X. Methods of Algebraic Geometry, 558-648

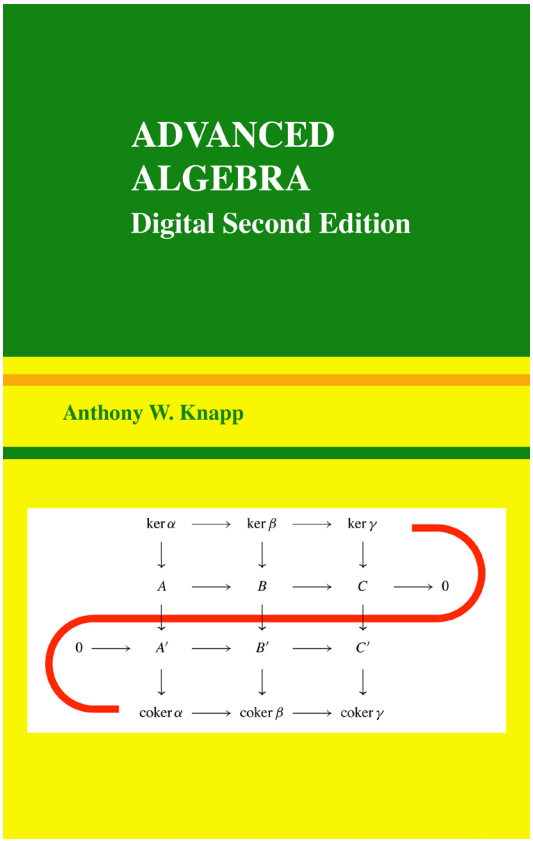
DOI: 10.3792/euclid/9781429799928-10

from

Advanced Algebra
Digital Second Edition

Anthony W. Knapp

Full Book DOI: 10.3792/euclid/9781429799928
ISBN: 978-1-4297-9992-8



Anthony W. Knapp
81 Upper Sheep Pasture Road
East Setauket, N.Y. 11733–1729, U.S.A.
Email to: aknapp@math.stonybrook.edu
Homepage: www.math.stonybrook.edu/~aknapp

Title: Advanced Algebra
Cover: Content of the Snake Lemma; see page 185.

Mathematics Subject Classification (2010): 11–01, 13–01, 14–01, 16–01, 18G99, 55U99, 11R04, 11S15, 12F99, 14A05, 14H05, 12Y05, 14A10, 14Q99.

First Edition, ISBN-13 978-0-8176-4522-9

Published by Birkhäuser Boston

Digital Second Edition, not to be sold, no ISBN

Published by the Author

CHAPTER X

Methods of Algebraic Geometry

Abstract. This chapter investigates the objects and mappings of algebraic geometry from a geometric point of view, making use especially of the algebraic tools of Chapter VII and of Sections 7–10 of Chapter VIII. In Sections 1–12, $\Bbbk$ denotes a fixed algebraically closed field.

Sections 1–6 establish the definitions and elementary properties of varieties, maps between varieties, and dimension, all over $\Bbbk$. Sections 1–3 concern varieties and dimension. Affine algebraic sets, affine varieties, and the Zariski topology on affine space are introduced in Section 1, and projective algebraic sets and projective varieties are introduced in Section 3. Section 2 defines the geometric dimension of an affine algebraic set, relating the notion to Krull dimension and transcendence degree. The actual context of Section 2 is a Noetherian topological space, the Zariski topology on affine space being an example. In such a space every closed subset is the finite union of irreducible closed subsets, and the union can be written in a certain way that makes the decomposition unique. Every nonempty closed set has a meaningful geometric dimension. In affine space the irreducible closed sets are the varieties, and each variety acquires a geometric dimension. The discussion in Section 2 applies in the context of projective space as well, and thus each projective variety acquires a geometric dimension. Moreover, any nonempty open subset of a Noetherian space is Noetherian. A nonempty open subset of an affine variety is called quasi-affine, and a nonempty open subset of a projective variety is called quasiprojective. Each quasi-affine variety or quasiprojective variety has a dimension equal to that of its closure, which is a variety.

Sections 4–6 take up maps between varieties. Section 4 introduces spaces of scalar-valued functions on quasiprojective varieties—rational functions, functions regular at a point, and functions regular on an open set. The section goes on to relate these notions for the different kinds of varieties. Section 5 introduces morphisms, which are a restricted kind of function between varieties. The tools of Sections 4–5 together show that for many purposes all the different kinds of varieties can be treated as quasiprojective varieties. Section 6 introduces rational maps between varieties; these are not everywhere-defined functions, but each can be restricted to an open dense subset on which it is a morphism. Rational maps with dense image correspond to field mappings of the fields of rational functions, with the order of the mappings reversed.

Section 7 concerns singularities at points of varieties, still over the field $\Bbbk$. Zariski's Theorem was stated in Chapter VII for affine varieties and partly proved at that time. In the current context it has a meaning for any point of any quasiprojective variety. The section proves the full theorem, which characterizes singular points in a way that shows they remain singular under isomorphisms of varieties.

Section 8 concerns classification questions over $\Bbbk$ for irreducible curves, i.e., quasiprojective varieties of dimension 1. From Section 6 it is known that two irreducible curves are equivalent under rational maps if and only if their fields of rational functions are isomorphic. The main theorem of Section 8 is that each such equivalence class of irreducible curves contains an everywhere nonsingular projective curve, and this curve is unique up to isomorphism of varieties. The points of this curve are parametrized by those discrete valuations of the underlying function field that are defined over $\Bbbk$.

Sections 9–12 relate the general theory of Sections 1–6 to the topic of solutions of simultaneous solutions of polynomial equations, as treated at length in Chapter VIII. Section 9 treats monomial ideals in $\Bbbk[X_1, \ldots, X_n]$, identifying their zero loci concretely and computing their dimension. The section goes on to introduce the affine Hilbert function of this ideal, which measures the proportion of polynomials of degree $\leq s$ not in the ideal. In the way that this function is defined, it is a polynomial for large s called the affine Hilbert polynomial of the ideal. Its degree equals the dimension of the zero locus of the ideal. Section 10 extends this theory from monomial ideals to all ideals, again concretely computing the dimension of the zero loci, obtaining an affine Hilbert polynomial, and showing that its degree equals the dimension of the zero locus of the ideal. Section 11 adapts the theory to homogeneous ideals and projective algebraic sets by making use of the cone in affine space over the set in projective space. Section 12 applies the theory of Section 11 to address the question how the dimension of a projective algebraic set is cut down when the set is intersected with a projective hypersurface. A consequence of the theory is the result that a homogeneous system of polynomial equations over an algebraically closed field with more unknowns than equations has a nonzero solution.

Section 13 is a brief introduction to the theory of schemes, which extends the theory of varieties by replacing the underlying algebraically closed field by an arbitrary commutative ring with identity.

1. Affine Algebraic Sets and Affine Varieties

We come now to the more geometric side of algebraic geometry. At least initially this means that we are interested in the set of simultaneous solutions of a system of polynomial equations in several variables. Because of the Nullstellensatz the natural starting point for the investigation is the case that the underlying field of coefficients is algebraically closed.

Accordingly, throughout Sections 1–6 of this chapter, $\Bbbk$ will denote an algebraically closed field.[1] We fix a positive integer n and denote by A the polynomial ring $A = \Bbbk[X_1, \ldots, X_n]$. Typical ideals of A will be denoted by $\mathfrak{a}$, $\mathfrak{b}$, ... We begin by expanding on some definitions made in Section VIII.2. The set

$$\mathbb{A}^n = \left\{(x_1, \ldots, x_n) \in \Bbbk^n\right\}$$

is called **affine n-space**. Members of $\mathbb{A}^n$ are called **points** in affine n-space, and the functions $P \mapsto x_j(P)$ give the **coordinates** of the points.

To each subset S of polynomials in A, we associate the **locus of common zeros**, or **zero locus** of the members of S:

$$V(S) = \left\{P \in \mathbb{A}^n \mid f(P) = 0 \text{ for all } f \in S\right\}.$$

Any such set $V(S)$ is called an **affine algebraic set** in $\mathbb{A}^n$. If S is a finite set $\{f_1, \ldots, f_k\}$ of polynomials, we allow ourselves to abbreviate $V(\{f_1, \ldots, f_k\})$

[1]The exposition in these sections is based in part on Chapters 2, 4, and 6 of Fulton's book, Chapter I of Hartshorne's book, and Chapter I of Volume 1 of Shafarevich's books.

as $V(f_1, \dots, f_k)$. It is immediate from the definitions that $V(S)$ is the same as $V(\mathfrak{a})$ if $\mathfrak{a}$ is the ideal in A generated by S. The Hilbert Basis Theorem shows that every ideal of A is finitely generated, and it follows that every affine algebraic set is of the form $V(f_1, \dots, f_k)$ for some k and some polynomials $f_1, \dots, f_k$.

In Chapter VIII we worked extensively with examples of ideals of A and their corresponding affine algebraic sets, and it will not be necessary to give further examples of that kind now.

Observe from the definition that $V(S) = \bigcap_{f \in S} V(f)$ for any subset S of A. It follows immediately that $S \mapsto V(S)$, as a function carrying each subset S of A to a subset $V(S)$ of $\mathbb{A}^n$, is inclusion reversing: $S_1 \subseteq S_2$ implies $V(S_1) \supseteq V(S_2)$. Using this same identity, we obtain the following further properties of V.

Proposition 10.1. Affine algebraic sets in $\mathbb{A}^n$ have the following properties:

(a) $V(\varnothing) = V(0) = \mathbb{A}^n$ and $V(A) = \varnothing$,
(b) $V\big(\bigcup_\alpha S_\alpha\big) = \bigcap_\alpha V(S_\alpha)$ if the S_α's are arbitrary subsets of A,
(c) $V(S) = V(S_1) \cup V(S_2)$ if S_1 and S_2 are subsets of A and if S is defined as the set of all products $f_1 f_2$ with $f_1 \in S_1$ and $f_2 \in S_2$.

PROOF. Property (a) is immediate. For (b), we have

$$V\Big(\bigcup_\alpha S_\alpha\Big) = \bigcap_{f \in \bigcup_\alpha S_\alpha} V(f) = \bigcap_\alpha \bigcap_{f \in S_\alpha} V(f) = \bigcap_\alpha V(S_\alpha).$$

For (c), we observe first that $V(f_1 f_2) = V(f_1) \cup V(f_2)$ for any f_1 and f_2 in A. Then

$$\begin{aligned} V(S) &= \bigcap_{\substack{f_1 \in S_1,\\ f_2 \in S_2}} V(f_1 f_2) = \bigcap_{f_1 \in S_1} \bigcap_{f_2 \in S_2} \big(V(f_1) \cup V(f_2)\big) \\ &= \Big(\bigcap_{f_1 \in S_1} V(f_1)\Big) \cup \Big(\bigcap_{f_2 \in S_2} V(f_2)\Big) = V(S_1) \cup V(S_2). \end{aligned}$$ □

Properties (a), (b), and (c) in the proposition are the axioms for the closed sets in a topology on $\mathbb{A}^n$. This topology is called the **Zariski topology** on affine n-space. Every one-point set is closed. The Zariski topology on $\mathbb{A}^n$ is never Hausdorff; for example, if $n = 1$, then it is the topology on $\mathbb{k}^1 = \mathbb{k}$ in which the nonempty open sets are the complements of the finite sets. Since one-point sets are closed and the topology is not Hausdorff, the Zariski topology on $\mathbb{A}^n$ is never regular. At first glance it looks like a useless topology, but we shall see already in Proposition 10.3b and again in Section 2 that it is quite helpful for handling the bookkeeping used in passing back and forth between algebra and geometry.

Next we introduce a function $E \mapsto I(E)$, carrying each subset E of $\mathbb{A}^n$ to an ideal $I(E)$ in A, by the definition

$$I(E) = \big\{ f \in A \mid f(P) = 0 \text{ for all } P \in E \big\}.$$

Then $I(E) = \bigcap_{P \in E} I(\{P\})$. It follows immediately that $E \mapsto I(E)$ is inclusion reversing: $E_1 \subseteq E_2$ implies $I(E_1) \supseteq I(E_2)$. The result for $I(\cdot)$ that parallels Proposition 10.1 is as follows.

Proposition 10.2. For fixed n, the function $I(\cdot)$ has the following properties:
(a) $I(\varnothing) = A$ and $I(A) = 0$,
(b) $I(E_1 \cup E_2) = I(E_1) \cap I(E_2)$ if E_1 and E_2 are subsets of $\mathbb{A}^n$,
(c) $I(E_1 \cap E_2) \supseteq I(E_1) + I(E_2)$ if E_1 and E_2 are subsets of $\mathbb{A}^n$.

REMARKS. Equality can fail in (c). For example, if E_1 is the one-point set $\{0\}$ and E_2 is its complement, then $I(E_1 \cap E_2) = I(\varnothing) = A$, while $I(E_2) = 0$ and $I(E_1)$ consists of all members of A with 0 constant term.

PROOF. Property (a) is immediate. For (b), we have

$$I(E_1 \cup E_2) = \bigcap_{P \in E_1 \cup E_2} I(\{P\}) = \Big(\bigcap_{P \in E_1} I(\{P\})\Big) \cap \Big(\bigcap_{P \in E_2} I(\{P\})\Big) = I(E_1) \cap I(E_2).$$

In (c), the fact that $I(\cdot)$ is inclusion reversing implies that $I(E_1 \cap E_2) \supseteq I(E_1)$ and that $I(E_1 \cap E_2) \supseteq I(E_2)$. Since $I(E_1 \cap E_2)$ is closed under addition, (c) follows. □

This is all quite elementary. The less trivial question is the extent to which $V(\cdot)$ and $I(\cdot)$ are inverse to one another. Proposition 10.3 gives the answer.

Proposition 10.3. For fixed n,
(a) $I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}$ for each ideal $\mathfrak{a}$ in A,
(b) $V(I(E)) = \overline{E}$ for each subset E of $\mathbb{A}^n$, where $\overline{E}$ is the Zariski closure of E,
(c) $V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}})$ for each ideal $\mathfrak{a}$ in A,
(d) any two ideals $\mathfrak{a}$ and $\mathfrak{b}$ in A have $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b} \subseteq \sqrt{\mathfrak{a}\mathfrak{b}}$ and consequently have $V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$.

REMARKS. Recall from Section VII.1 that $\sqrt{\mathfrak{a}}$ denotes the radical of $\mathfrak{a}$, consisting of all f in A such that f^k is in $\mathfrak{a}$ for some integer $k \geq 1$. The radical of $\mathfrak{a}$ equals $\mathfrak{a}$ itself if $\mathfrak{a}$ is prime.

PROOF. Conclusion (a) is the Nullstellensatz as formulated in Theorem 7.1b.

For (b), the definitions show that $V(I(E)) \supseteq E$. Since any set $V(S)$ is Zariski closed, we must have $V(I(E)) \supseteq \overline{E}$. On the other hand, the fact that $\overline{E}$ is closed means that $\overline{E} = V(S)$ for some S. Thus $V(S) = \overline{E} \supseteq E$, and the inclusion-reversing property of $I(\cdot)$ gives $I(V(S)) \subseteq I(E)$. Since the definitions imply that $S \subseteq I(V(S))$, we obtain $S \subseteq I(E)$. From the inclusion-reversing property of $V(\cdot)$, we conclude that $\overline{E} = V(S) \supseteq V(I(E))$.

For (c), (a) and (b) give $V(\sqrt{\mathfrak{a}}) = V(I(V(\mathfrak{a}))) = \overline{V(\mathfrak{a})} = V(\mathfrak{a})$ because $V(\mathfrak{a})$ is closed.

For (d), the inclusion $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$ is immediate. If f is in $\mathfrak{a} \cap \mathfrak{b}$, then f is in $\mathfrak{a}$ and in $\mathfrak{b}$, and hence f^2 is in $\mathfrak{ab}$. Thus f is in $\sqrt{\mathfrak{ab}}$. Applying $V(\cdot)$ gives $V(\mathfrak{ab}) \supseteq V(\mathfrak{a} \cap \mathfrak{b}) \supseteq V(\sqrt{\mathfrak{ab}})$. Since $V(\mathfrak{ab}) = V(\sqrt{\mathfrak{ab}})$ by (c), $V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{ab})$. Finally $V(\mathfrak{ab}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$ by Proposition 10.1c. □

An **affine variety** is any affine algebraic set of the form $V(\mathfrak{p})$, where $\mathfrak{p}$ is a prime ideal[2] of A. That is, an affine variety is the locus of common zeros of any prime ideal of A.

For example, if f is an irreducible polynomial in A, then f is prime because A is a unique factorization domain, and consequently the principal ideal (f) is prime. Thus the zero locus in $\mathbb{A}^2$ of an irreducible polynomial f in $\Bbbk[X, Y]$ is an example of an affine variety. This particular kind of affine variety is called an **irreducible affine plane curve**.[3,4] More generally, if f is irreducible in $A = \Bbbk[X_1, \ldots, X_n]$ with $n \geq 2$, then the zero locus of f in $\mathbb{A}^n$ is called an **irreducible affine hypersurface**.[5] Another example of an affine variety is any translate of any vector subspace of $\mathbb{A}^n$. Examples of affine varieties other than irreducible hypersurfaces, translates of vector subspaces, and varieties built from other varieties in simple ways often take some work to establish. The reason is that it is usually not easy to show that a particular nonprincipal ideal is prime. Here is one example that is manageable.

EXAMPLE. The **twisted cubic** in $\mathbb{A}^3$ is the zero locus $V(\mathfrak{p})$ of the ideal $\mathfrak{p}$ in $\Bbbk[X, Y, Z]$ given by $\mathfrak{p} = (Y - X^2, Z - X^3)$; that is, $V(\mathfrak{p}) = \{(x, x^2, x^3) \mid x \in \Bbbk\}$. The substitution homomorphism φ that fixes $\Bbbk$ and sends X to X, Y to X^2, and Z to X^3 carries $\Bbbk[X, Y, Z]$ into $\Bbbk[X]$. It is onto $\Bbbk[X]$ because any polynomial in X alone is sent to itself by φ. The kernel of φ manifestly contains $\mathfrak{p}$. To see that it equals $\mathfrak{p}$, we argue by contradiction. Choose a polynomial f in $\ker \varphi$ not in $\mathfrak{p}$ whose degree in Z is as small as possible and whose degree in Y is as small as possible among those of minimal degree in Z. If Z occurs somewhere in f, then by replacing all occurrences of Z in f with X^3, we replace f by another member of $f + \mathfrak{p}$ of lower degree in Z, contradiction. Thus f has no Z in it. Arguing

[2] *Warning:* The books by Fulton and Hartshorne in the Selected References use the narrow definition of variety that is reproduced here. Some books by other authors allow all affine algebraic sets to be called varieties. Volume 1 of Shafarevich's books does not use the word "variety."

[3] *Warning:* This definition represents a change from Chapters VIII and IX, corresponding to a change in point of view. Previously the word "curve" referred to the ideal, and now it is to refer to the zero locus. From a mathematical standpoint Proposition 10.3 shows that this distinction is not important in the presence of the irreducibility and the fact that $\Bbbk$ is algebraically closed. The change thus represents only a matter of convenience for the exposition.

[4] Some authors build the condition of irreducibility into the definition of "curve," but this book does not.

[5] Some authors build the condition of irreducibility into the definition of "hypersurface," but this book does not.

similarly, we see that f has no Y in it. So f is a polynomial in X. Since φ acts as the identity on polynomials in X alone, $f = 0$. This contradiction shows that $\ker\varphi = \mathfrak{p}$. Since $\operatorname{image}\varphi = \Bbbk[X]$ is an integral domain, $\mathfrak{p}$ is prime. By the Nullstellensatz, $\mathfrak{p}$ may be described alternatively as the ideal of all polynomials vanishing on $V(\mathfrak{p})$.

Every affine variety is nonempty, as a consequence of the Nullstellensatz. In fact, any prime ideal $\mathfrak{p}$ of A is contained in a maximal ideal $\mathfrak{m}$, whose zero locus is identified as some point P of $\mathbb{A}^n$. The inclusion $\mathfrak{p} \subseteq \mathfrak{m}$ implies that $V(\mathfrak{p}) \supseteq V(\mathfrak{m}) = \{P\}$. Affine varieties are characterized by a geometric irreducibility property that is stated in Corollary 10.4.

Corollary 10.4. The affine varieties in $\mathbb{A}^n$ are characterized as those nonempty Zariski closed sets that cannot be written as the union of two proper closed subsets.

REMARKS. One says that the affine varieties are those affine algebraic sets that are **irreducible**. Irreducible sets are nonempty by definition.

PROOF. Let $V(\mathfrak{p})$ be an affine variety with $\mathfrak{p}$ prime, and suppose that $V(\mathfrak{p}) = E_1 \cup E_2$ with E_1 and E_2 both closed and properly contained in $V(\mathfrak{p})$. Application of $I(\,\cdot\,)$ and use of Proposition 10.2b gives $I(V(\mathfrak{p})) = I(E_1) \cap I(E_2)$. Proposition 10.3a allows us to rewrite this conclusion as $\mathfrak{p} = \mathfrak{b}_1 \cap \mathfrak{b}_2$ with $\mathfrak{b}_1 = I(E_1)$ and $\mathfrak{b}_2 = I(E_2)$. By Problem 10a at the end of Chapter VII, $\mathfrak{p} = \mathfrak{b}_1$ or $\mathfrak{p} = \mathfrak{b}_2$. If $\mathfrak{p} = \mathfrak{b}_1$, then $V(\mathfrak{p}) = V(\mathfrak{b}_1) = V(I(E_1))$, and this equals E_1 by Proposition 10.3b because E_1 is closed. Similarly if $\mathfrak{p} = \mathfrak{b}_2$, then $V(\mathfrak{p}) = E_2$. Thus E_1 and E_2 cannot both be proper subsets of $V(\mathfrak{p})$.

Conversely suppose that E is an irreducible closed subset of $\mathbb{A}^n$. Let f and g be members of A with fg in $I(E)$. Then Propositions 10.3b and 10.1c give $E = V(I(E)) \subseteq V(fg) = V(f) \cup V(g)$. Therefore

$$E = \big(E \cap V(f)\big) \cup \big(E \cap V(g)\big)$$

exhibits E as the union of two closed sets. By irreducibility one of the two closed sets equals E. If $E = E \cap V(f)$, then $E \subseteq V(f)$ and $I(E) \supseteq I(V(f)) \supseteq (f)$. If $E = E \cap V(g)$, then similarly $I(E) \supseteq (g)$. Either way, one of f and g lies in $I(E)$. Since E is assumed nonempty, $I(E)$ is proper. Therefore $I(E)$ is prime. □

2. Geometric Dimension

We continue to assume that $\Bbbk$ is an algebraically closed field and to write A for $\Bbbk[X_1, \ldots, X_n]$. If $\mathfrak{p}$ is a prime ideal in A, then the **dimension** of the affine variety $V(\mathfrak{p})$ was defined in Section VII.2 to be the transcendence degree of the field of fractions of the integral domain $A/\mathfrak{p}$ over $\Bbbk$. This quantity depends only

on $V(\mathfrak{p})$ because $\mathfrak{p}$ can be recovered from $V(\mathfrak{p})$ by the formula $\mathfrak{p} = I(V(\mathfrak{p}))$ given in Proposition 10.3a. The integral domain $A/\mathfrak{p}$ is finitely generated as a $\Bbbk$ algebra with generators $X_1 + \mathfrak{p}, \ldots, X_n + \mathfrak{p}$, and Theorem 7.22 shows that this transcendence degree equals the Krull dimension of the ring $A/\mathfrak{p}$, which is denoted by $\dim A/\mathfrak{p}$. The latter quantity is the supremum of the indices d of all strictly increasing chains $\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_d$ of prime ideals in $A/\mathfrak{p}$.

Because of this equality, it is natural to use the notion of Krull dimension in order to generalize the definition of dimension from varieties to all nonempty affine algebraic sets.[6] If $\mathfrak{a}$ is an any proper ideal in A, not necessarily prime, and $V(\mathfrak{a})$ is its locus of common zeros, we might first try defining $\dim V(\mathfrak{a})$ to be the Krull dimension of $A/\mathfrak{a}$. This approach is a bit cumbersome because two distinct ideals $\mathfrak{a}$ and $\mathfrak{a}'$ can have $V(\mathfrak{a}) = V(\mathfrak{a}')$; thus some argument would be needed to see that $\dim V(\mathfrak{a})$ is well defined before it would be possible to proceed.

Instead, we shall give a direct geometric definition of dimension in terms of the Zariski topology on $\mathbb{A}^n$. Theorem 10.7 later in this section will show that the geometric quantity $\dim V(\mathfrak{a})$ equals the Krull dimension of $A\big/\sqrt{\mathfrak{a}}$, thus that the dimension of an affine algebraic set has an algebraic formulation. From this result we shall deduce that $\dim V(\mathfrak{a})$ equals the Krull dimension of $A/\mathfrak{a}$ itself. This algebraic formulation of a definition will not yet allow us to compute dimensions concretely, but we shall introduce in Sections 9–11 an equivalent combinatorial definition of dimension that is computable in terms of Gröbner bases.

A topological space X will be said to be **Noetherian** if every strictly decreasing sequence of closed subsets is finite in length. An example is affine n-space $\mathbb{A}^n$. In fact, if $E_1, E_2, \ldots$ are closed sets in $\mathbb{A}^n$ with $E_1 \supseteq E_2 \supseteq \cdots$, then the corresponding ideals have $I(E_1) \subseteq I(E_2) \subseteq \cdots$. Since A is Noetherian, there exists some integer k with $I(E_k) = I(E_{k+1}) = \cdots$. Applying $V(\cdot)$ and using Proposition 10.3b, we obtain $E_k = E_{k+1} = \cdots$.

We can generalize the definition of irreducibility for closed sets from $\mathbb{A}^n$ to an arbitrary Noetherian topological space. Namely a nonempty closed set E is **irreducible** if it is not the union of two proper closed subsets. An important observation about any Noetherian topological space is that any nonempty relatively open subset U of an irreducible closed set V is dense in V; in fact, if $\overline{U}$ denotes the closure of U, then $V = \overline{U} \cup (V - U)$ exhibits V as the union of two closed subsets, and the irreducibility forces $\overline{U} = V$ since $V - U \neq V$.

Proposition 10.5. If X is a Noetherian topological space, then any closed subset is the finite union of irreducible closed subsets. This decomposition of a closed set as such a union may be chosen in such a way that none of the closed sets in the union contains another set in the union, and in this case the decomposition is unique.

