z \neq \mathbb{A}^2$, and so $I(Z)$ contains a nonzero polynomial $f(X, Y)$. If $I(Z) \neq (f)$, then $\dim Z = 0$ by (2.25, 2.26). Hence $I(Z) = (f)$.

Case $\dim Z = 0$. Then Z is a point (a, b) (see 2.24c), and so $I(Z) = (X - a, Y - b)$.

2-5 The statement $\mathrm{Hom}_{k\text{-algebras}}(A \otimes_{\mathbb{Q}} k, B \otimes_{\mathbb{Q}} k) \neq \emptyset$ can be interpreted as saying that a certain set of polynomials has a zero in k. If the polynomials have a common zero in $\mathbb{C}$, then the ideal they generate in $\mathbb{C}[X_1, \ldots]$ does not contain 1. *A fortiori* the ideal they generate in $k[X_1, \ldots]$ does not contain 1, and so the Nullstellensatz (2.6) implies that the polynomials have a common zero in k.

3-1 A map $\alpha\colon \mathbb{A}^1 \to \mathbb{A}^1$ is continuous for the Zariski topology if the inverse images of finite sets are finite, whereas it is regular only if it is given by a polynomial $P \in k[T]$, so it is easy to give examples, e.g., any map α such that $\alpha^{-1}(\text{point})$ is finite but arbitrarily large.

3-2 The argument in the text shows that, for any $f \in S$,

$$f(a_1,\ldots,a_n) = 0 \implies f(a_1^q,\ldots,a_n^q) = 0.$$

This implies that φ maps V into itself, and it is obviously regular because it is defined by polynomials.

3-3 The image omits the points on the Y-axis except for the origin. The complement of the image is not dense, and so it is not open, but any polynomial zero on it is also zero at $(0,0)$, and so it not closed.

3-5 No, because both $+1$ and -1 map to $(0,0)$. The map on rings is

$$k[x,y] \to k[T], \quad x \mapsto T^2-1, \quad y \mapsto T(T^2-1),$$

which is not surjective (T is not in the image).

4-1 Let f be regular on $\mathbb{P}^1$. Then $f|U_0 = P(X) \in k[X]$, where X is the regular function $(a_0\colon a_1) \mapsto a_1/a_0\colon U_0 \to k$, and $f|U_1 = Q(Y) \in k[Y]$, where Y is $(a_0\colon a_1) \mapsto a_0/a_1$. On $U_0 \cap U_1$, X and Y are reciprocal functions. Thus $P(X)$ and $Q(1/X)$ define the same function on $U_0 \cap U_1 = \mathbb{A}^1 \smallsetminus \{0\}$. This implies that they are equal in $k(X)$, and must both be constant.

4-2 Note that $\Gamma(V,\mathcal{O}_V) = \prod \Gamma(V_i,\mathcal{O}_{V_i})$ — to give a regular function on $\bigsqcup V_i$ is the same as to give a regular function on each V_i (this is the "obvious" ringed space structure). Thus, if V is affine, it must equal $\mathrm{Specm}(\prod A_i)$, where $A_i = \Gamma(V_i,\mathcal{O}_{V_i})$, and so $V = \bigsqcup \mathrm{Specm}(A_i)$ (use the description of the ideals in $A \times B$ on p6). Etc..

4-3 Let H be an algebraic subgroup of G. By definition, H is locally closed, i.e., open in its Zariski closure $\bar{H}$. Assume first that H is connected. Then $\bar{H}$ is a connected algebraic group, and it is a disjoint union of the cosets of H. It follows that $H = \bar{H}$. In the general case, H is a finite disjoint union of its connected components; as one component is closed, they all are.

5-1 (b) The singular points are the common solutions to

$$\begin{cases} 4X^3 - 2XY^2 = 0 & \implies \quad X = 0 \text{ or } Y^2 = 2X^2 \\ 4Y^3 - 2X^2Y = 0 & \implies \quad Y = 0 \text{ or } X^2 = 2Y^2 \\ X^4 + Y^4 - X^2Y^2 = 0. & \end{cases}$$

Thus, only $(0,0)$ is singular, and the variety is its own tangent cone.

5-2 Directly from the definition of the tangent space, we have that

$$T_{\mathbf{a}}(V \cap H) \subset T_{\mathbf{a}}(V) \cap T_{\mathbf{a}}(H).$$

As

$$\dim T_{\mathbf{a}}(V \cap H) \geq \dim V \cap H = \dim V - 1 = \dim T_{\mathbf{a}}(V) \cap T_{\mathbf{a}}(H),$$

we must have equalities everywhere, which proves that $\mathbf{a}$ is nonsingular on $V \cap H$. (In particular, it can't lie on more than one irreducible component.)

