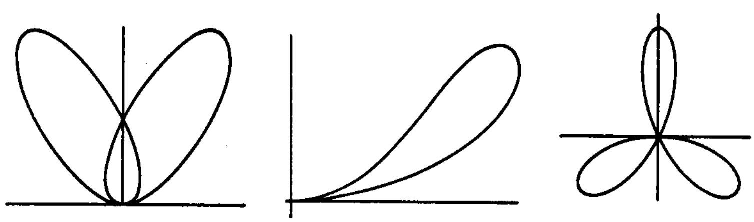
Algebraic Geometry

J.S. Milne



Version 6.10
November 11, 2024

These notes are an introduction to the theory of algebraic varieties emphasizing the similarities to the theory of manifolds. 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.

Before learning scheme theory everyone should understand algebraic varieties over algebraically closed fields: first the geometric intuition and then the abstractions.

```
BibTeX information
@misc{milneAG,
  author={Milne, James S.},
  title={Algebraic Geometry (v6.1)},
  year={2024},
  note={Available at www.jmilne.org/math/},
  pages={231}
}
```


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; TEXstyle changed, so page numbers changed; 241 pages.

v5.20 (September 14, 2009). Minor corrections; revised Chapters 1, 11, 16; 245 pages.

v5.22 (January 13, 2012). Minor fixes; 260 pages.

v6.00 (August 24, 2014). Major revision; split off the basic first course from the topics; 223 pages.

v6.01 (August 23, 2015). Minor fixes; 226 pages.

v6.02 (March 19, 2017). Minor fixes; 221 pages.

v6.03 (November 2, 2023). Minor fixes; 223 pages.

v6.10 (November 11, 2024). Minor improvements; 231 pages.

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

The curves are a tacnode, a ramphoid cusp, and an ordinary triple point.

Table of Contents

Notation

Throughout, k is an algebraically closed field. Unadorned tensor products are over k. For a k-algebra R and k-module M, we often write M_R for $R \otimes M$. The dual $\mathrm{Hom}_{k\text{-linear}}(E, k)$ of a k-vector space E is denoted by $E^\vee$. All rings are commutative with 1, and homomorphisms are required to map 1 to 1. Following Bourbaki, we require compact topological spaces to be Hausdorff.

$\mathbb{N} = \{0, 1, 2, \ldots\}$
$\mathbb{Z}$ = ring of integers
$\mathbb{C}$ = 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 $i \mapsto a_i : I \to A$. We sometimes write $|S|$ for the number of elements in a finite set S.

$X \subset Y$	X is a subset of Y, not necessarily proper.
$X \stackrel{\text{def}}{=} Y$	indicates that the equality in question is a definition.
$X \approx Y$	X and Y are isomorphic.
$X \simeq Y$	X and Y are isomorphic by a specific isomorphism, usually canonical.

We use Gothic (fraktur) letters to denote 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

A reference "Section 3m" is to Section m in Chapter 3; a reference "3.45 " is to item 45 in chapter 3; a reference "(67)" is to (displayed) equation 67 (often given with a page reference).

Prerequisites

The reader is assumed to be familiar with the basic objects of algebra, namely, rings, modules, fields, and so on.

References

CA: Milne, J.S., Commutative Algebra, v4.03, 2020.

FT: Milne, J.S., Fields and Galois Theory, Kea Books, 2022.

monnnn: Question nnnn on mathoverflow.net.

sxnnnn: Question nnnn on math.stackexchange.com.

We sometimes refer to the computer algebra programs

CoCoA (**Co**mputations in **Co**mmutative **A**lgebra) website.

Macaulay2 website; web version.

Acknowledgements

I thank the following for providing corrections and comments for earlier versions of these notes: Abhishek, Jorge Nicolás Caro Montoya, Sandeep Chellapilla, Rankeya Datta, Umesh V. Dubey, Mark Faucette, Shalom Feigelstock, Tony Feng, B.J. Franklin, Sergei Gelfand, Daniel Gerig, Darij Grinberg, Lucio Guerberoff, Isac Hedén, Guido Helmers, Florian Herzig, Christian Hirsch, Cheuk-Man Hwang, Seonho Hwangbo, Jasper Loy Jiabao, Dan Karliner, Lars Kindler, John Miller, Andrew Phillips, Devesh Rajpal, Joaquin Rodrigues, Sean Rostami, David Rufino, Hossein Sabzrou, Jyoti Prakash Saha, Tom Savage, Nguyen Quoc Thang, Bhupendra Nath Tiwari, Israel Vainsencher, Soli Vishkautsan, Kai Wang, Dennis Bouke Westra, Felipe Zaldivar, Luochen Zhao.

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

QUESTION: If we try to explain to a layman what algebraic geometry is, it seems to me that the title of the old book of Enriques is still adequate: Geometrical Theory of Equations ....
GROTHENDIECK: Yes! but your "layman" should know what a system of algebraic equations is. This would cost years of study to Plato.
QUESTION: It should be nice to have a little faith that after two thousand years every good high school graduate can understand what an affine scheme is ...

From the notes of a lecture series that Grothendieck gave at SUNY at Buffalo in the summer of 1973 (in 167 pages, Grothendieck manages to cover very little).

Introduction

I believe that you should begin by getting a solid foundation in what I call "elementary algebraic geometry," that is, the theory of "Serre varieties" as defined in FAC.[1] *I think that at the beginning you should should strictly limit yourself to varieties over an algebraically closed field (but of arbitrary characteristic).*
Dieudonné, Letter to Ribenboim, 1972.

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

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

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

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

One immediate difference between linear equations and polynomial equations is that theorems for linear equations do not depend on which field k you are working over,[2] 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	infinitely 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

[1]Serre, Jean-Pierre. Faisceaux algébriques cohérents. Ann. of Math. (2) 61, (1955). 197–278, commonly referred to as FAC.

[2]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.

than the others, but by restricting our study to polynomials we are able to do calculus over any field: we simply define

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

Moreover, calculations 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[3]

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

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 is an isomorphism on the tangent planes.

Now consider a nonzero polynomial $f(x, y, z)$ with coefficients in a field k. In these notes, 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 does not 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 cannot be integrated in the field of rational functions $k(X)$.

These notes form a basic first course on algebraic geometry. Throughout, we require the ground field to be algebraically closed in order to be able to concentrate on the geometry. Additional chapters, treating more advanced topics, can be found on my website.

The approach to algebraic geometry taken in these notes

In differential geometry it is important to define differentiable manifolds abstractly, i.e., not simply 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 and abelian varieties, Weil was forced to develop a theory of algebraic geometry for "abstract" algebraic varieties over arbitrary fields, but his "foundations" are unsatisfactory in two major respects:

- Lacking a sheaf theory, 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 together with a k-structure.

[3]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.

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 variety over an algebraically closed field to be a topological space with a sheaf of functions that is locally affine. Then, in the late 1950s Grothendieck resolved all such difficulties by developing the 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 advanced calculus and the abstractions of scheme theory.

The following complementary material is available my website.

10 Algebraic Schemes. Explains how the the theory in these notes extends to arbitrary base fields, nonreduced schemes, etc.

11 Surfaces. Develops enough of the theory of algebraic surfaces to explain what is still the most illuminating proof of the Riemann hypothesis for curves over finite fields (Weil, Mattuck, Tate, Grothendieck).

12 Divisors and Intersection Theory.

13 Coherent Sheaves and Vector Bundles.

14 Differentials (Outline).

15 Algebraic Varieties over the Complex Numbers.

17 Lefschetz Pencils.

Chapter 1

Preliminaries from commutative algebra

Algebraic geometry and commutative algebra are closely intertwined. For the most part, we develop the necessary commutative algebra in the context in which it is used. However, in this chapter, we review some basic definitions and results from commutative algebra.

a. Rings and ideals

Basic definitions

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 $x_1, \dots, x_n$ 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 $A[X_1, \dots, X_n] \to B$ acting as i_A on A and sending X_i to x_i is surjective.

When $A \subset B$ and $x_1, \dots, x_n \in B$, we let $A[x_1, \dots, x_n]$ denote the A-subalgebra of B generated by the x_i.

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. If $1_A \neq 0$, then the map $k \to A$ is injective, and we can identify k with its image, i.e., we can regard k as a subring of A. If $1_A = 0$, then A is the zero ring $\{0\}$.

A ring is an ***integral domain*** if it is not the zero ring and if $ab = 0$ implies that $a = 0$ or $b = 0$; in other words, if $ab = ac$ and $a \neq 0$, then $b = c$.

For a ring A, $A^\times$ is the group of elements of A with inverses (the units in the ring).

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

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 see that this is in fact an ideal, and that it consists of the finite sums of the form $\sum a_i s_i$ with $a_i \in A$, $s_i \in S$. The ideal generated by the empty set is the zero ideal $\{0\}$. When $S = \{s_1, s_2, ...\}$, we write $(s_1, s_2, ...)$ 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 $\mathfrak{a}\mathfrak{b}$. Clearly $\mathfrak{a}\mathfrak{b}$ 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 $\mathfrak{a}\mathfrak{b} = (a_1 b_1, \ldots, a_i b_j, \ldots, a_m b_n)$. Note that

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

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

$$ab = 0 \;\Rightarrow\; a = 0 \text{ or } b = 0,$$

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

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

If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in A and B, then $\mathfrak{a} \times \mathfrak{b}$ is an ideal in $A \times B$, and all ideals in $A \times B$ are of this form. 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

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

Ideals $\mathfrak{a}$ and $\mathfrak{b}$ in A are ***coprime*** (or ***relatively prime***) if $\mathfrak{a} + \mathfrak{b} = A$. Assume that $\mathfrak{a}$ and $\mathfrak{b}$ are coprime, and let $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ be such that $a + b = 1$. For $x, y \in A$, let $z = ay + bx$; then

$$\begin{aligned} z &\equiv bx \equiv x \mod \mathfrak{a} \\ z &\equiv ay \;\equiv y \mod \mathfrak{b}, \end{aligned}$$

and so the canonical map

$$A \to A/\mathfrak{a} \times A/\mathfrak{b} \tag{5}$$

is surjective. Clearly its kernel is $\mathfrak{a} \cap \mathfrak{b}$, which contains $\mathfrak{a}\mathfrak{b}$. Let $c \in \mathfrak{a} \cap \mathfrak{b}$; then

$$c = c1 = ca + cb \in \mathfrak{a}\mathfrak{b}.$$

Hence, $A \to A/\mathfrak{a} \times A/\mathfrak{b}$ is surjective with kernel $\mathfrak{a}\mathfrak{b}$. This statement extends to finite collections of ideals.

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 $\mathfrak{a}_j$ whenever $i \neq j$, then the canonical map*

$$A \to A/\mathfrak{a}_1 \times \cdots \times A/\mathfrak{a}_n \tag{6}$$

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

PROOF. We have proved the statement for $n = 2$, and we use induction to extend it to $n > 2$. For $i \geq 2$, there exist elements $a_i \in \mathfrak{a}_1$ and $b_i \in \mathfrak{a}_i$ such that

$$a_i + b_i = 1.$$

The product $\prod_{i \geq 2}(a_i + b_i)$ lies in $\mathfrak{a}_1 + \mathfrak{a}_2 \cdots \mathfrak{a}_n$ and equals 1, and so

$$\mathfrak{a}_1 + \mathfrak{a}_2 \cdots \mathfrak{a}_n = A.$$

Therefore,

$$\begin{aligned} A/\mathfrak{a}_1 \cdots \mathfrak{a}_n &= A/\mathfrak{a}_1 \cdot (\mathfrak{a}_2 \cdots \mathfrak{a}_n) \\ &\simeq A/\mathfrak{a}_1 \times A/\mathfrak{a}_2 \cdots \mathfrak{a}_n && \text{by the } n = 2 \text{ case} \\ &\simeq A/\mathfrak{a}_1 \times A/\mathfrak{a}_2 \times \cdots \times A/\mathfrak{a}_n && \text{by induction.} \end{aligned}$$

□

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., $\mathfrak{a}_m = \mathfrak{a}_{m+1} = \cdots$ for some m;*

(c) *every nonempty set of ideals in A has a maximal element.*

PROOF. (a) $\Rightarrow$ (b): Let $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$ be an ascending chain of ideals. Then $\bigcup \mathfrak{a}_i$ is an ideal, and hence has a finite set $\{a_1, \ldots, a_n\}$ of generators. For some m, all the a_i belong to $\mathfrak{a}_m$, and then

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

(b) $\Rightarrow$ (c): Let Σ be a nonempty set of ideals in A. If Σ has no maximal element, then the axiom of dependent choice[2] implies that there exists an infinite strictly ascending chain of ideals in Σ, contradicting (b).

(c) $\Rightarrow$ (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 $a \in \mathfrak{a} \smallsetminus \mathfrak{c}$, 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 $\mathfrak{c}$, and so $\mathfrak{c} = \mathfrak{a}$. □

A ring A is ***noetherian*** if every nonempty set of ideals has a maximal element. Applying this to the set of proper ideals containing a fixed ideal, we see that every proper ideal in a noetherian ring is contained in a maximal ideal. This last assertion is, in fact, true for all rings, but the proof for non-noetherian rings requires Zorn's lemma (CA, 2.2).

A ring A is ***local*** if it has exactly one maximal ideal $\mathfrak{m}_A$. If A is local, then $A^\times = A \smallsetminus \mathfrak{m}_A$. A homomorphism $\varphi\colon A \to B$ of local rings is ***local*** if $\varphi(\mathfrak{m}_A) \subset \mathfrak{m}_B$, in which case $\varphi^{-1}(\mathfrak{m}_B) = \mathfrak{m}_A$.

[2]This says the following: let R be a binary relation on a nonempty set X, and suppose that, for each a in X, there exists a b such that aRb; then there exists a sequence $(a_n)_{n \in \mathbb{N}}$ of elements of X such that $a_n R a_{n+1}$ for all n. This axiom is strictly weaker than the axiom of choice (Wikipedia: AXIOM OF DEPENDENT CHOICE).

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 $(1-a_1) \notin \mathfrak{m}$, it is a unit, and so $e_2, \ldots, e_n$ 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 $\mathfrak{m}$. Then $\mathfrak{m}$ is an A-module, and the action of A on $\mathfrak{m}/\mathfrak{m}^2$ factors through $k \stackrel{\text{def}}{=} A/\mathfrak{m}$.

COROLLARY 1.4. *Elements $a_1, \ldots, a_n$ of $\mathfrak{m}$ generate $\mathfrak{m}$ as an ideal if and only if their residues modulo $\mathfrak{m}^2$ span $\mathfrak{m}/\mathfrak{m}^2$ 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 span $\mathfrak{m}/\mathfrak{m}^2$. Conversely, suppose that their residues span $\mathfrak{m}/\mathfrak{m}^2$, 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 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

$$\mathfrak{p} = \mathfrak{p}_d \supset \mathfrak{p}_{d-1} \supset \cdots \supset \mathfrak{p}_0. \tag{7}$$

(b) The ***Krull dimension***, or simply ***dimension***, $\dim(A)$, of A is $\sup\{\mathrm{ht}(\mathfrak{p}) \mid \mathfrak{p} \text{ a prime ideal in } A\}$.

Thus, the Krull dimension of a noetherian 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). 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 (unless it is a field).

The height of every 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 (CA, p. 13).

DEFINITION 1.6. A ***regular local ring*** A is a noetherian local ring whose maximal ideal can be generated by d elements, where d is the Krull dimension of A.

It follows from Corollary 1.4 that a local noetherian ring is regular if and only if its 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 among those generated by a finite subset of S must contain every element of S (otherwise it would not be maximal), and so equals $\mathfrak{a}$. □

In the proof of the next theorem, we use that a polynomial ring over a noetherian ring is noetherian (Theorem 2.8).

THEOREM 1.8 (KRULL INTERSECTION THEOREM). *Let A be a noetherian local ring with maximal ideal $\mathfrak{m}$; then $\bigcap_{n\geq 1}\mathfrak{m}^n=\{0\}$.*

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 of the form $g(a_1,\ldots,a_r)$ for some homogeneous polynomial $g(X_1,\ldots,X_r)\in A[X_1,\ldots,X_r]$ of degree n. Let S_m denote 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, $\mathfrak{a}$ is generated by a finite subset $\{f_1,\ldots,f_s\}$ of $\bigcup_m S_m$. Let $d_i=\deg f_i$, and let $d=\max d_i$. If $b\in\bigcap_{n\geq 1}\mathfrak{m}^n$, 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

$$f=g_1f_1+\cdots+g_sf_s$$

for some $g_i\in A[X_1,\ldots,X_r]$. 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

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

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

ASIDE 1.9. Let A be the ring of germs of analytic functions at $0\in\mathbb{R}$ (see p. 60 for the notion of a germ of a function). Then A is a noetherian local ring with maximal ideal $\mathfrak{m}=(x)$, and $\mathfrak{m}^n$ consists of the functions f that vanish to order n at $x=0$. The theorem says (correctly) that only the zero function vanishes to all orders at 0. By contrast, the function e^{-1/x^2} shows that the Krull intersection theorem fails for the ring of germs of infinitely differentiable functions at 0 (this ring is not noetherian).

b. Rings of fractions

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

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

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

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

Write $\frac{a}{s}$ for the equivalence class containing (a, s), and define addition and multiplication of equivalence classes in the way suggested by the notation:

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

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

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

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

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

If A is an integral domain and $0 \notin S$, then $a \mapsto \frac{a}{1}$ is injective. On the other hand, if $0 \in S$, then $S^{-1}A$ is the zero ring.

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

PROPOSITION 1.10. *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 $\alpha : A \to B$ with this property factors uniquely through i,*

$$\begin{array}{ccc} A & \xrightarrow{\ i\ } & S^{-1}A \\ & \underset{\alpha}{\searrow} & \Big\downarrow{\scriptstyle \exists!\,\beta} \\ & & B \end{array}$$

PROOF. If β exists, then

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

and so β is unique. Define

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

Then

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

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

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

If A is an integral domain and $S = A \setminus \{0\}$, then $F = S^{-1}A$ 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 1.11. Let $h \in A$. Then $S_h \overset{\text{def}}{=} \{1, h, h^2, \ldots\}$ 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 $\frac{a}{h^m}$, $a \in A$, 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 $\frac{a}{h^m}$, $a \in A$, $m \in \mathbb{N}$.

EXAMPLE 1.12. Let $\mathfrak{p}$ be a prime ideal in A. Then $S_{\mathfrak{p}} \overset{\text{def}}{=} A \smallsetminus \mathfrak{p}$ 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 $\mathfrak{m} = \left\{\frac{a}{s} \mid a \in \mathfrak{p},\ s \notin \mathfrak{p}\right\}$ is a maximal ideal in $A_{\mathfrak{p}}$, and it is the only maximal ideal, i.e., $A_{\mathfrak{p}}$ is a local ring.[3] 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 1.13. *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*

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

PROOF. If $h = 0$, then both rings are zero, so we may suppose that $h \neq 0$. Let x be the class of X in the quotient ring $A[X]/(1 - hX)$. Then $A[x]$ is generated by x subject to the relation $1 = hx$, 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. □

Let S be a multiplicative subset of a ring A, and let $S^{-1}A$ be the corresponding ring of fractions. Each ideal $\mathfrak{a}$ in A, generates an ideal $S^{-1}\mathfrak{a}$ in $S^{-1}A$. If $\mathfrak{a}$ contains an element of S, then $S^{-1}\mathfrak{a}$ contains a unit, and so is the whole ring. Thus some of the ideal structure of A is lost in the passage to $S^{-1}A$, but, as the next proposition shows, much is retained.

PROPOSITION 1.14. *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 $S^{-1}A$. Its inverse sends a prime ideal of $S^{-1}A$ to its inverse image in A.

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

[3] 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.

LEMMA 1.15. *Let $\mathfrak{m}$ be a maximal ideal of a ring A, and let $\mathfrak{n} = \mathfrak{m}A_{\mathfrak{m}}$. For all n, the map*

$$a + \mathfrak{m}^n \mapsto \frac{a}{1} + \mathfrak{n}^n : A/\mathfrak{m}^n \to A_{\mathfrak{m}}/\mathfrak{n}^n \tag{8}$$

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 $S = A \setminus \mathfrak{m}$. Then $A_{\mathfrak{m}} = S^{-1}A$ and $\mathfrak{n}^n = \mathfrak{m}^n A_{\mathfrak{m}} = \left\{\frac{b}{s} \in A_{\mathfrak{m}} \mid b \in \mathfrak{m}^n,\ s \in S\right\}$. In order to show that the map (8) is injective, it suffices to show that

$$\frac{a}{1} = \frac{b}{s} \text{ with } a \in A,\ b \in \mathfrak{m}^n,\ s \in S \implies a \in \mathfrak{m}^n.$$

But if $\frac{a}{1} = \frac{b}{s}$, then $tas = tb \in \mathfrak{m}^n$ for some $t \in S$, and so $tas = 0$ in $A/\mathfrak{m}^n$. The only maximal ideal in A 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 $A/\mathfrak{m}^n$ is $\mathfrak{m}/\mathfrak{m}^n$. As st is not in $\mathfrak{m}/\mathfrak{m}^n$, it must be a unit in $A/\mathfrak{m}^n$, and as $sta = 0$ in $A/\mathfrak{m}^n$, a must be 0 in $A/\mathfrak{m}^n$, i.e., $a \in \mathfrak{m}^n$.

We now prove that the map (8) is surjective. Let $\frac{a}{s} \in A_{\mathfrak{m}}$, $a \in A$, $s \in S$. Because the only maximal ideal of A containing $\mathfrak{m}^n$ is $\mathfrak{m}$, no maximal ideal contains both s and $\mathfrak{m}^n$. It follows that $(s) + \mathfrak{m}^n = A$. Therefore, there exist $b \in A$ and $q \in \mathfrak{m}^n$ such that $sb + q = 1$ in A. It follows that s is invertible in $A_{\mathfrak{m}}/\mathfrak{n}^n$, and so $\frac{a}{s}$ is the *unique* element of this ring such that $s\frac{a}{s} = a$. As $s(ba) + qa = a$, the image of ba in $A_{\mathfrak{m}}/\mathfrak{n}^n$ also has this property and therefore equals $\frac{a}{s}$ in $A_{\mathfrak{m}}/\mathfrak{n}^n$. □

PROPOSITION 1.16. *In a 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 $\{b \in A \mid ba = 0\}$ 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 1.8), which implies that $a \notin \mathfrak{m}^n$ (by 1.15). □

Let A be an integral domain and let f be an element of its field of fractions. If A is a unique factorization domain (see below), then there is a preferred expression $f = \frac{a}{b}$ for f, unique up to multiplying top and bottom by a unit. In general, there is no such preferred expression.

Modules of fractions

Let S be a multiplicative subset of the ring A, and let M be an A-module. Define an equivalence relation on $M \times S$ by

$$(m, s) \sim (n, t) \iff u(tm - sn) = 0 \text{ for some } u \in S.$$

Write $\frac{m}{s}$ for the equivalence class containing (m, s), and define addition and scalar multiplication by the rules:

$$\frac{m}{s} + \frac{n}{t} = \frac{mt + ns}{st}, \quad \frac{a}{s}\frac{m}{t} = \frac{am}{st}, \quad m, n \in M, \quad s, t \in S, \quad a \in A.$$

It is easily checked that these do not depend on the choices of representatives for the equivalence classes, and that we obtain in this way an $S^{-1}A$-module

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

and a homomorphism $m \mapsto \frac{m}{1} \colon M \xrightarrow{i_S} S^{-1}M$ of A-modules whose kernel is

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

PROPOSITION 1.17. *The elements of S act invertibly on $S^{-1}M$, and every homomorphism from M to an A-module N with this property factors uniquely through i_S,*

$$\begin{array}{ccc} M & \xrightarrow{i_S} & S^{-1}M \\ & \searrow & \downarrow \exists! \\ & & N. \end{array}$$

PROOF. Similar to the proof of 1.10. □

PROPOSITION 1.18. *The functor $M \rightsquigarrow S^{-1}M$ is exact. In other words, if the sequence of A-modules*

$$M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$$

is exact, then so also is the sequence of $S^{-1}A$-modules

$$S^{-1}M' \xrightarrow{S^{-1}\alpha} S^{-1}M \xrightarrow{S^{-1}\beta} S^{-1}M''.$$

PROOF. Because $\beta \circ \alpha = 0$, we have $0 = S^{-1}(\beta \circ \alpha) = S^{-1}\beta \circ S^{-1}\alpha$. Therefore $\mathrm{Im}(S^{-1}\alpha) \subset \mathrm{Ker}(S^{-1}\beta)$. For the reverse inclusion, let $\frac{m}{s} \in \mathrm{Ker}(S^{-1}\beta)$, where $m \in M$ and $s \in S$. Then $\frac{\beta(m)}{s} = 0$ and so, for some $t \in S$, we have $t\beta(m) = 0$. Then $\beta(tm) = 0$, and so $tm = \alpha(m')$ for some $m' \in M'$. Now

$$\frac{m}{s} = \frac{tm}{ts} = \frac{\alpha(m')}{ts} \in \mathrm{Im}(S^{-1}\alpha).$$

□

PROPOSITION 1.19. *Let A be a ring, and let M be an A-module. The canonical map*

$$M \to \prod \{M_{\mathfrak{m}} \mid \mathfrak{m} \text{ a maximal ideal in } A\}$$

is injective.

PROOF. Let $m \in M$ map to zero in all $M_{\mathfrak{m}}$. The annihilator $\mathfrak{a} \overset{\text{def}}{=} \{a \in A \mid am = 0\}$ of m is an ideal in A. Because m maps to zero $M_{\mathfrak{m}}$, there exists an $s \in A \smallsetminus \mathfrak{m}$ such that $sm = 0$. Therefore $\mathfrak{a}$ is not contained in $\mathfrak{m}$. Since this is true for all maximal ideals $\mathfrak{m}$, $\mathfrak{a} = A$, and so it contains 1. Now $m = 1m = 0$. □

COROLLARY 1.20. *An A-module M is zero if $M_{\mathfrak{m}}$ is zero for all maximal ideals $\mathfrak{m}$ in A.*

PROOF. Immediate consequence of the proposition. □

PROPOSITION 1.21. *Let A be a ring. A sequence of A-modules*

$$M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \qquad (*)$$

is exact if and only if

$$M'_{\mathfrak{m}} \xrightarrow{\alpha_{\mathfrak{m}}} M_{\mathfrak{m}} \xrightarrow{\beta_{\mathfrak{m}}} M''_{\mathfrak{m}} \qquad (**)$$

is exact for all maximal ideals $\mathfrak{m}$.

PROOF. The necessity is a special case of Proposition 1.18. For the sufficiency, we have to show that $N \overset{\text{def}}{=} \operatorname{Ker}(\beta)/\operatorname{Im}(\alpha)$ is zero. Because the functor $M \rightsquigarrow M_{\mathfrak{m}}$ is exact,

$$N_{\mathfrak{m}} = \operatorname{Ker}(\beta_{\mathfrak{m}})/\operatorname{Im}(\alpha_{\mathfrak{m}}).$$

If (**) is exact for all $\mathfrak{m}$, then $N_{\mathfrak{m}} = 0$ for all $\mathfrak{m}$, and so $N = 0$ (by 1.20). □

COROLLARY 1.22. *A homomorphism $M \to N$ of A-modules is injective (resp. surjective) if and only if $M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective (resp. surjective) for all maximal ideals $\mathfrak{m}$.*

PROOF. Apply the proposition to $0 \to M \to N$ (resp. $M \to N \to 0$). □

Direct limits

A ***directed set*** is a pair $(I, \leq)$ comprising a set I and a partial order[4] $\leq$ on I such that for all $i, j \in I$, there exists a $k \in I$ with $i, j \leq k$.

Let $(I, \leq)$ be a directed set, and let A be a ring. A ***direct system*** of A-modules indexed by $(I, \leq)$ is a family $(M_i)_{i \in I}$ of A-modules together with a family $(\alpha^i_j : M_i \to M_j)_{i \leq j}$ of A-linear maps such that $\alpha^i_i = \mathrm{id}_{M_i}$ and $\alpha^j_k \circ \alpha^i_j = \alpha^i_k$ all $i \leq j \leq k$.[5] An A-module M together with A-linear maps $\alpha^i : M_i \to M$ such that $\alpha^i = \alpha^j \circ \alpha^i_j$ for all $i \leq j$ is the ***direct limit*** (or ***colimit***) of the system (M_i, α^j_i) 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 $j \geq i$.

Direct limits of A-algebras are defined similarly.

PROPOSITION 1.23. *Let S be a multiplicative subset of A. Then $S^{-1}A \simeq \varinjlim A_h$, where h runs over the elements of S (partially ordered by division).*

[4] i.e., reflexive transitive antisymmetric.

[5] Regard I as a category with $\operatorname{Hom}(a, b)$ empty unless $a \leq b$, in which case it contains a single element. Then a direct system is a functor from I to the category of A-modules.

PROOF. When $h|h'$, say, $h' = hg$, there is a canonical homomorphism $\frac{a}{h} \mapsto \frac{ag}{h'} : A_h \to A_{h'}$. 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 $\frac{a}{h} \mapsto \frac{a}{h} : A_h \to S^{-1}A$ (1.10), and these homomorphisms are compatible with the maps in the direct system. Now it is easy to see that $S^{-1}A$ satisfies the conditions to be the direct limit of the A_h. □

c. 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.,

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

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

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

If A is noetherian, then every nonzero nonunit element can be expressed as a finite product of irreducible elements. To see this, suppose that a cannot be so expressed and that (a) is maximal among the ideals generated by such elements; then a is not irreducible, so $a = bc$ with neither b nor c a unit; each of (b) and (c) properly contains (a), and at least one of b or c is not a finite product of irreducible elements, giving a contradiction.

An integral domain A is called a ***unique factorization domain*** (or a ***factorial 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. Principal ideal domains, for example, $\mathbb{Z}$ and $k[X]$, are unique factorization domains,

PROPOSITION 1.24. *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 $qc = 1$ because A is an integral domain, and so c is a unit. We have shown that a is irreducible.

For the converse, assume that a is irreducible and that A is a unique factorization domain. If $a|bc$, then

$$bc = aq, \text{ some } q \in A.$$

On writing each of b, c, and q as a product of irreducible elements, and using the uniqueness of factorizations, we see that a differs from one of the irreducible factors of b or c by a unit. Therefore a divides b or c. □

COROLLARY 1.25. *Let A be a noetherian integral domain. If A is a unique factorization domain, then every prime ideal of height 1 is principal.*

PROOF. Let $\mathfrak{p}$ be a prime ideal of height 1. Then $\mathfrak{p}$ contains a nonzero element, and hence an irreducible element a. We have $\mathfrak{p} \supset (a) \supset (0)$. As (a) is prime and $\mathfrak{p}$ has height 1, we must have $\mathfrak{p} = (a)$. □

PROPOSITION 1.26. *Let A be a noetherian integral domain. If every irreducible element of A is prime, then A is a unique factorization domain.*

PROOF. Suppose that

$$a_1 \cdots a_m = b_1 \cdots b_n \tag{9}$$

with the a_i and b_i irreducible elements in A. As a_1 is prime, it divides one of the b_i, say, b_1. As b_1 is irreducible, $b_1 = ua_1$ for some unit u. On cancelling a_1 from both sides of (9), we obtain the equality

$$a_2 \cdots a_m = (ub_2)b_3 \cdots b_n.$$

Continuing in this fashion, we find that the two factorizations are the same up to units and the order of the factors. □

ASIDE. The converse to 1.25 is also true: let a be an irreducible element of A, and let $\mathfrak{p}$ be minimal among the prime ideals containing (a); according to the principal ideal theorem (3.51; CA, 21.3), $\mathfrak{p}$ has height 1, and so is principal, say, $\mathfrak{p} = (b)$; now $a = bc$, and, because a is irreducible, c is a unit; therefore $(a) = (b) = \mathfrak{p}$, and a is prime. See 3.53.

PROPOSITION 1.27 (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

$$cdf = g_1h_1 \text{ in } A[X].$$

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 1.24, (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

$$(cd/p)f = g_2h_1 \text{ in } A[X].$$

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

$$f = a_0 + a_1X + \cdots + a_mX^m$$

in $A[X]$ is said to be ***primitive*** if the coefficients a_i have no common factor other than units.

Every polynomial f in $F[X]$ can be written $f = c(f) \cdot f_1$ with $c(f) \in F$ and f_1 primitive. The element $c(f)$, which is well-defined up to multiplication by a unit in A, is called the ***content*** of f. Note that $f \in A[X]$ if and only if $c(f) \in A$.

LEMMA 1.28. *The product of two primitive polynomials is primitive.*

PROOF. Let

$$f = a_0 + a_1X + \cdots + a_mX^m$$
$$g = b_0 + b_1X + \cdots + b_nX^n,$$

be primitive polynomials, and let p be an irreducible element of A. Let a_{i_0}, $i_0 \leq m$, be the first coefficient of f not divisible by p, and b_{j_0}, $j_0 \leq n$, the first coefficient of g not divisible by p. Then all the terms in the sum $\sum_{i+j=i_0+j_0} a_ib_j$ are divisible by p except $a_{i_0}b_{j_0}$, which is not divisible by p. Therefore, p does not 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. □

PROPOSITION 1.29. *Let A be a unique factorization domain with field of fractions F. For polynomials $f, g \in F[X]$,*

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

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

$$fg = c(f) \cdot c(g) \cdot f_1g_1$$

with f_1g_1 primitive, and so $c(fg) = c(f)c(g)$. □

COROLLARY 1.30. *An element $f \in A[X]$ is irreducible if and only if either*

(a) *f is constant, say, $f = a$, with a an irreducible element of A, or*

(b) *f is a nonconstant primitive polynomial that is irreducible in $F[X]$.*

PROOF. $\Leftarrow$: If f is as in (a) and $f = gh$ in $A[X]$, then g and h both lie in A and one must be a unit in A, and hence a unit in $A[X]$. If f is as in (b) and $f = gh$, then one of g or h must be constant because otherwise f would be reducible in $F[X]$. If it is g that is constant, then, because f is primitive, g must be a unit in A, and hence in $A[X]$.

$\Rightarrow$: Let $f \in A[X]$ be irreducible. If f is a constant polynomial, say, $f = a$, then a is obviously irreducible in A. If f nonconstant, then it must be primitive because otherwise $f = c(f) \cdot f_1$ would be a nontrivial factorization in $A[X]$. It must also be irreducible in $F[X]$, because otherwise it would have a nontrivial factorization in $A[X]$ (by 1.27). □

PROPOSITION 1.31. *If A is a unique factorization domain, then so also is $A[X]$.*

PROOF. We check that A satisfies the conditions of Proposition 1.26.

Let $f \in A[X]$, and write $f = c(f)f_1$. Then $c(f)$ is a product of irreducible elements in A, and f_1 is a product of irreducible primitive polynomials. This shows that f is a product of irreducible elements in $A[X]$.

Let a be an irreducible element of A. If a divides fg, then it divides $c(fg) = c(f)c(g)$. As a is prime (1.24), it divides $c(f)$ or $c(g)$, and hence also f or g.

Let f be an irreducible primitive polynomial in $A[X]$. Then f is irreducible in $F[X]$, and so if f divides the product gh of $g, h \in A[X]$, then it divides g or h in $F[X]$. Suppose the first, and write $fq = g$ with $q \in F[X]$. Then $c(q) = c(f)c(q) = c(fq) = c(g) \in A$, and so $q \in A[X]$. Therefore f divides g in $A[X]$.

We have shown that every element of $A[X]$ is a product of irreducible elements and that every irreducible element of $A[X]$ is prime, and so $A[X]$ is a unique factorization domain (1.26). □

Polynomial rings

Let k be a field. 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 $f = gh \Rightarrow g$ or h is constant.

THEOREM 1.32. *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 symbols $X_1, \ldots, X_n$ 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, as we noted, $k[X]$ is a unique factorization domain, the theorem follows by induction from Proposition 1.31. □

COROLLARY 1.33. *A nonzero proper principal ideal (f) in $k[X_1, \ldots, X_n]$ is prime if and only if f is irreducible.*

PROOF. Special case of Proposition 1.24. □

d. Integral dependence

Let A be a subring of a ring B. An element α of B is said to be ***integral*** over A if it is a root of a monic[6] polynomial with coefficients in A, i.e., if it satisfies an equation

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

More generally, if $f\colon A \to B$ is an A-algebra, then an element α of B is ***integral*** over A if it if it is integral over the subring $f(A)$ of B. When every element of B is integral over A, we say that B is ***integral*** over A.

In the next proof, we shall need to apply a variant of Cramer's rule: if $x_1, \ldots, x_m$ is a solution to the system of linear equations

$$\sum_{j=1}^{m} c_{ij}x_j = 0, \quad i = 1, \ldots, m,$$

with coefficients in a ring A, then

$$\det(C) \cdot x_j = 0, \quad j = 1, \ldots, m, \tag{10}$$

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

where C is the matrix of coefficients. To prove this, expand out the left hand side of

$$\det\begin{pmatrix} c_{11} & \ldots & c_{1\,j-1} & \sum_i c_{1i}x_i & c_{1\,j+1} & \ldots & c_{1m} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ c_{m1} & \ldots & c_{m\,j-1} & \sum_i c_{mi}x_i & c_{m\,j+1} & \ldots & c_{mm} \end{pmatrix} = 0$$

using standard properties of determinants.

An A-module M is ***faithful*** if $aM = 0$, $a \in A$, implies that $a = 0$.

PROPOSITION 1.34. *Let A be a subring of a ring B. An element α of B is integral over A if and only if there exists a faithful $A[\alpha]$-submodule M of B that is finitely generated as an A-module.*

PROOF. $\Rightarrow$: Suppose that

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

Then the A-submodule M of B generated by $1, \alpha, \ldots, \alpha^{n-1}$ has the property that $\alpha M \subset M$, and it is faithful because it contains 1.

$\Leftarrow$: Let M be a faithful $A[\alpha]$-submodule of B admitting a finite set $\{e_1, \ldots, e_n\}$ of generators as an A-module. Then, for each i,

$$\alpha e_i = \sum a_{ij}e_j, \text{ some } a_{ij} \in A.$$

We can rewrite this system of equations as

$$\begin{aligned} (\alpha - a_{11})e_1 - a_{12}e_2 - a_{13}e_3 - \cdots &= 0 \\ -a_{21}e_1 + (\alpha - a_{22})e_2 - a_{23}e_3 - \cdots &= 0 \\ \cdots &= 0. \end{aligned}$$

Let C be the matrix of coefficients on the left-hand side. Then Cramer's formula tells us that $\det(C) \cdot e_i = 0$ for all i. As M is faithful and the e_i generate M, this implies that $\det(C) = 0$. On expanding out the determinant, we obtain an equation

$$\alpha^n + c_1\alpha^{n-1} + c_2\alpha^{n-2} + \cdots + c_n = 0, \quad c_i \in A.$$

□

PROPOSITION 1.35. *An A-algebra B is finite if it is generated as an A-algebra by a finite set of elements each of which is integral over A.*

PROOF. We may replace A with its image in B. Suppose that $B = A[\alpha_1, \ldots, \alpha_m]$ and that

$$\alpha_i^{n_i} + a_{i1}\alpha_i^{n_i-1} + \cdots + a_{in_i} = 0, \quad a_{ij} \in A, \quad i = 1, \ldots, m.$$

Any monomial in the α_i divisible by some $\alpha_i^{n_i}$ is equal (in B) to a linear combination of monomials of lower degree. Therefore, B is generated as an A-module by the finite set of monomials $\alpha_1^{r_1} \cdots \alpha_m^{r_m}$, $1 \le r_i < n_i$. □

COROLLARY 1.36. *An A-algebra B is finite if and only if it is finitely generated and integral over A.*

PROOF. $\Leftarrow$: Immediate consequence of 1.35.

$\Rightarrow$: We may replace A with its image in B. Then B is a faithful $A[\alpha]$-module for all $\alpha \in B$ (because $1_B \in B$), and so 1.34 shows that every element of B is integral over A. As B is finitely generated as an A-module, it is certainly finitely generated as an A-algebra. □

PROPOSITION 1.37. *Consider rings $A \subset B \subset C$. If B is integral over A and C is integral over B, then C is integral over A.*

PROOF. Let $\gamma \in C$. Then
$$\gamma^n + b_1\gamma^{n-1} + \cdots + b_n = 0$$
for some $b_i \in B$. Now $A[b_1, \dots, b_n]$ is finite over A (see 1.35), and $A[b_1, \dots, b_n][\gamma]$ is finite over $A[b_1, \dots, b_n]$, and so it is finite over A. Therefore γ is integral over A by 1.34. □

THEOREM 1.38. *Let A be a subring of a ring B. The elements of B integral over A form an A-subalgebra of B.*

PROOF. Let α and β be two elements of B integral over A. Then $A[\alpha, \beta]$ is finitely generated as an A-module (1.35). It is stable under multiplication by $\alpha \pm \beta$ and $\alpha\beta$ and it is faithful as an $A[\alpha \pm \beta]$-module and as an $A[\alpha\beta]$-module (because it contains 1_A). Therefore 1.34 shows that $\alpha \pm \beta$ and $\alpha\beta$ are integral over A. □

DEFINITION 1.39. The A-subalgebra of B of elements integral over A is called the ***integral closure*** of A in B.

PROPOSITION 1.40. *Let A be an integral domain with field of fractions F, and let α be an element of some field containing F. If α 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 $da_i \in A$ for all i, and multiply the equation by d^m:
$$(d\alpha)^m + a_1 d(d\alpha)^{m-1} + \cdots + a_m d^m = 0.$$
As $a_1 d, \dots, a_m d^m \in A$, this shows that $d\alpha$ is integral over A. □

COROLLARY 1.41. *Let A be an integral domain and let E be an algebraic extension of the field of fractions of A. Then E is the field of fractions of the integral closure of A in E.*

PROOF. In fact, the proposition shows that every element of E is a quotient β/d with β integral over A and $d \in A$. □

DEFINITION 1.42. An integral domain A is said to be ***integrally closed*** if it is equal to its integral closure in its field of fractions F, i.e., if
$$\alpha \in F, \quad \alpha \text{ integral over } A \implies \alpha \in A.$$
An integrally closed integral domain is called an ***integrally closed domain*** or ***normal domain***.

PROPOSITION 1.43. *Unique factorization domains are integrally closed.*

PROOF. Let A be a unique factorization domain, and let a/b be an element of its field of fractions. If $a/b \notin A$, then we may suppose that b is divisible by some prime element p not dividing a. If a/b is integral over A, then it satisfies an equation

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

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 divides a^n. Since it does not divide a, this is a contradiction. □

Let $F \subset E$ be fields, and let $\alpha \in E$ be algebraic over F. The ***minimal polynomial*** of α over F is the monic polynomial of smallest degree in $F[X]$ having α as a root. If f is the minimal polynomial of α, then the homomorphism $X \mapsto \alpha\colon F[X] \to F[\alpha]$ defines an isomorphism $F[X]/(f) \to F[\alpha]$, i.e., $F[x] \simeq F[\alpha]$, $x \leftrightarrow \alpha$.

PROPOSITION 1.44. *Let A be an integrally closed domain, and let E be a finite extension of the field of fractions F of A. An element of E is integral over A if and only if its minimal polynomial over F has coefficients in A.*

PROOF. Let $\alpha \in E$ be integral over A, so that

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

Let $f(X)$ be the minimal polynomial of α over F, and let α' be a conjugate of α, i.e., a root of f in some splitting field of f. Then f is also the minimal polynomial of α' over F, and so there is an F-isomorphism

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

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. As the coefficients of f are polynomials in the conjugates of α, it follows from Theorem 1.38 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 1.45. *Let $A \subset F \subset E$ be as in the proposition, and let α be an element of E integral over A. Then $\mathrm{Nm}_{E/F}(\alpha) \in A$, and α divides $\mathrm{Nm}_{E/F}(\alpha)$ in $A[\alpha]$.*

PROOF. Let

$$f(X) = X^m + a_1X^{m-1} + \cdots + a_m$$

be the minimal polynomial of α over F. Then $\mathrm{Nm}(\alpha) = (-1)^{mn}a_m^n$, where $n = [E : F[\alpha]]$ (FT, 5.45), and so $\mathrm{Nm}(\alpha) \in A$. Because $f(\alpha) = 0$,

$$\begin{aligned} 0 &= a_m^{n-1}(\alpha^m + a_1\alpha^{m-1} + \cdots + a_m) \\ &= \alpha(a_m^{n-1}\alpha^{m-1} + \cdots + a_m^{n-1}a_{m-1}) + (-1)^{mn}\,\mathrm{Nm}(\alpha), \end{aligned}$$

and so α divides $\mathrm{Nm}_{E/F}(\alpha)$ in $A[\alpha]$. □

COROLLARY 1.46. *Let A be an integrally closed 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 minimal polynomial of α. As α is a root of f, it is integral over A, and so g has coefficients in A. □

PROPOSITION 1.47. *Let $A \subset B$ be rings, and let A' be the integral closure of A in B. For any multiplicative subset S of A, $S^{-1}A'$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.*

PROOF. Let $\frac{b}{s} \in S^{-1}A'$ with $b \in A'$ and $s \in S$. Then

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

for some $a_i \in A$, and so

$$\left(\frac{b}{s}\right)^n + \frac{a_1}{s}\left(\frac{b}{s}\right)^{n-1} + \cdots + \frac{a_n}{s^n} = 0.$$

Therefore b/s is integral over $S^{-1}A$. This shows that $S^{-1}A'$ is contained in the integral closure of $S^{-1}B$.

For the converse, let b/s ($b \in B$, $s \in S$) be integral over $S^{-1}A$. Then

$$\left(\frac{b}{s}\right)^n + \frac{a_1}{s_1}\left(\frac{b}{s}\right)^{n-1} + \cdots + \frac{a_n}{s_n} = 0.$$

for some $a_i \in A$ and $s_i \in S$. On multiplying this equation by $s^n s_1 \cdots s_n$, we find that $s_1 \cdots s_n b \in A'$, and therefore that $\frac{b}{s} = \frac{s_1 \cdots s_n b}{s s_1 \cdots s_n} \in S^{-1}A'$. □

COROLLARY 1.48. *Let $A \subset B$ be rings, and let S be a multiplicative subset of A. If A is integrally closed in B, then $S^{-1}A$ is integrally closed in $S^{-1}B$.*

PROOF. Special case of the proposition in which $A' = A$. □

PROPOSITION 1.49. *The following conditions on an integral domain A are equivalent:*

(a) *A is integrally closed;*

(b) *$A_{\mathfrak{p}}$ is integrally closed for all prime ideals $\mathfrak{p}$;*

(c) *$A_{\mathfrak{m}}$ is integrally closed for all maximal ideals $\mathfrak{m}$.*

PROOF. The implication (a)⇒(b) follows from 1.48, and (b)⇒(c) is obvious. It remains to prove (c)⇒(a). If c is integral over A, then it is integral over each $A_{\mathfrak{m}}$, and hence lies in each $A_{\mathfrak{m}}$. It follows that the ideal consisting of the $a \in A$ such that $ac \in A$ is not contained in any maximal ideal $\mathfrak{m}$, and therefore equals A. Hence $1 \cdot c \in A$. □

Let E/F be a finite extension of fields. Then

$$(\alpha, \beta) \mapsto \mathrm{Tr}_{E/F}(\alpha\beta) \colon E \times E \to F \tag{11}$$

is a symmetric bilinear form on E regarded as a vector space over F.

LEMMA 1.50. *If E/F is separable, then the trace pairing (11) is nondegenerate.*

PROOF. Let $\beta_1, ..., \beta_m$ be a basis for E as an F-vector space. We have to show that the discriminant $\det(\mathrm{Tr}(\beta_i\beta_j))$ of the trace pairing is nonzero. Let $\sigma_1, ..., \sigma_m$ be the distinct F-homomorphisms of E into some large Galois extension Ω of F. Recall (FT, 5.45) that

$$\mathrm{Tr}_{L/K}(\beta) = \sigma_1\beta + \cdots + \sigma_m\beta \tag{12}$$

By direct calculation, we have

$$\begin{aligned}
\det(\mathrm{Tr}(\beta_i\beta_j)) &= \det(\textstyle\sum_k \sigma_k(\beta_i\beta_j)) && \text{(by 12)}\\
&= \det(\textstyle\sum_k \sigma_k(\beta_i)\cdot\sigma_k(\beta_j))\\
&= \det(\sigma_k(\beta_i))\cdot\det(\sigma_k(\beta_j))\\
&= \det(\sigma_k(\beta_i))^2.
\end{aligned}$$

Suppose that $\det(\sigma_i\beta_j) = 0$. Then there exist $c_1, ..., c_m \in \Omega$ such that

$$\sum_i c_i\sigma_i(\beta_j) = 0 \text{ all } j.$$

By linearity, it follows that $\sum_i c_i\sigma_i(\beta) = 0$ for all $\beta \in E$, but this contradicts Dedekind's theorem on the independence of characters (FT, 5.14). □

PROPOSITION 1.51. *Let A be an integrally closed domain with field of fractions F, and let B be the integral closure of A in a separable extension E of F of degree m. There exist free A-submodules M and M' of E such that*

$$M \subset B \subset M'. \tag{13}$$

If A is noetherian, then B is a finite A-algebra.

PROOF. Let $\{\beta_1, ..., \beta_m\}$ be a basis for E over F. According to Proposition 1.40, there exists a $d \in A$ such that $d\cdot\beta_i \in B$ for all i. Clearly $\{d\cdot\beta_1, \dots, d\cdot\beta_m\}$ is still a basis for E as a vector space over F, and so we may assume to begin with that each $\beta_i \in B$. Because the trace pairing is nondegenerate, there is a dual basis $\{\beta'_1, ..., \beta'_m\}$ of E over F with the property that $\mathrm{Tr}(\beta_i\cdot\beta'_j) = \delta_{ij}$ for all i, j. We shall show that

$$A\beta_1 + A\beta_2 + \cdots + A\beta_m \subset B \subset A\beta'_1 + A\beta'_2 + \cdots + A\beta'_m.$$

Only the second inclusion requires proof. Let $\beta \in B$. Then β can be written uniquely as a linear combination $\beta = \sum b_j\beta'_j$ of the β'_j with coefficients $b_j \in F$, and we have to show that each $b_j \in A$. As β_i and β are in B, so also is $\beta\cdot\beta_i$, and so $\mathrm{Tr}(\beta\cdot\beta_i) \in A$ (1.44). But

$$\mathrm{Tr}(\beta\cdot\beta_i) = \mathrm{Tr}(\sum_j b_j\beta'_j\cdot\beta_i) = \sum_j b_j\,\mathrm{Tr}(\beta'_j\cdot\beta_i) = \sum_j b_j\cdot\delta_{ij} = b_i.$$

Hence $b_i \in A$.

If A is Noetherian, then M' is a Noetherian A-module, and so B is finitely generated as an A-module. □

LEMMA 1.52. *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 $a^{-1} \in A$. □

THEOREM 1.53 (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 intersecting S (see 1.14). 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), we 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 1.52.

(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 1.52 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). □

COROLLARY 1.54. *Let $A \subset B$ be rings with B integral over A. Let $\mathfrak{p} \subset \mathfrak{p}'$ be prime ideals of A, and let $\mathfrak{q}$ be a prime ideal of B such that $\mathfrak{q} \cap A = \mathfrak{p}$. Then there exists a prime ideal $\mathfrak{q}'$ of B containing $\mathfrak{q}$ and such that $\mathfrak{q}' \cap A = \mathfrak{p}'$,*

$$\begin{array}{ccccc} B & \quad & \mathfrak{q} & \subset & \mathfrak{q}' \\ | & & | & & | \\ A & & \mathfrak{p} & \subset & \mathfrak{p}'. \end{array}$$

PROOF. We have $A/\mathfrak{p} \subset B/\mathfrak{q}$, and $B/\mathfrak{q}$ is integral over $A/\mathfrak{p}$. According to Theorem 1.53, there exists a prime ideal $\mathfrak{q}''$ in $B/\mathfrak{q}$ such that $\mathfrak{q}'' \cap (A/\mathfrak{p}) = \mathfrak{p}'/\mathfrak{p}$. The inverse image $\mathfrak{q}'$ of $\mathfrak{q}''$ in B has the required properties. □

ASIDE 1.55. Let A be a noetherian integral domain, and let B be the integral closure of A in a finite extension E of the field of fractions F of A. Is B always a finite A-algebra? When A is integrally closed and E is separable over F, or A is a finitely generated k-algebra, then the answer is yes (1.51, 8.3). However, in 1935, Akizuki found an example of a noetherian integral domain A whose integral closure in its field of fractions is not a finite A-algebra. F.K. Schmidt found another example at about the same time.[7]

[7]According to Matsumura (1986, p. x), finding his example cost Akizuki a year's hard struggle. For a discussion of the examples of Akizuki and Schmidt, and generalizations, see Olberding, B., One-dimensional bad Noetherian domains. Trans. Amer. Math. Soc. 366 (2014), no.8, 4067–4095.

e. Tensor Products

Tensor products of modules

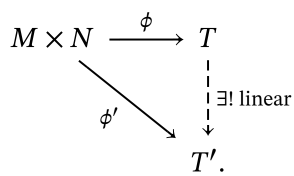
Let A be a ring, and let M, N, and P be A-modules. A map $\phi\colon M\times N \to P$ of A-modules is said to be A-***bilinear*** if

$$\begin{aligned} \phi(x+x',y) &= \phi(x,y)+\phi(x',y), && x,x'\in M, \quad y\in N\\ \phi(x,y+y') &= \phi(x,y)+\phi(x,y'), && x\in M, \quad y,y'\in N\\ \phi(ax,y) &= a\phi(x,y)=\phi(x,ay), && a\in A, \quad x\in M, \quad y\in N, \end{aligned}$$

i.e., if ϕ is A-linear in each variable.

An A-module T together with an A-bilinear map

$$\phi\colon M\times N\to T$$



is called the ***tensor product*** of M and N over A if it has the following universal property: every A-bilinear map

$$\phi'\colon M\times N\to T'$$

factors uniquely through ϕ.

As usual, the universal property determines the tensor product uniquely up to a unique isomorphism. We denote it by $M\otimes_A N$. It is determined by

$$\mathrm{Hom}_{A\text{-linear}}(M\otimes_A N, T)\simeq \mathrm{Hom}_{A\text{-bilinear}}(M\times N, T).$$

CONSTRUCTION

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

$$\sum a_i(x_i,y_i), \quad a_i\in A, \quad x_i\in M, \quad y_i\in N.$$

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

$$\begin{aligned} (x+x',y)-(x,y)-(x',y), &\quad x,x'\in M, \quad y\in N\\ (x,y+y')-(x,y)-(x,y'), &\quad x\in M, \quad y,y'\in N\\ (ax,y)-a(x,y), &\quad a\in A, \quad x\in M, \quad y\in N\\ (x,ay)-a(x,y), &\quad a\in A, \quad x\in M, \quad y\in N, \end{aligned}$$

and define

$$M\otimes_A N = A^{(M\times N)}/P.$$

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

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

is A-bilinear — we have imposed the fewest relations necessary to ensure this. Every element of $M\otimes_A N$ can be written as a finite sum[8]

$$\sum a_i(x_i\otimes y_i), \quad a_i\in A, \quad x_i\in M, \quad y_i\in N,$$

[8]"An element of the tensor product of two vector spaces is not necessarily a tensor product of two vectors, but sometimes a sum of such. This might be considered a mathematical shenanigan but if you start with the state vectors of two quantum systems it exactly corresponds to the notorious notion of entanglement which so displeased Einstein." Georges Elencwajg on mathoverflow.net.

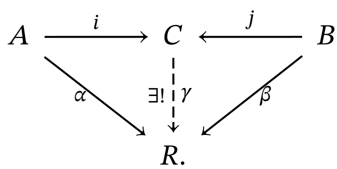
and all relations among these symbols are generated by the following relations

$$(x + x') \otimes y = x \otimes y + x' \otimes y$$
$$x \otimes (y + y') = x \otimes y + x \otimes y'$$
$$ax \otimes y = a(x \otimes y) = x \otimes ay.$$

The pair $(M \otimes_A N, (x, y) \mapsto x \otimes y)$ has the correct universal property because any A-bilinear map $\phi' : M \times N \to T'$ extends uniquely to an A-linear map $A^{(M \times N)} \to T'$, which factors uniquely through $A^{(M \times N)}/P$.

Tensor products of algebras

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



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

$$\mathrm{Hom}_k(A \otimes_k B, R) \simeq \mathrm{Hom}_k(A, R) \times \mathrm{Hom}_k(B, R)$$

(homomorphisms of k-algebras).

Construction

Form the tensor product $A \otimes_k B$ of A and B regarded as k-vector spaces. 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

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

are homomorphisms, and they make $A \otimes_k B$ into the tensor product of A and B in the above sense.

Example 1.56. A k-algebra B, equipped with the given map $k \to B$ and the identity map $B \to B$, has the universal property characterizing $k \otimes_k B$, so $k \otimes_k B \simeq B$. In terms of the constructive definition of tensor products, the isomorphism is $c \otimes b \mapsto cb : k \otimes_k B \to B$.

EXAMPLE 1.57. The ring $k[X_1,\ldots,X_m,X_{m+1},\ldots,X_{m+n}]$, equipped with the obvious inclusions

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

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 obvious bijection

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

In terms of the constructive definition of tensor products, the isomorphism is

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

REMARK 1.58. (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 $S \times T$.

f. Transcendence bases

We review the theory of transcendence bases. For the proofs, see Chapter 9 of FT.

1.59. Elements $\alpha_1,\ldots,\alpha_n$ of a k-algebra A are said to be ***algebraically dependent*** over k there exists a nonzero polynomial $f(X_1,\ldots,X_n) \in k[X_1,\ldots,X_n]$ such that $f(\alpha_1,\ldots,\alpha_n) = 0$. Otherwise, the α_i are said to be ***algebraically independent*** over k.

Now let Ω be a field containing k.

1.60. For a subset A of Ω, we let $k(A)$ denote the smallest subfield of Ω containing k and A. For example, if $A = \{x_1,\ldots,x_m\}$, then $k(A)$ consists of the quotients $\dfrac{f(x_1,\ldots,x_m\}}{g(x_1,\ldots,x_m\}}$ with $f,g \in k[X_1,\ldots,X_m]$. A subset B of Ω is ***algebraically dependent*** on A if each element of B is algebraic over $k(A)$.

1.61 (FUNDAMENTAL THEOREM). Let $A = \{\alpha_1,\ldots,\alpha_m\}$ and $B = \{\beta_1,\ldots,\beta_n\}$ be two subsets of Ω. Assume that

(a) A is algebraically independent (over k), and

(b) A is algebraically dependent on B (over k).

Then $m \le n$.

Note that this becomes the fundamental theorem of linear algebra when replace "algebraically" with "linearly" — the two topics are formally similar.

1.62. A ***transcendence basis*** for Ω over k is an algebraically independent set A such that Ω is algebraic over $k(A)$.

1.63. Assume that there is a finite subset $A \subset \Omega$ such that Ω is algebraic over $k(A)$. Then

(a) every maximal algebraically independent subset of Ω is a transcendence basis;

(b) every subset S of A minimal among those such that Ω is algebraic over $k(S)$ is a transcendence basis; in particular, a finite transcendence basis exists;

(c) all transcendence bases for Ω over k have the same finite number of elements (called the ***transcendence degree***, $\operatorname{tr}\deg_k \Omega$, of Ω over k).

1.64. Let $k \subset L \subset \Omega$ be fields. Then

$$\operatorname{tr}\deg_k \Omega = \operatorname{tr}\deg_k L + \operatorname{tr}\deg_L \Omega.$$

Indeed, if A is a transcendence basis for L/k and B is a transcendence basis for Ω/L, then $A \cup B$ is a transcendence basis for Ω/k.

Exercises

1-1. Let k be an infinite field (not necessarily algebraically closed). Show that an $f \in k[X_1, \dots, X_n]$ 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

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

1-3. A ring A is said to be ***normal*** if $A_{\mathfrak{p}}$ is an integrally closed domain for all prime ideals $\mathfrak{p}$ in A. Show that a noetherian ring is normal if and only if it is a finite product of normal integral domains.

1-4. Prove the statement in 1.64.

Chapter 2

Algebraic Sets

a. Definition of an algebraic set

An ***algebraic subset*** $V(S)$ of k^n is the set of common zeros of some collection S of polynomials in $k[X_1, \ldots, X_n]$,

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

We refer to $V(S)$ as the ***zero set*** of S. Note that

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

— more equations means fewer solutions.

Recall that the ideal $\mathfrak{a}$ generated by a set S consists of the 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 every 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 the zero set of the ideal generated by S. Therefore the algebraic subsets of k^n can also be described as the zero sets of ideals in $k[X_1, \ldots, X_n]$.

An empty set of polynomials imposes no conditions, and so $V(\emptyset) = k^n$. Therefore k^n is an algebraic subset. It is also the zero set of the zero ideal (0). We write $\mathbb{A}^n$ for k^n regarded as an algebraic set.

Examples

2.1. If S is a set of homogeneous linear equations,

$$a_{i1}X_1 + \cdots + a_{in}X_n = 0, \qquad i = 1, \ldots, m,$$

then $V(S)$ is a subspace of k^n. If S is a set of nonhomogeneous linear equations,

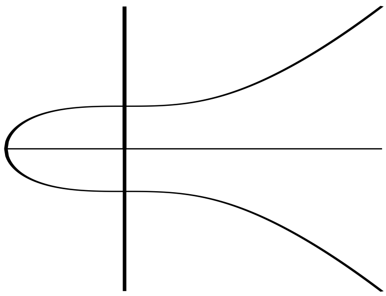
$$a_{i1}X_1 + \cdots + a_{in}X_n = d_i, \qquad i = 1, \ldots, m,$$

then $V(S)$ is either empty or is the translate of a subspace of k^n.

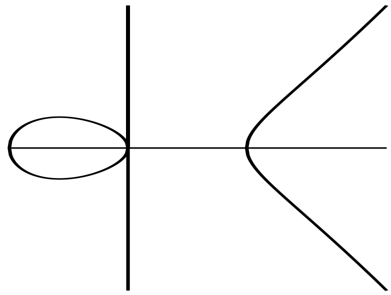
2.2. If S consists of the single equation

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

then $V(S)$ is an ***elliptic curve***. For example,



$Y^2 = X^3 + 1$



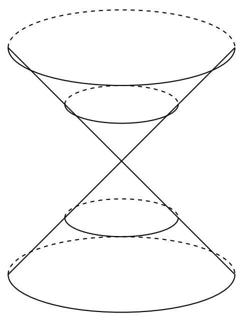
$Y^2 = X(X^2 - 1)$

We generally visualize algebraic sets as though the field k were $\mathbb{R}$, i.e., we draw the ***real locus*** of the curve. However, this can be misleading — see the examples 4.11 and 4.17 below.

2.3. If S consists of the single equation

$$Z^2 = X^2 + Y^2,$$

then $V(S)$ is a cone.



2.4. A nonzero constant polynomial has no zeros, and so the empty set is algebraic.

2.5. The proper algebraic subsets of $\mathbb{A}^1 = k$ are the finite subsets, because a polynomial $f(X)$ in one variable X has only finitely many roots, and every finite set is the set of roots of a polynomial.

2.6. Some generating sets for an ideal will be more useful than others for determining what the algebraic set is. For example, the ideal

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

can be generated by[1]

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

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

b. The Hilbert basis theorem

In our definition of an algebraic set, we did not require the set S of polynomials to be finite, but the Hilbert basis theorem shows that, in fact, every algebraic set is the zero set of a finite set of polynomials. More precisely, the theorem states 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 a set of generators of an ideal has the same zero set as the ideal.

[1]This is, in fact, a Gröbner basis for the ideal.

THEOREM 2.7 (HILBERT BASIS THEOREM). *The ring $k[X_1,\ldots,X_n]$ is noetherian.*

As we noted in the proof of 1.32,

$$k[X_1,\ldots,X_n] = k[X_1,\ldots,X_{n-1}][X_n].$$

Thus an induction argument shows that the theorem follows from the next statement.