[6] We shall leave the dimension of the empty set as undefined for now.

PROOF. For existence of some decomposition of each closed set as a finite union of irreducible closed subsets, we argue by contradiction. Assuming that there exists some closed subset E of X that is not the finite union of irreducible closed subsets, we may assume by the Noetherian condition on X that E is minimal among all such counterexamples. Since E cannot itself be irreducible, we can write $E = E_1 \cup E_2$ with E_1 and E_2 closed and properly contained in E. Since E is minimal among all closed subsets that are not the finite union of irreducible closed subsets, E_1 and E_2 can be expressed as finite unions of irreducible closed subsets. Substituting these expressions into the equality $E = E_1 \cup E_2$ gives a contradiction to the fact that E is a counterexample.

This proves existence of a decomposition. By going through the sets in the decomposition one at a time and by discarding any set that is contained in another set, we obtain a decomposition as in the second sentence of the proposition.

For uniqueness, suppose that $E = E_1 \cup \cdots \cup E_k = F_1 \cup \cdots \cup F_l$ gives two decompositions of the asserted kind. Say that $k \geq l$. Since $F_i \subseteq E_1 \cup \cdots \cup \cdots \cup E_k$, we obtain $F_i = (F_i \cap E_1) \cup \cdots \cup (F_i \cap E_k)$. Irreducibility of F_i implies that $F_i = F_i \cap E_{j(i)}$ for some $j = j(i)$. Hence $F_i \subseteq E_{j(i)}$ for some function $j(i)$ from $\{1, \ldots, l\}$ to $\{1, \ldots, k\}$. Reversing the roles of the E_i's and the F_j's yields a function $i(j)$ such that $E_j \subseteq F_{i(j)}$. Then $F_i \subseteq E_{j(i)} \subseteq F_{i(j(i))}$. Since no F_i contains some $F_{i'}$ with $i' \neq i$, we conclude that $i(j(i)) = i$ for all i. Therefore $k = l$, and $i(\cdot)$ and $j(\cdot)$ are inverse to each other. □

Corollary 10.6. Every affine algebraic set in $\mathbb{A}^n$ can be expressed uniquely as the finite (possibly empty) union of affine varieties in such a way that none of the varieties contains another of the varieties.

REMARKS. For example,

$$V(X^2 - Y^2) = V(X + Y) \cup V(X - Y)$$

by Proposition 10.1c, and the affine algebraic set on the left side is expressed as the union of the affine varieties on the right.

PROOF. We saw before Proposition 10.5 that $\mathbb{A}^n$ is a Noetherian topological space, and Corollary 10.4 shows that the irreducible subsets are the affine varieties. The closed sets are the affine algebraic sets by definition, and hence the result is a special case of Proposition 10.5. □

The **geometric dimension** of a nonempty closed subset E of a Noetherian topological space X is the supremum of the integers $d \geq 0$ such that there exists a strictly increasing chain $E_0 \subsetneqq E_1 \subsetneqq \cdots \subsetneqq E_d$ of irreducible closed subsets of E. This definition makes sense because a chain with $d = 0$ can always be formed with E_0 equal to one of the irreducible closed sets from Proposition 10.5;

however, there is no guarantee in this generality that the geometric dimension will be finite. In any event, it is clear from the definition that if two closed sets E and E' have $E \subseteq E'$, then the geometric dimension of E is $\leq$ the geometric dimension of E'.

In the case of a nonempty affine algebraic set $V(S)$, the geometric dimension of $V(S)$ is to refer to this kind of dimension relative to the Zariski topology.

EXAMPLES OF GEOMETRIC DIMENSION IN $\mathbb{A}^n$.

(1) Any one-point set in $\mathbb{A}^n$ is closed and plainly has geometric dimension 0. Any affine variety V with more than one point has geometric dimension ≥ 1, since $\{P\} \subsetneqq V$ is a strictly increasing chain of irreducible closed sets if P is chosen as a point in V.

(2) $\mathbb{A}^n$ has geometric dimension n. This fact will follow from Theorem 10.7 below because A has Krull dimension n as a consequence of Theorem 7.22.

(3) Twisted cubic in $\mathbb{A}^3$, namely $\{(x, x^2, x^3) \mid x \in \Bbbk\}$. According to the example in Section 1, this is $V(\mathfrak{p})$ for the prime ideal $\mathfrak{p} = (Y - X^2, Z - X^3) \subseteq \Bbbk[X, Y, Z]$. The inclusions of prime ideals $(X, Y, Z) \supsetneqq (Y - X^2, Z - X^3) \supsetneqq (Y - X^2) \supsetneqq 0$ give the strictly increasing chain $\{0\} \subsetneqq V(\mathfrak{p}) \subsetneqq \{(x, x^2, z)\} \subsetneqq \mathbb{A}^3$, which is of the kind described for $\mathbb{A}^3$. If another term could be included between $\{0\}$ and $V(\mathfrak{p})$, then we would obtain a sequence showing that $\mathbb{A}^3$ has geometric dimension ≥ 4, in contradiction to Example 2. So $V(\mathfrak{p})$ has geometric dimension ≤ 1. In view of Example 1, $V(\mathfrak{p})$ has geometric dimension equal to 1.

Theorem 10.7. If $\mathfrak{a}$ is any proper ideal of A, then the following four quantities are equal:

(a) the geometric dimension of $V(\mathfrak{a})$,
(b) the Krull dimension of $A/\sqrt{\mathfrak{a}}$,
(c) the maximum of the geometric dimension of V_j over all affine varieties V_j contained in $V(\mathfrak{a})$,
(d) the Krull dimension of $A/\mathfrak{a}$.

REMARKS. We take these equal quantities as the definition of the **dimension** $\dim V(\mathfrak{a})$ of the affine algebraic set $V(\mathfrak{a})$. Because of Theorem 7.22, these quantities equal the transcendence degree over $\Bbbk$ of the field of fractions of $A/\mathfrak{a}$ in the case that $\mathfrak{a}$ is a prime ideal. For $\mathfrak{a} = 0$, we know that $\dim A = n$; hence the equal quantities in the theorem are $\leq n$.

PROOF. Let

$$E_0 \subseteq E_1 \subseteq \cdots \subseteq E_d \tag{$*$}$$

be an increasing chain of irreducible closed subsets of $V(\mathfrak{a})$, and define $\mathfrak{p}_j$ to be the ideal $\mathfrak{p}_j = I(E_j)$. Then each $\mathfrak{p}_j$ is a prime ideal by Corollary 10.4, and also

$$\mathfrak{p}_d \subseteq \cdots \subseteq \mathfrak{p}_1 \subseteq \mathfrak{p}_0 \tag{$**$}$$

because $I(\cdot)$ is inclusion reversing. If $(*)$ is strictly increasing, then so is $(**)$; in fact, if $\mathfrak{p}_j$ were to equal $\mathfrak{p}_{j-1}$ for some j, then we would have $E_j = V(I(E_j)) = V(\mathfrak{p}_j) = V(\mathfrak{p}_{j-1}) = V(I(E_{j-1})) = E_{j-1}$, contradiction. In $(*)$, we have $E_d \subseteq V(\mathfrak{a})$, and thus Proposition 10.3a gives $\sqrt{\mathfrak{a}} = I(V(\mathfrak{a})) \subseteq I(E_d) = \mathfrak{p}_d$. In other words, any strictly increasing sequence $(*)$ of irreducible closed subsets of $V(\mathfrak{a})$ yields a strictly increasing sequence $(**)$ of prime ideals of A that contain $\sqrt{\mathfrak{a}}$.

Conversely if $(**)$ is a strictly increasing sequence of prime ideals of A containing $\sqrt{\mathfrak{a}}$, and if we define $E_j = V(\mathfrak{p}_j)$ for $0 \le j \le d$, then we obtain the sequence $(*)$ of irreducible closed subsets of $V(\sqrt{\mathfrak{a}}) = V(\mathfrak{a})$, and $(*)$ is strictly increasing, since an equality $E_j = E_{j-1}$ would imply that $\mathfrak{p}_j = I(V(\mathfrak{p}_j)) = I(E_j) = I(E_{j-1}) = I(V(\mathfrak{p}_{j-1})) = \mathfrak{p}_{j-1}$ because of Proposition 10.3a.

Thus the strictly increasing sequences $(*)$ of irreducible closed subsets of $V(\mathfrak{a})$ are in one-one correspondence with the strictly increasing sequences $(**)$ of prime ideals of A containing $\sqrt{\mathfrak{a}}$. Let $\varphi : A \to A\big/\sqrt{\mathfrak{a}}$ be the quotient homomorphism. Application of φ to $(**)$ yields a strictly increasing sequence of ideals of $A\big/\sqrt{\mathfrak{a}}$ by the First Isomorphism Theorem, and prime ideals map to prime ideals under this correspondence. Thus the existence of a strictly increasing sequence as in $(**)$ implies that the Krull dimension of $A\big/\sqrt{\mathfrak{a}}$ is $\ge d$. Meanwhile, the existence of a strictly increasing sequence as in $(*)$ implies that the geometric dimension of $V(\mathfrak{a})$ is $\ge d$. We have seen that these sequences are in one-one correspondence, and therefore the equality of (a) and (b) in the theorem follows.

In (c) certainly the geometric dimension of any V_j is $\le$ the geometric dimension of $V(\mathfrak{a})$. If d_0 denotes the geometric dimension of $V(\mathfrak{a})$, then we can find a strictly increasing chain as in $(*)$ with $d = d_0$ and with all the sets contained in $V(\mathfrak{a})$. Corollary 10.4 shows that E_{d_0} is an affine variety contained in $V(\mathfrak{a})$, and the sequence $(*)$ shows that the geometric dimension of E_{d_0} is at least d_0. Thus $V_j = E_{d_0}$ is an affine variety contained in $V(\mathfrak{a})$ whose geometric dimension equals that of $V(\mathfrak{a})$.

To complete the proof, we show the equality of (b) and (d), i.e., we show that $A/\mathfrak{a}$ and $A\big/\sqrt{\mathfrak{a}}$ have the same Krull dimension. Since $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$, it is enough to show that in any strictly increasing sequence of prime ideals as in $(**)$ such that all the ideals contain $\mathfrak{a}$, all the ideals actually contain $\sqrt{\mathfrak{a}}$. (Then the sequences $(**)$ for $\mathfrak{a}$ will be in one-one correspondence with the sequences for $\sqrt{\mathfrak{a}}$, and we can argue using the First Isomorphism Theorem as in the third paragraph of the proof.) Thus let x be in $\sqrt{\mathfrak{a}}$. By definition of radical, x^k lies in $\mathfrak{a}$ for some k. Since $\mathfrak{a} \subseteq \mathfrak{p}_d$, x^k lies in $\mathfrak{p}_d$. But $\mathfrak{p}_d$ is prime, and therefore x lies in $\mathfrak{p}_d$. Thus every ideal in the sequence $(**)$ for $\mathfrak{a}$ occurs in the sequence $(**)$ for $\sqrt{\mathfrak{a}}$, and the theorem follows. □

The dimension of an irreducible hypersurface in $A = \Bbbk[X_1, \ldots, X_n]$ is $n-1$, as was observed in Section VII.5. Proposition 10.9 below will prove a converse.

Lemma 10.8. Every minimal nonzero prime ideal in A is principal.

PROOF. Let $\mathfrak{p}$ be a minimal nonzero prime ideal, let $f \neq 0$ be a nonzero member, and write f as the product of irreducible elements. Since $\mathfrak{p}$ is prime, one of the irreducible elements, say g, lies in $\mathfrak{p}$. Since A is a unique factorization domain, g is prime. Consequently (g) is a prime ideal of A lying in $\mathfrak{p}$. By minimality of $\mathfrak{p}$, $\mathfrak{p} = (g)$. □

Proposition 10.9. Suppose that $\mathfrak{p}$ is a prime ideal of A and $V(\mathfrak{p})$ is the corresponding affine variety. If $\dim V(\mathfrak{p}) = n - 1$, then $\mathfrak{p}$ is principal, and hence $V(\mathfrak{p})$ is an irreducible hypersurface.

PROOF. For any $n \geq 1$, $\dim V(\mathfrak{p}) = n - 1 < n = \dim V(0)$ implies $\mathfrak{p} \neq 0$. Since $\dim V(\mathfrak{p}) = n - 1$, there exists a chain

$$0 = \mathfrak{q}_0 \subsetneqq \mathfrak{q}_1 \subsetneqq \cdots \subsetneqq \mathfrak{q}_{n-1}$$

of prime ideals in $A/\mathfrak{p}$. If $\varphi : A \to A/\mathfrak{p}$ denotes the quotient homomorphism, then this chain lifts to A as

$$0 \subsetneqq \mathfrak{p} \subsetneqq \varphi^{-1}(\mathfrak{q}_1) \subsetneqq \cdots \subsetneqq \varphi^{-1}(\mathfrak{q}_{n-1}).$$

This chain has n members after the 0 at the left, and A has Krull dimension n. Consequently the first nonzero element, which is $\mathfrak{p}$, is a minimal nonzero prime ideal of A. By Lemma 10.8, $\mathfrak{p}$ is principal. □

A **quasi-affine variety** is any nonempty Zariski open subset of an affine variety. These sets and their projective analogs, which will be defined in Section 3, will be the main objects of interest geometrically in Sections 1–6. If Y is a quasi-affine variety, then the closure $\overline{Y}$ is the affine variety in question because any nonempty relatively open subset of an affine variety is dense in the variety.[7]

Let us see that the relative Zariski topology on a quasi-affine variety Y makes Y into a Noetherian topological space. In fact, if X is a Noetherian topological space and Y is a topological subspace, then Y is Noetherian. To see this, we argue by contradiction, letting $E_1 \supseteq E_2 \supseteq \cdots$ be a strictly decreasing sequence of relatively closed sets in Y. Then the sequence of closures in X forms a decreasing sequence of closed sets in X with the property that $E_j = Y \cap \overline{E_j}$ for each j because E_j is assumed to be relatively closed in Y. It follows that the sequence of closures is strictly decreasing, contradiction.

Consequently any quasi-affine variety Y is Noetherian in the relative Zariski topology and has a meaningful geometric dimension. We write $\dim Y$ for this dimension.

[7]This important observation was made just before Proposition 10.5.

Lemma 10.10. If Y is a quasi-affine variety in $\mathbb{A}^n$ and if E is a nonempty relatively closed subset of Y, then E is irreducible[8] for Y if and only if $\overline{E}$ is irreducible for $\mathbb{A}^n$.

REMARKS. We shall actually prove the stronger result that if Y is a nonempty open subset of a Noetherian topological space X (such as $\mathbb{A}^n$) and if E is a nonempty relatively closed subset of Y, then E is irreducible for Y if and only if $\overline{E}$ is irreducible for X. This stronger result will be used in Section 3.

PROOF. First we check that E reducible implies $\overline{E}$ reducible. If E is reducible, say is a union $E = E_1 \cup E_2$ with E_1 and E_2 relatively closed proper subsets of E, then $\overline{E} = \overline{E_1} \cup \overline{E_2}$. Each of $\overline{E_1}$ and $\overline{E_2}$ is a closed subset of $\overline{E}$. To see that $\overline{E_1}$ is proper, we argue by contradiction. If $\overline{E_1} = \overline{E}$, then intersecting both sides with Y gives the contradiction $E_1 = Y \cap \overline{E_1} = Y \cap \overline{E} = E$ because E_1 and E are both relatively closed. Similarly $\overline{E_2}$ is proper, and thus $\overline{E}$ is reducible.

Conversely suppose that $\overline{E}$ is reducible, say is a union $\overline{E} = F_1 \cup F_2$ with F_1 and F_2 closed in X and properly contained in $\overline{E}$. Intersecting both sides with Y gives $E = Y \cap \overline{E} = Y \cap (F_1 \cup F_2) = (Y \cap F_1) \cup (Y \cap F_2)$ because E is relatively closed. The sets $Y \cap F_1$ and $Y \cap F_2$ are relatively closed, and their union is E. To see that E is reducible, we argue by contradiction. If $Y \cap F_1 = E$, then $E \subseteq F_1$. Since F_1 is closed in X, $\overline{E} \subseteq F_1$. Thus F_1 is not a proper subset of $\overline{E}$, contradiction. Similarly we cannot have $Y \cap F_2 = E$, and therefore E is exhibited as the union of the two proper relatively closed subsets $Y \cap F_1$ and $Y \cap F_2$. □

Proposition 10.11. If Y is a quasi-affine variety in $\mathbb{A}^n$, then $\dim Y = \dim \overline{Y}$. Here $\dim \overline{Y}$ refers to the dimension of the affine variety $\overline{Y}$ in any of the senses of Theorem 10.7.

REMARKS. This proposition is a formal consequence of Lemma 10.10. The stronger statement that we actually prove is that if Y is a nonempty open subset of a Noetherian topological space X, then the geometric dimension of Y as a Noetherian space equals the geometric dimension of X as a Noetherian space.

PROOF. Let $E_0 \subseteq E_1 \subseteq \cdots \subseteq E_d$ be a strictly increasing sequence of relatively closed irreducible subsets of Y. Then $\overline{E}_0 \subseteq \overline{E}_1 \subseteq \cdots \subseteq \overline{E}_d$ is an increasing sequence of closed subsets of $\mathbb{A}^n$, each of which is irreducible by Lemma 10.10. Since $E_j = Y \cap \overline{E_j}$ for each j, the sets $\overline{E_j}$ are strictly increasing. Since the given sequence of sets E_j is arbitrary, it follows that $\dim Y \leq \dim \overline{Y}$.

For the reverse inequality, let $F_0 \subseteq F_1 \subseteq \cdots \subseteq F_d$ be a strictly increasing sequence of irreducible closed subsets of $\overline{Y}$. If E_j denotes $F_j \cap Y$, then $E_0 \subseteq$

[8] ... in the sense of not being the union of two relatively closed proper subsets.

$E_1 \subseteq \cdots \subseteq E_d$ is an increasing sequence of relatively closed subsets of Y, each of which is irreducible by Lemma 10.10. Since $F_j = \overline{E_j}$, the sets E_j are strictly increasing. Since the given sequence of sets F_j is arbitrary, it follows that $\dim \overline{Y} \le \dim Y$. □

3. Projective Algebraic Sets and Projective Varieties

We continue to assume that $\Bbbk$ is an algebraically closed field and to write A for $\Bbbk[X_1, \dots, X_n]$. In Section VIII.3 we studied the projective analogs of affine plane curves, and the task for the present section is to study similarly the projective analogs of general affine algebraic sets, affine varieties, and quasi-affine varieties.

As in Section VIII.3, **projective n-space** over $\Bbbk$ is defined set theoretically as the quotient

$$\mathbb{P}^n = \big\{(x_0, \dots, x_n) \in \Bbbk^{n+1} - \{0\}\big\} \big/ \sim,$$

where $(x_0', \dots, x_n') \sim (x_0, \dots, x_n)$ if $(x_0', \dots, x_n') = \lambda(x_0, \dots, x_n)$ for some $\lambda \in \Bbbk^\times$. We write $[x_0, \dots, x_n]$ for the class of $(x_0, \dots, x_n)$ in $\mathbb{P}^n$.

Put $\widetilde{A} = \Bbbk[X_0, \dots, X_n]$. The polynomials of interest for algebraic geometry relative to $\mathbb{P}^n$ are the homogeneous polynomials in $\widetilde{A}$. The definitions of "monomial," "total degree" of a monomial, "homogeneous polynomial," and "degree" of a homogeneous polynomial all appear in Section VIII.3; monomials are defined so as to have coefficient 1. By convention the 0 polynomial is homogeneous of every degree. We write $\widetilde{A}_d = \Bbbk[X_0, \dots, X_n]_d$ for the $\Bbbk$ vector space of homogeneous polynomials of degree d. Each member F of $\widetilde{A}_d$ satisfies

$$F(\lambda x_0, \dots, \lambda x_n) = \lambda^d F(x_0, \dots, x_n)$$

for all $(x_0, \dots, x_n) \in \Bbbk^{n+1}$ and $\lambda \in \Bbbk^\times$. Conversely the fact that the mapping of polynomials into polynomial functions is one-one for an infinite field implies that a member F of $\widetilde{A}$ is homogeneous of degree d if it satisfies the above displayed property. Four further properties of $\widetilde{A}_d$ from Section VIII.3 are that

- the zero locus of a member of $\widetilde{A}_d$ is well defined as a subset of $\mathbb{P}^n$,
- the monomials of total degree d form a $\Bbbk$ basis of the vector space $\widetilde{A}_d$,
- $\dim_\Bbbk \widetilde{A}_d = \binom{d+n}{n}$,
- any polynomial factor of a homogeneous polynomial over a field $\Bbbk$ is homogeneous.

An ideal $\mathfrak{a}$ in $\widetilde{A}$ is called a **homogeneous ideal** if it is the vector-space sum over $d \ge 0$ of its intersections with $\widetilde{A}_d$: $\mathfrak{a} = \bigoplus_{d=0}^\infty (\mathfrak{a} \cap \widetilde{A}_d)$. Any ideal in $\widetilde{A}$ that is generated by homogeneous polynomials is a homogeneous ideal. A special case of this fact is that if a $\Bbbk$ vector subspace $\mathfrak{a}_d$ of $\widetilde{A}_d$ is specified for each

integer $d \geq 0$, then $\mathfrak{a} = \bigoplus_{d=0}^{\infty} \mathfrak{a}_d$ is a homogeneous ideal if and only if for each $d \geq 0$ and $e \geq 0$, the inclusion $F\widetilde{A}_d \subseteq \widetilde{A}_{d+e}$ holds for each F in $\widetilde{A}_e$.

We can now imitate some of the development of Sections 1 and 2 for the present context as long as we stick to homogeneous polynomials in $\widetilde{A}$ and to homogeneous ideals. For any homogeneous polynomial F in $\widetilde{A}$, the set

$$V(F) = \{P = [x_0, \ldots, x_n] \in \mathbb{P}^n \mid F(x_0, \ldots, x_n) = 0\}$$

is well defined by the first bulleted property above. Thus if S is any set of homogeneous elements in $\widetilde{A}$, we can associate the **locus of common zeros** in $\mathbb{P}^n$, or **zero locus**, of the members of S by the formula

$$V(S) = \bigcap_{F \in S} V(F).$$

If $\mathfrak{a}$ is a homogeneous ideal, then $V(\mathfrak{a})$ by convention means $V(S)$, where S is the subset of all homogeneous members of $\mathfrak{a}$. Any such set $V(S)$ is called a **projective algebraic set** in $\mathbb{P}^n$. The function $S \mapsto V(S)$ is inclusion reversing. The analog of Proposition 10.1 in the present context is that projective algebraic sets have the following properties:

(i) $V(\varnothing) = V(0) = \mathbb{P}^n$ and $V(\widetilde{A}) = \varnothing$,
(ii) $V\big(\bigcup_\alpha S_\alpha\big) = \bigcap_\alpha V(S_\alpha)$ if the S_α's are arbitrary sets of homogeneous elements in $\widetilde{A}$,
(iii) $V(S) = V(S_1) \cup V(S_2)$ if S_1 and S_2 are sets of homogeneous elements in $\widetilde{A}$ and if S is defined as the set of all products F_1F_2 with $F_1 \in S_1$ and $F_2 \in S_2$.

Consequently the projective algebraic sets in $\mathbb{P}^n$ form the closed sets for a topology on $\mathbb{P}^n$ called the **Zariski topology** on $\mathbb{P}^n$.

Next we associate to each point P of $\mathbb{P}^n$ a homogeneous ideal $I(P)$ in $\widetilde{A}$ by the definition

$$I(P) = \{F \in \widetilde{A} \mid F(x_0, \ldots, x_n) = 0 \text{ whenever } [x_0, \ldots, x_n] = P\}.$$

Problem 1 at the end of the chapter shows that $I(P)$ is indeed a homogeneous ideal. In terms of the ideals $I(P)$, we define $I(E) = \bigcap_{P \in E} I(P)$ for each subset E of $\mathbb{P}^n$. The result $E \mapsto I(E)$ is a function carrying subsets E of $\mathbb{P}^n$ to homogeneous ideals $I(E)$ in $\widetilde{A}^n$. The function $E \mapsto I(E)$ is inclusion reversing, and the same argument as for Proposition 10.2 shows that for each n it satisfies

(i) $I(\varnothing) = \widetilde{A}$ and $I(\mathbb{P}^n) = 0$,
(ii) $I(E_1 \cup E_2) = I(E_1) \cap I(E_2)$ if E_1 and E_2 are subsets of $\mathbb{P}^n$,
(iii) $I(E_1 \cap E_2) \supseteq I(E_1) + I(E_2)$ if E_1 and E_2 are subsets of $\mathbb{P}^n$.

If S is any set of homogeneous elements in $\widetilde{A}$ and if $V = V(S)$ is the corresponding projective algebraic set in $\mathbb{P}^n$, then we define the **cone** over V to be the subset of $\mathbb{A}^{n+1}$ given by

$$C(V) = (0, \dots, 0) \cup \big\{(x_0, \dots, x_n) \in \mathbb{A}^{n+1} \mid [x_0, \dots, x_n] \in V\big\}.$$

This kind of set has the following two properties:

(i) V nonempty implies that the ideals $I(C(V))$ and $I(V)$ in $\widetilde{A}$ are equal,
(ii) any homogeneous ideal $\mathfrak{a}$ in $\widetilde{A}$ with $V(\mathfrak{a})$ nonempty in $\mathbb{P}^n$ has $C(V(\mathfrak{a}))$ equal to the subset $V(\mathfrak{a})$ in affine $(n+1)$-space.

Use of this device reduces a number of questions about $\mathbb{P}^n$ to questions about $\mathbb{A}^{n+1}$. An example is a projective analog of Proposition 10.3, which appears as the next proposition.

Proposition 10.12. For fixed n,

(a) **(homogeneous Nullstellensatz)** a homogeneous ideal $\mathfrak{a}$ in $\widetilde{A}$ has $V(\mathfrak{a})$ empty in $\mathbb{P}^n$ if and only if there is an integer N such that $\mathfrak{a}$ contains $\widetilde{A}_k$ for $k \geq N$,
(b) $I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}$ for each homogeneous ideal $\mathfrak{a}$ in $\widetilde{A}$ for which $V(\mathfrak{a})$ is nonempty in $\mathbb{P}^n$,
(c) $V(I(E)) = \overline{E}$ for each subset E of $\mathbb{P}^n$, where $\overline{E}$ is the Zariski closure of E in $\mathbb{P}^n$.