The surface $Y^2 = X^2 + Z$ is smooth, but its intersection with the X-Y plane is singular.

No, P needn't be singular on $V \cap H$ if $H \supset T_P(V)$ — for example, we could have $H \supset V$ or H could be the tangent line to a curve.

5-3 We can assume V and W to affine, say

$$I(V) = \mathfrak{a} \subset k[X_1, \ldots, X_m]$$
$$I(W) = \mathfrak{b} \subset k[X_{m+1}, \ldots, X_{m+n}].$$

If $\mathfrak{a} = (f_1, \ldots, f_r)$ and $\mathfrak{b} = (g_1, \ldots, g_s)$, then $I(V \times W) = (f_1, \ldots, f_r, g_1, \ldots, g_s)$. Thus, $T_{(\mathbf{a},\mathbf{b})}(V \times W)$ is defined by the equations

$$(df_1)_{\mathbf{a}} = 0, \ldots, (df_r)_{\mathbf{a}} = 0, (dg_1)_{\mathbf{b}} = 0, \ldots, (dg_s)_{\mathbf{b}} = 0,$$

which can obviously be identified with $T_{\mathbf{a}}(V) \times T_{\mathbf{b}}(W)$.

5-4 Take C to be the union of the coordinate axes in $\mathbb{A}^n$. (Of course, if you want C to be irreducible, then this is more difficult...)

5-5 A matrix A satisfies the equations

$$(I + \varepsilon A)^{\mathrm{tr}} \cdot J \cdot (I + \varepsilon A) = I$$

if and only if

$$A^{\mathrm{tr}} \cdot J + J \cdot A = 0.$$

Such an A is of the form $\begin{pmatrix} M & N \\ P & Q \end{pmatrix}$ with M, N, P, Q $n \times n$-matrices satisfying

$$N^{\mathrm{tr}} = N, \quad P^{\mathrm{tr}} = P, \quad M^{\mathrm{tr}} = -Q.$$

The dimension of the space of A's is therefore

$$\frac{n(n+1)}{2} \text{ (for } N) + \frac{n(n+1)}{2} \text{ (for } P) + n^2 \text{ (for } M, Q) = 2n^2 + n.$$

5-6 Let C be the curve $Y^2 = X^3$, and consider the map $\mathbb{A}^1 \to C$, $t \mapsto (t^2, t^3)$. The corresponding map on rings $k[X, Y]/(Y^2) \to k[T]$ is not an isomorphism, but the map on the geometric tangent cones is an isomorphism.

5-7 The singular locus V_{sing} has codimension ≥ 2 in V, and this implies that V is normal. [Idea of the proof: let $f \in k(V)$ be integral over $k[V]$, $f \notin k[V]$, $f = g/h$, $g, h \in k[V]$; for any $P \in V(h) \smallsetminus V(g)$, $\mathcal{O}_P$ is not integrally closed, and so P is singular.]

5-8 No! Let $\mathfrak{a} = (X^2 Y)$. Then $V(\mathfrak{a})$ is the union of the X and Y axes, and $IV(\mathfrak{a}) = (XY)$. For $\mathbf{a} = (a, b)$,

$$(dX^2Y)_{\mathbf{a}} = 2ab(X - a) + a^2(Y - b)$$
$$(dXY)_{\mathbf{a}} = b(X - a) + a(Y - b).$$

If $a \neq 0$ and $b = 0$, then the equations

$$(dX^2Y)_{\mathbf{a}} = a^2 Y = 0$$
$$(dXY)_{\mathbf{a}} = aY = 0$$

have the same solutions.

6-1 Let $P = (a : b : c)$, and assume $c \neq 0$. Then the tangent line at $P = (\frac{a}{c} : \frac{b}{c} : 1)$ is

$$\left(\frac{\partial F}{\partial X}\right)_P X + \left(\frac{\partial F}{\partial Y}\right)_P Y - \left(\left(\frac{\partial F}{\partial X}\right)_P \left(\frac{a}{c}\right) + \left(\frac{\partial F}{\partial Y}\right)_P \left(\frac{b}{c}\right)\right) Z = 0.$$

Now use that, because F is homogeneous,

$$F(a, b, c) = 0 \implies \left(\frac{\partial F}{\partial X}\right)_P a + \left(\frac{\partial F}{\partial Y}\right)_P + \left(\frac{\partial F}{\partial Z}\right)_P c = 0.$$

(This just says that the tangent plane at (a, b, c) to the affine cone $F(X, Y, Z) = 0$ passes through the origin.) The point at ∞ is $(0 : 1 : 0)$, and the tangent line is $Z = 0$, the line at ∞. [The line at ∞ meets the cubic curve at only one point instead of the expected 3, and so the line at ∞ "touches" the curve, and the point at ∞ is a point of inflexion.]