THEOREM 2.8. *If A is noetherian, then so also is $A[X]$.*

PROOF. We shall show that every ideal in $A[X]$ is finitely generated. Recall that for a polynomial

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

a_0 is called the leading coefficient of f.

Let $\mathfrak{a}$ be a proper ideal in $A[X]$, and let $\mathfrak{a}(i)$ denote the set of elements of A that occur as the leading coefficient of a polynomial in $\mathfrak{a}$ of degree i (we also include 0). Clearly, $\mathfrak{a}(i)$ is an ideal in A, and $\mathfrak{a}(i) \subset \mathfrak{a}(i+1)$ because, if $cX^i + \cdots \in \mathfrak{a}$, then $X(cX^i + \cdots) \in \mathfrak{a}$.

Let $\mathfrak{b}$ be an ideal of $A[X]$ contained in $\mathfrak{a}$. Then $\mathfrak{b}(i) \subset \mathfrak{a}(i)$, and $\mathfrak{b} = \mathfrak{a}$ if the two are equal for all i. To see this, let f be a polynomial in $\mathfrak{a}$. Because $\mathfrak{b}(\deg f) = \mathfrak{a}(\deg f)$, there exists a $g \in \mathfrak{b}$ with the same leading coefficient as f, and so $f = g + f_1$ with $f_1 \in \mathfrak{a}$ and $\deg(f_1) < \deg(f)$. Similarly, $f_1 = g_1 + f_2$ with $g_1 \in \mathfrak{b}$ and $\deg(f_2) < \deg(f_1)$. Continuing in this fashion, we find that $f = g + g_1 + g_2 + \cdots \in \mathfrak{b}$..

As A is noetherian, the sequence

$$\mathfrak{a}(1) \subset \mathfrak{a}(2) \subset \cdots \subset \mathfrak{a}(i) \subset \cdots$$

eventually becomes constant, say,

$$\mathfrak{a}(d) = \mathfrak{a}(d+1) = \cdots$$

(and then $\mathfrak{a}(d)$ contains the leading coefficient of *every* polynomial in $\mathfrak{a}$). For each $i \leq d$, there exists a finite set of generators $\{a_{i1}, a_{i2}, \ldots, a_{in_i}\}$ for the ideal $\mathfrak{a}(i)$ (as A is noetherian), and we let f_{ij} denote a polynomial in $\mathfrak{a}$ with leading coefficient a_{ij}. The ideal $\mathfrak{b}$ of $A[X]$ generated by the (finitely many) f_{ij} is contained in $\mathfrak{a}$ and has the property that $\mathfrak{b}(i) = \mathfrak{a}(i)$ for all i. Therefore $\mathfrak{b} = \mathfrak{a}$, and $\mathfrak{a}$ is finitely generated. □

ASIDE 2.9. 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. For $n = 1$, the ring $k[X]$ is a principal ideal domain, and so every ideal is generated by a single element. 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 3.45), but often more are required. Determining exactly how many is an area of active research — see 3.58.

c. The Zariski topology

Recall that, for ideals $\mathfrak{a}$ and $\mathfrak{b}$ in $k[X_1,\ldots,X_n]$,

$$\mathfrak{a} \subset \mathfrak{b} \Rightarrow V(\mathfrak{a}) \supset V(\mathfrak{b}).$$

PROPOSITION 2.10. *There are the following relations:*

(a) $V(0) = k^n$; $V(k[X_1,\ldots,X_n]) = \emptyset$;

(b) $V(\mathfrak{ab}) = V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$;

(c) $V(\sum_{i\in I} \mathfrak{a}_i) = \bigcap_{i\in I} V(\mathfrak{a}_i)$ *for every family of ideals* $(\mathfrak{a}_i)_{i\in I}$.

PROOF. (a) Certainly, $V(0) = k^n$, and $V(k[X_1, \ldots, X_n])$ is empty because $1 \in k[X_1, \ldots, X_n]$.

(b) 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 $a \notin V(\mathfrak{ab})$.

(c) 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 (c) is obvious. □

The proposition shows that the algebraic subsets of $\mathbb{A}^n$ satisfy the axioms to be the closed subsets for a topology on $\mathbb{A}^n$: the empty set and the whole space are algebraic; intersections of algebraic sets are algebraic; finite unions of algebraic sets are algebraic. Thus, there is a topology on $\mathbb{A}^n$ for which the closed subsets are exactly the algebraic subsets — this is the ***Zariski topology*** on $\mathbb{A}^n$. The induced topology on a subset V of $\mathbb{A}^n$ 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 $\mathbb{A}^1$, the closed subsets are the finite subsets and the whole space, and so the topology is not Hausdorff (in fact, there are no disjoint nonempty open subsets at all). We shall see in 2.68 below that the proper closed subsets of $\mathbb{A}^2$ are the unions of finitely many points and curves. Note that the Zariski topologies on $\mathbb{C}$ and $\mathbb{C}^2$ are much coarser (have fewer open sets) than the complex topologies.

d. The Hilbert Nullstellensatz

Before examining the relation between the algebraic subsets of $\mathbb{A}^n$ and the ideals of $k[X_1, \ldots, X_n]$, we answer the question of when a collection S of polynomials has a common zero, i.e., when the system of equations

$$g(X_1, \ldots, X_n) = 0, \quad g \in S,$$

is "consistent". Obviously, the system of equations

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

is inconsistent if there exist $f_i \in k[X_1, \ldots, X_n]$ such that $\sum f_i g_i = 1$, that is, if 1 is in the ideal $(g_1, \ldots, g_m)$ generated by the g_i, which therefore equals $k[X_1, \ldots, X_n]$. The converse to this also holds.

THEOREM 2.11 (HILBERT NULLSTELLENSATZ[2]). *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"

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

[2] Nullstellensatz = zero-points-theorem.

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

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

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

Since every proper ideal is contained in a maximal ideal (see p. 14), it suffices to prove this for a maximal ideal $\mathfrak{m}$. Then $K \overset{\text{def}}{=} k[X_1,\dots,X_n]/\mathfrak{m}$ is a field, and it is finitely generated as a k-algebra. The next lemma shows that $K = k$, which completes the proof.

LEMMA 2.12 (ZARISKI'S LEMMA). *Let $k \subset K$ be fields, not necessarily algebraically closed. If K is finitely generated as a k-algebra, then it is algebraic over k. (Hence $K = k$ if k is algebraically closed.)*

PROOF. We begin by showing that $k[X]$ has infinitely many distinct monic irreducible polynomials. When k is infinite, the polynomials $X-a$, $a \in k$, are distinct and irreducible. When k is finite, we can adapt Euclid's argument: if $p_1,\dots,p_r$ are monic irreducible polynomials in $k[X]$, then $p_1 \cdots p_r + 1$ is divisible by a monic irreducible polynomial distinct from $p_1,\dots,p_r$.

We prove the lemma 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

$$K = k[x_1,\dots,x_r], \quad r \geq 1.$$

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. The induction hypothesis applied to $k(x_1) \subset K = k(x_1)[x_2,\dots,x_r]$ shows that K is algebraic over $k(x_1)$. In particular, $x_2,\dots,x_r$ are algebraic over $k(x_1)$, and so (1.40) there exists a $d \in k[x_1]$ such that $dx_2,\dots,dx_r$ are integral over $k[x_1]$.

Let $f \in k(x_1)$. Then $f \in K = k[x_1,\dots,x_r]$ and so, for a sufficiently large N, $d^N f \in k[x_1, dx_2,\dots,dx_r]$. As the dx_i are integral over $k[x_1]$, so also is $d^N f$ (by 1.38), and so it lies in $k[x_1]$ (by 1.43). In particular, for any monic irreducible polynomial $f \in k[x_1]$, $d^N/f \in k[x_1]$ for some N, but this contradicts the fact that there are infinitely many distinct such f. □

Let $k \subset K$ be fields. The lemma shows that if K is finitely generated as a k-algebra, then it is finitely generated as a k-module (FT, 1.30).

e. The correspondence between algebraic sets and radical ideals

The ideal attached to a subset of k^n

For a subset W of k^n, we write $I(W)$ for the set of polynomials that are zero on W:

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

Note that

$$V \subset W \implies I(V) \supset I(W).$$

Clearly, $I(W)$ is an ideal in $k[X_1,\dots,X_n]$. There are the following relations:

(a) $I(k^n) = \{0\}$; $\quad I(\emptyset) = k[X_1, \ldots, X_n]$;

(b) $I(\bigcup W_i) = \bigcap I(W_i)$.

Only the statement $I(k^n) = 0$ is (perhaps) not obvious. It says that every nonzero polynomial in $k[X_1, \ldots, X_n]$ is nonzero at some point of k^n. This is true for any infinite field k (see Exercise 1-1).

EXAMPLE 2.13. Let P be the point $(a_1, \ldots, a_n)$, and let

$$\mathfrak{m}_P = (X_1 - a_1, \ldots, X_n - a_n).$$

Clearly $I(P) \supset \mathfrak{m}_P$, but $\mathfrak{m}_P$ 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 $\mathfrak{m}_P$.

PROPOSITION 2.14. *Let W be a subset of k^n. Then $VI(W)$ is the smallest algebraic subset of k^n containing W. In particular, $VI(W) = W$ if W is an algebraic set.*

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

Radicals of ideals

The ***radical*** of an ideal $\mathfrak{a}$ in a ring A is

$$\mathrm{rad}(\mathfrak{a}) \stackrel{\text{def}}{=} \{f \mid f^r \in \mathfrak{a}, \text{ some } r \in \mathbb{N}\}.$$

PROPOSITION 2.15. *Let $\mathfrak{a}$ be an ideal in a ring A.*

(a) The radical of $\mathfrak{a}$ is an ideal.

(b) $rad(rad(\mathfrak{a})) = rad(\mathfrak{a})$.

PROOF. (a) If $a \in \mathrm{rad}(\mathfrak{a})$, then clearly $fa \in \mathrm{rad}(\mathfrak{a})$ for all $f \in A$. Suppose that $a, b \in \mathrm{rad}(\mathfrak{a})$, 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, and so $a \in \mathrm{rad}(\mathfrak{a})$. □

The radical of the ideal 0 is called the ***nilradical*** $\mathfrak{n}$ of A. Thus, $\mathfrak{n}$ consists of the nilpotent elements of A. It is an ideal in A, and $A/\mathfrak{n}$ is is ***reduced***, i.e., without nonzero nilpotent elements.

An ideal is said to be ***radical*** if it equals its radical. Thus $\mathfrak{a}$ is radical if and only if the ring $A/\mathfrak{a}$ is reduced. Since integral domains are reduced, prime ideals (a fortiori, maximal ideals) are radical. Note that $\mathrm{rad}(\mathfrak{a})$ is radical (2.15b), and hence is the smallest radical ideal containing $\mathfrak{a}$.

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 $X^2 \in \mathfrak{a} + \mathfrak{b}$, $X \notin \mathfrak{a} + \mathfrak{b}$. (See 2.22 below.)

The strong Nullstellensatz

For a polynomial f and point $P \in k^n$, $f^r(P) = f(P)^r$. Therefore f^r is zero at P if and only if f is zero at P, and so, for any subset W of k^n, the ideal $I(W)$ is radical. In particular, $IV(\mathfrak{a}) \supset \operatorname{rad}(\mathfrak{a})$. In fact, the two are equal.

THEOREM 2.16 (STRONG NULLSTELLENSATZ). *For any ideal* $\mathfrak{a}$ *in* $k[X_1, \ldots, X_n]$,

$$IV(\mathfrak{a}) = \operatorname{rad}(\mathfrak{a});$$

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 a polynomial h vanishes on $V(\mathfrak{a})$, then $h^N \in \mathfrak{a}$ for some $N > 0$. We may assume $h \neq 0$. Let $g_1, \ldots, g_m$ generate $\mathfrak{a}$, and consider the system of $m+1$ equations in $n+1$ symbols,

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

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 $(a_1, \ldots, a_n, b)$ does not satisfy the last equation. 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

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

(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

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

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

$$h^N = \sum_{i=1}^{m} (\text{polynomial in } X_1, \ldots, X_n) \cdot g_i(X_1, \ldots, X_n),$$

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

COROLLARY 2.17. *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 (2.16), and that $VI(W) = W$ if W is an algebraic set (2.14). Therefore, I and V are inverse bijections. □

COROLLARY 2.18. *The radical of an ideal in $k[X_1, \dots, X_n]$ is equal to the intersection of the maximal ideals containing it.*

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

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

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

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

(see 2.13). Thus $\mathfrak{m}_P \supset \mathfrak{a}$ if $P \in V(\mathfrak{a})$. 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

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

□

Remarks

2.19. 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 (which we knew already from Exercise 1-1).

2.20. The one-to-one correspondence in Corollary 2.17 is order reversing. Therefore the maximal proper radical ideals correspond to the minimal nonempty algebraic sets. But the maximal proper radical ideals are simply the maximal ideals in $k[X_1, \dots, X_n]$, and the minimal nonempty algebraic sets are the one-point sets. As

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

(see 2.13), we see that the maximal ideals of $k[X_1, \dots, X_n]$ are exactly the ideals $(X_1 - a_1, \dots, X_n - a_n)$ with $(a_1, \dots, a_n) \in k^n$.

2.21. An algebraic set $V(\mathfrak{a})$ is empty if and only if $\mathfrak{a} = k[X_1, \dots, X_n]$ (Nullstellensatz, 2.11).

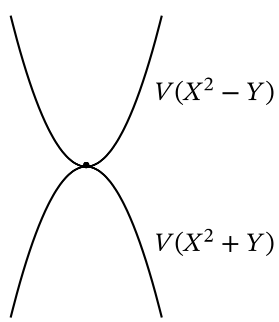
2.22. Let W and W' be algebraic sets. As $W \cap W'$ is the largest algebraic subset contained in both W and W', $I(W \cap W')$ must be the smallest radical ideal containing both $I(W)$ and $I(W')$:

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

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 $\mathrm{char}(k) \neq 2$). 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”.



2.23. Let $\mathcal{P}$ be the set of subsets of k^n and $\mathcal{Q}$ the set of subsets of $k[X_1,\ldots,X_n]$. Then $I:\mathcal{P}\to\mathcal{Q}$ and $V:\mathcal{Q}\to\mathcal{P}$ define a simple Galois correspondence between $\mathcal{P}$ and $\mathcal{Q}$: they are order reversing maps such that $VI(W)\supset W$ and $IV(\mathfrak{a})\supset\mathfrak{a}$. It follows that I and V define a one-to-one correspondence between $I(\mathcal{P})$ and $V(\mathcal{Q})$ (see FT, 7.19). But the strong Nullstellensatz shows that $I(\mathcal{P})$ consists exactly of the radical ideals, and (by definition) $V(\mathcal{Q})$ consists of the algebraic subsets. Thus we recover Corollary 2.17.

ASIDE 2.24. The algebraic subsets of $\mathbb{A}^n$ capture only part of the ideal theory of $k[X_1,\ldots,X_n]$ because two ideals with the same radical correspond to the same algebraic subset. There is a finer notion of an algebraic scheme over k for which the closed algebraic subschemes of $\mathbb{A}^n$ are in one-to-one correspondence with the ideals in $k[X_1,\ldots,X_n]$ (see Chapter 10 on my website).

f. Finding the radical of an ideal

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

PROPOSITION 2.25. *A 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 2.16. Conversely, from the identities

$$1=Y^Nh^N+(1-Y^Nh^N)=Y^Nh^N+(1-Yh)\cdot(1+Yh+\cdots+Y^{N-1}h^{N-1})$$

we see that, if $h^N\in\mathfrak{a}$, then $1\in\mathfrak{a}+(1-Yh)$. □

Given a set of generators of an ideal in $k[X_1,\ldots,X_n]$, there is an algorithm for deciding whether or not a polynomial belongs to the ideal, and hence an algorithm for deciding whether or not a polynomial belongs to the radical of the ideal. There are even algorithms for finding a set of generators for the radical. These algorithms have been implemented in the computer algebra systems CoCoA and Macaulay2.

g. Properties of the Zariski topology

We now examine more closely the Zariski topology on $\mathbb{A}^n$ and on its algebraic subsets. Proposition 2.14 says that, for a subset W of $\mathbb{A}^n$, $VI(W)$ is the closure of W, and 2.17 says that there is a one-to-one correspondence between the closed subsets of $\mathbb{A}^n$ 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 2.26. *Let V be an algebraic subset of $\mathbb{A}^n$.*

(a) *The points of V are closed for the Zariski topology.*

(b) *Every ascending chain of open subsets $U_1\subset U_2\subset\cdots$ of V eventually becomes constant. Equivalently, every descending chain of closed subsets of V eventually becomes constant.*

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

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

(b) We prove the second statement. A sequence $V_1 \supset V_2 \supset \cdots$ of closed subsets of V gives rise to a sequence of radical ideals $I(V_1) \subset I(V_2) \subset \dots$, which eventually becomes constant because $k[X_1, \dots, X_n]$ is noetherian.

(c) Suppose given an open covering of V, and let $\mathcal{U}$ be the collection of open subsets of V that can be expressed as a finite union of sets in the covering. If $\mathcal{U}$ does not contain V, then every element of $\mathcal{U}$ is properly contained in another element, and so there exists an infinite ascending chain of sets in $\mathcal{U}$ (axiom of dependent choice), contradicting (b). □

A topological space whose points are closed is said to be T_1; the condition means that, for any pair of distinct points, each has an open neighbourhood not containing the other. 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 topological space having property (c) is said to be ***quasi-compact***.[3] The proof of (c) shows that every noetherian space is quasi-compact. Since any open subset of a noetherian space is again noetherian, it is also quasi-compact.

h. Decomposition of an algebraic set into irreducible algebraic sets

A topological space is said to be ***irreducible*** if it is not the union of two proper closed subsets. Equivalent conditions: every pair of nonempty open subsets has nonempty intersection; every nonempty open subset is dense. By convention, the empty topological space is not irreducible.

The closure of an irreducible space is irreducible and a nonempty open subset of an irreducible space is irreducible.

A topological space is ***connected*** if it is not the union of two *disjoint* proper closed subsets. Therefore, irreducible topological spaces are connected.

In a Hausdorff topological space, any two points have disjoint open neighbourhoods. Therefore, the only irreducible Hausdorff spaces are those consisting of a single point.

PROPOSITION 2.27. *An algebraic set W is irreducible if and only if $I(W)$ is prime.*

PROOF. Let W be an irreducible algebraic set, and let $fg \in I(W)$ — we have to show that either f or g is 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 $f \in I(W)$.

Let W be an algebraic set such that $I(W)$ is prime, and let $W = V(\mathfrak{a}) \cup V(\mathfrak{b})$ with $\mathfrak{a}$ and $\mathfrak{b}$ radical ideals — we have to show that W equals $V(\mathfrak{a})$ or $V(\mathfrak{b})$. The ideal $\mathfrak{a} \cap \mathfrak{b}$ is radical, and $V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$ (2.10); hence $I(W) = \mathfrak{a} \cap \mathfrak{b}$. If $W \neq V(\mathfrak{a})$, then there exists an $f \in \mathfrak{a} \smallsetminus I(W)$. Let $g \in \mathfrak{b}$. Then $fg \in \mathfrak{a} \cap \mathfrak{b} = I(W)$, and so $g \in I(W)$ (here we use that $I(W)$ is prime). We conclude that $\mathfrak{b} \subset I(W)$, and so $V(\mathfrak{b}) \supset V(I(W)) = W$. □

[3] Bourbaki's terminology

SUMMARY 2.28. There are one-to-one correspondences,

$$\begin{aligned} \text{radical ideals in } k[X_1,\dots,X_n] &\leftrightarrow \text{algebraic subsets of } \mathbb{A}^n \\ \text{prime ideals in } k[X_1,\dots,X_n] &\leftrightarrow \text{irreducible algebraic subsets of } \mathbb{A}^n \\ \text{maximal ideals in } k[X_1,\dots,X_n] &\leftrightarrow \text{one-point subsets of } \mathbb{A}^n. \end{aligned}$$

EXAMPLE 2.29. Let $f \in k[X_1,\dots,X_n]$. We know that $k[X_1,\dots,X_n]$ is a unique factorization domain (1.32), and so (f) is a prime ideal if and only if f is irreducible (1.33). Thus

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

On the other hand, suppose that f factors as

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

Then

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

LEMMA 2.30. *Let W be an irreducible topological space. If $W = W_1 \cup \dots \cup W_r$ with each W_i closed, then W is equal to one of the W_i.*

PROOF. When $r = 2$, the statement is the definition of "irreducible". Suppose that $r > 2$. Then $W = W_1 \cup (W_2 \cup \dots \cup W_r)$, and so $W = W_1$ or $W = (W_2 \cup \dots \cup W_r)$; if the second, then $W = W_2$ or $W_3 \cup \dots \cup W_r$, etc. □

PROPOSITION 2.31. *Let V be a nonempty noetherian topological space. Then V is a finite union of irreducible closed subsets, $V = V_1 \cup \dots \cup V_m$. 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.*

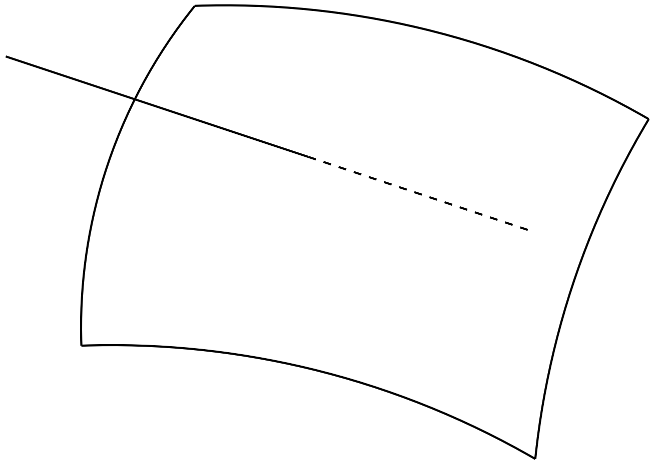
PROOF. Suppose that V cannot be written as a finite union of irreducible closed subsets. Then, because V is noetherian, there will be a nonempty closed subset W of V that is minimal among those that cannot be written in this way. But W itself cannot be irreducible, and so $W = W_1 \cup W_2$, with W_1 and W_2 proper closed subsets of W. Because W was minimal, each W_i is a finite union of irreducible closed subsets. Hence W is also, which is a contradiction.

Suppose that

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

are two irredundant decompositions of V. 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 $f : \{1,\dots,m\} \to \{1,\dots,n\}$ such that $V_i \subset W_{f(i)}$ for each i. Similarly, there is a function $g : \{1,\dots,n\} \to \{1,\dots,m\}$ 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 $fg = \text{id}$. Thus f and g are bijections, and the decompositions differ only in the numbering of the sets. □

The V_i given uniquely by the proposition are called the ***irreducible components*** of V. They are exactly the maximal irreducible subsets of V. In Example 2.29, the $V(f_i)$ are the irreducible components of $V(f)$.



A connected algebraic set with two irreducible components.

COROLLARY 2.32. *The radical of an ideal* $\mathfrak{a}$ *in* $k[X_1,\dots,X_n]$ *is a finite intersection of prime ideals,* $\mathrm{rad}(\mathfrak{a}) = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_n$. *If there are no inclusions among the* $\mathfrak{p}_i$, *then the* $\mathfrak{p}_i$ *are uniquely determined up to order (and they are exactly the minimal prime ideals containing* $\mathfrak{a}$*).*

PROOF. Write $V(\mathfrak{a})$ as a union of its irreducible components, $V(\mathfrak{a}) = \bigcup_{i=1}^n V_i$, and let $\mathfrak{p}_i = I(V_i)$. Then $\mathrm{rad}(\mathfrak{a}) = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_n$ because they are both radical ideals and

$$V(\mathrm{rad}(\mathfrak{a})) = V(\mathfrak{a}) = \bigcup V(\mathfrak{p}_i) \overset{2.10\mathrm{b}}{=} V(\bigcap\nolimits_i \mathfrak{p}).$$

The uniqueness similarly follows from the proposition. □

Remarks

An irreducible topological space is connected, but a connected topological space need not be irreducible. For example, the union of two surfaces in 3-space intersecting along a curve is reducible, but connected.

2.33. An algebraic subset V of $\mathbb{A}^n$ is disconnected if and only if there exist radical ideals $\mathfrak{a}$ and $\mathfrak{b}$ such that V is the disjoint union of $V(\mathfrak{a})$ and $V(\mathfrak{b})$, so

$$\begin{cases} V = V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b}) & \iff \quad \mathfrak{a} \cap \mathfrak{b} = I(V) \\ \emptyset = V(\mathfrak{a}) \cap V(\mathfrak{b}) = V(\mathfrak{a} + \mathfrak{b}) & \iff \quad \mathfrak{a} + \mathfrak{b} = k[X_1,\dots,X_n]. \end{cases}$$

Then

$$k[V] \simeq \frac{k[X_1,\dots,X_n]}{\mathfrak{a}} \times \frac{k[X_1,\dots,X_n]}{\mathfrak{b}}$$

by Theorem 1.1.

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

2.35. In $k[X_1,\dots,X_n]$, a principal ideal (f) is radical if and only if f is square-free, in which case f is a product of distinct irreducible polynomials, $f = f_1 \dots f_r$, and $(f) = (f_1) \cap \dots \cap (f_r)$.

ASIDE 2.36. Let A be a noetherian ring. A proper ideal $\mathfrak{q}$ in A is ***primary*** if every zero-divisor in $A/\mathfrak{q}$ is nilpotent. Every ideal $\mathfrak{a}$ in A can be written as an intersection of primary ideals

$$\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n.$$

Choose a minimal such decomposition, and let $\mathfrak{p}_i = \mathrm{rad}(\mathfrak{q}_i)$. Then each $\mathfrak{p}_i$ is prime, and

$$\mathrm{rad}(\mathfrak{a}) = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_n.$$

See CA, §19. For the ideal (f) in 2.35, with $f = \prod f_i^{m_i}$, these decompositions become

$$\begin{aligned}(f) &= (f_1^{m_1}) \cap \ldots \cap (f_n^{n_m}) \text{ and}\\ \mathrm{rad}(f) &= (f_1) \cap \ldots \cap (f_n).\end{aligned}$$

i. Regular functions; the coordinate ring of an algebraic set

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

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

This is a finitely generated k-algebra. It is reduced because $\mathfrak{a}$ is radical, but it is not necessarily an integral domain. An $f \in k[X_1, \ldots, X_n]$ defines a function

$$P \mapsto f(P) \colon V \to k.$$

Functions of this form are said to be ***regular.*** Two polynomials $f, g \in k[X_1, \ldots, X_n]$ define the same function on V if and only if they define the same element of $k[V]$, and so $k[V]$ is the ring of regular functions on V. The ***coordinate function***

$$x_i \colon V \to k, \quad (a_1, \ldots, a_n) \mapsto a_i$$

is regular, and $k[V] = k[x_1, \ldots, x_n]$, so the coordinate ring of V is the k-algebra generated by the coordinate functions on V.

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

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

— it is a closed subset of V. Let $W = V(\mathfrak{b})$. The quotient maps

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

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

Write π for the quotient map $k[X_1, \ldots, X_n] \twoheadrightarrow k[V]$. 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 (because 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.

Now 2.28 holds for ideals in $k[V]$ and algebraic subsets of V,

$$\begin{aligned} \text{radical ideals in } k[V] &\leftrightarrow \text{algebraic subsets of } V \\ \text{prime ideals in } k[V] &\leftrightarrow \text{irreducible algebraic subsets of } V \\ \text{maximal ideals in } k[V] &\leftrightarrow \text{one-point sets of } V. \end{aligned}$$

Moreover (see 2.33), the decompositions of a closed subset W of V into a disjoint union of closed subsets correspond to pairs of radical ideals $\mathfrak{a}, \mathfrak{b} \in k[V]$ such that

$$k[W] = k[V]/\mathfrak{a} \cap \mathfrak{b} \simeq k[V]/\mathfrak{a} \times k[V]/\mathfrak{b}.$$

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

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

It is an open subset of V, because its complement is the closed set $V((h))$. It is empty if and only if h is zero (2.19).

PROPOSITION 2.37. *The sets $D(h)$, $h \in k[V]$, form a base for the topology on V: each $D(h)$ is open and every open set is a (finite) union of sets $D(h)$.*

PROOF. We have already observed that $D(h)$ is open. Every open subset U of V is the complement of a set $V(\mathfrak{a})$, and if $f_1, \ldots, f_m$ generate the ideal $\mathfrak{a}$, 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

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

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

If the algebraic set V is irreducible, then $I(V)$ is a prime ideal, and $k[V]$ is an integral domain. Its field of fractions, $k(V)$ is called the ***function field*** of V or the ***field of rational functions*** on V.

j. Regular maps

Let $W \subset k^m$ and $V \subset k^n$ be algebraic sets, and let x_i denote the ith coordinate function

$$(b_1, \ldots, b_n) \mapsto b_i : V \to k.$$

The ith ***component*** of a map $\varphi : W \to V$ is

$$\varphi_i \stackrel{\text{def}}{=} x_i \circ \varphi.$$

Thus, φ is the map

$$P \mapsto (\varphi_1(P), \ldots, \varphi_n(P)) : W \to V \subset k^n.$$

DEFINITION 2.38. A continuous map $\varphi\colon W \to V$ of algebraic sets is ***regular*** if each of its components φ_i is a regular function on W.

As the coordinate functions generate $k[V]$, a continuous map φ is regular if and only if $f\circ\varphi$ is a regular function on W for every regular function f on V. Thus a regular map $\varphi\colon W \to V$ of algebraic sets defines a homomorphism $f \mapsto f\circ\varphi\colon k[V] \to k[W]$ of k-algebras, which we sometimes denote by φ^*.

k. Hypersurfaces; finite and quasi-finite maps

A ***hypersurface*** in $\mathbb{A}^{n+1}$ is the algebraic set H defined by a single nonzero nonconstant polynomial,

$$H\colon \quad f(T_1,\dots,T_n,X)=0.$$

We examine the regular map $H \to \mathbb{A}^n$ defined by the projection

$$(t_1,\dots,t_n,x) \mapsto (t_1,\dots,t_n).$$

We can write f in the form

$$f = a_0X^m + a_1X^{m-1} + \cdots + a_m, \quad a_i \in k[T_1,\dots,T_n], \quad a_0 \neq 0.$$

We assume that $m \neq 0$, i.e., that X occurs in f (otherwise, H is a cylinder over a hypersurface in $\mathbb{A}^n$). The fibre of the map $H \to \mathbb{A}^n$ over $(t_1,\dots,t_n) \in k^n$ is the set of points $(t_1,\dots,t_n,c)$ such that c is a root of the polynomial

$$a_0(t)X^m + a_1(t)X^{m-1} + \cdots + a_m(t), \quad a_i(t) \stackrel{\text{def}}{=} a_i(t_1,\dots,t_n) \in k.$$

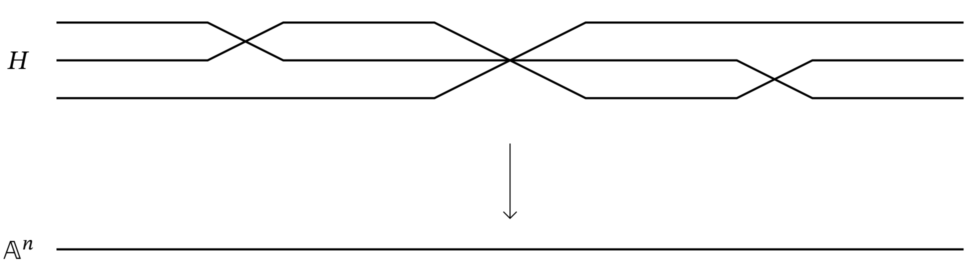
Suppose first that $a_0 \in k$, so that $a_0(t)$ is a nonzero constant independent of t. Then the fibre over t consists of the roots of the polynomial

$$a_0X^m + a_1(t)X^{m-1} + \cdots + a_m(t), \tag{14}$$

in $k[X]$. Counting multiplicities, there are exactly m of these. More precisely, let D be the discriminant of the polynomial[4]

$$a_0X^m + a_1X^{m-1} + \cdots + a_m.$$

Then $D \in k[X_1,\dots,X_m]$, and the fibre has exactly m points over the open subset where $D \neq 0$, and fewer then m points over the closed subset where $D = 0$.[5] We can picture it schematically as follows ($m = 3$):



[4]See FT, p. 57 et seq. for discriminants.

[5]I am ignoring the possibility that D is identically zero. This case occurs when the characteristic is $p \neq 0$, and f is a polynomial in $T_1,\dots,T_n$, and X^p.

Now drop the condition that a_0 is constant. For certain t, the degree of (14) may drop, which means that some roots have "disappeared off to infinity". For example, if $f(T,X) = TX - 1$, then there is one point $(t, 1/t)$ in the fibre over t when $t \neq 0$ but no point when $t = 0$. Worse, for certain t all coefficients may be zero, in which case the fibre is a line. In general, there is a nested collection of closed subsets of $\mathbb{A}^n$ such that the number of points in the fibre (counting multiplicities) drops as you pass to a smaller subset, except that over the smallest subset the fibre may be a full line.

DEFINITION 2.39. Let $\varphi \colon W \to V$ be a regular map of algebraic subsets and $\varphi^* \colon k[V] \to k[W]$ the corresponding map $f \mapsto f \circ \varphi$ on rings.

(a) The map φ is ***dominant*** if $\varphi(W)$ is dense in V, i.e., every nonempty open subset of V intersects $\varphi(W)$.

(b) The map φ is ***quasi-finite*** if $\varphi^{-1}(P)$ is finite for all $P \in V$.

(c) The map φ is ***finite*** if $k[W]$ is a finite $k[V]$-algebra.

Finite maps are quasi-finite. To see this, note that the points of W lying over a point P of V correspond to the maximal ideals $\mathfrak{m}$ of $k[W]$ such that $\varphi^{*-1}(\mathfrak{m}) = \mathfrak{m}_P$, and that these correspond to the maximal ideals of $A \stackrel{\text{def}}{=} k[W] \otimes_{k[V]} (k[V]/\mathfrak{m}_P)$. If φ is finite, then A is a finite k-algebra. Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ be maximal ideals in A. Then $\mathfrak{m}_i + \mathfrak{m}_j = A$ for $i \neq j$, and so the map

$$A \to A/\mathfrak{m}_1 \times \cdots \times A/\mathfrak{m}_n$$

is surjective (1.1). Thus n is at most the dimension of A as a k-algebra.

As $k[W]$ is finitely generated as a k-algebra, hence as a $k[V]$-algebra, to say that $k[W]$ is a finite $k[V]$-algebra means that it is integral over $k[V]$ (1.36).

The map $H \to \mathbb{A}^n$ considered above is finite if and only if a_0 is constant, and quasi-finite if and only if the polynomials $a_0, \ldots, a_m$ have no common zero in k^n.

PROPOSITION 2.40. *A regular map $\varphi \colon W \to V$ is dominant if and only if $\varphi^* \colon k[V] \to k[W]$ is injective.*

PROOF. If φ is dominant and $f \in k[V]$ is nonzero, then $D(f)$ intersects $\varphi(W)$, and so $f \circ \varphi \neq 0$. If φ is not dominant, then its image is contained in a proper closed subset of V, which is contained in $V(f)$ for some nonzero $f \in k[V]$; then $f \circ \varphi = 0$. □

PROPOSITION 2.41. *A dominant finite map is surjective.*

PROOF. Let $\varphi \colon W \to V$ be dominant and finite. Then $\varphi^* \colon k[V] \to k[W]$ is injective, and $k[W]$ is integral over the image of $k[V]$. According to the going-up theorem (1.53), for every maximal ideal $\mathfrak{m}$ of $k[V]$ there exists a maximal ideal $\mathfrak{n}$ of $k[W]$ such that $\mathfrak{m} = \mathfrak{n} \cap k[V]$. Because of the correspondence between points and maximal ideals, this implies that φ is surjective. □

l. Noether normalization theorem

Let H be a hypersurface in $\mathbb{A}^{n+1}$. We show that, after a linear change of coordinates, the projection map $(x_1, \ldots, x_{n+1}) \mapsto (x_1, \ldots, x_n) \colon \mathbb{A}^{n+1} \to \mathbb{A}^n$ defines a *finite* map $H \to \mathbb{A}^n$.

PROPOSITION 2.42. *Let*

$$H: \quad f(X_1, \dots, X_{n+1}) = 0$$

be a hypersurface in $\mathbb{A}^{n+1}$. *There exist* $c_1, \dots, c_n \in k$ *such that the map* $H \to \mathbb{A}^n$ *defined by*

$$(x_1, \dots, x_{n+1}) \mapsto (x_1 - c_1 x_{n+1}, \dots, x_n - c_n x_{n+1})$$

is finite.

PROOF. Let $c_1, \dots, c_n \in k$. In terms of the coordinates $x_i' = x_i - c_i x_{n+1}$, the hyperplane H is the zero set of

$$f(X_1 + c_1 X_{n+1}, \dots, X_n + c_n X_{n+1}, X_{n+1}) = a_0 X_{n+1}^m + a_1 X_{n+1}^{m-1} + \cdots.$$

The next lemma shows that the c_i can be chosen so that a_0 is a nonzero constant. This implies that the map $H \to \mathbb{A}^n$ defined by $(x_1, \dots, x_{n+1}) \mapsto (x_1', \dots, x_n')$ is finite. □

LEMMA 2.43. *Let* k *be an infinite field (not necessarily algebraically closed), and let* $f \in k[X_1, \dots, X_n, T]$. *There exist* $c_1, \dots, c_n \in k$ *such that*

$$f(X_1 + c_1 T, \dots, X_n + c_n T, T) = a_0 T^m + a_1 T^{m-1} + \cdots + a_m$$

with $a_0 \in k^\times$ *and all* $a_i \in k[X_1, \dots, X_n]$.

PROOF. Let F be the homogeneous part of highest degree of f and let $r = \deg(F)$. Then

$$F(X_1 + c_1 T, \dots, X_n + c_n T, T) = F(c_1, \dots, c_n, 1) T^r + \text{terms of degree} < r \text{ in } T,$$

because the polynomial $F(X_1 + c_1 T, \dots, X_n + c_n T, T)$ is still homogeneous of degree r in $X_1, \dots, X_n, T$, and so the coefficient of the monomial T^r can be obtained by setting each X_i equal to zero in F and T to 1. As $F(X_1, \dots, X_n, T)$ is a nonzero *homogeneous* polynomial, $F(X_1, \dots, X_n, 1)$ is a nonzero polynomial, and so we can choose the c_i so that $F(c_1, \dots, c_n, 1) \neq 0$ (Exercise 1-1). Now

$$f(X_1 + c_1 T, \dots, X_n + c_n T, T) = F(c_1, \dots, c_n, 1) T^r + \text{terms of degree} < r \text{ in } T,$$

with $F(c_1, \dots, c_n, 1) \in k^\times$, as required. □

In fact, *every* algebraic set V admits a finite surjective map to $\mathbb{A}^d$ for some d.

THEOREM 2.44. *Let* V *be an algebraic set. For some natural number* d, *there exists a finite surjective map* $\varphi: V \to \mathbb{A}^d$.

This follows from the next statement applied to $A = k[V]$: the regular functions $x_1, \dots, x_d$ define a map $V \to \mathbb{A}^d$, which is finite and surjective because $k[x_1, \dots, x_d] \to A$ is finite and injective.

THEOREM 2.45 (NOETHER NORMALIZATION THEOREM). *Let* A *be a finitely generated* k*-algebra. There exist elements* $x_1, \dots, x_d \in A$ *that are algebraically independent over* k, *and such that* A *is finite over* $k[x_1, \dots, x_d]$.

It is not necessary to assume that A is reduced in Theorem 2.45, nor that k is algebraically closed, although the proof we give requires it to be infinite (for the general proof, see CA, 8.1).

Let $A = k[x_1, \ldots, x_n]$. We prove the theorem by induction on n. If the x_i are algebraically independent, there is nothing to prove. Otherwise, the next lemma shows that A is finite over a subring $B = k[y_1, \ldots, y_{n-1}]$. By induction, B is finite over a subring $C = k[z_1, \ldots, z_d]$ with $z_1, \ldots, z_d$ algebraically independent, and A is finite over C.

LEMMA 2.46. *Let $A = k[x_1, \ldots, x_n]$ be a finitely generated k-algebra, and let $\{x_1, \ldots, x_d\}$ be a maximal algebraically independent subset of $\{x_1, \ldots, x_n\}$. If $n > d$, then there exist $c_1, \ldots, c_d \in k$ such that A is finite over $k[x_1 - c_1x_n, \ldots, x_d - c_dx_n, x_{d+1}, \ldots, x_{n-1}]$.*

PROOF. By assumption, the set $\{x_1, \ldots, x_d, x_n\}$ is algebraically dependent, and so there exists a nonzero $f \in k[X_1, \ldots, X_d, T]$ such that

$$f(x_1, \ldots, x_d, x_n) = 0. \tag{15}$$

Because $\{x_1, \ldots, x_d\}$ is algebraically independent, T occurs in f, and so

$$f(X_1, \ldots, X_d, T) = a_0T^m + a_1T^{m-1} + \cdots + a_m$$

with $a_i \in k[X_1, \ldots, X_d]$, $a_0 \neq 0$, and $m > 0$.

If $a_0 \in k$, then (15) shows that x_n is integral over $k[x_1, \ldots, x_d]$. Hence $x_1, \ldots, x_n$ are integral over $k[x_1, \ldots, x_{n-1}]$, and so A is finite over $k[x_1, \ldots, x_{n-1}]$.

If $a_0 \notin k$, then, for a suitable choice of $(c_1, \ldots, c_d) \in k$, the polynomial

$$g(X_1, \ldots, X_d, T) \stackrel{\text{def}}{=} f(X_1 + c_1T, \ldots, X_d + c_dT, T)$$

takes the form

$$g(X_1, \ldots, X_d, T) = bT^r + b_1T + \cdots + b_r$$

with $b \in k^\times$ (see 2.43). As

$$g(x_1 - c_1x_n, \ldots, x_d - c_dx_n, x_n) = 0 \tag{16}$$

this shows that x_n is integral over $k[x_1 - c_1x_n, \ldots, x_d - c_dx_n]$, and so A is finite over $k[x_1 - c_1x_n, \ldots, x_d - c_dx_n, x_{d+1}, \ldots, x_{n-1}]$ as before. □

Remarks

2.47. For an irreducible algebraic subset V of $\mathbb{A}^n$, the above argument can be modified to prove the following more precise statement:

> Let $x_1, \ldots, x_n$ be the coordinate functions on V; after possibly renumbering the coordinates, we may suppose that $\{x_1, \ldots, x_d\}$ is a maximal algebraically independent subset of $\{x_1, \ldots, x_n\}$; then there exist $c_{ij} \in k$ such that the map
>
> $$(x_1, \ldots, x_n) \mapsto \left(x_1 - \sum_{j=d+1}^{n} c_{1j}x_j, \ldots, x_d - \sum_{j=d+1}^{n} c_{dj}x_j\right) : \mathbb{A}^n \to \mathbb{A}^d$$
>
> induces a finite surjective map $V \to \mathbb{A}^d$.

Indeed, Lemma 2.46 shows that there exist $c_1, \ldots, c_n \in k$ such that $k[V]$ is finite over $k[x_1 - c_1x_n, \ldots, x_d - c_dx_n, x_{d+1}, \ldots, x_{n-1}]$. Now $\{x_1, \ldots, x_d\}$ is algebraically dependent on $\{x_1 - c_1x_n, \ldots, x_d - c_dx_n\}$. If the second set were not algebraically independent, we could drop one of its elements, but this would contradict 1.61. Therefore $\{x_1 - c_1x_n, \ldots, x_d - c_dx_n\}$ is a maximal algebraically independent subset of $\{x_1 - c_1x_n, \ldots, x_d - c_dx_n, x_{d+1}, \ldots, x_{n-1}\}$ and we can repeat the argument.

m. Dimension

The dimension of a topological space

Let V be a noetherian topological space whose points are closed.

DEFINITION 2.48. The ***dimension*** of V is the supremum of the lengths of the chains

$$V_0 \supset V_1 \supset \cdots \supset V_d$$

of distinct irreducible closed subsets (the length of the displayed chain is d).

2.49. Let $V_1, \ldots, V_m$ be the irreducible components of V. Then (obviously)

$$\dim(V) = \max_i(\dim(V_i)).$$

2.50. Assume that V is irreducible, and let W be a proper closed subspace of V. Then every chain $W_0 \supset W_1 \supset \cdots$ in W extends to a chain $V \supset W_0 \supset \cdots$, and so $\dim(W)+1 \leq \dim(V)$. If $\dim(V) < \infty$, then $\dim(W) < \dim(V)$.

Thus an irreducible topological space V has dimension 0 if and only if it is a point; it has dimension ≤ 1 if and only if every proper closed subset is a point; and, inductively, V has dimension $\leq n$ if and only if every proper closed subset has dimension $\leq n-1$.

The dimension of an algebraic set

DEFINITION 2.51. The ***dimension*** of an algebraic set is its dimension as a topological space.

Because of the correspondence between the prime ideals in $k[V]$ and irreducible closed subsets of V,

$$\dim(V) = \text{Krull dimension of } k[V].$$

Note that, if $V_1, \ldots, V_m$ are the irreducible components of V, then

$$\dim V = \max_i \dim(V_i).$$

When the V_i all have the same dimension d, we say that V has ***pure dimension*** d. A one-dimensional algebraic set is called a ***curve***; a two-dimensional algebraic set is called a ***surface***; and an n-dimensional algebraic set is called an ***n-fold***.

Let V be an irreducible algebraic set and W an algebraic subset of V. If W is irreducible, then its ***codimension*** in V is

$$\operatorname{codim}_V W \stackrel{\text{def}}{=} \dim V - \dim W.$$

Dimension and transcendent degree

THEOREM 2.52. *Let V be an irreducible algebraic set. Then*

$$\dim(V) = \operatorname{tr\,deg}_k k(V).$$

The proof will occupy the rest of this subsection.

Let A be an arbitrary commutative ring. Let $x \in A$, and let $S_{\{x\}}$ denote the multiplicative subset of A consisting of the elements of the form

$$x^n(1 - ax), \quad n \in \mathbb{N}, \quad a \in A.$$

The ***boundary*** $A_{\{x\}}$ of A at x is defined to be the ring of fractions $S_{\{x\}}^{-1}A$.

We write $\dim(A)$ for the Krull dimension of A.

PROPOSITION 2.53. *Let A be a ring and let $n \in \mathbb{N}$. Then*

$$\dim(A) \leq n \iff \textit{for all } x \in A,\ \dim(A_{\{x\}}) \leq n - 1.$$

PROOF. We shall use the one-to-one correspondence between the prime ideals of $S^{-1}A$ and the prime ideals of A disjoint from S (1.14). We begin with two observations.

(a) *For every $x \in A$ and maximal ideal $\mathfrak{m} \subset A$, $\mathfrak{m} \cap S_{\{x\}} \neq \emptyset$.* Indeed, if $x \in \mathfrak{m}$, then certainly $x \in \mathfrak{m} \cap S_{\{x\}}$. On the other hand, if $x \notin \mathfrak{m}$, then it is invertible modulo $\mathfrak{m}$, and so there exists an $a \in A$ such that $1 - ax \in \mathfrak{m}$ (hence also $\mathfrak{m} \cap S_{\{x\}}$).

(b) *Let $\mathfrak{m}$ be a maximal ideal, and let $\mathfrak{p}$ be a prime ideal contained in $\mathfrak{m}$; for every $x \in \mathfrak{m} \smallsetminus \mathfrak{p}$,* we have $\mathfrak{p} \cap S_{\{x\}} = \emptyset$. Indeed, if $x^n(1 - ax) \in \mathfrak{p}$, then $1 - ax \in \mathfrak{p}$ (as $x \notin \mathfrak{p}$); hence $1 - ax \in \mathfrak{m}$, and so $1 \in \mathfrak{m}$, which is a contradiction.

Statement (a) shows that every chain of prime ideals beginning with a maximal ideal is shortened when passing from A to $A_{\{x\}}$, while statement (b) shows that a maximal (i.e., nonrefinable) chain of prime ideals of length n is shortened only to $n - 1$ when x is chosen appropriately. From this, the proposition follows. □

PROPOSITION 2.54. *Let A be an integral domain, and let k be a subfield of A. Then*

$$\dim(A) \leq \operatorname{tr\,deg}_k F(A),$$

where $F(A)$ is the field of fractions of A.

PROOF. If $\operatorname{tr\,deg}_k F(A) = \infty$, there is nothing to prove, and so we suppose that $\operatorname{tr\,deg}_k F(A) = n \in \mathbb{N}$. We argue by induction on n. We can replace k with its algebraic closure in A without changing $\operatorname{tr\,deg}_k F(A)$.

Let $x \in A$. If $x \notin k$, then it is transcendental over k, and so

$$\operatorname{tr\,deg}_{k(x)} F(A) = n - 1$$

by 1.64; since $k(x) \subset A_{\{x\}}$, this implies (by induction) that $\dim(A_{\{x\}}) \leq n - 1$. If $x \in k$, then $0 = 1 - x^{-1}x \in S_{\{x\}}$, and so $A_{\{x\}} = 0$; again $\dim(A_{\{x\}}) \leq n - 1$. We deduce from 2.53 that $\dim(A) \leq n$. □

COROLLARY 2.55. *The polynomial ring $k[X_1, \ldots, X_n]$ has Krull dimension n.*

PROOF. The existence of the sequence of prime ideals

$$(X_1, \ldots, X_n) \supset (X_1, \ldots, X_{n-1}) \supset \cdots \supset (X_1) \supset (0)$$

shows that $k[X_1, \ldots, X_n]$ has Krull dimension at least n, and 2.54 shows that it has Krull dimension at most n. □

COROLLARY 2.56. *Let A be an integral domain and let k be a subfield of A. If A is finitely generated as a k-algebra, then*

$$\operatorname{tr}\deg_k F(A) = \dim(A).$$

PROOF. According to the Noether normalization theorem (2.45), A is integral over a polynomial subring $k[x_1, \ldots, x_n]$. Hence $F(A)$ is algebraic over $k(x_1, \ldots, x_n)$, and so $n = \operatorname{tr}\deg_k F(A)$. The going up theorem (1.54), implies that a chain of prime ideals in $k[x_1, \ldots, x_n]$ lifts to a chain in A, and so $\dim(A) \geq \dim(k[x_1, \ldots, x_n]) = n$. Now 2.54 shows that $\dim(A) = n$. □

COROLLARY 2.57. *Let V be an irreducible algebraic set. Then V has dimension n if and only if there exists a finite surjective map $V \to \mathbb{A}^n$.*

PROOF. The d in Theorem 2.44 is the dimension of V. □

ASIDE 2.58. In linear algebra, we justify saying that a vector space 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. All we can say is Corollary 2.57.

ASIDE 2.59. The inequality in Proposition 2.54 may be strict. Let A and k be as in Corollary 2.56, so that $\dim A = \operatorname{tr}\deg_k F(A)$. When we replace A with $A_{\mathfrak{p}}$, where $\mathfrak{p}$ is a nonmaximal prime ideal, the Krull dimension will drop but the field of fractions will be unchanged.

NOTES. The short proof of 2.55 is based on that in Coquand and Lombardi, Amer. Math. Monthly 112 (2005), no. 9, 826–829.

Examples

EXAMPLE 2.60. Let $V = \mathbb{A}^n$. Then $k(V) = k(X_1, \ldots, X_n)$, which has transcendence basis $X_1, \ldots, X_n$ over k, and so $\dim(V) = n$.

EXAMPLE 2.61. If V is a linear subspace of k^n (or a translate of a linear subspace), then the dimension of V as an algebraic set 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.

More specifically, 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

$$k[X_1, \ldots, X_n]/\mathfrak{c} \simeq k[X_{i_1}, \ldots, X_{i_{n-r}}].$$

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

$$\begin{aligned} k[X_1, \ldots, X_n]/\mathfrak{c} &= k[\ell_1, \ldots, \ell_r, X_{i_1}, \ldots, X_{i_{n-r}}]/\mathfrak{c} \\ &\simeq k[X_{i_1}, \ldots, X_{i_{n-r}}]. \end{aligned}$$

EXAMPLE 2.62. If W is a proper algebraic subset of an irreducible algebraic set V, then $\dim(W) < \dim(V)$ (see 2.50).

EXAMPLE 2.63. A point in an algebraic set is a closed irreducible subset. Therefore an irreducible algebraic set has dimension 0 if and only if it consists of a single point.

EXAMPLE 2.64. A hypersurface in $\mathbb{A}^n$ has dimension $n-1$. It suffices to prove this for an irreducible hypersurface H. Such an H is the zero set of an irreducible polynomial f (see 2.29). Let

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

and let $k(x_1,\ldots,x_n)$ be the field of fractions of $k[x_1,\ldots,x_n]$. As f is not the zero polynomial, 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. (Alternatively, use 2.57.)

EXAMPLE 2.65. Let $F(X,Y)$ and $G(X,Y)$ be nonconstant polynomials with no common factor. Then each irreducible component of $V(F)$ has dimension 1 (by 2.64), and so $V(F)\cap V(G)$ has dimension 0 (by 2.62). Therefore, $V(F)\cap V(G)$ is a finite set.

PROPOSITION 2.66. *Let W be an algebraic subset of codimension 1 in an algebraic set V. If $k[V]$ is a unique factorization domain, then $I(W) = (f)$ for some $f \in k[V]$.*

PROOF. Let $W_1,\ldots,W_s$ be the irreducible components of W; then $I(W) = \bigcap I(W_i)$, and so, if we can prove $I(W_i) = (f_i)$, then $I(W) = (f_1 \cdots f_r)$. This allows us to assume that W is irreducible. Let $\mathfrak{p} = I(W)$; it is a prime ideal, and it is not zero because otherwise $\dim(W) = \dim(V)$. Therefore it contains an irreducible polynomial f. From (1.33) we know (f) is prime. If $(f) \neq \mathfrak{p}$, then we have

$$\mathfrak{p} \supset (f) \supset (0) \qquad \text{(distinct prime ideals)}$$

and hence

$$W = V(\mathfrak{p}) \subset V(f) \subset V \qquad \text{(distinct irreducible closed subsets).}$$

But then (2.62)

$$\dim(W) < \dim(V(f)) < \dim V,$$

which contradicts the hypothesis. □

COROLLARY 2.67. *The algebraic sets of codimension 1 in $\mathbb{A}^n$ are exactly the hypersurfaces.*

PROOF. Combine 2.64 and 2.66. □

EXAMPLE 2.68. We classify the irreducible algebraic sets V of $\mathbb{A}^2$. If V has dimension 2, then it equals $\mathbb{A}^2$ (by 2.62). If V has dimension 1, then $V = V(f)$, where f is any irreducible polynomial in $I(V)$ (see 2.66 and its proof). Finally, if V has dimension zero, then it is a point. Correspondingly, the following is a complete list of the prime ideals in $k[X,Y]$:

$$(0), \quad (f) \text{ with } f \text{ irreducible}, \quad (X-a, Y-b) \text{ with } a,b \in k.$$

Exercises

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

2-2. Identify k^{mn} with the set of $m \times n$ matrices, and let $r \in \mathbb{N}$. Show that the set of matrices with rank $\leq r$ is an algebraic subset of k^{mn}.

2-3. Let $V = \{(t, t^2, \ldots, t^n) \mid t \in k\}$. Show that V is an algebraic subset of k^n, and that $k[V] \approx k[T]$ (polynomial ring in one symbol). (Assume char(k) = 0.)

2-4. Let $f_1, \ldots, f_m \in \mathbb{Q}[X_1, \ldots, X_n]$. If the f_i have no common zero in $\mathbb{C}$, prove that there exist $g_1, \ldots, g_m \in \mathbb{Q}[X_1, \ldots, X_n]$ such that $f_1 g_1 + \cdots + f_m g_m = 1$. (Hint: linear algebra).

2-5. Let $k \subset K$ be algebraically closed fields, and let $\mathfrak{a}$ be an ideal in $k[X_1, \ldots, X_n]$. Show that if $f \in K[X_1, \ldots, X_n]$ vanishes on $V(\mathfrak{a})$, then it vanishes on $V_K(\mathfrak{a})$. Deduce that the zero set $V(\mathfrak{a})$ of $\mathfrak{a}$ in k^n is dense in the zero set $V_K(\mathfrak{a})$ of $\mathfrak{a}$ in K^n. [Hint: Choose a basis $(e_i)_{i \in I}$ for K as a k-vector space, and write $f = \sum e_i f_i$ (finite sum) with $f_i \in k[X_1, \ldots, X_n]$.]

2-6. 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 there exists a $\mathbb{C}$-algebra homomorphism $\mathbb{C} \otimes_{\mathbb{Q}} A \to \mathbb{C} \otimes_{\mathbb{Q}} B$, then there exists a $\mathbb{Q}^{\mathrm{al}}$-algebra homomorphism $\mathbb{Q}^{\mathrm{al}} \otimes_{\mathbb{Q}} A \to \mathbb{Q}^{\mathrm{al}} \otimes_{\mathbb{Q}} B$. (Hint: The proof takes only a few lines.)

2-7. Let A be finite dimensional k-algebra, where k is an infinite field, and let M and N be A-modules. Show that if $k^{\mathrm{al}} \otimes_k M$ and $k^{\mathrm{al}} \otimes_k N$ are isomorphic $k^{\mathrm{al}} \otimes_k A$-modules, then M and N are isomorphic A-modules.

2-8. Show that the subset $\{(z, e^z) \mid z \in \mathbb{C}\}$ is not an algebraic subset of $\mathbb{C}^2$.

Chapter 3

Affine Algebraic Varieties

In this chapter, we define the structure of a ringed space on an algebraic set. In this way, we are led to the notion of an affine algebraic variety — roughly speaking, this is an algebraic set with no preferred embedding into $\mathbb{A}^n$. This is in preparation for Chapter 5, 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.

a. Sheaves

Let k be a field (in sections a, b, and d, the field k need not be algebraically closed).

DEFINITION 3.1. Let V be a topological space, and suppose that, for every open subset U of V we have a set $\mathcal{O}_V(U)$ of functions $U \to k$. Then $U \rightsquigarrow \mathcal{O}_V(U)$ is a ***sheaf of** k-**algebras*** if, for every open subset U of V,

(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 $f+g$ and fg whenever it contains f and g.

(b) the restriction of an f in $\mathcal{O}_V(U)$ to any open subset U' of U is in $\mathcal{O}_V(U')$;

(c) a function $f : U \to k$ lies in $\mathcal{O}_V(U)$ if there exists an open covering $U = \bigcup_{i\in I} U_i$ of U such that $f|U_i$ lies in $\mathcal{O}_V(U_i)$ for all $i \in I$.

Let U be a union of open subsets U_i. If the U_i are disjoint, then (b) and (c) require that

$$\mathcal{O}_V(U) \simeq \prod_i \mathcal{O}_V(U_i).$$

In the general case, they require that

$$\mathcal{O}_V(U) \simeq \left\{(f_i) \in \prod_i \mathcal{O}_V(U_i) \;\middle|\; f_i|U_i \cap U_j = f_j|U_i \cap U_j \text{ for all } i,j\right\}.$$

Examples

3.2. Let V be a topological space, and, for an 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.

3.3. A function $f : U \to \mathbb{R}$ on an open subset U of $\mathbb{R}^n$ is said to be ***smooth*** (infinitely differentiable) if its partial derivatives of all orders exist and are continuous. This condition is ***local***, i.e., a function on U is smooth if and only if it is smooth on an open neighbourhood of each point of U. As constant functions and sums and products of smooth functions are smooth, for any open subset V of $\mathbb{R}^n$, the smooth functions on the open subsets of V form a sheaf of $\mathbb{R}$-algebras.

3.4. A function $f : U \to \mathbb{C}$ on an open subset U of $\mathbb{C}^n$, is said to be ***analytic*** if it is described by a convergent power series in a neighbourhood of each point of U. This condition is local, and so, for any open subset V of $\mathbb{C}^n$, the analytic functions on the open subsets of V form a sheaf of $\mathbb{C}$-algebras.

3.5. Let V be a topological space, and, for an open subset U of V, let $\mathcal{O}_V(U)$ be the set of all constant functions $U \to k$. If V is not connected, then $\mathcal{O}_V$ is *not* a sheaf: let U_1 and U_2 be disjoint open subsets of V, and let f be the function on $U_1 \cup U_2$ that takes the constant value 0 on U_1 and the constant value 1 on U_2; then f is not in $\mathcal{O}_V(U_1 \cup U_2)$, and so condition (3.1c) fails. When "constant" is replaced with "locally constant", $\mathcal{O}_V$ becomes a sheaf of k-algebras (in fact, the smallest such sheaf).

3.6. Let V be a topological space, and, for an open subset U of V, let $\mathcal{O}_V(U)$ be the set of *all* functions $U \to k$. Then $\mathcal{O}_V$ is a sheaf of k-algebras. All our sheaves of k-algebras are subsheaves of this one.

b. Ringed spaces

A pair $(V, \mathcal{O}_V)$ comprising a topological space V and a sheaf of k-algebras on V will be called a k-***ringed space*** (or just a ***ringed space*** when the k is understood). For historical reasons, we sometimes write $\Gamma(U, \mathcal{O}_V)$ for $\mathcal{O}_V(U)$ and call its elements the ***sections*** of $\mathcal{O}_V$ over U.

Let $(V, \mathcal{O}_V)$ be a k-ringed space. For any open subset U of V, the restriction of $\mathcal{O}_V$ to the collection of open subsets of U is a sheaf of k-algebras on U.

Let $(V, \mathcal{O}_V)$ be a k-ringed space, and let $P \in V$. A ***germ*** of a function at P is an equivalence class of pairs (U, f) with U an open neighbourhood of P and $f \in \mathcal{O}_V(U)$; two pairs (U, f) and (U', f') are equivalent if the functions f and f' agree on some open neighbourhood of P in $U \cap U'$. The germs of functions at P form a k-algebra $\mathcal{O}_{V,P}$, called the ***stalk*** of $\mathcal{O}_V$ at P. In other words, $\mathcal{O}_{V,P}$ is the direct limit,

$$\mathcal{O}_{V,P} = \varinjlim \mathcal{O}_V(U),$$

over the open neighbourhoods U of P. In the interesting cases, $\mathcal{O}_{V,P}$ is a local ring with maximal ideal the set $\mathfrak{m}_P$ of germs zero at P. We often write $\mathcal{O}_P$ for $\mathcal{O}_{V,P}$.

EXAMPLE 3.7. Let $\mathcal{O}_V$ be the sheaf of analytic 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 said to be ***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 stalk $\mathcal{O}_{V,c}$ of $\mathcal{O}_V$ at c.

To prove this, let f be a analytic 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, II, 6). Another analytic function f' on a neighbourhood U' of c has the same power series expansion if and only if f 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 analytic functions at c to the ring of convergent power series, which is obviously surjective.

c. The ringed space structure on an algebraic set

Let V be an algebraic subset of k^n. Recall that the basic open subsets of V are those of the form

$$D(h) \stackrel{\text{def}}{=} \{Q \mid h(Q) \neq 0\}, \quad h \in k[V].$$

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

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

We say that a function is regular if it is locally of this form.

DEFINITION 3.8. Let U be an open subset of V. A function $f : U \to k$ is ***regular*** at $P \in U$ if there exist $g, h \in k[V]$ with $h(P) \neq 0$ such that $f(Q) = g(Q)/h(Q)$ for all Q in some neighbourhood of P. A function $f : U \to k$ is ***regular*** if it is regular at every $P \in U$.

Let $\mathcal{O}_V(U)$ denote the set of regular functions on an open subset U of V.