REMARK. For clarity in the proof, let us write $V_a(\,\cdot\,)$ and $V_p(\,\cdot\,)$ to distinguish zero loci in $\mathbb{A}^{n+1}$ from zero loci in $\mathbb{P}^n$.

PROOF. For (a), $V_p(\mathfrak{a})$ is empty in $\mathbb{P}^n$ if and only if $V_a(\mathfrak{a})$ is contained in $\{0\}$ in $\mathbb{A}^{n+1}$, if and only if $\sqrt{\mathfrak{a}} = I(V_a(\mathfrak{a}))$ contains $(X_0, \dots, X_n)$ by the affine Nullstellensatz. In this case if $f_1, \dots, f_r$ are generators of $\sqrt{\mathfrak{a}}$, then the elements $f_1^m, \dots, f_r^m$ are in $\mathfrak{a}$ for some m, and it follows that $\big(\sum_{j=1}^r c_r f_j\big)^k$ lies in $\mathfrak{a}$ for all scalars c_j whenever $k \geq rm$; hence $\widetilde{A}_k \subseteq \mathfrak{a}$ for $k \geq rm$. Conversely if $\sqrt{\mathfrak{a}}$ fails to contain some X_j, then X_j^k is not in $\mathfrak{a}$ for any $k \geq 1$, and $\widetilde{A}_k$ cannot be contained in $\mathfrak{a}$.

For (b), $I_p(V_p(\mathfrak{a})) = I_a(C(V_p(\mathfrak{a}))) = I_a(V_a(\mathfrak{a})) = \sqrt{\mathfrak{a}}$ by (i) of cones, (ii) of cones, and the affine Nullstellensatz.

Conclusion (c) is proved by the same argument as for Proposition 10.3b. □

A **projective variety** is any *nonempty*[9] projective algebraic set of the form $V(\mathfrak{p})$, where $\mathfrak{p}$ is a prime homogeneous ideal in $\widetilde{A}$. If the ideal $\mathfrak{p}$ is the principal

[9]The prime homogeneous ideal $\mathfrak{p} = (X_0, \dots, X_n)$ has $V(\mathfrak{p}) = \varnothing$, but no other prime homogeneous ideal $\mathfrak{q}$ has $V(\mathfrak{q}) = \varnothing$. In order to avoid trivial counterexamples to some results, we shall often want to exclude this particular prime ideal $\mathfrak{p}$ from consideration.

ideal generated by an irreducible homogeneous polynomial, then the ideal or the variety is called an **irreducible projective hypersurface**.[10]

Corollary 10.13. The projective varieties in $\mathbb{P}^n$ are characterized as those nonempty Zariski closed sets that cannot be written as the union of two proper closed subsets.

REMARK. Such a subset of $\mathbb{P}^n$ is said to be **irreducible**. As in the affine case, irreducible sets are understood to be nonempty.

PROOF. If $V(\mathfrak{p})$ is a projective variety, then the union of $\{0\}$ and the subset of $\Bbbk^{n+1}$ whose equivalence classes are in $V(\mathfrak{p})$ is an affine variety in $\mathbb{A}^{n+1}$. It is irreducible in $\mathbb{A}^{n+1}$, and this irreducibility in $\mathbb{A}^{n+1}$ implies irreducibility within $\mathbb{P}^n$.

Conversely if E is an irreducible closed subset of $\mathbb{P}^n$ and if F and G are *homogeneous* members of $\widetilde{A}$ with FG in $I(E)$, then we can argue as in the proof of Corollary 10.4 to see that one of F and G lies in $I(E)$ and that $I(E)$ is proper. Since $I(E)$ is a homogeneous ideal, this fact implies that $I(E)$ is prime. □

Since $\widetilde{A}$ is a Noetherian ring, it follows that $\mathbb{P}^n$ is a Noetherian topological space in the sense of Section 2. Consequently Proposition 10.5 is applicable. Combining this result with Corollary 10.13, we obtain the following corollary.

Corollary 10.14. Every projective algebraic set in $\mathbb{P}^n$ can be expressed uniquely as the finite (possibly empty) union of projective varieties in such a way that none of the varieties contains another of the varieties.

Geometric dimension is therefore meaningful for nonempty projective algebraic sets, and each such set in $\mathbb{P}^n$ has geometric dimension $\leq n$.

A **quasiprojective variety** is any nonempty Zariski open subset of a projective variety. Quasi-affine varieties and quasiprojective varieties will be the main objects of interest geometrically in Sections 1–7. If Y is a quasiprojective variety, then the relative Zariski topology on Y makes Y into a Noetherian topological space, just as in the quasi-affine case. Consequently Y has a meaningful geometric dimension. The arguments in Lemma 10.10 and Proposition 10.11 concerning quasi-affine varieties are arguments in point-set topology and valid proofs of facts about quasiprojective varieties. Therefore we obtain the following result.

Proposition 10.15. If Y is a quasiprojective variety in $\mathbb{P}^n$, then the closure $\overline{Y}$ in the Zariski topology of $\mathbb{P}^n$ is a projective variety, and the geometric dimensions of Y and $\overline{Y}$ are equal.

[10] As in the affine case, as long as the assumption of irreducibility is in force, the distinction between the ideal and the variety is unimportant.

We can identify $\mathbb{A}^n$ as a subset of $\mathbb{P}^n$ by the formula

$$\beta_0(x_1, \ldots, x_n) = [1, x_1, \ldots, x_n]$$

for $(x_1, \ldots, x_n)$ in $\mathbb{A}^n$. The complement of $\beta_0(\mathbb{A}^n)$ in $\mathbb{P}^n$ is the zero locus of the homogeneous polynomial X_0, and consequently $\beta_0(\mathbb{A}^n)$ is open in $\mathbb{P}^n$. Since the equality $\mathbb{P}^n = V(0)$ exhibits $\mathbb{P}^n$ as a projective variety, $\beta_0(\mathbb{A}^n)$ is a quasiprojective variety. We are going to show that β_0 respects topologies in that the Zariski topology of $\mathbb{A}^n$ is carried to the Zariski topology of the quasiprojective variety $\beta_0(\mathbb{A}^n)$. To do so, we make use of the corresponding transpose mapping $\beta_0^t : \widetilde{A} \to A$ on polynomials given by $\beta_0^t F = f$ with

$$f(X_1, \ldots, X_n) = F(\beta_0(X_1, \ldots, X_n)) = F(1, X_1, \ldots, X_n).$$

This is the substitution homomorphism that fixes $\Bbbk$, fixes $X_1, \ldots, X_n$, and carries X_0 to 1. Being an algebra homomorphism onto, β_0^t carries ideals of $\widetilde{A}$ to ideals of A. In particular, it carries homogeneous ideals of $\widetilde{A}$ to ideals of A.

Lemma 10.16. If $\mathfrak{a}$ is a homogeneous ideal in $\widetilde{A}$ and $\mathfrak{b} = \beta_0^t(\mathfrak{a})$ is its image under β_0^t, then β_0^t carries the set of homogeneous elements of $\mathfrak{a}$ onto $\mathfrak{b}$.

PROOF. Every member of $\mathfrak{b}$ is the sum of the images under β_0^t of finitely many homogeneous members of $\mathfrak{a}$. If $F_1, \ldots, F_k$ are these homogeneous members, then it is enough to produce $G_1, \ldots, G_k$ in $\mathfrak{a}$ all homogeneous of the same degree such that $\beta_0^t(F_j) = \beta_0^t(G_j)$ for all j. If $d_1, \ldots, d_k$ are the respective degrees of $F_1, \ldots, F_k$ and if $d = \max(d_1, \ldots, d_k)$, then the elements $G_j = X_0^{d-d_j} F_j$ have the required properties. □

Lemma 10.17. Let $\mathfrak{a}$ be a homogeneous ideal of $\widetilde{A}$, and let $\mathfrak{b}$ be the ideal of A given by $\mathfrak{b} = \beta_0^t(\mathfrak{a})$. Then $\beta_0(V(\mathfrak{b})) = V(\mathfrak{a}) \cap \beta_0(\mathbb{A}^n)$.

PROOF. If $(x_1, \ldots, x_n)$ is in $V(\mathfrak{b})$ and if F is a homogeneous member of $\mathfrak{a}$, then $f = \beta_0^t(F)$ is in $\mathfrak{b}$ with $0 = f(x_1, \ldots, x_n) = F(\beta_0(x_1, \ldots, x_n))$. Since F is arbitrary, $\beta_0(x_1, \ldots, x_n)$ is in $V(\mathfrak{a})$. Thus $\beta_0(V(\mathfrak{b})) \subseteq V(\mathfrak{a}) \cap \beta_0(\mathbb{A}^n)$.

For the reverse inclusion, let $[1, x_1, \ldots, x_n]$ be in $V(\mathfrak{a}) \cap \beta_0(\mathbb{A}^n)$. If f is in $\mathfrak{b}$, find by Lemma 10.16 a homogeneous F in $\mathfrak{a}$ with $\beta_0^t F = f$. Since $[1, x_1, \ldots, x_n]$ is in $V(\mathfrak{a})$, $F(1, x_1, \ldots, x_n) = 0$. Therefore $f(x_1, \ldots, x_n) = F(\beta_0(x_1, \ldots, x_n)) = F(1, x_1, \ldots, x_n) = 0$. Since f is arbitrary in $\mathfrak{b}$, the point $(x_1, \ldots, x_n)$ is in $V(\mathfrak{b})$, and $\beta_0(V(\mathfrak{b})) \supseteq V(\mathfrak{a}) \cap \beta_0(\mathbb{A}^n)$. □

Proposition 10.18. Under the inclusion $\beta_0 : \mathbb{A}^n \to \mathbb{P}^n$, the Zariski topology of affine n-space $\mathbb{A}^n$ coincides with the relative topology from $\mathbb{P}^n$.

PROOF. If we start from an affine algebraic set $V(\mathfrak{b})$ in $\mathbb{A}^n$, then Lemma 10.17 shows that $\beta_0(V(\mathfrak{b})) = V(\mathfrak{a}) \cap \beta_0(\mathbb{A}^n)$ for the homogeneous ideal $\mathfrak{a} = (\beta_0^t)^{-1}(\mathfrak{b})$ in $\widetilde{A}$. Since $V(\mathfrak{a})$ is Zariski closed in $\mathbb{P}^n$, $\beta_0(V(\mathfrak{b}))$ is exhibited as closed in the relative topology on $\beta_0(\mathbb{A}^n)$.

Conversely suppose that C is closed in the relative topology on $\beta_0(\mathbb{A}^n)$. Then it is of the form $\widetilde{C} \cap \beta_0(\mathbb{A}^n)$ for some projective algebraic set $\widetilde{C}$. The set $\widetilde{C}$ is of the form $V(\mathfrak{a})$ for some homogeneous ideal $\mathfrak{a}$. If $\mathfrak{b} = \beta_0^t(\mathfrak{a})$, then Lemma 10.17 shows that

$$\beta_0(V(\mathfrak{b})) = V(\mathfrak{a}) \cap \beta_0(\mathbb{A}^n) = \widetilde{C} \cap \beta_0(\mathbb{A}^n) = C,$$

and C is exhibited as β_0^t of an affine algebraic set in $\mathbb{A}^n$. □

Corollary 10.19. If V is a quasi-affine variety in $\mathbb{A}^n$, then $\beta_0(V)$ is a quasiprojective variety in $\mathbb{P}^n$. Moreover, the geometric dimension of V as a quasi-affine variety equals the geometric dimension of $\beta_0(V)$ as a quasiprojective variety.

REMARKS. In other words, the closure $\overline{\beta_0(V)}$ is a projective variety. It is called the **projective closure** of the quasi-affine variety V. If V is actually an affine variety, then it has an associated prime ideal in A, and the projective variety $\overline{\beta_0(V)}$ has an associated homogeneous prime ideal in $\widetilde{A}$. The correspondence between the prime ideal in A and the homogeneous prime ideal in $\widetilde{A}$ will be examined shortly.

PROOF. Because of the homeomorphism given by Proposition 10.18, Lemma 10.10 as restated in the lemma's remarks applies with $Y = \beta_0(\mathbb{A}^n)$, $X = \mathbb{P}^n$, and E equal to the closure of V in $\mathbb{A}^n$. The conclusion is that the closure of E in $\mathbb{P}^n$ is a projective variety, and the first conclusion of the corollary is proved. The second conclusion is immediate from the version of Proposition 10.11 mentioned in the remarks with that proposition. □

To each index i with $0 \le i \le n$, we can associate in a similar way a function $\beta_i : \mathbb{A}^n \to \mathbb{P}^n$. The formula for β_i is $\beta_i(x_1, \dots, x_n) = [y_0, \dots, y_n]$, where $y_j = x_{j+1}$ for $j < i$, $y_i = 1$, and $y_j = x_j$ for $j > i$. Just as in Proposition 10.18, under each β_i, the Zariski topology of affine n-space $\mathbb{A}^n$ coincides with the relative topology from $\mathbb{P}^n$. One consequence is that the notion of **projective closure** is meaningful if formed relative to any β_i in place of β_0. Another consequence is that $\mathbb{P}^n$ has a covering by $n+1$ open sets $\beta_i(\mathbb{A}^n)$ that are each Zariski homeomorphic to $\mathbb{A}^n$. The functions β_i may be viewed as playing a role similar to the inverses of charts in the definition of a smooth manifold.

Having used β_0 to associate a projective variety in $\mathbb{P}^n$ to each affine variety in $\mathbb{A}^n$ by passage to the topological closure, we turn to what happens with ideals.

Distinct homogeneous ideals in $\widetilde{A}$ can map under β_0^t to the same ideal in A; for example the principal ideals (1) and (X_0) in $\widetilde{A}$ both map to (1) in A. Theorem 10.20 will show that we can associate a particularly nice ideal of $\widetilde{A}$ to each ideal of A in such a way that prime ideals of A correspond to those nice ideals of $\widetilde{A}$ that are prime. Under this correspondence the ideals for an affine variety and its projective closure will match. It will be apparent from the construction in the proof that the ideal of $\widetilde{A}$ is generated by all homogeneous polynomials $F = F(f)$ of the form

$$F(X_0, \ldots, X_n) = X_0^d f(X_1/X_0, \ldots, X_n/X_0)$$

whenever $f \neq 0$ is in the ideal of A and $\deg f = d$.

Theorem 10.20. As a mapping of ideals in $\widetilde{A}$ to ideals in A, β_0^t is one-one from the set $\widetilde{\mathcal{I}}$ of all homogeneous ideals $\mathfrak{a}$ of $\widetilde{A}$ such that $X_0 F \in \mathfrak{a}$ implies $F \in \mathfrak{a}$ onto the set $\mathcal{I}$ of all ideals of A. Under this one-one correspondence prime ideals correspond to prime ideals.

PROOF. We are going to construct a two-sided inverse to the mapping induced by β_0^t from ideals in $\widetilde{\mathcal{I}}$ to ideals in $\mathcal{I}$.

Let $A_{\leq d}$ be the $\Bbbk$ vector space of all members of A, including the 0 polynomial, of degree $\leq d$. The homomorphism β_0^t carries $\widetilde{A}_d$ linearly into $A_{\leq d}$, and it carries the basis of homogeneous monomials in $\widetilde{A}$ of total degree d onto the basis of all monomials in A of total degree $\leq d$. Thus $\beta_0^t : \widetilde{A}_d \to A_{\leq d}$ is one-one onto. Observe for any f in $A_{\leq d}$ that the formula

$$F(X_0, \ldots, X_n) = X_0^d f(X_1/X_0, \ldots, X_n/X_0)$$

defines a member of $\widetilde{A}_d$. If we write $F = \varphi_d(f)$ when f and F are related in this way, then the function φ_d is a one-one $\Bbbk$ linear map from $A_{\leq d}$ into $\widetilde{A}_d$ such that $\varphi_d \beta_0^t$ is the identity on $\widetilde{A}_d$. Because of finite dimensionality, $\beta_0^t : \widetilde{A}_d \to A_{\leq d}$ and $\varphi_d : A_{\leq d} \to \widetilde{A}_d$ are two-sided inverses of one another.

Suppose that an ideal $\mathfrak{b}$ in A is given. Define $\mathfrak{a}_d = \varphi_d(\mathfrak{b} \cap A_{\leq d})$, and put $\mathfrak{a} = \bigoplus_{d=0}^{\infty} \mathfrak{a}_d$. According to remarks in the paragraph with the definition of homogeneous ideal, $\mathfrak{a}$ is a homogeneous ideal if $G\mathfrak{a}_d \subseteq \mathfrak{a}_{d+e}$ whenever G is in $\widetilde{A}_e$. Define $g = \beta_0^t(G)$. This polynomial has $\deg g \leq e$ and $\varphi_e(g) = G$, since $\varphi_e : A_{\leq e} \to \widetilde{A}_e$ is a two-sided inverse of $\beta_0^t : \widetilde{A}_e \to A_{\leq e}$. If f is in $\mathfrak{b} \cap A_{\leq d}$, then gf is in $\mathfrak{b} \cap A_{\leq (d+e)}$, and thus $G\varphi_d(f) = \varphi_e(g)\varphi_d(f) = \varphi_{d+e}(gf)$ is in $\mathfrak{a}_{d+e}$. This proves that $\mathfrak{a}$ is a homogeneous ideal in $\widetilde{A}$.

Under the construction $\mathfrak{b} \mapsto \mathfrak{a}$, let us see that $\mathfrak{a}$ is in $\widetilde{\mathcal{I}}$. If $X_0 F$ is in $\mathfrak{a}_{d+1}$, then we can write $X_0 F = \varphi_{d+1}(g)$ for some g in $\mathfrak{b} \cap A_{\leq d+1}$. That is, $X_0 F(X_0, \ldots, X_n) = X_0^{d+1} g(X_1/X_0, \ldots, X_n/X_0)$. Then $F(X_0, \ldots, X_n) = X_0^d g(X_1/X_0, \ldots, X_n/X_0)$. This formula shows that g is in $A_{\leq d}$ and that $F =$

$\varphi_d(g)$. Hence F is in $\mathfrak{a}_d$. In other words, the construction $\mathfrak{b} \mapsto \mathfrak{a}$ carries members of $\mathcal{I}$ to members of $\widetilde{\mathcal{I}}$.

Under the construction $\mathfrak{b} \mapsto \mathfrak{a}$, the homogeneous ideal $\mathfrak{a}$ has the property that

$$\beta_0^t(\mathfrak{a}) = \beta_0^t\Big(\bigoplus_{d=0}^{\infty} \mathfrak{a}_d\Big) = \sum_{d=0}^{\infty} \beta_0^t(\mathfrak{a}_d) = \sum_{d=0}^{\infty} (\mathfrak{b} \cap A_{\le d}) = \mathfrak{b}.$$

Thus our construction starting from an ideal of A, passing to an ideal in the set $\widetilde{\mathcal{I}}$, and passing back to an ideal of A recovers the original ideal of A.

Now suppose that $\mathfrak{a}$ is in $\widetilde{\mathcal{I}}$. Put $\mathfrak{b} = \beta_0^t(\mathfrak{a})$. To see that the above passage to a member of $\widetilde{\mathcal{I}}$ recovers $\mathfrak{a}$ from $\mathfrak{b}$, we are to show that

$$\mathfrak{a} \cap \widetilde{A}_d = \varphi_d(\mathfrak{b} \cap A_{\le d}). \tag{$*$}$$

First we establish that

$$\beta_0^t(\mathfrak{a} \cap \widetilde{A}_d) = \beta_0^t(\mathfrak{a}) \cap A_{\le d}. \tag{$**$}$$

The inclusion $\subseteq$ in $(**)$ is easy because $\beta_0^t(\mathfrak{a} \cap \widetilde{A}_d) \subseteq \beta_0^t(\mathfrak{a})$ and $\beta_0^t(\widetilde{A}_d) \subseteq A_{\le d}$. For the reverse inclusion, let f be in $\beta_0^t(\mathfrak{a} \cap \widetilde{A}_k) \cap A_{\le d}$ for some k. This means that $\deg f \le d$ and that $f = \beta_0^t(G)$ with $G \in \mathfrak{a} \cap \widetilde{A}_k$. Without loss of generality, we may assume that $k \ge d$. Let F be the element $F = \varphi_{\deg f}(f)$ of $\widetilde{A}_{\deg f}$. Then $X_0^{k-\deg f} F = \varphi_k(f)$, and $\beta_0^t(X_0^{k-\deg f} F) = \beta_0^t \varphi_k(f) = f = \beta_0^t(G)$. Hence $X_0^{k-\deg f} F$ and G are members of $\widetilde{A}_k$ with the same value under β_0^t. Since β_0^t is one-one on $\widetilde{A}_k$, $G = X_0^{k-\deg f} F$. Since G is in $\mathfrak{a}$ and since the ideal $\mathfrak{a}$ is in $\widetilde{\mathcal{I}}$, F is in $\mathfrak{a}$. Hence the element $X_0^{d-\deg f} F$ is in $\mathfrak{a} \cap \widetilde{A}_d$, and it has $\beta_0^t(X_0^{d-\deg f} F) = f$. This proves the inclusion $\supseteq$ in $(**)$. Application of φ_d to both sides of $(**)$ proves $(*)$ and completes the proof of the first statement of the theorem.

We are to show that prime ideals correspond to prime ideals. Let $\mathfrak{b}$ in $\mathcal{I}$ be prime, and let $\mathfrak{a}$ be the ideal in $\widetilde{\mathcal{I}}$ with $\beta_0^t(\mathfrak{a}) = \mathfrak{b}$. Let F and G be homogeneous elements in $\widetilde{A}$ of respective degrees d and e with FG in $\mathfrak{a}$. Then fg lies in $\mathfrak{b}$, where $f = \beta_0^t(F)$ and $g = \beta_0^t(G)$, and one of f and g lies in $\mathfrak{b}$ because $\mathfrak{b}$ is prime. Say f is in $\mathfrak{b}$. Then $F = \varphi_d(f)$ lies in the right side of $(*)$ and hence lies in the left side. Consequently F is in $\mathfrak{a}$, and $\mathfrak{a}$ is prime.

Conversely let $\mathfrak{a}$ in $\widetilde{\mathcal{I}}$ be prime, and let $\mathfrak{b} = \beta_0^t(\mathfrak{a})$. Suppose that f and g are members of A with fg in $\mathfrak{b}$. Put $d = \deg f$ and $e = \deg g$, and define $F = \varphi_d(f)$ and $G = \varphi_e(g)$. Then $FG = \varphi_{d+e}(fg)$ is in $\varphi_{d+e}(\mathfrak{b} \cap A_{\le d+e})$, and $(*)$ shows that FG is in $\mathfrak{a} \cap \widetilde{A}_{d+e}$. Since $\mathfrak{a}$ is prime, one of F and G is in $\mathfrak{a}$. Say that F is in $\mathfrak{a}$. Then $f = \beta_0^t(F)$ is in $\mathfrak{b}$, and $\mathfrak{b}$ is prime. □

Corollary 10.21. The inclusion $\beta_0 : \mathbb{A}^n \to \mathbb{P}^n$ sets up a one-one correspondence between the prime ideals in A and those prime homogeneous ideals in $\widetilde{A}$ that do not contain X_0.

PROOF. If $\mathfrak{a}$ is a prime homogeneous ideal in $\widetilde{A}$ and $X_0 F$ is in $\mathfrak{a}$, then either X_0 or F is in $\mathfrak{a}$. If we can always exclude X_0 from being in $\mathfrak{a}$, then F is in $\mathfrak{a}$, and the condition in the proposition for $\mathfrak{a}$ to be in $\widetilde{\mathcal{I}}$ is satisfied. The rest follows from Theorem 10.20. □

Corollary 10.22. Let $\mathfrak{a}$ be a prime homogeneous ideal of $\widetilde{A}$ not containing X_0, and let $\mathfrak{b} = \beta_0^t(\mathfrak{a})$ be the corresponding prime ideal of A. Then the Zariski closure in $\mathbb{P}^n$ of $\beta_0(V(\mathfrak{b}))$ is $V(\mathfrak{a})$.

REMARKS. In other words, if an affine variety V has $\mathfrak{b}$ as its ideal in A, then the projective closure of V has the corresponding $\mathfrak{a}$ from Theorem 10.20 as its ideal in $\widetilde{A}$.

PROOF. Corollary 10.19 shows that $\overline{\beta_0(V(\mathfrak{b}))} = V(\mathfrak{a}')$ for some prime homogeneous ideal of $\widetilde{A}$. Since $\beta_0(V(\mathfrak{b})) \subseteq V(\mathfrak{a})$ by Lemma 10.17 and since $V(\mathfrak{a})$ is closed in $\mathbb{P}^n$, $V(\mathfrak{a}') \subseteq V(\mathfrak{a})$. Arguing by contradiction, suppose that the inclusion is strict. Applying $I(\cdot)$ and using Proposition 10.12b, we obtain $\mathfrak{a}' \supseteq \mathfrak{a}$. Since application of $V(\cdot)$ to both sides of $\mathfrak{a}' \supseteq \mathfrak{a}$ has to yield a strict inclusion, we must have $\mathfrak{a}' \supsetneqq \mathfrak{a}$. Choose G homogeneous in $\mathfrak{a}'$ that is not in $\mathfrak{a}$, and put $f = \beta_0^t G$. If $(x_1, \dots, x_n)$ is in $V(\mathfrak{b})$, then $[1, x_1, \dots, x_n]$ is in $\beta_0(V(\mathfrak{b})) \subseteq V(\mathfrak{a}')$, and hence $f(x_1, \dots, x_n) = G(1, x_1, \dots, x_n) = 0$. Thus f is in $I(V(\mathfrak{b})) = \mathfrak{b}$. Since $\deg f \le \deg G$, the construction of $\mathfrak{a}$ from $\mathfrak{b}$ in the proof of Theorem 10.20 shows that $F = \varphi_{\deg G}(f)$ is in $\mathfrak{a}$. Then G and F are members of $\widetilde{A}_{\deg G}$ with $\beta_0^t(G) = f = \beta_0^t(F)$, and we obtain $G = F$, contradiction. □

EXAMPLE. Twisted cubic from the example in Section 1 and Example 2 in Section 2. The prime ideal $\mathfrak{b} \subseteq \Bbbk[X, Y, Z]$ is $(Y - X^2, Z - X^3)$, and we want to find the corresponding ideal $\mathfrak{a}$ given by Corollary 10.21. Let the additional indeterminate in $\widetilde{A}$ be W. Applying φ_2 and φ_3 to the respective generators $Y - X^2$ and $Z - X^3$ yields $WY - X^2$ and $W^2Z - X^3$. These must be in $\mathfrak{a}$. So must

$$(W^2Z - X^3) - X(WY - X^2) = W(WZ - XY)$$

and
$$X(W^2Z - X^3) - (WY + X^2)(WY - X^2) = W^2(XZ - Y^2).$$

Since we seek a prime ideal for $\mathfrak{a}$ and W is not to be in $\mathfrak{a}$, $WZ - XY$ and $XZ - Y^2$ are in $\mathfrak{a}$. Thus $\mathfrak{a} \supseteq (WY - X^2, WZ - XY, XZ - Y^2)$. If $\mathfrak{c}$ denotes the ideal on the right, then $\mathfrak{a} \supseteq \mathfrak{c}$ and

$$\begin{aligned}\beta_0^t(\mathfrak{c}) &= (Y - X^2, Z - XY, XZ - Y^2)\\ &= (Y - X^2, Z - X^3, XZ - X^4) = (Y - X^2, Z - X^3) = \beta_0^t(\mathfrak{a}).\end{aligned}$$

To show that $\mathfrak{a} = \mathfrak{c}$, it is enough according to Theorem 10.20 to show that if F is homogeneous and WF is in $\mathfrak{c}$, then F is in $\mathfrak{c}$. The three generators of $\mathfrak{c}$ are all in $\widetilde{A}_2$, and thus $\mathfrak{c} \cap \widetilde{A}_d = \widetilde{A}_{d-2}(\mathfrak{c} \cap \widetilde{A}_2)$. Hence it is enough to show that $\mathfrak{c} \cap \widetilde{A}_2$ contains no nonzero element divisible by W. Since $\mathfrak{c} \cap \widetilde{A}_2$ consists of all linear combinations of the three generators, we can check this fact by inspection. The result is that $\mathfrak{a} = \mathfrak{c}$. Once we know $\mathfrak{a}$, we can compute the projective closure of the twisted cubic from Corollary 10.22. We find that it consists of all $[w, x, y, z]$ of the form $[1, x, x^2, x^3]$ together with $[0, 0, 0, 1]$. We might have guessed this form for the projective closure from the parametric realization of the twisted cubic in $\mathbb{A}^3$ and from a passage to the limit, but proceeding in that fashion requires operations that we have certainly not justified.