6-2 The equation defining the conic must be irreducible (otherwise the conic is singular). After a linear change of variables, the equation will be of the form $X^2 + Y^2 = Z^2$ (this is proved in calculus courses). The equation of the line in $aX + bY = cZ$, and the rest is easy. [Note that this is a special case of Bezout's theorem (6.34) because the multiplicity is 2 in case (b).]

6-3 (a) The ring

$$k[X, Y, Z]/(Y - X^2, Z - X^3) = k[x, y, z] = k[x] \simeq k[X],$$

which is an integral domain. Therefore, $(Y - X^2, Z - X^3)$ is a radical ideal.

(b) The polynomial $F = Z - XY = (Z - X^3) - X(Y - X^2) \in I(V)$ and $F^* = ZW - XY$. If

$$ZW - XY = (YW - X^2)f + (ZW^2 - X^3)g,$$

then, on equating terms of degree 2, we would find

$$ZW - XY = a(YW - X^2),$$

which is false.

6-4 Let $P = (a_0 : \ldots : a_n)$ and $Q = (b_0 : \ldots : b_n)$ be two points of $\mathbb{P}^n$, $n \geq 2$. The condition that the hyperplane $L_{\mathbf{c}}$: $\sum c_i X_i = 0$ pass through P and not through Q is that

$$\sum a_i c_i = 0, \quad \sum b_i c_i \neq 0.$$

The $(n + 1)$-tuples $(c_0, \ldots, c_n)$ satisfying these conditions form a nonempty open subset of the hyperplane $H: \sum a_i X_i = 0$ in $\mathbb{A}^{n+1}$. On applying this remark to the pairs (P_0, P_i), we find that the $(n + 1)$-tuples $\mathbf{c} = (c_0, \ldots, c_n)$ such that P_0 lies on the hyperplane $L_{\mathbf{c}}$ but not $P_1, \ldots, P_r$ form a nonempty open subset of H.

6-5 The subset

$$C = \{(a : b : c) \mid a \neq 0, \quad b \neq 0\} \cup \{(1 : 0 : 0)\}$$

of $\mathbb{P}^2$ is not locally closed. Let $P = (1 : 0 : 0)$. If the set C were locally closed, then P would have an open neighbourhood U in $\mathbb{P}^2$ such that $U \cap C$ is closed. When we look in U_0, P becomes the origin, and

$$C \cap U_0 = (\mathbb{A}^2 \smallsetminus \{X\text{-axis}\}) \cup \{\text{origin}\}.$$

The open neighbourhoods U of P are obtained by removing from $\mathbb{A}^2$ a finite number of curves not passing through P. It is not possible to do this in such a way that $U \cap C$ is closed in U ($U \cap C$ has dimension 2, and so it can't be a proper closed subset of U; we can't have $U \cap C = U$ because any curve containing all nonzero points on X-axis also contains the origin).

7-2 Define $f(v) = h(v, Q)$ and $g(w) = h(P, w)$, and let $\varphi = h - (f \circ p + g \circ q)$. Then $\varphi(v, Q) = 0 = \varphi(P, w)$, and so the rigidity theorem (7.13) implies that φ is identically zero.

6-6 Let $\sum c_{ij} X_{ij} = 0$ be a hyperplane containing the image of the Segre map. We then have

$$\sum c_{ij} a_i b_j = 0$$

for all $\mathbf{a} = (a_0, \ldots, a_m) \in k^{m+1}$ and $\mathbf{b} = (b_0, \ldots, b_n) \in k^{n+1}$. In other words,

$$\mathbf{a} C \mathbf{b}^t = 0$$

for all $\mathbf{a} \in k^{m+1}$ and $\mathbf{b} \in k^{n+1}$, where C is the matrix (c_{ij}). This equation shows that $\mathbf{a}C = 0$ for all $\mathbf{a}$, and this implies that $C = 0$.

8-2 For example, consider

$$(\mathbb{A}^1 \smallsetminus \{1\}) \to \mathbb{A}^1 \stackrel{x \mapsto x^n}{\to} \mathbb{A}^1$$

for $n > 1$ an integer prime to the characteristic. The map is obviously quasi-finite, but it is not finite because it corresponds to the map of k-algebras

$$X \mapsto X^n \colon k[X] \to k[X, (X-1)^{-1}]$$

which is not finite (the elements $1/(X-1)^i$, $i \geq 1$, are linearly independent over $k[X]$, and so also over $k[X^n]$).