PROPOSITION 3.9. *The map $U \rightsquigarrow \mathcal{O}_V(U)$ is a sheaf of k-algebras on V.*

PROOF. The condition to be regular is local, and so we only have to check 3.1(a). Clearly, a constant function is regular. Suppose that 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 on a neighbourhood U' of P. Then $f + f'$ agrees with $\frac{gh' + g'h}{hh'}$ on U', and so $f + f'$ is regular at P. Similarly, ff' agrees with $\frac{gg'}{hh'}$ on U', and so is regular at P. □

LEMMA 3.10. *Let $g, h \in k[V]$ with $h \neq 0$. The function*

$$P \mapsto g(P)/h(P)^m : D(h) \to k$$

is zero if and only if and only if $gh = 0$ in $k[V]$.

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 $P \in D(h)$. □

Let $k[V]_h$ denote the ring $k[V]$ with h inverted (1.11). The lemma shows that the map

$$\frac{g}{h^m} \mapsto \left(P \mapsto \frac{g(P)}{h(P)^m}\right) : k[V]_h \to \mathcal{O}_V(D(h)),$$

is well-defined and injective.

PROPOSITION 3.11. *The map $k[V]_h \to \mathcal{O}_V(D(h))$ is an isomorphism of k-algebras.*

PROOF. It remains to show that every regular function f on $D(h)$ arises from an element of $k[V]_h$. By definition, there exists an open covering $D(h) = \bigcup V_i$ of $D(h)$ 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 p. 49). 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 quasi-compact, we can assume that the covering is finite. As $\frac{g_i}{h_i} = \frac{g_j}{h_j}$ on $D(h_i) \cap D(h_j) = D(h_i h_j)$,

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

— this follows from Lemma 3.10 if $h_i h_j \neq 0$ and is obvious otherwise. Because $D(h) = \bigcup D(h_i) = \bigcup D(h_i^2)$,

$$V((h)) = V((h_1^2, \ldots, h_m^2)),$$

and so h lies 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 $k[V]$:

$$h_j^2 \sum_{i=1}^m a_i g_i h_i \overset{(*)}{=} \sum_{i=1}^m a_i g_j h_i^2 h_j \overset{(**)}{=} g_j h_j h^N.$$

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 $\sum a_i g_i h_i$. □

On taking $h = 1$ in the proposition, we see that the definition of a regular function on V in this section agrees with that in Section 2i.

COROLLARY 3.12. *For any $P \in V$, $\mathcal{O}_P \simeq k[V]_{\mathfrak{m}_P}$, where $\mathfrak{m}_P$ is the maximal ideal $I(P)$.*

PROOF. 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,

$$\mathcal{O}_P \simeq \varinjlim_{h(P)\neq 0} \mathcal{O}_V(D(h)) \overset{3.11}{\simeq} \varinjlim_{h \notin \mathfrak{m}_P} k[V]_h \overset{1.23}{\simeq} k[V]_{\mathfrak{m}_P}.$$

□

Notes

3.13. Let V be an algebraic set and let P be a point on V. Proposition 1.14 says that there is a canonical 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 irreducible closed subsets of V passing through P and the prime ideals in $\mathcal{O}_P$. The irreducible components of V passing through P correspond to the minimal prime ideals in $\mathcal{O}_P$. The ideal $\mathfrak{p}$ corresponding to an irreducible closed subset Z consists of the elements of $\mathcal{O}_P$ that can be represented by a pair (U, f) with $f|_{Z\cap U} = 0$.

3.14. If P lies on a single irreducible component of V, then $\mathcal{O}_{V,P}$ is an integral domain. As $\mathcal{O}_{V,P}$ depends only on $(U, \mathcal{O}_V|U)$ for U an open neighbourhood of P, in proving this, we may suppose that V itself is irreducible, in which case the statement follows from 3.12. On the other hand, if P lies on more than one irreducible component of V, then $\mathcal{O}_P$ contains more than one minimal prime ideal (by 3.13), and so (0) is not prime.

3.15. Let V be an algebraic subset of k^n, and let $A = k[V]$. Propositions 2.37 and 3.11 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.
- For $f \in A_h$ and $\mathfrak{m} \in D(h)$, let $f(\mathfrak{m})$ denote the image of f in $A_h/\mathfrak{m}A_h \simeq k$; this identifies A_h with a k-algebra of functions $D(h) \to k$, and $\mathcal{O}_V$ is the unique sheaf of k-valued functions such that $\Gamma(D(h), \mathcal{O}_V) = A_h$ for all $h \in A$.

3.16. When V is irreducible, all the rings attached to it can be identified with subrings of its function field $k(V)$. For example,

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

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.[1]

Examples

3.17. The ring of regular functions on $\mathbb{A}^n$ is $k[X_1, \ldots, X_n]$. For a nonzero polynomial $h(X_1, \ldots, X_n)$, the ring of regular functions on $D(h)$ is

$$\left\{\frac{g}{h^N} \in k(X_1, \ldots, X_n) \;\middle|\; g \in k[X_1, \ldots, X_n],\quad N \in \mathbb{N}\right\}.$$

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

For a point $P = (a_1, \dots, a_n)$, the local ring at P is

$$\begin{aligned}\mathcal{O}_P &= \left\{ \frac{g}{h} \in k(X_1, \dots, X_n) \;\middle|\; h(P) \neq 0 \right\} \\ &= k[X_1, \dots, X_n]_{(X_1 - a_1, \dots, X_n - a_n)},\end{aligned}$$

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

3.18. Let $U = \mathbb{A}^2 \smallsetminus \{(0,0)\}$. It is an open subset of $\mathbb{A}^2$, but it is not a basic open subset because its complement $\{(0,0)\}$ has dimension 0, and so is not of the form $V((f))$ (see 2.64). Since $U = D(X) \cup D(Y)$, the ring of regular functions on U is

$$\Gamma(U, \mathcal{O}_{\mathbb{A}^2}) = k[X,Y]_X \cap k[X,Y]_Y$$

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

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

We may assume that $X \nmid g$ 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 does not divide the left hand side, it cannot divide the right hand side either, and so $N = 0$. Similarly, $M = 0$, and so $f \in k[X,Y]$. We have shown that every regular function on U extends uniquely to a regular function on $\mathbb{A}^2$:

$$\Gamma(U, \mathcal{O}_{\mathbb{A}^2}) = k[X,Y] = \Gamma(\mathbb{A}^2, \mathcal{O}_{\mathbb{A}^2}).$$

d. Morphisms of ringed spaces

Let $(V, \mathcal{O}_V)$ and $(W, \mathcal{O}_W)$ be k-ringed spaces. A continuous map $\varphi\colon V \to W$ is a ***morphism of k-ringed spaces*** if

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

for all open subsets U of W. If $\varphi\colon V \to W$ is a morphism of k-ringed spaces and U' and U are open subsets of V and W such that $\varphi(U') \subset U$, then

$$f \mapsto f \circ \varphi\colon \mathcal{O}_W(U) \to \mathcal{O}_V(U'),$$

is a homomorphism of k-algebras, and these homomorphisms are compatible with restriction to smaller open subsets.

For example, when $(V, \mathcal{O}_V)$ is a k-ringed space and U is an open subset of V, the inclusion $U \hookrightarrow V$ is a morphism of k-ringed spaces $(U, \mathcal{O}_V|U) \to (V, \mathcal{O}_V)$.

A morphism of ringed spaces maps germs of functions to germs of functions. More precisely, a morphism $\varphi\colon (V, \mathcal{O}_V) \to (W, \mathcal{O}_W)$ induces a k-algebra homomorphism

$$\mathcal{O}_{W,\varphi(P)} \to \mathcal{O}_{V,P}$$

for each $P \in V$, which sends the germ represented by (U, f) to the germ represented by $(\varphi^{-1}(U), f \circ \varphi)$. In the interesting cases, $\mathcal{O}_{V,P}$ is a local ring with maximal ideal $\mathfrak{m}_P$ consisting of the germs represented by pairs (U, f) with $f(P) = 0$. Then $\mathcal{O}_{W,\varphi(P)} \to \mathcal{O}_{V,P}$ maps $\mathfrak{m}_{\varphi(P)}$ into $\mathfrak{m}_P$, i.e., it is a local homomorphism of local rings.

Examples

3.19. Let V and W be topological spaces endowed with their sheaves $\mathcal{O}_V$ and $\mathcal{O}_W$ of continuous real valued functions (3.2). As composites of continuous maps are continuous, every continous map $V \to W$ is a morphism of $\mathbb{R}$-ringed spaces $(V, \mathcal{O}_V) \to (W, \mathcal{O}_W)$.

3.20. Let V and W be open subsets of $\mathbb{R}^n$ and $\mathbb{R}^m$ respectively, and let x_i be the coordinate function $(a_1, \dots, a_m) \mapsto a_i : W \to \mathbb{R}$. Recall from advanced calculus that a map

$$\varphi : V \to W \subset \mathbb{R}^m$$

is said to be smooth if each of its component functions $\varphi_i \stackrel{\text{def}}{=} x_i \circ \varphi : V \to \mathbb{R}$ is smooth. Endow V and W with their sheaves of smooth functions (3.3), and let $\varphi : V \to W$ be a continuous map. If φ is smooth, then $f \circ \varphi$ is smooth for every smooth function f on an open subset of W, and so φ is a morphism of $\mathbb{R}$-ringed spaces. Conversely, if φ is a morphism of $\mathbb{R}$-ringed spaces, then, in particular, the component functions $x_i \circ \varphi$ are smooth, and so φ is smooth.

3.21. Same as 3.20, but replace $\mathbb{R}$ with $\mathbb{C}$ and "smooth" with "analytic". A continuous map $\varphi : V \to W$ is analytic if and only if it is a morphism of $\mathbb{C}$-ringed spaces.

e. Affine algebraic varieties

We have just seen that every algebraic set $V \subset k^n$ has the structure of a k-ringed space $(V, \mathcal{O}_V)$. A k-ringed space isomorphic to one of this form is called an ***affine algebraic variety over*** k. We often shorten $(V, \mathcal{O}_V)$ to V.

Let $(V, \mathcal{O}_V)$ and $(W, \mathcal{O}_W)$ be affine algebraic varieties. A map $\varphi : V \to W$ is ***regular*** (or a ***morphism of affine algebraic varieties***) if it is a morphism of k-ringed spaces. With these definitions, the affine algebraic varieties become a category. We usually shorten "affine algebraic variety" to "affine variety".

In particular, the regular functions define the structure of an affine variety on every algebraic set. We now regard $\mathbb{A}^n$ as an affine algebraic variety. The affine varieties we have constructed so far have all been embedded in $\mathbb{A}^n$. We now explain how to construct affine varieties with no preferred embedding.

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

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

is a radical ideal. Therefore 2.18 implies that the intersection of the maximal ideals in A is 0. Moreover, 2.12 implies that, for every 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., $f(\mathfrak{m}) = f \pmod{\mathfrak{m}}$. This allows us to identify elements of A with functions $\{\text{maximal ideals in } A\} \to k$.

We attach a ringed space $(V, \mathcal{O}_V)$ to A by letting

$$V = \{\text{maximal ideals in } A\}.$$

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 $g, h \in A$, $h \neq 0$, defines a function

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

For U an open subset of V, we define $\mathcal{O}_V(U)$ to be the set of functions $f \colon U \to k$ that are of this form in some neighbourhood of each point of U.

PROPOSITION 3.22. *The pair $(V, \mathcal{O}_V)$ is an affine algebraic variety with $\Gamma(D(h), \mathcal{O}_V) \simeq A_h$ for each $h \in A \smallsetminus \{0\}$.*

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 k-ringed space attached to the algebraic set $V(\mathfrak{a})$ (see 3.15). □

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

ASIDE 3.23. We have shown that we can recover an algebraic set from its ring of regular functions as the set of maximal ideals in the ring (equipped with the Zariski topology). 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 80 years.

> Gel'fand and Kolmogorov (1939) prove that if S_1 and S_2 are completely regular spaces, and if their rings of real-valued continuous functions are algebraically isomorphic as rings, then S_1 and S_2 are homeomorphic. The proof begins by showing that there is a one-to-one correspondence between the maximal ideals in the ring of functions and the points in the underlying space. The space is recovered by introducing a suitable topology on the set of maximal ideals.

Allen Shields, Banach Algebras, 1939–1989, Math. Intelligencer, Vol 11, no. 3, p15.

f. The category of affine algebraic varieties

For each affine k-algebra A, we have an affine variety $\text{Spm}(A)$, and for each affine variety $(V, \mathcal{O}_V)$, we have an affine k-algebra $k[V] \stackrel{\text{def}}{=} \mathcal{O}_V(V)$. We make this correspondence into an anti-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

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

If $\mathfrak{n}$ is a maximal ideal in B, then $\mathfrak{m} \stackrel{\text{def}}{=} \alpha^{-1}(\mathfrak{n})$ is a maximal ideal 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

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

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 by $f(\mathfrak{m})$. The commutativity of the diagram means that, for $f \in A$,

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

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

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 proved the following proposition.

PROPOSITION 3.24. *For all affine algebras A and B,*

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

for all affine varieties V and W,

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

In terms of categories, Proposition 3.24 says the following.

PROPOSITION 3.25. *The functor $A \rightsquigarrow \mathrm{Spm}\, A$ is a contravariant equivalence from the category of affine k-algebras to the category of affine algebraic varieties over k, with quasi-inverse $(V, \mathcal{O}_V) \rightsquigarrow \mathcal{O}_V(V)$.*

g. Explicit description of morphisms of affine varieties

PROPOSITION 3.26. *Let $V \subset k^m$ and $W \subset k^n$ be algebraic subsets. The following conditions on a map $\varphi\colon V \to W$ are equivalent:*

(a) *φ is a morphism of ringed spaces $(V, \mathcal{O}_V) \to (W, \mathcal{O}_W)$;*

(b) *the components $\varphi_1, \ldots, \varphi_m$ of φ are regular functions on V;*

(c) *$f \in k[W] \Rightarrow f \circ \varphi \in k[V]$.*

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

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

Hence this implication follows directly from the definition of a regular map (2.38).

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

(c) $\Rightarrow$ (a). The map $f \mapsto f \circ \varphi$ is a homomorphism $\alpha\colon k[W] \to k[V]$. It therefore defines a map $\operatorname{spm}(k[V]) \to \operatorname{spm}(k[W])$, 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. □

The equivalence of (a) and (b) means that $\varphi\colon V \to W$ is a regular map of algebraic sets in the sense of Chapter 2 if and only if it is a regular map of the associated affine algebraic varieties.

Consider equations

$$Y_1 = f_1(X_1, \ldots, X_m)$$
$$\cdots$$
$$Y_n = f_n(X_1, \ldots, X_m).$$

On the one hand, they define a regular map $\varphi\colon \mathbb{A}^m \to \mathbb{A}^n$, 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 $\alpha\colon k[Y_1, \ldots, Y_n] \to k[X_1, \ldots, X_m]$ of k-algebras, namely, that sending Y_i to $f_i(X_1, \ldots, X_m)$. 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 $V(\mathfrak{a}) \subset \mathbb{A}^m$ and $V(\mathfrak{b}) \subset \mathbb{A}^n$ 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 $Q \in V(\mathfrak{a})$,

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

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

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

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

We have shown that the regular maps

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

are all of the form

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

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

Examples of regular maps

3.27. Let R be a k-algebra. To give a k-algebra homomorphism $k[X] \to R$ is the same as giving an element of R (the image of X under the homomorphism):

$$\mathrm{Hom}_{k\text{-algebra}}(k[X], R) \simeq R.$$

Therefore

$$\mathrm{Mor}(V, \mathbb{A}^1) \overset{3.24}{\simeq} \mathrm{Hom}_{k\text{-algebra}}(k[X], k[V]) \simeq k[V].$$

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

3.28. Let $\mathbb{A}^0 = \mathrm{Spm}\, k$. Then $\mathbb{A}^0$ consists of a single point and $\Gamma(\mathbb{A}^0, \mathcal{O}_{\mathbb{A}^0}) = k$. The regular maps $\mathbb{A}^0 \to V$, where V is an affine variety, are just the maps of sets, so $\mathrm{Mor}(\mathbb{A}^0, V) \simeq V$. Alternatively,

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

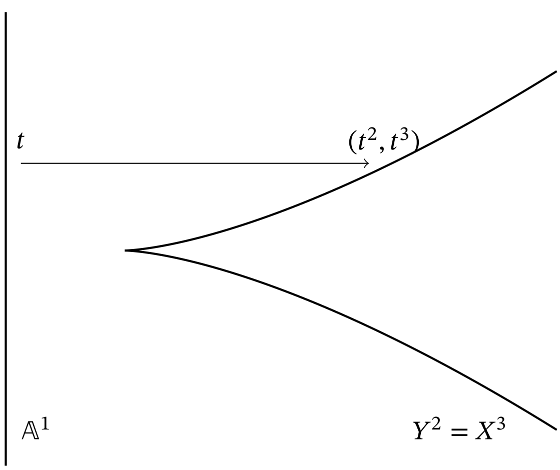
where the second map sends $\alpha\colon k[V] \to k$ to the point corresponding to the maximal ideal $\mathrm{Ker}(\alpha)$.

3.29. Let k be of characteristic $\neq 2$.

(a) The regular map $t \mapsto (t^2, t^3)\colon \mathbb{A}^1 \to \mathbb{A}^2$ is bijective onto its image,

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

but it is not an isomorphism onto its image because the inverse map is not regular. In view of 3.25, to prove this it suffices to show that $t \mapsto (t^2, t^3)$ does not 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

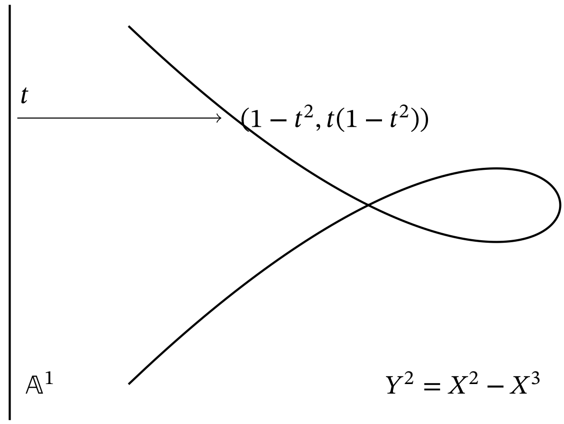
$$x \mapsto T^2, \quad y \mapsto T^3, \quad k[x,y] \to k[T],$$

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 $k(x,y) \hookrightarrow k(T)$).

(b) The regular map $t \mapsto (1-t^2, t(1-t^2))\colon \mathbb{A}^1 \to \mathbb{A}^2$ is bijective onto its image,

$$V\colon Y^2 = X^2 - X^3$$

except that both ± 1 map to $(0,0)$.



3.30. Let $\mathrm{char}(k) = p \neq 0$. The regular map

$$(a_1, \ldots, a_n) \mapsto (a_1^p, \ldots, a_n^p)\colon \mathbb{A}^n \to \mathbb{A}^n$$

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.*** Let k be the algebraic closure of $\mathbb{F}_p$, and write F for the map. 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, 4.23). 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,

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

If $f(a_1, \ldots, a_n) = 0$, 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 $\mathbb{F}_{p^m}$.

ASIDE 3.31. 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 $\mathbb{F}_{p^m}$ 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 article *The Riemann hypothesis over finite fields: from Weil to the present day* and my notes *Lectures on Étale Cohomology*.

h. Subvarieties

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

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

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

Now let $\mathfrak{a}$ be a radical ideal in A, so that $A/\mathfrak{a}$ is again an affine k-algebra. 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.

PROPOSITION 3.32. *Let $(V, \mathcal{O}_V)$ be an affine variety and let h be a nonzero element of $k[V]$. Then*

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

PROOF. The map $A \to A_h$ defines a morphism $\operatorname{spm}(A_h) \to \operatorname{spm}(A)$, and induces an isomorphism

$$\operatorname{Spm}(A_h) \xrightarrow{\simeq} ((D(h), \mathcal{O}_V|D(h)) \subset \operatorname{Spm}(A).$$

□

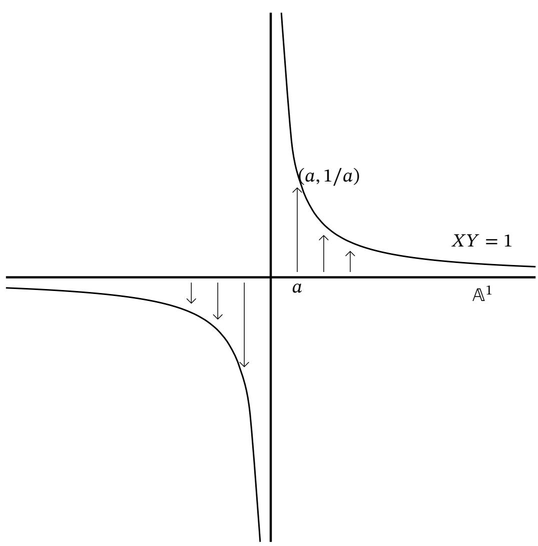
In particular, $(D(h), \mathcal{O}_V|D(h))$ is an affine variety. If V is a closed subvariety of $\mathbb{A}^n$, say, $V = V(\mathfrak{a}) \subset \mathbb{A}^n$, then

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

defines an isomorphism of $D(h)$ onto $V(\mathfrak{a}, 1 - hX_{n+1})$, thereby realizing $D(h)$ as a closed subvariety of $\mathbb{A}^{n+1}$. For example,

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

is an isomorphism from $D(X) = \mathbb{A}^1 \smallsetminus \{0\} \subset \mathbb{A}^1$ onto the curve $XY = 1$ in $\mathbb{A}^2$,



By an ***open affine (subset)*** U of an affine algebraic variety V, we mean an open subset U such that $(U, \mathcal{O}_V|U)$ is an affine algebraic variety. The proposition says that, for all nonzero $h \in \Gamma(V, \mathcal{O}_V)$, the open subset of V, where h is nonzero is an open affine. An open affine subset of an irreducible affine algebraic variety V is irreducible with the same dimension as V (2.52).

REMARK 3.33. 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 of V. For an open affine subset U, the natural map $U \to \operatorname{spm} \Gamma(U, \mathcal{O}_V)$ is a bijection. However, for

$$U \overset{\text{def}}{=} \mathbb{A}^2 \smallsetminus \{(0,0)\} = D(X) \cup D(Y) \subset \mathbb{A}^2,$$

we know that $\Gamma(U, \mathcal{O}_{\mathbb{A}^2}) = k[X,Y]$ (see 3.18), but $U \to \operatorname{spm} k[X,Y]$ is not a bijection, because the ideal (X,Y) is not in the image. Clearly $(U, \mathcal{O}_{\mathbb{A}^2}|U)$ is a union of affine algebraic varieties, and in Chapter 5 we shall recognize it as a (nonaffine) algebraic variety.

i. Properties of the regular map Spm(α)

PROPOSITION 3.34. *Let $\alpha\colon A \to B$ be a homomorphism of affine k-algebras, and let*

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

be the corresponding morphism of affine varieties.

(a) *The image of φ is dense for the Zariski topology if and only if α is injective.*

(b) *The morphism φ is an isomorphism from* Spm(B) *onto a closed subvariety of* Spm(A) *if and only if α is surjective.*

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

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

On the other hand, if the image of φ is not dense, then the closure of its image is a proper closed subset of Spm(A), and so there is a nonzero function $f \in A$ that is zero on it. Then $f \circ \varphi = 0$. (See 2.40.)

(b) If α is surjective, then it defines an isomorphism $A/\mathfrak{a} \to B$, where $\mathfrak{a}$ is the kernel of α. This induces an isomorphism of Spm(B) with its image in Spm(A). The converse follows from the description of the closed subvarieties of Spm(A) in the last section. □

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

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

A regular map $\varphi\colon V \to W$ of affine algebraic varieties is said to be a ***closed immersion*** if it is an isomorphism of V onto a closed subvariety of W. The proposition then says that

$$\varphi\colon V \to W \text{ is a closed immersion} \iff \Gamma(W, \mathcal{O}_W) \xrightarrow{f \mapsto f\circ\varphi} \Gamma(V, \mathcal{O}_V) \text{ is surjective.}$$

j. 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 a 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. The ***tensor algebra*** of V is

$$T^*V \stackrel{\text{def}}{=} \bigoplus_{i \geq 0} V^{\otimes i} = k \oplus V \oplus (V \otimes V) \oplus (V \otimes V \otimes V) \oplus \cdots$$

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 a noncommutative k-algebra, and the choice of a basis $e_1, \ldots, e_n$ for V defines an isomorphism

$$e_1 \cdots e_i \mapsto e_1 \otimes \cdots \otimes e_i : k\{e_1, \ldots, e_n\} \to T^*(V)$$

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 elements

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

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

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

to $S^*(V)$ from the commutative polynomial ring in the symbols $e_1, \ldots, e_n$. This shows that $S^*(V)$ is an affine k-algebra. The pair $(S^*(V), i)$ comprising $S^*(V)$ and the natural k-linear map $i : V \to S^*(V)$ has the following universal property: every k-linear map $V \to A$ from V into a k-algebra A extends uniquely to a k-algebra homomorphism $S^*(V) \to A$:

$$\begin{array}{ccc} V & \xrightarrow{\ i\ } & S^*(V) \\ & {}_{k\text{-linear}}\searrow & \Big\downarrow{\scriptstyle \exists!\ k\text{-algebra}} \\ & & A. \end{array} \tag{17}$$

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

We now define $\mathbb{A}(E)$ to be $\operatorname{Spm}(S^*(E^\vee))$, where $E^\vee$ is the dual vector space. For an affine k-algebra A,

$$\begin{aligned} \operatorname{Mor}(\operatorname{Spm}(A), \mathbb{A}(E)) &\simeq \operatorname{Hom}_{k\text{-algebra}}(S^*(E^\vee), A) && (3.24) \\ &\simeq \operatorname{Hom}_{k\text{-linear}}(E^\vee, A) && (17) \\ &\simeq E \otimes_k A && \text{(linear algebra).} \end{aligned}$$

In particular,

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

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

$$e \mapsto (f_1(e), \dots, f_n(e)) \colon E \to k^n.$$

k. Birational equivalence

Recall that if V is irreducible, then $k[V]$ is an integral domain, and we let $k(V)$ denote its field of fractions. If U is an open affine subvariety of V, then $k[V] \subset k[U] \subset k(V)$, and so $k(V)$ is also the field of fractions of $k[U]$.

DEFINITION 3.35. Two irreducible affine algebraic varieties over k are ***birationally equivalent*** if their function fields are isomorphic over k.

PROPOSITION 3.36. *Two irreducible affine varieties V and W are birationally equivalent if and only if there exist open affine subvarieties U_V and U_W of V and W such that $U_V \approx U_W$.*

PROOF. Let V and W be birationally equivalent irreducible affine varieties, and let $A = k[V]$ and $B = k[W]$. We use the isomorphism to identify $k(V)$ and $k(W)$. This allows us to suppose that A and B have a common field of fractions K. Let $x_1, \dots, x_n$ generate B as k-algebra. As K is the field of fractions of A, there exists a $d \in A$ such that $dx_i \in A$ for all i; then $B \subset A_d$. The same argument shows that there exists an $e \in B$ such that $A_d \subset B_e$. Now

$$B \subset A_d \subset B_e \implies B_e \subset A_{de} \subset (B_e)_e = B_e,$$

and so $A_{de} = B_e$. This shows that the open subvarieties $D(de) \subset V$ and $D(e) \subset W$ are isomorphic. We have proved the "only if" part, and the "if" part is obvious. □

THEOREM 3.37. *Every irreducible affine 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 Proposition 3.38 below, there exist rational functions $x_1, \dots, x_{d+1}$ on V such that $k(V) = k(x_1, \dots, x_d, x_{d+1})$. Let $f \in k[X_1, \dots, X_{d+1}]$ be an irreducible polynomial satisfied by the x_i, and let H be the hypersurface $f = 0$. Then $k(V) \approx k(H)$ and so V and H are birationally equivalent. □

We review some definitions from FT, Chapter 2. Let F be a field. A polynomial $f \in F[X]$ is ***separable*** if it is nonzero and has no multiple roots. Equivalent condition: $\gcd(f, \frac{df}{dX}) = 1$. When f is irreducible, this just says that $\frac{df}{dX} \neq 0$ because $\deg \frac{df}{dX} < \deg f$. An element of an algebraic extension E of F is ***separable*** over F if its minimal polynomial over F is separable, and E is ***separable*** over F if all its elements are separable over F.

PROPOSITION 3.38. *Let F be a perfect field and E a finitely generated field extension of F of transcendence degree d.*

(a) *If $E = F(x_1, \dots, x_{d+1})$, then, after the x_i have been renumbered, $\{x_1, \dots, x_d\}$ will be a transcendence basis for E over F and x_{d+1} will be separable over $F(x_1, \dots, x_d)$.*

(b) *There exist* $x_1, \dots, x_{d+1} \in E$ *such that* $E = F(x_1, \dots, x_{d+1})$.

PROOF. First observe that, if F has characteristic $p \neq 0$, then, because F is perfect, every polynomial in $X_1^p, \dots, X_n^p$ with coefficients in F is a pth power in $F[X_1, \dots, X_n]$:

$$\sum a_{i_1 \cdots i_n} X_1^{i_1 p} \dots X_n^{i_n p} = \left(\sum a_{i_1 \cdots i_n}^{1/p} X_1^{i_1} \dots X_n^{i_n} \right)^p. \quad (18)$$

(a) Suppose $E = F(x_1, \dots, x_{d+1})$. Then $f(x_1, \dots, x_{d+1}) = 0$ for some nonzero $f \in F[X_1, \dots, X_{d+1}]$, which we may take to be irreducible. If all the polynomials $\partial f / \partial X_i$ are zero, then F has characteristic $p \neq 0$ and f is a polynomial in $X_1^p, \dots, X_{d+1}^p$, and hence not irreducble. Thus some polynomial $\partial f / \partial X_i$, which (after renumbering) we may suppose to be $\partial f / \partial X_{d+1}$, is not zero. Now x_{d+1} is separable over $F(x_1, \dots, x_d)$.

(b) Let $\{x_1, \dots, x_n\}$ be a generating set for E over F with n minimal. We assume that $n > d+1$ and obtain a contradiction. After renumbering, we may suppose that $\{x_1, \dots, x_d\}$ is a transcendence basis for E over F (1.63). On applying (a) to $F(x_1, \dots, x_{d+1})$, we see that we may also suppose that x_{d+1} is separable over $F(x_1, \dots, x_d)$. As x_{d+2} is algebraic over $F(x_1, \dots, x_d)$, the primitive element theorem (FT, 5.1), shows that $F(x_1, \dots, x_{d+2}) = F(x_1, \dots, x_d, y)$ for some $y \in E$. Now $E = F(x_1, \dots, x_d, y, x_{d+3}, \dots, x_n)$, contradicting the minimality of n. □

In particular, there exists a separating transcendence basis for E/F if E is finitely generated of finite transcendence degree over F and F is perfect.

l. Dimension

DEFINITION 3.39. The ***dimension*** of an affine algebraic variety is the dimension of the underlying topological space (2.48).

Thus, the dimension of an affine variety V is the maximum length of a chain

$$V_0 \supset V_1 \supset \cdots \supset V_d$$

of distinct closed irreducible subvarieties. Later in this section, we shall see that it is the length of *every maximal* chain of closed irreducible subvarieties.

DEFINITION 3.40. A regular map $\varphi : W \to V$ of affine algebraic varieties is ***finite*** if the homomorphism $\varphi^* : k[V] \to k[W]$ makes $k[W]$ a finite $k[V]$-algebra.

THEOREM 3.41. *Let V be an affine algebraic variety of dimension n. Then there exists a finite map $V \to \mathbb{A}^n$.*

PROOF. This is a geometric restatement of the Noether normalization theorem (2.45). □

QUESTION. Let A be a finitely generated k-algebra. Assume that A is an integral domain, and let d be the transcendence degree of its field of fractions F. Does there exist a transcendence basis $\{x_1, \dots, x_d\}$ for F over k such that

(a) A is finite over $k[x_1, \dots, x_d]$, and

(b) F is separable over $k(x_1, \dots, x_d)$.

According 2.45 and 3.38 there exist transcendence bases satisfying (a) or (b). Does there always exist one satisfying both?

THEOREM 3.42. *Let V be an irreducible affine algebraic variety and f a nonzero regular function on V. If f has a zero in V, then its zero set is of pure codimension* 1.

PROOF. Let $d = \dim(V)$. When $V = \mathbb{A}^d$, we proved this in 2.64, and an argument of Tate allows us to deduce the general case from the Noether normalization theorem.

Let $Z_1, \ldots, Z_n$ be the irreducible components of $V(f)$. We have to show that $\dim Z_i = \dim V - 1$ for each i. There exists a point $P \in Z_i$ not contained in any other Z_j. As the Z_j are closed, there exists an open affine neighbourhood U of P in V not intersecting any Z_j with $j \neq i$. Then $Z_i \cap U$ is irreducible, and it is the zero set of the regular function $f|U$. We may replace V and f with U and $f|U$, and so assume that $V(f)$ is irreducible.

As $V(f)$ is irreducible, the radical of (f) is a prime ideal $\mathfrak{p}$ in $k[V]$. According to Theorem 2.45, there exists an inclusion $k[\mathbb{A}^d] \hookrightarrow k[V]$ realizing $k[V]$ as a finite $k[\mathbb{A}^d]$-algebra. The norm

$$f_0 \overset{\text{def}}{=} \mathrm{Nm}_{k(V)/k(\mathbb{A}^d)} f$$

of f lies in $k[\mathbb{A}^d]$ and f divides f_0 in $k[V]$ (by 1.45). Hence $f_0 \in (f) \subset \mathfrak{p}$, and so $\mathrm{rad}(f_0) \subset \mathfrak{p} \cap k[\mathbb{A}^d]$. We claim that, in fact,

$$\mathrm{rad}(f_0) = \mathfrak{p} \cap k[\mathbb{A}^d].$$

Let $g \in \mathfrak{p} \cap k[\mathbb{A}^d]$. Then $g \in \mathfrak{p} \overset{\text{def}}{=} \mathrm{rad}(f)$, and so $g^m = fh$ for some $h \in k[V]$, $m \in \mathbb{N}$. Taking norms, we find that

$$g^{me} = \mathrm{Nm}(fh) = f_0 \cdot \mathrm{Nm}(h) \in (f_0), \qquad e = [k(V) : k(\mathbb{A}^n)],$$

and so $g \in \mathrm{rad}(f_0)$, as claimed.

The inclusion $k[\mathbb{A}^d] \hookrightarrow k[V]$ therefore induces an inclusion

$$k[\mathbb{A}^d]/\operatorname{rad}(f_0) \hookrightarrow k[V]/\mathfrak{p}.$$

This makes $k[V]/\mathfrak{p}$ into a finite algebra over $k[\mathbb{A}^d]/\operatorname{rad}(f_0)$, and so the fields of fractions of these two k-algebras have the same transcendence degree over k. Hence (2.56)

$$\dim V(\mathfrak{p}) = \dim V(f_0).$$

Clearly $f \neq 0 \Rightarrow f_0 \neq 0$, and $f_0 \in \mathfrak{p} \Rightarrow f_0$ is nonconstant. Therefore $\dim V(f_0) = d - 1$ by 2.64. □

We can restate Theorem 3.42 as follows: let V be a closed irreducible subvariety of $\mathbb{A}^n$ and let $F \in k[X_1, \ldots, X_n]$; then

$$V \cap V(F) = \begin{cases} V & \text{if } F \text{ is identically zero on } V \\ \emptyset & \text{if } F \text{ has no zeros on } V \\ \text{pure codimension } 1 & \text{otherwise.} \end{cases}$$

COROLLARY 3.43. *Let V be an irreducible affine variety, and let Z be a maximal proper irreducible closed subset of V. Then* $\dim(Z) = \dim(V) - 1$.

PROOF. Because Z is a proper closed subset of V, there exists a nonzero regular function f on V vanishing on Z. Let $V(f)$ be the zero set of f in V. Then $Z \subset V(f) \subset V$, and Z must be an irreducible component of $V(f)$ for otherwise it would not be maximal in V. Thus Theorem 3.42 shows that $\dim Z = \dim V - 1$. □

COROLLARY 3.44. *Let V be an irreducible affine variety. Every maximal chain*

$$V = V_0 \supset V_1 \supset \cdots \supset V_d \tag{19}$$

of distinct irreducible closed subsets of V has length $d = \dim(V)$.

PROOF. As the chain is maximal, the last set V_d must be a point and each V_i must be maximal in V_{i-1}, and so, from 3.43, we find that

$$\dim V_0 = \dim V_1 + 1 = \dim V_2 + 2 = \cdots = \dim V_d + d = d.$$

□

COROLLARY 3.45. *Let V be an irreducible affine variety, and let $f_1, \ldots, f_r$ be regular functions on V. Every irreducible component Z of $V(f_1, \ldots f_r)$ has codimension at most r:*

$$\operatorname{codim}(Z) \leq r.$$

PROOF. We use induction on r. Because Z is an irreducible closed subset of $V(f_1, \ldots, f_{r-1})$, it is contained in some irreducible component Z' of $V(f_1, \ldots f_{r-1})$. By induction, $\operatorname{codim}(Z') \leq r-1$. Also Z is an irreducible component of $Z' \cap V(f_r)$ because

$$Z \subset Z' \cap V(f_r) \subset V(f_1, \ldots, f_r)$$

and Z is a maximal irreducible closed subset of $V(f_1, \ldots, f_r)$. 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 $\operatorname{codim}(Z) = \operatorname{codim}(Z') + 1 \leq r$. □

EXAMPLE 3.46. In the setting of 3.45, 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 3-dimensional cone

$$X_1X_4 - X_2X_3 = 0$$

in $\mathbb{A}^4$. Then $V(X_1) \cap V$ is the union of two planes:

$$V(X_1) \cap V = \{(0,0,*,*)\} \cup \{(0,*,0,*)\}.$$

Both of these have codimension 1 in V (as required by 3.42). Similarly,

$$V(X_2) \cap V = \{(0,0,*,*)\} \cup \{(*,0,*,0)\},$$

and so $Z \overset{\text{def}}{=} V(X_1, X_2) \cap V$ consists of a single plane $\{(0,0,*,*)\}$. Thus, Z still has codimension 1 in V, but it requires two equations to define it.

PROPOSITION 3.47. *Let Z be an irreducible closed 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 irreducible closed subsets

$$V \supset Z_1 \supset \cdots \supset Z_r = Z$$

with 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 nonzero $f_1 \in I(Z_1)$, and apply Theorem 3.42. Suppose that $f_1, \ldots, f_{s-1}$ have been chosen, and let $Y_1, Y_2, \ldots, Y_m$, be the irreducible components of $V(f_1, \ldots, f_{s-1})$, numbered so that $Z_{s-1} = Y_1$. 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 no Y_i is contained in Z_s because Z_s has smaller dimension than Y_i, and so $I(Z_s)$ is not contained in any of the ideals $I(Y_i)$. Now the prime avoidance lemma (see below) tells us that there exist an $f_s \in I(Z_s) \smallsetminus \left(\bigcup_i I(Y_i)\right)$, and this is the function we want. □

LEMMA 3.48 (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 $\mathfrak{p}_i$ is contained in a second, because then we could omit it. For a fixed i, choose an $f_i \in \mathfrak{a} \smallsetminus \mathfrak{p}_i$ and, for each $j \neq i$, choose an $f_j \in \mathfrak{p}_j \smallsetminus \mathfrak{p}_i$. Then $h_i \stackrel{\text{def}}{=} \prod_{j=1}^{r} f_j$ lies in each $\mathfrak{p}_j$ with $j \neq i$ and $\mathfrak{a}$, but not in $\mathfrak{p}_i$ (here we use that $\mathfrak{p}_i$ is prime). The element $\sum_{i=1}^{r} h_i$ is therefore in $\mathfrak{a}$ but not in any $\mathfrak{p}_i$ (e.g, $h_2, \ldots, h_r \in \mathfrak{p}_1$ but $h_1 \notin \mathfrak{p}_1$). □

EXAMPLE 3.49. When V is an affine variety whose coordinate ring is a unique factorization domain, every closed subset Z of codimension 1 is of the form $V(f)$ for some $f \in k[V]$ (see 2.66). The condition that $k[V]$ be a unique factorization domain is definitely needed. Again consider the cone,

$$V : X_1X_4 - X_2X_3 = 0$$

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 has codimension 2, in violation of 3.42. Thus Z is not of the form $V(f)$, and so

$$k[X_1, X_2, X_3, X_4]/(X_1X_4 - X_2X_3)$$

is not a unique factorization domain.

Restatement in terms of affine k-algebras

Let A be a finitely generated k-algebra. Assume that A is an integral domain with field of fractions F.

3.50. *The Krull dimension of A,* $\dim A = \operatorname{tr\,deg}_k F$.

See Corollary 2.56.

3.51 (PRINCIPAL IDEAL THEOREM). *Let $f_1, \ldots, f_r$ be elements of A. If $\mathfrak{p}$ is minimal among the prime ideals containing $(f_1, \ldots, f_r)$, then* $\operatorname{ht}(\mathfrak{p}) \leq r$. *In particular,* $\operatorname{ht}(\mathfrak{p}) \leq r$ *if $\mathfrak{p}$ can be generated by r elements.*

See Corollary 3.45.

3.52. *Let $\mathfrak{p}$ be a prime ideal in A. If $\mathfrak{p}$ has height r, then there exist $f_1, \ldots, f_r \in A$ such that*

(a) *$\mathfrak{p}$ is minimal among the prime ideals containing $(f_1, \ldots, f_r)$, and*

(b) *every prime ideal minimal among those containing $(f_1, \ldots, f_r)$ has height r.*

See Proposition 3.47.

3.53. *If every prime ideal of height 1 in A is principal, then A is a unique factorization domain.*

In order to prove this, it suffices to show that every irreducible element f of A is prime (1.26). Let $\mathfrak{p}$ be minimal among the prime ideals containing (f). According to 3.51, $\mathfrak{p}$ has height 1, and so it is principal, say, $\mathfrak{p} = (g)$. As $(f) \subset (g)$, $f = gq$ for some $q \in A$. Because f is irreducible, q is a unit, and so $(f) = (g) = \mathfrak{p}$ — the element f is prime.

3.54. *Let $\mathfrak{p}$ be a minimal nonzero prime ideal in A. Then* $\mathrm{ht}(\mathfrak{p}) = 1$.

According to 3.51, $\mathrm{ht}(\mathfrak{p}) \leq 1$ and 3.43 says that it equals 1.

3.55. *Every maximal chain of distinct prime ideals*

$$\mathfrak{p}_0 \supset \cdots \supset \mathfrak{p}_d$$

in A has length $\dim(A)$. *In particular, all maximal ideals in A have height* $\dim(A)$.

See Corollary 3.44.

3.56. *Let $\mathfrak{q} \supset \mathfrak{p}$ be prime ideals in A. Any two maximal chains of distinct prime ideals*

$$\mathfrak{q} = \mathfrak{p}_d \supset \mathfrak{p}_{d-1} \supset \cdots \supset \mathfrak{p}_0 = \mathfrak{p}$$

have the same length.

Indeed, if follows from 3.54 that their length is $\mathrm{ht}(\mathfrak{q}) - \mathrm{ht}(\mathfrak{p})$.

REMARK 3.57. The first four statements (3.50, 3.51, 3.52, 3.53) hold for all noetherian rings, but with more difficult proofs. The remaining statements (3.54, 3.55, 3.56) may fail. Rings satisfying 3.56 are said to be ***catenary***. Noncatenary rings are hard to find, but here is an example of a ring that fails 3.55. Let $A = R[X]$, where $R \overset{\text{def}}{=} k[T]_{(T)}$ is a discrete valuation ring with maximal ideal (T). The Krull dimension of A is 2, and $(T, X) \supset (T) \supset (0)$ is a maximal chain of prime ideals, but the ideal $(1 - TX)$ is (a) maximal and (b) has height 1. To see (a), note that

$$A/(1 - TX) \overset{1.13}{\simeq} R_T = k(T).$$

To see (b), note that the ideal $(1 - TX)$ in $k[T, X]$ has height 1, and that A is the ring of fractions of $k[T, X]$ obtained by inverting the elements of $k[T] \smallsetminus (T)$.

ASIDE 3.58. Proposition 3.47 shows that an irreducible 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 (exercise). Apparently, it is not known whether two polynomials always suffice to define an irreducible curve in $\mathbb{A}^3$.

More generally, one can ask whether an irreducible curve C in $\mathbb{A}^n$ can be defined by $n-1$ polynomials, i.e., do there exist $f_1, \ldots, f_{n-1} \in k[X_1, \ldots, X_n]$ such that

$$C = V(f_1, \ldots, f_{n-1})?$$

A positive answer to this question is known in the following cases:

(a) $k[C]$ is a Dedekind domain (Mohan Kumar);

(b) k is of nonzero characteristic (Cowsik and Nori).

For proofs, see Chapter 10 of Ischebeck and Rao, Ideals and Reality, Springer 2005.

Exercises

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

3-2. Let $V = \mathrm{Spm}(A)$, and let $Z = \mathrm{Spm}(A/\mathfrak{a}) \subset \mathrm{Spm}(A)$. Show that a function f on an open subset U of Z is regular if and only if, for each $P \in U$, there exists a regular function f' on an open neighbourhood U' of P in V such that f and f' agree on $U' \cap U$.

3-3. Find the image of the regular map

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

and verify that it is neither open nor closed.

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 $\mathbb{A}^1$. (Assume $\mathrm{char}(k) \neq 2$.)

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

Local Study

Geometry is the art of drawing correct conclusions from incorrect figures. (La géométrie est l'art de raisonner juste sur des figures fausses.)
Descartes

In this chapter, we examine the structure of an affine algebraic variety near a point. We begin with the case of a plane curve, since the ideas in the general case are the same but the proofs are more difficult.

a. Tangent spaces to plane curves

Consider the curve V in the plane defined by a nonconstant polynomial $F(X,Y)$,

$$V : F(X,Y) = 0.$$

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 (see 2.29). Each component $V(F_i)$ has dimension 1 (by 2.64) and so V has pure dimension 1.

If $F(X,Y)$ itself is irreducible, then

$$k[V] = k[X,Y]/(F(X,Y)) = k[x,y]$$

is an integral domain. Moreover, 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. If we were doing calculus, we would say that the tangent space at $P = (a,b)$ is defined by the equation

$$\frac{\partial F}{\partial X}(a,b)(X-a) + \frac{\partial F}{\partial Y}(a,b)(Y-b) = 0. \tag{20}$$

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.

We are not doing calculus, but we can define $\frac{\partial}{\partial X}$ and $\frac{\partial}{\partial Y}$ by

$$\frac{\partial}{\partial X}\left(\sum a_{ij}X^iY^j\right) = \sum i a_{ij}X^{i-1}Y^j, \quad \frac{\partial}{\partial Y}\left(\sum a_{ij}X^iY^j\right) = \sum j a_{ij}X^iY^{j-1},$$

and make the same definition.

DEFINITION 4.1. The ***tangent space*** $T_P V$ to V at $P = (a,b)$ is the algebraic subset defined by equation (20).

If $\frac{\partial F}{\partial X}(a,b)$ and $\frac{\partial F}{\partial Y}(a,b)$ are not both zero, then $T_P(V)$ is a line through (a,b), 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*** if all its points are nonsingular.

As in advanced calculus, we often write $\left.\frac{\partial F}{\partial X}\right|_{(a,b)}$ for $\frac{\partial F}{\partial X}(a,b)$.

Examples

For each of the following examples, the reader is invited to sketch the curve. Assume that $\mathrm{char}(k) \neq 2, 3$.

4.2. $X^m + Y^m = 1$. The tangent space at (a,b) is given by the equation

$$ma^{m-1}(X-a) + mb^{m-1}(Y-b) = 0.$$

All points on the curve are nonsingular unless the characteristic of k divides m, in which case $X^m + Y^m - 1$ has multiple factors,

$$X^m + Y^m - 1 = X^{m_0 p} + Y^{m_0 p} - 1 = (X^{m_0} + Y^{m_0} - 1)^p.$$

4.3. $Y^2 = X^3$ (sketched in 4.12 below). The tangent space at (a,b) is given by the equation

$$-3a^2(X-a) + 2b(Y-b) = 0.$$

The only singular point is $(0,0)$.

4.4. $Y^2 = X^2(X+1)$ (sketched in 4.10 below). Here again only $(0,0)$ is singular.

4.5. $Y^2 = X^3 + aX + b$. In 2.2 we sketched two nonsingular examples of such curves, and in 4.10 and 4.11 we sketch two singular examples. The singular points of the curve are the common zeros of the polynomials

$$Y^2 - X^3 - aX - b, \quad 2Y, \quad 3X^2 + a,$$

which consist of the points $(c,0)$ with c a common zero of

$$X^3 + aX + b, \quad 3X^2 + a.$$

As $3X^2 + a$ 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.

4.6. $V = V(FG)$, where FG has no multiple factors (so F and G are coprime). 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 product rule:

$$\frac{\partial (FG)}{\partial X} = F \cdot \frac{\partial G}{\partial X} + \frac{\partial F}{\partial X} \cdot G, \quad \frac{\partial (FG)}{\partial Y} = F \cdot \frac{\partial G}{\partial Y} + \frac{\partial F}{\partial Y} \cdot G.$$

The singular locus

PROPOSITION 4.7. *The nonsingular points of a plane curve form a dense open subset of the curve.*

PROOF. Let $V = V(F)$, where F is a nonconstant polynomial in $k[X,Y]$ without multiple factors. It suffices to show that the nonsingular points form a dense open subset of each irreducible component of V, and so we may suppose that V (hence F) is irreducible. It suffices to show that the set of singular points is a proper closed subset. It is closed because it is the set of common zeros of the polynomials

$$F, \quad \frac{\partial F}{\partial X}, \quad \frac{\partial F}{\partial Y}.$$

It will be proper unless $\partial F/\partial X$ and $\partial F/\partial Y$ are both identically zero on V, and hence both multiples of F, but, as they have lower degree than F, 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 pth power (characteristic p, see (18), p. 75). These are contrary to our assumptions. □

Thus the singular points form a proper closed subset, called the ***singular locus***.

ASIDE 4.8. 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).

b. Tangent cones to plane curves

A polynomial $F(X,Y)$ can be written (uniquely) as a finite sum

$$F = F_0 + F_1 + F_2 + \cdots + F_m + \cdots \tag{21}$$

with each F_m 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 (21) (the nonzero 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 (21) becomes

$$F = aX + bY + \text{higher degree terms},$$

and the equation of the tangent space is

$$aX + bY = 0.$$

DEFINITION 4.9. 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 $(V(F_*), k[X,Y]/F_*)$. To obtain the tangent cone at any other point, translate to the origin, and then translate back.

Note that the geometric tangent cone at a point on a curve always has dimension 1. While the tangent space tells you whether a point is nonsingular or not, the tangent cone also gives you information on the nature of a singularity.

In general we can factor F_* as

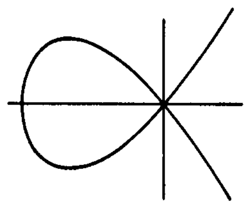
$$F_*(X,Y) = cX^{r_0}\prod_i (Y - a_i X)^{r_i}.$$

Then $\deg F_* \stackrel{\text{def}}{=} \sum r_i$ is called the ***multiplicity*** of the singularity. 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***. There are many names for special types of singularities — see any book, especially an old book, on algebraic curves.

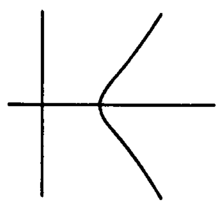
Examples

The following examples are adapted from Walker 1950. We assume that the characteristic of k is 0.

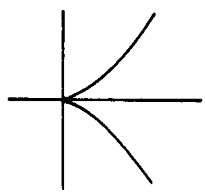
4.10. $F(X,Y) = X^3+X^2-Y^2$. The tangent cone at $(0,0)$ is defined by Y^2-X^2. It is the pair of lines $Y = \pm X$, and the singularity is a node.



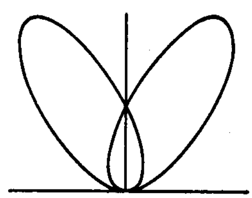
4.11. $F(X,Y) = X^3-X^2-Y^2$. The origin is an isolated point of the real locus. It is again a node, but the tangent cone is defined by Y^2+X^2, which is the pair of lines $Y = \pm iX$. In this case, the real locus of the tangent cone is just the point (0,0).



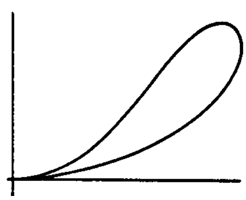
4.12. $F(X,Y) = X^3 - Y^2$. Here the origin is a cusp. The tangent cone is defined by Y^2, which is the X-axis (doubled).



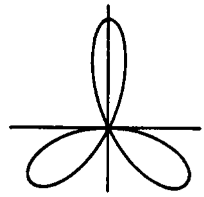
4.13. $F(X,Y) = 2X^4-3X^2Y+Y^2-2Y^3+Y^4$. The origin is again a double point, but this time it is a tacnode. The tangent cone is again defined by Y^2.



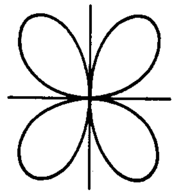
4.14. $F(X,Y) = X^4+X^2Y^2-2X^2Y-XY^2-Y^2$. The origin is again a double point, but this time it is a ramphoid cusp. The tangent cone is again defined by Y^2.



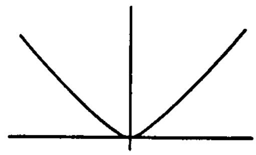
4.15. $F(X,Y) = (X^2+Y^2)^2 + 3X^2Y - Y^3$. The origin is an ordinary triple point. The tangent cone is defined by $3X^2Y - Y^3$, which is the triple of lines $Y = 0$, $Y = \pm\sqrt{3}X$.



4.16. $F(X,Y) = (X^2+Y^2)^3 - 4X^2Y^2$. The origin has multiplicity 4. The tangent cone is defined by $4X^2Y^2$, which is the union of the X and Y axes, each doubled.



4.17. $F(X,Y) = X^6 - X^2Y^3 - Y^5$. The tangent cone is defined by $X^2Y^3 + Y^5$, which consists of a triple line $Y^3 = 0$ and a pair of lines $Y = \pm iX$.



ASIDE 4.18. Note that the real locus of the algebraic curve in 4.17 is smooth even though the curve itself is singular. Another example of such a curve is $Y^3 + 2X^2Y - X^4 = 0$. This is singular at $(0,0)$, but its real locus is the image of $\mathbb{R}$ under the analytic map $t \mapsto (t^3+2t, t(t^3+2))$, which is injective, proper, and immersive, and hence an embedding into $\mathbb{R}^2$ with closed image. See mo98366 for a discussion of this question.

c. The local ring at a point on a curve

PROPOSITION 4.19. *Let P be a point on a plane 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 $\mathfrak{m} \cdot k[V]_\mathfrak{m}$ 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 1.15), 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. As $\mathcal{O}_P$ has Krull dimension one (2.64), for its maximal ideal to be principal means that it is a regular local ring of dimension 1 (see 1.6). Thus, for a point P on a curve,

$$P \text{ nonsingular} \iff \mathcal{O}_P \text{ regular}.$$

PROPOSITION 4.20. *Every regular local ring of dimension one is a principal ideal domain.*

PROOF. Let A be such a ring, and let $\mathfrak{m} = (\pi)$ be its maximal ideal. According to the Krull intersection theorem (1.8), $\bigcap_{r\geq 0} \mathfrak{m}^r = (0)$. Let $\mathfrak{a}$ be a proper nonzero ideal in A. As $\mathfrak{a}$ is finitely generated, there exists an $r \in \mathbb{N}$ such that $\mathfrak{a} \subset \mathfrak{m}^r$ but $\mathfrak{a} \not\subset \mathfrak{m}^{r+1}$. Therefore, there exists an $a = c\pi^r \in \mathfrak{a}$ such that $a \notin \mathfrak{m}^{r+1}$. The second condition implies that $c \notin \mathfrak{m}$, and so it is a unit. Therefore $(\pi^r) = (a) \subset \mathfrak{a} \subset (\pi^r)$, and so $\mathfrak{a} = (\pi^r) = \mathfrak{m}^r$. We have shown that all ideals in A are principal.

By assumption, there exists a prime ideal $\mathfrak{p}$ properly contained in $\mathfrak{m}$. Then $A/\mathfrak{p}$ is an integral domain. As $\pi \notin \mathfrak{p}$, it is not nilpotent in $A/\mathfrak{p}$, and hence not nilpotent in A.

Let a and b be nonzero elements of A. There exist $r, s \in \mathbb{N}$ such that $a \in \mathfrak{m}^r \smallsetminus \mathfrak{m}^{r+1}$ and $b \in \mathfrak{m}^s \smallsetminus \mathfrak{m}^{s+1}$. Then $a = u\pi^r$ and $b = v\pi^s$ with u and v units, and $ab = uv\pi^{r+s} \neq 0$. Hence A is an integral domain. □

It follows from the elementary theory of principal ideal domains that the following conditions on a principal ideal domain A are equivalent:

(a) A has exactly one nonzero prime ideal;

(b) A has exactly one prime element up to associates;

(c) A is local and is not a field.

A ring satisfying these conditions is called a ***discrete valuation ring***.[1]

THEOREM 4.21. *A point P on a plane algebraic curve is nonsingular if and only if $\mathcal{O}_P$ is regular, in which case it is a discrete valuation ring.*

PROOF. The statement summarizes the above discussion. □

d. Tangent spaces to algebraic subsets of $\mathbb{A}^m$

Before defining tangent spaces at points of an algebraic subset of $\mathbb{A}^m$ we review some terminology from linear algebra.

LINEAR ALGEBRA

For a vector space k^m, let X_i be the ith 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 $(k^m)^\vee \stackrel{\text{def}}{=} \mathrm{Hom}_{k\text{-linear}}(k^m, k)$.

Let $A = (a_{ij})$ be an $n \times m$ matrix. It defines a linear map $\alpha\colon k^m \to k^n$, by

$$\begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} \mapsto A \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^m a_{1j} a_j \\ \vdots \\ \sum_{j=1}^m a_{nj} a_j \end{pmatrix}.$$

[1] Let A be a discrete valuation ring and π a prime element of A. For an element a of the field of fractions F of A, let

$$v(a) = \begin{cases} r & \text{if } a = c\pi^r \text{ with } c \in A^\times, \\ \infty & \text{if } a = 0. \end{cases}$$

Then v is an additive valuation on F with discrete value group $v(F) = \mathbb{Z} \sqcup \{\infty\}$ and valuation ring $A = \{a \in F \mid v(a) \geq 0\}$. The discrete valuation rings are exactly the valuation rings of discrete valuations, which explains the name.

Let $Y_1, \ldots, Y_n$ for the coordinate functions on k^n. Then

$$Y_i \circ \alpha = \sum_{j=1}^{m} a_{ij} X_j.$$

This says that the ith coordinate of $\alpha(\mathbf{a})$ is

$$\sum_{j=1}^{m} a_{ij}(X_j \mathbf{a}) = \sum_{j=1}^{m} a_{ij} a_j.$$

TANGENT SPACES

DEFINITION 4.22. Let $V \subset k^m$ be an algebraic subset of k^m, and let $\mathfrak{a} = I(V)$. The ***tangent space*** $T_{\mathbf{a}}(V)$ to V at a point $\mathbf{a} = (a_1, \ldots, a_m)$ of V is the subspace of the vector space with origin $\mathbf{a}$ cut out by the linear equations

$$\sum_{i=1}^{m} \left.\frac{\partial F}{\partial X_i}\right|_{\mathbf{a}} (X_i - a_i) = 0, \qquad F \in \mathfrak{a}. \tag{22}$$

In other words, $T_{\mathbf{a}}(\mathbb{A}^m)$ 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 (22).

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:

$$(dF)_{\mathbf{a}} = \sum_{i=1}^{m} \left.\frac{\partial F}{\partial X_i}\right|_{\mathbf{a}} (dX_i)_{\mathbf{a}}.$$

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:

$$(dF)_{\mathbf{a}} = 0, \quad F \in \mathfrak{a}. \tag{23}$$

I claim that, in (22) and (23), it suffices to take the F to lie 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-vector space $\{(dF)_{\mathbf{a}} \mid F \in \mathfrak{a}\}$.

DEFINITION 4.23. A point $\mathbf{a}$ on an algebraic set V is ***nonsingular*** (or ***smooth***) if it lies on a single irreducible component W of V and the dimension of the tangent space at $\mathbf{a}$ is equal to the dimension of W; otherwise it is ***singular*** (or ***multiple***).

Thus, a point $\mathbf{a}$ on an irreducible algebraic set V is nonsingular if and only if $\dim T_{\mathbf{a}}(V) = \dim V$. As in the case of plane curves, a point on V is nonsingular if and only if it lies on a single irreducible component of V and is nonsingular on it.

Let $\mathfrak{a} = (F_1, \dots, F_r)$, and let

$$J = \operatorname{Jac}(F_1, \dots, F_r) = \left(\frac{\partial F_i}{\partial X_j}\right) = \begin{pmatrix} \frac{\partial F_1}{\partial X_1}, & \dots, & \frac{\partial F_1}{\partial X_m} \\ \vdots & & \vdots \\ \frac{\partial F_r}{\partial X_1}, & \dots, & \frac{\partial F_r}{\partial X_m} \end{pmatrix}.$$

Then the equations defining $T_{\mathbf{a}}(V)$ as a subspace of $T_{\mathbf{a}}(\mathbb{A}^m)$ have matrix $J(\mathbf{a})$. Therefore, linear algebra shows that

$$\dim_k T_{\mathbf{a}}(V) = m - \operatorname{rank} J(\mathbf{a}),$$

and so $\mathbf{a}$ is nonsingular if and only if the rank of $\operatorname{Jac}(F_1, \dots, F_r)(\mathbf{a})$ is equal to $m - \dim(V)$. For example, if V is a hypersurface, say, $I(V) = (F(X_1, \dots, X_m))$, then

$$\operatorname{Jac}(F)(\mathbf{a}) = \left(\frac{\partial F}{\partial X_1}(\mathbf{a}), \dots, \frac{\partial F}{\partial X_m}(\mathbf{a})\right),$$

and $\mathbf{a}$ is nonsingular if and only if not all of the partial derivatives $\frac{\partial F}{\partial X_i}$ vanish at $\mathbf{a}$.

We can regard J as a matrix of regular functions on V. For each r,

$$\{\mathbf{a} \in V \mid \operatorname{rank} J(\mathbf{a}) \leq r\}$$

is closed in V, because it is the set where certain determinants vanish. Therefore, there is an open subset U of V on which $\operatorname{rank} J(\mathbf{a})$ attains its maximum value, and the rank jumps on closed subsets. Later (4.37) we shall show that the maximum value of $\operatorname{rank} J(\mathbf{a})$ is $m - \dim V$, and so the nonsingular points of V form a nonempty open subset of V.

e. The differential of a regular map

Consider a regular map

$$\varphi\colon \mathbb{A}^m \to \mathbb{A}^n, \quad \mathbf{a} \mapsto (P_1(a_1, \dots, a_m), \dots, P_n(a_1, \dots, a_m)).$$

We can think of φ as being given by the equations

$$Y_i = P_i(X_1, \dots, X_m), \quad i = 1, \dots, n.$$

It corresponds to the map of rings $\varphi^*\colon k[Y_1, \dots, Y_n] \to k[X_1, \dots, X_m]$ sending Y_i to $P_i(X_1, \dots, X_m)$, $i = 1, \dots, n$.