4. Rational Functions and Regular Functions

We continue to assume that $\Bbbk$ is an algebraically closed field and to write A for $\Bbbk[X_1, \ldots, X_n]$ and $\widetilde{A}$ for $\Bbbk[X_0, \ldots, X_n]$. In this section we investigate certain classes of $\Bbbk$-valued functions on quasiprojective varieties, specifically the "rational" functions, the "regular" functions, and the local ring of functions regular at a particular point. For each kind of variety that we have introduced (affine, quasi-affine, projective, and quasiprojective), there are simple global definitions and there are complicated but *equivalent* local definitions for these notions. The complicated definitions have three advantages over the simple ones: they are virtually the same for all four kinds of varieties and therefore make it possible to work with all kinds of varieties uniformly, they make it possible in practice to construct a function by constructing only a local part of it, and they prepare the way better for a definition of isomorphism of varieties that does not insist on a particular dimension for the ambient affine or projective space.

In this section we shall first give the simple definitions in the affine and quasi-affine cases and then prove results saying that certain more complicated local-sounding versions of these definitions amount to the same thing as the simple definitions. Then we shall give the simple definitions in the projective and quasiprojective cases. Finally we shall relate the quasi-affine and quasiprojective cases and show that certain more complicated local-sounding definitions in the quasiprojective case amount to the same thing as the simple definitions.

We begin with affine varieties. Suppose that $V = V(\mathfrak{p})$ is an affine variety in $\mathbb{A}^n$, $\mathfrak{p}$ being a prime ideal in A. The **affine coordinate ring** of V is $A(V) = A/\mathfrak{p}$, which is an integral domain. Let us write the quotient homomorphism $A \to A(V)$ as $a \mapsto \bar{a}$. Because of the Nullstellensatz, $A(V)$ can be identified with the ring of all restrictions of polynomials to V; in particular, $\bar{a}(P)$ is meaningful for every $\bar{a} \in A(V)$ and $P \in V$.

Proposition 10.23. If V is an affine variety in $\mathbb{A}^n$, then the points P of V are in one-one correspondence with the maximal ideals $\mathfrak{m}_P$ of the affine coordinate ring $A(V)$, the correspondence being that $\mathfrak{m}_P$ is the maximal ideal of all members $\bar{a}$ of $A(V)$ with $\bar{a}(P) = 0$.

PROOF. Each $\mathfrak{m}_P$ is a maximal ideal, being the kernel of a multiplicative linear functional. In the reverse direction, if $\mathfrak{m}$ is a maximal ideal of $A(V)$, then its inverse image in A under the homomorphism $A \to A/\mathfrak{p} = A(V)$ is a maximal ideal M of A containing $\mathfrak{p}$, by the First Isomorphism Theorem. The Nullstellensatz shows that M consists of all polynomials vanishing at some point P. Applying $V(\cdot)$ to the inclusion $M \supseteq \mathfrak{p}$ gives $\{P\} = V(M) \subseteq V(\mathfrak{p}) = V$. Thus P is in V. □

Members of the field of fractions $\Bbbk(V)$ of $A(V)$ are called **rational functions** on V, and $\Bbbk(V)$ is called the **function field** on V. Rational functions on V are not really functions on V in the traditional sense, since their denominators can vanish here and there. By way of compensation, an allowable denominator never vanishes identically; the reason is that the construction of a field of fractions of an integral domain does not involve using the zero element of the integral domain in a denominator. If f is a rational function on V and P is in V, one says that f is **regular** at P, or **defined** at P, if there exist $\bar{a}$ and $\bar{b}$ in $A(V)$ with $\bar{b}(P) \neq 0$ such that $f = \bar{a}/\bar{b}$. In this case, an equality $\bar{a}/\bar{b} = \bar{a}'/\bar{b}'$ with $\bar{b}(P) \neq 0$ and $\bar{b}'(P) \neq 0$ implies that $\bar{a}\bar{b}' = \bar{a}'\bar{b}$, from which we see that $\bar{a}(P)\bar{b}'(P) = \bar{a}'(P)\bar{b}(P)$ and that $\bar{a}(P)/\bar{b}(P) = \bar{a}'(P)/\bar{b}'(P)$. Hence $f(P)$ can be defined unambiguously as $f(P) = \bar{a}(P)/\bar{b}(P)$. For P in V, the set of rational functions on V that are regular at P is a $\Bbbk$ algebra, as we see by carrying out the usual manipulations to add or multiply fractions. This $\Bbbk$ algebra is denoted by $\mathcal{O}_P(V)$. It has $A(V) \subseteq \mathcal{O}_P(V) \subseteq \Bbbk(V)$.

As in Proposition 10.23, let $\mathfrak{m}_P$ be the maximal ideal of all members $\bar{a}$ of $A(V)$ with $\bar{a}(P) = 0$. The localization of $A(V)$ with respect to this maximal ideal is exactly $\mathcal{O}_P(V)$. In fact, the localization is a subring of $\Bbbk(V)$ because $A(V)$ is an integral domain. The members of $\mathcal{O}_P(V)$ are exactly the quotients $f = \bar{a}/\bar{b}$ with $\bar{a}$ and $\bar{b}$ in $A(V)$ and with $\bar{b}$ not in $\mathfrak{m}_P$. Hence $\mathcal{O}_P(V) = S^{-1}A(V)$, where S is the set-theoretic complement of $\mathfrak{m}_P$. Thus $\mathcal{O}_P(V)$ is the asserted localization. It has a unique maximal ideal and is called the **local ring** of V at P.

A rational function is said to be **regular** on an open subset U of V if it is regular at every point of U. The regular functions on U form a $\Bbbk$ algebra denoted by $\mathcal{O}(U)$. In symbols the definition of $\mathcal{O}(U)$ is $\mathcal{O}(U) = \bigcap_{P \in V} \mathcal{O}_P(V)$.

When $A(V)$ is a unique factorization domain, the definition of regular at a point is simple enough to implement globally: we write $f = \bar{a}/\bar{b}$ in some fashion, reduce the fraction to lowest terms, and then read off all the points P for which f is defined from the single expression of f as a quotient. Ordinarily,

however, $A(V)$ is not a unique factorization domain, and then the definition is more subtle, as the following example shows.

EXAMPLE. $V = V(\mathfrak{p})$ with $\mathfrak{p} = (XW - YZ)$ and $n = 4$. The polynomial $XW - YZ$ is irreducible, and thus V is an affine variety in $\mathbb{A}^4$. The affine coordinate ring is $A(V) = \Bbbk[W, X, Y, Z]/(XW - YZ)$. The quotient $f = \overline{X}/\overline{Y}$ is a rational function on V, since $\overline{Y}$ is not the 0 element of $A(V)$, and the definition shows that f is regular at all points (w, x, y, z) of V having $y \neq 0$. From $\overline{X}\,\overline{W} - \overline{Y}\,\overline{Z} = 0$, we have $\overline{X}/\overline{Y} = \overline{Z}/\overline{W}$, and thus f is defined also at all points (w, x, y, z) of V having $w \neq 0$. For example it is defined at the additional point $(w, x, y, z) = (1, 0, 0, 0)$. Actually, there exist no members $\bar{a}$ and $\bar{b}$ of $A(V)$ with $f = \bar{a}/\bar{b}$ and $\bar{b}(w, x, y, z) \neq 0$ whenever $xw = yz$ and one or both of w and y are nonzero. The details are carried out in Problem 8 at the end of the chapter.

The set of points P in the affine variety V at which a rational function f on V fails to be regular is called the **pole set** of f.

Proposition 10.24. If f is a rational function on the affine variety $V = V(\mathfrak{p})$, then the pole set of f is the affine algebraic set $V(\mathfrak{a}) \subseteq V(\mathfrak{p})$ corresponding to the ideal $\mathfrak{a} \supseteq \mathfrak{p}$ of all $b \in A$ such that $\bar{b}f$ is in $A(V)$.

PROOF. The set $\mathfrak{a}$ in the statement is an ideal in A that contains $\mathfrak{p}$. Hence $V(\mathfrak{a}) \subseteq V(\mathfrak{p})$. If P is in $V(\mathfrak{p})$ and f is defined at P, then there are members $\bar{a}$ and $\bar{b}$ of $A(V)$ with $\bar{b}(P) \neq 0$ such that $\bar{b}f = \bar{a}$; any representative of this $\bar{b}$ in A lies in $\mathfrak{a}$, and consequently P is not in $V(\mathfrak{a})$. Conversely if f is not defined at P, then no $\bar{b}$ such that $\bar{b}f$ is in $A(V)$ has $\bar{b}(P) \neq 0$. That is, no member b of $\mathfrak{a}$ has $\bar{b}(P) \neq 0$. So P is in $V(\mathfrak{a})$. This proves that the pole set of f is exactly $V(\mathfrak{a})$. □

Corollary 10.25. If $V = V(\mathfrak{p})$ is an affine variety, then

$$A(V) = \bigcap_{P \in V} \mathcal{O}_P(V).$$

REMARKS. In the notation introduced above, the corollary says that $A(V) = \mathcal{O}(V)$.

PROOF. The inclusion $\subseteq$ follows from the fact that $A(V) \subseteq \mathcal{O}_P(V)$ for each P. For the reverse inclusion, suppose that f lies in $\bigcap_{P \in V} \mathcal{O}_P(V)$. Then the pole set of f in V is empty. The pole set for f is the set $V(\mathfrak{a})$ for the ideal $\mathfrak{a}$ in Proposition 10.24, and it follows from the Nullstellensatz that $\mathfrak{a} = A$. Then 1 is in $\mathfrak{a}$, and the definition of $\mathfrak{a}$ shows that f is in $A(V)$. □

If we consider the complement of the pole set of f, then we see from Proposition 10.24 that the subset of V at which f is regular is (relatively) open in V. Hence it is empty or dense in V. On the set where f is regular, f is continuous into $\mathbb{A}^1$, according to the following proposition.

Proposition 10.26. If a rational function f on the affine variety V is regular on the nonempty open set U of V, then it is continuous from U into $\mathbb{A}^1$ with the Zariski topology (in which the proper closed sets are the finite sets).

PROOF. It is to be proved that f^{-1} of any finite subset of $\mathbb{A}^1$ is relatively closed in U. Since the finite union of closed sets is closed, it is enough to consider $f^{-1}(\{c\})$ for an element c of $\Bbbk$. This is the intersection with U of the pole set of $1/(f-c)$, which is relatively closed in U by Proposition 10.24. □

Now we can give the simple definitions in the quasi-affine case. Let the quasi-affine variety U in $\mathbb{A}^n$ have closure the affine variety V. If f is a rational function on V, then Proposition 10.24 shows that f is regular on a nonempty open subset of V. Since the intersection of any two nonempty open subsets is nonempty, f is regular on a nonempty open subset of U. Therefore it is meaningful to view f as a rational function on U. We define the **function field** of **rational functions** on U to be the same as the function field of V: $\Bbbk(U) = \Bbbk(V)$. The definition of **regular function** at P is the same for the quasi-affine variety U as for its Zariski closure V, and thus the **local ring** of U at P is given by $\mathcal{O}_P(U) = \mathcal{O}_P(V)$. A rational function is said to be **regular** on the quasi-affine variety U if it is regular at every point of U. Since $\Bbbk(U) = \Bbbk(V)$, the set of regular functions on U is the $\Bbbk$ algebra $\mathcal{O}(U) = \bigcap_{P \in U} \mathcal{O}_P(U)$.

The next step is to prove results saying that certain more complicated local-sounding definitions of the above notions amount to the same thing.

Lemma 10.27. If V is an affine variety, then any two members of the affine coordinate ring $A(V)$ that are equal on a nonempty open subset of V are the same.

PROOF. Subtracting, we may suppose that $\bar{a} \in A(V)$ is 0 on the nonempty open subset U of V. By Proposition 10.26, $\bar{a}$ is continuous from V into $\mathbb{A}^1$. The complement of $\bar{a}^{-1}(\{0\})$ has to be open in V and disjoint from U, and therefore it is empty. So $\bar{a}$ is everywhere 0 and is the 0 element of $A(V)$. □

Proposition 10.28. Let U be a nonempty open subset of the affine variety V in $\mathbb{A}^n$. Suppose that $f_0 : U \to \Bbbk$ is a function with the following property: for each P in U, there exist an open subset W of U containing P and polynomials a and b in A such that b is nowhere vanishing on W and $f_0 = a/b$ on W. Then there exists one and only one member f of $\Bbbk(V)$ such that f is regular on U and agrees with f_0 at every point of U.

REMARKS. For the quasi-affine case the more complicated local-sounding definition of "regular function" on U, mentioned in the first paragraph of this section, is what is assumed of f_0 in the statement of this proposition. The proposition says that such an f_0 necessarily comes from a global rational function on V that is regular on U in the sense just above.

PROOF OF UNIQUENESS. If there are two such members of $\Bbbk(V)$, then subtracting them gives a member g of $\Bbbk(V)$ that is 0 on U. By definition of $\Bbbk(V)$, $g = \bar{a}/\bar{b}$ with $\bar{a}$ and $\bar{b}$ in $A(V)$ with with $\bar{b} \neq 0$. Then $\bar{a} = g\bar{b}$ is a member of $A(V)$ that is 0 on U. By Lemma 10.27, $\bar{a} = 0$ in $A(V)$. Thus $g\bar{b} = 0$ in $\Bbbk(V)$. Since $\Bbbk(V)$ is a field and $\bar{b} \neq 0$, $g = 0$. □

PROOF OF EXISTENCE. If P is in U, then the hypothesis supplies some open subset W of U containing P and members a and b of A with b nowhere 0 on W and with $f_0 = a/b$ on W. Let $\bar{a}$ and $\bar{b}$ be the images of a and b in $A(V)$. Since b is not identically 0 on U, $\bar{b}$ is not the 0 element of $A(V)$. Therefore $f = \bar{a}/\bar{b}$ is a well-defined member of $\Bbbk(V)$, and it is regular on W and agrees with f_0 there. If we start with another point P' and an open subset W' of U containing P', then we similarly obtain $f' = \bar{a}'/\bar{b}'$ in $\Bbbk(V)$ that is regular on W' and agrees with f_0 there. The open subset $W \cap W'$ is nonempty, and $\bar{a}/\bar{b} = \bar{a}'/\bar{b}'$ on $W \cap W'$. Therefore $\bar{b}'\bar{a} = \bar{b}\bar{a}'$ on $W \cap W'$. By Lemma 10.27, $\bar{b}'\bar{a} = \bar{b}\bar{a}'$ as members of $A(V)$. Dividing, we obtain $f = f'$. Since the member f of $\Bbbk(V)$ is regular on an open neighborhood of each point of U, it is regular on U. □

Proposition 10.28 allows us also to give a local-sounding definition of rational function and see that it reduces to the original definition. Specifically we consider pairs (U_0, f_0) with U_0 nonempty open in the quasi-affine variety U and with f_0 satisfying the regularity condition on U_0 in the proposition.[11] Say that the pair (U_0, f_0) is equivalent to the pair (U_1, f_1) if $f_0 = f_1$ on $U_0 \cap U_1$. This relation is reflexive and symmetric. Let us see from the proposition why it is transitive. If (U_0, f_0) is equivalent to (U_1, f_1), then the existence part of the proposition yields three members of $\Bbbk(V)$—one for (U_0, f_0), one for $(U_0 \cap U_1, f_0) = (U_0 \cap U_1, f_1)$, and one for (U_1, f_1). The uniqueness part shows that the first two members of $\Bbbk(V)$ are equal and the last two are equal. Hence they are all equal. Now if (U_0, f_0) is equivalent to (U_1, f_1) and (U_1, f_1) is equivalent to (U_2, f_2), then we routinely find that $(U_0 \cap U_1, f_0)$ is equivalent to $(U_1 \cap U_2, f_2)$. From what we have just seen, (U_0, f_0) is equivalent to (U_2, f_2), and the relation is therefore transitive. We could take the union of all the sets U_0 appearing in the pairs within an equivalence class and obtain the **largest domain** within U on which the rational function in question is regular. This notion for a rational function will not be too useful for us, but an analogous notion for rational maps in Section 6 will be quite handy.

In similar fashion the local ring $\mathcal{O}_P(U)$ can be formulated in terms of "germs" of regular functions as follows. Fix P in U, and consider all pairs (U_0, f_0) such that U_0 is an open subset of U containing P and f_0 is a scalar-valued function on

[11] That is, for each P in U_0, there exist an open subset W of U_0 containing P and polynomials a and b in A such that b is nowhere vanishing on W and $f_0 = a/b$ on W.

U_0 satisfying the regularity condition on U_0 in the proposition.[12] Say that (U_0, f_0) is equivalent to (U_1, f_1) if $f_0 = f_1$ on some open neighborhood of U containing P. It is easy to see that the result is an equivalence relation. An equivalence class is called a **germ** of regular functions at P. Germs inherit a natural addition, scalar multiplication, and multiplication, and the set of germs at P is therefore a $\Bbbk$ algebra. The use of germs is the traditional device in mathematics for isolating local behavior of functions in arbitrarily small neighborhoods of points.

Corollary 10.29. Let U be a nonempty open subset of the affine variety V in $\mathbb{A}^n$, and let P be in U. To each germ $\{(U_0, f_0)\}$ of regular functions at P corresponds one and only one member f of $\Bbbk(V)$ that is associated via Proposition 10.28 to each pair (U_0, f_0). Moreover, this correspondence is a $\Bbbk$ algebra isomorphism of the ring of germs onto the local ring $\mathcal{O}_P(U)$.

PROOF. If (U_0, f_0) and (U_0', f_0') are two pairs in a germ at P, then the definition of germ gives a pair (W, g_0) such that W is a neighborhood of P contained in $U_0 \cap U_0'$ and g agrees with f_0 and f_0' on W. Proposition 10.28 supplies unique members f, f', and g of $\Bbbk(V)$ such that f is regular on U_0 and agrees with f_0 there, such that f' is regular on U_0' and agrees with f_0' there, and such that g is regular on W and agrees with g_0 there. The uniqueness in the proposition shows that $f = g$ and that $g = f'$. Therefore $f = f'$. So we have a well-defined map of germs into $\Bbbk(V)$.

The image f of the pair (U_0, f_0) is a member of $\Bbbk(V)$ that is regular on U_0, hence is defined at P. Thus the map on germs is into $\mathcal{O}_P(U)$. It is a $\Bbbk$ algebra homomorphism because of the definitions of the operations on germs. If the germ of (U_0, f_0) maps to 0, then f_0 is the 0 function on U_0, and any representative (W, g_0) of the germ with $W \subseteq U_0$ has g_0 equal to the 0 function on W. Thus the germ is the 0 germ, and the $\Bbbk$ algebra homomorphism is one-one. Finally if f is a member of $\mathcal{O}_P(U)$, then $f = \bar{a}/\bar{b}$ with $\bar{a}$ and $\bar{b}$ in $A(V)$ and with $\bar{b}$ nonvanishing at P. By Proposition 10.26, $\bar{b}$ is nonvanishing on some open neighborhood U_0 of P. Then the germ of (U_0, f_0) maps to f if f_0 is defined as the restriction of $\bar{a}/\bar{b}$ to U_0. Therefore the $\Bbbk$ algebra homomorphism is onto $\mathcal{O}_P(U)$. □

This completes the discussion of the definitions in the cases of affine and quasi-affine varieties. Next we consider projective varieties, beginning with the simple definitions. Let $V = V(\mathfrak{p})$ be a projective variety, $\mathfrak{p}$ being a prime homogeneous ideal in $\widetilde{A}$ different from $\bigoplus_{d\geq 1} \widetilde{A}_d$. The integral domain $\widetilde{A}(V) = \widetilde{A}/\mathfrak{p}$ is called the **homogeneous coordinate ring** of V. Since $\mathfrak{p}$ is homogeneous, we can write $\widetilde{A}(V)$ as

$$\widetilde{A}(V) = \bigoplus_{d=0}^{\infty} \widetilde{A}_d \big/ (\widetilde{A}_d \cap \mathfrak{p}) = \bigoplus_{d=0}^{\infty} \widetilde{A}(V)_d.$$

[12] See the previous footnote.

Let us write the quotient homomorphism $\widetilde{A} \to \widetilde{A}(V)$ as $F \mapsto \overline{F}$. We say that $\overline{F}$ is **homogeneous** of degree d if it lies in $\widetilde{A}(V)_d = \widetilde{A}_d \big/ (\widetilde{A}_d \cap \mathfrak{p})$.

Despite Proposition 10.12, homogeneous members of $\widetilde{A}(V)$ do not yield well-defined functions on V, and we cannot simply imitate the affine case in defining the function field of V. The **function field** $\Bbbk(V)$ of V is a certain *proper* subfield of the field of fractions of $\widetilde{A}(V)$, namely the set of all quotients $\overline{F}/\overline{G}$ with $\overline{F}$ and $\overline{G}$ homogeneous of the same degree and with $\overline{G} \neq 0$. If the common degree of $\overline{F}$ and $\overline{G}$ is d, then the quotient $\overline{F}/\overline{G}$ is homogeneous of degree 0 in $(x_0, \ldots, x_n)$ and is therefore well-defined on the equivalence class $[x_0, \ldots, x_n]$ in $\mathbb{P}^n$. Such quotients form a field because if $\overline{F}_1$ and $\overline{G}_1$ are homogeneous of degree d and $\overline{F}_2$ and $\overline{G}_2$ are homogeneous of degree e, then $\overline{F}_1/\overline{G}_1 + \overline{F}_2/\overline{G}_2 = (\overline{F}_1\,\overline{G}_2 + \overline{G}_1\,\overline{F}_2)/(\overline{G}_1\,\overline{G}_2)$ and $(\overline{F}_1\,\overline{F}_2)/(\overline{G}_1\,\overline{G}_2)$ are each the quotient of two members of $\widetilde{A}(V)$ that are homogeneous of degree $d + e$, the denominator not being the zero element, and because the inverse of $\overline{F}/\overline{G}$ is $\overline{G}/\overline{F}$. Elements of $\Bbbk(V)$ are called **rational functions** on V.

Although the values of homogeneous members of $\widetilde{A}$ are not meaningful on $\mathbb{P}^n$, the zero locus of such a polynomial *is* well defined. If $\overline{F}$ is a member of the quotient $\widetilde{A}(V)$ homogeneous of degree d, then its set of preimages in $\widetilde{A}_d$ is $F + (\widetilde{A}_d \cap \mathfrak{p})$. The members of $\widetilde{A}_d \cap \mathfrak{p}$ all vanish at every point of V, and therefore whether F vanishes at a point P of V depends only on the coset of F in $\widetilde{A}(V)$. Accordingly, a member h of $\Bbbk(V)$ is said to be **regular** at the point $P = [x_0, \ldots, x_n]$ of V, or **defined** at P, if h can be written as a quotient $h = \overline{F}/\overline{G}$ of homogeneous members of $\widetilde{A}(V)$ of the same degree in such a way that $\overline{G}(P) \neq 0$. In this case, $h(P)$ is well defined as the quotient $F(x_0, \ldots, x_n)/G(x_0, \ldots, x_n)$ for any $(x_0, \ldots, x_n)$ representing the point $P = [x_0, \ldots, x_n]$.

The set of points P in the projective variety V at which a rational function h on V fails to be regular is called the **pole set** of h. The proof of the following result is similar to the proof of Proposition 10.24 and is therefore omitted.

Proposition 10.30. If h is a rational function on the projective variety $V = V(\mathfrak{p})$, then the pole set of h is the projective algebraic set $V(\mathfrak{a}) \subseteq V(\mathfrak{p})$ corresponding to the homogeneous ideal $\mathfrak{a} \supseteq \mathfrak{p}$ generated by all homogeneous $G \in \widetilde{A}$ such that $\overline{G}h$ is in $\widetilde{A}(V)$.

As in the case of affine varieties, the set of members of $\Bbbk(V)$ regular at P in V is a $\Bbbk$ subalgebra of $\Bbbk(V)$ called the **local ring** of V at P and denoted by $\mathcal{O}_P(V)$.

Corollary 10.31. If $V = V(\mathfrak{p})$ is a projective variety, then

$$\Bbbk = \bigcap_{P \in V} \mathcal{O}_P(V).$$

REMARKS. The classical prototype of this corollary is that a rational function without poles on the Riemann sphere is constant. A direct proof of this fact for the Riemann sphere in the style of this book follows by applying Proposition 6.9 to the sum of the given rational function and any constant function. A generalization appears as Corollary 9.4.