8-3 Assume that V is separated, and consider two regular maps $f, g \colon Z \rightrightarrows W$. We have to show that the set on which f and g agree is closed in Z. The set where $\varphi \circ f$ and $\varphi \circ g$ agree is closed in Z, and it contains the set where f and g agree. Replace Z with the set where $\varphi \circ f$ and $\varphi \circ g$ agree. Let U be an open affine subset of V, and let $Z' = (\varphi \circ f)^{-1}(U) = (\varphi \circ g)^{-1}(U)$. Then $f(Z')$ and $g(Z')$ are contained in $\varphi^{-1}(U)$, which is an open affine subset of W, and is therefore separated. Hence, the subset of Z' on which f and g agree is closed. This proves the result.

[Note that the problem implies the following statement: if $\varphi \colon W \to V$ is a finite regular map and V is separated, then W is separated.]

8-4 Let $V = \mathbb{A}^n$, and let W be the subvariety of $\mathbb{A}^n \times \mathbb{A}^1$ defined by the polynomial

$$\prod_{i=1}^n (X - T_i) = 0.$$

The fibre over $(t_1, \ldots, t_n) \in \mathbb{A}^n$ is the set of roots of $\prod (X - t_i)$. Thus, $V_n = \mathbb{A}^n$; V_{n-1} is the union of the linear subspaces defined by the equations

$$T_i = T_j, \quad 1 \leq i, j \leq n, \quad i \neq j;$$

V_{n-2} is the union of the linear subspaces defined by the equations

$$T_i = T_j = T_k, \quad 1 \leq i, j, k \leq n, \quad i, j, k \text{ distinct},$$

and so on.

10-1 Consider an orbit $O = Gv$. The map $g \mapsto gv \colon G \to O$ is regular, and so O contains an open subset U of $\bar{O}$ (10.2). If $u \in U$, then $gu \in gU$, and gU is also a subset of O which is open in $\bar{O}$ (because $P \mapsto gP \colon V \to V$ is an isomorphism). Thus O, regarded as a topological subspace of $\bar{O}$, contains an open neighbourhood of each of its points, and so must be open in $\bar{O}$.

We have shown that O is locally closed in V, and so has the structure of a subvariety. From (5.18), we know that it contains at least one nonsingular point P. But then gP is nonsingular, and every point of O is of this form.

From set theory, it is clear that $\bar{O} \smallsetminus O$ is a union of orbits. Since $\bar{O} \smallsetminus O$ is a proper closed subset of $\bar{O}$, all of its subvarieties must have dimension $< \dim \bar{O} = \dim O$.

Let O be an orbit of lowest dimension. The last statement implies that $O = \bar{O}$.

10-2 An orbit of type (a) is closed, because it is defined by the equations

$$\mathrm{Tr}(A) = -a, \quad \det(A) = b,$$

(as a subvariety of V). It is of dimension 2, because the centralizer of $\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$, $\alpha \neq \beta$, is $\left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \right\}$, which has dimension 2.

An orbit of type (b) is of dimension 2, but is not closed: it is defined by the equations

$$\mathrm{Tr}(A) = -a, \quad \det(A) = b, \quad A \neq \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}, \quad \alpha = \text{root of } X^2 + aX + b.$$

An orbit of type (c) is closed of dimension 0: it is defined by the equation $A = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$. An orbit of type (b) contains an orbit of type (c) in its closure.

10-3 Let ζ be a primitive d^{th} root of 1. Then, for each i, j, $1 \leq i, j \leq d$, the following equations define lines on the surface

$$\begin{cases} X_0 + \zeta^i X_1 = 0 \\ X_2 + \zeta^j X_3 = 0 \end{cases} \quad \begin{cases} X_0 + \zeta^i X_2 = 0 \\ X_1 + \zeta^j X_3 = 0 \end{cases} \quad \begin{cases} X_0 + \zeta^i X_3 = 0 \\ X_1 + \zeta^j X_2 = 0. \end{cases}$$

There are three sets of lines, each with d^2 lines, for a total of $3d^2$ lines.

10-4 (a) Compare the proof of Theorem 10.9.

(b) Use the transitivity, and apply Proposition 8.24.