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

$$\operatorname{Jac}(P_1, \dots, P_n)(\mathbf{a}) \stackrel{\text{def}}{=} \begin{pmatrix} \frac{\partial P_1}{\partial X_1}(\mathbf{a}), & \dots, & \frac{\partial P_1}{\partial X_m}(\mathbf{a}) \\ \vdots & & \vdots \\ \frac{\partial P_n}{\partial X_1}(\mathbf{a}), & \dots, & \frac{\partial P_n}{\partial X_m}(\mathbf{a}) \end{pmatrix}.$$

For example, suppose $\mathbf{a} = (0, \dots, 0)$ and $\mathbf{b} = (0, \dots, 0)$, so that $T_{\mathbf{a}}(\mathbb{A}^m) = k^m$ and $T_{\mathbf{b}}(\mathbb{A}^n) = k^n$. If

$$P_i(X_1, \dots, X_m) = \sum_{j=1}^{m} c_{ij} X_j + (\text{higher terms}), \qquad i = 1, \dots, n,$$

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 $F \in k[X_1, \dots, X_m]$. We can regard F as a regular map $\mathbb{A}^m \to \mathbb{A}^1$, whose differential will be a linear map

$$(dF)_{\mathbf{a}} : T_{\mathbf{a}}(\mathbb{A}^m) \to T_{\mathbf{b}}(\mathbb{A}^1), \qquad \mathbf{b} = F(\mathbf{a}).$$

When we identify $T_{\mathbf{b}}(\mathbb{A}^1)$ with k, we obtain an identification of the differential of F (regarded as a regular map) with the differential of F (regarded as a regular function).

LEMMA 4.24. *Let $\varphi : \mathbb{A}^m \to \mathbb{A}^n$ be a regular map. If φ maps $V \stackrel{\text{def}}{=} V(\mathfrak{a}) \subset k^m$ into $W \stackrel{\text{def}}{=} V(\mathfrak{b}) \subset k^n$, 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:

$$\frac{\partial f}{\partial X_i} = \sum_{j=1}^{n} \frac{\partial f}{\partial Y_j} \frac{\partial Y_j}{\partial X_i}, \quad Y_j = P_j(X_1, \dots, X_m), \quad f = f(Y_1, \dots, Y_n).$$

If φ is the map given by the equations

$$Y_j = P_j(X_1, \dots, X_m), \qquad j = 1, \dots, n,$$

then the chain rule implies that

$$d(f \circ \varphi)_{\mathbf{a}} = (df)_{\mathbf{b}} \circ (d\varphi)_{\mathbf{a}}, \quad \mathbf{b} = \varphi(\mathbf{a}).$$

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 $(d\varphi)_{\mathbf{a}} : T_{\mathbf{a}}(V) \to T_{\mathbf{b}}(W)$. The usual rules from advanced calculus hold. For example,

$$(d\psi)_{\mathbf{b}} \circ (d\varphi)_{\mathbf{a}} = d(\psi \circ \varphi)_{\mathbf{a}}, \quad \mathbf{b} = \varphi(\mathbf{a}).$$

f. Tangent spaces to affine algebraic varieties

The definition 4.22 of the tangent space at a point on an algebraic set uses the embedding of the algebraic set into $\mathbb{A}^n$. In this section, we give an intrinsic definition of the tangent space at a point of an affine algebraic variety that makes clear that it depends only on the local ring at the point.

Dual numbers

For an affine algebraic variety V and a k-algebra R (not necessarily affine), we let

$$V(R) = \mathrm{Hom}(k[V], R) \qquad \text{(homomorphisms of } k\text{-algebras).}$$

For example, if $V \subset \mathbb{A}^n$, then

$$V(R) = \{(a_1, \ldots, a_n) \in R^n \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in I(V)\}.$$

A homomorphism $R \to S$ of k-algebras defines a map $V(R) \to V(S)$ of sets.

The ***ring of dual numbers*** is $k[\varepsilon] \overset{\text{def}}{=} k[X]/(X^2)$, where $\varepsilon = X + (X^2)$. Thus $k[\varepsilon] = k \oplus k\varepsilon$ as a k-vector space, and

$$(a + b\varepsilon)(c + d\varepsilon) = ac + (ad + bc)\varepsilon, \quad a, b, c, d \in k.$$

Note that there is a k-algebra homomorphism $\varepsilon \mapsto 0\colon\ k[\varepsilon] \to k$.

DEFINITION 4.25. Let P be a point on an affine algebraic variety V over k. The tangent space to V at P is

$$T_P(V) \overset{\text{def}}{=} \{P' \in V(k[\varepsilon]) \mid P' \mapsto P \text{ under } V(k[\varepsilon]) \to V(k)\}.$$

Thus an element of $T_P(V)$ is a homomorphism of k-algebras $\alpha\colon\ k[V] \to k[\varepsilon]$ whose composite with $k[\varepsilon] \xrightarrow{\varepsilon \mapsto 0} k$ is the point P. To say that $k[V] \to k$ is the point P means that its kernel is $\mathfrak{m}_P$, and so $\mathfrak{m}_P = \alpha^{-1}((\varepsilon))$.

PROPOSITION 4.26. *Let V be an algebraic subset of $\mathbb{A}^n$, and let $V' = (V, \mathcal{O}_V)$ be V equipped with its canonical structure of an affine algebraic variety. Let $P \in V$. Then*

$$T_P(V) \text{ (as defined in 4.22)} \simeq T_P(V') \text{ (as defined in 4.25).}$$

PROOF. Let $I(V) = \mathfrak{a}$ and let $P = (a_1, \ldots, a_n)$. On rewriting a polynomial $F(X_1, \ldots, X_n)$ in terms of the variables $X_i - a_i$, we obtain the (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 $(X_i - a_i)$.

According to 4.25, $T_P(V')$ consists of the elements $\mathbf{a} + \varepsilon\mathbf{b}$ of $k[\varepsilon]^n = k^n \oplus k^n\varepsilon$ lying in $V(k[\varepsilon])$. Let $F \in \mathfrak{a}$. On setting X_i equal to $a_i + \varepsilon b_i$ in the above formula, we get,

$$F(a_1 + \varepsilon b_1, \ldots, a_n + \varepsilon b_n) = \varepsilon\left(\sum \left.\frac{\partial F}{\partial X_i}\right|_{\mathbf{a}} b_i\right).$$

Thus, $(a_1 + \varepsilon b_1, \ldots, a_n + \varepsilon b_n)$ lies in $V(k[\varepsilon])$ if and only if $(b_1, \ldots, b_n) \in T_{\mathbf{a}}(V)$. □

We can restate this as follows. Let V be an affine algebraic variety, and let $P \in V$. Choose an embedding $V \hookrightarrow \mathbb{A}^n$, and let P map to $(a_1, \ldots, a_n)$. Then the point

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n)\varepsilon$$

of $\mathbb{A}^n(k[\varepsilon])$ is an element of $T_P(V)$ (definition 4.25) if and only if $(b_1, \ldots, b_n)$ is an element of $T_P(V)$ (definition 4.22).

PROPOSITION 4.27. *Let V be an affine variety, and let $P \in V$. There is a canonical isomorphism*

$$T_P(V) \simeq \mathrm{Hom}(\mathcal{O}_P, k[\varepsilon]) \qquad \text{(local homomorphisms of local } k\text{-algebras).}$$

PROOF. By definition, an element of $T_P(V)$ is a homomorphism $\alpha\colon k[V] \to k[\varepsilon]$ such that $\alpha^{-1}((\varepsilon)) = \mathfrak{m}_P$. Therefore α maps elements of $k[V] \smallsetminus \mathfrak{m}_P$ into $(k[\varepsilon] \smallsetminus (\varepsilon)) = k[\varepsilon]^\times$, and so α extends (uniquely) to a homomorphism $\alpha'\colon \mathcal{O}_P \to k[\varepsilon]$. By construction, α' is a local homomorphism of local k-algebras, and clearly every such homomorphism arises in this way from a (unique) element of $T_P(V)$. □

Derivations

DEFINITION 4.28. Let A be a k-algebra and M an A-module. A k-***derivation*** is a map $D\colon A \to M$ such that

(a) $D(c) = 0$ for all $c \in k$;

(b) $D(f + g) = D(f) + D(g)$;

(c) $D(fg) = f \cdot Dg + g \cdot Df$ (Leibniz's rule).

Note that the conditions imply that D is k-linear (but not A-linear). The k-derivations $A \to M$ form a k-vector space $\mathrm{Der}_k(A, M)$.

For example, let A be a local k-algebra with maximal ideal $\mathfrak{m}$, and assume that $A/\mathfrak{m} = k$. For $f \in A$, let $f(\mathfrak{m})$ denote the image of f in $A/\mathfrak{m}$. Then $f - f(\mathfrak{m}) \in \mathfrak{m}$, and the map

$$f \mapsto df \stackrel{\text{def}}{=} f - f(\mathfrak{m}) \mod \mathfrak{m}^2$$

is a k-derivation $A \to \mathfrak{m}/\mathfrak{m}^2$ because, modulo $\mathfrak{m}^2$,

$$\begin{aligned} 0 &= (f - f(\mathfrak{m}))(g - g(\mathfrak{m})) \\ &= -fg + f(\mathfrak{m})g(\mathfrak{m}) + f \cdot (g - g(\mathfrak{m})) + g(f - f(\mathfrak{m})) \\ &= -d(fg) + f \cdot dg + g \cdot df. \end{aligned}$$

PROPOSITION 4.29. *Let $(A, \mathfrak{m})$ be as above. There are canonical isomorphisms*

$$\underset{\text{local } k\text{-algebra homs}}{\mathrm{Hom}(A, k[\varepsilon])} \simeq \mathrm{Der}_k(A, k) \simeq \underset{k\text{-linear maps}}{\mathrm{Hom}(\mathfrak{m}/\mathfrak{m}^2, k)}.$$

PROOF. The composite of the maps $k \xrightarrow{c \mapsto c} A \xrightarrow{f \mapsto f(\mathfrak{m})} k$ is the identity, and so, when regarded as k-vector space, A decomposes into

$$A = k \oplus \mathfrak{m}, \quad f \leftrightarrow (f(\mathfrak{m}), f - f(\mathfrak{m})).$$

Let $\alpha\colon A \to k[\varepsilon]$ 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, $a_0 = a(\mathfrak{m})$. We have

$$\begin{aligned} \alpha(ab) &= (ab)_0 + D_\alpha(ab)\varepsilon, \text{ and} \\ \alpha(a)\alpha(b) &= (a_0 + D_\alpha(a)\varepsilon)(b_0 + D_\alpha(b)\varepsilon) = a_0 b_0 + (a_0 D_\alpha(b) + b_0 D_\alpha(a))\varepsilon. \end{aligned}$$

On comparing these expressions, we see that D_α satisfies Leibniz's rule, and therefore is a k-derivation $A \to k$. Conversely, if $D\colon A \to k$ is a k-derivation, then

$$\alpha\colon a \mapsto a(\mathfrak{m}) + D(a)\varepsilon$$

is a local homomorphism of k-algebras $A \to k[\varepsilon]$, and all such homomorphisms arise in this way. This proves the first isomorphism.

A derivation $D\colon A \to k$ is zero on k and on $\mathfrak{m}^2$ (by Leibniz's rule). It therefore defines a k-linear map $\mathfrak{m}/\mathfrak{m}^2 \to k$. Conversely, a k-linear map $\mathfrak{m}/\mathfrak{m}^2 \to k$ defines a derivation by composition

$$A \xrightarrow{f \mapsto df} \mathfrak{m}/\mathfrak{m}^2 \to k. \qquad \square$$

Tangent spaces and differentials

We summarize the above discussion in the context of affine algebraic varieties.

4.30. Let V be an affine algebraic variety, and let P be a point on V. Write $\mathfrak{m}_P$ for the corresponding maximal ideal in $k[V]$ and $\mathfrak{n}_P$ for the maximal ideal $\mathfrak{m}_P\mathcal{O}_{V,P}$ in the local ring at P. There are canonical isomorphisms

$$\begin{array}{ccccc}
T_P(V) & \longrightarrow & \mathrm{Der}_k(k[V],k) & \longrightarrow & \underset{k\text{-linear homs}}{\mathrm{Hom}(\mathfrak{m}_P/\mathfrak{m}_P^2,k)} \\
\downarrow & & \downarrow & & \downarrow \\
\underset{\text{local } k\text{-algebra homs}}{\mathrm{Hom}(\mathcal{O}_P,k[\varepsilon])} & \longrightarrow & \mathrm{Der}_k(\mathcal{O}_P,k) & \longrightarrow & \underset{k\text{-linear homs}}{\mathrm{Hom}(\mathfrak{n}_P/\mathfrak{n}_P^2,k)}.
\end{array} \tag{24}$$

In the term $\mathrm{Der}_k(k[V],k)$ on the top row, $k[V]$ acts on k through $k[V] \to k[V]/\mathfrak{m}_P \simeq k$ (so it depends on P), and in the term $\mathrm{Der}_k(\mathcal{O}_P,k)$ on the bottom row, $\mathcal{O}_P$ acts on k through $\mathcal{O}_P \to \mathcal{O}_P/\mathfrak{n}_P \simeq k$. The maps have the following descriptions.

(a) By definition, $T_P(V)$ is the fibre of $V(k[\varepsilon]) \to V(k)$ over P. To give an element of $T_P(V)$ amounts to giving a homomorphism $\alpha\colon k[V] \to k[\varepsilon]$ such that $\alpha^{-1}((\varepsilon)) = \mathfrak{m}_P$.

(b) The homomorphism α in (a) can be written,

$$\alpha(f) = f(\mathfrak{m}_P) \oplus D_\alpha(f)\varepsilon, \quad f \in k[V],\, f(\mathfrak{m}_P) \in k,\, D_\alpha(f) \in k.$$

Then D_α is a k-derivation $k[V] \to k$, and D_α induces a k-linear map $\mathfrak{m}_P/\mathfrak{m}_P^2 \to k$.

(c) The homomorphism $\alpha\colon k[V] \to k[\varepsilon]$ in (a) extends uniquely to a local homomorphism $\mathcal{O}_P \to k[\varepsilon]$. Similarly, a k-derivation $k[V] \to k$ extends uniquely to a k-derivation $\mathcal{O}_P \to k$.

(d) The two vector spaces at the right of the diagram are related through the isomorphism $\mathfrak{m}_P/\mathfrak{m}_P^2 \to \mathfrak{n}_P/\mathfrak{n}_P^2$ of (1.15).

4.31. A regular map $\varphi\colon V \to W$ defines a map $\varphi(k[\varepsilon])\colon V(k[\varepsilon]) \to W(k[\varepsilon])$, which sends the fibre over P to the fibre over $Q \overset{\text{def}}{=} \varphi(P)$, i.e., it defines a map

$$d\varphi\colon T_P(V) \to T_Q(W).$$

$$\begin{array}{ccc}
T_P(V) & \xrightarrow{d\varphi} & T_Q(W) \\
\downarrow & & \downarrow \\
V(k[\varepsilon]) & \xrightarrow{\varphi} & W(k[\varepsilon]) \\
\downarrow{\scriptstyle \varepsilon\mapsto 0} & & \downarrow{\scriptstyle \varepsilon\mapsto 0} \\
V(k) & \xrightarrow{\varphi} & W(k)
\end{array}$$

This map of tangent spaces is called the *differential* of φ at P.

(a) When V and W are embedded as closed subvarieties of $\mathbb{A}^n$, $d\varphi$ has the description in p. 89.

(b) As a map $\mathrm{Hom}(\mathcal{O}_P, k[\varepsilon]) \to \mathrm{Hom}(\mathcal{O}_Q, k[\varepsilon])$, $d\varphi$ is induced by $\varphi^* : \mathcal{O}_Q \to \mathcal{O}_P$.

(c) As a map $\mathrm{Hom}(\mathfrak{m}_P/\mathfrak{m}_P^2, k) \to \mathrm{Hom}(\mathfrak{m}_Q/\mathfrak{m}_Q^2, k)$, $d\varphi$ is induced by the map $\mathfrak{m}_Q/\mathfrak{m}_Q^2 \to \mathfrak{m}_P/\mathfrak{m}_P^2$ defined by $\varphi^* : k[W] \to k[V]$.

EXAMPLE 4.32. Let E be a finite dimensional vector space over k. Then $T_0(\mathbb{A}(E)) \simeq E$.

ASIDE 4.33. A map $\mathrm{Spm}(k[\varepsilon]) \to V$ should be thought of as a curve in V but with only the first infinitesimal structure retained. Thus, the descriptions of the tangent space provided by the terms in the top row of (24) correspond to the three standard descriptions of the tangent space in differential geometry: via tangent curves, via derivations, via cotangent spaces (Wikipedia: TANGENT SPACE).

g. Tangent cones

Let V be an algebraic subset of k^m, and let $\mathfrak{a} = I(V)$. Assume that $P = (0, \dots, 0) \in V$. Define $\mathfrak{a}_*$ to be the ideal generated by the leading forms F_* of the polynomials $F \in \mathfrak{a}$. The ***geometric tangent cone*** at P, $C_P(V)$ is $V(\mathfrak{a}_*)$, and the ***tangent cone*** is the pair $(V(\mathfrak{a}_*), k[X_1, \dots, X_n]/\mathfrak{a}_*)$. Obviously, $C_P(V) \subset T_P(V)$.[2]

☡ If $\mathfrak{a}$ is principal, say, $\mathfrak{a} = (F)$, then $\mathfrak{a}_* = (F_*)$, but if $\mathfrak{a} = (F_1, \dots, F_r)$, then it need not be true that $\mathfrak{a}_* = (F_{1*}, \dots, F_{r*})$. Consider for example $\mathfrak{a} = (XY, XZ + Z(Y^2 - Z^2))$. One can show that this is an intersection of prime ideals, and hence is radical. As the polynomial

$$YZ(Y^2 - Z^2) = Y \cdot (XZ + Z(Y^2 - Z^2)) - Z \cdot (XY)$$

lies in $\mathfrak{a}$ and is homogeneous, it lies in $\mathfrak{a}_*$, but it is not in the ideal generated by XY, XZ. In fact, $\mathfrak{a}_* = (XY, XZ, YZ(Y^2 - Z^2)$.

Let A be a local ring with maximal ideal $\mathfrak{n}$. The ***associated graded ring*** is

$$\mathrm{gr}(A) = \bigoplus_{i \geq 0} \mathfrak{n}^i/\mathfrak{n}^{i+1}.$$

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 1.15).

PROPOSITION 4.34. *The homomorphism of k-algebras*

$$k[X_1, \dots, X_n]/\mathfrak{a}_* \to \mathrm{gr}(\mathcal{O}_P)$$

sending the class of X_i in $k[X_1, \dots, X_n]/\mathfrak{a}_*$ to the class of X_i in $\mathrm{gr}(\mathcal{O}_P)$ 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

$$(X_1, \dots, X_n)^i/(X_1, \dots, X_n)^{i+1} + \mathfrak{a}_i = i\text{th homogeneous piece of } k[X_1, \dots, X_n]/\mathfrak{a}_*. \qquad \square$$

[2] There is a more natural definition of the tangent cone as an algebraic scheme — see Chapter 10.

For an affine algebraic 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 $(C_P(V), \mathrm{gr}(\mathcal{O}_P))$.

As in the case of a curve, the dimension of the geometric tangent cone at P is the same as the dimension of V (because the Krull dimension of a noetherian local ring is equal to that of its graded ring; Matsumura 1989, Theorem 13.9). Moreover, $\mathrm{gr}(\mathcal{O}_P)$ is a polynomial ring in $\dim V$ variables if and only if $\mathcal{O}_P$ is regular (ibid., Exercise 19.1). Therefore, P is nonsingular (see below) if and only if $\mathrm{gr}(\mathcal{O}_P)$ is a polynomial ring in $\dim(V)$ variables, in which case $C_P(V) = T_P(V)$.

A regular map $\varphi\colon V \to W$ sending P to Q induces a homomorphism $\mathrm{gr}(\mathcal{O}_Q) \to \mathrm{gr}(\mathcal{O}_P)$, and hence a map $C_P(V) \to C_Q(V)$ of the geometric tangent cones. We say that φ is ***étale*** at P if $\mathrm{gr}(\mathcal{O}_Q) \to \mathrm{gr}(\mathcal{O}_P)$ is an isomorphism. When P and Q are nonsingular points, this just says that the map $d\varphi\colon T_P(V) \to T_Q(W)$ on tangent spaces is an isomorphism.

☡ The map on the rings $k[X_1, \ldots, X_n]/\mathfrak{a}^*$ 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 4.34, i.e., it is necessary to work with the rings $\mathrm{gr}(\mathcal{O}_P)$.

h. Nonsingular points; the singular locus

DEFINITION 4.35. A point P on an affine algebraic variety V is said to be ***nonsingular*** or ***smooth*** if it lies on a single irreducible component W of V and $\dim T_P(V) = \dim W$; otherwise the point is said to be ***singular***. A variety is ***nonsingular*** if all of its points are nonsingular. The set of singular points of a variety is called its ***singular locus.***

Thus, on an irreducible variety V of dimension d,

$$P \text{ is nonsingular} \iff \dim_k T_P(V) = d \iff \dim_k(\mathfrak{n}_P/\mathfrak{n}_P^2) = d.$$

PROPOSITION 4.36. *Let V be an irreducible variety of dimension d, and let P be a nonsingular point on V. 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. Because P is nonsingular, there exist regular functions $f_1, \ldots, f_d$ on an open neighbourhood U of P whose images in $\mathcal{O}_P$ generate its maximal ideal $\mathfrak{n}_P$. We show that P is an irreducible component of the zero set of the $f_1, \ldots, f_d$ in U. If not, there exists an irreducible component Z of $V(f_1, \ldots, f_d)$ properly containing P. Write $Z = V(\mathfrak{p})$ with $\mathfrak{p}$ is a prime ideal in $k[U]$. As $V(\mathfrak{p}) \subset V(f_1, \ldots, f_d)$ and Z properly contains P,

$$(f_1, \ldots, f_d) \subset \mathfrak{p} \subsetneqq \mathfrak{m}_P \qquad \text{(ideals in } k[U]).$$

On passing to the local ring $\mathcal{O}_P = k[U]_{\mathfrak{m}_P}$, we find (using 1.14) 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. □

Let P be a point (possibly singular) on an irreducible variety V. The argument in the above proof shows that, if $f_1, \ldots, f_r$ generate the maximal ideal $\mathfrak{n}_P$ in $\mathcal{O}_P$, then P is an irreducible component of $V(f_1, \ldots, f_r)$, and so $r \geq d$ (by 3.45). Nakayama's lemma (1.3) shows that $f_1, \ldots, f_r$ generate $\mathfrak{n}_P$ if and only if their images span $\mathfrak{n}_P/\mathfrak{n}_P^2$. Thus

$$\dim T_P(V) \geq \dim V, \text{ with equality if and only if } P \text{ is nonsingular.}$$

A point P on V is nonsingular if and only if there exists an open affine neighbourhood U of P and functions $f_1, \ldots f_d$ on U such that $(f_1, \ldots, f_d)$ is the ideal of all regular functions on U zero at P.

THEOREM 4.37. *The set of nonsingular points of an affine algebraic variety V is dense and open.*

PROOF. We first show that the singular locus is closed. We may suppose that V is affine, say, $V = V(\mathfrak{a}) \subset \mathbb{A}^n$. Let $P_1, \ldots, P_r$ generate $\mathfrak{a}$. Then the singular locus is the zero set of the ideal generated by the $(n-d) \times (n-d)$ minors of the matrix

$$\operatorname{Jac}(P_1, \ldots, P_r)(\mathbf{a}) = \begin{pmatrix} \frac{\partial P_1}{\partial X_1}(\mathbf{a}) & \cdots & \frac{\partial P_1}{\partial X_n}(\mathbf{a}) \\ \vdots & & \vdots \\ \frac{\partial P_r}{\partial X_1}(\mathbf{a}) & \cdots & \frac{\partial P_r}{\partial X_n}(\mathbf{a}) \end{pmatrix}.$$

This is closed.

We next assume that V is irreducible and prove that $V_{\text{sing}} \neq V$. According to 3.36 and 3.37 some nonempty open affine subset of V is isomorphic to a nonempty open affine subset of an irreducible hypersurface in $\mathbb{A}^{d+1}$, and so we may suppose that V itself is an irreducible hypersurface in $\mathbb{A}^{d+1}$, say, equal to the zero set of the nonconstant irreducible polynomial $F(X_1, \ldots, X_{d+1})$. The singular locus is the set of common zeros of the polynomials

$$F, \frac{\partial F}{\partial X_1}, \ldots, \frac{\partial F}{\partial X_{d+1}},$$

and so it will be proper unless the polynomials $\partial F/\partial X_i$ are identically zero on V. As in the proof of 4.7, if $\partial F/\partial X_i$ is identically zero on $V(F)$, then it is the zero polynomial, and so F is a polynomial in $X_1, \ldots, X_{i-1}, X_{i+1}, \ldots X_{d+1}$ (characteristic zero) or in $X_1, \ldots, X_i^p, \ldots, X_{d+1}$ (characteristic p). Therefore, if the singular locus equals V, then F is constant (characteristic 0) or a pth power (characteristic p), which contradicts the hypothesis.

We now consider the general case, in which V has irreducible components $V_1, \ldots, V_r$. Each of $V_i \cap V_j$ is a proper closed subset of V_i, and we have proved that $(V_i)_{\text{sing}}$ is a proper closed subset of V_i. It follows that $V_i \cap V_{\text{sing}}$ is a finite union of proper closed subsets of V_i, and so it is proper and closed in V_i. Hence the points of V_i that are nonsingular on V form a nonempty open (hence dense) subset of V_i. □

COROLLARY 4.38. *If V is irreducible, then*

$$\dim V = \min_{P \in V} \dim T_P(V).$$

PROOF. We know that $\dim T_P(V) \geq \dim V$, with equality if and only if P is nonsingular. As there exists a nonsingular P, $\dim V$ is the minimum value of $\dim T_P(V)$. □

This formula can be useful in computing the dimension of a variety.

COROLLARY 4.39. *An irreducible algebraic variety is nonsingular if and only if the tangent spaces $T_P(V)$, $P \in V$, have constant dimension.*

PROOF. The constant dimension is the dimension of V, and so all points are nonsingular. □

COROLLARY 4.40. *Every variety on which a group acts transitively by regular maps is nonsingular.*

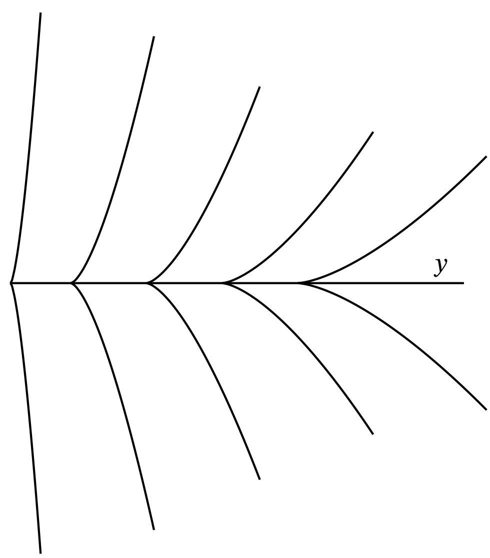
PROOF. The group must act by isomorphisms, and so the tangent spaces have constant dimension. □

In particular, every group variety (see p. 110) is nonsingular.

Examples

4.41. For the surface $Z^3 = XY$, the only singular point is $(0,0,0)$. The tangent cone at $(0,0,0)$ has equation $XY = 0$, and so it is the union of two planes intersecting in the z-axis.

4.42. For the surface $V: Z^3 = X^2Y$, the singular locus is the line $X = 0 = Z$, i.e., the y-axis. The singularity at $(0,0)$ is very bad: for example, it lies in the singular set of the singular set.[3] The intersection of the surface with the surface $Y = c$ is the cuspidal curve $X^2 = Z^3/c$. In the picture, each curve lies in a plane $Y = c$ orthogonal to the y-axis, and has its cusp on the y-axis.



4.43. 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 o to the

[3] In fact, it belongs to the worst class of singularities (sx2848895, KReiser).

singular point 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, V and W are not isomorphic.

i. Nonsingularity and regularity

THEOREM 4.44. *Let P be a point on an irreducible variety V. Every 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 4.36 shows that P is an irreducible component of $V(f_1, \ldots, f_r)$ in some open neighbourhood U of P. Therefore 3.45 shows that $0 \geq d - r$, and so $r \geq d$. The rest of the statement has already been noted. □

COROLLARY 4.45. *A point P on a variety V is nonsingular if and only if $\mathcal{O}_P$ is regular.*

PROOF. If P lies on a single irreducible component of V, then this is a restatement of the second part of the theorem. According to CA, 22.3, a regular local ring is an integral domain. If P lies on more than one irreducible component of a V, then P is not nonsingular (by definition) and $\mathcal{O}_P$ is not regular because not an integral domain (3.14). □

j. Examples of tangent spaces

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.

4.46. A matrix $I + \varepsilon A$ has inverse $I - \varepsilon A$ in $M_n(k[\varepsilon])$, and so lies in $\mathrm{GL}_n(k[\varepsilon])$. In fact,

$$\begin{aligned} T_e(\mathrm{GL}_n) &= \{I + \varepsilon A \mid A \in M_n\} \\ &\simeq M_n(k). \end{aligned}$$

4.47. On expanding $\det(I + \varepsilon A)$ as a sum of signed products and using that $\varepsilon^2 = 0$, we find that

$$\det(I + \varepsilon A) = I + \varepsilon \mathrm{trace}(A).$$

Hence

$$\begin{aligned} T_e(\mathrm{SL}_n) &= \{I + \varepsilon A \mid \mathrm{trace}(A) = 0\} \\ &\simeq \{A \in M_n(k) \mid \mathrm{trace}(A) = 0\}. \end{aligned}$$

4.48. Assume that the characteristic $\neq 2$, and let O_n be the 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 $\det\colon \mathrm{O}_n \to \{\pm 1\}$, 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

$$T_e(\mathrm{O}_n) = T_e(\mathrm{SO}_n) = \{I + \varepsilon A \in M_n(k[\varepsilon]) \mid A \text{ is skew-symmetric}\}$$
$$\simeq \{A \in M_n(k) \mid A \text{ is skew-symmetric}\}.$$

ASIDE 4.49. On the tangent space $T_e(\mathrm{GL}_n) \simeq M_n$ of GL_n, there is a bracket operation

$$[M,N] \overset{\text{def}}{=} MN - NM$$

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 (it has an intrinsic definition in terms of left invariant derivations), and $G \rightsquigarrow \mathrm{Lie}(G)$ is a functor from the category of linear group varieties to that of Lie algebras.

This functor is not fully faithful, for example, every étale homomorphism $G \to G'$ defines an isomorphism $\mathrm{Lie}(G) \to \mathrm{Lie}(G')$, but it is nevertheless very useful.

Assume that k has characteristic zero. A connected group variety 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 $\mathrm{diag}(\zeta, \ldots, \zeta)$ with $\zeta^n = 1$, 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 group varieties and the set of isomorphism classes of Lie algebras. The classification of semisimple group varieties can be deduced from that of semisimple Lie algebras and a study of the finite coverings of semisimple group varieties arXiv:0705.1348— this is quite similar to the relation between Lie groups and Lie algebras.

Exercises

4-1. 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 that the characteristic is not 2).

4-2. 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 $\sum a_iX_i = d$ 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 $H \supset T_P(V)$?

4-3. Given a smooth point on a variety and a tangent vector at the point, show that there is a smooth curve passing through the point with the given vector as its tangent vector (see mo111467).

4-4. Let P and Q be points on varieties V and W. Show that

$$T_{(P,Q)}(V \times W) \simeq T_P(V) \oplus T_Q(W).$$

4-5. 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 cannot be embedded in $\mathbb{A}^{n-1}$).

4-6. Let I be the $n \times n$ identity matrix, and let J be the matrix $\left(\begin{smallmatrix} 0 & I \\ -I & 0 \end{smallmatrix}\right)$. 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.

4-7. 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.

4-8. Show that the cone $X^2 + Y^2 = Z^2$ is a normal variety, even though the origin is singular (characteristic $\neq 2$). See p. 177.

4-9. 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?

4-10. Let W be a finite-dimensional k-vector space, and let $R_W = k \oplus W$ endowed with the k-algebra structure for which $W^2 = 0$. Let V be an affine algebraic variety over k. Show that the elements of $V(R_W) \stackrel{\text{def}}{=} \mathrm{Hom}_{k\text{-algebra}}(k[V], R_W)$ are in natural one-to-one correspondence with the pairs (P, t) with $P \in V$ and $t \in W \otimes T_P(V)$ (cf. Mumford 1966b, p. 25).

Chapter 5

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 $\mathbb{R}^n$. We require both to satisfy a separation axiom.

a. Algebraic prevarieties

As motivation, recall the following definitions.

DEFINITION 5.1. (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. 3.2).

(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. 3.3).

(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 of holomorphic functions on an open subset of $\mathbb{C}^n$ (cf. 3.4).

These definitions are easily seen to be equivalent to the more classical definitions in terms of charts and atlases (when stated correctly). Sometimes additional conditions are imposed on V, for example, that it is connected or have a countable base of open subsets.

DEFINITION 5.2. An ***algebraic prevariety over*** k is a k-ringed space $(V, \mathcal{O}_V)$ such that V is quasi-compact and every point of V has an open neighbourhood U for which $(U, \mathcal{O}_V|U)$ is isomorphic to the ringed space of regular functions on an algebraic set over k.

Thus, a k-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.

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 5.3. (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

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

(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.

b. Regular maps

In each of the examples (5.1a,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 k-ringed spaces. In other words, a continuous map $\varphi: V \to W$ is regular if $f \mapsto f \circ \varphi$ sends a regular function on an open subset U of W to a regular function on $\varphi^{-1}(U)$. 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 5.4. *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. □

REMARK 5.5. 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 4).

(b) The inverse function theorem fails in our context: a regular map that induces an isomorphism on the tangent space at a point P need not induce an isomorphism in a neighbourhood of P. However, see 5.55 below.

c. Algebraic varieties

In the study of topological manifolds, the Hausdorff condition eliminates such bizarre possibilities as the line with the origin doubled in which a sequence tending to the origin has two limits (see 5.9 below).

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 $Z \to V$ that agree on a dense subset U of Z, then they should agree on the whole of Z.[1] 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 5.6. *Let $\varphi_1, \varphi_2 : Z \rightrightarrows V$ regular maps of affine algebraic varieties. 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 5.7. An algebraic prevariety V is said to be ***separated*** if it satisfies the separation axiom:

> for any 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.

An ***algebraic variety*** over k is a separated algebraic prevariety over k.[2]

[1] Let $z \in Z$, and let $z = \lim u_n$ with $u_n \in U$. Then $\varphi_1(z) = \lim \varphi_1(u_n)$ because φ_1 is continuous, and $\lim \varphi_1(u_n) = \lim \varphi_2(u_n) = \varphi_2(z)$.

[2] These are sometimes called "algebraic varieties in the sense of FAC" (see the footnote p. 9). For Grothendieck, they are the "espaces algébriques de Serre" (EGA I, Appendice); alternatively, they are reduced separated schemes of finite type over k (assumed to be algebraically closed) with the nonclosed points omitted — we explain this in Chapter 10. Some authors use a more restrictive definition — they may require a variety to be connected, irreducible, or quasi-projective — usually because their foundations do not allow for a more flexible definition.

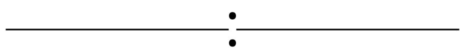
PROPOSITION 5.8. *Let φ_1 and φ_2 be regular maps $Z \rightrightarrows V$ from an algebraic prevariety Z to a variety V. The subset of Z on which φ_1 and φ_2 agree is closed.*

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 5.9. (The affine line with the origin doubled.)[3] 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,



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 $\mathbb{A}^1$.

5.10. When V is irreducible, all the rings attached to it have a common field of fractions $k(V)$ (see p. 115 below). Moreover,

$$\begin{aligned} \mathcal{O}_P &= \{g/h \in k(V) \mid h(P) \neq 0\} \\ \mathcal{O}_V(U) &= \bigcap \{\mathcal{O}_V(U') \mid U' \subset U,\ U' \text{ open affine}\} \\ &= \bigcap \{\mathcal{O}_P \mid P \in U\}. \end{aligned}$$

d. 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.

[3]This is the algebraic analogue of the standard example of a non Hausdorff topological space. Let $\mathbb{R}^*$ denote the real line with the origin removed but with two points $a_1 \neq a_2$ added. The subspace $\mathbb{R} \smallsetminus \{0\}$ has its usual topology, and, for $i = 1, 2$, a base for the neighbourhoods of a_i is formed by the sets $(U \smallsetminus \{0\}) \cup \{a_i\}$ with U an open neighbourhood of 0 in $\mathbb{R}$. Then $\mathbb{R}^*$ is not Hausdorff because a_1 and a_2 cannot be separated by disjoint open sets. Every sequence that converges to a_1 also converges to a_2. For example, $1/n$ converges to both a_1 and a_2.

PROPOSITION 5.11. *For an algebraic variety V and an affine k-algebra A, there is a canonical bijection*

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

Let V be an algebraic variety such that $\Gamma(V, \mathcal{O}_V)$ is an affine k-algebra. The 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: every regular map from V to an affine algebraic variety U factors uniquely through φ:

$$\begin{array}{ccc} V & \xrightarrow{\varphi} & \mathrm{Spm}(\Gamma(V, \mathcal{O}_V)) \\ & \searrow & \downarrow{\scriptstyle \exists!} \\ & & U. \end{array}$$

In particular, we recover 3.24: for affine k-algebras A and B,

$$\mathrm{Hom}_k(A, B) \simeq \mathrm{Mor}(\mathrm{Spm}(B), \mathrm{Spm}(A)).$$

Let Var_k denote the category of algebraic varieties over k and regular maps. The functor $A \rightsquigarrow \mathrm{Spm}\,(A)\colon \mathsf{Aff}_k \to \mathsf{Var}_k$ defines a contravariant equivalence of the first category with the subcategory of the second whose objects are the affine algebraic varieties.

For a nonaffine algebraic variety V, $\Gamma(V, \mathcal{O}_V)$ need not be finitely generated as a k-algebra.

e. Subvarieties

Let $(V, \mathcal{O}_V)$ be an algebraic variety over k.

Open subvarieties

Let U be an open subset of V. Then U is a union of open affines, and it follows that $(U, \mathcal{O}_V|U)$ is a variety, called an ***open subvariety*** 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 varieties.

EXAMPLE 5.12. The open subspace $U = \mathbb{A}^2 \smallsetminus \{(0,0)\}$ of $\mathbb{A}^2$ becomes an algebraic variety when endowed with the sheaf $\mathcal{O}_{\mathbb{A}^2}|U$.

Closed subvarieties

Every closed subset Z of V has a canonical structure of an algebraic variety. Define a function f on an open subset U of Z to be regular if, for every $P \in U$, there exists a germ (U', f') of a regular function at P on V such that $f'|U' \cap U = f|U' \cap U$. This defines a ringed structure $\mathcal{O}_Z$ on Z. To show that $(Z, \mathcal{O}_Z)$ is a variety it suffices to check that, for every open affine $U \subset V$, the ringed space $(U \cap Z, \mathcal{O}_Z|U \cap Z)$ is an affine algebraic variety, but this is an easy exercise (Exercise 3-2 to be precise). Such a pair $(Z, \mathcal{O}_Z)$ is called a ***closed subvariety*** 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 varieties.

Subvarieties

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 variety V has a canonical structure of an algebraic variety. Write W as the intersection $W = U \cap Z$ of an open and a closed subset. Now Z is a closed subvariety of V and W is an open subvariety of Z. Alternatively, U is an open subvariety of V and W is closed subvariety of U. Either way, the structure on W is characterized by having the following property: the inclusion map $W \hookrightarrow V$ is regular, and a map from a variety to W is regular if and only if it is regular as a map to V.

With this structure, W is called a ***subvariety*** of V. A regular map $\varphi\colon W \to V$ is an ***immersion*** if it induces an isomorphism of W onto a subvariety of V. Every immersion is the composite of an open immersion with a closed immersion (in both orders).

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. Note that every quasi-affine variety is an open subvariety of some affine variety.

Application

PROPOSITION 5.14. *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 (5.8), and so must be the whole of the Z if it contains a dense subset.

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 that 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. Then $\bar{S}$ 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. □

f. Prevarieties obtained by patching

PROPOSITION 5.15. *Suppose that the set V is a finite union $V = \bigcup_{i\in I} V_i$ of subsets V_i and that each V_i is equipped with ringed space structure. If 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 is the same as 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. □

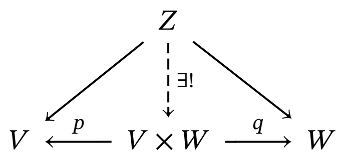
Clearly, the V_i may be separated without V being separated (see, for example, 5.9). In 5.29 below, we give a condition on an open affine covering of a prevariety sufficient to ensure that the prevariety is separated.

g. 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



commute. In other words, the triple 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.

For example, the product of two sets (in the category of sets) is the usual cartesian product of the sets, and the product of two topological spaces (in the category of topological spaces) is the product of the underlying 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. 3.28). 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.

There can be at most one such structure on the set $V \times W$. We first consider the affine case.

Products of affine varieties

EXAMPLE 5.16. 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

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

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 (3.25), 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 5.17. *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_j is a linear combination of the remaining b_i, say, $b_n=\sum_{i=1}^{n-1}c_ib_i$, $c_i\in k$, then, using the bilinearity of $\otimes$, we find that

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

Thus we may suppose that in the original expression of α, the b_i 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 $\sum\bar{a}_ib_i$ of α under this homomorphism is a nilpotent element of B, and hence is zero (because B is reduced). As the b_i are linearly independent over k, this means that the $\bar{a}_i$ are all zero. Thus, the a_i lie in all maximal ideals $\mathfrak{m}$ of A, and so are zero (see 2.18). 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 $\{b_1, b_2, ...\}$ and $\{b_1', b_2', ...\}$ each linearly independent over k. For each maximal ideal $\mathfrak{m}$ of A, we know $(\sum \bar{a}_i b_i)(\sum \bar{a}_i' b_i') = 0$ in B, and so either $(\sum \bar{a}_i b_i) = 0$ or $(\sum \bar{a}_i' b_i') = 0$. Thus either all the $a_i \in \mathfrak{m}$ or all the $a_i' \in \mathfrak{m}$. This shows that

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

As spm(A) is irreducible (see 2.27), it follows that spm(A) equals either $V(a_1, \dots, a_m)$ or $V(a_1', \dots, a_n')$. In the first case $\alpha = 0$, and in the second $\alpha' = 0$. □

REMARK 5.18. The proof of 5.17 fails when k is not algebraically closed, because then $A/\mathfrak{m}$ may be a finite extension of k over which the b_i become linearly dependent. The following examples show that the statement of 5.17 also fails in this case.

(a) Suppose that 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 E 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 E is large enough to split f, say, $f(X) = \prod_i (X - \alpha_i)$ with $\alpha_i \in E$. Because K/k is separable, the α_i are distinct, and so

$$\begin{aligned}E \otimes_k K &\simeq E[X]/(f(X)) && \text{(1.58(b))} \\ &\simeq \prod E[X]/(X - \alpha_i), && \text{(1.1)}\end{aligned}$$

which 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 5.19. The ***product*** of the affine varieties V and W is

$$(V \times W, \mathcal{O}_{V \times W}) = \operatorname{Spm}(k[V] \otimes_k k[W])$$

with the projection maps $p, q\colon V \times W \to V, W$ defined by the homomorphisms

$$\begin{aligned}f &\mapsto f \otimes 1\colon k[V] \to k[V] \otimes_k k[W] \\ g &\mapsto 1 \otimes g\colon k[W] \to k[V] \otimes_k k[W].\end{aligned}$$

PROPOSITION 5.20. *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 5.17(a), and the second statement then follows by the argument on p. 106.

(b) This follows from 5.17(b) and 2.27. □

COROLLARY 5.21. *Let* V *and* W *be affine varieties. For every 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 5.20 implies that φ is regular when restricted to any open affine of T, which implies that it is regular on T. □

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 5.22. (a) It follows from 1.57 that $\mathbb{A}^{m+n}$ endowed with the projection maps

$$\mathbb{A}^m \xleftarrow{p} \mathbb{A}^{m+n} \xrightarrow{q} \mathbb{A}^n, \qquad \begin{cases} p(a_1, \dots, a_{m+n}) = (a_1, \dots, a_m) \\ q(a_1, \dots, a_{m+n}) = (a_{m+1}, \dots, a_{m+n}), \end{cases}$$

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

(b) It follows from 5.16 that

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

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

☡ When V and W have dimension > 0, the topology on $V \times W$ is strictly finer than product topology. For example, for the product topology on $\mathbb{A}^2 = \mathbb{A}^1 \times \mathbb{A}^1$, every proper closed subset is contained in a finite union of vertical and horizontal lines, whereas $\mathbb{A}^2$ has many more closed subsets (see 2.68).

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 (5.15). 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 5.23. *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 $\varphi\colon T \to V \times W$ be a map of sets such that $p\circ\varphi$ and $q\circ\varphi$ are regular. Then 5.21 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. □

PROPOSITION 5.24. *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. □

PROPOSITION 5.25. *If V and W are connected, then so also is $V \times W$.*

PROOF. For $v_0 \in V$, we have continuous maps

$$W \simeq v_0 \times W \xhookrightarrow{\text{closed}} V \times W.$$

Similarly, for $w_0 \in W$, we have continuous maps

$$V \simeq V \times w_0 \xhookrightarrow{\text{closed}} V \times W.$$

The images of V and W in $V \times W$ intersect in (v_0, w_0) and are connected, which shows that (v_0, w) and and (v, w_0) lie in the same connected component of $V \times W$ for all $v \in V$ and $w \in W$. Since v_0 and w_0 were arbitrary, this shows that any two points lie in the same connected component. □

Group varieties

A ***group variety*** is an algebraic variety G together with a group structure m (map of sets $G \times G \to G$ satisfying the group axioms) such that the maps

$$m\colon G \times G \to G, \quad \text{inv}\colon G \to G, \quad e\colon \mathbb{A}^0 \to G$$

are regular. A ***homomorphism*** of group varieties is a regular map that is also a homomorphism of groups.

The algebraic variety,

$$\begin{cases} \mathrm{SL}_n = \operatorname{Spm} \dfrac{k[X_{11}, X_{12}, \ldots, X_{nn}]}{(\det(X_{ij}) - 1)} \\ \mathrm{SL}_n(k) = \{M \in M_n(k) \mid \det M = 1\} \end{cases}$$

becomes a group variety when endowed with its usual group structures. Matrix multiplication

$$(a_{ij}) \cdot (b_{ij}) = (c_{ij}), \quad c_{ij} = \textstyle\sum_{l=1}^{n} a_{il} b_{lj},$$

is given by polynomials, and Cramer's rule gives an explicit expression of the entries of A^{-1} as polynomials in the entries of A. The only affine group varieties of dimension 1 over k are

$$\mathbb{G}_m = \operatorname{Spm} k[X, X^{-1}] \quad \text{and} \quad \mathbb{G}_a = \operatorname{Spm} k[X].$$

Every finite group N can be made into a group variety by setting

$$N = \operatorname{Spm}(A)$$

with A the k-algebra of all maps $f\colon N \to k$.

h. The separation axiom revisited

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 an open neighbourhood $U \times U'$ such that $(U \times U') \cap \Delta = \emptyset$. In other words, if x and y are distinct points in V, then there are open neighbourhoods U and U' of x and y respectively such that $U \cap U' = \emptyset$. 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 5.26. *An algebraic prevariety V is separated if and only if Δ_V is closed.*[4]

PROOF. We shall use the criterion 5.8: V is separated if and only if regular regular maps to V agree on a closed subset of their source.

Suppose that Δ_V is closed. 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 components φ_1 and φ_2 are regular (definition of a product). In particular, it is continuous, and so $(\varphi_1,\varphi_2)^{-1}(\Delta_V)$ is closed, but this is exactly the subset on which φ_1 and φ_2 agree.

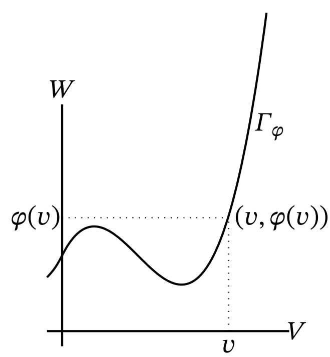
Conversely, Δ_V is the set on which the two projection maps $V \times V \to V$ agree, and so it is closed if V is separated. □

COROLLARY 5.27. *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 (5.6). □

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

$$\{(v, \varphi(v)) \in V \times W \mid v \in V\}.$$



COROLLARY 5.28. *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

$$(v,w) \mapsto (\varphi(v), w)\colon V \times W \to W \times W$$

[4] Thus does not contradict the fact that V is not Hausdorff because the Zariski topology on $V \times V$ is not the product topology.

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 5.29. *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;

(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_V is closed then $U \cap U'$ affine,
(ii) when $U \cap U'$ is affine,

$$(U \times U') \cap \Delta_V \text{ is closed} \iff k[U] \otimes_k k[U'] \to k[U \cap U'] \text{ is surjective.}$$

Assume (a); then these statements imply (b). Assume that the condition in (b) holds for the sets in some 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 $(U \times U') \cap \Delta_V$ 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. Now 5.28 implies that $U \cap U'$ is affine.

Proof of (ii): Assume that $U \cap U'$ is affine. Then

$$\begin{aligned} &(U \times U') \cap \Delta_V \text{ is closed in } U \times U' \\ &\iff v \mapsto (v, v) \colon U \cap U' \to U \times U' \text{ is a closed immersion} \\ &\iff k[U \times U'] \to k[U \cap U'] \text{ is surjective (3.34).} \end{aligned}$$

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 5.30. (a) Let $V = \mathbb{P}^1$, and let U_0 and U_1 be the standard open subsets (see 5.3). Then $U_0 \cap U_1 = \mathbb{A}^1 \smallsetminus \{0\}$, and the maps on rings corresponding to the inclusions $U_0 \cap U_1 \hookrightarrow U_i$ are

$$f(X) \mapsto f(X) \colon k[X] \to k[X, X^{-1}]$$
$$f(X) \mapsto f(X^{-1}) \colon k[X] \to k[X, X^{-1}].$$

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 5.9), and let U and U' be the upper and lower copies of $\mathbb{A}^1$ in V. Then $U \cap U' = (\mathbb{A}^1 \smallsetminus 0)$ is affine, but the maps on rings corresponding to the inclusions $U \cap U' \hookrightarrow U_i$ are

$$X \mapsto X \colon k[X] \to k[X, X^{-1}]$$
$$X \mapsto X \colon k[X] \to k[X, X^{-1}].$$

Thus the sets U and U' fail the condition in (b) (and V is not separated).

(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 3.33).

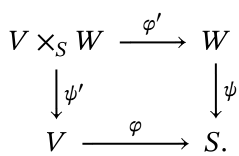
i. Fibred products

Let $\varphi \colon V \to S$ and $\psi \colon W \to S$ be regular maps of algebraic varieties. The set

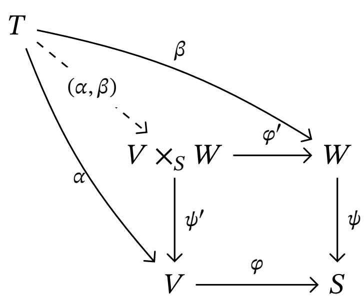
$$V \times_S W \stackrel{\text{def}}{=} \{(v, w) \in V \times W \mid \varphi(v) = \psi(w)\}$$

is closed in $V \times W$, because it is the set where $\varphi \circ p$ and $\psi \circ q$ agree, and so it has a canonical structure of an algebraic variety (see p. 104). The algebraic variety $V \times_S W$ is called the ***fibred product*** of V and W over S. Note that if S consists of a single point, then $V \times_S W = V \times W$.

Writing φ' for the map $(v, w) \mapsto w \colon V \times_S W \to W$ and ψ' for $(v, w) \mapsto v \colon V \times_S W \to V$, we get a commutative diagram:



The system $(V \times_S W, \varphi', \psi')$ has the following universal property: for any regular maps $\alpha \colon T \to V$, $\beta \colon T \to W$ such that $\varphi\alpha = \psi\beta$, there is a unique regular map $(\alpha, \beta) \colon T \to V \times_S W$ such that the following diagram



commutes. In other words,

$$\mathrm{Hom}(T, V \times_S W) \simeq \mathrm{Hom}(T, V) \times_{\mathrm{Hom}(T,S)} \mathrm{Hom}(T, W).$$

Indeed, there is a unique such map of sets, namely, $t \mapsto (\alpha(t), \beta(t))$, which is regular because it is as a map into $V \times W$.

The map φ' in the above diagrams 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 5.31. If $f : V \to S$ is a regular map and U is a subvariety of S, then $U \times_S V$ is the inverse image of U in V, $\varphi^{-1}(U) = U \times_S V$.

Notes

5.32. 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

$$\mathrm{Spm}(A) \times_{\mathrm{Spm}(R)} \mathrm{Spm}(B) \overset{??}{=} \mathrm{Spm}(A \otimes_R B).$$

This is true if $A \otimes_R B$ is an affine k-algebra, but in general it may have nonzero nilpotent elements. For example, let k have characteristic p, let $R = k[X]$, and consider the $k[X]$-algebras

$$\begin{cases} k[X] \to k, & X \mapsto a \\ k[X] \to k[X], & X \mapsto X^p. \end{cases}$$

Then

$$A \otimes_R B \simeq k \otimes_{k[X^p]} k[X] \simeq k[X]/(X^p - a),$$

which contains the nilpotent element $x - a^{1/p}$.

The correct statement is

$$\mathrm{Spm}(A) \times_{\mathrm{Spm}(R)} \mathrm{Spm}(B) \simeq \mathrm{Spm}(A \otimes_R B/\mathfrak{N}), \tag{25}$$

where $\mathfrak{N}$ is the ideal of nilpotent elements in $A \otimes_R B$. To prove this, note that for any algebraic variety T,

$$\begin{aligned} \mathrm{Mor}(T, \mathrm{Spm}(A \otimes_R B/\mathfrak{N})) &\simeq \mathrm{Hom}(A \otimes_R B/\mathfrak{N}, \mathcal{O}_T(T)) && (5.11) \\ &\simeq \mathrm{Hom}(A \otimes_R B, \mathcal{O}_T(T)) \\ &\simeq \mathrm{Hom}(A, \mathcal{O}_T(T)) \underset{\mathrm{Hom}(R,\mathcal{O}_T(T))}{\times} \mathrm{Hom}(B, \mathcal{O}_T(T)) \\ &\simeq \mathrm{Mor}(T, \mathrm{Spm}(A)) \underset{\mathrm{Mor}(T,\mathrm{Spm}(R))}{\times} \mathrm{Mor}(T, \mathrm{Spm}(B)) && (5.11). \end{aligned}$$

For the second isomorphism we used that the ring $\mathcal{O}_T(T)$ is reduced, and for the third isomorphism, we used the universal property of $A \otimes_R B$.

5.33. Fibred products exist also for prevarieties. In this case, $V \times_S W$ is only locally closed in $V \times W$.

ASIDE 5.34. Fibred products may differ depending on whether we are working in the category of algebraic varieties or algebraic schemes. For example,

$$\mathrm{Spec}(A) \times_{\mathrm{Spec}(R)} \mathrm{Spec}(B) \simeq \mathrm{Spec}(A \otimes_R B)$$

in the category of schemes. Consider the map $x \mapsto x^2 : \mathbb{A}^1 \xrightarrow{\varphi} \mathbb{A}^1$ (see 5.49). The fibre $\varphi^{-1}(a)$ consists of two points if $a \neq 0$, and one point if $a = 0$. Thus $\varphi^{-1}(0) = \mathrm{Spm}(k[X]/(X))$. However, the scheme-theoretic fibre is $\mathrm{Spec}(k[X]/(X^2))$, which reflects the fact that 0 is "doubled" in the fibre over 0. This will be explained in Chapter 10.

j. Dimension

Recall p. 45 that, in an irreducible topological space, every nonempty open subset is dense and irreducible.

Let V be an irreducible algebraic variety V, and let U and U' be nonempty open affines in V. Then $U \cap U'$ is also a nonempty open affine (5.29), which is dense in U, and so the restriction map $\mathcal{O}_V(U) \to \mathcal{O}_V(U \cap U')$ is injective. Therefore

$$k[U] \subset k[U \cap U'] \subset k(U),$$

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 $k[U']$.[5] Thus, attached to V there is a field $k(V)$, called the ***function field of*** V or ***the field of rational functions on*** V, which is the field of fractions of $k[U]$ for any open affine U in V. 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 5.35. *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 and y 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 1.63), and so $\dim(V) = d$ and $\dim(W) = e$. Now[6]

$$k[V \times W] \overset{\text{def}}{=} k[V] \otimes_k k[W] \supset k[x_1, \ldots, x_d] \otimes_k k[y_1, \ldots, y_e],$$

which is a polynomial ring in the symbols $x_1 \otimes 1, \ldots, x_d \otimes 1, 1 \otimes y_1, \ldots, 1 \otimes y_e$ (see 1.57). In particular, the elements $x_1 \otimes 1, \ldots, x_d \otimes 1, 1 \otimes y_1, \ldots, 1 \otimes y_e$ are algebraically independent in $k[V] \otimes_k k[W]$. Obviously $k[V \times W]$ is generated as a k-algebra by the elements $x_i \otimes 1$, $1 \otimes y_j$, $1 \leq i \leq m$, $1 \leq j \leq n$, 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 2.31), 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).

---

[5]If A is an integral domain and f is a nonzero element of A, then $A \subset A_f \subset \mathrm{FF}(A)$ and A and A_f have the same field of fractions. Thus $k(U)$ does not change when we shrink U.

[6]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.

PROPOSITION 5.36. *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 Theorem 5.29, we saw 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 3.45. □

REMARK 5.37. (a) The subvariety

$$\begin{cases} X^2 + Y^2 & = Z^2 \\ \quad\quad Z & = 0 \end{cases}$$

of $\mathbb{A}^3$ is the curve $X^2 + Y^2 = 0$, which is the pair of lines $Y = \pm iX$ if $k = \mathbb{C}$; in particular, the codimension is 2. Note however, that real locus is $\{(0,0)\}$, which has codimension 3. Thus, Proposition 5.36 becomes false if one looks only at real points (and the pictures we draw can mislead).

(b) Proposition 5.36 becomes 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,

$$\begin{aligned} Z &: X_2 = 0 = X_4; \qquad & Z &= \{(*, 0, *, 0)\} \\ Z' &: X_1 = 0 = X_3; \qquad & Z' &= \{(0, *, 0, *)\} \end{aligned}$$

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 5.36 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.

k. Dominant maps

As in the affine case, a regular map $\varphi : V \to W$ is said to be ***dominant*** if its image is dense in W.

Let $\varphi : V \to W$ be a dominant map. For any open subset U of W, the map

$$f \mapsto f \circ \varphi : \Gamma(U, \mathcal{O}_W) \to \Gamma(\varphi^{-1}(U), \mathcal{O}_V) \tag{*}$$

is injective. Now assume that V and W are irreducible. On passing to the direct limit in (*), we get a homomorphism of fields

$$k(W) \to k(V).$$

If U_V and U_W are open affines of V and W such that $\varphi(U_V) \subset U_W$, then

$$k[U_W] \to k[U_V]$$

is injective, so $\varphi|U_V : U_V \to U_W$ is dominant. An elementary, but nontrivial, argument shows that $\varphi(V)$ contains a dense open subset of W (see Theorem 9.1 below).

l. Rational maps; birational equivalence

Loosely speaking, a rational map from a variety V to a variety W is a regular map from a dense open subset of V to W, and a birational map is a rational map admitting a rational inverse.

Let V and W be varieties over k, and consider pairs (U, φ_U), where U is a dense open subset of V and φ_U is a regular map $U \to W$. Two such pairs (U, φ_U) and $(U', \varphi_{U'})$ are said to be ***equivalent*** if φ_U and $\varphi_{U'}$ agree on $U \cap U'$. An equivalence class of pairs is called a ***rational map*** $\varphi : V \dashrightarrow W$. A rational map φ is said to be ***defined*** at a point v of V if $v \in U$ for some $(U, \varphi_U) \in \varphi$. The set U_1 of v at which φ is defined is open, and there is a regular map $\varphi_1 : U_1 \to W$ such that $(U_1, \varphi_1) \in \varphi$ — clearly, $U_1 = \bigcup_{(U,\varphi_U)\in\varphi} U$ and we can define φ_1 to be the regular map such that $\varphi_1|U = \varphi_U$ for all $(U, \varphi_U) \in \varphi$. Hence, in the equivalence class, there is always a pair (U, φ_U) with U largest (and U is called "the open subvariety on which φ is defined").

PROPOSITION 5.38. *Let V and V' be irreducible varieties over k. A regular map $\varphi : U' \to U$ from an open subset U' of V' onto an open subset U of V defines a k-algebra homomorphism $k(V) \to k(V')$, and every such homomorphism arises in this way.*

PROOF. The first part of the statement is obvious, so let $k(V) \hookrightarrow k(V')$ be a k-algebra homomorphism. We use it to identify $k(V)$ with a subfield of $k(V')$. Let U (resp. U') be an open affine subset of V (resp. V'). Let $k[U] = k[x_1, \ldots, x_m]$. Each $x_i \in k(V')$, which is the field of fractions of $k[U']$, and so there exists a nonzero $d \in k[U']$ such that $dx_i \in k[U']$ for all i. After inverting d, i.e., replacing U' with basic open subset, we may suppose that $k[U] \subset k[U']$. The inclusion $k(V) \hookrightarrow k(V')$ is induced by the inclusion $k[U] \hookrightarrow k[U']$, hence by the corresponding dominant map $\varphi : U' \to U$. The image of φ contains an open subset U_0 of U (see the preceding subsection), and the restriction of φ to $\varphi^{-1}(U_0) \to U_0$ is the required map. □

A rational (or regular) map $\varphi : V \dashrightarrow W$ is ***birational*** if there exists a rational map $\varphi' : W \dashrightarrow V$ such that $\varphi' \circ \varphi = \mathrm{id}_V$ and $\varphi \circ \varphi' = \mathrm{id}_W$ as rational maps. Two varieties V and V' are ***birationally equivalent*** if there exists a birational map from one to the other. In this case, there exist dense open subsets U and U' of V and V' respectively such that $U \approx U'$.

PROPOSITION 5.39. *Two irreducible varieties V and V' are birationally equivalent if and only if their function fields are isomorphic over k.*

PROOF. Assume that $k(V) \approx k(V')$. We may suppose that V and W are affine, in which case the existence of $U \approx U'$ is proved in 3.36. This proves the "if" part, and the "only if" part is obvious. □

PROPOSITION 5.40. *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 Proposition 3.38, there exist $x_1, \ldots, x_d, x_{d+1} \in k(V)$ such that $k(V) = k(x_1, \ldots, x_d, x_{d+1})$. 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 $k(V) \approx k(H)$. □

m. Local study

Everything in Chapter 4, being local, extends mutatis mutandis, to general algebraic varieties.

5.41. The ***tangent space*** $T_P(V)$ at a point P on an algebraic variety V is the fibre of $V(k[\varepsilon]) \to V(k)$ over P. There are canonical isomorphisms

$$T_P(V) \simeq \mathrm{Der}_k(\mathcal{O}_P, k) \simeq \mathrm{Hom}_{k\text{-linear}}(\mathfrak{n}_P/\mathfrak{n}_P^2, k),$$

where $\mathfrak{n}_P$ is the maximal ideal of $\mathcal{O}_P$.

5.42. A point P on an algebraic variety V is ***nonsingular*** (or ***smooth***) if it lies on a single irreducible component W and $\dim T_P(V) = \dim W$. A point P is nonsingular if and only if the local ring $\mathcal{O}_P$ is regular. The singular points form a proper closed subvariety, called the ***singular locus***.

5.43. A variety is ***nonsingular*** (or ***smooth***) if every point is nonsingular.

n. Étale maps

An étale morphism is the analogue in algebraic geometry of a local isomorphism of manifolds in differential geometry, a covering of Riemann surfaces with no branch points in complex analysis, and an unramified extension in algebraic number theory.