PROOF. The inclusion $\subseteq$ is automatic. For the reverse inclusion, suppose that the rational function h on V lies in $\bigcap_{P\in V} \mathcal{O}_P(V)$. Then the pole set of h in V is empty. The pole set for h is the set $V(\mathfrak{a})$ for the ideal $\mathfrak{a}$ in Proposition 10.30, and it follows from the homogeneous Nullstellensatz (Proposition 10.12a) that $\widetilde{A}_N \subseteq \mathfrak{a}$ for all N sufficiently large. For any such N, $\widetilde{A}(V)_N\, h$ lies in $\widetilde{A}(V)$. It is homogeneous of degree N and hence is in $\widetilde{A}(V)_N$. Iterating this inclusion gives

$$\widetilde{A}(V)_N\, h^k \subseteq \widetilde{A}(V)_N \quad \text{for all } k \geq 0. \tag{$*$}$$

Since V is nonempty, some X_j is not in $\mathfrak{p}$; to fix the notation, let us suppose that X_0 is not in $\mathfrak{p}$. Then $\overline{X_0} \neq 0$. Inclusion $(*)$ shows that $\overline{X_0}^N h^k$ lies in $\widetilde{A}(V)$ for all $k \geq 0$. Thus h^k lies in the subset $\overline{X_0}^{-N} \widetilde{A}(V)$ of the field of fractions of $\widetilde{A}(V)$, and the ring $\widetilde{A}(V)[h]$, given by the substitution homomorphism $X \mapsto h$ applied to the polynomial ring $\widetilde{A}(V)[X]$, is exhibited as an $\widetilde{A}(V)$ submodule of the finitely generated $\widetilde{A}(V)$ module $\overline{X_0}^{-N} \widetilde{A}(V)$ of the field of fractions of $\widetilde{A}(V)$. Since $\widetilde{A}(V)$ is Noetherian as a homomorphic image of $\widetilde{A}$, $\widetilde{A}(V)[h]$ is a finitely generated $\widetilde{A}(V)$ module. By Proposition 8.35 of *Basic Algebra*, h is a root of some monic polynomial in $\widetilde{A}(V)[X]$. Say that h satisfies

$$h^l + c_{l-1}h^{l-1} + \cdots + c_1 h + c_0 = 0$$

with each c_j in $\widetilde{A}(V)$. Decomposing each term into homogeneous parts and equating to 0 the sum of the terms homogeneous of degree 0 shows that we can assume each c_j to be in $\widetilde{A}(V)_0 = \Bbbk$. That is, we may assume that h is algebraic over $\Bbbk$. Since $\Bbbk$ is algebraically closed, h is in $\Bbbk$. □

If we consider the complement of the pole set of h, then we see from Proposition 10.30 that the subset of V at which h is regular is open in V. Hence it is empty or dense in V. On the set where h is regular, h is continuous into $\mathbb{A}^1$, according to the following proposition, whose proof is the same as for Proposition 10.26.

Proposition 10.32. If a rational function h on the projective variety V is regular on the nonempty open set U of V, then it is continuous from U into $\mathbb{A}^1$ with the Zariski topology (in which the proper closed sets are the finite sets).

The procedure for extending the above remarks from projective varieties to quasiprojective varieties is the same as for extending the earlier remarks from affine varieties to quasi-affine varieties. Let the quasiprojective variety U in $\mathbb{P}^n$ have closure the projective variety V. If h is a rational function on V, then Proposition 10.32 shows that h is regular on a nonempty open subset of V. Since the intersection of any two nonempty open subsets is nonempty, h is regular on a nonempty open subset of U. Therefore it is meaningful to view h as a rational function on U. Thus we define the **function field** of U to be the same as the function field of V: $\Bbbk(U) = \Bbbk(V)$. The definition of **regular function** at P is the same for the quasiprojective variety U as for its Zariski closure V, and thus the **local ring** of U at P is given by $\mathcal{O}_P(U) = \mathcal{O}_P(V)$. A rational function is said to be **regular** on the quasiprojective variety U if it is regular at every point of U. The set of regular functions on U is a $\Bbbk$ algebra denoted by $\mathcal{O}(U)$. Thus

$$\mathcal{O}(U) = \bigcap_{P \in U} \mathcal{O}_P(U).$$

For the special case that $U = V$, Corollary 10.31 shows that $\mathcal{O}(V)$ reduces to the constants.

The next step is to check that the simple definitions in this section in the affine and quasi-affine cases are consistent with the simple definitions in the projective and quasi-projective cases. Proposition 10.18 and Corollary 10.19 tell us the extent of the overlap—that any of the mappings $\beta_j : \mathbb{A}^n \to \mathbb{P}^n$ with $0 \le j \le n$ allows us to identify any quasi-affine variety with a quasiprojective variety. Thus what we need to show is that the definitions of function field, functions regular at a point, and functions regular on a variety amount to the same thing for a quasi-affine variety U and for the quasiprojective variety $\beta_j(U)$. For concreteness we shall take $j = 0$.

Corollaries 10.21 and 10.22 tell us exactly what we are to compare. The prime ideals $\mathfrak{a}$ of $\widetilde{A}$ not containing X_0 are in one-one correspondence with the prime ideals $\mathfrak{b}$ of A, the correspondence being $\mathfrak{b} = \beta_0^t(\mathfrak{a})$, and the Zariski closure of $V(\beta_0^t(\mathfrak{b}))$ in $\mathbb{P}^n$ is $V(\mathfrak{a})$. The correspondence does not yield a natural map of $\mathfrak{b}$ into $\mathfrak{a}$. Instead, the system of linear mappings $\varphi_d : A_{\le d} \to \widetilde{A}_d$ given by

$$F(X_0, \dots, X_n) = \varphi_d(f)(X_0, \dots, X_n) = X_0^d f(X_1/X_0, \dots, X_n/X_0)$$

is a system of inverses to the system of restrictions $\beta_0^t\big|_{\widetilde{A}_d} : \widetilde{A}_d \to A_{\le d}$ of the homomorphism $\beta_0^t : \widetilde{A} \to A$ given by

$$f(X_1, \dots, X_n) = \beta_0^t(F)(X_1, \dots, X_n) = F(1, X_0, \dots, X_n),$$

and these systems have the properties that

$$\mathfrak{a} \cap \widetilde{A}_d = \varphi_d(\mathfrak{b} \cap A_{\le d}) \qquad \text{and} \qquad \beta_0^t(\mathfrak{a} \cap \widetilde{A}_d) = \mathfrak{b} \cap A_{\le d}.$$

Proposition 10.33. Let a prime ideal $\mathfrak{a}$ of $\widetilde{A}$ not containing X_0 correspond to the prime ideal $\mathfrak{b}$ of A under the formula $\mathfrak{b} = \beta_0^t(\mathfrak{a})$ as in Theorem 10.20, and let $U = V(\mathfrak{b})$ and $V = V(\mathfrak{a})$ be the respective affine and projective varieties for $\mathfrak{b}$ and $\mathfrak{a}$, V being the Zariski closure of $\beta_0(U)$ in $\mathbb{P}^n$. Then β_0^t descends to a ring homomorphism ψ of $\widetilde{A}(V)$ onto $A(U)$, and ψ in turn induces a canonical field isomorphism $\Psi : \Bbbk(V) \to \Bbbk(U)$. Under the field isomorphism Ψ, the image of the local ring $\mathcal{O}_{\beta_0(P)}(V)$ is $\mathcal{O}_P(U)$ for each P in U.

PROOF. Since β_0^t carries $\widetilde{A}$ onto A and carries $\mathfrak{a}$ into $\mathfrak{b}$, β_0^t descends to a homomorphism ψ of $\widetilde{A}/\mathfrak{a} = \widetilde{A}(V)$ onto $A/\mathfrak{b} = A(U)$. If $\overline{F}$ and $\overline{G}$ are in the same homogeneous summand $\widetilde{A}(V)_d$ of $\widetilde{A}(V)$, then we define $\Psi(\overline{F}/\overline{G}) = \psi(\overline{F})/\psi(\overline{G})$ as a member of the field of fractions $\Bbbk(U)$ of $A(U)$. If $\overline{F}/\overline{G} = \overline{F}'/\overline{G}'$, then $\overline{F}\,\overline{G}' = \overline{F}'\,\overline{G}$. Applying ψ, using that ψ is a homomorphism, and reinterpreting matters in $\Bbbk(U)$, we see that $\Psi(\overline{F}/\overline{G}) = \Psi(\overline{F}'/\overline{G}')$, i.e., that Ψ is well defined. A similar argument that involves clearing fractions and applying ψ shows that Ψ respects addition and multiplication. Therefore Ψ is a field mapping of $\Bbbk(V)$ into $\Bbbk(U)$.

Let $A(U)_{\le d}$ be the image of $A_{\le d}$ in $A/\mathfrak{b} = A(U)$. Since β_0^t carries $\widetilde{A}_d$ onto $A_{\le d}$ and carries $\mathfrak{a} \cap \widetilde{A}_d$ onto $\mathfrak{b} \cap A_{\le d}$, ψ carries $\widetilde{A}(V)_d$ onto $A(U)_{\le d}$. Any member of $\Bbbk(U)$ is the quotient of two members of $A(U)_{\le d}$ for some d, and it is consequently Ψ of the quotient of the corresponding members of $\widetilde{A}(V)_d$. Therefore Ψ carries $\Bbbk(V)$ onto $\Bbbk(U)$ and is a field isomorphism.

Let $\overline{F}$ and $\overline{G}$ in $\widetilde{A}(V)$ be the cosets $F + \mathfrak{a}$ and $G + \mathfrak{a}$, let $f = \beta_0^t(F)$ and $g = \beta_0^t(G)$, and let $\bar{f}$ and $\bar{g}$ in $A(U)$ be the cosets of $f + \mathfrak{b}$ and $g + \mathfrak{b}$. Then $\psi(\overline{F}) = \bar{f}$ and $\psi(\overline{G}) = \bar{g}$, and hence $\Psi(\overline{F}/\overline{G}) = \bar{f}/\bar{g}$. Let $P = (x_1, \dots, x_n)$ be in U, so that $\beta_0(P) = [1, x_1, \dots, x_n]$ is in $\beta_0(U)$. Define $\beta_0^{\#}(P) = (1, x_1, \dots, x_n)$ in $\mathbb{A}^{n+1}$, so that the class of $\beta_0^{\#}(P)$ in $\mathbb{P}^n$ is $\beta_0(P)$. Then $\bar{g}(P) = g(P) = (\beta_0^t G)(P) = G(\beta_0^{\#}(P)) = \overline{G}(\beta_0^{\#}(P))$. Therefore $\bar{f}/\bar{g}$ lies in $\mathcal{O}_P(U)$ if and only if $\overline{F}/\overline{G}$ lies in $\mathcal{O}_{\beta_0(P)}(V)$. So Ψ carries $\mathcal{O}_{\beta_0(P)}(V)$ onto $\mathcal{O}_P(U)$. □

Corollary 10.34. Let V be a projective variety, and let U be a nonempty open subset of V. Then each member of $\mathcal{O}(U) \subseteq \Bbbk(V)$ is determined as an element in $\Bbbk(V)$ by its restriction to U.

PROOF. Subtracting two such members, we may assume that their difference h is 0 on U. We are to prove that $h = 0$ in $\Bbbk(V)$. For some j with $0 \le j \le n$, $\beta_j(\mathbb{A}^n) \cap V$ is nonempty, and we may assume that this is the case for $j = 0$. The subset $V_0 = \beta_0^{-1}(V)$ of $\mathbb{A}^n$ is an affine variety. Since U and $\beta_0(\mathbb{A}^n) \cap V$ are

nonempty open subsets of V, their intersection is nonempty, and $U_0 = \beta_0^{-1}(U)$ is a nonempty open subset of V_0. Let $\Psi : \Bbbk(V) \to \Bbbk(V_0)$ be the field isomorphism in Proposition 10.33. By assumption, h is in $\mathcal{O}_{\beta_0(P)}(V)$ for every P in U_0. Since the value of h at P is 0, h is actually in the maximal ideal of $\mathcal{O}_{\beta_0(P)}(V)$ for P in U_0. Proposition 10.33 shows that $\Psi(h)$ is in the maximal ideal of $\mathcal{O}_P(V_0)$ for all P in U_0. Fix P_0 in U_0. Then we can write the member $\Psi(h)$ of $\Bbbk(V_0)$ as $\Psi(h) = \bar{a}/\bar{b}$ with $\bar{b}(P_0) \neq 0$. Since $\bar{b}$ is continuous on V_0 by Proposition 10.26, $\bar{b}(P)$ is nonzero for all P in some neighborhood W of P_0 contained in U_0. Then the formula $\Psi(h) = \bar{a}/\bar{b}$ shows explicitly that $\Psi(h)$ is defined at such points P and satisfies $\Psi(h)(P) = \bar{a}(P)/\bar{b}(P)$. Since $\Psi(h)$ is in the maximal ideal of $\mathcal{O}_P(V_0)$ for all P in U_0, $\Psi(h)(P) = 0$ for P in W. Hence $\bar{a}(P) = 0$ for P in W. Consequently $\bar{a}$ and 0 are two members of $A(V)$ that are equal on W, and Lemma 10.27 allows us to conclude that $\bar{a} = 0$. Therefore $h = 0$. □

Proposition 10.35. Let U be a nonempty open subset of the projective variety V in $\mathbb{P}^n$. Suppose that $h_0 : U \to \Bbbk$ is a function with the following property: for each P in U, there exist an open subset W of U containing P and homogeneous polynomials F and G in $\widetilde{A}$ of the same degree such that G is nowhere vanishing on W and $h_0 = F/G$ on W. Then there exists one and only one member h of $\Bbbk(V)$ such that h is regular on U and agrees with h_0 at every point of U.

REMARKS. For the quasiprojective case the more complicated local-sounding definition of "regular function" on U, mentioned in the first paragraph of this section, is what is assumed of h_0 in the statement of this proposition. The proposition says that such an h_0 necessarily comes from a global rational function on V that is regular on U in the sense just above.

PROOF. For each j with $0 \leq j \leq n$ such that $V_j = \beta_j(\mathbb{A}^n) \cap V$ is nonempty, $\beta_j^{-1}(V_j)$ is an affine variety, and $U_j = U \cap V_j$ is a nonempty open subset such that $h_{j,0} = h_0\big|_{U_j}$ is a function on U_j with the following property: for each P in U_j, there exist an open subset W of U_j containing P and homogeneous polynomials F and G in $\widetilde{A}$ of the same degree such that G is nowhere vanishing on W and $h_{j,0} = F/G$ on W. We pull back this situation by β_j^{-1}, writing $\beta_j^t h_{j,0}$ for the function on $\beta_j^{-1}(W)$ given by $(\beta_j^t h_{j,0})(Q) = h_{j,0}(\beta_j(Q))$. The set $\beta_j^{-1}(V_j)$ is an affine variety, and the Zariski closure of V_j in $\mathbb{P}^n$ is V. The homomorphism β_j^t on $\widetilde{A}$ descends to a ring homomorphism $\psi_j : \widetilde{A}(V) \to A(\beta_j^{-1}(V_j))$, and ψ_j induces a field isomorphism $\Psi_j : \Bbbk(V) \to \Bbbk(\beta_j^{-1}(V_j))$, according to Proposition 10.33.

The set $\beta_j^{-1}(U_j)$ is a nonempty open subset of the affine variety $\beta_j^{-1}(V_j)$, and $\beta_j^t h_{j,0}$ is a function on $\beta_j^{-1}(U_j)$ with the following property: for each P in $\beta_j^{-1}(U_j)$, there exist an open subset W of $\beta_j^{-1}(U_j)$ containing P and homogeneous

polynomials F and G in $\widetilde{A}$ of the same degree such that their images $\overline{F}$ and $\overline{G}$ in $\widetilde{A}(V)$ have $\overline{G}$ nowhere vanishing on W and have $\beta_j^t h_{j,0} = \psi_j(\overline{F})/\psi_j(\overline{G}) = \Psi(\overline{F}/\overline{G})$ on W. Proposition 10.33 says that $\psi_j(\overline{F}) = \bar{a}$ and $\psi_j(\overline{G}) = \bar{b}$ for members $\bar{a}$ and $\bar{b}$ of $A(\beta_j^{-1}(V_j))$. We are in the situation of Proposition 10.28 with $f_0 = \beta_j^t h_{j,0}$, and that proposition produces a unique member h_j of $\Bbbk(\beta_j^{-1}(V_j))$ that is regular on $\beta_j^{-1}(U_j)$ and agrees with $\beta_j^t h_{j,0}$ at every point of $\beta_j^{-1}(U_j)$.

The member h of $\Bbbk(V)$ that we seek is $h = \Psi_j^{-1}(h_j)$. To verify this assertion, we are to show that $\Psi_j^{-1}(h_j)$ is independent of j. Thus suppose that $V_i \cap V_j \neq \varnothing$. Fix P in $U_i \cap U_j = U \cap V_i \cap V_j$, and choose the above open neighborhood W of P small enough for the above construction to apply for both indices i and j. By the uniqueness in Proposition 10.28, h_j is the unique member of $\Bbbk(\beta_j^{-1}(V_j))$ that is regular on $\beta_j^{-1}(W)$ and agrees with $\beta_j^t h_{j,0} = \beta_j^t(h_0\big|_{U_j})$ at every point of $\beta_j^{-1}(W)$. Thus $\Psi_j^{-1}(h_j) = \overline{F}/\overline{G}$ on W, where $\overline{F}$ and $\overline{G}$ are as in the previous paragraph. By the same uniqueness argument, $\Psi_i^{-1}(h_i) = \overline{F}/\overline{G}$ on W. The difference $\Psi_i^{-1}(h_i) - \Psi_j^{-1}(h_j)$ is a member of $\Bbbk(V)$ that is regular on W and vanishes there. By Corollary 10.34, the difference is 0 as an element of $\Bbbk(V)$. Therefore $\Psi_j^{-1}(h_j)$ is independent of j, and we can take h to be this member of $\Bbbk(V)$. □

Just as in the quasi-affine case, it is possible in the quasiprojective case to give a local-sounding definition of rational function and a formulation of $\mathcal{O}_P(U)$ in terms of germs. We shall not use these notions, and we omit any further discussion of them.

5. Morphisms

The goal of this section and the next is to introduce maps that make the collection of all quasiprojective varieties over an algebraically closed field $\Bbbk$ into the objects of a category in a way that does not depend on the ambient space $\mathbb{A}^n$ or $\mathbb{P}^n$ of the variety. These maps will all be algebraic in nature, and there will be two choices of which class of maps to use, one involving good denominators and one allowing occasional bad denominators. The first kind of map will be called a "morphism," and the second kind of map will be called a "dominant rational map." The relationships between these two kinds of maps and the interpretation of these maps in terms of function fields will be of great importance in applying this theory.

A **variety** over the algebraically closed field $\Bbbk$ henceforth will be any affine, quasi-affine, projective, or quasiprojective variety as in the previous sections. To

each such variety V, Section 4 associates a function field $\Bbbk(V)$, a local ring $\mathcal{O}_P(V) \subseteq \Bbbk(V)$ of regular functions at each point P, and a ring $\mathcal{O}(E) = \bigcap_{P\in E} \mathcal{O}_P(V) \subseteq \Bbbk(V)$ of regular functions on each nonempty open subset E of V. We have observed that each rational function on a variety V is regular on some nonempty open subset of V, namely the complement of the pole set. One further fact that we shall use about rational functions is the following.

Proposition 10.36. If P and Q are distinct points of a variety V, then there exists a rational function $h \in \Bbbk(V)$ such that h is defined at both P and Q, has $h(P) = 0$, and has $h(Q) \neq 0$.

PROOF. Without loss of generality, we may assume that V is projective. Say that $V \subseteq \mathbb{P}^n$. Let $\mathfrak{p}$ be the prime homogeneous ideal in $\widetilde{A} = \Bbbk[X_0, \ldots, X_n]$ such that $\widetilde{A}(V) = \widetilde{A}/\mathfrak{p}$, and let $F \mapsto \overline{F}$ be the quotient homomorphism $\widetilde{A} \mapsto \widetilde{A}(V)$. Let $P = [x_0, \ldots, x_n]$ and $Q = [y_0, \ldots, y_n]$. Choose a homogeneous polynomial F in $\widetilde{A}$ such that $F(x_0, \ldots, x_n) = 0$ and $F(y_0, \ldots, y_n) \neq 0$, and choose a homogeneous polynomial G with $\deg G = \deg F$ such that $G(x_0, \ldots, x_n) \neq 0$ and $G(y_0, \ldots, y_n) \neq 0$. Then $\overline{G}$ is not 0, and $h = \overline{F}/\overline{G}$ has the required properties. □

If U and V are varieties, then a continuous function $\varphi : U \to V$ relative to the Zariski topology is called a **morphism** if for each nonempty open subset E of V and each regular function f on E, the composition $f \circ \varphi$ is a regular function on the open subset $\varphi^{-1}(E)$ of U. Thus φ is to be continuous and is to induce by composition a function from $\mathcal{O}(E)$ into $\mathcal{O}(\varphi^{-1}(E))$ for each open subset E of V. An **isomorphism** of varieties is a morphism having an inverse function that is a morphism.

It is immediate that the composition of two morphisms is a morphism and that the identity function is a morphism. Thus the varieties over $\Bbbk$ form a category if morphisms are used as the maps.

EXAMPLES OF MORPHISMS. Suppose that $\Bbbk$ has characteristic different from 2. Let U be $\mathbb{P}^1$, written as

$$\mathbb{P}^1 = \big\{[s, t] \mid (s, t) \neq (0, 0)\big\},$$

and let V be the projective variety in $\mathbb{P}^2$ defined by the irreducible homogeneous polynomial $X^2 + Y^2 - Z^2$, i.e.,

$$V = \big\{[x, y, z] \mid x^2 + y^2 = z^2 \text{ and } (x, y, z) \neq (0, 0, 0)\big\}.$$

Let $\varphi : U \to V$ be the function given by

$$\varphi\big([s, t]\big) = [s^2 - t^2, 2st, s^2 + t^2].$$

This is well defined, and it is continuous because the Zariski closed proper subsets of V are the finite sets, whose inverse images are finite sets. If F and G are two homogeneous members of $\Bbbk[X, Y, Z]$ and if $\overline{F}$ and $\overline{G}$ are the images in $\widetilde{A}(V) = \Bbbk[X, Y, Z]/(X^2 + Y^2 - Z^2)$, we are to assume that $\overline{G}$ is not 0, i.e., that G is not divisible by $X^2 + Y^2 - Z^2$, and then $h = \overline{F}/\overline{G}$ is a typical rational function on V. We are to show that if h is regular on an open subset E of V, then $h \circ \varphi$ is regular on $\varphi^{-1}(E) \subseteq \mathbb{P}^1$. The expression $h = \overline{F}/\overline{G}$ exhibits h as regular on the open set E of points $[x, y, z]$ of V with $G(x, y, z) \neq 0$. The set $\varphi^{-1}(E)$ is the set of points $[s, t]$ in $\mathbb{P}^1$ with $G(s^2 - t^2, 2st, s^2 + t^2) \neq 0$. At such points the function $h \circ \varphi$ is given by

$$(h \circ \varphi)(s, t) = F(s^2 - t^2, 2st, s^2 + t^2)/G(s^2 - t^2, 2st, s^2 + t^2),$$

and it is given by a rational expression with nonvanishing denominator. Thus φ is a morphism.

Let us see that $\psi : V \to \mathbb{P}^1$ given by

$$\psi[x, y, z] = \begin{cases} [x + z, y] & \text{if } [x, y, z] \neq [1, 0, -1], \\ [-y, x - z] & \text{if } [x, y, z] \neq [1, 0, 1] \end{cases}$$

consistently defines another morphism. For the consistency we observe that $x^2 + y^2 = z^2$ implies that $(x + z)(x - z) = -y^2$; hence on the common domain of the two expressions, $[x + z, y] = [-y^2/(x - z), y] = [-y/(x - z), 1] = [-y, x - z]$. Continuity of ψ follows because the inverse image of any finite set is a finite set. For the regularity we observe that if F and G are homogeneous members of the same degree in $\widetilde{A}(\mathbb{P}^1) = \Bbbk[S, T]$ with $G \neq 0$ and if $h = F/G$, then the expression $h = F/G$ exhibits h as regular on the open set E of points $[s, t]$ in $\mathbb{P}^1$ with $G(s, t) \neq 0$. The set $\psi^{-1}(E)$ is the set of points $[x, y, z]$ on V with $G(x + z, y) \neq 0$. At such points the function $h \circ \psi$ is given by

$$(h \circ \psi)[x, y, z] = F(x + z, y)/G(x + z, y),$$

and it is given by a rational expression with a nonvanishing denominator. Thus ψ is a morphism. In other words, φ is an isomorphism.

Proposition 10.37. Let $\beta_0 : \mathbb{A}^n \to \mathbb{P}^n$ be the usual inclusion. If U is a quasi-affine variety in $\mathbb{A}^n$, then β_0 is an isomorphism of the quasi-affine variety U onto the quasiprojective variety $\beta_0(U)$.

PROOF. Proposition 10.18 shows that β_0 is a homeomorphism of U onto its image. The last conclusion of Proposition 10.33 implies that the regular functions for U match those for $\beta_0(U)$ under β_0, and the result follows. □

Theorem 10.38. Let U be any variety, let V be any affine variety, and let $A(V)$ be the affine coordinate ring of V. Then the morphisms $\varphi : U \to V$ are in one-one correspondence with the $\Bbbk$ algebra homomorphisms $\widetilde{\varphi} : A(V) \to \mathcal{O}(U)$ via the formula

$$\widetilde{\varphi}(f) = f \circ \varphi \qquad \text{for } f \in A(V).$$

REMARKS. Members f of $A(V)$ lie in $\mathcal{O}(V)$. The $\Bbbk$ algebra homomorphism $\widetilde{\varphi}$ is meaningful because the fact that φ is a morphism implies that $f \circ \varphi$ is in $\mathcal{O}(\varphi^{-1}(E))$ for every open E in V; here we take $E = V$ and $\varphi^{-1}(E) = U$. The proof of Theorem 10.38 will be preceded by a lemma.

Lemma 10.39. If U is a variety and V is an affine variety in $\mathbb{A}^n$, then a function $\psi : U \to V$ is a morphism if and only if $\overline{X_i} \circ \psi$ is a regular function on U for the image $\overline{X_i}$ in $A(V)$ of each coordinate function X_i with $1 \le i \le n$.