12-1 Let H be a hyperplane in $\mathbb{P}^n$ intersecting V transversally. Then $H \approx \mathbb{P}^{n-1}$ and $V \cap H$ is again defined by a polynomial of degree δ. Continuing in this fashion, we find that

$$V \cap H_1 \cap \ldots \cap H_d$$

is isomorphic to a subset of $\mathbb{P}^1$ defined by a polynomial of degree δ.

12-2 We may suppose that X is not a factor of F_m, and then look only at the affine piece of the blow-up, $\sigma \colon \mathbb{A}^2 \to \mathbb{A}^2$, $(x, y) \mapsto (x, xy)$. Then $\sigma^{-1}(C \smallsetminus (0,0))$is given by equations

$$X \neq 0, \quad F(X, XY) = 0.$$

But

$$F(X, XY) = X^m(\prod(a_i - b_iY)^{r_i}) + X^{m+1}F_{m+1}(X, Y) + \cdots,$$

and so $\sigma^{-1}(C \smallsetminus (0,0))$ is also given by equations

$$X \neq 0, \quad \prod(a_i - b_iY)^{r_i} + XF_{m+1}(X, Y) + \cdots = 0.$$

To find its closure, drop the condition $X \neq 0$. It is now clear that the closure intersects $\sigma^{-1}(0,0)$ (the Y-axis) at the s points $Y = a_i/b_i$.

12-3 We have to find the dimension of $k[X, Y]_{(X,Y)}/(Y^2 - X^r, Y^2 - X^s)$. In this ring, $X^r = X^s$, and so $X^s(X^{r-s} - 1) = 0$. As $X^{r-s} - 1$ is a unit in the ring, this implies that $X^s = 0$, and it follows that $Y^2 = 0$. Thus $(Y^2 - X^r, Y^2 - X^s) \supset (Y^2, X^s)$, and in fact the two ideals are equal in $k[X, Y]_{(X,Y)}$. It is now clear that the dimension is $2s$.

12-4 Note that

$$k[V] = k[T^2, T^3] = \left\{\sum a_iT^i \mid a_i = 0\right\}.$$

For each $a \in k$, define an effective divisor D_a on V as follows:
D_a has local equation $1 - a^2T^2$ on the set where $1 + aT \neq 0$;
D_a has local equation $1 - a^3T^3$ on the set where $1 + aT + aT^2 \neq 0$.
The equations

$$(1 - aT)(1 + aT) = 1 - a^2T^2, \quad (1 - aT)(1 + aT + a^2T^2) = 1 - a^3T^3$$

show that the two divisors agree on the overlap where

$$(1 + aT)(1 + aT + aT^2) \neq 0.$$

For $a \neq 0$, D_a is not principal, essentially because

$$\gcd(1 - a^2T^2, 1 - a^3T^3) = (1 - aT) \notin k[T^2, T^3]$$

— if D_a were principal, it would be a divisor of a regular function on V, and that regular function would have to be $1 - aT$, but this is not allowed.

In fact, one can show that $\mathrm{Pic}(V) \approx k$. Let $V' = V \smallsetminus \{(0,0)\}$, and write $P(*)$ for the principal divisors on $*$. Then $\mathrm{Div}(V') + P(V) = \mathrm{Div}(V)$, and so

$$\mathrm{Div}(V)/P(V) \simeq \mathrm{Div}(V')/\mathrm{Div}(V') \cap P(V) \simeq P(V')/P(V') \cap P(V) \simeq k.$$

Appendix B

Annotated Bibliography

Apart from Hartshorne 1977, 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.

Matsumura, H., Commutative Ring Theory, Cambridge 1986. This is the most useful medium-length text (but read Atiyah and MacDonald or Reid first).

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

Abhyankar, S., Algebraic Geometry for Scientists and Engineers, AMS, 1990. Mainly curves, from a very explicit and down-to-earth point of view.

Reid, M., Undergraduate Algebraic Geometry. A brief, elementary introduction. The final chapter contains an interesting, but idiosyncratic, account of algebraic geometry in the twentieth century.

Smith, Karen E.; Kahanpää, Lauri; Kekäläinen, Pekka; Traves, William. An invitation to algebraic geometry. Universitext. Springer-Verlag, New York, 2000. An introductory overview with few proofs but many pictures.

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

Harris, Joe: Algebraic Geometry: A first course, Springer, 1992. The emphasis is on examples.

Musili, C. Algebraic geometry for beginners. Texts and Readings in Mathematics, 20. Hindustan Book Agency, New Delhi, 2001.

Shafarevich, I., Basic Algebraic Geometry, Book 1, Springer, 1994. Very easy to read.

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, Birkhäuser, 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. 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, 1999. 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.

Index