DEFINITION 5.44. A regular map $\varphi\colon V \to W$ of smooth varieties is ***étale at a point*** P of V if the map $(d\varphi)_P\colon T_P(V) \to T_{\varphi(P)}(W)$ is an isomorphism; φ is ***étale*** if it is étale at all points of V.

Examples

5.45. A regular map

$$\varphi\colon \mathbb{A}^n \to \mathbb{A}^n, \quad a \mapsto (P_1(a_1, \ldots, a_n), \ldots, P_n(a_1, \ldots, a_n))$$

is étale at $\mathbf{a}$ if and only if rank $\mathrm{Jac}(P_1, \ldots, P_n)(\mathbf{a}) = n$, because the map on the tangent spaces has matrix $\mathrm{Jac}(P_1, \ldots, P_n)(\mathbf{a})$. Equivalent condition: $\det\left(\frac{\partial P_i}{\partial X_j}(\mathbf{a})\right) \neq 0$.

5.46. Let $V = \mathrm{Spm}(A)$ 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 $W = \mathrm{Spm}(A[X]/(f(X)))$, and consider the map $W \to V$ corresponding to the inclusion $A \hookrightarrow A[X]/(f)$. Thus,

$$\begin{array}{ccc} A[X]/(f) & \twoheadleftarrow & A[X] \\ & \nwarrow & \uparrow \\ & & A \end{array} \qquad \begin{array}{ccc} W & \hookrightarrow & V \times \mathbb{A}^1 \\ & \searrow & \downarrow \\ & & V. \end{array}$$

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 $A = k[X_1, \ldots, X_n]/\mathfrak{a}$, $\mathfrak{a} = (f_1, \ldots, f_r)$, so that

$$A[X]/(f) = k[X_1, \ldots, X_n]/(f_1, \ldots, f_r, f).$$

The tangent spaces to W and V at $(\mathbf{a}, b)$ and $\mathbf{a}$ respectively are the null spaces of the matrices

$$\begin{pmatrix} \frac{\partial f_1}{\partial X_1}(\mathbf{a}) & \ldots & \frac{\partial f_1}{\partial X_n}(\mathbf{a}) & 0 \\ \vdots & & \vdots & \\ \frac{\partial f_r}{\partial X_1}(\mathbf{a}) & \ldots & \frac{\partial f_r}{\partial X_n}(\mathbf{a}) & 0 \\ \frac{\partial f}{\partial X_1}(\mathbf{a}) & \ldots & \frac{\partial f}{\partial X_n}(\mathbf{a}) & \frac{\partial f}{\partial X}(\mathbf{a}, b) \end{pmatrix} \qquad \begin{pmatrix} \frac{\partial f_1}{\partial X_1}(\mathbf{a}) & \ldots & \frac{\partial f_1}{\partial X_n}(\mathbf{a}) \\ \vdots & & \vdots \\ \frac{\partial f_r}{\partial X_1}(\mathbf{a}) & \ldots & \frac{\partial f_r}{\partial X_n}(\mathbf{a}) \end{pmatrix}$$

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 every 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 (see p. 50).

5.47. Consider a dominant map $\varphi\colon V \to W$ of smooth affine varieties, corresponding to a map $A \to B$ of rings. Suppose that B can be written $B = A[Y_1, \ldots, Y_n]/(P_1, \ldots, P_n)$ (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.

5.48. The example in 5.46 is typical: in fact, locally, every étale map is of this form. Let $\varphi\colon V \to W$ be étale at $P \in V$. Then there exist a regular map $\varphi'\colon V' \to W'$ of affine varieties with $k[V'] = k[W'][X]/(f(X))$, and a commutative diagram

$$\begin{array}{ccccc} V & \hookleftarrow & U_P & \xrightarrow[\text{immersion}]{\text{open}} & V' \\ \downarrow{\scriptstyle \varphi} & & {\scriptstyle \text{étale}}\downarrow & & \downarrow{\scriptstyle \varphi'} \\ W & \hookleftarrow & U_Q & \xrightarrow[\text{immersion}]{\text{open}} & W' \end{array}$$

with U_P and U_Q open neighbourhoods of P and $Q \overset{\text{def}}{=} \varphi(P)$. See Milne 1980, I, 3.14, for the proof, which uses the affine case of Zariski's main theorem.

The failure of the inverse function theorem for the Zariski topology

5.49. 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

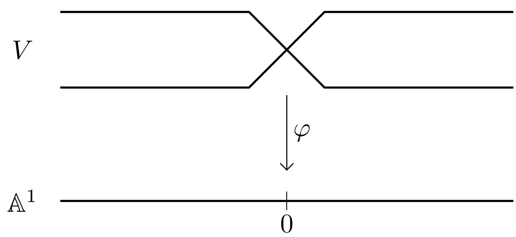
$$\varphi\colon \mathbb{A}^1 \to \mathbb{A}^1, \quad a \mapsto a^2,$$

and assume the characteristic is $\neq 2$. Then φ is étale at any point $a \neq 0$ because the Jacobian matrix is $(2X)$, which has rank one for $X = a \neq 0$ (alternatively, it is of the form 5.46 with $f(X) = X^2 - T$, where T is the coordinate function on $\mathbb{A}^1$, and $X^2 - a$ has distinct roots for $a \neq 0$). Nevertheless, I claim that there do not exist nonempty open subsets U and U' of $\mathbb{A}^1$ such that φ induces an isomorphism $U \to U'$. If there did, then φ would define an isomorphism $k[U'] \to k[U]$ and hence an isomorphism of the fields of fractions $k(\mathbb{A}^1) \to k(\mathbb{A}^1)$. But on the fields of fractions, φ corresponds to the map

$$k(X) \to k(X), \quad X \mapsto X^2,$$

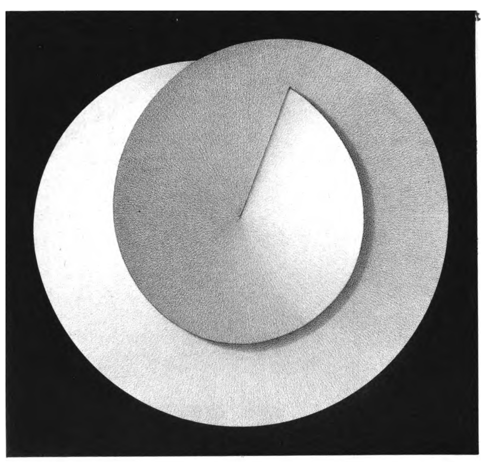
which is not an isomorphism.

5.50. Let V be the plane curve $Y^2 = X$ and φ the map $V \to \mathbb{A}^1$, $(x, y) \mapsto x$. Then φ is $2:1$ except over 0, and so we may view it schematically as



However, when viewed as a Riemann surface, $V(\mathbb{C})$ consists of two sheets joined at a single point O. As a point on the surface moves around O, it shifts from one sheet to the other. Thus the true picture is more complicated. To get a section to φ, it is necessary to remove a line in $\mathbb{C}$ from 0 to infinity, which is not closed for the Zariski topology.

It is not possible to fit the graph of the complex curve $Y^2 = X$ into 3-space, but the picture at right is an early depiction of it (from Neumann, Carl, Vorlesungen über Riemann's theorie der Abel'schen integrale, Leipzig: Teubner, 1865).



Die Riemann'sche Windungsfläche erster Ordnung.

Vergl. Seite 162–168, 213–214 und 218–221

Lith. Anst. v. M. Singer, Leipzig.

Étale maps of singular varieties

Using tangent cones, we can extend the notion of an étale morphism to singular varieties. A regular map $\varphi: V \to W$ induces a homomorphism $\mathrm{gr}(\mathcal{O}_{\varphi(P)}) \to \mathrm{gr}(\mathcal{O}_P)$ for each $P \in V$. We say that φ is ***étale*** at P if this is an isomorphism. Note that then there is an isomorphism of the geometric tangent cones $C_P(V) \to C_{\varphi(P)}(W)$, but the map on the geometric tangent cones may be an isomorphism without φ 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 $\varphi\colon A \to B$ induces an isomorphism on the graded rings if and only if it induces an isomorphism on the completions. Thus $\varphi\colon V \to W$ is étale at P if and only if the map $\hat{\mathcal{O}}_{\varphi(P)} \to \hat{\mathcal{O}}_P$ is an isomorphism. Now 5.53 shows that the choice of a system of local parameters $f_1, \ldots, f_d$ at a nonsingular point P determines an isomorphism $\hat{\mathcal{O}}_P \to k[[X_1, \ldots, X_d]]$.

We can rewrite this as follows: let $t_1, \ldots, t_d$ be a system of local parameters at a nonsingular point P; then there is a canonical isomorphism $\hat{\mathcal{O}}_P \to k[[t_1, \ldots, t_d]]$. For $f \in \hat{\mathcal{O}}_P$, the image of $f \in k[[t_1, \ldots, t_d]]$ 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: $a_n = f^{(n)}(a)/n!$.

PROPOSITION 5.51. *Let $\varphi\colon W \to V$ be a map of irreducible affine varieties. If $k(W)$ is a finite separable extension of $k(V)$, then φ is étale on a nonempty open subvariety of W.*

PROOF. After passing to open subvarieties, we may assume that W and V are nonsingular, and that $k[W] = k[V][X]/(f(X))$, where $f(X)$ is separable when considered as a polynomial in $k(V)$. Now the statement follows from 5.46. □

ASIDE 5.52. There is an old conjecture that every étale map $\varphi\colon \mathbb{A}^n \to \mathbb{A}^n$ is an isomorphism. When we write $\varphi = (P_1, \ldots, P_n)$, this becomes the statement:

$$\text{if } \det\left(\frac{\partial P_i}{\partial X_j}(\mathbf{a})\right) \text{ is never zero (for } \mathbf{a} \in k^n\text{), then } \varphi \text{ has an inverse.}$$

The condition, $\det\left(\frac{\partial P_i}{\partial X_j}(\mathbf{a})\right)$ never zero, implies that the polynomial $\det\left(\frac{\partial P_i}{\partial X_j}\right)$ is a nonzero constant (by the Nullstellensatz 2.11 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 the Wikipedia: JACOBIAN CONJECTURE.

o. Étale neighbourhoods

Let P be a nonsingular point on a variety V of dimension d. A ***system of local 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 the dual space to $T_P(V)$. We also say that $f_1, \ldots, f_n$ are ***local parameters at*** P.[7]

PROPOSITION 5.53. *Let $\{f_1, \ldots, f_d\}$ be a system of local 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 $(\tilde{f}_1, \ldots, \tilde{f}_d)\colon U \to \mathbb{A}^d$ is étale.*

[7] Sometimes also called local uniformizing parameters at P.

PROOF. Obviously, the f_i are represented by regular functions $\tilde{f}_i$ defined on a single open neighbourhood U' of P, which, because of 4.37, we can choose to be nonsingular. The map $\varphi = (\tilde{f}_1, \ldots, \tilde{f}_d)\colon U' \to \mathbb{A}^d$ is étale at P, because the dual map to $(d\varphi)_{\mathbf{a}}$ is $(dX_i)_o \mapsto (d\tilde{f}_i)_{\mathbf{a}}$. The next lemma then shows that φ is étale on an open neighbourhood U of P. □

LEMMA 5.54. *Let V and W be nonsingular varieties. If $\varphi\colon V \to W$ is étale at P, then it is étale at all points in an open neighbourhood of P.*

PROOF. The hypotheses imply that V and W have the same dimension d, and that their tangent spaces all have dimension d. We may assume V and W to be affine, say, $V \subset \mathbb{A}^m$ and $W \subset \mathbb{A}^n$, and that φ is given by polynomials $P_1(X_1, \ldots, X_m), \ldots, P_n(X_1, \ldots, X_m)$. Then $(d\varphi)_{\mathbf{a}}\colon T_{\mathbf{a}}(\mathbb{A}^m) \to T_{\varphi(\mathbf{a})}(\mathbb{A}^n)$ is a linear map with matrix $\left(\frac{\partial P_i}{\partial X_j}(\mathbf{a})\right)$, and φ is not étale at $\mathbf{a}$ if and only if the kernel of this map contains a nonzero vector in the subspace $T_{\mathbf{a}}(W)$ of $T_{\mathbf{a}}(\mathbb{A}^n)$. Let $f_1, \ldots, f_r$ generate $I(V)$. Then φ 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 does not contain P. □

Let V be a nonsingular variety, and let $P \in V$. An ***étale neighbourhood*** of a point P of V is a 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 5.55. *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 5.56. (a) Note the similarity to the definition of a differentiable manifold: every point P on a 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 Étale Cohomology*.

(b) Smooth functions $x_1, \ldots, x_n$ defined on an open neighbourhood U of a point P of a differential manifold M are local coordinates at P if they are zero at P and the map $x_1, \ldots, x_n\colon U \to \mathbb{R}^n$ is an isomorphism (of manifolds) from U onto an open submanifold of $\mathbb{R}^n$.

Compare: regular functions $f_1, \ldots, f_n$ defined on an open neighbourhood U of a point P of a nonsingular algebraic variety V are local parameters at P if they are zero at P and the map $f_1, \ldots, f_n\colon U \to \mathbb{A}^n$ is an étale map from U onto an open subvariety U' of $\mathbb{A}^n$. In general, $(U; f_1, \ldots, f_n)$ cannot be chosen so that the map $U \to U'$ is an isomorphism. However, when $k = \mathbb{C}$, there exists a neighbourhood U for the complex topology such that $f_1, \ldots, f_n$ define an isomorphism (of complex manifolds) from U onto an open complex submanifold of $\mathbb{C}^n$.

The inverse function theorem (for the étale topology)

THEOREM 5.57 (INVERSE FUNCTION THEOREM). *Let $\varphi\colon V \to W$ be a regular map. If φ is étale at $P \in V$, then there exists a commutative diagram*

$$\begin{array}{ccc} (V,P) & \xleftarrow{\text{open}} & (U,P) \\ \downarrow{\scriptstyle\varphi} & \swarrow{\scriptstyle\text{étale}} & \\ (W,Q) & & \end{array} \qquad \begin{array}{l} Q=\varphi(P) \\ U \text{ an open neighbourhood of } P \\ (U,P) \text{ an étale neighbourhood of } Q. \end{array}$$

PROOF. According to 5.54, there exists an open neighbourhood U of P such that the restriction $\varphi|U$ of φ to U is étale. □

The rank theorem

For vector spaces, the rank theorem says the following: let $\varphi\colon V \to W$ be a linear map of k-vector spaces of rank r; then there exist bases for V and W relative to which φ has matrix $\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$. In other words, there is a commutative diagram

$$\begin{array}{ccc} V & \xrightarrow{\quad\alpha\quad} & W \\ \downarrow{\scriptstyle\approx} & & \downarrow{\scriptstyle\approx} \\ k^m & \xrightarrow{(x_1,\ldots,x_m)\mapsto(x_1,\ldots,x_r,0,\ldots)} & k^n. \end{array}$$

A similar result holds locally for differentiable manifolds. In algebraic geometry, there is the following weaker analogue.

THEOREM 5.58 (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*

$$\begin{array}{ccc} U_P & \xrightarrow{\quad\varphi|U_P\quad} & U_{\varphi(P)} \\ \downarrow{\scriptstyle\text{étale}} & & \downarrow{\scriptstyle\text{étale}} \\ \mathbb{A}^m & \xrightarrow{(x_1,\ldots,x_m)\mapsto(x_1,\ldots,x_n)} & \mathbb{A}^n \end{array}$$

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 system of local 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 system of local parameters at P. According to 5.54, 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. □

ASIDE 5.59. Tangent vectors at a point P on a smooth manifold V can be defined to be certain equivalence classes of curves through P (Wikipedia: TANGENT SPACE). For $V = \mathbb{A}^n$, there is a similar description with a curve taken to be a regular map from an open neighbourhood U of 0 in $\mathbb{A}^1$ to V. In the general case there is a map from an open neighbourhood of the point P in X onto affine space sending P to 0 and inducing an isomorphism from tangent space at P to that at 0 (5.53). Unfortunately, the maps from $U \subset \mathbb{A}^1$ to $\mathbb{A}^n$ need not lift to X, and so it is necessary to allow maps from smooth curves into X (pull-backs of the covering $X \to \mathbb{A}^n$ by the maps from U into $\mathbb{A}^n$). There is a description of the tangent vectors at a point P on a smooth algebraic variety V as certain equivalence classes of regular maps from an étale neighbourhood U of 0 in $\mathbb{A}^1$ to V.

p. Smooth maps

DEFINITION 5.60. 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 5.61. *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 5.62. *Let V and W be nonsingular varieties. If $\varphi\colon V \to W$ 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. □

Separable maps

A transcendence basis S of an extension $E \supset F$ of fields is ***separating*** if the algebraic extension $E \supset F(S)$ is separable. A finitely generated extension $E \supset F$ of fields is ***separable*** if it admits a separating transcendence basis.

DEFINITION 5.63. A dominant map $\varphi\colon W \to V$ of irreducible algebraic varieties is ***separable*** if $k(W)$ is a separable extension of $k(V)$.

THEOREM 5.64. *Let $\varphi\colon W \to V$ be a regular map of irreducible varieties.*

(a) *If there exists a nonsingular point P of W such that φP is nonsingular and $(d\varphi)_P$ is surjective, then φ is dominant and separable.*

(b) *Conversely if φ is dominant and separable, then the set of $P \in W$ satisfying (a) is open and dense.*

PROOF. Replace W and V with their open subsets of nonsingular points. Then apply the rank theorem. □

q. Algebraic varieties as functors

Let R be an affine k-algebra and V an algebraic variety over k. We define a ***point of V with coordinates in*** R (or an R-***point*** of V) to be a regular map $\mathrm{Spm}(R) \to V$. For example, if $V = V(\mathfrak{a}) \subset \mathbb{A}^n$, then

$$V(R) = \{(a_1, \dots, a_n) \in R^n \mid f(a_1, \dots, a_n) = 0 \text{ all } f \in \mathfrak{a}\},$$

as the terminology suggests. For example, $V(k) = V$ (as a set). In other words, V (as a set) can be identified with the set of points of V with coordinates in k.

From the universal property of products, we see that

$$(V \times W)(R) = V(R) \times W(R).$$

CAUTION 5.65. If V is the union of two subvarieties, $V = V_1 \cup V_2$, then it need ***not*** be true that $V(R) = V_1(R) \cup V_2(R)$. For example, for any polynomial $f(X_1, \dots, X_n)$,

$$\mathbb{A}^n = D(f) \cup V(f),$$

but, in general,

$$R^n \neq \{\mathbf{a} \in R^n \mid f(\mathbf{a}) \in R^\times\} \cup \{\mathbf{a} \in R^n \mid f(\mathbf{a}) = 0\}.$$

In fact, this need not be true even when V_1 and V_2 are open in V because that would require every regular map $U \to V$ with U affine to factor through V_1 or V_2, which is nonsense. For example, $V \stackrel{\text{def}}{=} \mathbb{A}^2 \smallsetminus \{(0,0)\} = D(X) \cup D(Y)$, but the line $X + Y = 1$ in V is not contained in $D(X_1)$ or $D(X_2)$.

THEOREM 5.66. *A regular map $\varphi\colon V \to W$ of algebraic varieties defines a family of maps of sets, $\varphi(R)\colon V(R) \to W(R)$, one for each affine k-algebra R, such that for every homomorphism $\alpha\colon R \to S$ of affine k-algebras, the diagram*

$$\begin{array}{ccc} V(R) & \xrightarrow{\varphi(R)} & W(R) \\ \downarrow{\scriptstyle V(\alpha)} & & \downarrow{\scriptstyle V(\beta)} \\ V(S) & \xrightarrow{\varphi(S)} & W(\alpha 1) \end{array} \qquad (*)$$

commutes. Every family of maps with this property arises from a unique morphism of algebraic varieties.

The first sentence just says that $R \rightsquigarrow V(R)$ is a functor from affine k-algebras to sets, which is obvious. We prove the second after restating it in terms of categories.

Let Var_k (resp. Aff_k) denote the category of algebraic varieties over k (resp. affine algebraic varieties over k). For a variety V, let h_V^{aff} denote the functor sending an affine variety $T = \mathrm{Spm}(R)$ to $V(R) = \mathrm{Hom}(T, V)$. We can restate the second sentence of Theorem 5.66 as follows.

THEOREM 5.67. *The functor*

$$V \rightsquigarrow h_V^{aff}\colon \mathsf{Var}_k \to \mathsf{Fun}(\mathsf{Aff}_k, \mathsf{Sets})$$

is fully faithful.

PROOF. For an algebraic variety V over k, let h_V denote the functor

$$T \rightsquigarrow \mathrm{Hom}(T,V)\colon \mathsf{Var}_k \to \mathsf{Set}.$$

According to the Yoneda lemma (Wikipedia: YONEDA LEMMA) the functor

$$V \rightsquigarrow h_V\colon \mathsf{Var}_k \to \mathsf{Fun}(\mathsf{Var}_k,\mathsf{Sets})$$

is fully faithful. Let φ be a morphism of functors $h_V^{\mathrm{aff}} \to h_{V'}^{\mathrm{aff}}$, and let T be an algebraic variety. Let $(U_i)_{i\in I}$ be a finite affine covering of T. Each intersection $U_i \cap U_j$ is affine (5.29), and so φ gives rise to a commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & h_V(T) & \longrightarrow & \prod_i h_V(U_i) & \rightrightarrows & \prod_{i,j} h_V(U_i\cap U_j) \\
 & & \downarrow & & \downarrow{\scriptstyle \varphi(U_i)} & & \downarrow{\scriptstyle \varphi(U_i\cap U_j)} \\
0 & \longrightarrow & h_{V'}(T) & \longrightarrow & \prod_i h_{V'}(U_i) & \rightrightarrows & \prod_{i,j} h_{V'}(U_i\cap U_j)
\end{array}$$

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 (5.15, last sentence), 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 5.68. *To give an affine group variety over k is the same as giving a functor G from affine k-algebras to sets such that for some n and finite set S of polynomials in $k[X_1,X_2,\ldots,X_n]$, G is isomorphic to the functor sending R to the set of zeros of S in R^n.*

PROOF. Certainly an affine group variety 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 $G(R)\times G(R) \to G(R)$ 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 $m\colon V\times V \to V$. Similarly, the maps $a \mapsto a^{-1}\colon G(R)\to G(R)$ arise from a regular map $\mathrm{inv}\colon V\to V$. □

Often a variety is most naturally defined in terms of its points functor. For example, the group varieties

$$\begin{aligned}
\mathrm{SL}_n &\colon R \rightsquigarrow \{M \in M_n(R) \mid \det(M) = 1\}\\
\mathrm{GL}_n &\colon R \rightsquigarrow \{M \in M_n(R) \mid \det(M) \in R^\times\}\\
\mathbb{G}_a &\colon R \rightsquigarrow (R,+).
\end{aligned}$$

Which functors arise from algebraic varieties?

We now describe the essential image of $h \mapsto h_V\colon \mathsf{Var}_k \to \mathsf{Fun}(\mathsf{Aff}_k,\mathsf{Sets})$. The ***fibred 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

$$(F_1 \times_{F_3} F_2)(R) = F_1(R) \times_{F_3(R)} F_2(R)$$

for all affine k-algebras R.

To simplify the statement of the next proposition, we write U for h_U when U is an affine variety.

PROPOSITION 5.69. *A functor* $F: \mathsf{Aff}_k \to \mathsf{Sets}$ *is in the essential image of* Var_k *if and only if there exists an affine variety* 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 5-2). The functor R is $h_{U'}$, where U' is the disjoint union of the varieties $U_i \cap U_j$. These are affine (5.29), and so U' is affine. As U' is the inverse image of Δ_V in $U \times U$, it is closed (5.26). This proves (a), and (b) is obvious.

The converse is omitted for the present. □

ASIDE 5.70. A variety V defines a functor $R \rightsquigarrow V(R)$ from the category of all k-algebras to Sets. Again, we call the elements of $V(R)$ the ***points of*** V ***with coordinates in*** R.

For example, if V is affine,

$$V(R) = \mathrm{Hom}_{k\text{-algebra}}(k[V], R).$$

More explicitly, if $V \subset k^n$ and $I(V) = (f_1, \dots, f_m)$, then $V(R)$ is the set of solutions in R^n of the system equations

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

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 $V(\mathfrak{a}) = V$.[8]

For a general variety V, we write V as a finite union of open affines $V = \bigcup_i V_i$, and we define $V(R)$ to be the set of families $(\alpha_i)_{i \in I} \in \prod_{i \in I} V_i(R)$ such that α_i agrees with α_j on $V_i \cap V_j$ for all $i, j \in I$. This is independent of the choice of the covering, and agrees with the previous definition when V is affine.

The functor defined by $\mathbb{A}(E)$ (see p. 73) is $R \rightsquigarrow R \otimes_k E$.

A criterion for a functor to arise from an algebraic prevariety

5.71. By a functor we mean a functor from the category of affine k-algebras to sets. A subfunctor U of a functor X is ***open*** if, for all maps $\varphi: h^A \to X$, the subfunctor $\varphi^{-1}(U)$ of h^A is defined by an open subvariety of $\mathrm{Spm}(A)$. A family $(U_i)_{i \in I}$ of open subfunctors of X is an ***open covering*** of X if each U_i is open in X and $X(K) = \bigcup U_i(K)$ for every field K. A functor X is ***local*** if, for all k-algebras R and all finite families $(f_i)_i$ of elements of A generating A as an ideal, the sequence of sets

$$X(R) \to \prod_i X(R_{f_i}) \rightrightarrows \prod_{i,j} X(R_{f_i f_j})$$

is exact.

Let $\mathbb{A}^1$ denote the functor sending a k-algebra R to its underlying set. For a functor U, let $\mathcal{O}(U) = \mathrm{Hom}(U, \mathbb{A}^1)$ — it is a k-algebra.[9] A functor U is ***affine*** if $\mathcal{O}(U)$ is an

[8]Let $\mathfrak{a}$ be an ideal in $k[X_1, \dots]$. If A has no nonzero nilpotent elements, then every k-algebra homomorphism $k[X_1, \dots] \to A$ that is zero on $\mathfrak{a}$ is also zero on $\mathrm{rad}(\mathfrak{a})$, and so

$$\mathrm{Hom}_k(k[X_1, \dots]/\mathfrak{a}, A) \simeq \mathrm{Hom}_k(k[X_1, \dots]/\mathrm{rad}(\mathfrak{a}), A).$$

This is not true if A has nonzero nilpotents.

[9]Actually, one needs to be more careful to ensure that $\mathcal{O}(U)$ is a set; for example, restrict U and $\mathbb{A}^1$ to the category of k-algebras of the form $k[X_0, X_1, \dots]/\mathfrak{a}$ for a fixed family of symbols (X_i) indexed by $\mathbb{N}$.

affine k-algebra and the canonical map $U \to h^{\mathcal{O}(U)}$ is an isomorphism. A local functor admitting a finite covering by open affines is representable by an algebraic variety over k.

In the functorial approach to algebraic geometry, an algebraic prevariety over k is *defined* to be a functor satisfying this criterion. See, for example, Demazure and Gabriel 1970, I, §1, 3.11, p. 13.

r. Rational and unirational varieties

In this section, k is an infinite field, not necessarily algebraically closed.

DEFINITION 5.72. Let V be a smooth projective variety over k of dimension n.

(a) V is ***unirational*** if there exists a dominant rational map $\mathbb{P}^n \dashrightarrow V$.

(b) V is ***rational*** if there exists a birational map $\mathbb{P}^n \dashrightarrow V$.

(c) V is ***stably rational*** if $V \times \mathbb{P}^r$ is rational for some r.

If V is stably rational, then there exists a dominant rational map $\mathbb{P}^{n+r} \dashrightarrow V$, and this will restrict to a dominant rational map on some linear subspace $\mathbb{P}^n \subset \mathbb{P}^{n+r}$. Therefore,

$$\text{rational} \Rightarrow \text{stably rational} \Rightarrow \text{unirational.}$$

An irreducible variety V is rational if $k(V)$ is a pure transcendental extension of k, and it is unirational if $k(V)$ is contained in a pure transcendental extension of k.

In 1876 (over $\mathbb{C}$), Lüroth proved that every unirational curve is rational (see FT, 9.19). The Lüroth problem asks whether every unirational variety is rational.

Already for surfaces, this is a difficult problem. In characteristic zero, Castelnuovo and Severi proved that all unirational surfaces are rational, but in characteristic $p \neq 0$, Zariski showed that some surfaces of the form

$$Z^p = f(X, Y),$$

while obviously unirational, are not rational. Surfaces of this form are now called Zariski surfaces.

Fano attempted to find counter-examples to the Lüroth problem in dimension 3 among the so-called Fano varieties, but none of his attempted proofs satisfies modern standards. In 1971-72, three examples of nonrational unirational three-folds were found.

REFERENCES.

Beauville, A., The Lüroth problem, Lecture Notes in Math., 2172, Fond. CIME/CIME Found. Subser., Springer, Cham, 2016, 1–27, arXiv:1507.02476.

Hochenegger, A., Lehn, M., and Stellari, P. (Editors), Birational geometry of hypersurfaces, Gargnano del Garda, Italy, 2018. Lectures from the school held in March 2018. Lecture Notes of the Unione Matematica Italiana, 26. Springer, Cham, 2019.

A little history

In his first proof of the Riemann hypothesis for curves over finite fields, Weil made use of the Jacobian variety of the curve, but initially he was not able to construct this as a projective variety. This led him to introduce "abstract" algebraic varieties, neither affine nor projective (in Weil 1946). Weil first made use of the Zariski topology when he introduced fibre spaces into algebraic geometry (in 1949). For more on this, see my article: *The Riemann hypothesis over finite fields: from Weil to the present day.*

Exercises

5-1. 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.]

5-2. 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.

5-3. Show that an algebraic variety G equipped with a group structure is a group variety if the map $(x, y) \mapsto x^{-1}y\colon G \times G \to G$ is regular.

5-4. Let G be a group variety. Show:

(a) The neutral element e of G is contained in a unique irreducible component G° of G, which is also the unique connected component of G containing e.

(b) The subvariety G° is a normal subgroup of G of finite index, and every subgroup variety of G of finite index contains G°.

5-5. Show that every subgroup variety of a group variety is closed.

5-6. Show that a prevariety V is separated if and only if it satisfies the following condition: a regular map $U \smallsetminus \{P\} \to V$ with U a curve and P a nonsingular point on U extends in at most one way to a regular map $U \to V$.

5-7. Prove the final statement in 5.71.

5-8. Let V be an algebraic variety. Show that the Zariski topology on $V \times V$ agrees with the product topology if and only $\dim(V) = 0$.

Chapter 6

Projective Varieties

Recall (5.3) that we defined $\mathbb{P}^n$ to be the set of equivalence classes in $k^{n+1} \smallsetminus \{\text{origin}\}$ for the relation

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

Let $(a_0 : \dots : a_n)$ denote the equivalence class of $(a_0, \dots, a_n)$, and let π denote the map

$$\frac{k^{n+1} \smallsetminus \{(0, \dots, 0)\}}{\sim} \to \mathbb{P}^n.$$

Let U_i be the set of $(a_0 : \dots : a_n) \in \mathbb{P}^n$ such that $a_i \neq 0$, and let u_i be the bijection

$$(a_0 : \dots : a_n) \mapsto \left(\frac{a_0}{a_i}, \dots, \widehat{\frac{a_i}{a_i}}, \dots, \frac{a_n}{a_i}\right) : U_i \xrightarrow{u_i} \mathbb{A}^n \quad (\tfrac{a_i}{a_i} \text{ omitted}).$$

In this chapter, we show that $\mathbb{P}^n$ has 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 ***quasiprojective variety***. Every affine variety is quasi-projective, but not all algebraic varieties are quasi-projective. We study morphisms between quasi-projective 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 6.37 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.

a. Algebraic subsets of $\mathbb{P}^n$

A polynomial $F(X_0, \dots, X_n)$ is said to be ***homogeneous of degree*** d if it is a sum of terms $a_{i_0,\dots,i_n} X_0^{i_0} \cdots X_n^{i_n}$ with $i_0 + \cdots + i_n = d$; equivalently,

$$F(tX_0, \dots, tX_n) = t^d F(X_0, \dots, X_n)$$

for all $t \in k$. The polynomials homogeneous of degree d form a subspace $k[X_0, \dots, X_n]_d$ of $k[X_0, \dots, X_n]$, and

$$k[X_0, \dots, X_n] = \bigoplus_{d \geq 0} k[X_0, \dots, X_n]_d;$$

in other words, every 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 cannot 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 of $\mathbb{P}^2$ defined by the homogeneous equation

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3. \tag{26}$$

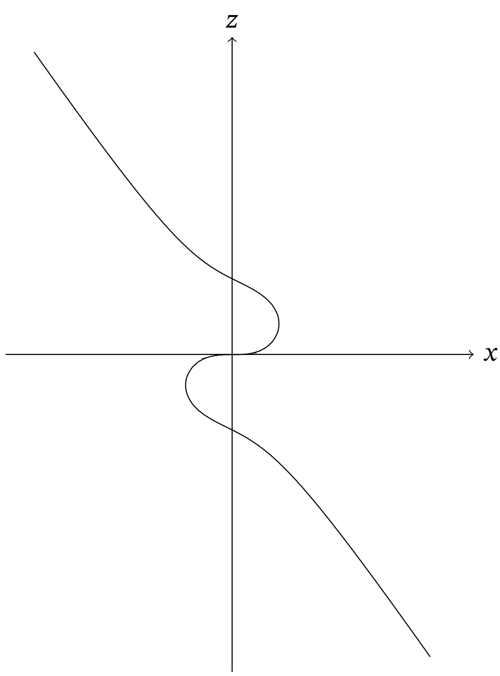
It consists of the points $(x : y : 1)$ on the affine curve $E \cap U_2$

$$Y^2 = X^3 + aX + b$$

(see 2.2) together with the point "at infinity" $(0 : 1 : 0)$. Note that $E \cap U_1$ is the affine curve

$$Z = X^3 + aXZ^2 + bZ^3,$$

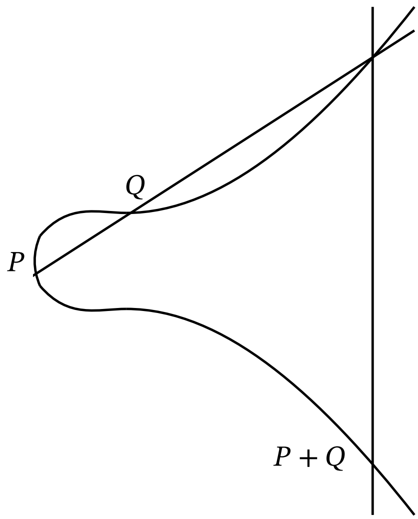
and that $(0 : 1 : 0)$ corresponds to the point $(0, 0)$ on $E \cap U_1$:



$Z = X^3 + XZ^2 + Z^3$

As $(0, 0)$ is nonsingular on $E \cap U_1$, we deduce from (4.5) that E is nonsingular unless $X^3 + aX + b$ has a multiple root. A nonsingular curve of the form (26) is called an ***elliptic curve***.

An elliptic curve has a unique structure of a group variety for which the point at infinity is the zero:



When $a, b \in \mathbb{Q}$, we can speak of the zeros of (26) 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 works in practice, but which has not been proved to always terminate after a finite amount of time. There is a very beautiful theory surrounding elliptic curves over $\mathbb{Q}$ and other number fields, whose origins can be traced back almost 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 ***graded*** or ***homogeneous*** if it contains with any polynomial F all the homogeneous components of F, i.e., if

$$F \in \mathfrak{a} \Rightarrow F_d \in \mathfrak{a}, \text{ all } d.$$

It is straightforward to check that

- an ideal is graded if and only if it is generated by (a finite set of) homogeneous polynomials;
- the radical of a graded ideal is graded;
- an intersection, product, or sum of graded ideals is graded.

For a graded ideal $\mathfrak{a}$, we let $V(\mathfrak{a})$ denote the set of common zeros of the homogeneous polynomials in $\mathfrak{a}$. Clearly

$$\mathfrak{a} \subset \mathfrak{b} \Rightarrow V(\mathfrak{a}) \supset V(\mathfrak{b}).$$

If $F_1, \ldots, F_r$ are homogeneous generators for $\mathfrak{a}$, then $V(\mathfrak{a})$ is also 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 $V^{\mathrm{aff}}(\mathfrak{a})$ for the set of common zeros of $\mathfrak{a}$ in k^{n+1}. It is a ***cone*** in k^{n+1}, i.e., together with any point P it contains the line through P and the origin, and

$$V(\mathfrak{a}) = \frac{V^{\mathrm{aff}}(\mathfrak{a}) \smallsetminus \{(0, \ldots, 0)\}}{\sim}.$$

The sets $V(\mathfrak{a})$ in $\mathbb{P}^n$ have similar properties to their namesakes in $\mathbb{A}^n$.

PROPOSITION 6.2. *There are the following relations:*

(a) $V(0) = \mathbb{P}^n$; $\quad V(\mathfrak{a}) = \emptyset \iff \mathrm{rad}(\mathfrak{a}) \supset (X_0, \ldots, X_n)$;

(b) $V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$;

(c) $V(\sum \mathfrak{a}_i) = \bigcap V(\mathfrak{a}_i)$.

PROOF. For the second statement in (a), note that

$$\begin{aligned} V(\mathfrak{a}) = \emptyset &\iff V^{\mathrm{aff}}(\mathfrak{a}) \subset \{(0, \ldots, 0)\} \\ &\iff \mathrm{rad}(\mathfrak{a}) \supset (X_0, \ldots, X_n) \qquad \text{(strong Nullstellensatz 2.16).} \end{aligned}$$

The remaining statements can be proved directly, as in Proposition 2.10, or by using the relation between $V(\mathfrak{a})$ and $V^{\mathrm{aff}}(\mathfrak{a})$. □

Proposition 6.2 shows that the projective algebraic sets are the closed sets for a topology on $\mathbb{P}^n$ — this is called the ***Zariski topology*** on $\mathbb{P}^n$.

If C is a cone in k^{n+1}, then $I(C)$ is a graded 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

$$C = \pi^{-1}(S) \cup \{\text{origin}\}$$

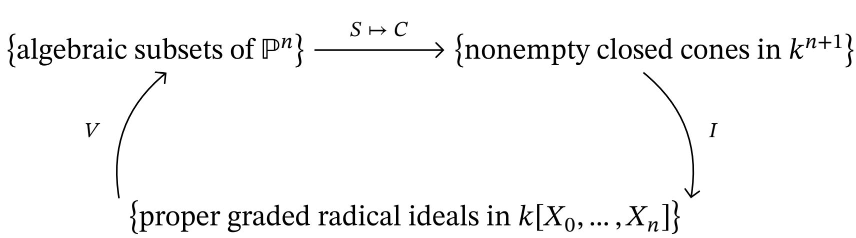
and we set

$$I(S) = I(C).$$

Note that if S is nonempty and closed, then C is the closure of $\pi^{-1}(S) \neq \emptyset$, and that $I(S)$ is spanned by the homogeneous polynomials in $k[X_0, \ldots, X_n]$ 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 graded 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. We have bijections



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 the graded ideals $(X_0,\dots,X_n)$ and $k[X_0,\dots,X_n]$ are both radical, but

$$V(X_0,\dots,X_n)=\emptyset=V(k[X_0,\dots,X_n])$$

and so the correspondence between irreducible subsets of $\mathbb{P}^n$ and radical graded ideals is not quite one-to-one.

ASIDE 6.4. In English "homogeneous ideal" is more common than "graded ideal", but we follow Bourbaki, Alg, II, §11. A ***graded ring*** is a pair $(S,(S_d)_{d\in\mathbb{N}})$ comprising a ring S and a family of additive subgroups S_d such that

$$S=\bigoplus\nolimits_{d\in\mathbb{N}}S_d,\quad S_dS_e\subset S_{d+e},\text{ all }d,e\in\mathbb{N}.$$

An ideal $\mathfrak{a}$ in S is ***graded*** if and only if

$$\mathfrak{a}=\bigoplus\nolimits_{d\in\mathbb{N}}(\mathfrak{a}\cap S_d);$$

this means that it is a graded submodule of $(S,(S_d))$. The quotient of a graded ring S by a graded ideal $\mathfrak{a}$ is a graded ring $S/\mathfrak{a}=\bigoplus_d S_d/(\mathfrak{a}\cap S_d)$.

b. The Zariski topology on $\mathbb{P}^n$

For a graded 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 $\mathbb{P}^n$. As in the opening paragraph of this chapter, we let $U_i=D(X_i)$.

To each polynomial $f(X_1,\dots,X_n)$, we attach the homogeneous polynomial of the same degree

$$f^*(X_0,\dots,X_n)=X_0^{\deg(f)}f\left(\frac{X_1}{X_0},\dots,\frac{X_n}{X_0}\right),$$

and to each homogeneous polynomial $F(X_0,\dots,X_n)$, we attach the polynomial

$$F_*(X_1,\dots,X_n)=F(1,X_1,\dots,X_n).$$

PROPOSITION 6.5. *Each subset U_i of $\mathbb{P}^n$ is open in the Zariski topology on $\mathbb{P}^n$, and when we endow it with the induced topology, the bijection*

$$U_i\leftrightarrow\mathbb{A}^n,\ (a_0:\dots:1:\dots:a_n)\leftrightarrow(a_0,\dots,a_{i-1},a_{i+1},\dots,a_n)$$

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 $F\in k[X_0,\dots,X_n]$,

$$D(F(X_0,\dots,X_n))\cap U_0=D(F(1,X_1,\dots,X_n))=D(F_*)$$

and, for any polynomial $f\in k[X_1,\dots,X_n]$,

$$D(f)=D(f^*)\cap U_0.$$

Thus, under the bijection $U_0\leftrightarrow\mathbb{A}^n$, 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 6.6. 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 p. 45). 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 intersect $U_i \cap U_j$. Therefore U intersects every U_j, and so is dense in every U_j. It follows that its closure is all of $\mathbb{P}^n$.

c. 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 graded 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 graded 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 6.7. *(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. □

Examples

6.8. For

$$V : Y^2 = X^3 + aX + b,$$

we have

$$V^* : Y^2Z = X^3 + aXZ^2 + bZ^3,$$

and $(V^*)_* = V$.

6.9. 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 $V(X_0X_1, X_1^2 + X_0X_2)$ consists of the two points $(1 : 0 : 0)$ (the closure of V) and $(0 : 0 : 1)$ (which is contained in H_∞).[1]

6.10. For $V = H_\infty = V(X_0)$, we have $V_* = \emptyset = V(1)$ and $(V_*)^* = \emptyset \neq V$.

[1]Of course, in this case $\mathfrak{a} = (X_1, X_2)$, $\mathfrak{a}^* = (X_1, X_2)$, and $V^* = \{(1 : 0 : 0)\}$, and so this example does not contradict the proposition.

d. 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, we identify the set U_0 with $\mathbb{A}^n$. The complement of U_0 in $\mathbb{P}^n$ is

$$H_\infty = \{(0 : a_1 : \ldots : a_n) \in \mathbb{P}^n\},$$

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 intersect 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 replace U_0 with U_n in the above discussion, and write $\mathbb{P}^n = U_n \sqcup H_\infty$ with $H_\infty = \{(a_0 : \ldots : a_{n-1} : 0)\}$, as in Example 6.1. Note that in this example 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_∞.

e. $\mathbb{P}^n$ 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 $u_i : U_i \to \mathbb{A}^n$.

LEMMA 6.11. *Let $U_{ij} = U_i \cap U_j$; then $\mathcal{O}_i|U_{ij} = \mathcal{O}_j|U_{ij}$. When endowed with this sheaf, U_{ij} is an affine algebraic 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

$$U_0 = \{(a_0 : a_1 : \ldots : a_n) \mid a_0 \neq 0\} \quad (a_0 : a_1 : \ldots : a_n) \leftrightarrow \left(\frac{a_1}{a_0}, \frac{a_2}{a_0}, \ldots, \frac{a_n}{a_0}\right) \in \mathbb{A}^n.$$

Let $k\left[\frac{X_1}{X_0}, \frac{X_2}{X_0}, \ldots, \frac{X_n}{X_0}\right]$ 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 $f\left(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}\right) \in k\left[\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}\right]$ defines a map

$$(a_0 : a_1 : \ldots : a_n) \mapsto f\left(\frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}\right) : U_0 \to k,$$

and in this way $k\left[\frac{X_1}{X_0}, \frac{X_2}{X_0}, \ldots, \frac{X_n}{X_0}\right]$ becomes identified with the ring of regular functions on U_0, and U_0 with $\operatorname{Spm}\left(k\left[\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}\right]\right)$.

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 $D\left(\frac{X_1}{X_0}\right)$, 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 $k\left[\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}\right] \hookrightarrow k\left[\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}, \frac{X_0}{X_1}\right]$. An element $f\left(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}, \frac{X_0}{X_1}\right)$ of $k\left[\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}, \frac{X_0}{X_1}\right]$ defines the function $(a_0 : \ldots : a_n) \mapsto f\left(\frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}, \frac{a_0}{a_1}\right)$ on U_{01}.

Similarly,

$$U_1 = \{(a_0 : a_1 : \ldots : a_n) \mid a_1 \neq 0\}; (a_0 : a_1 : \ldots : a_n) \leftrightarrow \left(\frac{a_0}{a_1}, \ldots, \frac{a_n}{a_1}\right) \in \mathbb{A}^n,$$

and we identify U_1 with $\operatorname{Spm}\left(k\left[\frac{X_0}{X_1}, \frac{X_2}{X_0}, \ldots, \frac{X_n}{X_1}\right]\right)$. A polynomial $f\left(\frac{X_0}{X_1}, \ldots, \frac{X_n}{X_1}\right)$ in $k\left[\frac{X_0}{X_1}, \ldots, \frac{X_n}{X_1}\right]$ defines the map $(a_0 : \ldots : a_n) \mapsto f\left(\frac{a_0}{a_1}, \ldots, \frac{a_n}{a_1}\right) : U_1 \to k$.

When regarded as an open subset of U_1, $U_{01} = D\left(\frac{X_0}{X_1}\right)$, 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 $k\left[\frac{X_0}{X_1}, \ldots, \frac{X_n}{X_1}\right] \hookrightarrow k\left[\frac{X_0}{X_1}, \ldots, \frac{X_n}{X_1}, \frac{X_1}{X_0}\right]$. An element $f\left(\frac{X_0}{X_1}, \ldots, \frac{X_n}{X_1}, \frac{X_1}{X_0}\right)$ of $k\left[\frac{X_0}{X_1}, \ldots, \frac{X_n}{X_1}, \frac{X_1}{X_0}\right]$ defines the function $(a_0 : \ldots : a_n) \mapsto f\left(\frac{a_0}{a_1}, \ldots, \frac{a_n}{a_1}, \frac{a_1}{a_0}\right)$ on U_{01}.

The two subrings $k\left[\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}, \frac{X_0}{X_1}\right]$ and $k\left[\frac{X_0}{X_1}, \ldots, \frac{X_n}{X_1}, \frac{X_1}{X_0}\right]$ 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 (3.15). This proves the first two assertions, and the third is obvious: $k\left[\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}, \frac{X_0}{X_1}\right]$ is generated by its subrings $k\left[\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}\right]$ and $k\left[\frac{X_0}{X_1}, \frac{X_2}{X_1}, \ldots, \frac{X_n}{X_1}\right]$. □

PROPOSITION 6.12. *There is a unique structure of an 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. Moreover, $\mathbb{P}^n$ is separated.*

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 5.15, 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 5.29(c) to be separated. □

EXAMPLE 6.13. Let C be the plane projective curve

$$C : Y^2 Z = X^3$$

and assume that $\operatorname{char}(k) \neq 2$. For each $a \in k^\times$, there is an automorphism

$$(x : y : z) \mapsto (ax : y : a^3 z) : C \xrightarrow{\varphi_a} C.$$

Patch two copies of $C \times \mathbb{A}^1$ together along $C \times (\mathbb{A}^1 - \{0\})$ by identifying (P, a) with $(\varphi_a(P), a^{-1})$, $P \in C$, $a \in \mathbb{A}^1 \smallsetminus \{0\}$. One obtains in this way a singular surface that is not quasi-projective (see Hartshorne 1977, Exercise 7.13). It is even complete — see below — and so if it were quasi-projective, it would be projective. In Shafarevich 1994, VI 2.3, there is an example of a nonsingular complete variety of dimension 3 that is not projective. It is known that every irreducible separated curve is quasi-projective, and every nonsingular complete surface is projective, and so these examples are minimal.

f. The homogeneous coordinate ring of a projective variety

Recall (p. 115) that attached to each irreducible variety V, there is 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 $k[U_0] = k\left[\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0}\right]$. We regard this as a subring of $k(X_0, \dots, X_n)$, and wish to identify the field of fractions of $k[U_0]$ as a subfield of $k(X_0, \dots, X_n)$. Every nonzero $F \in k[U_0]$ can be written

$$F\left(\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0}\right) = \frac{F^*(X_0, \dots, X_n)}{X_0^{\deg(F)}}$$

with F^* homogeneous of degree $\deg(F)$, and it follows that the field of fractions of $k[U_0]$ is

$$k(U_0) = \left\{ \frac{G(X_0, \dots, X_n)}{H(X_0, \dots, X_n)} \;\middle|\; G, H \text{ homogeneous of the same degree} \right\} \cup \{0\}.$$

Write $k(X_0, \dots, X_n)_0$ for this field (the subscript 0 is short for "subfield of elements of degree 0"), so that $k(\mathbb{P}^n) = k(X_0, \dots, X_n)_0$. Note that for $F = \frac{G}{H}$ in $k(X_0, \dots, X_n)_0$,

$$(a_0 : \dots : a_n) \mapsto \frac{G(a_0, \dots, a_n)}{H(a_0, \dots, a_n)} : D(H) \to k,$$

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 graded radical ideal in $k[X_0, \dots, X_n]$, and we define the ***homogeneous*** coordinate ring of V (with its given embedding) to be

$$k_{\text{hom}}[V] = k[X_0, \dots, X_n]/\mathfrak{p}.$$

Note that $k_{\text{hom}}[V]$ 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. For example,

$$(a_0 : a_1) \mapsto (a_0^2 : a_0 a_1 : a_1^2) : \mathbb{P}^1 \xrightarrow{\nu} \mathbb{P}^2$$

is an isomorphism from $\mathbb{P}^1$ onto its image $\nu(\mathbb{P}^1) : X_0 X_2 = X_1^2$ (see 6.23 below), but $k_{\text{hom}}[\mathbb{P}^1] = k[X_0, X_1]$, 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 $X_0 X_2 - X_1^2$.

We say that a nonzero $f \in k_{\text{hom}}[V]$ is ***homogeneous of degree*** d if it can be represented by a homogeneous polynomial F of degree d in $k[X_0, \dots, X_n]$, and we say that 0 is homogeneous of degree 0.

LEMMA 6.14. *Each element of $k_{\text{hom}}[V]$ 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; when read modulo $\mathfrak{p}$, this gives a decomposition of f of the required type. Suppose that 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 $k_{\text{hom}}[V]$ is an integral domain, we can form its field of fractions $k_{\text{hom}}(V)$. Define

$$k_{\text{hom}}(V)_0 = \left\{ \frac{g}{h} \in k_{\text{hom}}(V) \;\middle|\; g \text{ and } h \text{ homogeneous of the same degree} \right\} \cup \{0\}.$$

PROPOSITION 6.15. *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 $k_{\text{hom}}(V)_0$. □

g. 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 $h(P) \neq 0$,

$$f(P) \stackrel{\text{def}}{=} \frac{g(a_0, \ldots, a_n)}{h(a_0, \ldots, a_n)}$$

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,[2] 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, if $h'(P) \neq 0$, the two representations give the same value for $f(P)$.

[2] Unless $k_{\text{hom}}[V]$ is a unique factorization domain, there will be no preferred representation $f = \frac{g}{h}$.

PROPOSITION 6.16. *For each $f \in k(V) \overset{\text{def}}{=} k_{\text{hom}}(V)_0$, 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 6.17. (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 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 (6.24) that, for any nonzero homogeneous $h \in k_{\text{hom}}[V]$, $D(h)$ 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 need not even be a finitely generated k-algebra!

h. Maps from projective varieties

We describe the morphisms from a projective variety to another variety.

PROPOSITION 6.18. *The map*

$$\pi\colon \mathbb{A}^{n+1} \setminus \{\text{origin}\} \to \mathbb{P}^n,\ (a_0, \dots, a_n) \mapsto (a_0 : \dots : a_n)$$

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

$$(a_0, \dots, a_n) \mapsto \left(\frac{a_0}{a_i} : \dots : \frac{a_n}{a_i}\right)\colon k^{n+1} \setminus V(X_i) \to U_i,$$

which is the regular map of affine varieties corresponding to the map of k-algebras

$$k\left[\frac{X_0}{X_i}, \dots, \frac{X_n}{X_i}\right] \to k[X_0, \dots, X_n][X_i^{-1}].$$

(In the first algebra $\frac{X_j}{X_i}$ is to be thought of as a single symbol.) It now follows from Proposition 5.4 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 intersect 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 6.19. Consider polynomials $F_0(X_0, \dots, X_m), \dots, F_n(X_0, \dots, X_m)$ of the same degree. The map

$$(a_0 : \dots : a_m) \mapsto (F_0(a_0, \dots, a_m) : \dots : F_n(a_0, \dots, a_m))$$

obviously defines a regular map to $\mathbb{P}^n$ on the open subset of $\mathbb{P}^m$, where not all F_i vanish, that is, on the set $\bigcup D(F_i) = \mathbb{P}^n \smallsetminus V(F_1, \dots, F_n)$. Its restriction to any subvariety V of $\mathbb{P}^m$ will also be regular. It may be possible to extend the map to a larger set by representing it by different polynomials. Conversely, every such map arises in this way, at least locally. More precisely, there is the following result.

PROPOSITION 6.20. *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*

$$F_0(X_0, \dots, X_m), \dots, F_n(X_0, \dots, X_m),$$

homogeneous of the same degree, such that

$$\varphi((b_0 : \dots : b_n)) = (F_0(b_0, \dots, b_m) : \dots : F_n(b_0, \dots, b_m))$$

for all points $(b_0 : \dots : b_m)$ in some neighbourhood of P in $V(\mathfrak{a})$.

PROOF. Straightforward. □

EXAMPLE 6.21. We prove that the circle $X^2 + Y^2 = Z^2$ is isomorphic to $\mathbb{P}^1$ ($\text{char}(k) \neq 2$). 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.

i. Some classical maps of projective varieties

A ***hypersurface of degree*** m in $\mathbb{P}^n$ is an algebraic subset defined by nonzero homogeneous of degree $m \geq 1$. When $m = 1$, the hypersurface is called a ***hyperplane***. As in the affine case (2.67), the hypersurfaces in $\mathbb{P}^n$ are exactly the closed subvarieties of $\mathbb{P}^n$ of codimension 1. The intersection of a projective variety $W \subset \mathbb{P}^n$ with a hypersurface (of degree m) is called a ***hypersurface section*** (of degree m) of W.

After proving that complements of hyperplane sections are affine, we study some classical maps of projective varieties.

HYPERPLANE SECTIONS AND COMPLEMENTS

We show that the complement of a hyperplane section of a projective variety is an affine variety, and deduce that any finite set of points of a projective variety is contained in an affine subvariety.

6.22. 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 $k\left[\frac{X_0}{\sum c_i X_i}, \ldots, \frac{X_n}{\sum c_i X_i}\right]$. 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.

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

$$L_{\mathbf{c}}(P) \overset{\text{def}}{=} \sum c_i a_i \neq 0$$

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.

THE VERONESE MAP

The Veronese map embeds $\mathbb{P}^n$ in a higher dimensional projective space in such a way that hypersurface sections of subvarieties are transformed into hyperplane sections.

6.23. Let

$$I = \{(i_0, \dots, i_n) \in \mathbb{N}^{n+1} \mid \sum i_j = m\}.$$

Note that I indexes the monomials of degree m in $n+1$ variables. It has $\binom{m+n}{m}$ elements (see 6.39 below). 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 $(\dots : b_{i_0 \dots i_n} : \dots)$. The Veronese mapping is defined to be

$$v : \mathbb{P}^n \to \mathbb{P}^{\nu_{n,m}}, (a_0 : \dots : a_n) \mapsto (\dots : b_{i_0 \dots i_n} : \dots), \quad b_{i_0 \dots i_n} = a_0^{i_0} \dots a_n^{i_n}.$$

In other words, the Veronese mapping sends an $n+1$-tuple $(a_0 : \dots : a_n)$ to the set of monomials in the a_i of degree m. For example, when $n = 1$ and $m = 2$, the Veronese map is

$$(a_0 : a_1) \mapsto (a_0^2 : a_0 a_1 : a_1^2) : \mathbb{P}^1 \to \mathbb{P}^2.$$

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 6.22.)

When $n = 1$ and m is general, the Veronese map is

$$(a_0 : a_1) \mapsto (a_0^m : a_0^{m-1} a_1 : \dots : a_1^m) : \mathbb{P}^1 \to \mathbb{P}^m.$$

We shall show that, in the general case, the image of ν is a closed subset of $\mathbb{P}^{\nu_{n,m}}$ and that ν defines an isomorphism of projective varieties $\nu : \mathbb{P}^n \to \nu(\mathbb{P}^n)$.

First note that the map has the following interpretation: if we regard the coordinates a_i of a point P of $\mathbb{P}^n$ as being the coefficients of a linear form $L = \sum a_i X_i$ (well-defined up to multiplication by nonzero scalar), then the coordinates of $\nu(P)$ are the coefficients of the homogeneous polynomial L^m with the binomial coefficients omitted.

As $L \neq 0 \Rightarrow L^m \neq 0$, the map ν is defined on the whole of $\mathbb{P}^n$, that is,

$$(a_0, \dots, a_n) \neq (0, \dots, 0) \Rightarrow (\dots, b_{i_0 \dots i_n}, \dots) \neq (0, \dots, 0).$$

Moreover,

$$L_1 \neq c L_2 \Rightarrow L_1^m \neq c L_2^m$$

because $k[X_0, \dots, X_n]$ is a unique factorization domain. Therefore, ν is injective, and it is obvious from its definition that it is regular.

We shall see in the next chapter that the image of any projective variety under a regular map is closed, but here we can prove directly that $\nu(\mathbb{P}^n)$ is defined by the system of equations

$$b_{i_0 \dots i_n} b_{j_0 \dots j_n} = b_{k_0 \dots k_n} b_{\ell_0 \dots \ell_n}, \qquad i_h + j_h = k_h + \ell_h, \text{ all } h. \tag{*}$$

Obviously $\mathbb{P}^n$ maps into the algebraic set defined by these equations. Conversely, let

$$V_i = \{(\dots. : b_{i_0 \dots i_n} : \dots) \mid b_{0 \dots 0m0 \dots 0} \neq 0\}.$$

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

$$(\dots : b_{i_0 \dots i_n} : \dots) \mapsto (b_{m,0,\dots,0} : b_{m-1,1,0,\dots,0} : b_{m-1,0,1,0,\dots,0} : \dots : b_{m-1,0,\dots,0,1}).$$

Finally, one checks that $\nu(\mathbb{P}^n) \subset \bigcup V_i$.

As $\mathbb{P}^n \xrightarrow{\nu} \nu(\mathbb{P}^n)$ is an isomorphism, for any closed subvariety W of V, $\nu(W)$ is a closed subvariety of $\nu(\mathbb{P}^n)$ (hence of $\mathbb{P}^{\nu_{n,m}}$) and $\nu | W : W \to \nu(W)$ is an isomorphism.

6.24. The Veronese mapping has a very important property. 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 hyper*surface* section $W \cap H$ of V onto the hyper*plane* section $\nu(W) \cap L$ of $\nu(W)$. This observation often allows us to replace questions about hypersurface sections with 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.

AUTOMORPHISMS OF $\mathbb{P}^n$

We show that the automorphisms of $\mathbb{P}^n$ are exactly the invertible changes of variables.

6.25. A ***Möbius transformation*** of $\mathbb{P}^1$ is a regular map of the form

$$(x : y) \mapsto (ax + by : cx + dy) \colon \mathbb{P}^1 \to \mathbb{P}^1,$$

where $a, b, c, d \in k$ are such that $ad - bc \neq 0$. The Möbius transformations are exactly the automorphisms of $\mathbb{P}^1$, and two quadruples a, b, c, d define the same transformation if and only if one is a nonzero multiple of the other.[3] Thus,

$$\mathrm{Aut}(\mathbb{P}^1) = \mathrm{PGL}_2(k) \stackrel{\text{def}}{=} \mathrm{GL}_2(k)/k^\times I, \quad \text{where } I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

A similar statement is true for $\mathbb{P}^n$. An element $A = (a_{ij})$ of GL_{n+1} defines a regular map

$$(x_0 : \ldots : x_n) \mapsto (\ldots : \sum a_{ij} x_j : \ldots) \colon \mathbb{P}^n \to \mathbb{P}^{n\prime}$$

It is an automorphism with inverse defined by the inverse matrix. 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 group variety.

[3]Therefore, when $k = \mathbb{C}$, the automorphisms of $\mathbb{P}^1$ coincide with the holomorphic automorphisms of the Riemann sphere (Cartan 1963, VI.2.4).

The homomorphism $\mathrm{PGL}_{n+1} \to \mathrm{Aut}(\mathbb{P}^n)$ is obviously injective. We sketch a proof that it is surjective.[4]

First note that the collection of lines in $\mathbb{P}^n$ has a natural structure of an algebraic variety and, in particular, a (Zariski) topology. Indeed, the lines in $\mathbb{P}^n$ correspond to 2-dimensional subspaces of k^{n+1}, and hence to the points on the Grassmann variety $G_2(k^{n+1})$ (see section 6m below).

Fix a hypersurface

$$H: F(X_0, \ldots, X_n) = 0$$

in $\mathbb{P}^n$ and consider a line

$$L = \{(a_0 + tb_0 : \ldots : a_n + tb_n) \mid t \in k\}$$

in $\mathbb{P}^n$. The points of $H \cap L$ are given by the solutions of

$$F(a_0 + tb_0 : \ldots : a_n + tb_n) = 0,$$

which is a polynomial of degree $\leq \deg(F)$ in t unless $L \subset H$. Therefore, if $L \not\subset H$, then $H \cap L$ contains at most $\deg(F)$ points, and it is not hard to show that, for the L in an open subset of the space of all lines, 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 an open set of lines L.

These are geometric conditions, and so any automorphism of $\mathbb{P}^n$ must map hyperplanes to hyperplanes. But on an open subset of $\mathbb{P}^n$, any 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 6.20). Such a map will take hyperplanes to hyperplanes if and only if $d = 1$.

The Segre map

The Segre map embeds a product of projective spaces into a projective space, and allows us to show that products of projective varieties are projective.

6.26. The Segre map is

$$((a_0 : \ldots : a_m), (b_0 : \ldots : b_n)) \mapsto (\underbrace{a_0 b_0}_{w_{00}} : \ldots : \underbrace{a_i b_j}_{w_{ij}} : \ldots)) : \mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^{mn+m+n}.$$

The index set for $\mathbb{P}^{mn+m+n}$ is $\{(i,j) \mid 0 \leq i \leq m,\ 0 \leq j \leq n\}$. Note that if we interpret the tuples on the left as 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 $L_1 L_2$, which is a homogeneous form of degree 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. Its image is obviously contained the hypersurface

$$H : W_{ij} W_{kl} - W_{il} W_{kj} = 0.$$

[4]This is related to the fundamental theorem of projective geometry. See Wikipedia: Fundamental theorem of projective geometry or E. Artin, Geometric Algebra, Interscience, 1957, Theorem 2.26.

In fact, the Segre map is an isomorphism

$$\mathbb{P}^m \times \mathbb{P}^n \xrightarrow{\simeq} H \subset \mathbb{P}^{mn+m+n}.$$

To see this, note that the Segre map defines an isomorphism from the open affine $\mathbb{P}^m \times \mathbb{P}^n$ where $a_0 b_0 \neq 0$ onto the open affine of H where $w_{00} \neq 0$, with inverse

$$(w_{00} : \ldots : w_{ij} : \ldots) \mapsto ((w_{00} : \ldots : w_{m0}), (w_{00} : \ldots : w_{0n})),$$

and that a similar statement holds with $0, 0$ replaced by i, j.