PROOF. If ψ is a morphism, then the definition of morphism forces $\overline{X_i} \circ \psi$ to be a regular function.

Conversely suppose ψ has the property that each $\overline{X_i} \circ \psi$ is a regular function. Then $f \circ \psi$ is a regular function on U for each f in $A(V)$, since every member of $A(V)$ is a polynomial in the elements $\overline{X_i}$. If E is a closed set in V, then E is the locus of common zeros of some set $\{f_\alpha\}$ of polynomials, and $\psi^{-1}(E)$ is the set of points P such that $f_\alpha(\psi(P)) = 0$ for all α. Hence $\psi^{-1}(E)$ is the locus of common zeros of a subset $\{f_\alpha \circ \psi\}$ of regular functions on U and is relatively closed in U. Thus ψ is continuous.

If E is nonempty open in V, then $\Bbbk(E) = \Bbbk(V)$ shows that each regular function h on E is locally the quotient of members of $A(V)$ with nonvanishing denominator. Let us write $h = f/g$ with g nonvanishing near a point of interest. Then $h \circ \psi = (f \circ \psi)/(g \circ \psi)$ is exhibited locally as a rational function with nonvanishing denominator. □

PROOF OF THEOREM 10.38. Suppose that $\alpha : A(V) \to \mathcal{O}(U)$ is a $\Bbbk$ algebra homomorphism. Define $\psi : U \to V$ by $\psi(P) = (\alpha(\overline{X_1})(P), \dots, \alpha(\overline{X_n})(P))$. Then $\overline{X_i} \circ \psi = \alpha(\overline{X_i})$ is in $\mathcal{O}(U)$ by definition of α, and Lemma 10.39 shows that ψ is a morphism.

The $\Bbbk$ algebra homomorphism $\widetilde{\psi}$ defined by $\widetilde{\psi}(f) = f \circ \psi$ has $\widetilde{\psi}(\overline{X_i}) = \overline{X_i} \circ \psi = \alpha(\overline{X_i})$. Since the elements $\overline{X_i}$ generate $A(V)$, $\widetilde{\psi} = \alpha$. Thus starting from α, forming ψ, and obtaining $\widetilde{\psi}$ recovers α. In the reverse direction if we start from φ, form $\widetilde{\varphi}$, and use the construction of the previous paragraph to obtain ψ, then $\psi(P) = \big(\widetilde{\varphi}(\overline{X_1})(P), \dots, \widetilde{\varphi}(\overline{X_n})(P)\big) = \big(\overline{X_1}(\varphi(P)), \dots \overline{X_n}(\varphi(P))\big) = \varphi(P)$ for P in U. Hence $\psi = \varphi$. Thus the function $\alpha \mapsto \psi$ is a two-sided inverse of the function $\varphi \mapsto \widetilde{\varphi}$. □

Corollary 10.40. If U and V are affine varieties, then the morphisms $\varphi : U \to V$ are in one-one correspondence with the $\Bbbk$ algebra homomorphisms $\widetilde{\varphi} : A(V) \to A(U)$ via the formula

$$\widetilde{\varphi}(f) = f \circ \varphi \qquad \text{for } f \in A(V).$$

PROOF. This is immediate from Theorem 10.38, since Corollary 10.25 shows that $\mathcal{O}(U) = A(U)$. □

Proposition 10.41. If U and V are varieties and if $\varphi : U \to V$ and $\psi : U \to V$ are morphisms such that $\varphi\big|_E = \psi\big|_E$ for some nonempty open set E in U, then $\varphi = \psi$.

PROOF. Let h be a rational function on V, and let E' be the nonempty open subset of V on which h is regular. Since φ and ψ are morphisms, $h \circ \varphi$ and $h \circ \psi$ are regular on the respective nonempty open subsets $\varphi^{-1}(E')$ and $\psi^{-1}(E')$ of U. The equality $\varphi\big|_E = \psi\big|_E$ shows that $h \circ \varphi$ and $h \circ \psi$ are equal on the nonempty open subset $E \cap \varphi^{-1}(E') \cap \psi^{-1}(E')$ of U. The function $h \circ \varphi - h \circ \psi$ is therefore a rational extension from $E \cap \varphi^{-1}(E') \cap \psi^{-1}(E')$ to U of the 0 function, and Proposition 10.34 shows that $h \circ \varphi - h \circ \psi = 0$ on U. Therefore $h \circ \varphi = h \circ \psi$ as elements of $\Bbbk(U)$ for every h in $\Bbbk(V)$.

Arguing by contradiction, suppose that P is a point in U for which $\varphi(P) \neq \psi(P)$. Then Proposition 10.36 produces h in $\Bbbk(U)$ such that h is regular on an open subset F of V containing $\varphi(P)$ and $\psi(P)$ and has $h(\varphi(P)) = 0$ and $h(\psi(P)) \neq 0$. Since φ and ψ are morphisms, $h \circ \varphi$ and $h \circ \psi$ are regular on the open set $\varphi^{-1}(F) \cap \psi^{-1}(F)$. Their respective values at P are $h(\varphi(P)) = 0$ and $h(\psi(P)) \neq 0$. Since $h \circ \varphi = h \circ \psi$ as rational functions, this is a contradiction. □

Proposition 10.42. Suppose that U and V are varieties and that $\varphi : U \to V$ is a morphism. If P is in U, then φ induces a $\Bbbk$ algebra homomorphism $\varphi_P^* : \mathcal{O}_{\varphi(P)}(V) \to \mathcal{O}_P(U)$. Composition of morphisms goes to composition of these homomorphisms in the reverse order.

Proof. Propositions 10.33 and 10.37 together imply that we may assume U and V to be quasi-affine. Let f in $\Bbbk(V)$ be defined at $\varphi(P)$. Proposition 10.24 shows that the set E on which f is regular is open in V. Since φ is a morphism and f is regular on E, $f \circ \varphi$ is regular on the open subset $\varphi^{-1}(E)$ of U. Proposition 10.28, applied to $\varphi^{-1}(E) \subseteq U$, shows that there exists a unique member F of $\Bbbk(U)$ that is regular on $\varphi^{-1}(E)$ and agrees with $f \circ \varphi$ on $\varphi^{-1}(E)$. We put $\varphi_P^*(f) = F$. It is a routine matter to check that φ_P^* is a $\Bbbk$ algebra homomorphism and that compositions go to compositions in the reverse order. □

6. Rational Maps

This section will introduce a second kind of map that makes the collection of all (quasiprojective) varieties over the algebraically closed field $\Bbbk$ into a category. These maps will not be ordinary functions, and the definition requires some care.

If U and V are varieties over the algebraically closed field $\Bbbk$, then a **rational map** $\varphi : U \to V$ is an equivalence class of pairs (E, φ_E), where E is a nonempty open set of U and φ_E is a morphism of E into V. The equivalence relation on two such pairs is that $(E, \varphi_E) \sim (E', \varphi_{E'})$ if $\varphi_E\big|_{E\cap E'} = \varphi_{E'}\big|_{E\cap E'}$. This is meaningful, since the intersection of any two nonempty open sets is nonempty. The relation $\sim$ is certainly reflexive and symmetric, and Proposition 10.41 shows that it is transitive. We can therefore take the union of the open subsets E such that some pair (E, φ_E) is in the equivalence class, and φ will be definable as a morphism on this union. This union is called the **largest domain** on which φ is a morphism.

A morphism from U to V defines a rational map. But a rational map need not be an everywhere-defined function, and forming the composition of two rational maps is problematic. For example, if E is the open subset of U on which a rational map $\varphi : U \to V$ is defined and F is the open subset of V on which a rational map $\psi : V \to W$ is defined, then it may happen that $\varphi(E)$ is disjoint from F. In this case the composition $\psi \circ \varphi$ makes no sense.

A rational map $\varphi : U \to V$ is said to be **dominant** if φ_E has dense image in V for some (and hence every) pair (E, φ_E) in the equivalence class. It is evident that the composition of two *dominant* rational maps makes sense as a rational map. The identity mapping is a dominant rational map, and thus the collection of all varieties over $\Bbbk$ becomes a category if the dominant rational maps are used as the maps of the category.

A **birational map** is a dominant rational map $\varphi : U \to V$ that has a dominant rational map $\psi : V \to U$ as a two-sided inverse. Two varieties admitting a birational map from the one to the other are said to be **birationally equivalent** varieties, or to be **birational**.

EXAMPLE. The irreducible affine plane curves defined by $T^2 - (S^4 + 1)$ and $Y^2 - (X^3 - 4X)$ are birationally equivalent if $\Bbbk$ has characteristic different from 2. Birational mappings in the two directions are given by

$$\left.\begin{aligned} S &= \frac{Y}{2X} \\ T &= \frac{Y^2 + 8X}{4X^2} \end{aligned}\right\} \quad \text{and} \quad \left\{\begin{aligned} X &= \frac{2}{T - S^2} \\ Y &= \frac{4S}{T - S^2}. \end{aligned}\right.$$

The rational map from (X, Y) to (S, T) is a morphism on the complement of $(0, 0)$ in the locus $y^2 = x^3 - 4x$ in $\mathbb{A}^2$. The rational map from (S, T) to (X, Y) is a morphism on the entire locus $t^2 = s^4 + 1$ in $\mathbb{A}^2$.

Let $\varphi : U \to V$ be a dominant rational map, and let (E, φ_E) be any pair in the equivalence class φ. If $f \in \Bbbk(V)$ is a rational function on V, then the subset F of V on which f is defined is open and nonempty. So $f\big|_F$ is a regular function on F. Since φ_E is continuous and has dense image, $E' = \varphi_E^{-1}(F)$ is a nonempty open set in $E \subseteq U$. The function $\varphi_{E'}$ is a morphism from E' into F, and thus $f\big|_F \circ \varphi_{E'}$ is a regular function on E'. We can therefore regard it as a rational function on U, i.e., a member of $\Bbbk(U)$. Consequently the dominant rational map $\varphi : U \to V$ induces a function $\widetilde{\varphi} : \Bbbk(V) \to \Bbbk(U)$ that is easily seen to be a field mapping respecting $\Bbbk$. Compositions of dominant rational maps lead to compositions of such field mappings in the reverse order.

EXAMPLE, CONTINUED. The two irreducible affine plane curves in the example earlier in this section have been observed to be birationally equivalent. In view of the previous paragraph, their function fields must be isomorphic. Taking into account that the genus of a curve, as defined in Section IX.3, depends only on the function field, we see that the two curves must have the same genus. This equality is confirmed by Example 3 of genus in Section IX.3, which shows that the genus of $\Bbbk[x, y]/(y^2 - p(x))$, where $p(x)$ is a square-free polynomial of degree m in characteristic different from 2, is $\frac{1}{2}m - 1$ if m is even and is $\frac{1}{2}(m-1)$ if m is odd. The two curves under study have $m = 4$ and $m = 3$, and the genus is 1 in both cases.

The main result of this section will be a converse to the construction just made, showing how to pass from a $\Bbbk$ algebra homomorphism between function fields to a dominant rational map in the reverse order. We require two lemmas.

Lemma 10.43. Let $V = V(f)$ be the hypersurface[13] in $\mathbb{A}^n$ defined by a nonconstant polynomial f in $\Bbbk[X_1, \ldots, X_n]$. Then the open set $\mathbb{A}^n - V$ is isomorphic to an affine variety, specifically to the hypersurface in $\mathbb{A}^{n+1}$ corresponding to the irreducible polynomial $X_{n+1}f(X_1, \ldots, X_n) - 1$ in $\Bbbk[X_1, \ldots, X_{n+1}]$.

REMARKS. Even though f is not assumed irreducible, $X_{n+1}f - 1$ is irreducible. In fact, consideration of the degree in X_{n+1} shows that the only possible nontrivial factorization is of the form $(X_{n+1}a - b)(c)$ with a, b, c in $\Bbbk[X_1, \ldots, X_n]$. Then $bc = 1$, and c has to be scalar. The open set $\mathbb{A}^n - V$ is a quasi-affine variety (having closure $\mathbb{A}^n$), and the lemma therefore asserts that this quasi-affine variety is isomorphic to a certain affine variety in $\mathbb{A}^{n+1}$.

PROOF. Let $W = V(X_{n+1}f - 1)$. Let $\varphi : W \to \mathbb{A}^n$ be the map defined by $\varphi(x_1, \ldots, x_{n+1}) = (x_1, \ldots, x_n)$ for $(x_1, \ldots, x_{n+1})$ in W. Then $X_j \circ \varphi$ is projection

[13] In the application of Lemma 10.43 to Lemma 10.44, it is important that the polynomial f is allowed to be reducible.

to the j^{th} coordinate for $1 \le j \le n$, which is a regular function on W. Lemma 10.39 shows that φ is a morphism, and φ is one-one onto by inspection. The inverse function is given by $\varphi^{-1}(x_1, \dots, x_n) = \big(x_1, \dots, x_n, 1/f(x_1, \dots, x_n)\big)$. Let $\overline{X_j}$ be the image of X_j in $\Bbbk[X_1, \dots, X_{n+1}]/(X_{n+1}f - 1)$ for $1 \le j \le n+1$. Then $(\overline{X_j} \circ \varphi^{-1})(x_1, \dots, x_n)$ equals x_j for $j \le n$ and equals $1/f(x_1, \dots, x_n)$ for $j = n+1$, and these are regular functions on the complement of $V(f)$ in $\mathbb{A}^n$. By Lemma 10.39, φ^{-1} is a morphism. □

Lemma 10.44. If V is a variety, then there is a base for the Zariski topology on V consisting of open sets that are isomorphic to affine varieties.

PROOF. Let P be in V, and let U be an open subset of V containing P. We are to produce an open subset W of U containing P that is isomorphic to an affine variety. Since any nonempty open set of a quasiprojective variety is a quasiprojective variety, U is a variety. Thus we may assume that $U = V$. Since any projective variety in $\mathbb{P}^n$ is covered by the affine varieties isomorphic via Proposition 10.37 to nonempty intersections with $\beta_j(\mathbb{A}^n)$, any quasiprojective variety is covered by quasi-affine varieties. Thus we may assume that $U = V$ is quasi-affine in $\mathbb{A}^n$. Let X be the closed subset $X = \overline{V} - V$ in $\mathbb{A}^n$, and let $\mathfrak{a} = I(X)$. Since P is in V, it is not in X, and there exists some f in $\mathfrak{a}$ with $f(P) \ne 0$. Let $Y = V(f)$. The point P is not in Y, and thus $W = V - V(f)$ is relatively open in V and contains P.

Being relatively open in V, W is a quasi-affine variety. Since f vanishes on X, $V(f)$ contains $X = \overline{V} - V$. Thus the equality $W = \overline{V} - V(f)$ exhibits W as a relatively closed subset of $\mathbb{A}^n - V(f)$, which Lemma 10.43 shows is isomorphic to an affine variety. Hence W itself is isomorphic to a quasi-affine variety that is closed in an affine variety. That is, W is isomorphic to an affine variety. □

Theorem 10.45. Let U and V be varieties, and let $\varphi \mapsto \widetilde{\varphi}$ be the function carrying dominant rational maps $\varphi : U \to V$ to field mappings $\widetilde{\varphi} : \Bbbk(V) \to \Bbbk(U)$ respecting the operations by $\Bbbk$ and given by

$$\widetilde{\varphi}(f) = (\text{class of } f\big|_F \circ \varphi_{E'}),$$

where f is in $\Bbbk(V)$, f is regular on F, (E, φ_E) is a pair in the class φ, and $E' = \varphi_E^{-1}(F)$. Then $\varphi \mapsto \widetilde{\varphi}$ is one-one onto the set of all field mappings from $\Bbbk(V)$ into $\Bbbk(U)$ respecting $\Bbbk$. Furthermore, if $P \in U$ and $Q \in V$ are points, then the maximal ideal of $\widetilde{\varphi}(\mathcal{O}_Q(V))$ is contained in the maximal ideal of $\mathcal{O}_P(U)$ if and only if P is in the largest domain on which φ is a morphism and has $\varphi(P) = Q$.

REMARK. The ring $\mathcal{O}_P(U)$ is the $\Bbbk$ vector space sum of its maximal ideal and the constants, since evaluation at P is a well-defined multiplicative linear functional on $\mathcal{O}_P(U)$, and a similar comment applies to $\mathcal{O}_Q(V)$. Whatever $\widetilde{\varphi}$

does, it certainly carries 1 to 1, and hence if $\widetilde{\varphi}$ carries the maximal ideal of $\mathcal{O}_Q(V)$ to the maximal ideal of $\mathcal{O}_P(U)$, then it carries $\mathcal{O}_Q(V)$ to $\mathcal{O}_P(U)$ also.

PROOF. We begin by inverting $\varphi \mapsto \widetilde{\varphi}$. Lemma 10.44 shows that any variety is covered by open subvarieties isomorphic to affine varieties, and the function fields of the variety and the subvarieties may all be identified with one another. Thus there is no loss in generality in assuming that V is an affine variety in $\mathbb{A}^n$. Let $\overline{X_1}, \dots, \overline{X_n}$ be the images in $A(V)$ of $X_1, \dots, X_n$, and suppose that a $\Bbbk$ algebra homomorphism $\gamma : \Bbbk(V) \to \Bbbk(U)$ is given. Then $\gamma(\overline{X_1}), \dots, \gamma(\overline{X_n})$ are rational functions on U, and we can find a nonempty open subset E of U on which all these functions are regular. Since γ is a homomorphism, γ yields by restriction of the images a homomorphism $\gamma : A(V) \to \mathcal{O}(E)$. Moreover, this version of γ is one-one on $A(V)$ because γ as a field mapping is one-one and because Proposition 10.34 shows that each member of $\mathcal{O}(E)$ extends in only one way to a member of $\Bbbk(U)$. Theorem 10.38 produces a morphism $\psi : E \to V$ such that $\widetilde{\psi} = \gamma$ for this restricted version of γ. Then the equivalence class φ of the pair (ψ, E) is a rational map of U into V.

To see that φ is dominant, suppose on the contrary that $\overline{\psi(E)}$ is a proper closed subset of V. Then we can find a polynomial f that is 0 on $\overline{\psi(E)}$ but is not identically 0 on V. The image $\bar{f}$ of f in $A(V)$ is nonzero. Since the restricted version of γ is one-one, $\gamma(\bar{f})$ is nonzero in $\mathcal{O}(E)$. However, $\gamma(\bar{f}) = \widetilde{\psi}(\bar{f}) = \bar{f} \circ \psi$, and the right side is 0 on E, contradiction.

The construction is arranged in such a way that if we start from φ, form $\widetilde{\varphi}$, and go through the construction to produce a rational map of U into V, then the resulting rational map is φ. In the reverse direction, suppose that we start from γ, produce φ, and then form $\widetilde{\varphi}$, and suppose that $\bar{f}$ in $\Bbbk(V)$ is in $A(V)$. If $E \subseteq U$ is as in the first paragraph of the proof, then a representative of φ is the pair (E, φ_E), where φ_E is the morphism such that $(\varphi_E)^{\sim} = \gamma$. Then $\gamma_\varphi(\bar{f})$ is the class of $\bar{f} \circ \varphi_E$, which equals $\widetilde{\varphi}(f)$ and hence $\gamma(\bar{f})$. In other words, γ and $\widetilde{\varphi}$ agree on $A(V)$; being field mappings, they agree on $\Bbbk(V)$. This completes the proof of the first conclusion of the theorem.

Now suppose that φ is a dominant rational map from U to V and that $\widetilde{\varphi}$ is the corresponding field map of $\Bbbk(V)$ to $\Bbbk(U)$. Let $P \in U$ and $Q \in V$ be points, suppose that there is an open neighborhood E of P such that (E, φ_E) is in the equivalence class φ, and suppose that $\varphi_E(P) = Q$. Lemma 10.44 shows that there is a base of open neighborhoods of Q in V consisting of open sets that are isomorphic to affine varieties. Since φ_E is by assumption continuous, we can select any such open neighborhood and assume that φ_E carries E into it. Thus there is no loss of generality in assuming that V is isomorphic to an affine variety. We associate to φ_E the $\Bbbk$ algebra homomorphism $(\varphi_E)^{\sim} : \mathcal{O}(V) \to \mathcal{O}(E)$ given by $(\varphi_E)^{\sim}(f) = f \circ \varphi_E$ for $f \in \mathcal{O}(V)$. This formula shows that the members f of $\mathcal{O}(V)$ that vanish at Q are carried to members of $\mathcal{O}(E)$ that vanish at P and

that members of $\mathcal{O}(V)$ that do not vanish at Q go to members of $\mathcal{O}(E)$ that do not vanish at P. Therefore $(\varphi_E)^\sim$ carries $\mathcal{O}_Q(V)$ into $\mathcal{O}_P(E) = \mathcal{O}_P(U)$.

Conversely suppose that the field map $\widetilde{\varphi}$ has the property that the maximal ideal of $\widetilde{\varphi}(\mathcal{O}_Q(V))$ is contained in the maximal ideal of $\mathcal{O}_P(U)$. Possibly by passing to an open subneighborhood from the outset, we may assume by Lemma 10.44 that U and V are isomorphic to affine varieties. Dropping the isomorphism from the notation, we can write $\mathcal{O}(V) = A(V) = \Bbbk[y_1, \ldots, y_m]$ by Corollary 10.25. Each $\widetilde{\varphi}(y_j)$ is a rational function on U, which we can write as $\widetilde{\varphi}(y_j) = a_j/b_j$ with a_j and b_j in $\mathcal{O}(U) = A(U)$. The hypothesis on $\widetilde{\varphi}$ implies that $\widetilde{\varphi}(\mathcal{O}_Q(V)) \subseteq \mathcal{O}_P(U)$, hence that each $\widetilde{\varphi}(y_j)$ is regular at P. Thus we may take each denominator b_j to have $b_j(P) \neq 0$. Choose an open neighborhood of P on which all b_j are nonvanishing and an open subneighborhood E that is isomorphic to an affine variety. Since $\widetilde{\varphi}$ respects the field operations, it carries any polynomial in $y_1, \ldots, y_m$ to a quotient c/d with c and d in $\mathcal{O}(E)$ and with d nowhere 0 on E. Therefore c/d is in $\bigcap_{P' \in E} \mathcal{O}_{P'}(E) = \mathcal{O}(E)$. That is, $\widetilde{\varphi}$ carries $\mathcal{O}(V)$ into $\mathcal{O}(E)$. Since V is isomorphic to an affine variety, Corollary 10.25 and Theorem 10.38 show that $\widetilde{\varphi} : \mathcal{O}(V) \to \mathcal{O}(E)$ is given by the formula

$$\widetilde{\varphi}(h)(u) = h(\varphi_E(u)) \qquad (*)$$

for some morphism $\varphi_E : E \to V$ and all $h \in \mathcal{O}(V)$ and $u \in E$. The first part of the proof shows that the pair (E, φ_E) is in the equivalence class φ. Hence P is in the largest domain on which φ is a morphism. Arguing by contradiction, suppose that $\varphi_E(P) = Q' \neq Q$. Choose by Proposition 10.36 a rational function h on V that is defined at both Q and Q' and has $h(Q) = 0$ and $h(Q') \neq 0$. Then $\widetilde{\varphi}$ carries $\mathcal{O}_Q(V)$ and its maximal ideal into $\mathcal{O}_P(U)$ and its maximal ideal, and we obtain $0 = \widetilde{\varphi}(h)(P) = h(\varphi_E(P)) = h(Q') \neq 0$, contradiction. We therefore conclude that $\varphi_E(P) = Q$, and the proof of the second conclusion of the theorem is complete. □

Corollary 10.46. If U and V are varieties, then the following conditions are equivalent:

(a) U and V are birationally equivalent,
(b) $\Bbbk(U)$ and $\Bbbk(V)$ are isomorphic as $\Bbbk$ algebras,
(c) there are nonempty open subsets E of U and F of V such that E and F are isomorphic as varieties.

PROOF. The equivalence of (a) and (b) follows from Theorem 10.45 and the fact that composition of dominant rational maps corresponds to composition of homomorphisms of $\Bbbk$ algebras in the reverse order.

Let us check that (c) implies (a). If (c) holds, let $\varphi : E \to F$ and $\psi : F \to E$ be morphisms that are inverse to each other. Then the equivalence classes of

(E, φ) and (F, ψ) are rational maps from U to V and from V to U, respectively. The equivalence class of $(E, \psi \circ \varphi) = (E, 1_E)$ is the identity rational map on U, and the equivalence class of $(F, \varphi \circ \psi) = (F, 1_F)$ is the identity rational map on V. Hence the rational maps are inverses of one another. This proves (a).

Finally let us check that (a) implies (c). If (a) holds, let $\varphi : U \to V$ and $\psi : V \to U$ be rational maps that are inverse to each other. Let (E_1, φ) and (F_1, ψ) be pairs representing φ and ψ. Then a pair representing $\psi \circ \varphi$ is $(\varphi^{-1}(F_1), \psi \circ \varphi)$ because φ is a morphism on the open subset $\varphi^{-1}(F_1)$ of E_1 and ψ is a morphism on the open set F_1 containing $\varphi(\varphi^{-1}(F_1))$. Since $\psi \circ \varphi$ is the identity on U as a rational map, $\psi \circ \varphi$ is the identity morphism on $\varphi^{-1}(F_1)$. Put $E = \varphi^{-1}(F_1) \subseteq E_1$. Similarly $\varphi \circ \psi$ is the identity morphism on $\psi^{-1}(E_1)$, and we put $F = \psi^{-1}(E_1) \subseteq F_1$. Let us see that $\varphi(E) \subseteq F$. If e is in E, we are to exhibit some $e_1 \in E_1$ with $\psi(\varphi(e))$ in E_1, and then $\varphi(e)$ will be in $F = \psi^{-1}(E_1)$; for this purpose we can take $e_1 = e$, since $\psi \circ \varphi$ is the identity morphism on E. Similarly $\psi(F) \subseteq E$. Thus φ and ψ exhibit E and F as isomorphic varieties. This proves (c). □

7. Zariski's Theorem about Nonsingular Points

Sections 1–6 have established the definitions and elementary properties of varieties, maps between varieties, and dimension. The present section concerns singularities, which are a fundamental topic of interest in algebraic geometry.[14] This topic was introduced in Section VII.5 in a context that we now recognize as affine varieties.