For example, the map

$$((a_0 : a_1), (b_0 : b_1)) \mapsto (\underset{w}{a_0 b_0} : \underset{x}{a_0 b_1} : \underset{y}{a_1 b_0} : \underset{z}{a_1 b_1}) \colon \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$$

is an isomorphism from $\mathbb{P}^1 \times \mathbb{P}^1$ onto the hypersurface

$$H : \quad WZ = XY,$$

with inverse

$$(w : x : y : z) \mapsto ((w : y), (w : x))$$

on the open affine of H where $w \neq 0$.

In particular, we see that $\mathbb{P}^1 \times \mathbb{P}^1$ is a projective variety. It is not isomorphic to $\mathbb{P}^2$, because, in $\mathbb{P}^2$, any two closed curves intersect (section 6p), whereas, in $\mathbb{P}^1 \times \mathbb{P}^1$, this is not true (consider two vertical lines).

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.

The product $\mathbb{P}^1 \times \mathbb{P}^n$ contains many disjoint copies of $\mathbb{P}^n$ as closed subvarieties. Thus finite disjoint unions of copies of $\mathbb{P}^n$ are projective, and so finite disjoint unions of projective varieties are projective.

There is an explicit description of the topology on $\mathbb{P}^m \times \mathbb{P}^n$: the closed subsets 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_i and in the Y_j.

PROJECTIONS WITH GIVEN CENTRE

Projections with a given centre allow us to map closed subvarieties of a projective space onto closed subvarieties of a lower-dimensional projective space, possibly with the introduction of singularities.

6.27. 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 $\varphi \colon V \to \mathbb{P}^{n-d-1}$. Its image is closed (7.22, 7.7) and the map $\varphi \colon V \to \varphi(V)$ is finite (8.53).

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.[5] For example, suppose that we have a nonsingular curve C in $\mathbb{P}^3$. To project to $\mathbb{P}^2$ we need three linear forms L_0, L_1, L_2 and the centre of the projection is the point P_0 where all the 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 does not 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 1966.

Projecting a nonsingular variety in $\mathbb{P}^n$ to a lower dimensional projective space usually introduces singularities. Hironaka proved that every singular variety arises in this way in characteristic zero. See Chapter 8 below.

APPLICATION

PROPOSITION 6.28. *Every finite set S of points of a quasi-projective 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 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. □

j. 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 a 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.

k. The functor defined by projective space

Let R be a k-algebra. A submodule M of an R-module N is said to be a direct summand of N if there exists another submodule M' of M (a complement of M) such that $N = M \oplus M'$. Let M be a direct summand of a finitely generated projective R-module N. Then M is also finitely generated and projective, and so $M_{\mathfrak{m}}$ is a free $R_{\mathfrak{m}}$-module of finite rank for every maximal ideal $\mathfrak{m}$ in R. If $M_{\mathfrak{m}}$ is of constant rank r, then we say that M has rank r. See CA, §12.

Let

$$P^n(R) = \{\text{direct summands of rank 1 of } R^{n+1}\}.$$

[5]This is best possible: a nonsingular curve of degree d in $\mathbb{P}^2$ has genus $(d-1)(d-2)/2$, and so, if g is not of this form, no curve of genus g can be realized as a nonsingular curve in $\mathbb{P}^2$.

Then P^n is a functor from k-algebras to sets. When K is a field, every K-subspace of K^{n+1} is a direct summand, and so $P^n(K)$ consists of the lines through the origin in K^{n+1}.

Let H_i be the hyperplane $X_i = 0$ in k^{n+1}, and let

$$P_i(R) = \{L \in P^n(R) \mid L \oplus H_{iR} = R^{n+1}\}.$$

Let $L \in P_i(R)$; then

$$e_i = \ell + \sum_{j \neq i} a_j e_j.$$

Now

$$L \mapsto (a_j)_{j \neq i} : P_i(R) \to U_i(R) \simeq R^n$$

is a bijection. These combine to give an isomorphism $P^n(R) \to \mathbb{P}^n(R)$:

$$\begin{array}{ccccc} P^n(R) & \longrightarrow & \prod_{0 \leq i \leq n} P_i(R) & \rightrightarrows & \prod_{0 \leq i,j \leq n} P_i(R) \cap P_j(R) \\ \downarrow & & \downarrow & & \downarrow \\ \mathbb{P}^n(R) & \longrightarrow & \prod_{0 \leq i \leq n} U_i(R) & \rightrightarrows & \prod_{0 \leq i,j \leq n} U_i(R) \cap U_j(R). \end{array}$$

Let R be a commutative ring, and let L be a direct summand of rank 1 of R^{n+1}. Then L is a projective R-module of rank 1 and the images s_0, is a projective

l. Maps to projective space

In this section, we assume the reader is familiar with the definitions of coherent sheaves and vector bundles (Chapter 13).

To give a regular map from a variety V to $\mathbb{P}^n$ is the same as giving an isomorphism class of pairs $(L, (s_0, \ldots, s_n))$ where L is an invertible sheaf on V and $s_0, \ldots, s_n$ are global sections of L

Let V be a complete variety. A map $\varphi : V \to \mathbb{P}^n$ is an isomorphism onto its (closed) image if and only if it separates points and tangent directions (ZMT).

For D a divisor on a variety V, we let

$$\begin{aligned} L(D) &= \{f \in k(V) \mid (f) + D \geq 0\} \cup \{0\} = H^0(V, \mathcal{L}(D)), \\ |D| &= \{(f) + D \mid f \in L(D)\}. \end{aligned}$$

Thus $|D|$ is the complete linear system containing D.

A projective embedding of an elliptic curve can be constructed as follows: let $D = P_0$, where P_0 is the zero element of A, and choose a suitable basis $1, x, y$ of $L(3D)$; then the map $A \to \mathbb{P}^2$ defined by $\{1, x, y\}$ identifies A with the cubic projective curve

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

(see Hartshorne 1977, IV, 4.6). This argument can be extended to every abelian variety.

Under construction.

m. Grassmann varieties

We show that the linear subvarieties of fixed dimension in a given projective space, for example, the lines in $\mathbb{P}^n$, form a projective variety.

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 6.29. *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 (6.34) 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 6.30. 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 (9.41, 9.42) below.

REMARK 6.31. 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,

$$G_d(V)_{S'} \approx \mathrm{Hom}(S_0, S') \approx \mathrm{Hom}(E/S', S'). \tag{27}$$

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

$$\mathrm{End}(E) = \begin{pmatrix} \mathrm{End}(S_0) & \mathrm{Hom}(S', S_0) \\ \mathrm{Hom}(S_0, S') & \mathrm{End}(S') \end{pmatrix},$$

and the bijections (27) 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 6.32. The bijection (27) 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. p. 73). Therefore, the tangent space to $G_d(E)$ at S_0,

$$T_{S_0}(G_d(E)) \simeq \mathrm{Hom}(S_0, S') \simeq \mathrm{Hom}(S_0, E/S_0). \tag{28}$$

Since the dimension of this space does not depend on the choice of S_0, this shows that $G_d(E)$ is nonsingular (4.39).

REMARK 6.33. 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 6.34. 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

$$e_{i_1} \wedge \ldots \wedge e_{i_d} \quad (i_1 < \cdots < i_d)$$

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

$$S \mapsto \bigwedge^d S : G_d(E) \to \mathbb{P}(\bigwedge^d E) \tag{29}$$

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. 6.35 below).

FIRST PROOF OF PROPOSITION 6.29.

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

$$P(S) = (a_0 : \ \ldots : a_{ij} : \ \ldots : \ \ldots),$$

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 ith column with the jth column. Let U_0 be the ("typical") standard open subset of $\mathbb{P}^{\binom{n}{d}-1}$ consisting of the points with nonzero zeroth coordinate. Clearly,[6] $P(S) \in U_0$ if and only if $S \in G_d(E)_{S'}$. We shall prove the proposition by showing that $P : G_d(E)_{S'} \to U_0$ 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

$$e_i' = e_i + \textstyle\sum_{d<j\leq n} a_{ij} e_j \tag{30}$$

[6]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 $S' \cap S$.

denote the unique element of S projecting to e_i. Then $e_1',\dots,e_d'$ is a basis for S. Conversely, for any $(a_{ij})\in k^{d(n-d)}$, the e_i' defined by (30) span an $S\in G_d(E)_{S'}$ and project to the e_i. 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 (27) in terms of matrices).

Now, if $S\leftrightarrow(a_{ij})$, then

$$P(S)=(1:\dots:a_{ij}:\ \dots:\ \dots:f_k(a_{ij}):\ \dots).$$

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

$$(\dots,a_{ij},\dots)\mapsto(\dots,f_k(a_{ij}),\dots)\colon \mathbb{A}^{d(n-d)}\to\mathbb{A}^{\binom{n}{d}-d(n-d)-1},$$

which is closed (5.28).

SECOND PROOF OF PROPOSITION 6.29.

An exterior d-vector v is said to be ***pure*** (or ***decomposable***) if there exist vectors $e_1,\dots,e_d\in V$ such that $v=e_1\wedge\dots\wedge e_d$. According to 6.34, the image of $G_d(E)$ in $\mathbb{P}(\bigwedge^d E)$ consists of the lines through the pure d-vectors.

LEMMA 6.35. *Let w be a nonzero d-vector and let*

$$M(w)=\{v\in E\mid v\wedge w=0\};$$

then $\dim_k M(w)\le d$*, with equality if and only if w is pure.*

PROOF. Let $e_1,\dots,e_m$ be a basis of $M(w)$, and extend it to a basis $e_1,\dots,e_m,\dots,e_n$ of V. Write

$$w=\sum_{1\le i_1<\dots<i_d} a_{i_1\dots i_d}e_{i_1}\wedge\dots\wedge e_{i_d},\quad a_{i_1\dots i_d}\in k.$$

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 $ae_1\wedge\dots\wedge e_m\wedge\dots$. It follows that $m\le d$, and $m=d$ if and only if $w=ae_1\wedge\dots\wedge e_d$ with $a\neq0$. □

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 $\le n-d$ (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.

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 $\le n-d$ 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

$$G_d(E)=\mathbb{P}(\bigwedge^d E)\cap W.$$

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***

$$F: \quad E \supset E^1 \supset \cdots \supset E^r \supset 0 \tag{31}$$

with E^i a subspace of E of dimension d_i. The map

$$G_{\mathbf{d}}(E) \xrightarrow{F \mapsto (E^i)} \prod_i G_{d_i}(E) \subset \prod_i \mathbb{P}(\textstyle\bigwedge^{d_i} E)$$

realizes $G_{\mathbf{d}}(E)$ as a closed subset[7] $\prod_i G_{d_i}(E)$, 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

$$\varphi^i : E^i \to E/E^i, \quad 1 \le i \le r, \tag{32}$$

that are compatible in the sense that

$$\varphi^i | E^{i+1} \equiv \varphi^{i+1} \bmod E^{i+1}.$$

ASIDE 6.36. 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 (6.33), 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

$$g \mapsto gF_0 : \ \mathrm{GL}(E)/P(F_0) \to G_{\mathbf{d}}(E)$$

is an isomorphism of algebraic varieties. Because $G_{\mathbf{d}}(E)$ is projective, this shows that $P(F_0)$ is a parabolic subgroup of $\mathrm{GL}(E)$.

n. Bézout'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.[8]

THEOREM 6.37. *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 2.62 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 $(a : b : c) \in C \cap D$.

---

[7] 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 (6.35) that $M(u_i) \subset M(u_{i+1})$ if and only if the map

$$v \mapsto (v \wedge u_i, v \wedge u_{i+1}) : E \to \textstyle\bigwedge^{d_i+1} E \oplus \bigwedge^{d_{i+1}+1} E$$

has rank $\le n - d_i$ (in which case it has rank $n - d_i$). Thus, $G_{\mathbf{d}}(E)$ is defined by the vanishing of many minors.

[8] Bézout 1779, but announced earlier by MacLaurin 1720.

Let $F(X,Y,Z)$ and $G(X,Y,Z)$ be the polynomials defining C and D, and write

$$F = s_0Z^m + s_1Z^{m-1} + \cdots + s_m, \qquad G = t_0Z^n + t_1Z^{n-1} + \cdots + t_n$$

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 (7.27 below; Wikipedia: RESULTANT) of F and G, regarded as polynomials in Z. It is either a homogeneous polynomial of degree mn in X and Y or 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 7.28 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 6.38. 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.

o. Hilbert polynomials

Recall that for a projective variety $V \subset \mathbb{P}^n$, the homogeneous coordinate ring

$$k_{\mathrm{hom}}[V] = k[X_0, \ldots, X_n]/\mathfrak{b} = k[x_0, \ldots, x_n],$$

where $\mathfrak{b} = I(V)$. The ideal $\mathfrak{b}$ is graded, and so $k_{\mathrm{hom}}[V]$ 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 k-subspace spanned by the monomials in the x_i of degree m. In particular, $k_{\mathrm{hom}}[V]_m$ is a finite-dimensional k-vector space, and we define the ***Hilbert function*** of V to be

$$H(V,m) \stackrel{\mathrm{def}}{=} \dim_k k_{\mathrm{hom}}[V]_m.$$

It is a function $\mathbb{N} \to \mathbb{N}$. Note that

$$k_{\text{hom}}[V]_m = k[X_0, \dots, X_n]_m / \mathfrak{b}_m,$$

so $H(V, m)$ is the codimension, in the space of homogeneous polynomials of degree m in the X_i, of the subspace of those that vanish on V.

EXAMPLE 6.39. By definition $k_{\text{hom}}[\mathbb{P}^n] = k[X_0, \dots, X_n]$, so $k_{\text{hom}}[\mathbb{P}^n]_m$ consists of the homogeneous polynomials of degree m in $X_0, \dots, X_n$. There are $\binom{m+n}{n}$ monomials of degree m in $n+1$ variables, so

$$H(\mathbb{P}^n, m) = \binom{m+n}{n} = \frac{(m+n)\cdots(m+1)}{n!}.$$

That there are $\binom{m+n}{n}$ monomials 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

$$F(X_0, X_1, \dots, X_n) = F_1(X_1, \dots, X_n) + X_0 F_2(X_0, X_1, \dots, X_n)$$

with F_1 homogeneous of degree m and F_2 homogeneous of degree $m-1$. But

$$\binom{m+n}{m} = \binom{m+n-1}{m} + \binom{m+n-1}{m-1}$$

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.

EXAMPLE 6.40. Let $V = \{P_1, P_2, P_3\}$ be a set of three points in $\mathbb{P}^2$. There exists a nonzero linear polynomial vanishing at all the points if and only if they are collinear. Thus

$$H(V, 1) = \begin{cases} 1 & \text{if the points are collinear} \\ 2 & \text{otherwise.} \end{cases}$$

For $m \geq 2$, the map

$$f \mapsto (f(P_0), f(P_1), f(P_2)) \colon k[X_0, X_1, X_2]_m \to k^3$$

is surjective, and so its kernel has codimension 3. Thus

$$H(V, m) = 3 \text{ for } m \geq 2.$$

Similarly, if V is a set of δ points $\mathbb{P}^2$, then $H(V, 1)$ depends on the dimension of the subspace spanned by the points, but

$$H(V, m) = \delta \text{ for } m \geq \delta - 1.$$

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. For example, if V is the hypersurface in $\mathbb{P}^n$ defined by a homogeneous polynomial of degree δ and $H_1, \dots, H_{n-1}$ are hyperplanes in $\mathbb{P}^n$, then "in general",

$$|V \cap H_1 \cap \dots \cap H_{n-1}| = \delta.$$

THEOREM 6.41. *Let $V \subset \mathbb{P}^n$ be a projective variety. There exists a unique polynomial $P(V,T) \in \mathbb{Q}[T]$ such that*

$$P(V,m) = H(V,m)$$

for all sufficiently large m. Moreover,

$$P(V,T) = \frac{\delta}{d!}T^d + \text{terms of lower degree,}$$

where d is the dimension of V and δ its degree.

PROOF. Omitted (for the present). □

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.

For example,

$$P(\mathbb{P}^n,T) = \binom{T+n}{n} = \frac{(T+n)\cdots(T+1)}{n!},$$

and if V is a set of δ points in $\mathbb{P}^2$, then

$$P(V,T) = \delta.$$

EXAMPLE 6.42. Let V be the image of the Veronese map

$$(a_0 : a_1) \mapsto (a_0^\delta : a_0^{\delta-1}a_1 : \ldots : a_1^\delta) \colon \mathbb{P}^1 \to \mathbb{P}^\delta, \quad \delta \in \mathbb{N}.$$

Then $k_{\text{hom}}[V]_m$ can be identified with the set of homogeneous polynomials of degree $m \cdot \delta$ in two variables (look at the map $\mathbb{A}^2 \to \mathbb{A}^{\delta+1}$ given by the same equations), which is a space of dimension $\delta m + 1$, and so

$$P(V,T) = \delta T + 1.$$

Thus V has dimension 1 (which we knew) and degree δ.

EXAMPLE 6.43. Let V be the curve in $\mathbb{P}^2$ defined by a homogeneous polynomial F of degree δ. If $\mathfrak{b}$ is the ideal in $k[X_0,X_1,X_2]$ corresponding to $\mathfrak{b}$, then $\mathfrak{b}_m$ consists of the polynomials of degree m divisible by F, and so

$$\dim \mathfrak{b}_m = \binom{m-\delta+2}{2}$$

if $m \geq \delta$. Therefore, for $m \geq \delta$,

$$H(V,m) = \binom{m+2}{2} - \binom{m-\delta+2}{2} = \delta m - \frac{\delta(\delta-2)}{2}.$$

Hence

$$P(V,T) = \delta T - \frac{\delta(\delta-2)}{2}.$$

Macaulay2 knows how to compute Hilbert polynomials.

p. Dimensions

The results for affine varieties extend to projective varieties with one important simplification: if V and W are closed subvarieties of dimensions r and s in $\mathbb{P}^n$ and $r+s \geq n$, then $V \cap W \neq \emptyset$. For example, any two closed curves in $\mathbb{P}^2$ intersect.

THEOREM 6.43. *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 does not follow immediately from 3.42 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 $V(\mathfrak{a}) \cap V(f) \neq \emptyset$. □

COROLLARY 6.44. *Let $f_1,\ldots,f_r$ 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. □

PROPOSITION 6.45. *Let Z be an irreducible closed 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 3.47. □

PROPOSITION 6.46. *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 6.47. *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 $W' = V(\mathfrak{b})$ 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 6.48. *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 lemma below shows that there is a hyperplane in k^{n+1} not intersecting V.

Suppose that $r > 0$, 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 below 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 intersecting $V \cap H$. Take $E = E' \cap H$. □

LEMMA 6.49. *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, cannot be identically zero on k^n (Exercise 1-1). □

Let V and E be as in Proposition 6.48. 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.

In general, a regular map from a variety V to $\mathbb{P}^n$ corresponds to a line bundle on V and a set of global sections of the line bundle. All line bundles on $\mathbb{A}^n \smallsetminus \{\text{origin}\}$ are trivial (see, for example, Hartshorne II 7.1 and II 6.2), from which it follows that all regular maps $\mathbb{A}^{n+1} \smallsetminus \{\text{origin}\} \to \mathbb{P}^m$ are given by a family of homogeneous polynomials. Assuming this, it is possible to prove the following result.

COROLLARY 6.50. *Let $\alpha : \mathbb{P}^n \to \mathbb{P}^m$ be regular; if $m < n$, then α is constant.*

PROOF. Let $\pi : \mathbb{A}^{n+1} - \{\text{origin}\} \to \mathbb{P}^n$ 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 6.43 shows they have a common zero and so α is not defined on all of $\mathbb{P}^n$. Hence the F_i must be constant. □

q. Products

It is useful to have an explicit description of the topology on some product varieties.

The topology on $\mathbb{P}^m \times \mathbb{P}^n$.

Suppose that we have a collection of polynomials $F_i(X_0, \ldots, X_m; Y_0, \ldots, Y_n)$, $i \in I$, each of which is separately homogeneous in the X_i and Y_j. Then the equations

$$F_i(X_0, \ldots, X_m; Y_0, \ldots, Y_n) = 0, \quad i \in I,$$

define a closed subset of $\mathbb{P}^m \times \mathbb{P}^n$, and every closed subset of $\mathbb{P}^m \times \mathbb{P}^n$ arises in this way from a (finite) set of polynomials.

The topology on $\mathbb{A}^m \times \mathbb{P}^n$

The closed subsets of $\mathbb{A}^m \times \mathbb{P}^n$ are exactly those defined by sets of equations

$$F_i(X_1, \ldots, X_m; Y_0, \ldots, Y_n) = 0, \quad i \in I,$$

with each F_i homogeneous in the Y_j.

The topology on $V \times \mathbb{P}^n$

Let V be an irreducible affine algebraic variety. We look more closely at the topology on $V \times \mathbb{P}^n$ in terms of ideals. Let $A = k[V]$, 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 $V \times \mathbb{A}^{n+1}$: for $f \in A$ and $g \in k[X_0, \ldots, X_n]$, $f \otimes g$ is the function

$$(v, \mathbf{a}) \mapsto f(v) \cdot g(\mathbf{a}) \colon V \times \mathbb{A}^{n+1} \to k.$$

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 graded ideal $\mathfrak{b} \subset B$. It makes sense to speak of the zero set $V(\mathfrak{b}) \subset V \times \mathbb{P}^n$ of such an ideal. For any ideal $\mathfrak{a} \subset A$, $\mathfrak{a}B$ is graded, and $V(\mathfrak{a}B) = V(\mathfrak{a}) \times \mathbb{P}^n$.

LEMMA 6.51. *(a) For each graded ideal* $\mathfrak{b} \subset B$*, the set* $V(\mathfrak{b})$ *is closed, and every closed subset of* $V \times \mathbb{P}^n$ *is of this form.*

(b) The set $V(\mathfrak{b})$ *is empty if and only if* $\mathrm{rad}(\mathfrak{b}) \supset (X_0, \ldots, X_n)$.

(c) If V *is irreducible, then* $V = V(\mathfrak{b})$ *for some graded prime ideal* $\mathfrak{b}$.

PROOF. (a) 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 $V^{\mathrm{aff}}(\mathfrak{b}) \subset V \times \mathbb{A}^{n+1}$ defined by $\mathfrak{b}$ is contained in $V \times \{\text{origin}\}$. But

$$\sum a_{i_0 \ldots i_n} X_0^{i_0} \ldots X_n^{i_n}, \quad a_{i_0 \ldots i_n} \in k[V],$$

is zero on $V \times \{\text{origin}\}$ if and only if its constant term is zero, and so

$$I^{\mathrm{aff}}(V \times \{\text{origin}\}) = (X_0, X_1, \ldots, X_n).$$

Thus, the Nullstellensatz shows that $V(\mathfrak{b}) = \emptyset \Rightarrow \mathrm{rad}(\mathfrak{b}) = (X_0, \ldots, X_n)$. 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 $V \times \mathbb{A}^{n+1}$ is also irreducible, and so $IV(\mathfrak{b})$ is prime. □

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 $Y^2Z = X^3 + aXZ^2 + bZ^3$ 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 6.26) is not contained in any hyperplane of $\mathbb{P}^{mn+m+n}$.

6-7. Write $0, 1, \infty$ for the points $(0:1)$, $(1:1)$, and $(1:0)$ on $\mathbb{P}^1$.

(a) Let α be an automorphism of $\mathbb{P}^1$ such that

$$\alpha(0) = 0, \quad \alpha(1) = 1, \quad \alpha(\infty) = \infty.$$

Show that α is the identity map.

(b) Let P_0, P_1, P_2 be distinct points on $\mathbb{P}^1$. Show that there exists an $\alpha \in \mathrm{PGL}_2(k)$ such that

$$\alpha(0) = P_0, \quad \alpha(1) = P_1, \quad \alpha(\infty) = P_2.$$

(c) Deduce that $\mathrm{Aut}(\mathbb{P}^1) \simeq \mathrm{PGL}_2(k)$.

6-8. Show that the functor

$$R \rightsquigarrow P^n(R) = \{\text{direct summands of rank 1 of } R^{n+1}\}$$

satisfies the criterion 5.71 to arise from an algebraic prevariety. (This gives an alternative definition of $\mathbb{P}^n$.)

6-9. (a) Let $V \subset \mathbb{A}^n$ and $W \subset \mathbb{P}^m$ be algebraic varieties and $\varphi\colon V \to W$ a map. Show that φ is regular if and only if every point in V has an open neighbourhood U on which there are regular functions $f_0, \dots, f_m$ such that

$$\varphi(a_1, \dots, a_n) = (f_0(a_1, \dots, a_n) : \dots : f_m(a_1, \dots, a_n))$$

for all $(a_1, \dots, a_n) \in U$.

(b) Show that, for a regular map φ as in (a), it may not be possible to take $U = V$. Hint: Let $V \subset \mathbb{A}^4$ be the complement of $(0,0,0,0)$ in

$$XY - ZW = 0,$$

and let $\varphi\colon V \to \mathbb{P}^1$ send (w, x, y, z) to $(x : z)$ if one of x or z is nonzero and $(w, 0, y, 0)$ to $(w : y)$. See sx4626969 (Mohan).

Chapter 7

Complete Varieties

Complete varieties are the analogues in the category of algebraic varieties of compact topological spaces in the category of Hausdorff topological spaces.

If V is compact, then every continuous map $V \to T$ with T Hausdorff sends compact sets to compact sets, hence closed sets to closed sets, i.e., it is a closed map. Moreover, a Hausdorff space V is compact if and only if the map $V \to \{\text{point}\}$ is universally closed, i.e., for all topological spaces T, the projection map $q\colon V \times T \to T$ is closed (Bourbaki TG, I, 10.2, Cor. 1 to Thm 1).

a. Definition and basic properties

Definition

DEFINITION 7.1. A prevariety V over k is ***complete*** if

(a) it is separated, and

(b) for all algebraic varieties T, the projection map $q\colon V \times T \to T$ is closed.

We shall see (7.22) that projective varieties are complete.

EXAMPLE 7.2. The projection map

$$(x, y) \mapsto y\colon \mathbb{A}^1 \times \mathbb{A}^1 \to \mathbb{A}^1.$$

is not closed. For example, the variety $V\colon XY = 1$ is closed in $\mathbb{A}^2$ but its image in $\mathbb{A}^1$ omits the origin. On the other hand, the projection map $\mathbb{P}^1 \times \mathbb{A}^1 \to \mathbb{A}^1$ is closed. The closure of V in $\mathbb{P}^1 \times \mathbb{A}^1$ is

$$\bar{V} \overset{\text{def}}{=} \{((x\colon z), y) \in \mathbb{P}^1 \times \mathbb{A}^1 \mid xy = z^2\},$$

and the point $((x\colon 0), 0)$ of $\bar{V}$ projects to 0.

Properties

7.3. *Closed subvarieties of complete varieties are complete.*

Let Z be a closed subvariety of a complete variety V. For any variety T, $Z \times T$ is closed in $V \times T$, and so the restriction of the closed map $q\colon V \times T \to T$ to $Z \times T$ is also closed.

7.4. *A variety is complete if and only if its irreducible components are complete.*

Each irreducible component is closed, and hence complete if the variety is complete (7.3). Conversely, suppose that the irreducible components V_i of a variety V are complete. If Z is closed in $V \times T$, then $Z_i \stackrel{\text{def}}{=} Z \cap (V_i \times T)$ is closed in $V_i \times T$. Therefore, $q(Z_i)$ is closed in T, and so $q(Z) = \bigcup q(Z_i)$ is also closed.

7.5. *Products of complete varieties are complete.*

Let $V_1, \ldots, V_n$ be complete varieties, and let T be a variety. The projection $\left(\prod_i V_i\right) \times T \to T$ is the composite of the projections

$$V_1 \times \cdots \times V_n \times T \to V_2 \times \cdots \times V_n \times T \to \cdots \to V_n \times T \to T,$$

all of which are closed.

7.6. *If $\varphi\colon V \to W$ is surjective and V is complete, then W is complete.*

Let T be a variety, and let Z be a closed subset of $W \times T$. Let Z' be the inverse image of Z in $V \times T$. Then Z' is closed, and its image in T equals that of Z.

7.7. *Let $\varphi\colon V \to W$ be a regular map of varieties. If V is complete, then $\varphi(V)$ is a complete closed subvariety of W. In particular, every complete subvariety of a variety is closed.*

Let $\Gamma_\varphi \stackrel{\text{def}}{=} \{(v, \varphi(v))\} \subset V \times W$ be the graph of φ. It is a closed subset of $V \times W$ (because V is a variety, see 5.28), and $\varphi(V)$ is the projection of Γ_φ into W. Therefore $\varphi(V)$ is closed, and 7.6 shows that it is complete. The second statement follows from the first applied to the inclusion map.

7.8. *A regular map $V \to \mathbb{P}^1$ from a complete connected variety V is either constant or surjective.*

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).

7.9. *The only regular functions on a complete connected variety are the constant functions.*

A regular function on a variety V is a regular map $f\colon V \to \mathbb{A}^1 \subset \mathbb{P}^1$, to which we can apply 7.8.

7.10. *A regular map $\varphi\colon V \to W$ from a complete connected variety to an affine variety has image equal to a point. In particular, every complete connected affine variety is a point.*

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 $x_i\colon \mathbb{A}^n \to \mathbb{A}^1$. Each φ_i is a regular function on V, and hence is constant. (Alternatively, apply 5.11.) This proves the first statement, and the second follows from the first applied to the identity map.

7.11. *In order to show that a variety V is complete, it suffices to check that $q\colon V \times T \to T$ is a closed mapping when T is affine (or even an affine space $\mathbb{A}^n$).*

Every variety T can be written as a finite union of open affine subvarieties $T = \bigcup T_i$. If Z is closed in $V \times T$, then $Z_i \stackrel{\text{def}}{=} Z \cap (V \times T_i)$ is closed in $V \times T_i$. Therefore, $q(Z_i)$ is closed in T_i for all i. As $q(Z_i) = q(Z) \cap T_i$, this shows that $q(Z)$ is closed. This shows that it suffices to check that $V \times T \to T$ is closed for all affine varieties T. But T can be realized as a closed subvariety of $\mathbb{A}^n$, and then $V \times T \to T$ is closed if $V \times \mathbb{A}^n \to \mathbb{A}^n$ is closed.

Remarks

7.12. The statement that a complete variety V is closed in every larger variety W perhaps explains the name: if V is a complete subvariety of a connected variety W and $\dim V = \dim W$, then $V = W$. Contrast $\mathbb{A}^n \subset \mathbb{P}^n$.

7.13. Here is another criterion: a variety V is complete if and only if every regular map $C \smallsetminus \{P\} \to V$ extends uniquely to a regular map $C \to V$; here P is a nonsingular point on a curve C. Intuitively, this says that all Cauchy sequences have limits in V and that the limits are unique.

b. Proper maps

DEFINITION 7.14. 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 regular maps $T \to S$, the base change $\varphi'\colon V \times_S T \to T$ of φ is closed.

7.15. For example, a variety V is complete if and only if the map $V \to \{\text{point}\}$ is proper.

7.16. From its very definition, it is clear that the base change of a proper map is proper. In particular,

(a) if V is complete, then $V \times S \to S$ is proper,

(b) if $\varphi\colon V \to S$ is proper, then the fibre $\varphi^{-1}(P)$ over a point P of S is complete.

7.17. If $\varphi\colon V \to S$ is proper, and W is a closed subvariety of V, then $W \xrightarrow{\varphi} S$ is proper.

PROPOSITION 7.18. *A composite of proper maps is proper.*

PROOF. Let $V_3 \to V_2 \to V_1$ be proper maps, and let T be a variety. Consider the diagram

$$\begin{array}{ccc}
V_3 & \longleftarrow & V_3 \times_{V_2} (V_2 \times_{V_1} T) \simeq V_3 \times_{V_1} T \\
\downarrow & & \downarrow \text{closed} \\
V_2 & \longleftarrow & V_2 \times_{V_1} T \\
\downarrow & & \downarrow \text{closed} \\
V_1 & \longleftarrow & T.
\end{array}$$

Both smaller squares are cartesian, and hence so also is the outer square. The statement is now obvious from the fact that a composite of closed maps is closed. □

COROLLARY 7.19. *If $V \to S$ is proper and S is complete, then V is complete.*

PROOF. Apply the proposition to $V \to S \to \{\text{point}\}$. □

COROLLARY 7.20. *The inverse image of a complete variety under a proper map is complete.*

PROOF. Let $\varphi\colon V \to S$ be proper, and let Z be a complete subvariety of S. Then $V \times_S Z \to Z$ is proper, and $V \times_S Z \simeq \varphi^{-1}(Z)$. □

EXAMPLE 7.21. Let $f \in k[T_1, \ldots, T_n, X, Y]$ be homogeneous of degree m in X and Y, and let H be the subvariety of $\mathbb{A}^n \times \mathbb{P}^1$ defined by

$$f(T_1, \ldots, T_n, X, Y) = 0.$$

The projection map $\mathbb{A}^n \times \mathbb{P}^1 \to \mathbb{A}^n$ defines a regular map $H \to \mathbb{A}^n$, which is proper (7.22, 7.15). The fibre over a point $(t_1, \ldots, t_n) \in \mathbb{A}^n$ is the subvariety of $\mathbb{P}^1$ defined by the polynomial

$$f(t_1, \ldots, t_n, X, Y) = a_0 X^m + a_1 X^{m-1} Y + \cdots + a_m Y^m, \quad a_i \in k.$$

Assume that not all a_i are zero. Then this is a homogeneous of degree m and so the fibre always has m points counting multiplicities. The points that "disappeared off to infinity" when $\mathbb{P}^1$ was taken to be $\mathbb{A}^1$ (see p. 50) have literally become the point at infinity on $\mathbb{P}^1$.

c. Projective varieties are complete

The reader may skip this section since the main theorem is given a more explicit proof in Theorem 7.31 below.

THEOREM 7.22. *A projective variety is complete.*

PROOF. After 7.3, it suffices to prove the Theorem for projective space $\mathbb{P}^n$ itself; thus we have to prove that the projection map $\mathbb{P}^n \times W \to W$ is a closed mapping in the case that W is an irreducible affine variety (7.11).

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 that $p(Z)$ 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 graded prime ideal in $B = A[X_0, \ldots, X_n]$ (6.51).

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 3.34a) 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 graded 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 6.51b), 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 graded 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 $g = \sum m_i b_i$, $m_i \in \mathfrak{m}$, $b_i \in B$, then $g_N = \sum m_i b_{iN}$; and $h_N \in \mathfrak{b}$ because $\mathfrak{b}$ is homogeneous. Together these show $f \in \mathfrak{m}B_N + B_N \cap \mathfrak{b}$.

Let $M = B_N / B_N \cap \mathfrak{b}$, regarded as an A-module. The displayed equation says that $M = \mathfrak{m}M$. The argument in the proof of Nakayama's lemma (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. □

Notes

7.23. Every complete curve is projective.

7.24. Every nonsingular complete surface is projective (Zariski), but there exist singular complete surfaces that are not projective (Nagata).

7.25. There exist nonsingular complete three-dimensional varieties that are not projective (Nagata, Hironaka).

7.26. A nonsingular complete irreducible variety V is projective if and only if every finite set of points of V is contained in an open affine subset of V (Conjecture of Chevalley; proved by Kleiman[1]; see 6.22 for the necessity).

d. Elimination theory

When given a system of polynomial equations to solve, we first use some of the equations to eliminate some of the variables; we then find the solutions of the reduced system, and go back to find the solutions of the original system. Elimination theory does this more systematically.

The fact that $\mathbb{P}^n$ is complete has the following explicit restatement: for each system of polynomial equations

$$(*)\begin{cases} P_1(X_1,\dots,X_m;Y_0,\dots,Y_n) = 0 \\ \quad\vdots \\ P_r(X_1,\dots,X_m;Y_0,\dots,Y_n) = 0 \end{cases}$$

such that each P_i is homogeneous in the Y_j, there exists a system of polynomial equations

$$(**)\begin{cases} R_1(X_1,\dots,X_m) = 0 \\ \quad\vdots \\ R_s(X_1,\dots,X_m) = 0 \end{cases}$$

with the following property; an m-tuple $(a_1,\dots,a_m)$ is a solution of (**) if and only if there exists a nonzero n-tuple $(b_0,\dots,b_n)$ such that $(a_1,\dots,a_m,b_0,\dots,b_n)$ is a solution of (*). In other words, the polynomials $P_i(a_1,\dots,a_m;Y_0,\dots,Y_n)$ have a common zero if and only if $R_j(a_1,\dots,a_m) = 0$ for all j. The polynomials R_j are said to have been obtained from the polynomials P_i by elimination of the variables Y_i.

Unfortunately, the proof we gave of the completeness of $\mathbb{P}^n$, while short and elegant, gives no indication of how to construct (**) from (*). The purpose of elimination theory is to provide an algorithm for doing this.

[1] Kleiman, Steven L., Toward a numerical theory of ampleness. Ann. of Math. (2) 84 1966 293–344 (Theorem 3, p. 327, et seq.). See also, Hartshorne, Robin, Ample subvarieties of algebraic varieties. Lecture Notes in Mathematics, Vol. 156 Springer, 1970, I §9 p45.

Elimination theory: special case

Let $P = s_0X^m + s_1X^{m-1} + \cdots + s_m$ and $Q = t_0X^n + t_1X^{n-1} + \cdots + t_n$ be polynomials. The ***resultant*** of P and Q is defined to be the determinant

$$\begin{vmatrix} s_0 & s_1 & \ldots & s_m & & \\ & s_0 & \ldots & & s_m & \\ & & \ldots & & & \ldots \\ t_0 & t_1 & \ldots & t_n & & \\ & t_0 & \ldots & & t_n & \\ & & \ldots & & & \ldots \end{vmatrix} \qquad \begin{matrix} n \text{ rows} \\ \\ \\ \\ m \text{ rows} \end{matrix}$$

There are n rows with $s_0 \ldots s_m$ and m rows with $t_0 \ldots t_n$, 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 7.27. *The resultant $Res(P,Q) = 0$ 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

$$P(X)Q_1(X) - Q(X)P_1(X) = 0. \tag{33}$$

On equating the coefficients of $X^{m+n-1}, \ldots, X, 1$ in (33) 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 (33). 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 (33), 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 7.28. *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 $Q(X,Y)$, 7.28 is a restatement of 7.27. □

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 $R_j(T_1,\ldots,T_m)$ such that the $P_i(a_1,\ldots,a_m;X_0,\ldots,X_n)$ have a common zero if and only if $R_j(a_1,\ldots,a_m) = 0$ for all j. (Theorem 7.22 shows only that the R_j exist.)