The definition of "nonsingular" was motivated by the classical Implicit Function Theorem. Let $\Bbbk$ be an algebraically closed field, let the affine space in question be $\mathbb{A}^n$, and let $\mathfrak{p}$ be the prime ideal such that the affine variety to study in $\mathbb{A}^n$ is $V(\mathfrak{p})$. If $\{f_i\}$ is a finite set of generators of $\mathfrak{p}$ and if P is in $V(\mathfrak{p})$, then P is said to be a **nonsingular** point of $V(\mathfrak{p})$ if $\operatorname{rank}\left[\frac{\partial f_i}{\partial X_j}(P)\right] = n - \dim V(\mathfrak{p})$, and otherwise it is **singular**. Zariski's Theorem, which was formulated as Theorem 7.23 but only partially proved in Chapter VII, addressed this situation. In order to rephrase the theorem in our current notation, let $A(V)$ be the affine coordinate ring of V, and let $\Bbbk(V)$ be the field of fractions of $A(V)$, i.e., the function field of V. Let $\mathfrak{m}_P$ be the maximal ideal of all members of $A(V)$ vanishing at P, and let $\mathcal{O}_P(V)$ be the local ring at P; this is the localization of $A(V)$ with respect to the maximal ideal $\mathfrak{m}_P$ and is a subring of $\Bbbk(V)$. The maximal ideal of $\mathcal{O}_P(V)$, consisting of all members of $\Bbbk(V)$ defined and vanishing at P, will be denoted by M_P. Theorem 7.23, translated into this notation, is as follows.

[14] The exposition in this section is based in part on Chapter I of Hartshorne's book, Chapter III of Reid's book, and Chapter II of Volume 1 of Shafarevich's books.

Theorem 10.47 (Zariski's Theorem, rephrased). In the above notation,

$$\dim_{\Bbbk}(M_P/M_P^2) = \dim_{\Bbbk}(\mathfrak{m}_P/\mathfrak{m}_P^2) \geq \dim V(\mathfrak{p}),$$

and P is nonsingular if and only if equality holds. The set of nonsingular points of $V(\mathfrak{p})$ is nonempty and open.

Toward the proof of this theorem, we showed in Section VII.5 for all $P \in V(\mathfrak{p})$ that

(a) $$\dim_{\Bbbk}(M_P/M_P^2) = \dim_{\Bbbk}(\mathfrak{m}_P/\mathfrak{m}_P^2),$$

(b) $$\dim_{\Bbbk}(\mathfrak{m}_P/\mathfrak{m}_P^2) + \operatorname{rank}\left[\tfrac{\partial f_i}{\partial X_j}(P)\right] = n,$$

(c) P is a nonsingular point if and only if $\dim_{\Bbbk}(\mathfrak{m}_P/\mathfrak{m}_P^2) = \dim V(\mathfrak{p})$.

In addition, we completed most of the proof in the special case that $V(\mathfrak{p})$ is an irreducible affine hypersurface by showing that

(d) $$\dim_{\Bbbk}(\mathfrak{m}_P/\mathfrak{m}_P^2) \geq \dim V(\mathfrak{p}) \qquad \text{for all } P \in V(\mathfrak{p}),$$

(e) $$\dim_{\Bbbk}(\mathfrak{m}_P/\mathfrak{m}_P^2) = \dim V(\mathfrak{p}) \qquad \text{for some } P \in V(\mathfrak{p}).$$

Our goal in this section is to complete the proof of Zariski's Theorem in the general case as stated by reducing (d) and (e) for the general case to what has already been proved for the special case that $V(\mathfrak{p})$ is an irreducible affine hypersurface. We need also to see in all cases that the set of nonsingular points is Zariski open.

Before proceeding, let us mention the significance of Theorem 10.47. The definition above of **nonsingular** and **singular** points extends immediately to quasi-affine varieties, using the same defining polynomials, and the theorem is then applicable because the open set of nonsingular points in an affine variety meets any nonempty open subset of the variety. In the projective case we can pull matters back to affine space by means of one of the maps $\beta_i : \mathbb{A}^n \to \mathbb{P}^n$. In this way we obtain definitions of **nonsingular** and **singular** point for quasiprojective varieties, and the theorem remains valid.[15] What is far from obvious with such a definition is that the decision nonsingular vs. singular for a point is unaffected by isomorphisms of varieties. On the other hand, the equivalent condition on M_P/M_P^2 as stated in Zariski's Theorem is manifestly unaffected by isomorphisms of varieties because of Proposition 10.42.

[15] Problems 13–16 at the end of the chapter show that the rank computation can alternatively be made directly with the homogeneous polynomials defining the projective variety in question.

Proposition 10.48. Any m-dimensional variety is birationally equivalent to an irreducible affine hypersurface H in $\mathbb{A}^{m+1}$.

PROOF. Let V be the variety in question. By definition of $\dim V$, the function field $\Bbbk(V)$ is a finitely generated extension field of $\Bbbk$ of transcendence degree m over $\Bbbk$. Since algebraically closed fields are perfect, Theorem 7.20 shows that $\Bbbk(V)$ is "separably generated" over $\Bbbk$, and Theorem 7.18 shows as a consequence that $\Bbbk(V)$ has a "separating transcendence basis," i.e., a transcendence basis $\{x_1, \dots, x_m\}$ such that $\Bbbk(V)$ is a finite separable algebraic extension of $\Bbbk(x_1, \dots, x_m)$. By the Theorem of the Primitive Element, there exists an element x_{m+1} of $\Bbbk(V)$ such that $\Bbbk(V) = \Bbbk(x_1, \dots, x_m)[x_{m+1}]$. Let $P(X_{m+1})$ be the minimal polynomial of x_{m+1} over $\Bbbk(x_1, \dots, x_m)$. Writing out the equation $P(x_{m+1}) = 0$ and clearing fractions, we see that x_{m+1} satisfies a polynomial equation

$$a_r(x_1, \dots, x_m)x_{m+1}^r + \cdots + a_1(x_1, \dots, x_m)x_{m+1} + a_0(x_1, \dots, x_m) = 0$$

in which the coefficient polynomials $a_j(X_1, \dots, X_m) \in \Bbbk[X_1, \dots, X_m]$ have no nontrivial common factor. In this case the polynomial $f(X_1, \dots, X_{m+1})$ equal to

$$a_r(X_1, \dots, X_m)X_{m+1}^r + \cdots + a_1(X_1, \dots, X_m)X_{m+1} + a_0(X_1, \dots, X_m)$$

is irreducible in $\Bbbk[X_1, \dots, X_{m+1}]$. Thus the principal ideal (f) defines an irreducible affine hypersurface $H = V(f)$ in $\mathbb{A}^{m+1}$ whose affine coordinate ring is $\Bbbk[X_1, \dots, X_{m+1}]/(f)$. The field of fractions $\Bbbk(H)$ is isomorphic to $\Bbbk(V)$, and H is birationally equivalent to V by the equivalence of (a) and (b) in Corollary 10.46. □

Lemma 10.49. Every point P in $V(\mathfrak{p})$ has $0 \le \dim_{\Bbbk}(M_P/M_P^2) \le n$, and the set of points P in $V(\mathfrak{p})$ with $\dim_{\Bbbk}(M_P/M_P^2) \ge r$ is a Zariski closed subset for each integer r.

PROOF. The entries of the matrix $\left[\frac{\partial f_i}{\partial X_j}\right]$ are polynomials, and the set of points P of $V(\mathfrak{p})$ for which the matrix $\left[\frac{\partial f_i}{\partial X_j}(P)\right]$ has rank $\le s$ is a Zariski closed subset, being the set on which all $(s+1)$-by-$(s+1)$ minors of the matrix vanish. By display formula (b) above, the set of points P for which $\dim_{\Bbbk}(\mathfrak{m}_P/\mathfrak{m}_P^2) \ge n - s$ is closed, and (a) therefore shows that the set with $\dim_{\Bbbk}(M_P/M_P^2) \ge n - s$ is closed. □

PROOF OF THEOREM 10.47. Let $m = \dim V(\mathfrak{p})$, and let a birational mapping of $V(\mathfrak{p})$ to an affine hypersurface H of $\mathbb{A}^{m+1}$ be given. By the equivalence of (a)

and (c) in Corollary 10.46, there exist nonempty open subsets E of $V(\mathfrak{p})$ and F of H that are isomorphic as varieties, say by an isomorphism $\varphi : E \to F$. Since $m = \dim V(\mathfrak{p}) = \dim H$, Proposition 10.11 shows that $m = \dim E = \dim F$ also. For each integer $r \geq 0$, let

$$\begin{aligned} S_r &= \big\{P \in V(\mathfrak{p}) \mid \dim_{\Bbbk}(M_P/M_P^2) \leq r\big\}, \\ T_r &= \big\{P \in E \mid \dim_{\Bbbk}(M_P/M_P^2) \leq r\big\}, \\ U_r &= \big\{P \in F \subseteq H \mid \dim_{\Bbbk}(M_P/M_P^2) \leq r\big\}. \end{aligned}$$

Lemma 10.49 shows that

$$S_r, T_r, U_r \text{ are relatively open in } V(\mathfrak{p}), E, F, \text{ respectively, for each } r. \tag{$*$}$$

Application of Proposition 10.42 to φ and φ^{-1} gives

$$\varphi(T_r) = U_r \qquad \text{for all } r \geq 0, \tag{$**$}$$

and the special case of Theorem 10.47 proved in Section VII.5 shows that

$$U_m \neq \varnothing \qquad \text{and} \qquad U_{m-1} = \varnothing. \tag{$\dagger$}$$

Combining ($**$) and ($\dagger$) yields

$$T_m \neq \varnothing \qquad \text{and} \qquad T_{m-1} = \varnothing. \tag{$\dagger\dagger$}$$

Since $S_r \supseteq T_r$, the first of these shows that

$$S_m \neq \varnothing. \tag{$\ddagger$}$$

If $S_{m-1} \neq \varnothing$, then $E \cap S_{m-1} \neq \varnothing$ because any two nonempty open subsets of $V(\mathfrak{p})$ have nonempty intersection; but $T_{m-1} = E \cap S_{m-1}$ would then be nonempty, in contradiction to ($\dagger\dagger$). Thus

$$S_{m-1} = \varnothing. \tag{$\ddagger\ddagger$}$$

In view of (a), ($\ddagger$) proves (e) for $V(\mathfrak{p})$, and ($\ddagger\ddagger$) proves (d) for $V(\mathfrak{p})$. Because of ($\ddagger\ddagger$), Lemma 10.49 implies that S_m is Zariski open; thus the set of nonsingular points is open. □

8. Classification Questions about Irreducible Curves

Sections 1–7 give the fundamentals concerning (quasiprojective) varieties over the algebraically closed field $\Bbbk$. The remainder of the chapter will address aspects of three problems:

(i) What are all varieties, or in what senses can varieties be classified?
(ii) To what extent can one make computations in the subject?
(iii) What can be said when the algebraically closed field $\Bbbk$ is replaced by a general commutative ring with identity?

Algebraic geometry is an enormous subject, going well beyond these problems. For example the investigation of the nature of singularities is in itself a large subject, with striking applications to topology and differential equations. The use of homological methods ties algebraic geometry closely to topology and to number theory, and these methods have bearing on the extent to which compact complex manifolds admit the structure of projective varieties. Algebraic geometry is an ingredient in the subject of invariant theory, which studies classical varieties using representation theory. It is an ingredient also in the subject of algebraic groups, which concerns varieties with a group structure in which multiplication and inversion are morphisms.

The present section concerns the first of the three problems listed above, and we limit our discussion to **irreducible curves**, i.e., to varieties of dimension 1. We say that an irreducible curve is **nonsingular** if it is nonsingular at every point. We are going to show in this section that each birational equivalence class of irreducible curves over $\Bbbk$ contains a nonsingular projective curve and that any two nonsingular projective curves in the birational equivalence class are isomorphic as projective varieties.[16] We also will get some information about how this nonsingular curve in the class is related to the other curves in the class. To a great extent the classification of irreducible curves will therefore have been reduced to the classification of the birational equivalence classes, which Corollary 10.46 says is the same thing as a classification of the function fields in one variable over $\Bbbk$. We will not have anything to say about classifying the function fields in one variable except to say that each class has a genus, according to Section IX.3, and that every nonnegative integer can arise as a genus, according to Example 3 of genus in Section IX.3.[17]

Chapter IX already contains clues about where to begin. Section IX.1 mentioned the relevance of Dedekind domains to the study, and Problems 5–11 at the end of that chapter attached a discrete valuation to each nonsingular point of any irreducible affine plane curve. The notions of Dedekind domains, discrete

[16]The exposition in this section is based in part on Chapter 7 of Fulton's book, Chapter I of Hartshorne's book, Chapter II of Reid's book, and Volume I by Zariski–Samuel.

[17]The subject of Teichmüller theory in effect addresses this question when $\Bbbk = \mathbb{C}$.

valuations, and nonsingular points are very closely related, and we begin with some equivalences concerning them. Recall from Sections 2 and 4 that the affine coordinate ring $A(C)$ of any irreducible affine curve C has Krull dimension 1. That is, the Noetherian domain $A(C)$ has the property that every nonzero prime ideal is maximal. We have seen that the local ring $\mathcal{O}_P(C)$ at any point is a localization of $A(C)$, namely the localization of $A(C)$ with respect to the maximal ideal $\mathfrak{m}_P$ of functions vanishing at P. Furthermore, the proper ideals of such a localization are exactly the sets $S^{-1}\mathfrak{a}$ with $\mathfrak{a}$ equal to an ideal disjoint from the set-theoretic complement of $\mathfrak{m}_P$ in $A(C)$. It follows that every nonzero prime ideal in $\mathcal{O}_P(C)$ is maximal. This conclusion extends to the quasiprojective case as a consequence of Proposition 10.33. Zariski's Theorem in Section 7 shows that nonsingularity of the point P of C can be detected from $\mathcal{O}_P(C)$. Consequently the following proposition is relevant.

Proposition 10.50. Let R be a Noetherian local ring that is an integral domain with the property that the only nonzero prime ideal is the maximal ideal. Let M be the unique maximal ideal of R, let K be the field of fractions of R, and let $F = R/M$ be the quotient field. Under the assumption that $M \neq 0$ and therefore that $R \neq K$, the following conditions on R are equivalent:

(a) R is integrally closed,
(b) R is a Dedekind domain,
(c) R is a principal ideal domain,
(d) R is the valuation ring relative to some discrete valuation of K,
(e) M is a principal ideal,
(f) $\dim_F M/M^2 = 1$.

REMARKS. Consider (f). To see how M/M^2 becomes an F vector space in a natural way, let $r + M$ be a member of F, and let $m + M^2$ be a member of M/M^2. Then $(r + M)(m + M^2) = rm + M^2$ is a well-defined scalar multiplication of F on M/M^2, and M/M^2 becomes a vector space over F. Nakayama's Lemma (Lemma 8.51 of *Basic Algebra*, restated in the present book on page xxv) shows that an equality $MN = N$ for a finitely generated R module N is possible only if $N = 0$; since M itself is a finitely generated R module, being an ideal in a Noetherian ring, and since $M \neq 0$ by assumption, $M^2 = M$ is not possible. Therefore $\dim_F M/M^2 \geq 1$.

PROOF. If (a) holds, then R satisfies the three conditions (Noetherian, integrally closed, every nonzero prime ideal maximal) in the definition of Dedekind domain. Thus (a) implies (b). A Dedekind domain with only finitely many maximal ideals is a principal ideal domain by Corollary 8.62 of *Basic Algebra*, and thus (b) implies (c). A principal ideal domain is a unique factorization domain by Theorem 8.15 of *Basic Algebra*, and thus (c) implies (a) by Proposition 8.41 of *Basic Algebra*.

To see that (a) through (c) are equivalent to (d), first suppose that (a) through (c) hold. Then every fractional ideal in K relative to R is of the form M^k for some integer k. If $x \neq 0$ is in K, then the principal fractional ideal xR is of the form $xR = M^k$ for some k. Section VI.2 shows that the formula $v(x) = k$ (with $v(0) = \infty$) defines a discrete valuation on K, and the definition of v shows that the valuation ring of v is R. Hence (d) holds. Conversely if (d) holds, then R is a principal ideal domain by Proposition 6.2; thus (c) and necessarily (a) and (b) hold.

Let us prove that (e) and (f) are equivalent. If (e) holds, then we can write $M = (\pi)$ for some π in R. If $m + M^2$ is a given element of M/M^2, then m is of the form $m = r\pi$ for some r in R. Hence $(r + M)(\pi + M^2) = r\pi + M^2 = m + M^2$, and $\dim_F M/M^2 \leq 1$. Since the remarks before the proof show that $\dim_F M/M^2 \geq 1$, (f) holds.

If (f) holds, let $\{\pi + M^2\}$ be an F basis of M/M^2. If $m \in M$ is given, then $m + M^2 = (r + M)(\pi + M^2)$ for some $r \in R$. Therefore $m = r\pi + m'$ with $m' \in M^2$, and we see that $(\pi) + M^2 = M$. We shall apply Nakayama's Lemma in the local ring $R/(\pi)$ with maximal ideal $M/(\pi)$ and with module $N = M/(\pi)$: Given $m \in M$, we expand $m = r\pi + m'$ with $m' \in M^2$ as $m = r\pi + \sum_{i,j} m_i m_j$. Then the equality $m + (\pi) = \sum_{i,j} m_i m_j$ in $M/(\pi)$ shows that $m \equiv \sum_i m_i \sum_j m_j$, hence that the coset $m + (\pi)$ lies in $\sum_i (m_i + (\pi))(M/(\pi))$. In other words, $M/(\pi) = (M/(\pi))^2$. Nakayama's Lemma shows that $M/(\pi) = 0$, and therefore $M = (\pi)$. Thus (e) holds.

Finally let us prove that (c) and (e) are equivalent. If (c) holds, then M has to be principal, and hence (e) holds. Suppose that (e) holds, i.e., that $M = (\pi)$. Let I be a nonzero proper ideal in R. The ideal $N = \bigcap_{k=1}^{\infty} M^k$ is a finitely generated R module because R is Noetherian, and it has $MN = N$. By Nakayama's Lemma, $N = 0$. Since $I \subseteq M$ and since $I \neq 0$, there exists a largest integer $k \geq 1$ such that $I \subseteq M^k$. Choose $y \neq 0$ in I with y in $M^k = (\pi^k)$ but not in $M^{k+1} = (\pi^{k+1})$. Let us write $y = a\pi^k$ for some $a \in R$. Since y is not in M^{k+1} and since R is local, a is a unit in R. Hence $a^{-1}y = \pi^k$ is in I, and therefore $M^k = (\pi^k) \subseteq I$. Since we arranged that $I \subseteq M^k$, we obtain $I = M^k = (\pi^k)$. Thus (c) holds. □

Corollary 10.51. Let C be an irreducible quasiprojective curve over $\Bbbk$, and let $\Bbbk(C)$ be its function field. If P is a point of C, then the following conditions are equivalent:

(a) P is a nonsingular point,
(b) $\mathcal{O}_P(C)$ is the valuation ring of some discrete valuation of $\Bbbk(C)$ defined over $\Bbbk$,
(c) $\mathcal{O}_P(C)$ is integrally closed.

PROOF. Let M_P be the unique maximal ideal of $\mathcal{O}_P(C)$. Zariski's Theorem (Theorem 10.47) shows that (a) holds if and only if $\dim_{\Bbbk} M_P/M_P^2 = 1$. The

corollary therefore follows from the equivalence of (f), (d), and (a) in Proposition 10.50, along with the observation that any discrete valuation produced by (d) has to be 0 on $\Bbbk^\times$. □

Corollary 10.52. If C is an irreducible affine curve over $\Bbbk$ with affine coordinate ring $A(C)$, then the following conditions on C are equivalent:

(a) $A(C)$ is integrally closed,
(b) $\mathcal{O}_P(C)$ is integrally closed for each point P of the curve,
(c) C is nonsingular.

PROOF. If $A(C)$ is integrally closed, then Corollary 8.48c of *Basic Algebra* shows that each localization $\mathcal{O}_P(C)$ is integrally closed. Conversely if each $\mathcal{O}_P(C)$ is integrally closed and if a member f of the function field $\Bbbk(C)$ is given that is a root of a monic polynomial with coefficients in $A(C)$, then f is a root of the same polynomial with coefficients in $\mathcal{O}_P(C)$ and is in $\mathcal{O}_P(C)$ because $\mathcal{O}_P(C)$ is integrally closed. Corollary 10.25 shows that $A(C) = \bigcap_P \mathcal{O}_P(C)$. Therefore f lies in $A(C)$, and $A(C)$ is integrally closed. This proves that (a) and (b) are equivalent. The equivalence of (b) and (c) follows from Corollary 10.51. □

We turn our attention to constructing a nonsingular irreducible projective curve whose field of rational functions is a given function field $\mathbb{K}$ in one variable over $\Bbbk$. If C is any irreducible quasiprojective curve with $\Bbbk(C) = \mathbb{K}$, then Corollary 10.51 associates a discrete valuation of $\mathbb{K}$ over $\Bbbk$ to each nonsingular point of C. To get an idea what C must be like if it is to be nonsingular at every point, we now prove a theorem in the converse direction, associating a point of the curve to each discrete valuation of $\mathbb{K}$ over $\Bbbk$.

Theorem 10.53. Let C be an irreducible projective curve with function field $\Bbbk(C)$ equal to $\mathbb{K}$, and let v be a discrete valuation of $\mathbb{K}$ defined over $\Bbbk$. If R_v is the valuation ring of v and $\mathfrak{p}_v$ is the valuation ideal, then there exists a unique point P on the curve for which the maximal ideal M_P of $\mathcal{O}_P(C)$ has $M_P \subseteq \mathfrak{p}_v$.

PROOF OF UNIQUENESS. Assume the contrary. If P and Q are distinct points with $M_P \subseteq \mathfrak{p}_v$ and $M_Q \subseteq \mathfrak{p}_v$, then Proposition 10.36 constructs a function h in $\Bbbk(C)$ with h defined at P and Q, $h(P) = 0$, and $h(Q) \neq 0$. This function h is in M_P, and $h - h(Q)$ is in M_Q. The assumed inclusions of maximal ideals imply that $v(h) \geq 1$ and that $v(h - h(Q)) \geq 1$. On the other hand, $h(Q) \neq 0$ implies that $v(h(Q)) = 0$. Thus $0 = v(h(Q)) \geq \min\big(v(h(Q) - h), v(h)\big) \geq 1$, contradiction. □

PROOF OF EXISTENCE. It is shown in Problem 12 at the end of the chapter that any projective variety in $\mathbb{P}^r$ is isomorphic to a projective variety V in some $\mathbb{P}^n$ with $n \leq r$ such that V is not contained in any subvariety $\big\{[x_0, \dots, x_n] \mid x_j = 0\big\}$

with $0 \le j \le n$. That being so, we may assume that C is a projective variety in $\mathbb{P}^n$ and that $C \cap \beta_j(\mathbb{A}^n) \neq \varnothing$ for $0 \le j \le n$, where $\beta_j : \mathbb{A}^n \to \mathbb{P}^n$ is the embedding defined after Proposition 10.18. Let $\widetilde{A}(C) = \Bbbk[X_0, \ldots, X_n]/I(C)$ be the homogeneous coordinate ring of C, and for each j, let x_j be the image of X_j in $\widetilde{A}(C)$. Since $I(C)$ does not contain X_j, x_j is not the 0 element of $\widetilde{A}(C)$. Since X_i and X_j are homogeneous of the same degree, each function x_i/x_j is a well-defined member of the function field $\Bbbk(C)$.

Let $N = \max_{i,j} v(x_i/x_j)$. Possibly by renaming some coordinate x_{j_0} as x_0, we may assume that $v(x_{i_0}/x_0) = N$ for some i_0. Then we have $v(x_i/x_0) = v(x_{i_0}/x_0) + v(x_i/x_{i_0}) = N - v(x_{i_0}/x_i) \ge 0$ for all i. Consequently each function x_i/x_0 lies in the subring R_v of $\Bbbk(C)$.

Theorem 10.20 and Corollary 10.22 show that $C_0 = \beta_0^{-1}(C)$ is an irreducible affine curve and that its prime ideal is $I(C_0) = \beta_0^t(I(C))$. Consequently the substitution homomorphism $\beta_0^t : \Bbbk[X_0, \ldots, X_n] \to \Bbbk[X_1, \ldots, X_n]$ descends to a homomorphism of $\widetilde{A}(C) = \Bbbk[X_0, \ldots, X_n]/I(C)$ onto $A(C_0) = \Bbbk[X_1, \ldots, X_n]/I(C_0)$ that carries x_0 in $\widetilde{A}(C)$ to 1 and carries the members $x_1, \ldots, x_n$ of $\widetilde{A}(C)$ to the generators of $A(C_0)$. The members x_i/x_0 of $\Bbbk(C)$ therefore get identified with the generators of $A(C_0)$, and we conclude that $A(C_0) \subseteq R_v$.

Define $\mathfrak{q} = \mathfrak{p}_v \cap A(C_0)$. This is a prime ideal of $A(C_0)$, and it pulls back under the quotient homomorphism $\Bbbk[X_1, \ldots, X_n] \to A(C_0)$ to a prime ideal $\widetilde{\mathfrak{q}}$ containing $I(C_0)$. Then $V(\widetilde{\mathfrak{q}})$ is an affine subvariety of C_0. Since $\dim C_0 = 1$, there are only two possibilities. One is that $\dim V(\widetilde{\mathfrak{q}}) = 1$, in which case $V(\widetilde{\mathfrak{q}}) = C_0$, $\widetilde{\mathfrak{q}} = I(C_0)$, and $\mathfrak{q} = 0$. The other is that $\dim V(\widetilde{\mathfrak{q}}) = 0$, in which case $V(\widetilde{\mathfrak{q}}) = \{P\}$ for some point P that necessarily lies on C_0. In the first case, v is 0 on every nonzero member of $A(C)$ and hence is 0 on $\Bbbk(C)^\times$, contradiction. Thus we are in the second case. Then $\widetilde{\mathfrak{q}}$ is maximal in $\Bbbk[X_1, \ldots, X_n]$, $\mathfrak{q}$ is maximal in $A(C_0)$, $\mathfrak{q}$ is the ideal $\mathfrak{m}_P$ of all members of $A(C_0)$ vanishing at P, and $A(C_0)/\mathfrak{q} \cong \Bbbk$. If S denotes the set-theoretic complement of $\mathfrak{q}$ in $A(C_0)$, then no member of S can be in $\mathfrak{p}_v$ because then $\mathfrak{q} + \Bbbk 1 = A(C_0)$ would be in $\mathfrak{p}_v$, contradiction. Thus $v(s) = 0$ for all $s \in S$, and $M_P = S^{-1}\mathfrak{m}_P \subseteq \mathfrak{p}_v$. □

Corollary 10.54. If φ is a rational map from an irreducible curve C' to an irreducible projective curve C, then the largest domain on which φ is a morphism contains every nonsingular point of C'. If C' is nonsingular, then φ is a morphism from C' into C.