Macaulay2Web can find the resultant of two polynomials in one variable: for example, entering

```
R=ZZ[x,a,b] (and then)
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.

Elimination theory: general case

In this subsection, we give a proof of Theorem 7.22, following Cartier and Tate[2], that is more explicit than that given above. Throughout, k is a field (not necessarily algebraically closed) and K is an algebraically closed field containing k.

THEOREM 7.29. *For any graded ideal* $\mathfrak{a}$ *in* $k[X_0,\ldots,X_n]$, *exactly one of the following statements is true:*

(a) *there exists an integer* $d_0 \geq 0$ *such that* $\mathfrak{a}$ *contains every homogeneous polynomial of degree* $d \geq d_0$;

(b) *the ideal* $\mathfrak{a}$ *has a nontrivial zero in* K^{n+1}.

[2] Cartier, P., Tate, J., A simple proof of the main theorem of elimination theory in algebraic geometry. Enseign. Math. (2) 24 (1978), no. 3-4, 311–317.

PROOF. Statement (a) says that the radical of $\mathfrak{a}$ contains $(X_0, \ldots, X_n)$, and so the theorem is a restatement of 6.2(a), which we deduced from the strong Nullstellensatz. For a direct proof of it, see the article of Cartier and Tate. □

THEOREM 7.30. *Let $R = \bigoplus_{d \in \mathbb{N}} R_d$ be a graded k-algebra such that $R_0 = k$, R is generated as a k-algebra by R_1, and R_d is finite-dimensional for all d. Then exactly one of the following statements is true:*

(a) *there exists an integer $d_0 \geq 0$ such that $R_d = 0$ for all $d \geq d_0$;*

(b) *no $R_d = 0$, and there exists a k-algebra homomorphism $R \to K$ whose kernel is not equal to $R^+ \stackrel{\text{def}}{=} \bigoplus_{d \geq 1} R_d$.*

PROOF. The hypotheses on R say that it is a quotient of $k[X_0, \ldots, X_n]$ by a graded ideal. Therefore 7.30 is a restatement of 7.29. □

Let $P_1, \ldots, P_r$ be polynomials in $k[T_1, \ldots, T_m; X_0, \ldots, X_n]$ with P_j homogeneous of degree d_j in the variables $X_0, \ldots, X_n$. Let J be the ideal $(P_1, \ldots, P_r)$ in $k[T_1, \ldots, T_m; X_0, \ldots, X_n]$, and let $\mathfrak{A}$ be the ideal of polynomials f in $k[T_1, \ldots, T_m]$ with the following property: there exists an integer $N \geq 1$ such that $fX_0^N, \ldots, fX_n^N$ all lie in J.

THEOREM 7.31. *Let V be the zero set of J in $\mathbb{A}^n(K) \times \mathbb{P}^n(K)$. The projection of V into $\mathbb{A}^n(K)$ is the zero set of $\mathfrak{A}$.*

Consider the ring $B = k[T_1, \ldots, T_m; X_0, \ldots, X_n]$ and its subring $B_0 = k[T_1, \ldots, T_m]$. Then B is a graded B_0-algebra with B_d the B_0-submodule generated by the monomials of degree d in $X_0, \ldots, X_n$, and J is a homogeneous (graded) ideal in B. Let $A = \bigoplus_{d \in \mathbb{N}} A_d$ be the quotient graded ring $B/J = \bigoplus_{d \in \mathbb{N}} B_d/(B_d \cap J)$. Let $\mathfrak{S}$ be the ideal of elements a of A_0 such that $aA_d = 0$ for all sufficiently large d.

THEOREM 7.32. *A ring homomorphism $\varphi\colon A_0 \to K$ extends to a ring homomorphism $\Psi\colon A \to K$ not annihilating the ideal $A^+ \stackrel{\text{def}}{=} \bigoplus_{d \geq 1} A_d$ if and only if $\varphi(\mathfrak{S}) = 0$.*

Following Cartier and Tate, we leave it to reader to check that 7.32 is equivalent to 7.31.

Proof of Theorem 7.32

We shall prove 7.32 for any graded ring $A = \bigoplus_{d \geq 0} A_d$ satisfying the following two conditions:

(a) as an A_0-algebra, A is generated by A_1;

(b) for every $d \geq 0$, A_d is finitely generated as an A_0-module.

In the statement of the theorem, K is any algebraically closed field.

The proof proceeds by replacing A with other graded rings with the properties (a) and (b) and also having the property that no A_d is zero.

Let $\varphi\colon A_0 \to K$ be a homomorphism such that $\varphi(\mathfrak{S}) = 0$, and let $\mathfrak{P} = \operatorname{Ker}(\varphi)$. Then $\mathfrak{P}$ is a prime ideal of A_0 containing $\mathfrak{S}$.

Step 1. Let J be the ideal of elements a of A for which there exists an $s \in A_0 \smallsetminus \mathfrak{P}$ such that $sa = 0$. For every $d \geq 0$, the annihilator of the A_0-module A_d is contained in $\mathfrak{S}$, hence in $\mathfrak{P}$, and so $J \cap A_d \neq A_d$. The ideal J is graded, and the quotient ring $A' = A/J$ has the required properties.

Step 2. Let A'' be the ring of fractions of A' whose denominators are in $\Sigma \stackrel{\text{def}}{=} A'_0 \smallsetminus \mathfrak{P}$. Let A''_d be the set of fractions with numerator in A'_d and denominator in Σ. Then $A'' = \bigoplus_{d \geq 0} A''_d$ is a graded ring with the required properties, and A''_0 is a local ring with maximal ideal $\mathfrak{P}'' \stackrel{\text{def}}{=} \mathfrak{P}' \cdot A'_0$.

Step 3. Let R be the quotient of A'' by the graded ideal $\mathfrak{P}'' \cdot A''$. As A''_d is a nonzero finitely generated module over the local ring A''_0, Nakayama's lemma shows that $A''_d \neq \mathfrak{P}'' A''_d$. Therefore R is graded ring with the required properties, and $k = R_0 \stackrel{\text{def}}{=} A''_0 / \mathfrak{P}''$ is a field.

Step 4. At this point R satisfies the hypotheses of Theorem 7.30. Let ε be the composite of the natural maps

$$A \to A' \to A'' \to R.$$

In degree 0, this is nothing but the natural map from A_0 to k with kernel $\mathfrak{P}$. As φ has the same kernel, it factors through ε_0, making K into an algebraically closed extension of k. Now, by Theorem 7.30, there exists a k-algebra homomorphism $f\colon R \to K$ such that $f(R^+) \neq 0$. The composite map $\Psi = f \circ \varepsilon$ has the required properties. □

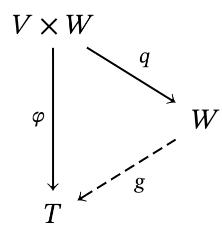
For more on elimination theory, see Cox et al. 2015, Chapter 8, Section 5.

ASIDE 7.33. Elimination theory became unfashionable several decades ago — one prominent algebraic geometer went so far as to announce that Theorem 7.22 eliminated elimination theory from mathematics,[3] 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.

e. The rigidity theorem; abelian varieties

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 7.34 (RIGIDITY THEOREM). *Let $\varphi\colon V \times W \to T$ be a regular map, and assume that V is complete, V and W are irreducible, and T is separated. If $\varphi(v, w_0)$ is independent of v for one $w_0 \in W$, then $\varphi(v, w) = g(w)$ with g a regular map $g\colon W \to T$.*



PROOF. Choose a $v_0 \in V$, and consider the regular map

$$g\colon W \to T, \quad w \mapsto \varphi(v_0, w).$$

We shall show that $\varphi = g \circ q$. Because V is complete, the projection map $q\colon V \times W \to W$ is closed. Let U be an open affine neighbourhood U of $\varphi(v_0, w_0)$; then $T \smallsetminus U$ is closed in T, $\varphi^{-1}(T \smallsetminus U)$ is closed in $V \times W$, and

$$C \stackrel{\text{def}}{=} q(\varphi^{-1}(T \smallsetminus U))$$

[3] Weil 1946, p. 31: "The device that follows, which, it may be hoped, finally eliminates from algebraic geometry the last traces of elimination-theory, is borrowed from C. Chevalley's Princeton lectures." Demazure credits Dieudonné with saying: "Il faut éliminer la théorie de l'élimination."

is closed in W. By definition, C consists of the $w \in W$ such that $\varphi(v, w) \notin U$ for some $v \in V$, and so

$$W \smallsetminus C = \{w \in W \mid \varphi(V \times \{w\}) \subset U\}.$$

As $\varphi(V, w_0) = \varphi(v_0, w_0)$, we see that $w_0 \in W \smallsetminus C$. Therefore $W \smallsetminus C$ 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 $w \in W \smallsetminus C$ (see 7.10); in fact

$$\varphi(V \times \{w\}) = \varphi(v_0, w) = g(w).$$

We have shown that φ and $g \circ q$ agree on the dense subset $V \times (W \smallsetminus C)$ of $V \times W$, and therefore on the whole of $V \times W$. □

COROLLARY 7.35. *Let $\varphi\colon V \times W \to T$ be a regular map, and assume that V is complete, that V and W are irreducible, and that T is separated. If there exist points $v_0 \in V$, $w_0 \in W$, $t_0 \in T$ such that*

$$\varphi(V \times \{w_0\}) = \{t_0\} = \varphi(\{v_0\} \times W),$$

then $\varphi(V \times W) = \{t_0\}$.

PROOF. With g as in the proof of the theorem,

$$\varphi(v, w) = g(w) = \varphi(v_0, w) = t_0.$$

□

In more colloquial terms, the corollary 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".

DEFINITION 7.36. An ***abelian variety*** is a complete connected group variety.

THEOREM 7.37. *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 7.38. *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 theorem shows that it is a homomorphism. □

ASIDE. Abelian varieties arose out of the study of Abelian integrals, whence their name.

f. Chow's Lemma

The next theorem is a useful tool in extending results from projective varieties to complete varieties. It shows that a complete variety is not far from a projective variety.

THEOREM 7.39 (CHOW'S LEMMA). *Let V be a complete irreducible variety. There exists a projective algebraic variety V' and a surjective regular map $f: V' \to V$ such that f induces an isomorphism $f^{-1}(U) \to U$ for some dense open subset U of V (in particular, f is birational),*

$$\begin{array}{ccc} f^{-1}(U) & \xrightarrow{\text{isomorphism}} & U \\ \cap & & \cap \\ V' & \xrightarrow[f]{\text{onto}} & V. \end{array}$$

Write V as a finite union of nonempty open affines, $V = U_1 \cup \ldots \cup U_n$, and let $U = \bigcap U_i$. Because V is irreducible, U is a dense in V. Realize each U_i as a dense open subset of a projective variety P_i. Then $P \stackrel{\text{def}}{=} \prod_i P_i$ is a projective variety (6.26). We shall construct an algebraic variety V' and regular maps $f: V' \to V$ and $g: V' \to P$ such that

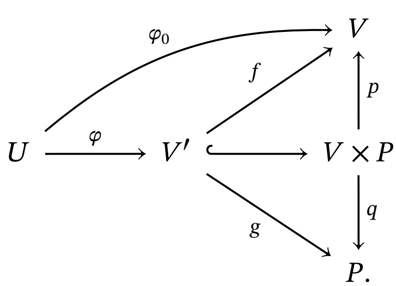
(a) f is surjective and induces an isomorphism $f^{-1}(U) \to U$;

(b) g is a closed immersion (hence V' is projective).

Let φ_0 (resp. φ_i) denote the given inclusion of U into V (resp. into P_i), and let

$$\varphi = (\varphi_0, \varphi_1, \ldots, \varphi_n): U \to V \times P_1 \times \cdots \times P_n,$$

be the diagonal map. We set $U' = \varphi(U)$ and V' equal to the closure of U' in $V \times P_1 \times \cdots \times P_n$. The projection maps $p: V \times P \to V$ and $q: V \times P \to P$ restrict to regular maps $f: V' \to V$ and $g: V' \to P$. Thus, we have a commutative diagram



(34)

PROOF OF (a)

In the upper-left triangle of the diagram (34), the maps φ and φ_0 are isomorphisms from U onto its images U' and U. Therefore f restricts to an isomorphism $U' \to U$. Note that

$$U' = \{(u, \varphi_1(u), \ldots, \varphi_n(u)) \mid u \in U\},$$

which is the graph of the map $(\varphi_1, \ldots, \varphi_n): U \to P$. Therefore, U' is closed in $U \times P$ (5.28), and so

$$U' = V' \cap (U \times P) = f^{-1}(U).$$

The map f is dominant, and $f(V') = p(V)$, which is closed because P is complete. Hence f is surjective.

PROOF OF (b)

We first show that g is an immersion. As this is a local condition, it suffices to find open subsets $V_i \subset P$ such that $\bigcup q^{-1}(V_i) \supset V'$ and each map $V' \cap q^{-1}(V_i) \xrightarrow{g} V_i$ is an immersion.

We set

$$V_i = p_i^{-1}(U_i) = P_1 \times \cdots \times U_i \times \cdots \times P_n$$

where p_i is the projection map $P \to P_i$.

We first show that the sets $q^{-1}(V_i)$ cover V'. The sets U_i cover V, hence the sets $f^{-1}(U_i)$ cover V', and so it suffices to show that

$$q^{-1}(V_i) \supset f^{-1}(U_i)$$

for all i. Consider the diagrams

$$\begin{array}{ccc} q^{-1}(V_i) & \longrightarrow & U_i \\ \downarrow & & \downarrow{\scriptstyle \varphi_i} \\ V \times P & \xrightarrow{p_i \circ q} & P_i \end{array} \qquad \begin{array}{ccc} f^{-1}(U_i) & \xrightarrow{f} & U_i \\ \downarrow & & \downarrow{\scriptstyle \varphi_i} \\ V \times P & \xrightarrow{p_i \circ q} & P_i \end{array} \qquad \begin{array}{ccc} U & \xrightarrow{\varphi_0} & U_i \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi_i} \\ V \times P & \xrightarrow{p_i \circ q} & P_i. \end{array}$$

The diagram at left is cartesian, i.e., it realizes $q^{-1}(V_i)$ as the fibred product

$$q^{-1}(V_i)\_ = (V \times P) \times_{P_i} U_i,$$

and so it suffices to show that the middle diagram commutes. But U' is dense in V', hence in $f^{-1}(U_i)$, and so it suffices to prove that the middle diagram commutes with $f^{-1}(U_i)$ replaced by U'. But then it becomes the diagram at right, which obviously commutes.

We next show that

$$V' \cap q^{-1}(V_i) \xrightarrow{g} V_i$$

is an immersion for each i. Recall that

$$V_i = U_i \times P^i, \quad \text{where } P^i = \prod\nolimits_{j \neq i} P_j.$$

and so

$$q^{-1}(V_i) = V \times U_i \times P^i \subset V \times P.$$

Let Γ_i denote the graph of the map

$$\left(U_i \times P^i \xrightarrow{p_i} U_i \hookrightarrow V\right).$$

Being a graph, Γ_i is closed in $V \times (U_i \times P^i)$ and the projection map $V \times (U_i \times P^i) \to U_i \times P^i$ restricts to an isomorphism $\Gamma_i \to U_i \times P^i$. In other words, Γ_i is closed in $q^{-1}(V_i)$, and the projection map $q^{-1}(V_i) \to V_i$ restricts to an isomorphism $\Gamma_i \to V_i$. As Γ_i is closed in $q^{-1}(V_i)$ and contains U', it contains $V' \cap q^{-1}(V_i)$, and so the projection map $q^{-1}(V_i) \to V_i$ restricts to an immersion $V' \cap q^{-1}(V_i) \to V_i$.

Finally, $V \times P$ is complete because V and P are, and so V' is complete (7.3). Hence $g(V)$ is closed (7.7), and so g is a closed immersion.

Notes

7.40. Let V be a complete variety, and let $V_1, \ldots, V_s$ be the irreducible components of V. Each V_i is complete (7.4), and so there exists a surjective birational regular map $V_i' \to V_i$ with V_i' projective (7.39). Now $\bigsqcup V_i'$ is projective 6.26, and the composite

$$\bigsqcup V_i' \to \bigsqcup V_i \to V$$

is surjective and birational.

7.41. Chow (1956, Lemma 1)[4] proved essentially the statement 7.42 by essentially the above argument. He used the lemma to prove that all homogeneous spaces are quasi-projective. See also EGA II, 5.6.1.

g. Analytic spaces; Chow's theorem

We summarize a little of Serre, J-P., Géométrie algébrique et géométrie analytique. Ann. Inst. Fourier, Grenoble 6 (1955–1956), 1–42, commonly referred to as GAGA.

7.42. The following statement is more general than Theorem 7.39: for every algebraic variety V, there exists a projective algebraic variety V' and a birational regular map φ from an open dense subset U of V' onto V whose graph is closed in $V' \times V$; the subset U equals V' if and only if V is complete (GAGA, p. 12).

PROPOSITION 7.43. *An algebraic variety V over $\mathbb{C}$ is complete if and only if $V(\mathbb{C})$ is compact in the complex topology.*

PROOF. The proof uses Chow's lemma (GAGA, Proposition 6, p. 12). □

A subset V of $\mathbb{C}^n$ is ***analytic*** if every $P \in V$ admits an open neighbourhood U in $\mathbb{C}^n$ such that $V \cap U$ is the zero set of a finite collection of holomorphic functions on U. Analytic subsets are locally closed.

Let V' be an open subset of an analytic set V. A function $f : V' \to \mathbb{C}$ is ***analytic*** if, for every $P \in V'$, there exists an open neighbourhood U of P in $\mathbb{C}^n$ and a holomorphic function h on U such that $f = h$ on $V' \cap U$. The holomorphic functions on open subsets of V define on V the structure of a $\mathbb{C}$-ringed space.

DEFINITION 7.44. An ***analytic space*** is a $\mathbb{C}$-ringed space $(V, \mathcal{O}_V)$ satisfying the following two conditions:

(a) there exists an open covering $V = \bigcup V_i$ of V such that, for each i, the $\mathbb{C}$-ringed space $(V_i, \mathcal{O}_V|V_i)$ is isomorphic to an analytic set equipped with its sheaf of analytic 1 functions;

(b) the topological space V is Hausdorff.

Let V be an algebraic variety over $\mathbb{C}$. Then $V(\mathbb{C})$ has a natural structure of a complex analytic space, and so there is a canonical functor $V \rightsquigarrow V^{\mathrm{an}}$ from algebraic varieties over $\mathbb{C}$ to complex analytic spaces (GAGA, §2).

[4]Chow, Wei-Liang. On the projective embedding of homogeneous varieties. Algebraic geometry and topology. A symposium in honor of S. Lefschetz, pp. 122–128. Princeton University Press, Princeton, N. J., 1957.

We refer the reader to Chapter 13 for the notion of a coherent module. Every coherent module $\mathcal{F}$ on a algebraic variety V over $\mathbb{C}$ defines a coherent module $\mathcal{F}^{\mathrm{an}} \overset{\text{def}}{=} \mathcal{F} \otimes_{\mathcal{O}_B} \mathcal{O}_{V^{\mathrm{an}}}$ on V^{an}.

THEOREM 7.45. *Let V be a projective variety over $\mathbb{C}$. The functor $\mathcal{F} \rightsquigarrow \mathcal{F}^{\mathrm{an}}$ is an equivalence from the category of coherent $\mathcal{O}_V$-modules to the category of coherent $\mathcal{O}_{V^{\mathrm{an}}}$-modules, under which locally free modules correspond to locally free modules. Moreover,*

$$\Gamma(V^{\mathrm{an}}, \mathcal{O}_{V^{\mathrm{an}}}) \simeq \Gamma(V, \mathcal{O}_V).$$

PROOF. This summarizes the main results of GAGA (Théorémes 2,3, p. 19, p. 20). □

THEOREM 7.46 (CHOW'S THEOREM). *Every closed analytic subset of a projective variety is algebraic.*

PROOF. Let V be a projective space, and let Z be a closed analytic subset of V^{an}. A theorem of Henri Cartan states that $\mathcal{O}_{Z^{\mathrm{an}}}$ is a coherent analytic sheaf on V^{an}, and so there exists a coherent algebraic sheaf $\mathcal{F}$ on V such that $\mathcal{F}^{\mathrm{an}} = \mathcal{O}_{Z^{\mathrm{an}}}$. The support of $\mathcal{F}$ is Zariski closed, and equals Z (GAGA, p. 29). □

In particular, projective analytic spaces are projective algebraic varieties.

THEOREM 7.47. *Every compact analytic subset of an algebraic variety is algebraic.*

PROOF. Let V be an algebraic variety, and let Z be a compact analytic subset of V^{an}. By Chow's lemma (7.42), there exists a projective variety V', a dense open subset U of V', and a surjective regular map $\varphi\colon U \to V$ whose graph Γ is closed in $V \times V'$. Let $\Gamma' = \Gamma \cap (Z \times V')$. As Z and V' are compact and Γ is closed, Γ' is compact, and so its projection V'' on V' is also compact. On the other hand, $V'' = f^{-1}(Z)$, which shows that it is an analytic subset of U, and therefore also of V'. According to Chow's theorem, it is a Zariski closed subset of V' (hence an algebraic variety). Now $Z = f(V'')$ is constructible (Zariski sense; see 9.7 below), and therefore its Zariski closure coincides with its closure for the complex topology, but (by assumption) it is closed. □

COROLLARY 7.48. *Let V and W be algebraic varieties over $\mathbb{C}$. If V is complete, then every analytic map $f\colon V^{\mathrm{an}} \to W^{\mathrm{an}}$ is algebraic.*

PROOF. Apply Theorem 7.47 to the graph of f. □

EXAMPLE 7.49. The graph of $z \mapsto e^z\colon \mathbb{C} \to \mathbb{C}$ is closed in $\mathbb{C} \times \mathbb{C}$ but it is not Zariski closed.

h. Nagata's Embedding Theorem

A necessary condition for a prevariety to be an open subvariety of a complete variety is that it be separated. An important theorem of Nagata says that this condition is also sufficient.

THEOREM 7.50. *Every variety V admits an open immersion $V \hookrightarrow W$ into a complete variety W.*

If V is affine, then one can embed $V \hookrightarrow \mathbb{A}^n \hookrightarrow \mathbb{P}^n$, and take W to be the closure of V in $\mathbb{P}^n$. The proof in the general case is quite difficult. See:

Nagata, Masayoshi. Imbedding of an abstract variety in a complete variety. J. Math. Kyoto Univ. 2 1962 1–10; A generalization of the imbedding problem of an abstract variety in a complete variety. J. Math. Kyoto Univ. 3 1963 89–102.

For a modern exposition, see:

Lütkebohmert, W. On compactification of schemes. Manuscripta Math. 80 (1993), no. 1, 95–111.

In the 1970s, Deligne translated Nagata's work into the language of schemes. His personal notes are available in three versions.

Deligne, P., Le théorème de plongement de Nagata, Kyoto J. Math. 50, Number 4 (2010), 661-670.

Conrad, B., Deligne's notes on Nagata compactifications. J. Ramanujan Math. Soc. 22 (2007), no. 3, 205–257.

Vojta, P., Nagata's embedding theorem, 19pp., 2007, arXiv:0706.1907.

See also:

Temkin, Michael. Relative Riemann-Zariski spaces. Israel J. Math. 185 (2011), 1–42.

A little history

As noted earlier (p. 129), initially Weil was unable to construct the Jacobian variety of a curve as projective variety, which led him to introduce "abstract varieties" and also the notion of a complete abstract variety. Later he (and others) showed that Jacobian varieties are in fact projective.

Exercises

7-1. Identify the set of homogeneous polynomials $F(X,Y)=\sum a_{ij}X^iY^j$, $0\le i,j\le m$, 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

Normal Varieties; (Quasi-)finite maps; Zariski's Main Theorem

We begin by studying normal varieties. Nonsingular varieties are normal, and normal varieties have some of the good properties of nonsingular varieties, but it is easy to show that every variety is birationally equivalent to a normal variety. After studying finite and quasi-finite maps, we discuss the celebrated Zariski's Main Theorem (ZMT), which says that every quasi-finite map of algebraic varieties can be obtained from a finite map by removing a closed subset from the source variety. In its original form, the theorem says that a birational regular map to a normal algebraic variety fails to be a local isomorphism only at points where the fibre has dimension > 0.

a. Normal varieties

Recall (1.42) that an integrally closed domain is an integral domain that is integrally closed in its field of fractions. Moreover (1.49), that an integral domain A is integrally closed if and only if $A_{\mathfrak{m}}$ is integrally closed for every maximal ideal $\mathfrak{m}$ in A.

DEFINITION 8.1. A point P on an algebraic variety V is ***normal*** if $\mathcal{O}_{V,P}$ is an integrally closed domain. An algebraic variety is said to be ***normal*** if all of its points are normal.

Since the local ring at a point lying on two irreducible components cannot be an integral domain (3.14), a normal variety is a disjoint union of its irreducible components, which are therefore its connected components.

PROPOSITION 8.2. *The following conditions on an irreducible variety V are equivalent.*

(a) *The variety V is normal.*

(b) *For all open affine subsets U of V, the ring $\mathcal{O}_V(U)$ is an integrally closed domain.*

(c) *For all open subsets U of V, a rational function on V that satisfies a monic polynomial equation on U whose coefficients are regular on U is itself regular on U.*

PROOF. The equivalence of (a) and (b) follows from 1.49.

(a) ⇒ (c). Let U be an open subset of V, and let $f \in k(V)$ satisfy

$$f^n + a_1 f^{n-1} + \cdots + a_n = 0, \quad a_i \in \mathcal{O}_V(U),$$

(equality in $k(V)$). Then $a_i \in \mathcal{O}_V(U) \subset \mathcal{O}_P$ for all $P \in U$, and so $f \in \mathcal{O}_P$ for all $P \in U$. This implies that $f \in \mathcal{O}_V(U)$ (5.10).

(c) ⇒ (b). The condition applied to an open affine subset U of V implies that $\mathcal{O}_V(U)$ is integrally closed in $k(V)$. □

Regular local rings are unique factorization domains (Matsumura 1989, Theorem 20.3), hence normal (1.43). Conversely, a normal local 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 it is singular at the origin — the tangent space at the origin is k^3.

The singular locus of a normal variety V must have dimension $\leq \dim V - 2$ (see 8.12 below). For example, a normal surface can only have isolated singularities — the singular locus cannot contain a curve. In particular, the surface $Z^3 = X^2Y$ (see 4.42) is not normal.

The normalization of an algebraic variety

Let $E \supset F$ be a finite extension of fields. The extension E/F is said to be normal if the minimal polynomial of every element of E splits in E. Let F^{al} be an algebraic closure of F containing E. The composite in F^{al} of the fields σE, $\sigma \in \mathrm{Aut}(E/F)$, is normal over F (and is called the normal closure of F in F^{al}). If E is normal over F, then E is Galois over $E^{\mathrm{Aut}(E/F)}$ (FT, 3.10), and $E^{\mathrm{Aut}(E/F)}$ is purely inseparable over F (because $\mathrm{Hom}_F(E^{\mathrm{Aut}(E/F)}, F^{\mathrm{al}})$ consists of a single element).

PROPOSITION 8.3. *Let A be a finitely generated k-algebra. Assume that A is an integral domain, and let E be a finite field extension of its field of fractions F. Then the integral closure A' of A in E is a finite A-algebra (hence a finitely generated k-algebra).*

PROOF. According to the Noether normalization theorem (2.45), A contains a polynomial subalgebra A_0 and is finite over A_0. Now E is a finite extension of $F(A_0)$ and A' is the integral closure of A_0 in E, and so we only need to consider the case that A is a polynomial ring $k[X_1, \ldots, X_d]$.

Let $\tilde{E}$ denote the normal closure of E in some algebraic closure of F containing E, and let $\tilde{A}$ denote the integral closure of A in $\tilde{E}$. If $\tilde{A}$ is finitely generated as an A-module, then so is its submodule A' (because A is noetherian). Therefore we only need to consider the case that E is normal over F.

According to the above discussion, $E \supset E_1 \supset F$ with E Galois over E_1 and E_1 purely inseparable over F. Let A_1 denote the integral closure of A in E_1. Then A' is a finite A_1-algebra (1.51), and so it suffices to show that A_1 is a finite A-algebra. Therefore we only need to consider the case that E is purely inseparable over F.

In this case, k has characteristic $p \neq 0$, and, for each $x \in E$, there is a power $q(x)$ of p such that $x^{q(x)} \in F$. As E is finitely generated over F, there is a single power q of p such that $x^q \in F$ for all $x \in E$. Let F^{al} denote an algebraic closure of F containing E. For each i, there is a unique $Y_i \in F^{\mathrm{al}}$ such that $Y_i^q = X_i$. Now

$$F = k(X_1, \ldots, X_d) \subset E \subset k(Y_1, \ldots, Y_d)$$

and

$$A = k[X_1, \ldots, X_d] \subset A' \subset k[Y_1, \ldots, Y_d]$$

because $k[Y_1, \ldots, Y_d]$ contains A and is integrally closed (1.32, 1.43). Obviously $k[Y_1, \ldots, Y_d]$ is a finite A-algebra, and this implies, as before, that A' is a finite A-algebra. □

COROLLARY 8.4. *Let A be as in 8.3. If $A_{\mathfrak{m}}$ is normal for some maximal ideal $\mathfrak{m}$ in A, then A_h is normal for some $h \in A \smallsetminus \mathfrak{m}$.*

PROOF. Let A' be the integral closure of A in its field of fractions. Then $A' = A[f_1, \ldots, f_m]$ for some $f_i \in A'$. Now $(A')_{\mathfrak{m}} \overset{1.47}{=} (A_{\mathfrak{m}})' = A_{\mathfrak{m}}$, and so there exists an $h \in A \smallsetminus \mathfrak{m}$ such that, for all i, $hf_i \in A$. Now $A'_h = A_h$, and so A_h is normal. □

The proposition shows that if A is an integral domain finitely generated over k, then the integral closure A' of A in a finite extension E of $F(A)$ has the same properties. Therefore, $\mathrm{Spm}(A')$ is an irreducible algebraic variety, called the ***normalization*** of $\mathrm{Spm}(A)$ in E. This construction extends without difficulty to nonaffine varieties.

PROPOSITION 8.5. *Let V be an irreducible algebraic variety, and let K be a finite field extension of $k(V)$. Then there exists an irreducible algebraic variety W with $k(W) = K$ and a regular map $\varphi\colon W \to V$ such that, for all open affines U in V, $\varphi^{-1}(U)$ is affine and $k[\varphi^{-1}(U)]$ is the integral closure of $k[U]$ in K.*

The map φ (or just W) is called the ***normalization*** of V in K.

PROOF. For each $v \in V$, let $W(v)$ be the set of maximal ideals in the integral closure of $\mathcal{O}_v$ in K. Let $W = \bigsqcup_{v \in V} W(v)$, and let $\varphi\colon W \to V$ be the map sending the points of $W(v)$ to v. For an open affine subset U of V,

$$\varphi^{-1}(U) \simeq \mathrm{spm}(k[U]'),$$

where $k[U]'$ is the integral closure of $k[U]$ in K. We endow W with the k-ringed space structure for which

$$(\varphi^{-1}(U), \mathcal{O}_W|\varphi^{-1}(U)) \simeq \mathrm{Spm}(k[U]').$$

A routine argument shows that $(W, \mathcal{O}_W)$ is an algebraic variety with the required properties. □

EXAMPLE 8.6. (a) The normalization of the cuspidal cubic $V\colon Y^2 = X^3$ in $k(V)$ is the map $\mathbb{A}^1 \to V$, $t \mapsto (t^2, t^3)$ (see 3.29).

(b) The normalization of the nodal cubic $V\colon Y^2 = X^3 + X^2$ (4.10) in $k(V)$ is the map $\mathbb{A}^1 \to V$, $t \mapsto (t^2 - 1, t^3 - t)$.

PROPOSITION 8.7. *The normal points in an irreducible algebraic variety form a dense open subset.*

PROOF. Corollary 8.4 shows that the set of normal points is open, and so it remains to show that it is nonempty. This follows from 4.37 and the fact (difficult to prove) that nonsingular points are normal, but we shall give a direct proof.

Let V be an irreducible algebraic variety. According to (3.37, 3.38), V is birationally equivalent to a hypersurface H in $\mathbb{A}^{d+1}$, $d = \dim V$,

$$H\colon \quad a_0X^m + a_1X^{m-1} + \cdots + a_m, \quad a_i \in k[T_1, \ldots, T_d], \quad a_0 \neq 0, \quad m \in \mathbb{N};$$

moreover, $T_1, \ldots, T_d$ can be chosen to be a separating transcendence basis for $k(V)$ ($= k(H)$) over k. Therefore the discriminant D of $k(H)$ over $k(T_1, \ldots, T_d)$ (an element of $k[H]$) is nonzero.[1] We shall see that open subset of H where D is nonzero is normal.

[1] Let $B \supset A$ be rings. Assume that B is free of rank m as an A-module, and let $\beta_1, \ldots, \beta_m$ be a basis for B as an A-module. We call $D(\beta_1, \ldots, \beta_m) \overset{\text{def}}{=} \det(\mathrm{Tr}_{B/A}(\beta_i\beta_j))$ the ***discriminant*** of B/A (it is well-defined up to a unit in A). The discriminant of a finite separable extension of fields is nonzero (Proposition 2.26 of my notes on *Algebraic Number Theory*).

Let $A = k[T_1, \dots, T_d]$; then $k[H] = A[X]/(a_0X^m + \cdots + a_m) = A[x]$. Let

$$y = c_0 + \cdots + c_{m-1}x^{m-1}, \quad c_i \in k(T_1, \dots, T_d), \tag{35}$$

be an element of $k(H)$ integral over A. For each $j \in \mathbb{N}$, $\mathrm{Tr}_{k(H)/F(A)}(yx^j)$ is a sum of conjugates of yx^j, and hence is integral over A (cf. the proof of 1.44). As it lies in $F(A)$, it is an element of A. On multiplying (35) with x^j and taking traces, we get a system of linear equations

$$c_0 \cdot \mathrm{Tr}(x^j) + c_1 \cdot \mathrm{Tr}(x^{1+j}) + \cdots + c_{m-1} \cdot \mathrm{Tr}(x^{m-1+j}) = \mathrm{Tr}(yx^j), \quad j = 0, \dots, m-1.$$

By Cramer's rule (p. 25),

$$\det(\mathrm{Tr}(x^{i+j})) \cdot c_l \in A, \quad l = 0, \dots, m-1.$$

But $\det(\mathrm{Tr}(x^{i+j})) = D$, and so $c_l \in A[D^{-1}]$. Hence $k[H]$ becomes normal once we invert the nonzero element D. We have shown that H contains a dense open normal subvariety, which implies that V does also. □

PROPOSITION 8.8. *For every irreducible algebraic variety V, there exists a surjective regular map $\varphi: V' \to V$ from a normal algebraic variety V' to V such that, for some dense open subset U of V, φ induces an isomorphism $\varphi^{-1}(U) \to U$ (in particular φ is birational).*

PROOF. Proposition 8.7 shows that the normalization of V in $k(V)$ has this property. □

8.9. More generally, for a dominant map $\varphi: W \to V$ of irreducible algebraic varieties, there exists a ***normalization*** of V in W. For each open affine U in V we have

$$k[U] \subset \Gamma(\varphi^{-1}(U), \mathcal{O}_W) \subset k(W).$$

The integral closure $k[U]'$ of $\Gamma(U, \mathcal{O}_V)$ in $\Gamma(\varphi^{-1}(U), \mathcal{O}_W)$ is a finite $k[U]$-algebra (because it is a $k[U]$-submodule of the integral closure of $k[U]$ in $k(W)$). The normalization of V in W is a regular map $\varphi': V' \to V$ such that, for every open affine U in V,

$$(\varphi'^{-1}(U), \mathcal{O}_{V'}) = \mathrm{Spm}(k[U]').$$

In particular, φ' is an affine map. For example, if W and V are affine, then $V' = \mathrm{Spm}(k[V]')$, where $k[V]'$ is the integral closure of $k[V]$ in $k[W]$. There is a commutative triangle

$$\begin{array}{ccc} W & \xrightarrow{\;j\;} & V' \\ & {\scriptstyle\varphi}\searrow \quad \swarrow{\scriptstyle\varphi'} & \\ & V. & \end{array}$$

b. Regular functions on normal varieties

DEFINITION 8.10. An algebraic variety V is ***factorial at a point*** P if $\mathcal{O}_P$ is a factorial domain. The variety V is ***factorial*** if it is factorial at all points P.

When V is factorial, it *does not follow* that $\mathcal{O}_V(U)$ is factorial for all open affines U in V.

A ***prime divisor*** Z on a variety V is a closed irreducible subvariety of codimension 1. Let Z be a prime divisor on V, and let $P \in V$; we say that Z is ***locally principal*** at P if there exists an open affine neighbourhood U of P and an $f \in k[U]$ such that $I(Z \cap U) = (f)$; the regular function f is then called a ***local equation*** for Z at P. If $P \notin Z$, then Z is locally principal at P because then we can choose U so that $Z \cap U = \emptyset$, and $I(Z \cap U) = (1)$.

PROPOSITION 8.11. *An irreducible variety V is factorial at a point P if and only if every prime divisor on V is locally principal at P.*

PROOF. Recall that an integral domain is factorial (finitely generated over a field) if and only if every prime ideal of height 1 is principal (1.24, 3.53). □

PROPOSITION 8.12. *The codimension of the singular locus in a normal variety is at least* 2.

PROOF. Let V be a normal algebraic variety of dimension d, and suppose that its singular locus has an irreducible component W of codimension 1. After replacing V with an open subvariety, we may suppose that it is affine and that W is principal, say, $W = (f)$ (see 8.11). There exists a nonsingular point P on W (4.37). Let $(U, f_1), \ldots, (U, f_{d-1})$ be germs of functions at P (on V) whose restrictions to W generate the maximal ideal in $\mathcal{O}_{W,P}$ (cf. 4.36). Then $(U, f_1), \ldots, (U, f_{d-1}), (U, f)$ generate the maximal ideal in $\mathcal{O}_{V,P}$, and so P is nonsingular on V. This contradicts the definition of W. □

SUMMARY 8.13. For an algebraic variety V,

$$\text{nonsingular} \Rightarrow \text{factorial} \Rightarrow \text{normal} \Rightarrow \text{singular locus has codimension } \geq 2.$$

- The variety $X_1^2 + \cdots + X_5^2$ is factorial but singular.
- The cone $Z^2 = XY$ in $\mathbb{A}^3$ is normal but not factorial (see 9.39 below).
- The variety $\mathrm{Spm}(k[X, XY, Y^2, Y^3])$ is a surface in $\mathbb{A}^4$ with exactly one singular point, namely, the origin. Its singular locus has codimension 2, but the variety is not normal (the normalization $k[X, XY, Y^2, Y^3]$ is $k[X, Y]$).
- Every singular curve has singular locus of codimension 1 (hence fails all conditions).

ZEROS AND POLES OF RATIONAL FUNCTIONS ON NORMAL VARIETIES

Let V be a normal irreducible variety. 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. 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 an integrally closed domain with exactly one nonzero prime ideal $\mathfrak{p}R_{\mathfrak{p}}$ — it is therefore a discrete valuation ring (4.20), 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 intersecting Z.

Let ord_Z be the valuation $k(V)^\times \xrightarrow{\text{onto}} \mathbb{Z}$ with valuation ring $\mathcal{O}_Z$; thus, if π is a prime element of $\mathcal{O}_Z$, then

$$a = \text{unit} \times \pi^{\mathrm{ord}_Z(a)}.$$

The divisor of a nonzero element f of $k(V)$ is defined to be

$$\operatorname{div}(f) = \sum \operatorname{ord}_Z(f) \cdot Z.$$

The sum is over all the prime divisors of V, but in fact $\operatorname{ord}_Z(f) = 0$ for all but finitely many Z. In proving this, we can assume that V is affine (because it is a finite union of affines), say, $V = \operatorname{Spm}(R)$. Then $k(V)$ is the field of fractions of R, and so we can write $f = g/h$ with $g, h \in R$, and $\operatorname{div}(f) = \operatorname{div}(g) - \operatorname{div}(h)$. 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 3.42) and $\operatorname{ord}_Z(f) = 0$ unless Z is one of the Z_i.

The map

$$f \mapsto \operatorname{div}(f)\colon\ k(V)^{\times} \to \operatorname{Div}(V)$$

is a homomorphism. A divisor of the form $\operatorname{div}(f)$ 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*** $\operatorname{Pic}(V)$ of V is defined to be the group of divisors on V modulo principal divisors. (The definition of the Picard group of a general algebraic variety agrees with this definition only for nonsingular varieties; it may differ for normal varieties.)

THEOREM 8.14. *Let V be a normal variety, and let f be rational function on V. If f has no zeros or poles on an open subset U of V, then f is regular on U.*

PROOF. We may assume that V is connected, hence irreducible, and apply the following statement (see Chapter 12): if a noetherian integral domain A is normal, then $A = \bigcap_{\operatorname{ht}(\mathfrak{p})=1} A_{\mathfrak{p}}$ (intersection in the field of fractions of A). □

COROLLARY 8.15. *A rational function on a normal variety, regular outside a subset of codimension ≥ 2, is regular everywhere.*

PROOF. This is a restatement of the theorem. □

COROLLARY 8.16. *Let V and W be affine varieties with V normal, and let $\varphi\colon V \smallsetminus Z \to W$ be a regular map defined on the complement of a closed subset Z of V. If $\operatorname{codim}(Z) \geq 2$, then φ extends to a regular map on the whole of V.*

PROOF. We may suppose that W is affine, and embed it as a closed subvariety of $\mathbb{A}^n$. The map $V \smallsetminus Z \to W \hookrightarrow \mathbb{A}^n$ is given by n regular functions on $V \smallsetminus Z$, each of which extends to V. Therefore $V \smallsetminus Z \to \mathbb{A}^n$ extends to $\mathbb{A}^n$, and its image is contained in W. □

c. Finite and quasi-finite maps

Finite maps

DEFINITION 8.17. A regular map $\varphi\colon W \to V$ of algebraic varieties is ***finite*** if there exists a finite covering $V = \bigcup_i U_i$ of V by open affines such that, for each i, the set $\varphi^{-1}(U_i)$ is affine and $k[\varphi^{-1}(U_i)]$ is a finite $k[U_i]$-algebra.

EXAMPLE 8.18. Let V be an irreducible algebraic variety. The normalization $\varphi\colon W \to V$ of V in a finite extension of $k(V)$ is finite. This follows from the definition 8.5 and Proposition 8.3.

The next lemma shows that, for maps of affine algebraic varieties, the above definition agrees with Definition 2.39.

LEMMA 8.19. *A regular map $\varphi: W \to V$ of affine algebraic varieties is finite if and only if $k[W]$ is a finite $k[V]$-algebra.*

PROOF. The necessity being obvious, we prove the sufficiency. For simplicity, we shall assume in the proof that V and W are irreducible. Let $(U_i)_i$ be a finite family of open affines covering V and such that, for each i, the set $\varphi^{-1}(U_i)$ is affine and $k[\varphi^{-1}(U_i)]$ is a finite $k[U_i]$-algebra.

Each U_i is a finite union of basic open subsets of V. These are also basic open subsets of U_i, because $D(f) \cap U_i = D(f|U_i)$, and so we may assume that the original U_i are basic open subsets of V, say, $U_i = D(f_i)$ with $f_i \in A$.

Let $A = k[V]$ and $B = k[W]$. We are given that $(f_1, \ldots, f_n) = A$ and that B_{f_i} is a finite A_{f_i}-algebra for each i. We have to show that B is a finite A-algebra.

Let $\{b_{i1}, \ldots, b_{im_i}\}$ generate B_{f_i} as an A_{f_i}-module. After multiplying through by a power of f_i, we may assume that the b_{ij} lie in B. We shall show that the family of all b_{ij} generate B as an A-module. Let $b \in B$. Then $b/1 \in B_{f_i}$, so

$$b = \frac{a_{i1}}{f_i^{r_i}} b_{i1} + \cdots + \frac{a_{im_i}}{f_i^{r_i}} b_{im_i}, \text{ some } a_{ij} \in A \text{ and } r_i \in \mathbb{N}.$$

The ideal $(f_1^{r_1}, \ldots, f_n^{r_n}) = A$ because any maximal ideal containing $(f_1^{r_1}, \ldots, f_n^{r_n})$ would have to contain $(f_1, \ldots, f_n) = A$. Therefore,

$$1 = h_1 f_1^{r_1} + \cdots + h_n f_n^{r_n}, \text{ some } h_i \in A.$$

Now

$$\begin{aligned} b = b \cdot 1 &= h_1 \cdot b f_1^{r_1} + \cdots + h_n \cdot b f_n^{r_n} \\ &= h_1(a_{11} b_{11} + \cdots + a_{1m_1} b_{1m_1}) + \cdots + h_n(a_{n1} b_{n1} + \cdots + a_{nm_n} b_{nm_n}), \end{aligned}$$

as required. □

LEMMA 8.20. *Let $\varphi: W \to V$ be a regular map with V affine, and let U be an open affine in V. Then*

$$\Gamma(W, \mathcal{O}_W) \otimes_{k[V]} k[U] \simeq \Gamma(\varphi^{-1}(U), \mathcal{O}_W).$$

PROOF. Let $U' = \varphi^{-1}(U)$, so we have to prove

$$\Gamma(W, \mathcal{O}_W) \otimes_{k[V]} k[U] \simeq \Gamma(U', \mathcal{O}_W)$$

The map is defined by the $k[V]$-bilinear pairing

$$(f, g) \mapsto f|_{U'} \cdot g \circ \varphi|_{U'} : \Gamma(W, \mathcal{O}_W) \times k[U] \to \Gamma(U', \mathcal{O}_W).$$

When W is affine, the statement is proved in 5.32.

Let $S = \{f \in k[V] \mid \forall P \in U,\ f(P) \neq 0\}$. Then $k[U] = S^{-1} k[V]$, and so, for any $k[V]$-module M, $M \otimes_{k[V]} k[U] \simeq S^{-1} M$. Hence the functor $- \otimes_{k[V]} k[U]$ is exact.

Let $W = \bigcup W_i$ be a finite open affine covering of W, and consider the commutative diagram:

$$\begin{array}{ccccc}
0 \longrightarrow \Gamma(W, \mathcal{O}_W) \otimes_{k[V]} k[U] & \rightarrow & \prod_i \Gamma(W_i, \mathcal{O}_W) \otimes_{k[V]} k[U] & \rightrightarrows & \prod_{i,j} \Gamma(W_{ij}, \mathcal{O}_W) \otimes_{k[V]} k[U] \\
\downarrow & & \downarrow & & \downarrow \\
0 \longrightarrow \Gamma(U', \mathcal{O}_W) & \longrightarrow & \prod_i \Gamma(U' \cap W_i, \mathcal{O}_W) & \rightrightarrows & \prod_{i,j} \Gamma(U' \cap W_{ij}, \mathcal{O}_W).
\end{array}$$

Here $W_{ij} = W_i \cap W_j$. The rows are exact because $\mathcal{O}_W$ is a sheaf. 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. This implies that the first is also an isomorphism. □

PROPOSITION 8.21. *Let $\varphi\colon W \to V$ be a regular map of algebraic varieties. If φ is finite, then, for every open affine U in V, $\varphi^{-1}(U)$ is affine and $k[\varphi^{-1}(U)]$ is a finite $k[U]$-algebra.*

PROOF. Let V_i be an open affine covering of V (which we may suppose to be finite) such that $W_i \overset{\text{def}}{=} \varphi^{-1}(V_i)$ is an affine subvariety of W for all i and $k[W_i]$ is a finite over $k[V_i]$. 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

$$\begin{array}{ccc}
U' & \xrightarrow{\text{canonical}} & \operatorname{Spm}(\Gamma(U', \mathcal{O}_W)) \\
& \searrow \quad \swarrow & \\
& V &
\end{array} \tag{36}$$

which we shall show to be an isomorphism. We know that each of the maps

$$U' \cap W_i \to \operatorname{Spm}(\Gamma(U' \cap W_i, \mathcal{O}_W))$$

is an isomorphism. But $\operatorname{Spm}(\Gamma(U' \cap W_i, \mathcal{O}_W))$ is the inverse image of V_i in $\operatorname{Spm}(\Gamma(U', \mathcal{O}_W))$. Therefore the canonical morphism is an isomorphism over each V_i, and so it is an isomorphism. □

SUMMARY 8.22. Let $\varphi\colon W \to V$ be a regular map, and consider the following condition on an open affine subset U of V:

(*) $\varphi^{-1}(U)$ is affine and $k[\varphi^{-1}(U)]$ is a finite over $k[U]$.

The map φ is finite if (*) holds for the open affines in some covering of V, in which case (*) holds for all open affines of V.

PROPOSITION 8.23. (a) *Closed immersions are finite.*

(b) *The composite of two finite morphisms is finite.*

(c) *The product of two finite morphisms is finite.*

---

[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 over a noetherian ring is finitely generated.

PROOF. (a) Let Z be a closed subvariety of a variety V, and 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.

This proves (a). As to be finite is a local condition, it suffices to prove (a) and (b) for maps of affine varieties. Then the statements become statements in commutative algebra.

(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, then $\{b_i \otimes b'_j\}$ is a set of generators for $B \otimes_A B'$ as an $A \otimes A'$-module. □

By way of contrast, open immersions are rarely finite. For example, the inclusion $\mathbb{A}^1 \smallsetminus \{0\} \hookrightarrow \mathbb{A}^1$ is not finite because the ring $k[T, T^{-1}]$ is not finitely generated as a $k[T]$-module.

THEOREM 8.24. *Finite maps of algebraic varieties are closed.*

PROOF. It suffices to prove this for affine varieties. Let $\varphi\colon W \to V$ be a finite map of affine varieties, and let Z be a closed subset of W. The restriction of φ to Z is finite (by 8.23a 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 going-up theorem (1.53). □

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 8.25. *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. □

PROPOSITION 8.26. *Finite maps of algebraic varieties are proper.*

PROOF. The base change of a finite map is finite, and hence closed. □

COROLLARY 8.27. *Let $\varphi\colon V \to S$ be finite; if S is complete, then so also is V.*

PROOF. Combine 7.19 and 8.26. □

Quasi-finite maps

Recall that the fibres of a regular map $\varphi\colon W \to V$ are the closed subvarieties $\varphi^{-1}(P)$ of W for $P \in V$. As for affine varieties (2.39), we say that a regular map of algebraic varieties is ***quasi-finite*** if all of its fibres are finite.

PROPOSITION 8.28. *A finite map $\varphi\colon W \to V$ is quasi-finite.*

PROOF. Let $P \in V$; we wish to show that $\varphi^{-1}(P)$ is finite. After replacing V with an affine neighbourhood of P, we may suppose that it is affine, and then W will be affine also. The map φ then corresponds to a map $\alpha\colon A \to B$ 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 $B/\alpha(\mathfrak{m}_P)B$. Clearly $B/\alpha(\mathfrak{m}_P)B$ is generated as a k-vector space by the image of any generating set for B as an A-module, and so it is a finite k-algebra. The next lemma shows that it has only finitely many maximal ideals. □

LEMMA 8.29. *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 coprime in pairs, and so 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

$$\dim_k A \geq \sum \dim_k(A/\mathfrak{m}_i) \geq n$$

— here $\dim_k$ means dimension as a k-vector space. □

Finite and ***quasi-finite*** maps of prevarieties are defined as for varieties.

Examples

8.30. The projection from the curve $XY = 1$ onto the X axis (see p. 71) is quasi-finite but not finite — its image is not closed in $\mathbb{A}^1$, and $k[X, X^{-1}]$ is not finite over $k[X]$.

8.31. 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 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 $k[T]$ as a $k[T^2, T^3]$-module (see 3.29).

8.32. The map $\mathbb{A}^1 \to \mathbb{A}^1$, $a \mapsto a^m$ is finite.

8.33. 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).

8.34. The map $\mathbb{A}^2 \smallsetminus \{\text{origin}\} \hookrightarrow \mathbb{A}^2$ is quasi-finite but not finite, because the inverse image of $\mathbb{A}^2$ is not affine (see 3.33). The map

$$\mathbb{A}^2 \smallsetminus \{(0,0)\} \sqcup * \to \mathbb{A}^2$$

sending $*$ to $(0,0)$ is bijective but not finite (here $* = \operatorname{Spm}(k) = \mathbb{A}^0$).

8.35. The map in 8.31 and the Frobenius map

$$(t_1, \dots, t_n) \mapsto (t_1^p, \dots, t_n^p) \colon \mathbb{A}^n \to \mathbb{A}^n$$

in characteristic $p \neq 0$, are examples of finite bijective regular maps that are not isomorphisms.

8.36. Let f be the regular map

$$(x, y) \mapsto (x, xy^2 + y + 1) \colon \mathbb{A}^2 \to \mathbb{A}^2.$$

Then f is (obviously) quasi-finite, but it is not finite. For this we have to show that $k[X, Y]$ is not integral over its subring $k[A, B]$, where

$$\begin{aligned} A &= X \\ B &= XY^2 + Y + 1. \end{aligned}$$

The minimal polynomial of Y over $k[A, B]$ is

$$AY^2 + Y + 1 - B = 0,$$

which shows that it is not integral over $k[A, B]$ (see 1.44). Alternatively, one can show directly that Y can never satisfy an equation

$$Y^s + g_1(A, B)Y^{s-1} + \cdots + g_s(A, B) = 0, \qquad g_i(A, B) \in k[A, B],$$

by multiplying the equation by A.

8.37. Let V be the hyperplane

$$X^n + T_1X^{n-1} + \cdots + T_n = 0$$

in $\mathbb{A}^{n+1}$, and consider the projection map

$$(a_1, \dots, a_n, x) \mapsto (a_1, \dots, a_n) \colon V \to \mathbb{A}^n.$$

The fibre over a point $(a_1, \dots, a_n) \in \mathbb{A}^n$ 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,

$$k[T_1, \dots, T_n] \to k[T_1, \dots, T_n, X]/(X^n + T_1X^{n-1} + \cdots + T_n).$$

See also the more general example p. 51.

8.38. Let V be the hyperplane

$$T_0X^n + T_1X^{n-1} + \cdots + T_n = 0$$

in $\mathbb{A}^{n+2}$. The projection map

$$(a_0, \dots, a_n, x) \mapsto (a_0, \dots, a_n) \colon V \xrightarrow{\varphi} \mathbb{A}^{n+1}$$

has finite fibres except for the fibre above $o = (0, \dots, 0)$, which is $\mathbb{A}^1$. Its restriction to $V \smallsetminus \varphi^{-1}(o)$ is quasi-finite, but not finite. Above points of the form $(0, \dots, 0, *, \dots, *)$ some of the roots "vanish off to ∞". (Example 8.30 is a special case of this.) See also the more general example p. 51.

8.39. Let

$$P(X, Y) = T_0X^n + T_1X^{n-1}Y + \cdots + T_nY^n,$$

and let V be its zero set in $\mathbb{P}^1 \times (\mathbb{A}^{n+1} \smallsetminus \{0\})$. In this case, the projection map $V \to \mathbb{A}^{n+1} \smallsetminus \{0\}$ is finite.

d. The fibres of finite maps

Let $\varphi \colon W \to V$ 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. The map φ is said to be ***separable*** if the field $k(W)$ is separable over $k(V)$. Recall that $|S|$ denotes the number of elements in a finite set S.

THEOREM 8.40. *Let $\varphi \colon W \to V$ be a finite surjective regular map of irreducible varieties with V normal.*

(a) *For all $P \in V$, $\left|\varphi^{-1}(P)\right| \leq \deg(\varphi)$.*

(b) *The set of points P of V such that $\left|\varphi^{-1}(P)\right| = \deg(\varphi)$ is an open subset of V, and it is nonempty if φ is separable.*

Before proving the theorem, we give examples to show that we need W to be separated and V to be normal in (a), and that we need $k(W)$ to be separable over $k(V)$ for the second part of (b).

EXAMPLE 8.41. (a) The map

$$\{\mathbb{A}^1 \text{ with origin doubled }\} \to \mathbb{A}^1$$

has degree one and is one-to-one except over the origin where it is two-to-one.

(b) Let C be the curve $Y^2 = X^3 + X^2$, and consider the map

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

It is one-to-one except that the points $t = \pm 1$ both map to 0. On coordinate rings, it corresponds to the inclusion

$$k[x, y] \hookrightarrow k[T], \quad \begin{cases} x \mapsto T^2 - 1 \\ y \mapsto T(T^2 - 1), \end{cases}$$

and so is of degree one. The ring $k[x, y]$ is not integrally closed — in fact $k[T]$ is the integral closure of $k[x, y]$ in its field of fractions $k(x, y) = k(T)$.

(c) The Frobenius map

$$(a_1, \dots, a_n) \mapsto (a_1^p, \dots, a_n^p) : \mathbb{A}^n \to \mathbb{A}^n$$

in characteristic $p \neq 0$ is bijective on points, but has degree p^n. The field extension corresponding to the map is

$$k(X_1, \dots, X_n) \supset k(X_1^p, \dots, X_n^p)$$

which is purely inseparable.

LEMMA 8.42. *Let $Q_1, \dots, Q_r$ be distinct points on an affine variety V. Then there is a regular function f on V taking distinct values at the Q_i.*

PROOF. We can embed V as closed subvariety of $\mathbb{A}^n$, and then it suffices to prove the statement with $V = \mathbb{A}^n$ — almost any linear form will do. □

PROOF (OF 8.40). In proving (a) of the theorem, we may assume that V and W are affine, and so the map corresponds to a finite map of k-algebras, $k[V] \to k[W]$. Let $\varphi^{-1}(P) = \{Q_1, \dots, Q_r\}$. According to the lemma, there exists an $f \in k[W]$ taking distinct values at the Q_i. Let

$$F(T) = T^m + a_1 T^{m-1} + \cdots + a_m$$

be the minimal 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 1.44). 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

$$k[V] \longrightarrow k[V][T]/(F) \xrightarrow{T \mapsto f} k[W]$$

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 an

$f \in k[W]$ such that $k(V)[f] = k(W)$. Its minimal polynomial F has degree $\deg(\varphi)$ and its discriminant is a nonzero element of $k[V]$. The diagram

$$W \to \mathrm{Spm}(k[V][T]/(F)) \to V$$

shows that $|\varphi^{-1}(P)| \geq \deg(\varphi)$ for P a point such that $\mathrm{disc}(f)(P) \neq 0$. □

Let $E \supset F$ be a finite extension of fields. The elements of E separable over F form a subfield F' of E, and the separable degree of E over F is defined to be the degree of F' over F. The ***separable degree*** of a finite surjective map $\varphi\colon W \to V$ of irreducible varieties is the separable degree of $k(W)$ over $k(V)$.

THEOREM 8.43. *Let $\varphi\colon W \to V$ be a finite surjective regular map of irreducible varieties, and assume that V is normal.*

(a) *For all $P \in V$, $\left|\varphi^{-1}(P)\right| \leq \mathrm{sep}\ \deg(\varphi)$, with equality holding on a dense open subset.*

(b) *For all i,*

$$V_i = \{P \in V \mid \left|\varphi^{-1}(P)\right| \leq i\}$$

is closed in V.

PROOF. If φ is separable, this was proved in 8.40. If φ is purely inseparable, then φ is one-to-one because, for some q, the Frobenius map $V^{(q^{-1})} \xrightarrow{F} V$ factors through φ. In the general case, φ factors through the normalization of V in F', which realizes φ as the composite of a purely inseparable map with a separable map. □

ASIDE 8.44. A finite map from a variety onto a normal variety is open (hence both open and closed). See 8.52.

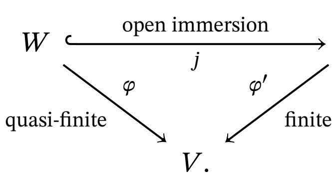
e. Zariski's main theorem

In this section, we explain a fundamental theorem of Zariski.

Statement and proof

An obvious way of constructing nonfinite quasi-finite map is to take a finite map $W \to V$ and remove a closed subset of W. Zariski's Main Theorem (ZMT) shows that, for algebraic varieties, every quasi-finite map arises in this way.

THEOREM 8.45 (ZARISKI'S MAIN THEOREM). *Every quasi-finite map of algebraic varieties $\varphi\colon W \to V$ factors into $W \overset{j}{\hookrightarrow} V' \overset{\varphi'}{\to} V$ with φ' finite and j an open immersion:*



When φ is a dominant map of irreducible varieties, the statement is true with $\varphi'\colon V' \to V$ equal to the normalization of V in W (in the sense of 8.9).

The key result needed to prove 8.45 is the following statement from commutative algebra. For a ring A and a prime ideal $\mathfrak{p}$ in A, $\kappa(\mathfrak{p})$ denotes the field of fractions of $A/\mathfrak{p}$.

THEOREM 8.46 (LOCAL VERSION OF ZMT). *Let A be a commutative ring, and let $i\colon A \to B$ be a finitely generated A-algebra. Let $\mathfrak{q}$ be a prime ideal of B, and let $\mathfrak{p} = i^{-1}(\mathfrak{q})$. Finally, let A' denote the integral closure of A in B. If $B_{\mathfrak{q}}/\mathfrak{p}B_{\mathfrak{q}}$ is a finite $\kappa(\mathfrak{p})$-algebra, then there exists an $f \in A'$ not in $\mathfrak{q}$ such that the map $A'_f \to B_f$ is an isomorphism.*

PROOF. The proof is quite elementary, but intricate — see §17 of my notes CA. □

Recall that a point v in a topological space V is isolated if $\{v\}$ is an open subset of V. The isolated points v of an algebraic variety V are those such that $\{v\}$ is both open and closed. Thus they are the irreducible components of V of dimension 0. Thus, if $\{v\}$ is isolated in V, then $V = \{v\} \sqcup V'$, and, if V is affine, then $k[V] \simeq k \times k[V']$.

Let $\varphi\colon W \to V$ be a continuous map of topological spaces. We say that $w \in W$ is ***isolated in its fibre*** if it is isolated in the subspace $\varphi^{-1}(\varphi(w))$ of W. Let $\varphi\colon A \to B$ be a homomorphism of finitely generated k-algebras, and consider $\mathrm{spm}(\varphi)\colon \mathrm{spm}(B) \to \mathrm{spm}(A)$; then $\mathfrak{n} \in \mathrm{spm}(B)$ is isolated in its fibre if and only if $B_{\mathfrak{n}}/\mathfrak{m}B_{\mathfrak{n}}$ is a finite k-algebra; here $\mathfrak{m} = \varphi^{-1}(\mathfrak{n})$.

PROPOSITION 8.47. *Let $\varphi\colon W \to V$ be a regular map of algebraic varieties. The set W' of points of W isolated in their fibres is open in W.*

PROOF. Let $w \in W'$. Let W_w and V_v be open affine neighbourhoods of w and $v = \varphi(w)$ such that $\varphi(W_w) \subset V_v$, and let $A = k[V_v]$ and $B = k[W_w]$. Let $\mathfrak{n} = \{f \in B \mid f(w) = 0\}$ — it is the maximal ideal in B corresponding to w.

Let A' be the integral closure of A in B. Theorem 8.46 shows that there exists an $f \in A'$ not in $\mathfrak{m}$ such that $A'_f \simeq B_f$. Write A' as the union of the finitely generated A-subalgebras A_i of A' containing f:

$$A' = \bigcup\nolimits_i A_i.$$

Because A' is integral over A, each A_i is finite over A (see 1.35). We have

$$B_f \simeq A'_f = \bigcup\nolimits_i A_{if}.$$

Because B_f is a finitely generated A-algebra, $B_f = A_{if}$ for all sufficiently large A_i. As the A_i are finite over A, B_f is quasi-finite over A, and $\mathrm{spm}(B_f)$ is an open neighbourhood of w consisting of quasi-finite points. □

PROPOSITION 8.48. *Every quasi-finite map of affine algebraic varieties $\varphi\colon W \to V$ factors into $W \xrightarrow{j} V' \xrightarrow{\varphi'} V$ with j a dominant open immersion and φ' finite.*

PROOF. Let $A = k[V]$ and $B = k[W]$. Because φ is quasi-finite, Theorem 8.46 shows that there exist $f_i \in A'$ such that the sets $\mathrm{spm}(B_{f_i})$ form an open covering of W and $A'_{f_i} \simeq B_{f_i}$ for all i. As W quasi-compact, finitely many sets $\mathrm{spm}(B_{f_i})$ suffice to cover W. The argument in the proof of (8.47) shows that there exists an A-subalgebra A'' of A', finite over A, which contains $f_1, \ldots, f_n$ and is such that $B_{f_i} \simeq A''_{f_i}$ for all i. Now the map $W = \mathrm{Spm}(B) \to \mathrm{Spm}(A'')$ is an open immersion because it is when restricted to $\mathrm{Spm}(B_{f_i})$ for each i. As $\mathrm{Spm}(A'') \to \mathrm{Spm}(A) = V$ is finite, we can take $V' = \mathrm{Spm}(A'')$. □

A regular map $\varphi\colon W \to V$ is said to be ***affine*** if $\varphi^{-1}(U)$ is an open affine subset of W whenever U is an open affine subset of V.

PROPOSITION 8.49. *Let $\varphi\colon W \to V$ be an affine map of irreducible algebraic varieties. Then the map $j\colon W \to V'$ from W into the normalization V' of V in W (8.9) is an open immersion.*

PROOF. Let U be an open affine in V. Let $A = k[U]$ and $B = k[\varphi^{-1}(U)]$. The integral closure A' of A in B is finite over A because it is contained in the integral closure of A in $k(W)$, which is finite over A (8.3)). Thus, in the proof of 8.48 we can take $A'' = A'$, and then $\varphi^{-1}(U) \to \mathrm{Spm}(A')$ is an open immersion. As $\mathrm{Spm}(A')$ is an open subvariety of V' and the sets $\varphi^{-1}(U)$ cover W, this implies that $j\colon W \to V'$ is an open immersion. □

As $V' \to V$ is finite, this proves Theorem 8.45 in the case that φ is an affine map of irreducible varieties. To deduce the general case of Theorem 8.45 from 8.44 requires an additional argument. See Theorem 12.83 of Görtz, U. and Wedhorn, T., *Algebraic Geometry* I., Springer Spektrum, Wiesbaden, 2020.

NOTES

8.50. Let $\varphi\colon W \to V$ be a quasi-finite map of algebraic varieties. In 8.45, we may replace V' with the closure of the image of j. Thus, there is a factorization $\varphi = \varphi' \circ j$ with φ' finite and j a dominant open immersion.

8.51. Theorem 8.45 is false for prevarieties (see 8.33). However, it is true for *separated* maps of prevarieties. A regular map $\varphi\colon V \to S$ of algebraic prevarieties is ***separated*** if the image $\Delta_{V/S}$ of the map $v \mapsto (v,v)\colon V \to V \times_S V$ is closed.

8.52. If V is normal in 8.45, then φ' is open (8.44), and so φ is open. Thus, every quasi-finite map to a normal algebraic variety is open.

ASIDE. The normalization map of an affine cuspidal cubic $Y^2 = X^3$ is a universal homeomorphism without being an isomorphism. The normalization map of an affine nodal cubic with one of the points lying over the node removed is a homeomorphism but not a universal homeomorphism. In particular, a regular map may be étale and bijective, without being a homeomorphism, much less an isomorphism. See mo479766.

Applications to quasi-finite maps

Zariski's main theorem allows us to give a geometric criteria for a regular map to be finite.

PROPOSITION 8.53. *A quasi-finite map $\varphi\colon W \to V$ of algebraic varieties is finite if W is complete.*

PROOF. The map $j\colon W \hookrightarrow V'$ in 8.45 is an isomorphism of W onto its image $j(W)$ in V'. If W is complete, then $j(W)$ is closed (7.7), and so the restriction of φ' to $j(W)$ is finite. □

PROPOSITION 8.54. *A quasi-finite map $\varphi\colon W \to V$ of algebraic varieties is finite if (and only if) it is proper.*

PROOF. Factor φ into $W \overset{j}{\hookrightarrow} W' \overset{\alpha}{\to} V$ with α finite and j an open immersion. Factor j into

$$W \xrightarrow{w \mapsto (w, jw)} W \times_V W' \xrightarrow{(w,w') \mapsto w'} W'.$$

The image of the first map is Γ_j, which is closed because W' is a variety (see 5.28; W' is separated because it is finite over a variety — exercise). Because φ is proper, the second map is closed. Hence j 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. □

NOTES

8.55. When W and V are curves, every surjective map $W \to V$ is closed. Thus it is easy to give examples of closed surjective quasi-finite, but nonfinite, maps. Consider, for example, the map

$$(\mathbb{A}^1 \smallsetminus \{0\}) \sqcup \mathbb{A}^0 \to \mathbb{A}^1,$$

sending each $a \in \mathbb{A}^1 \smallsetminus \{0\}$ to a and $O \in \mathbb{A}^0$ to 0. This does not violate the Proposition 8.54, because the map is only closed, not universally closed.

Applications to birational maps

Recall (p. 117) that 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.

8.56. 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 subvariety into a variety is birational.

(b) The map (8.31) from $\mathbb{A}^1$ to the cuspidal cubic,

$$\mathbb{A}^1 \to C, \quad t \mapsto (t^2, t^3),$$

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 $V' \smallsetminus \varphi^{-1}(P)$ is an isomorphism onto $V \smallsetminus P$, but $\varphi^{-1}(P)$ is the projective space attached to the vector space $T_P(V)$. See the section on blow-ups below.

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).

PROPOSITION 8.57. *Let $\varphi\colon W \to V$ be a birational regular map of irreducible varieties. If V is normal and the map φ is quasi-finite, then φ is an isomorphism from W onto an open subvariety of V.*

PROOF. Factor φ as in the Theorem 8.45 (so, in particular, $\varphi'\colon V' \to V$ is the normalization of V in W). For each open affine subset U of V, $k[\varphi'^{-1}(U)]$ is the integral closure of $k[U]$ in $k(W)$. Because φ is birational, the inclusion $k(V) \subset k(V') = k(W)$ is an equality. Now $k[U]$ is integrally closed in $k(V)$ (because V is normal), and so $U = \varphi'^{-1}(U)$ (as varieties). We have shown that $\varphi'\colon V' \to V$ is an isomorphism locally on the base V, and hence an isomorphism. □

8.58. In topology, a continuous bijective map $\varphi: W \to V$ need not be a homeomorphism, but it is if W is compact and V is Hausdorff. Similarly, a bijective regular map of algebraic varieties need not be an isomorphism. Here are three examples:

(a) In characteristic p, the Frobenius map

$$(x_1, \dots, x_n) \mapsto (x_1^p, \dots, x_n^p) : \mathbb{A}^n \to \mathbb{A}^n$$

is bijective and regular, but it is not an isomorphism even though $\mathbb{A}^n$ is normal.

(b) The map $t \mapsto (t^2, t^3)$ from $\mathbb{A}^1$ to the cuspidal cubic (see 8.56b) is bijective, but not an isomorphism.

(c) Consider the regular map $\mathbb{A}^1 \to \mathbb{A}^1$ sending x to $1/x$ for $x \neq 0$ and 0 to 0. Its graph Γ is the union of $(0,0)$ and the hyperbola $xy = 1$, which is a closed subvariety of $\mathbb{A}^1 \times \mathbb{A}^1$. The projection $(x, y) \mapsto x : \Gamma \to \mathbb{A}^1$ is a bijective, regular, birational map, but it is not an isomorphism even though $\mathbb{A}^1$ is normal.

If we require the map to be birational (thereby excluding example (a)), V to be normal (thereby excluding example (b)), and the varieties to be irreducible (thereby excluding example (c)), then the map is an isomorphism.

PROPOSITION 8.59. *Let $\varphi: W \to V$ be a bijective regular map of irreducible algebraic varieties. If the map φ is birational and V is normal, then φ is an isomorphism.*

PROOF. The hypotheses imply that φ is an isomorphism of W onto an open subset of V (8.57). Because φ is bijective, the open subset must be the whole of V. □

In fact, example (a) can be excluded by requiring that φ be generically separable (instead of birational), and (b) can be excluded by requiring that the map be étale.

PROPOSITION 8.60. *Let $\varphi: W \to V$ be a bijective regular map of irreducible varieties. If V is normal and $k(W)$ is separably generated over $k(V)$, then φ is an isomorphism.*

PROOF. Because φ is bijective, $\dim(W) = \dim(V)$ (see Theorem 9.9 below) and the separable degree of $k(W)$ over $k(V)$ is 1 (apply 8.40 to the variety V' in 8.45). Hence φ is birational, and we may apply 8.59. □

8.61. In functional analysis, the closed graph theorem states that, if a linear map $\varphi: W \to V$ between two Banach spaces has a closed graph $\Gamma \stackrel{\text{def}}{=} \{(w, \varphi w) \mid w \in W\}$, then φ is continuous (Wikipedia: CLOSED GRAPH THEOREM). One can ask whether a similar statement is true in algebraic geometry. Specifically, if $\varphi: W \to V$ is a map (in the set-theoretic sense) of algebraic varieties V, W whose graph is closed (for the Zariski topology), then is φ a regular map? The answer is no in general. For example, even in characteristic zero, the map $(t^2, t^3) \to t : C \to \mathbb{A}^1$ inverse to that in 8.56(b) has closed graph but is not regular. In characteristic p, the inverse of the Frobenius map $x \mapsto x^p$ provides another counterexample. For a third counterexample, see 8.58(c). The projection π from Γ to W is a bijective regular map, and so φ will be regular if π is an isomorphism. According to 8.60, π is an isomorphism if the varieties are irreducible, W is normal, and π is generically separable. In particular, a map between irreducible normal algebraic varieties in characteristic zero is regular if its graph is closed.

A condition for an algebraic monoid to be a group

Recall (p. 110) that we defined an algebraic variety V with a group structure $V \times V \to V$ to be a group variety if both the multiplication map $a, b \mapsto a \cdot b \colon V \times V \to V$ and inversion map $a \mapsto a^{-1} \colon V \to V$ are regular. Here we show that the second condition is unnecssary.

A ***monoid variety*** is an algebraic variety G together with the structure of a monoid defined by regular maps

$$m \colon G \times G \to G, \quad e \colon \mathbb{A}^0 \to G.$$

LEMMA 8.62. *Let (G, m, e) be a monoid variety. The map*

$$T_e G \oplus T_e G \simeq T_{(e,e)}(G \times G) \xrightarrow{(dm)_{(e,e)}} T_e(G)$$

is addition.

PROOF. The first isomorphism is $(X, Y) \mapsto (d\alpha)_e(X) + (d\beta)_e(Y)$, where α is the map $x \mapsto (x, e) \colon G \to G \times G$ and β is $x \mapsto (e, x)$. To compute $(dm)_{(e,e)}((d\beta)_e(X) + (d\alpha)_e(Y))$, note that $m \circ \alpha = \mathrm{id}_G = m \circ \beta$. □

PROPOSITION 8.63. *Let G be an algebraic variety with a group structure $m \colon G \times G \to G$. If m is regular, then (G, m) is a group variety, i.e., the map $a \mapsto a^{-1}$ is regular.*

PROOF. Let $a \in G(k)$. The translation map $L_a \colon x \mapsto ax$ is an isomorphism $G \to G$ because it has an inverse $L_{a^{-1}}$. Therefore G is homogeneous as an algebraic variety: for any two points in G, there is an isomorphism $G \to G$ mapping one to the other. It follows that G normal (8.7).

The map

$$(x, y) \mapsto (x, xy) \colon G \times G \to G \times G$$

is regular, bijective, and induces an isomorphism on the tangent spaces at (e, e) (apply the lemma). It is therefore an isomorphism of algebraic varieties over k. Therefore, its inverse $(x, y) \mapsto (x, x^{-1}y)$ is regular, and so

$$(x, y) \mapsto x^{-1}y \colon G \times G \to G$$

is regular. This implies that (G, m) is an algebraic group. □

Variants of Zariski's main theorem

Mumford 1966a, III, §9, lists the following variants of ZMT.

Original form (8.57) Let $\varphi \colon W \to V$ be a birational regular map of irreducible varieties. If V is normal and φ is quasi-finite, then φ is an isomorphism of W onto an open subvariety of V.

Topological form Let V be a normal variety over $\mathbb{C}$, and let $v \in V$. Let S be the singular locus of V. Then the complex neighbourhoods U of v such that $U \setminus U \cap S$ is connected form a base for the system of complex neighbourhoods of v.

Power series form Let V be a normal variety, and let $\mathcal{O}_{V,Z}$ be the local ring attached to an irreducible closed subset of V (cf. p. 180). If $\mathcal{O}_{V,Z}$ is an integrally closed integral domain, then so also is its completion.

Grothendieck's form (8.45) Every quasi-finite map of algebraic varieties factors as the composite of an open immersion with a finite map.

Connectedness theorem Let $\varphi\colon W \to V$ be a proper birational map, and let v be a (closed) normal point of V. The $\varphi^{-1}(v)$ is a connected set (in the Zariski topology).

The original form of the theorem was proved by Zariski using a fairly direct argument whose method does not seem to generalize.[3] The power series form was also proved by Zariski, who showed that it implied the original form. The last two forms are much deeper and were proved by Grothendieck.

NOTES. The original form of the theorem (8.57) is the "Main theorem" of Zariski, O., Foundations of a general theory of birational correspondences. Trans. Amer. Math. Soc. 53, (1943). 490–542.

f. Stein factorization

The following important theorem shows that the fibres of a proper map are disconnected only because the fibres of finite maps are disconnected.

THEOREM 8.64 (STEIN FACTORIZATION). *Every proper map $\varphi\colon W \to V$ of algebraic varieties factors into $W \overset{\varphi_1}{\to} W' \overset{\varphi_2}{\to} V$ with φ_1 proper with connected fibres and φ_2 finite.*

When V is affine, this is the factorization

$$W \to \operatorname{Spm}(\mathcal{O}_W(W)) \to V.$$

The first major step in the proof of the theorem is to show that $\varphi_*\mathcal{O}_W$ is a coherent sheaf on V (see Chapter 13). Here $\varphi_*\mathcal{O}_W$ is the sheaf of $\mathcal{O}_V$-algebras on V,

$$U \rightsquigarrow \mathcal{O}_W(\varphi^{-1}(U)).$$

To say that $\varphi_*\mathcal{O}_W$ is coherent means that, on every open affine subset U of V, it is the sheaf of $\mathcal{O}_U$-algebras defined by a finite $k[U]$-algebra. This, in turn, means that there exists a regular map $\varphi_2\colon \operatorname{Spm}(\varphi_*\mathcal{O}_W) \to V$ that, over every open affine subset U of V, is the map attached by Spm to the map of k-algebras $k[U] \to \mathcal{O}_W(\varphi^{-1}(U))$.

The Stein factorization is then

$$W \xrightarrow{\varphi_1} W' \overset{\text{def}}{=} \operatorname{Spm}(\varphi_*\mathcal{O}_W) \xrightarrow{\varphi_2} V.$$

By construction, φ_2 is finite and $\varphi_1\colon W \to W'$ has the property that $\mathcal{O}_{W'} \to \varphi_{1*}\mathcal{O}_W$ is an isomorphism. That its fibres are connected is a consequence of the following extension of Zariski's connectedness theorem to non birational maps.

THEOREM 8.65. *Let $\varphi\colon W \to V$ be a proper map such that the map $\mathcal{O}_V \to \varphi_*\mathcal{O}_W$ is an isomorphism. Then the fibres of φ are connected.*

See Hartshorne 1977, III, §11.

NOTES. The Stein factorization was originally proved (in 1956) by Stein for complex spaces (Wikipedia: STEIN FACTORIZATION).

[3] See Lang, S., Introduction to Algebraic Geometry, 1958, V 2, for Zariski's original statement and proof of this theorem. See Springer, T.A., Linear Algebraic Groups, 1998, 5.2.8, for a direct proof of (8.59).

g. Blow-ups

Under construction.

Let P be a nonsingular point on an algebraic variety V, and let $T_p(V)$ be the tangent space at P. The blow-up of V at P is a regular map $\tilde{V} \to V$ that replaces P with the projective space $\mathbb{P}(T_P(V))$. More generally, the blow-up at P replaces P with $\mathbb{P}(C_P(V))$, where $C_P(V)$ is the geometric tangent cone at P.

Blowing up the origin in $\mathbb{A}^n$

Let O be the origin in $\mathbb{A}^n$, and let $\pi\colon \mathbb{A}^n \smallsetminus \{O\} \to \mathbb{P}^{n-1}$ be the map $(a_1, \ldots, a_n) \mapsto (a_1 : \ldots : a_n)$. Let Γ_π be the graph of π, and let $\widetilde{\mathbb{A}^n}$ be the closure of Γ_π in $\mathbb{A}^n \times \mathbb{P}^{n-1}$. The map $\sigma\colon \widetilde{\mathbb{A}^n} \to \mathbb{A}^n$ defined by the projection map $\mathbb{A}^n \times \mathbb{P}^{n-1} \to \mathbb{A}^n$ is the blow-up of $\mathbb{A}^n$ at O.

Blowing up a point on a variety

Examples

8.66. The nodal cubic

8.67. The cuspidal cubic

h. Resolution of singularities

Let V be an algebraic variety. A ***desingularization*** of V is birational regular map $\pi\colon W \to V$ such that W is nonsingular and π is proper; if V is projective, then W should also be projective, and π should induce an isomorphism

$$W \smallsetminus \pi^{-1}(\mathrm{Sing}(V)) \to V \smallsetminus \mathrm{Sing}(V).$$

In other words, the nonsingular variety W is the same as V except over the singular locus of V. When a variety admits a desingularization, then we say that ***resolution of singularities*** holds for V.

Note that with "nonsingular" replaced by "normalization", the normalization of V (see 8.5) provides such a map (resolution of abnormalities).

Nagata's embedding theorem 7.50 shows that it suffices to prove resolution of singularities for complete varieties, and Chow's lemma 7.39 then shows that it suffices to prove resolution of singularities for projective varieties. From now on, we shall consider only projective varieties.

Resolution of singularities for curves was first obtained using blow-ups (see Chapter 7 of Fulton's book, Algebraic Curves). Zariski introduced the notion of the normalization of a variety, and observed that the normalization $\pi\colon \tilde{V} \to V$ of a curve V in $k(V)$ is a desingularization of V.

There were several proofs of resolution of singularities for surfaces over $\mathbb{C}$, but the first to be accepted as rigorous is that of Walker (patching Jung's local arguments; 1935). For a surface V, normalization gives a surface with only point singularities (8.12), which can then be blown up. Zariski showed that the desingularization of a surface in characteristic zero can be obtained by alternating normalizations and blow-ups.

The resolution of singularities for three-folds in characteristic zero is much more difficult, and was first achieved by Zariski (Ann. of Math. 1944). His result was extended to nonzero characteristic by his student Abhyankar and to all varieties in characteristic zero by his student Hironaka.

The resolution of singularities for higher dimensional varieties in nonzero characteristic is one of the most important outstanding problems in algebraic geometry. In 1996, de Jong proved a weaker result in which, instead of the map π being birational, $k(W)$ is allowed to be a finite extension of $k(V)$.

The article Wikipedia: Resolution of singularities is excellent.

A little history

Normal varieties were introduced by Zariski in a paper, Amer. J. Math. 61, 1939, p. 249–194. There he noted that the singular locus of a normal variety has codimension at least 2 and that the system of hyperplane sections of a normal variety relative to a projective embedding is complete (i.e., is a complete rational equivalence class). Zariski's introduction of the notion of a normal variety and of the normalization of a variety was an important insertion of commutative algebra into algebraic geometry. It is not easy to give a geometric intuition for "normal". One criterion is that a variety is normal if and only if every surjective finite birational map onto it is an isomorphism (8.57). See mo109395 for a discussion of this question.

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 $\varphi\colon W \to V$ be an affine map. Show that W is separated if V is separated.

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 nonempty closed subvariety of dimension i.

Chapter 9

Regular Maps and Their Fibres

Consider again the regular map $\varphi\colon \mathbb{A}^2 \to \mathbb{A}^2$, $(x,y) \mapsto (x,xy)$ (Exercise 3-3). The line $Y = c$ maps to the line $Y = cX$. As c runs over the elements of k, this line sweeps out the whole x,y-plane except for the y-axis, and so the image of φ is

$$C = (\mathbb{A}^2 \smallsetminus \{y\text{-axis}\}) \cup \{(0,0)\},$$

which is neither open nor closed, and, in fact, is not even locally closed. The fibre over (a,b) is

$$\varphi^{-1}(a,b) = \begin{cases} \text{point } (a, b/a) & \text{if } a \neq 0 \\ Y\text{-axis} & \text{if } (a,b) = (0,0) \\ \emptyset & \text{if } a = 0,\, b \neq 0. \end{cases}$$

From this unpromising example, it would appear that it is not possible to say anything about the image of a regular map or its fibres. However, it turns out that almost everything that can go wrong already goes wrong in this example. 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 (upper semicontinuity)

(c) the number of elements (if finite) in the fibres can drop only on closed subsets (lower semicontinuity), provided the map is finite, the target variety is normal, and k has characteristic zero.

a. The constructibility theorem

THEOREM 9.1. *Let $\varphi\colon W \to V$ be a dominant map of irreducible affine algebraic varieties. Then $\varphi(W)$ contains a nonempty open subset of V.*

PROOF. Because φ is dominant, the map $f \mapsto f\circ\varphi\colon k[V] \to k[W]$ is injective (3.34). According to Lemma 9.4 below, there exists a nonzero $a \in k[V]$ such that every homomorphism of k-algebras $\alpha\colon k[V] \to k$ such that $\alpha(a) \neq 0$ extends to a homomorphism $\beta\colon k[W] \to k$. In particular, for any point P in $D(a) \subset V$, the homomorphism $g \mapsto g(P)\colon k[V] \to k$ extends to a homomorphism $\beta\colon k[W] \to k$. The kernel of β is a maximal ideal of $k[W]$ whose zero set is a point Q of W such that $\varphi(Q) = P$. □

Before beginning the proof of Lemma 9.4, we should look at an example.

EXAMPLE 9.2. Let A be an affine k-algebra, and let $B = A[T]/(f)$ with $f = a_m T^m + \cdots + a_0$, $m > 0$. When does a homomorphism $\alpha\colon A \to k$ extend to B? The extensions of α correspond to roots of the polynomial $\alpha(a_m)T^m + \cdots + \alpha(a_0)$ in k, and so there exists an extension unless this is a nonzero constant polynomial. In particular, α extends if $\alpha(a_m) \neq 0$.

LEMMA 9.3. *Let A and $B = A[T]/\mathfrak{a}$ be affine k-algebras. Assume that A and B are integral domains, and let $\mathfrak{c} \subset A$ be the ideal of leading coefficients of the polynomials in $\mathfrak{a}$. Then every homomorphism $\alpha\colon A \to k$ such that $\alpha(\mathfrak{c}) \neq 0$ extends to a homomorphism $B \to k$.*

PROOF. If $\mathfrak{a} = 0$, then every homomorphism α extends, and so we may suppose that $\mathfrak{a} \neq 0$. Let $\alpha\colon A \to k$ be a homomorphism such that $\alpha(\mathfrak{c}) \neq 0$, and choose a polynomial $f = a_m T^m + \cdots + a_0$ in $\mathfrak{a}$ of least degree such that $\alpha(a_m) \neq 0$. Then $m \geq 1$ otherwise $B = 0$. We shall use induction on m.

Extend α to a homomorphism $\tilde{\alpha}\colon A[T] \to k[T]$ by sending T to T. Then $\tilde{\alpha}(\mathfrak{a})$ is an ideal in $k[T]$.

If $\tilde{\alpha}(\mathfrak{a}) \neq k[T]$, then it has a zero c in k (2.11). This means that the homomorphism

$$A[T] \xrightarrow{\tilde{\alpha}} k[T] \xrightarrow{h \mapsto h(c)} k$$

is zero on $\mathfrak{a}$, and so it factors through a homomorphism $B = A[T]/\mathfrak{a} \to k$. This is an extension of α to B.

If $\tilde{\alpha}(\mathfrak{a}) = k[T]$, then $\mathfrak{a}$ contains a polynomial

$$g(T) = b_n T^n + \cdots + b_0, \quad n > 0, \quad \alpha(b_n) = \cdots = \alpha(b_1) = 0, \quad \alpha(b_0) \neq 0.$$

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 $m \geq 0$, we must have $\tilde{\alpha}(q) = 0$, and so $\tilde{\alpha}(r)$ is a nonzero constant. We may replace $g(T)$ with $r(T)$, and so suppose that $n < m$. If $m = 1$, such a $g(T)$ cannot exist, so we may suppose that $m > 1$.

For a polynomial $h(T) = c_r T^r + \cdots + c_0$, we let $h'(T) = c_r + \cdots + c_0 T^r$. The A-module generated by the polynomials $T^s h'(T)$ with $s \in \mathbb{N}$ and $h \in \mathfrak{a}$ is an ideal $\mathfrak{a}'$ in $A[T]$. If $\mathfrak{a}' \cap k \neq \{0\}$, then $\mathfrak{a}$ contains a nonzero polynomial cT^r, so B is generated over A by a nilpotent, which implies that $A = B$ (recall that B is an integral domain). Otherwise, we let $B' = A[T]/\mathfrak{a}'$, and note that $\mathfrak{a}'$ contains the polynomial

$$g' = b_n + \cdots + b_0 T^n, \quad n < m, \quad \alpha(b_0) \neq 0.$$

Because $\deg g' < m$, the induction hypothesis implies that α extends to a homomorphism $B' = A[T]/\mathfrak{a}' \to k$. Let c denote the image of T in k. Then, for all $h = c_r T^r + \cdots + c_0 \in \mathfrak{a}$, $\alpha(c_r) + \cdots + \alpha(c_0)c^r = 0$. On applying this with $h = g$, we find that $c = 0$. On applying it with $h = f$, we find that $\alpha(a_m) = 0$, which is a contradiction. This completes the proof. □

LEMMA 9.4. *Let $A \subset B$ be affine k-algebras, and assume that A and B are integral domains. For any nonzero $b \in B$, there exists a nonzero $a \in A$ with the following property: every homomorphism $\alpha\colon A \to k$ from A into k such that $\alpha(a) \neq 0$ extends to a homomorphism $\beta\colon B \to k$ with $\beta(b) \neq 0$.*

PROOF Suppose first that B is generated by a single element, say, $B = A[x]$. Let $\mathfrak{a}$ be the kernel of the homomorphism $T \mapsto x$, $A[T] \to A[x]$.

If $\mathfrak{a} = (0)$, 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 $\alpha\colon A \to k$ is such that $\alpha(a_0) \neq 0$, then there exists a $c \in k$ such that $f(c) \neq 0$, and we can take β to be the homomorphism $\sum d_i x^i \mapsto \sum \alpha(d_i) c^i$.

If $\mathfrak{a} \neq (0)$, let

$$f(T) = a_m T^m + \cdots + a_0, \quad a_m \neq 0,$$

be an element of $\mathfrak{a}$ of smallest possible degree. Let $h(T) \in A[T]$ represent b. As b is nonzero, $h \notin \mathfrak{a}$. 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 $c \in A \smallsetminus \{0\}$ such that

$$uh + vf = c.$$

It follows now that ca_m satisfies our requirements, for if $\alpha(ca_m) \neq 0$, then α can be extended to $\beta\colon B \to k$ by the preceding lemma, and $\beta(u(x) \cdot b) = \beta(c) \neq 0$, and so $\beta(b) \neq 0$.

In the general case, we can write $B = A[x_1, \ldots, x_n]$. There exists an element $b_{n-1} \in A[x_1, \ldots, x_{n-1}]$ with the following property: every homomorphism $\alpha\colon A[x_1, \ldots, x_{n-1}] \to k$ such that $\alpha(b_{n-1}) \neq 0$ extends to a homomorphism $\beta\colon B \to k$ with $\beta(b) \neq 0$. Then there exists a $b_{n-2} \in A[x_1, \ldots, x_{n-2}]$ etc. Continuing in this fashion, we obtain an element $a \in A$ with the required property. □

ASIDE 9.5. For an alternative proof of Theorem 9.1 using the generic flatness theorem, see 9.28 below.

In order to generalize 9.1 to regular maps of arbitrary varieties, we need the notion of a constructible set. Let W be a noetherian 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,

$$C = \bigcup_{1 \le i \le n} U_i \cap Z_i.$$

On passing to the complements, we find that

$$C' = \bigcup_{1 \le i \le n} U_i' \cap Z_i',$$

so the complement of a constructible set is constructible. It follows that finite unions and finite intersections of constructible sets are constructible. Obviously, if C is constructible in W and $V \subset W$, then $C \cap V$ is constructible in V, and it is constructible in W if V is open or closed.

A constructible subset of $\mathbb{A}^n$ is one that is definable by a finite number of polynomials. More precisely, it is defined by a finite number of statements of the form

$$f(X_1, \ldots, X_n) = 0, \qquad g(X_1, \ldots, X_n) \neq 0$$

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 an infinite subset of $\mathbb{A}^1$ that omits an infinite set.

PROPOSITION 9.6. *Let C be a constructible set whose closure $\bar{C}$ is irreducible. Then C contains a nonempty open subset of its closure $\bar{C}$.*

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,

$$U_i \cap Z_i \supset U_i \cap \bar{C} \supset U_i \cap C \supset U_i \cap (U_i \cap Z_i) = U_i \cap Z_i.$$

Thus $U_i \cap Z_i = U_i \cap \bar{C}$, which is a nonempty open subset of $\bar{C}$ contained in C. □

THEOREM 9.7. *Every regular map $\varphi\colon W \to V$ sends constructible sets to constructible sets.*

PROOF We first show that it suffices to prove the theorem with W and V affine. Write V as a finite union of open affines, and then write the inverse image of each of the affines as a finite union of open affines. In this way, we get $W = \bigcup_{i \in I} W_i$ with each W_i open affine and $\varphi(W_i)$ contained in an open affine of V. If C is a constructible subset of W, then $\varphi(C) = \bigcup_{i \in I} \varphi(C \cap W_i)$, and so $\varphi(C)$ is constructible if each set $\varphi(C \cap W_i)$ is constructible.

Now assume that W and V are affine, and let C be a constructible subset of W. Let W_i be the irreducible components of W. They are closed in W, and so $C \cap W_i$ is constructible in W. As $\varphi(W) = \bigcup \varphi(C \cap W_i)$, it is constructible if the $\varphi(C \cap W_i)$ are. Hence we may suppose that W is irreducible. Moreover, C is a finite union of its irreducible components. As these are closed in C, they are constructible in W. We may therefore assume that C is also irreducible; $\bar{C}$ is then an irreducible closed subvariety of W.

We 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 $\varphi(C)$ is constructible by the induction hypothesis applied to $\bar{C} \xrightarrow{\varphi} V$. We may therefore assume that $\bar{C} = W$. Replace V with $\overline{\varphi(C)}$. According to Proposition 9.6, C contains a dense open subset U' of W, and Theorem 9.1 applied to $U' \xrightarrow{\varphi} V$ shows that $\varphi(C)$ contains a dense open subset U of V. Write

$$\varphi(C) = U \cup \varphi(C \cap \varphi^{-1}(V \smallsetminus U)).$$

Then $\varphi^{-1}(V \smallsetminus U)$ is a proper closed subset of W (the complement of $V \smallsetminus U$ is dense in V and φ is dominant). As $C \cap \varphi^{-1}(V \smallsetminus U)$ is constructible in $\varphi^{-1}(V \smallsetminus U)$, the set $\varphi(C \cap \varphi^{-1}(V \smallsetminus U))$ is constructible in V by induction, which completes the proof. □

ASIDE 9.8. Let X be a subset of $\mathbb{C}^n$. If X is constructible for the Zariski topology on $\mathbb{C}^n$, then the closure of X for the Zariski topology is equal to its closure for the complex topology.

b. The fibres of morphisms

We examine the fibres of a regular map $\varphi\colon W \to V$. After replacing V with the closure of the image of φ, we may suppose that φ is dominant.

THEOREM 9.9. *Let $\varphi\colon W \to V$ be a dominant map of irreducible algebraic varieties.*

(a) $\dim(W) \geq \dim(V)$.

(b) *If $P \in \varphi(W)$, then*

$$\dim(\varphi^{-1}(P)) \geq \dim(W) - \dim(V)$$

with equality holding exactly on a nonempty open subset U of V.

(c) *For each $i \in \mathbb{N}$, the set*

$$V_i = \{P \in V \mid \dim(\varphi^{-1}(P)) \geq i\}$$

is closed in $\varphi(W)$.

In other words, for P in a dense open subset U of V, the dimension of the fibre $\varphi^{-1}(P)$ has the expected value $\dim(W) - \dim(V)$, and it jumps on the closed complement of U (possibly empty). It may jump further on closed subsets of the closed complement of U.

Before proving the theorem, we look at an example.

EXAMPLE 9.10. Consider a system of linear equations

$$\sum_{j=1}^{n} a_{ij} X_j = 0, \quad i = 1, \dots, m,$$

with coefficients in a field k (not necessarily algebraically closed). The quotient

$$\frac{k[X_1, \dots, X_n]}{(\sum a_{ij} X_j)} \simeq k[X_{j_1}, \dots, X_{j_d}],$$

where $X_{j_1}, \dots, X_{j_d}$ are the "free" variables for the system of equations (cf. 2.61). Thus the field of fractions of $k[X_1, \dots, X_n]/(\sum a_{ij} X_j)$ has transcendence degree d over k, where $d = n - \operatorname{rank}(a_{ij})$.

Now consider the subvariety $W \subset V \times \mathbb{A}^n$ defined by a system of linear equations

$$\sum_{j=1}^{n} a_{ij} X_j = 0, \quad i = 1, \dots, m,$$

with coefficients $a_{ij} \in k[V]$. The projection map $\varphi \colon W \to V$ is surjective, and the above discussion shows that $k(W)$ has transcendence degree d over $k(V)$, where

$$d = n - \operatorname{rank} A, \quad A \stackrel{\text{def}}{=} (a_{ij}).$$

Thus,

$$\dim W = \dim V + n - \operatorname{rank}(A).$$

The fibre $\varphi^{-1}(P)$ over $P \in V$ is the subvariety of $\mathbb{A}^n$ defined by the system of linear equations

$$\sum_{j=1}^{n} a_{ij}(P) X_j = 0, \quad i = 1, \dots, m,$$

with coefficients in k. It has dimension

$$\dim \varphi^{-1}(P) = n - \operatorname{rank} A(P), \quad A(P) = (a_{ij}(P)).$$

Let $r = \operatorname{rank}(A)$. Then $\operatorname{rank} A(P) = r$ on the open subset U of V where some $r \times r$-minor of A does not vanish, and it drops on the closed complement of U. Correspondingly, $\dim \varphi^{-1}(P) = \dim W - \dim V$ on U, and it jumps on the closed complement of U.

PROOF (OF THEOREM 9.9). (a) Because the map is dominant, there is a homomorphism $k(V) \hookrightarrow k(W)$, and obviously $\operatorname{tr}\deg_k k(V) \leq \operatorname{tr}\deg_k k(W)$ (an algebraically independent subset of $k(V)$ remains algebraically independent in $k(W)$).

(b) In proving the first part of (b), we may replace V with an open neighbourhood of P. In particular, we can assume V to be affine. Let m and n be the dimensions of V and W. From Proposition 3.47 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 open neighbourhood of P, we may 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 (by 3.45). 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 $k(V) \subset k(W)$, and $k(W)$ has transcendence degree $\dim W - \dim V = n - m$ over $k(V)$. Let $k[V] = k[x_1, \ldots, x_M]$ and let $k[W] = k[y_1, \ldots, y_N]$. Then $\{x_1, \ldots, x_M\}$ contains a transcendence basis for $k(V)$ over k, which we may suppose to be $\{x_1, \ldots, x_m\}$. Similarly, after renumbering, we may suppose that $\{y_1, \ldots, y_{n-m}\}$ is a transcendence basis for $k(W)$ over $k(V)$. Now $\{x_1, \ldots, y_{n-m}\}$ is a transcendence basis for $k(W)$ over k, and so, for each $i > n - m$, there is a nonzero polynomial $F_i(X_1, \ldots, X_m, Y_1, \ldots, Y_{n-m}, Y_i)$ such that

$$F_i(x_1, \ldots, x_m, y_1, \ldots, y_{n-m}, y_i) = 0. \tag{37}$$

Let $P \in V$ and let $\bar{y}_i$ denote the restriction of y_i to $\varphi^{-1}(P)$. Then

$$k[\varphi^{-1}(P)] = k[\bar{y}_1, \ldots, \bar{y}_N].$$

The equation (37) is an algebraic relation among the functions $x_1, \ldots, y_i$ on W. When restricted to $\varphi^{-1}(P)$, it becomes

$$F_i(x_1(P), \ldots, x_m(P), \bar{y}_1, \ldots, \bar{y}_{n-m}, \bar{y}_i) = 0.$$

If this is a nontrivial algebraic relations for all i, 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 the zero polynomial, then $\operatorname{tr}\deg_k(k(\bar{y}_1, \ldots, \bar{y}_N) \leq n - m$, so $\dim \varphi^{-1}(P) \leq n - m$.

Regard $F_i(x_1, \ldots, x_m, Y_1, \ldots, Y_{n-m}, Y_i)$ as a polynomial in the Y with coefficients polynomials in the x. Let U_i be the open subset of V where some coefficient of the polynomial is nonzero — this is nonempty because F_i is a nonzero element of $k[V][Y_1, \ldots, Y_{n-m}, Y_i]$. The last remark shows that, for $P \in \bigcap U_i$, $\dim \varphi^{-1}(P) \leq n - m$, hence $= n - m$ by (a).

Finally, if for a particular point P, $\dim \varphi^{-1}(P) = n - m$, then we 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. □

Recall that a regular map $\varphi: W \to V$ of algebraic varieties is closed if, for example, W is complete (7.7).

PROPOSITION 9.11. *Let $\varphi: W \to V$ be a regular surjective closed map of varieties, and let $n \in \mathbb{N}$. If V is irreducible and all fibres $\varphi^{-1}(P)$ of φ are irreducible of dimension n, then W is irreducible of dimension* $\dim(V) + n$*.*

PROOF. Let Z be an irreducible closed subset of W, and consider the map $\varphi|Z: Z \to V$; 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 (9.9) 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 $P \in U$, the fibre $\varphi^{-1}(P)$ is not contained in Z.

(c) $\varphi(Z) = V$, $\dim(Z) \geq n + \dim(V)$. Then 9.9(b) 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 $\dim Z = \dim V + n$.

Now let $Z_1, \ldots, Z_r$ be the irreducible components of W. I claim that (c) 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, $\varphi^{-1}(P)$ is contained in *none* of the Z_i; but $\varphi^{-1}(P)$ is irreducible and $\varphi^{-1}(P) = \bigcup(\varphi^{-1}(P) \cap Z_i)$, and so this is impossible. □

☡ It is possible for all the fibres of regular map $W \to V$ to be reducible without W being reducible. The subvariety of $\mathbb{A}^2 \times \mathbb{A}^2$ with equation $x_1^2 y_1 - x_2^2 y_2 = 0$ is irreducible, but the fibres of the projection to the first factor (obtained by fixing the values of y_1 and y_2) are all reducible. To extend this to $\mathbb{P}^2 \times \mathbb{P}^2$, pass to the projective closure.

c. Flat maps and their fibres

A flat map is the algebraic analogue of a map whose fibres form a continuously varying family. For example, a surjective regular map of smooth varieties is flat if and only if all fibres have the same dimension. A finite map is flat if and only if, over every connected component, all fibres have the same number of points (counting multiplicities). Flat maps of algebraic varieties are open.

Flat homomorphisms of rings

Let A be a ring and B an A-algebra. If the sequence of A-modules

$$0 \to N' \xrightarrow{\alpha} N \xrightarrow{\beta} N'' \to 0$$

is exact, then the sequence of B-modules

$$B \otimes_A N' \xrightarrow{1\otimes\alpha} B \otimes_A N \xrightarrow{1\otimes\beta} B \otimes_A N'' \longrightarrow 0 \qquad (*)$$

is exact, but $B \otimes_A N' \to B \otimes_A N$ need not be injective. For example, when we tensor the exact sequence of $k[X]$-modules

$$0 \to k[X] \xrightarrow{f \mapsto X \cdot f} k[X] \xrightarrow{f \mapsto f \bmod (X)} k[X]/(X) \to 0$$

with k, we get the sequence

$$k \xrightarrow{0} k \xrightarrow{\text{id}} k \to 0.$$

We prove that (*) is exact. The surjectivity of $1 \otimes \beta$ is obvious. Let $q\colon B \otimes_A N \to Q$ be the cokernel of $1 \otimes \alpha$. As $(1 \otimes \beta) \circ (1 \otimes \alpha) = 1 \otimes (\beta \circ \alpha) = 0$, the map $1 \otimes \beta$ factors through q,

$$\begin{array}{ccccccc} B \otimes_A N' & \xrightarrow{1 \otimes \alpha} & B \otimes_A N & \xrightarrow{1 \otimes \beta} & B \otimes_A N'' & \longrightarrow & 0. \\ & & & \searrow^{q} & \uparrow{\scriptstyle f} & & \\ & & & & Q & & \end{array}$$

We construct an inverse g to f. If $n_1, n_2 \in N$ have the same image in N'', then they differ by an element of $\alpha(N')$, and so $\phi(b \otimes n_1) = \phi(b \otimes n_2)$ for all $b \in B$. Hence the A-bilinear map

$$B \times N \to Q, \quad (b, n) \mapsto \phi(b \otimes n)$$

factors through $B \times N''$, and so defines an A-linear map $g\colon\ B \otimes_A N'' \to Q$. This is inverse to f.

DEFINITION 9.12. An A-algebra B is ***flat*** if

$$M \to N \text{ injective} \implies B \otimes_A M \to B \otimes_A N \text{ injective}.$$

It is ***faithfully flat*** if, in addition,

$$B \otimes_A M = 0 \implies M = 0.$$

A homomorphism $\alpha\colon\ A \to B$ of rings is ***flat*** (resp. ***faithfully flat***) if it makes B into a flat (resp. faithfully flat) algebra.

Therefore, an A-algebra B is flat if and only if the functor $M \rightsquigarrow B \otimes_A M$ from A-modules to B-modules is exact.

EXAMPLE 9.13. If S is a multiplicative subset of A, then $S^{-1}A$ is a flat A-algebra (1.18). As tensor products commute with direct sums, and direct sums of exact sequences are exact, an A-algebra is flat if it is free as an A-module (and faithfully flat if it also nonzero).

PROPOSITION 9.14. *Let $A \to A'$ be a homomorphism of rings. If $A \to B$ is flat, then so also is $A' \to B \otimes_A A'$.*

PROOF. For any A'-module M,

$$(B \otimes_A A') \otimes_{A'} M \simeq B \otimes_A (A' \otimes_{A'} M) \simeq B \otimes_A M.$$

In other words, tensoring an A'-module M with $B \otimes_A A'$ is the same as tensoring M (regarded as an A-module) with B. Therefore it preserves exact sequences. □

PROPOSITION 9.15. *Let $\alpha\colon A \to B$ be a homomorphism of rings. If $\alpha\colon A \to B$ is flat, then $A_{\alpha^{-1}(\mathfrak{q})} \to B_{\mathfrak{q}}$ is flat for all prime ideals $\mathfrak{q}$ of B; conversely, $\alpha\colon A \to B$ is flat if $A_{\alpha^{-1}(\mathfrak{n})} \to B_{\mathfrak{n}}$ is flat for all maximal ideals $\mathfrak{n}$ of B*

PROOF. Let $\mathfrak{q}$ be a prime ideal of B, and let $\mathfrak{p} = \alpha^{-1}(\mathfrak{q})$ — it is a prime ideal in A. If $A \to B$ is flat, then $A_{\mathfrak{p}} \to A_{\mathfrak{p}} \otimes_A B \simeq S_{\mathfrak{p}}^{-1}B$ (9.14). The map $S_{\mathfrak{p}}^{-1}B \to S_{\mathfrak{q}}^{-1}B = B_{\mathfrak{q}}$ is flat (9.13a), and so the composite $A_{\mathfrak{p}} \to B_{\mathfrak{q}}$ is flat (9.13c).

For the converse, let $N' \to N$ be an injective homomorphism of A-modules, and let $\mathfrak{n}$ be a maximal ideal of B. Then $A_{\mathfrak{m}} \otimes_A (N' \to N)$ is injective (9.13). Therefore, the map

$$B_{\mathfrak{n}} \otimes_A (N' \to N) \simeq B_{\mathfrak{n}} \otimes_{A_{\mathfrak{m}}} (A_{\mathfrak{m}} \otimes_A (N' \to N))$$

is injective, and so the kernel M of $B \otimes_A (N' \to N)$ has the property that $M_{\mathfrak{n}} = 0$. Let $x \in M$, and let $\mathfrak{a} = \{b \in B \mid bx = 0\}$. For each maximal ideal $\mathfrak{n}$ of B, x maps to zero in $M_{\mathfrak{n}}$, and so $\mathfrak{a}$ contains an element not in $\mathfrak{n}$. Hence $\mathfrak{a} = B$, and so $x = 0$. □

PROPOSITION 9.16. *A flat homomorphism $\alpha\colon A \to B$ is faithfully flat if and only if every maximal ideal $\mathfrak{m}$ of A is of the form $\alpha^{-1}(\mathfrak{n})$ for some maximal ideal $\mathfrak{n}$ of B, i.e., if and only if the map*

$$\operatorname{spm}(\alpha)\colon\ \operatorname{spm}(B) \to \operatorname{spm}(A)$$

is surjective.

PROOF. $\Rightarrow$: Let $\mathfrak{m}$ be a maximal ideal of A, and let $M = A/\mathfrak{m}$; then

$$B \otimes_A M \simeq B/\alpha(\mathfrak{m})B.$$

As $B \otimes_A M \neq 0$, we see that $\alpha(\mathfrak{m})B \neq B$. Therefore $\alpha(\mathfrak{m})$ is contained in a maximal ideal $\mathfrak{n}$ of B. Now $\alpha^{-1}(\mathfrak{n})$ is a proper ideal in A containing $\mathfrak{m}$, and hence equals $\mathfrak{m}$.

$\Leftarrow$: Let M be a nonzero A-module. Let x be a nonzero element of M, and let $\mathfrak{a} = \operatorname{ann}(x) \stackrel{\text{def}}{=} \{a \in A \mid ax = 0\}$. Then $\mathfrak{a}$ is an ideal in A, and $M' \stackrel{\text{def}}{=} Ax \simeq A/\mathfrak{a}$. Moreover, $B \otimes_A M' \simeq B/\alpha(\mathfrak{a}) \cdot B$ and, because $A \to B$ is flat, $B \otimes_A M'$ is a submodule of $B \otimes_A M$. Because $\mathfrak{a}$ is proper, it is contained in a maximal ideal $\mathfrak{m}$ of A, and therefore

$$\alpha(\mathfrak{a}) \subset \alpha(\mathfrak{m}) \subset \mathfrak{n}$$

for some maximal ideal $\mathfrak{n}$ of A. Hence $\alpha(\mathfrak{a})\cdot B \subset \mathfrak{n} \neq B$, and so $B \otimes_A M \supset B \otimes_A M' \neq 0$. □

COROLLARY 9.17. *A flat local homomorphism $A \to B$ of local rings is faithfully flat.*

PROOF. Let $\mathfrak{m}$ and $\mathfrak{n}$ be the (unique) maximal ideals of A and B. By hypothesis, $\mathfrak{n}^c = \mathfrak{m}$, and so the statement follows from the proposition. □

Properties of flat homomorphisms of rings

LEMMA 9.18. *Let B be an A-algebra, and let $\mathfrak{p}$ be a prime ideal of A. The prime ideals of B contracting to $\mathfrak{p}$ are in natural one-to-one correspondence with the prime ideals of $B \otimes_A \kappa(\mathfrak{p})$.*

PROOF. Let $S = A \smallsetminus \mathfrak{p}$. Then $\kappa(\mathfrak{p}) \stackrel{\text{def}}{=} S^{-1}(A/\mathfrak{p})$. Therefore we obtain $B \otimes_A \kappa(\mathfrak{p})$ from B by first passing to $B/\mathfrak{p}B$ and then making the elements of A not in $\mathfrak{p}$ act invertibly. After the first step, we are left with the prime ideals $\mathfrak{q}$ of B such that $\mathfrak{q}^c \supset \mathfrak{p}$, and after the second step only with those such that $\mathfrak{q}^c \cap S = \emptyset$, i.e., such that $\mathfrak{q}^c = \mathfrak{p}$. □

PROPOSITION 9.19. *Let B be a faithfully flat A-algebra. Every prime ideal $\mathfrak{p}$ of A is of the form $\mathfrak{q}^c$ for some prime ideal $\mathfrak{q}$ of B.*

PROOF. The ring $B \otimes_A \kappa(\mathfrak{p})$ is not zero, because $\kappa(\mathfrak{p}) \neq 0$ and $A \to B$ is faithfully flat, and so it has a prime (even maximal) ideal $\mathfrak{q}$. For this ideal, $\mathfrak{q}^c = \mathfrak{p}$. □

SUMMARY 9.20. A flat homomorphism $\alpha\colon A \to B$ is faithfully flat if the image of

$$\operatorname{spec}(\alpha)\colon \operatorname{spec}(B) \to \operatorname{spec}(A)$$

includes all maximal ideals of A, in which case it includes all prime ideals of A.

THEOREM 9.21 (GOING-DOWN THEOREM FOR FLAT MAPS). *Let B be a flat A-algebra. Let $\mathfrak{p} \supset \mathfrak{p}'$ be prime ideals in A, and let $\mathfrak{q}$ be a prime ideal in B such that $\mathfrak{q}^c = \mathfrak{p}$. Then $\mathfrak{q}$ contains a prime ideal $\mathfrak{q}'$ such that $\mathfrak{q}'^c = \mathfrak{p}'$:*

$$\begin{array}{ccccc} B & & \mathfrak{q} & \supset & \mathfrak{q}' \\ \Big| & & \Big| & & \Big| \\ A & & \mathfrak{p} & \supset & \mathfrak{p}'. \end{array}$$

PROOF. Because $A \to B$ is flat, the homomorphism $A_{\mathfrak{p}} \to B_{\mathfrak{q}}$ is flat, and because $\mathfrak{p}A_{\mathfrak{p}} = (\mathfrak{q}B_{\mathfrak{q}})^c$, it is faithfully flat (9.16). The ideal $\mathfrak{p}'A_{\mathfrak{p}}$ is prime (1.14), and so there exists a prime ideal of $B_{\mathfrak{q}}$ lying over $\mathfrak{p}'A_{\mathfrak{p}}$ (by 9.19). The contraction of this ideal to B is contained in $\mathfrak{q}$ and contracts to $\mathfrak{p}'$ in A. □

For example, let $\alpha\colon A \to B$ be a flat local homomorphism of local rings. By definition, $\alpha^{-1}(\mathfrak{n}) = \mathfrak{m}$, where $\mathfrak{m}$ and $\mathfrak{n}$ are the maximal ideals of A and B. The theorem says that, for every prime ideal $\mathfrak{p}$ in A, there exists a prime ideal $\mathfrak{q}$ in B such that $\alpha^{-1}(\mathfrak{q}) = \mathfrak{p}$, i.e., the map

$$\operatorname{Spec} B \to \operatorname{Spec} A$$

is surjective.

Flat maps of algebraic varieties

DEFINITION 9.22. A regular map $\varphi\colon W \to V$ of algebraic varieties is ***flat*** if, for all $P \in W$, the local homomorphism $\mathcal{O}_{V,\varphi(P)} \to \mathcal{O}_{W,P}$ is flat, and it is ***faithfully flat*** if it is flat and surjective.

Open immersions are flat and composites of flat maps are flat.

PROPOSITION 9.23. *A regular map $\varphi\colon W \to V$ of affine algebraic varieties is flat (resp. faithfully flat) if and only if the map $f \mapsto f\circ\varphi\colon k[V] \to k[W]$ is flat (resp. faithfully flat).*

PROOF. Apply 9.15 and 9.16. □

THEOREM 9.24. *Let $\varphi\colon W \to V$ be a flat map of affine algebraic varieties. Let $S' \supset S$ be closed irreducible subsets of V, and let T be a closed irreducible subset of W such that $\varphi(T)$ is a dense subset of S. Then there exists a closed irreducible subset T' of W containing T and such that $\varphi(T')$ is a dense subset of S':*

$$\begin{array}{ccccc} W & \supset & T' & \supset & T \\ \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle\varphi} \\ V & \supset & S' & \supset & S. \end{array}$$

PROOF. In view of the correspondence between closed irreducible subsets and prime ideals (2.28), this is just a geometric restatement of Theorem 9.21. Let $\mathfrak{p} = I(S)$, $\mathfrak{p}' = I(S')$, and $\mathfrak{q} = I(T)$. Then $\mathfrak{p} \supset \mathfrak{p}'$ because $S \subset S'$. As $T \to S$ is dominant, the homomorphism

$$k[S] = k[V]/\mathfrak{p} \to k[T]/\mathfrak{q} = k[T]$$

is injective (2.40), and so $\mathfrak{q}^c = \mathfrak{p}$. According to Theorem 9.21, there exists a prime ideal $\mathfrak{q}'$ in $k[W]$ contained in $\mathfrak{q}$ and such that $\mathfrak{q}'^c = \mathfrak{p}'$. Now $T' \stackrel{\text{def}}{=} V(\mathfrak{q}')$ has the required properties. □

COROLLARY 9.25. *Let $\varphi\colon W \to V$ be a flat map of algebraic varieties. Let $w \in W$ and let $v = \varphi(w)$. For any closed irreducible subset S of V through v, there exists a closed irreducible subset T through w such that $\varphi(T) \subset S$ and the map $T \xrightarrow{\varphi} S$ is dominant.*

PROOF. When W and V are affine, this is a special case of the theorem. The general case can be proved by replacing W and V with suitable affine neighbourhoods of w and v. □

THEOREM 9.26 (GENERIC FLATNESS). *Let $\varphi\colon W \to V$ be a dominant map of irreducible algebraic varieties. There exist nonempty open subsets $U \subset V$ and $U' \subset W$ such that $\varphi(U') \subset U$ and $U' \xrightarrow{\varphi} U$ is faithfully flat.*

PROOF. In the proof we keep replacing W and V with smaller nonempty open subvarieties until they have the required property. First, we may replace W and V with open affines, so that φ is the map $\mathrm{Spm}(B) \to \mathrm{Spm}(A)$ defined by a homomorphism $A \hookrightarrow B$ of integral domains (finitely generated over k). Let F be the field of fractions of A, and regard B as a subring of $F \otimes_A B$.

As $F \otimes_A B$ is a finitely generated F-algebra, it contains elements $x_1, \ldots, x_m$ algebraically independent over F and such that $F \otimes_A B$ is a finite $F[x_1, \ldots, x_m]$-algebra (2.45). After multiplying each x_i by an element of A, we may suppose that it lies in B. Let $b_1, \ldots, b_n$ generate B as an A-algebra. Each b_i satisfies a monic polynomial equation with coefficients in $F[x_1, \ldots, x_m]$. If $a \in A$ is a common denominator for the coefficients of these polynomials, then each b_i is integral over $A_a[x_1, \ldots, x_m]$. As the b_i generate B_a as an A_a-algebra, this shows that B_a is a finite $A_a[x_1, \ldots, x_m]$-algebra (1.36). After replacing A with A_a and B with B_a, we may suppose that B is a finite $A[x_1, \ldots, x_m]$-algebra. We have constructed the left-hand part of the diagram,

$$\begin{array}{ccccc}
B & \xrightarrow{\text{injective}} & F \otimes_A B & \longrightarrow & E \otimes_{A[x_1,\ldots,x_m]} B \\
\uparrow{\scriptstyle\text{finite}} & & \uparrow{\scriptstyle\text{finite}} & & \uparrow{\scriptstyle\text{finite}} \\
A[x_1, \ldots, x_m] & \longrightarrow & F[x_1, \ldots, x_m] & \longrightarrow & E \stackrel{\text{def}}{=} F(x_1, \ldots, x_m) \\
\uparrow & & \uparrow & & \\
A & \longrightarrow & F. & &
\end{array}$$

and we now construct the rest. Let $E = F(x_1, \ldots, x_m)$ be the field of fractions of $F[x_1, \ldots, x_m]$. It is also the field of fractions of $A[x_1, \ldots, x_m]$. Let $e_1, \ldots, e_r$ be elements of B forming a basis for $E \otimes_{A[x_1,\ldots,x_m]} B$ as an E-vector space. Each element of B can be expressed as a linear combination of the e_i with coefficients in E. Let q be a common denominator for the coefficients arising from a set of generators for B as an $A[x_1, \dots, x_m]$-module. Then $e_1, \dots, e_r$ generate B_q as an $A[x_1, \dots, x_m]_q$-module. In other words, the map

$$(c_1, \dots, c_r) \mapsto \sum c_i e_i : A[x_1, \dots, x_m]_q^r \to B_q \qquad (*)$$

is surjective. This map becomes an isomorphism when tensored with E over $A[x_1, \dots, x_m]_q$. Thus its kernel M is an $A[x_1, \dots, x_m]_q$-submodule that becomes zero when tensored with the field of fractions of $A[x_1, \dots, x_m]_q$. As $A[x_1, \dots, x_m]_q$ is an integral domain, $M = 0$, and so (*) is an isomorphism. Let a be some nonzero coefficient of the polynomial q, and consider the homomorphisms

$$A_a \to A_a[x_1, \dots, x_m] \to A_a[x_1, \dots, x_m]_q \to B_{aq}.$$

The first and third arrows are faithfully flat because their targets are free modules over their sources, and the second arrow is flat because it is a localization (9.13). In sum, we have a flat map

$$D(aq) = \operatorname{Spm}(B_{aq}) \to \operatorname{Spm}(A_a) = D(a)$$

from an open subvariety of W to an open subvariety of V.

Let $\mathfrak{m}$ be a maximal ideal in A_a. Then $\mathfrak{m}A_a[x_1, \dots, x_m]$ does not contain the polynomial q because the coefficient a of q is invertible in A_a. Hence $\mathfrak{m}A_a[x_1, \dots, x_m]_q$ is a proper ideal of $A_a[x_1, \dots, x_m]_q$. Any maximal ideal of $A_a[x_1, \dots, x_m]_q$ containing it will intersect A_a in $\mathfrak{m}$, and so the map $A_a \to A_a[x_1, \dots, x_m]_q$ is faithfully flat by 9.16. Hence $A_a \to B_{aq}$ is faithfully flat, which completes the proof. □

THEOREM 9.27. *Every flat map $\varphi : W \to V$ of algebraic varieties is open.*

PROOF. It suffices to show that $\varphi(W)$ is open. Let $W = V \smallsetminus \varphi(V)$, and let $Z_1, \dots, Z_n$ be the irreducible components of the closure $\overline{W}$ of W. It suffices to show that W contains every Z_i. Suppose not, and let $v \in Z_j \cap \varphi(W)$. Then $v = \varphi(w)$ for some $w \in W$, and according to 9.25 there exists a closed irreducible subset S of W through w such that the map $S \to Z_j$ is dominant. This means that there exists an open subset U of V such that $\varphi(W) \supset U \cap Z_j \neq \emptyset$.

Let $U' = V \smallsetminus \bigcup_{i \neq j} Z_i$. As $V = \bigcup_i Z_i \cup \varphi(W)$, we have $U' \subset Z_j \cup \varphi(W)$, and so

$$\varphi(W) \supset U \cap U'.$$

Note that U and U' are both open subsets of V meeting Z_j. As Z_j is irreducible, $U \cap Z_j$ and $U' \cap Z_j$ are both dense open subsets of Z_j. Hence $U \cap U' \cap Z_j$ is nonempty. As its elements are not in the closure of W, this contradicts the definition of Z_j. We have shown that all Z_i are contained in W, as required. □

COROLLARY 9.28. *Let $\varphi : W \to V$ be a dominant map of irreducible algebraic varieties. There exists a dense open subset U of W such that $\varphi(U)$ is open, $U = \varphi^{-1}(\varphi U)$, and $U \xrightarrow{\varphi} \varphi(U)$ is flat.*

PROOF. According to 9.26, there exists a dense open subset U of V such that $\varphi^{-1}(U) \xrightarrow{\varphi} U$ is flat. In particular, $\varphi(\varphi^{-1}(U))$ is open in V (9.27). Note that $\varphi^{-1}(\varphi(\varphi^{-1}(U)) = \varphi^{-1}(U)$. Let $U' = \varphi^{-1}(U)$. Then U' is a dense open subset of W, $\varphi(U')$ is open, $U' = \varphi^{-1}(\varphi U')$, and $U' \xrightarrow{\varphi} \varphi(U')$ is flat. □

Fibres and flatness

The notion of flatness allows us to sharpen our earlier results.

PROPOSITION 9.29. *Let $\varphi: W \to V$ be a dominant map of irreducible algebraic varieties, and let $P \in \varphi(W)$. Then*

$$\dim\left(\varphi^{-1}(P)\right) \geq \dim(W) - \dim(V) \tag{38}$$

with equality if φ is flat.

PROOF. The inequality was proved in 9.9. Assume that φ is flat, and let Z be an irreducible component of $\varphi^{-1}(P)$.

After replacing V with an open neighbourhood of P and W with an open subset intersecting Z, we may suppose that both V and W are affine. Let

$$V \supset V_1 \supset \cdots \supset V_m = \{P\}$$

be a maximal chain of distinct irreducible closed subsets of V (so $m = \dim(V)$ by 3.44). Now $\varphi(Z) = \{P\}$, and so, by Theorem 9.24, there exists a chain of irreducible closed subsets

$$W \supset W_1 \supset \cdots \supset W_m = Z$$

such that $\varphi(W_i)$ is a dense subset of V_i. Let

$$Z \supset Z_1 \supset \cdots \supset Z_n$$

be a maximal chain of distinct irreducible closed subsets of V (so $n = \dim(Z)$). The existence of the chain

$$W \supset W_1 \supset \cdots \supset W_m \supset Z_1 \supset \cdots \supset Z_n$$

shows that

$$\dim(W) \geq m + n = \dim(V) + \dim(Z).$$

Together with the inequality (38), this gives the equality. □

PROPOSITION 9.30. *Let $\varphi: W \to V$ be a dominant map of irreducible algebraic varieties. There exists a dense open subset U of W such that $\varphi(U)$ is open in V, $U = \varphi^{-1}(\varphi(U))$, and*

$$\dim\left(\varphi^{-1}(P)\right) = \dim(W) - \dim(V).$$

for all $P \in \varphi(U)$.

PROOF. According to Proposition 9.29, the open subset U of W in 9.28 has these properties. □

PROPOSITION 9.31. *Let $\varphi: W \to V$ be a dominant map of irreducible varieties. Let S be a closed irreducible subset of V, and let T be an irreducible component of $\varphi^{-1}(S)$ such that $\varphi(T)$ is dense in S. Then*

$$\dim(T) \geq \dim(S) + \dim(W) - \dim(V)$$

with equality if φ is flat.

In other words,

$$\operatorname{codim}(S) \geq \operatorname{codim}(T),$$

with equality if φ is flat.

PROOF. When S is a point, this becomes 9.9(b) and 9.29. As we now explain, the general case can be proved by an easy modification of the proofs of those statements.

In proving the inequality, we may replace V with any open subvariety intersecting S. In particular, we can assume V to be affine. Let $m = \operatorname{codim}(S)$. From Proposition 3.47 we know that there exist regular functions $f_1, \ldots, f_m$ such that S is an irreducible component of $V(f_1, \ldots, f_m)$. After replacing V by a smaller open subset, we may suppose that $S = V(f_1, \ldots, f_m)$. Then $\varphi^{-1}(S)$ is the zero set of the regular functions $f_1 \circ \varphi, \ldots, f_m \circ \varphi$, and every irreducible component has codimension $\leq m$ in W by 3.45.

When φ is flat, we shall prove (more precisely) that, if Z is an irreducible component of $\varphi^{-1}(S)$, then

$$\dim(Z) = \dim(S) + \dim(W) - \dim(V).$$

After replacing V (resp. W) with an open subvariety that intersects S (resp. Z), we may suppose that both V and W are affine. Let

$$V \supset V_1 \supset \cdots \supset V_m = \{S\}$$

be a maximal chain of distinct irreducible closed subsets (so $m = \operatorname{codim}(S)$ by 3.44). Now $\varphi(Z)$ is a dense subset of S, and so (see 9.24) there exists a chain of irreducible closed subsets

$$W \supset W_1 \supset \cdots \supset W_m = Z$$

such that $\varphi(W_i)$ is a dense subset of V_i. Let

$$Z \supset Z_1 \supset \cdots \supset Z_n$$

be a maximal chain of distinct irreducible closed subsets of V (so $n = \dim(Z)$). The existence of the chain

$$W \supset W_1 \supset \cdots \supset W_m \supset Z_1 \supset \cdots \supset Z_n$$

shows that

$$\dim(W) \geq m + n = \dim(V) - \dim S + \dim(Z),$$

i.e.,

$$\operatorname{codim}(Z) \geq \operatorname{codim}(S).$$

Together with the previous inequality, this implies that $\operatorname{codim}(Z) = \operatorname{codim}(S)$. □

PROPOSITION 9.32. *Let $\varphi\colon W \to V$ be a dominant map of irreducible algebraic varieties. There exists a dense open subset U of W such that $\varphi(U)$ is open in V, $U = \varphi^{-1}(\varphi U)$, and*

$$\dim(T) = \dim(S) + \dim(W) - \dim(V)$$

for all closed irreducible subsets S of V intersecting $\varphi(U)$ and all irreducible components T of $\varphi^{-1}(S)$ intersecting U.

PROOF. According to Proposition 9.31, the open subset U in 9.28 has these properties. □

FINITE MAPS

PROPOSITION 9.33. *Let V be an irreducible algebraic variety. A finite map $\varphi : W \to V$ is flat if and only if*

$$\sum_{Q \mapsto P} \dim_k \mathcal{O}_Q/\mathfrak{m}_P\mathcal{O}_Q$$

is independent of $P \in V$.

PROOF. It suffices to prove this with V affine, in which case it follows from CA, 12.6 (equivalence of (d) and (e)). □

The integer $\dim_k \mathcal{O}_Q/\mathfrak{m}_P\mathcal{O}_Q$ is the ***multiplicity*** of Q in its fibre. The theorem says that a finite map is flat if and only if the number of points in each fibre (counting multiplicities) is constant.

For example, let V be the subvariety of $\mathbb{A}^{n+1}$ defined by an equation

$$X^m + a_1X^{m-1} + \cdots + a_m = 0, \quad a_i \in k[T_1, \ldots, T_n]$$

and let $\varphi : V \to \mathbb{A}^n$ be the projection map (see p. 50). The fibre over a point P of $\mathbb{A}^n$ is the set of points (P, c) with c a root of the polynomial

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

The multiplicity of (P, c) in its fibre is the multiplicity of c as a root of the polynomial. Therefore $\sum_{Q \mapsto P} \dim_k \mathcal{O}_Q/\mathfrak{m}_P\mathcal{O}_Q = m$ for every P, and so the map φ is flat.

Criteria for flatness

Let A be a local noetherian ring with maximal ideal $\mathfrak{m}$. A sequence of elements $a_1, \ldots, a_n$ of A is ***regular*** if a_1 is a nonzerodivisor in A, a_2 is a nonzerodivisor in $A/(a_1)$, etc., and $A/(a_1, \ldots, a_n) \neq 0$. According to a theorem of Rees, all maximal regular sequences $a_1, \ldots, a_n$, $a_i \in \mathfrak{m}$, in A have the same length, called the ***depth*** of A. According to the Auslander–Buchsbaum formula, $\operatorname{depth}(A) \leq \dim(A)$. When the two are equal, the ring is said to be ***Cohen–Macaulay***. More generally, a noetherian ring A is said to be ***Cohen–Macaulay*** if it is zero or $A_\mathfrak{m}$ is Cohen–Macaulay for all maximal ideals $\mathfrak{m}$ of A.

THEOREM 9.34. *Let $\varphi : A \to B$ be a local homomorphism of noetherian local rings, and let $\mathfrak{m}$ be the maximal ideal of A. If A is regular, B is Cohen–Macaulay, and*

$$\dim(B) = \dim(A) + \dim(B/\mathfrak{m}B),$$

then φ is flat.

PROOF. See Matsumura 1989, 23.1. □

9.35. There are the following examples.

(a) Zero-dimensional and reduced one-dimensional noetherian rings are Cohen–Macaulay (ibid. p. 139).

(b) Regular noetherian rings are Cohen–Macaulay (ibid. p. 137).

(c) Let $\varphi : A \to B$ be a flat local homomorphism of noetherian local rings, and let $\mathfrak{m}$ be the maximal ideal of A. Then B is Cohen–Macaulay if and only if both A and $B/\mathfrak{m}B$ are Cohen–Macaulay (ibid. p. 181).

PROPOSITION 9.36. *Let $\varphi: A \to B$ be a finite homomorphism of noetherian rings with A regular. Then φ is flat if and only if B is Cohen–Macaulay.*

PROOF. Note that $B/\mathfrak{m}B$ is zero-dimensional,[1] hence Cohen–Macaulay, for every maximal ideal $\mathfrak{m}$ of A (9.35a), and that $\mathrm{ht}(\mathfrak{n}) = \mathrm{ht}(\mathfrak{n}^c)$ for every maximal ideal $\mathfrak{n}$ of B. If φ is flat, then B is Cohen–Macaulay by (9.35c). Conversely, if B is Cohen–Macaulay, then φ is flat by (9.34). □

EXAMPLE 9.37. Let A be a finite $k[X_1, \ldots, X_n]$-algebra (cf. 2.45). The map $k[X_1, \ldots, X_n] \to A$ is flat if and only if A is Cohen–Macaulay.

An algebraic variety V is said to be ***Cohen–Macaulay*** if $\mathcal{O}_{V,P}$ is Cohen–Macaulay for all $P \in V$. An affine algebraic variety V is Cohen–Macaulay if and only if $k[V]$ is Cohen–Macaulay (9.35c). A nonsingular variety is Cohen–Macaulay (9.35b).

THEOREM 9.38. *Let V and W be algebraic varieties with V nonsingular and W Cohen–Macaulay. A regular map $\varphi: W \to V$ is flat if and only if*

$$\dim \varphi^{-1}(P) = \dim W - \dim V \tag{39}$$

for all $P \in V$.

PROOF. Immediate consequence of (9.34). □

ASIDE 9.39. The theorem fails with "nonsingular" weakened to "normal". Let $G \stackrel{\text{def}}{=} \mathbb{Z}/2\mathbb{Z}$ act on $W \stackrel{\text{def}}{=} \mathbb{A}^2$ by $(x,y) \mapsto (-x,-y)$, and let $V \subset \mathbb{A}^3$ be the quadric cone defined by $TV = U^2$. The map

$$\varphi: W \to V, \quad (x,y) \mapsto (t,u,v) = (x^2, xy, y^2),$$

has as fibres the orbits for the action (it is the "quotient map" for the action). The variety W is nonsingular, and V is normal because $k[V] = k[X,Y]^G$. Moreover φ is finite, and so its fibres have constant dimension 0, but it is not flat because

$$\sum_{Q \mapsto P} \dim_k \mathcal{O}_Q/\mathfrak{m}_P\mathcal{O}_Q = \begin{cases} 3 & \text{if } P = (0,0,0) \\ 2 & \text{otherwise} \end{cases}$$

contradicting Proposition 9.33. See mo117043.

d. Lines on surfaces

Every algebraic geometer knows the traditional proof that there exists at least one line on a nonsingular cubic surface in $\mathbb{P}^3$

Miles Reid.

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

[1] Note that $C \stackrel{\text{def}}{=} B/\mathfrak{m}B = B \otimes_A A/\mathfrak{m}$ is a finite k-algebra. Therefore it has only finitely many maximal ideals. Every prime ideal in C is an intersection of maximal ideals (2.18), but a prime ideal can equal a finite intersection of ideals only if it equals one of the ideals.

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

$$p(L) = (p_{01} : p_{02} : p_{03} : p_{12} : p_{13} : p_{23}) \in \mathbb{P}^5, \quad p_{ij} \overset{\text{def}}{=} \begin{vmatrix} x_i & x_j \\ y_i & y_j \end{vmatrix},$$

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 9.40. *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 9.41. *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 9.42. *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

$$(-p_{01}p_{03} : -p_{02}p_{03} : -p_{03}^2 : \underbrace{p_{01}p_{23} - p_{02}p_{13}}_{-p_{03}p_{12}} : -p_{03}p_{13} : -p_{03}p_{23})$$
$$= (p_{01} : p_{02} : p_{03} : p_{12} : p_{13} : p_{23}).$$

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,

$$F(X_0, X_1, X_2, X_3) = \sum_{i_0+i_1+i_2+i_3=m} a_{i_0 i_1 i_2 i_3} X_0^{i_0} \dots X_3^{i_3}.$$

LEMMA 9.43. *The set of homogeneous polynomials of degree m in 4 variables is a vector space of dimension $\binom{3+m}{m}$*

PROOF. See the 6.39. □

Let $\nu = \binom{3+m}{m} - 1 = \dfrac{(m+1)(m+2)(m+3)}{6} - 1$, and regard $\mathbb{P}^\nu$ as the projective space attached to the vector space of homogeneous polynomials of degree m in 4 variables (p. 147). Then we have a surjective map

$$\mathbb{P}^\nu \to \{\text{surfaces of degree } m \text{ in } \mathbb{P}^3\},$$

$$(\dots : a_{i_0 i_1 i_2 i_3} : \dots) \mapsto V(F), \qquad F = \sum a_{i_0 i_1 i_2 i_3} X_0^{i_0} X_1^{i_1} X_2^{i_2} X_3^{i_3}.$$

The map is not quite injective — for example, X^2Y and XY^2 define the same surface — but nevertheless, we can (somewhat loosely) think of the points of $\mathbb{P}^\nu$ as being (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 9.44. *The set Γ_m is an irreducible closed subset of $\Pi \times \mathbb{P}^\nu$; it is therefore a projective variety. The dimension of Γ_m is* $\dfrac{m(m+1)(m+5)}{6} + 3$.

EXAMPLE 9.45. 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 9.40 we see that L lies on the surface $F(X_0, X_1, X_2, X_3) = 0$ if and only if

$$F(\sum b_j p_{0j} : \sum b_j p_{1j} : \sum b_j p_{2j} : \sum b_j p_{3j}) = 0, \text{ all } (b_0, \ldots, b_3) \in k^4.$$

Expand this out as a polynomial in the b_j with coefficients polynomials in the $a_{i_0 i_1 i_2 i_3}$ and p_{ij}. Then $F(\ldots) = 0$ 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 6.51).

It remains to compute the dimension of Γ_m. We shall apply Proposition 9.11 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 9.11 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 9.46. Let $m = 1$. Then $\nu = 3$ and $\dim \Gamma_1 = 5$. The projection $\psi : \Gamma_1 \to \mathbb{P}^3$ is surjective (every plane contains at least one line), and 9.9 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 9.47. *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 6.26)

$$(a_0 : a_1), (b_0 : b_1) \mapsto (a_0b_0 : a_0b_1 : a_1b_0 : a_1b_1) : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3.$$

There are two obvious families of lines on $\mathbb{P}^1 \times \mathbb{P}^1$, namely, the horizontal family and the vertical family; each is parametrized by $\mathbb{P}^1$, and so is called a ***pencil of lines***. They map to two families of lines on the quadric:

$$\begin{cases} t_0X = t_1Z \\ t_0Y = t_1W \end{cases} \text{and} \begin{cases} t_0X = t_1Y \\ t_0Z = t_1W. \end{cases}$$

Since a degenerate quadric is a surface or a union of two surfaces, we see that every quadric surface contains a line, that is, that $\psi : \Gamma_2 \to \mathbb{P}^9$ is surjective. Thus (9.9) 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:

$$\begin{array}{lcl} \Gamma_2 - \psi^{-1}(S) & = & \text{pairs } (F, L) \text{ with } L \text{ on } F; \\ \quad\downarrow & & \\ \quad R & = & \text{set of reguli;} \\ \quad\downarrow & & \\ \mathbb{P}^9 - S & = & \text{set of nondegenerate quadrics.} \end{array}$$

The fibres of the top map are connected, and of dimension 1 (they are all isomorphic to $\mathbb{P}^1$), and the second map is finite and two-to-one. Factorizations of this type occur quite generally (see the Stein factorization theorem, 8.64).

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 9.48. *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 9.49. (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, $0 \leq i, j \leq 2$:

$$\begin{cases} X_0 + \zeta^i X_1 = 0 \\ X_2 + \zeta^j X_3 = 0 \end{cases} \qquad \begin{cases} X_0 + \zeta^i X_2 = 0 \\ X_1 + \zeta^j X_3 = 0 \end{cases} \qquad \begin{cases} X_0 + \zeta^i X_3 = 0 \\ X_1 + \zeta^j X_2 = 0. \end{cases}$$

There are three sets, each with nine lines, for a total of 27 lines.

(b) Consider the surface

$$X_1 X_2 X_3 = X_0^3.$$

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 $X_1 X_2 X_3 = 1$. A line in $\mathbb{A}^3$ can be written in parametric form $X_i = a_i t + b_i$, 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 $X_1 X_2 X_3 = 0$ (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:

$$\begin{cases} t_0 X_1 = t_1 X_0 \\ t_0 X_2 = -t_1 X_0. \end{cases}$$

(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 9.48. If $\psi : \Gamma_3 \to \mathbb{P}^{19}$ 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 9.9), which contradicts two of the above examples. Therefore the map is surjective, 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. In fact, U' can be taken to be the set of nonsingular cubics. According to 8.26, the restriction of ψ to $\psi^{-1}(U)$ is finite, and so we can apply 8.40 to see that all cubics in $U - U'$ have fewer than 27 lines.

REMARK 9.50. 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 intersect 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 $\mathbb{P}^2$.

e. Bertini's theorem

Let $X \subset \mathbb{P}^n$ be a nonsingular projective variety. The hyperplanes H in $\mathbb{P}^n$ form a projective space $\mathbb{P}^{n\vee}$ (the "dual" projective space). The hyperplanes H not containing X and such that $X \cap H$ is nonsingular, form an open subset of $\mathbb{P}^{n\vee}$. If $\dim(X) \geq 2$, then the intersections $X \cap H$ are connected. For a proof of a weak version of the theorem, see 11.45 (Chapter 11).

f. Birational classification

Recall that two varieties V and W are birationally equivalent if $k(V) \approx k(W)$. This means that the varieties themselves become isomorphic once a proper closed subset has been removed from each (3.36).

The main problem of birational algebraic geometry is to classify algebraic varieties up to birational equivalence by finding a particularly good representative in each equivalence class.

For curves this is easy: in each birational equivalence class there is exactly one nonsingular projective curve (up to isomorphism). More precisely, the functor $V \rightsquigarrow k(V)$ is a contravariant equivalence from the category of nonsingular projective algebraic curves over k and dominant maps to the category of fields finitely generated and of transcendence degree 1 over k.

For surfaces, the problem is already much more difficult because many surfaces, even projective and nonsingular, will have the same function field. For example, every blow-up of a point on a surface produces a birationally equivalent surface.

A nonsingular projective surface is said to be ***minimal*** if it cannot be obtained from another such surface by blowing up. The main theorem for surfaces (Enriques 1914, Kodaira 1966) says that a birational equivalence class contains either

(a) a unique minimal surface, or

(b) a surface of the form $C \times \mathbb{P}^1$ for a unique nonsingular projective curve C.

In higher dimensions, the problem becomes very involved, although much progress has been made — see Wikipedia: MINIMAL MODEL PROGRAM. For a beautiful article on the minimal model program, see Notices AMS, Jan. 2024.

Exercises

9-1. Let G be a connected group variety, 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 open in its closure $\bar{O}$, and that $\bar{O} \smallsetminus O$ is a union of orbits of strictly lower dimension. Deduce that each orbit is a nonsingular subvariety of V, and that there exists at least one closed orbit.

9-2. 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 group variety 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.]

9-3. Find $3d^2$ lines on the Fermat projective surface

$$X_0^d + X_1^d + X_2^d + X_3^d = 0, \quad d \geq 3, \quad (p, d) = 1, \quad p \text{ the characteristic.}$$

9-4. (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 a group variety 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.

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 $k[V] \to k[T]$. [Hence $t \mapsto (t, \ldots, t^n)$ is an isomorphism of affine varieties $\mathbb{A}^1 \to V$.]

2-4 On tensoring the exact sequence of $\mathbb{Q}$-vector spaces

$$0 \to (f_1, \ldots, f_m) \to \mathbb{Q}[X_1, \ldots, X_n] \to \mathbb{Q}[X_1, \ldots, X_n]/(f_1, \ldots, f_m) \to 0$$

with $\mathbb{C}$, we get an exact sequence of $\mathbb{C}$-vector spaces

$$0 \to (f_1, \ldots, f_m) \to \mathbb{C}[X_1, \ldots, X_n] \to \mathbb{C}[X_1, \ldots, X_n]/(f_1, \ldots, f_m) \to 0.$$

As the f_i have no common zero in $\mathbb{C}$, the right-most term of the second sequence is zero, which implies that the same is true of the first sequence.

2-6 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.[2] 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 $\mathbb{Q}[X_1, \ldots]$ does not contain 1, and so the Nullstellensatz (2.11) implies that the polynomials have a common zero in k.

[2] Choose bases for A and B as $\mathbb{Q}$-vector spaces. Now a linear map from A to B is given by a matrix M. The condition on the coefficients of the matix for the map to be a homomorphism of algebras is polynomial.

2-7 Regard $\mathrm{Hom}_A(M,N)$ as an affine space over k; the elements not isomorphisms are the zeros of a polynomial; because M and N become isomorphic over k^{al}, the polynomial is not identically zero; therefore it has a nonzero in k (Exercise 1-1).

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.

3-3 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. See the introduction to Chapter 9.

3-4 Let i be an element of k with square -1. The map $(x,y) \mapsto (x+iy, x-iy)$ from the circle to the hyperbola has inverse $(x,y) \mapsto ((x+y)/2, (x-y)/2i)$. The k-algebra $k[X,Y]/(XY-1) \simeq k[X,X^{-1}]$, which is not isomorphic to $k[X]$ (too many units).

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 (b) The singular points are the common solutions to

$$\begin{cases} 4X^3 - 2XY^2 = 0 & \Rightarrow \quad X = 0 \text{ or } Y^2 = 2X^2 \\ 4Y^3 - 2X^2Y = 0 & \Rightarrow \quad Y = 0 \text{ or } X^2 = 2Y^2 \\ X^4 + Y^4 - X^2Y^2 = 0. \end{cases}$$

Thus, only $(0,0)$ is singular, and the variety is its own tangent cone.

4-2 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 cannot 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 need not 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.

4-4 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 $T_{\mathbf{a}}(V) \times T_{\mathbf{b}}(W)$.

4-5 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...)

4-6 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

$$\frac{n(n+1)}{2}\text{ (for }N)+\frac{n(n+1)}{2}\text{ (for }P)+n^2\text{ (for }M,Q)=2n^2+n.$$

4-7 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.

4-8 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.]

4-9 No! Let $\mathfrak{a}=(X^2Y)$. Then $V(\mathfrak{a})$ is the union of the X and Y axes, and $IV(\mathfrak{a})=(XY)$. For $\mathbf{a}=(a,b)$,

$$\begin{aligned}(dX^2Y)_{\mathbf{a}}&=2ab(X-a)+a^2(Y-b)\\(dXY)_{\mathbf{a}}&=b(X-a)+a(Y-b).\end{aligned}$$

If $a\neq 0$ and $b=0$, then the equations

$$\begin{aligned}(dX^2Y)_{\mathbf{a}}&=a^2Y=0\\(dXY)_{\mathbf{a}}&=aY=0\end{aligned}$$

have the same solutions.

5-1 Let f be regular on $\mathbb{P}^1$. Then $f|U_0=P(X)\in k[X]$, where X is the regular function $(a_0:a_1)\mapsto a_1/a_0\colon U_0\to k$, and $f|U_1=Q(Y)\in k[Y]$, where Y is $(a_0:a_1)\mapsto a_0/a_1$. 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.

5-2 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 $\operatorname{Specm}(\prod A_i)$, where $A_i=\Gamma(V_i,\mathcal{O}_{V_i})$, and so $V=\bigsqcup\operatorname{Specm}(A_i)$ (use the description of the ideals in $A\times B$ on in Section 1a). Etc..

5-5 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.

5-8 The diagonal in $V \times V$ is closed for the Zariski topology. Therefore, if the Zariski topology on $V \times V$ equals the product topology, then V is Hausdorff for the Zariski topology, hence has dimension 0.

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,

$$F(a,b,c) = 0 \Rightarrow \left(\frac{\partial F}{\partial X}\right)_P a + \left(\frac{\partial F}{\partial Y}\right)_P + \left(\frac{\partial F}{\partial Z}\right)_P c = 0.$$

(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 ∞ intersects 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 (6.37) 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 cannot be a proper closed subset of U; we cannot have $U \cap C = U$ because any curve containing all nonzero points on X-axis also contains the origin).

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 $\mathbf{a} = (a_0, \dots, a_m) \in k^{m+1}$ and $\mathbf{b} = (b_0, \dots, b_n) \in k^{n+1}$. 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 $C = 0$.

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 (7.35) implies that φ is identically zero.

8-2 For example, consider

$$(\mathbb{A}^1 \smallsetminus \{1\}) \to \mathbb{A}^1 \overset{x \mapsto x^n}{\to} \mathbb{A}^1$$

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

$$X \mapsto X^n : k[X] \to k[X, (X-1)^{-1}]$$

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 $f, g : Z \rightrightarrows W$. 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 $\varphi : W \to V$ 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 $(t_1, \dots, t_n) \in \mathbb{A}^n$ 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

$$T_i = T_j = T_k, \quad 1 \le i, j, k \le n, \quad i, j, k \text{ distinct},$$

and so on.

9-1 Consider an orbit $O = Gv$. The map $g \mapsto gv : G \to O$ is regular, and so O contains an open subset U of $\bar{O}$ (9.7). If $u \in U$, then $gu \in gU$, and gU is also a subset of O which is open in $\bar{O}$ (because $P \mapsto gP : V \to V$ 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 (4.37), 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 $O = \bar{O}$.

9-2 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.

9-3 Let ζ be a primitive dth root of 1. Then, for each i, j, $1 \le i, j \le d$, 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.

9-4 (a) Compare the proof of Theorem 9.9.

(b) Use the transitivity, and apply Proposition 8.26.

Hartshorne 1977

Bibliography

BOURBAKI, N. TG. Topologie Générale. Éléments de mathématique. Hermann, Paris. Chap. I, II, Hermann 1965 (4th edition); Chap. III, IV, Hermann 1960 (3rd edition) (English translation available from Springer).

CARTAN, H. 1963. Elementary theory of analytic functions of one or several complex variables. Éditions Scientifiques Hermann, Paris; Addison-Wesley Publishing Co., Inc., Reading, Mass.-Palo Alto, Calif.-London.

COX, D. A., LITTLE, J., AND O'SHEA, D. 2015. Ideals, varieties, and algorithms. Undergraduate Texts in Mathematics. Springer, Cham, fourth edition. An introduction to computational algebraic geometry and commutative algebra.

DEMAZURE, M. AND GABRIEL, P. 1970. Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs. Masson & Cie, Éditeurs, Paris; North-Holland Publishing Co., Amsterdam.

HARTSHORNE, R. 1977. Algebraic geometry. Springer-Verlag, New York-Heidelberg.

MATSUMURA, H. 1989. Commutative ring theory, volume 8 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, first paperback edition. Translated from the Japanese by M. Reid.

MILNE, J. S. 1980. Étale cohomology, volume No. 33 of *Princeton Mathematical Series*. Princeton University Press, Princeton, NJ.

MUMFORD, D. 1966a. Introduction to algebraic geometry. Mimeographed notes based on a 1965–66 course at Harvard University. Reprinted (with the introduction of misprints) by Springer 1999.

MUMFORD, D. 1966b. Lectures on curves on an algebraic surface, volume No. 59 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ. With a section by G. M. Bergman.

SAMUEL, P. 1966. Lectures on old and new results on algebraic curves, volume No. 36 of *Tata Institute of Fundamental Research Lectures on Mathematics*. Tata Institute of Fundamental Research, Bombay. Notes by S. Anantharaman.

SHAFAREVICH, I. R. 1994. Basic algebraic geometry. 1, 2. Springer-Verlag, Berlin.

WALKER, R. J. 1950. Algebraic Curves, volume vol. 13 of *Princeton Mathematical Series*. Princeton University Press, Princeton, NJ. Reprinted by Dover 1962.

WEIL, A. 1946. Foundations of Algebraic Geometry, volume Vol. 29 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, New York.

Index