PROOF. If φ is not dominant, then Problem 6 at the end of the chapter shows that φ is constant. Certainly the largest domain on which a constant φ is a morphism is C'.

Thus suppose that φ is dominant. Using the notation introduced early in Section 6, let $\widetilde{\varphi} : \Bbbk(C) \to \Bbbk(C')$ be the associated field map of function fields.

Since $\Bbbk(C)$ and $\Bbbk(C')$ both have transcendence degree 1 over $\Bbbk$ and since $\Bbbk(C)$ is finitely generated as a field over $\Bbbk$, the field $\Bbbk(C')$ is a finite algebraic extension of the field $\widetilde{\varphi}(\Bbbk(C))$. If v is any discrete valuation of $\Bbbk(C')$, then it follows from the finiteness of this extension that v cannot be identically 0 on $\widetilde{\varphi}(\Bbbk(C))^\times$; in fact, if it were identically 0, then the expansion $x = \sum_{j=1}^m c_j x_j$ of a general element x of $\Bbbk(C')$ in terms of a vector-space basis $\{x_1, \dots, x_m\}$ of $\Bbbk(C')$ over $\widetilde{\varphi}(\Bbbk(C))$ would yield the inequality $v'(x) \geq \min_j v(x_j)$, which cannot be true for all x.

Meanwhile, if P is a nonsingular point of C', then Corollary 10.51 shows that $\mathcal{O}_P(C')$ is the valuation ring R_v for some valuation v of $\Bbbk(C')$ over $\Bbbk$. The maximal ideal M_P of $\mathcal{O}_P(C')$ equals the valuation ideal $\mathfrak{p}_v$ of v. Since the restriction of v to $\widetilde{\varphi}(\Bbbk(C))^\times$ is not identically 0, the restriction comes from some positive multiple e of a discrete valuation on $\widetilde{\varphi}(\Bbbk(C))$. Let v_0 be the corresponding discrete valuation of $\Bbbk(C)$; this is given by $v_0(f) = e^{-1}v(\widetilde{\varphi}(f))$. Let R_0 be its valuation ring and $\mathfrak{p}_0$ be its valuation ideal in $\Bbbk(C)$; the latter is given by $\mathfrak{p}_0 = \widetilde{\varphi}^{-1}(\mathfrak{p}_v)$. Theorem 10.53 shows that there exists a unique point Q on the curve C such that the maximal ideal M_Q of $\mathcal{O}_Q(C)$ is contained in $\mathfrak{p}_0$. That is, $M_Q \subseteq \mathfrak{p}_0 = \widetilde{\varphi}^{-1}(\mathfrak{p}_v)$. Application of $\widetilde{\varphi}$ gives $\widetilde{\varphi}(M_Q) \subseteq \widetilde{\varphi}\widetilde{\varphi}^{-1}(\mathfrak{p}_v) \subseteq \mathfrak{p}_v = M_P$. Theorem 10.45 shows that consequently P is in the largest domain on which φ is a morphism and that $\varphi(P) = Q$. □

Corollary 10.55. If two nonsingular irreducible projective curves are birationally equivalent, then they are isomorphic as varieties.

PROOF. This follows by applying Corollary 10.54 twice. □

Corollary 10.56. If C is a nonsingular irreducible projective curve with function field $\mathbb{K} = \Bbbk(C)$, then the points of C are in one-one correspondence with the discrete valuations of $\mathbb{K}$ defined over $\Bbbk$.

PROOF. This is the correspondence given in one direction by Corollary 10.51 and in the reverse direction by Theorem 10.53. □

Corollary 10.56 has a remarkable conclusion, but the corollary assumes the existence of a nonsingular projective curve, which we have not yet proved. In more detail we now know that a nonsingular point P of any irreducible projective curve C picks out a unique discrete valuation v of the function field $\mathbb{K} = \Bbbk(C)$, namely the one whose valuation ring is given by $R_v = \mathcal{O}_P(C)$, and that conversely when C is projective, any discrete valuation v' defined over $\Bbbk$ picks out a certain point P' of C with the property that $\mathcal{O}_{P'}(C) \subseteq R_{v'}$. If P is nonsingular and we go through the first step and then the second, using $v' = v$, we obtain $\mathcal{O}_{P'}(C) \subseteq \mathcal{O}_P(C)$. Proposition 10.36 shows that $P' = P$, and hence the second process inverts the first. That is what Corollary 10.56 says. Also, we know from Theorem 10.47 that many discrete valuations are involved in this process, since the set of nonsingular

points of a variety is Zariski open. What we do not know is that any given discrete valuation over $\Bbbk$ ever yields a nonsingular point for *any* curve with the function field $\mathbb{K}$. This missing piece of information will be supplied in Corollary 10.58 below. To prove Corollary 10.58, we shall make use of the following theorem, which we need only in the case that the field k is our algebraically closed field $\Bbbk$. We postpone the proof of the theorem for a moment, and when we give the proof, we shall give it only for the case that the field k in the statement is algebraically closed.

Theorem 10.57. Let k be a field, let $R = k[x_1, \ldots, x_n]$ be a finitely generated integral domain over k, let K be the field of fractions of R, and let L be a finite algebraic extension of K. Then the integral closure T of R in L is a finitely generated R module.

Corollary 10.58. Let C be an irreducible projective curve with function field $\mathbb{K} = \Bbbk(C)$, let P be a point of C, and let M_P be the maximal ideal of $\mathcal{O}_P(C)$. Then there exists a discrete valuation v of $\mathbb{K}$ defined over $\Bbbk$ whose valuation ideal $\mathfrak{p}_v$ has $M_P \subseteq \mathfrak{p}_v$.

REMARKS. This result is a supplement to Theorem 10.53. It says that the map of that theorem, carrying discrete valuations of $\mathbb{K}$ defined over $\Bbbk$ to points of C, is onto.

PROOF. Without loss of generality, we may assume that C is affine. Let $\mathfrak{m}_P$ be the maximal ideal in the affine coordinate ring $A(C)$ consisting of all functions vanishing at P, and let S be the set-theoretic complement of $\mathfrak{m}_P$ in $A(C)$, so that $M_P = S^{-1}\mathfrak{m}_P$. Evaluation at P is a linear functional on $A(C)$ with kernel $\mathfrak{m}_P$, and therefore $A(C) = \mathfrak{m}_P + \Bbbk 1$. In other words, $\mathfrak{m}_P$ and any element of S together generate $A(C)$ as a $\Bbbk$ vector space.

If T denotes the integral closure of $A(C)$ in $\mathbb{K}$, then Theorem 10.57 implies that T is Noetherian, and Proposition 8.45 of *Basic Algebra* shows that every nonzero prime ideal of T is maximal. Hence T is a Dedekind domain. Proposition 8.53 of *Basic Algebra* shows that there exists a maximal ideal $\mathfrak{q}$ of T such that $\mathfrak{m}_P = A(C) \cap \mathfrak{q}$. Since T is a Dedekind domain, $\mathfrak{q}$ is contained in the valuation ideal $\mathfrak{p}_v$ of a unique discrete valuation v of $\mathbb{K}$, and T is contained in the valuation ring T_v of v. Thus $\mathfrak{m}_P \subseteq \mathfrak{p}_v$, and $S \subseteq T$ implies that $v(s) \geq 0$ for all $s \in S$. On the other hand, 1 lies in $\mathfrak{m}_P + \Bbbk s$ for any s in S, and hence $0 = v(1) \geq \min(1, v(s))$. Therefore $v(s) = 0$ for all $s \in S$, and $M_P = S^{-1}\mathfrak{m}_P \subseteq \mathfrak{p}_v$. □

Corollary 10.59. If $\mathbb{K}$ is a function field in one variable over $\Bbbk$ and if v is a discrete valuation of $\mathbb{K}$ defined over $\Bbbk$ with valuation ring R_v, then there exists an irreducible nonsingular *affine* curve C over $\Bbbk$ with function field $\mathbb{K}$ and with a point P such that $\mathcal{O}_P(C) = R_v$.

PROOF. Choose an element x of $\mathbb{K}$ such that $v(x) > 0$. Define $R = \Bbbk[x]$. Since $v(x) \neq 0$, x is transcendental over $\Bbbk$, and $\mathbb{K}$ is a finite algebraic extension of the field of fractions $\Bbbk(x)$ of R. Corollary 7.14 shows that the integral closure T of R in $\mathbb{K}$ is a Dedekind domain, and Theorem 10.57 shows that T is a finitely generated R module. Thus we can write T as $T = \Bbbk[x_1, \ldots, x_n]$ with $x_1 = x$. The substitution homomorphism with $X_j \mapsto x_j$ for all j carries $\Bbbk[X_1, \ldots, X_n]$ onto T and has a prime ideal $\mathfrak{p}$ as kernel, since T is an integral domain. Thus $V(\mathfrak{p})$ is an affine variety with T as its affine coordinate ring. The dimension of $V(\mathfrak{p})$ is the transcendence degree of $\mathbb{K}$ over $\Bbbk$, which is 1 by assumption. Thus $C = V(\mathfrak{p})$ is an irreducible curve. Since T is integrally closed by construction, Corollary 10.52 shows that C is nonsingular.

Let $R_v \subseteq \mathbb{K}$ be the valuation ring of v, and let $\mathfrak{p}_v$ be the valuation ideal. The inequality $v(x) > 0$ shows that v is ≥ 0 on $R = \Bbbk[x]$, and Proposition 6.7 says that v is consequently ≥ 0 on the integral closure T of R in $\mathbb{K}$. In other words, T is contained in R_v. Since T is a Dedekind domain and $\mathbb{K}$ is its field of fractions, Theorem 6.5 shows that $\mathfrak{q} = \mathfrak{p}_v \cap T$ is a nonzero prime (= maximal) ideal of T and that the discrete valuation $v_{\mathfrak{q}}$ of $\mathbb{K}$ over $\Bbbk$ determined by $\mathfrak{q}$ coincides with v. The maximal ideals of the affine coordinate ring of an affine variety correspond to the points of the variety by Proposition 10.23, and thus there exists a point P of C such that $\mathfrak{q}$ is the maximal ideal of T consisting of all functions vanishing at P. The localization of T with respect to $\mathfrak{q}$ is $\mathcal{O}_P(C)$ by definition and is R_v by Proposition 6.4. Therefore $\mathcal{O}_P(C) = R_v$. □

Corollary 10.60. Let C be the irreducible nonsingular affine curve constructed in Corollary 10.59 and having function field $\mathbb{K} = \Bbbk(C)$, and regard C as a subvariety of its projective closure $\overline{C}$. Then there are only finitely many discrete valuations v' of $\mathbb{K}$ defined over $\Bbbk$ such that the unique point P of $\overline{C}$ with $M_P \subseteq \mathfrak{p}_{v'}$, where M_P is the maximal ideal of $\mathcal{O}_P(\overline{C})$ and $\mathfrak{p}_{v'}$ is the valuation ideal of v', lies outside C.

PROOF. We go over the argument in Corollary 10.59 with the same element x and with any discrete valuation v' defined over $\Bbbk$ such that $v'(x) \geq 0$. This inequality implies that v' is ≥ 0 on $\Bbbk[x]$, and Proposition 6.7 then shows that v' is ≥ 0 on $T = A(C)$. Thus $A(C)$ is contained in the valuation ring $R_{v'}$ of v'. Define $\mathfrak{q} = \mathfrak{p}_{v'} \cap A(C)$. Arguing as in the existence proof for Theorem 10.53, we find that $\mathfrak{q}$ equals the ideal $\mathfrak{m}_P$ of all members of $A(C)$ vanishing at a certain point P of C, and that proof then shows that $M_P \subseteq \mathfrak{p}_{v'}$. By uniqueness in Theorem 10.53, this P is the one and only point produced by that theorem.

In other words, the only discrete valuations v' of $\mathbb{K}$ defined over $\Bbbk$ for which the point P lies outside C are those with $v'(x) < 0$. Corollary 6.10 shows that there are only finitely many of these. □

We come to the proof of Theorem 10.57, but only under the assumption that k is algebraically closed. The proof is rather technical, and the reader is encouraged to skip it on first reading. To underscore this point, the proof appears in small print. We need two lemmas.

Lemma 10.61. Let R be a Noetherian integrally closed domain with field of fractions F, let K be a finite *separable* extension of F, and let T be the integral closure of R in K. Then T is Noetherian and is finitely generated as an R module.

PROOF. In effect, this result was proved in *Basic Algebra*. In more detail: With the above assumptions and also the assumption that every nonzero prime ideal of R is maximal (i.e., that R is a Dedekind domain), the proof of Theorem 8.54 of *Basic Algebra* showed that T is a Dedekind domain. The hard part of that proof appeared in Section IX.15; it showed from the separability that T is finitely generated as an R module, and it did not make use of the assumption that every nonzero prime ideal of R is maximal. Since T is finitely generated and R is Noetherian, every R submodule of T is a finitely generated R module, by Proposition 8.34 of *Basic Algebra*. In particular, every ideal of T is finitely generated as an R module and therefore is finitely generated as a T module. Consequently T is Noetherian. □

Lemma 10.62 (Noether Normalization Lemma). Let k be an infinite field, let $R = k[x_1, \dots, x_n]$ be a finitely generated integral domain over k, and let $K = k(x_1, \dots, x_n)$ be the field of fractions of k. Then for a suitable d with $0 \le d \le n$, there exist d linear combinations $y_1, \dots, y_d$ of $x_1, \dots, x_n$ with coefficients in k such that $y_1, \dots, y_d$ are algebraically independent over k and such that every element of R is integral over $k[y_1, \dots, y_d]$. If K is separably generated over k, then the y_i may be chosen in such a way that K is a separable extension of $k(y_1, \dots, y_d)$.

REMARKS. It is immediate from the conclusion that d is the transcendence degree of K over k. The lemma is a result about the extension of rings that improves upon Theorem 7.7 for fields; the latter says that every field extension can be accomplished by a transcendental extension followed by an algebraic extension. The present lemma says that the passage from a field to a finitely generated integral domain can be accomplished by a full polynomial extension followed by an extension in which each generator is not merely algebraic but actually is a root of a monic polynomial with coefficients in the full polynomial ring.

PROOF. Let I be the kernel of the quotient homomorphism $k[X_1, \dots, X_n] \to k[x_1, \dots, x_n]$. The core of the proof involves a single nonzero f in I. The idea is to replace $X_1, \dots, X_{n-1}$ by new indeterminates $X'_1, \dots, X'_{n-1}$ to make the equation $f(x_1, \dots, x_n) = 0$ become a monic polynomial equation satisfied by x_n over $R' = k[X'_1, \dots, X'_{n-1}]$. With $c_1, \dots, c_{n-1}$ equal to members of k to be specified later, define $x'_j = x_j - c_j x_n$ for $1 \le j \le n-1$. The equation $f(x_1, \dots, x_n) = 0$ becomes

$$f(x'_1 + c_1 x_n, \dots, x'_{n-1} + c_{n-1} x_n, x_n) = 0. \tag{$*$}$$

For a suitable choice of $c_1, \dots, c_{n-1}$, we shall show in a moment that

$$\text{the polynomial} \quad f(X'_1 + c_1 X_n, \dots, X'_{n-1} + c_{n-1} X_n, X_n) \quad \text{is monic in } X_n \tag{$**$}$$

after multiplication by a member of $k^\times$.

Assuming $(**)$, let us see how the first conclusion of the lemma follows by induction on n. For $n = 1$, there are two cases. One case is that K is a simple algebraic extension field of k, and then every element of the extension field $R = K$ is a root of its minimal polynomial over k. This is the case $d = 0$. The other case is that K is a simple transcendental extension, and then we can take $y_1 = x_1$. This is the case $d = 1$.

For the inductive step, assume the first conclusion of the lemma for $n - 1 \ge 1$, d being an integer with $0 \le d \le n - 1$. If $I = 0$, there is nothing to prove, since $x_1, \dots, x_n$ are then algebraically

independent and the lemma follows with $d = n$ and with $y_j = x_j$ for $1 \le j \le n$. If $I \ne 0$, fix $f \ne 0$ in I, and choose $c_1, \dots, c_{n-1}$ in k to make $(**)$ hold. Then $(*)$ shows that x_n is a root of a monic polynomial with coefficients in $R' = k[x'_1, \dots, x'_{n-1}]$. By the inductive hypothesis we can choose members $y'_1, \dots, y'_d$ of R' with $0 \le d \le n-1$ such that $y'_1, \dots, y'_d$ are algebraically independent over k and such that every element of R' is integral over $k[y'_1, \dots, y'_d]$. By transitivity of integral dependence, every element of $R'[x_n]$ is integral over $k[y'_1, \dots, y'_d]$. Since the definition of x'_j in terms of x_j shows that $R'[x_n] = k[x'_1, \dots, x'_{n-1}, x_n] = k[x_1, \dots, x_{n-1}, x_n] = R$, every element of R is integral over $k[y'_1, \dots, y'_d]$. This completes the induction, and the first sentence of conclusions of the lemma is proved except for $(**)$.

To prove $(**)$, let $r = \deg f$, and write $f = h_r + g$ with h_r nonzero and homogeneous of degree r and with $\deg g \le r-1$ (or $g = 0$). Then

$$\begin{aligned} f(X_1, \dots, X_n) &= f(X'_1 + c_1 X_n, \dots, X'_{n-1} + c_{n-1} X_n, X_n) \\ &= h_r(c_1 X_n, \dots, c_{n-1} X_n) + (\text{terms involving } 1, X_n, X_n^2, \dots, X_n^{r-1}) \\ &= h_r(c_1, \dots, c_{n-1}, 1) X_n^r + (\text{terms involving } 1, X_n, X_n^2, \dots, X_n^{r-1}). \end{aligned}$$

Thus $(**)$ is proved if $c_1, \dots, c_{n-1}$ can be chosen with the scalar $h_r(c_1, \dots, c_{n-1}, 1)$ not 0. Here the fact that h_r is nonzero and homogeneous implies that $h_r(X_1, \dots, X_{n-1}, 1)$ is not the 0 polynomial in $k[X_1, \dots, X_{n-1}]$. Since k is an infinite field, Corollary 4.32 of *Basic Algebra* shows that the evaluation mapping of $k[X_1, \dots, X_{n-1}]$ into the algebra of functions from k^{n-1} into k is one-one, and therefore there exist $c_1, \dots, c_{n-1}$ with $h_r(c_1, \dots, c_{n-1}, 1) \ne 0$. This proves $(**)$.

We are left with proving that if K is separably generated over k, then the y_i may be chosen with K separable over $k(y_1, \dots, y_d)$. We proceed as above but with an amended version of $(**)$ that we mention in a moment. In the induction the extra hypothesis for $n = 1$ is that either x_1 is separable algebraic over k or x_1 is transcendental, and in both cases K is a separable extension of $k(y_1)$. For the inductive step when $I \ne 0$, Theorem 7.18 shows that $\{x_1, \dots, x_n\}$ contains a separating transcendence basis; possibly by renumbering the variables, we may assume that this transcendence basis is a subset of $\{x_1, \dots, x_{n-1}\}$. In particular, x_n is separable algebraic over $k(x_1, \dots, x_{n-1})$. For the polynomial f, we start from the minimal polynomial of x_n over $k(x_1, \dots, x_{n-1})$, next multiply by a common denominator to get all coefficients of powers of X_n to be in $k[x_1, \dots, x_{n-1}]$, and then replace the occurrences of $x_1, \dots, x_{n-1}$ by $X_1, \dots, X_{n-1}$. The result is f. We choose $y'_1, \dots, y'_d$ as above, and the inductive hypothesis shows that $k(x'_1, \dots, x'_{n-1})$ is separable over $k(y'_1, \dots, y'_d)$. If we can show that x_n is separable over $k(x'_1, \dots, x'_{n-1})$, then we will have proved that K is a separable extension of $k(y'_1, \dots, y'_d)$ because of the transitivity of separability. So the induction will be complete.

To get that x_n is separable over $k(x'_1, \dots, x'_{n-1})$, it is enough to prove that we can arrange for

$$x_n \quad \text{to be a simple root of} \quad f(x'_1 + c_1 X_n, \dots, x'_{n-1} + c_{n-1} X_n, X_n) \tag{$\dagger$}$$

in addition to $(**)$. Indeed, then x_n is a root of a separable polynomial over $k(x'_1, \dots, x'_{n-1})$ and hence is a separable element over $k(x'_1, \dots, x'_{n-1})$. The condition $(\dagger)$ is the same as the condition that the derivative of $(\dagger)$ with respect to X_n, when evaluated at x_n, be nonzero. Thus we want to arrange that

$$f_n(x_1, \dots, x_{n-1}, x_n) + c_1 f_1(x_1, \dots, x_{n-1}, x_n) + \cdots + c_{n-1} f_{n-1}(x_1, \dots, x_{n-1}, x_n) \ne 0, \tag{$\dagger\dagger$}$$

where the subscripts on f indicate first partial derivatives in the indicated variables. The left side of $(\dagger\dagger)$ is the sum of a constant and a linear functional on the vector space of all $(c_1, \dots, c_{n-1})$ in k^{n-1}. The constant term is $f_n(x_1, \dots, x_{n-1}, x_n)$, which is nonzero because x_n is separable over $k(x_1, \dots, x_{n-1})$ and is therefore a simple root of its minimal polynomial over $k(x_1, \dots, x_{n-1})$. Thus the left side of $(\dagger\dagger)$ is the value of a nonzero polynomial $p(X_1, \dots, X_{n-1}) = a_n + \sum_{j=1}^{n-1} a_j X_j$ at $(c_1, \dots, c_{n-1})$. Consequently $(**)$ and $(\dagger\dagger)$ will hold simultaneously if we choose a point $(c_1, \dots, c_{n-1})$ in k^{n-1} at which the nonzero polynomial $p(X_1, \dots, X_{n-1}) h_r(X_1, \dots, X_{n-1}, 1)$ is not zero. □

PROOF OF THEOREM 10.57 UNDER THE ASSUMPTION THAT k IS ALGEBRAICALLY CLOSED. The first step is to reduce to the case that $L = K$, i.e., that the field of fractions of R coincides with L. To do so, choose a vector-space basis $\{z_1, \ldots, z_r\}$ of L over K consisting of elements integral over R; this is possible by Proposition 8.42 of *Basic Algebra*. Put $S = R[z_1, \ldots, z_r]$. This is a finitely generated integral domain over k, all of its elements are integral over k, and it has L as field of fractions. The integral closure of R in L equals the integral closure of S in L.

Thus we may assume that $R = k[x_1, \ldots, x_n]$ is an integral domain with field of fractions K and that we are to prove that the integral closure T of R in K is a finitely generated R module. Let d be the transcendence degree of K over k. Since algebraically closed fields are perfect, Theorem 7.20 shows that K is separably generated over k. Lemma 10.62 is therefore applicable, and it produces d linear combinations $y_1, \ldots, y_d$ of $x_1, \ldots, x_n$ over k such that the subring $S = k[y_1, \ldots, y_d]$ of R is a full polynomial ring, every element of R is integral over S, and K is a separable extension of the field $k(y_1, \ldots, y_d)$. Since every element of T is integral over R, the transitivity of integral dependence implies that every element of T is integral over S. Therefore T is the integral closure of S in K. Being a full polynomial ring, S is Noetherian and is a unique factorization domain; the latter property implies that S is integrally closed, according to Proposition 8.41 of *Basic Algebra*. Taking S to be the Noetherian integrally closed domain in Lemma 10.61, we see that T is finitely generated as an S module. Since $S \subseteq R$, T is certainly finitely generated as an R module. □

Now we come to the main theorem of this section.

Theorem 10.63. Every birational equivalence class of irreducible projective curves contains a nonsingular such curve, and this curve is unique within the equivalence class up to isomorphism of varieties. Any irreducible nonsingular quasiprojective curve is isomorphic to an open subvariety of some irreducible nonsingular projective curve.

REMARKS. The new content of the theorem is the existence of the nonsingular projective curve. The uniqueness is immediate from Corollary 10.55. The statement about nonsingular quasiprojective curves is a formality: Such a curve C_0 is birational to the nonsingular projective curve C produced by the theorem and also to the projective closure $\overline{C_0}$ of C_0. The birational maps from C_0 into C and from C into $\overline{C_0}$ yield morphisms from C_0 into C and from C into $\overline{C_0}$ by Corollary 10.54; sorting out these morphisms shows that C_0 is isomorphic to an open subvariety of C.

The idea for proving the existence of the projective curve in the theorem is to start with any function field $\mathbb{K}$ in one variable over $\Bbbk$, take any discrete valuation v of $\mathbb{K}$ defined over $\Bbbk$ (these exist as a consequence of Section VI.2), and use Corollary 10.59 to obtain some irreducible nonsingular affine curve having $\mathbb{K}$ as function field and having its local ring at some point equal to the valuation ring of v. Corollary 10.60 shows that except for finitely many discrete valuations, we have associated a nonsingular point on some irreducible affine curve in the birational equivalence class to each discrete valuation of $\mathbb{K}$ defined over $\Bbbk$. Applying Corollary 10.59 to each of these exceptional discrete valuations, we end up with a finite set of irreducible nonsingular affine curves such that each discrete valuation

of $\mathbb{K}$ over $\Bbbk$ corresponds to some point of at least one of the curves. We shall glue together these irreducible nonsingular affine curves in a suitable fashion to obtain the desired irreducible nonsingular projective curve.

The proof makes use of the fact that the product of two projective varieties is a projective variety and that morphisms behave as one might expect. Let us postpone the details of establishing a rigorous theory of product varieties, going right to the proof of Theorem 10.63.

PROOF OF THEOREM 10.63. Let $\mathbb{K}$ be the given function field, and let $C_1, \ldots, C_m$ be the irreducible nonsingular affine curves described two paragraphs before this paragraph. In each case the function field of the curve is isomorphic to $\mathbb{K}$ by some fixed isomorphism, but we shall treat this fixed isomorphism as if it were the identity in order to avoid unnecessary complications in the notation. Let $\mathbb{V}_{\mathbb{K}}$ be the set of discrete valuations of $\mathbb{K}$ defined over $\Bbbk$. For $v \in \mathbb{V}_{\mathbb{K}}$, we write $R_v \subseteq \mathbb{K}$ for the valuation ring of v and $\mathfrak{p}_v$ for the valuation ideal of v.

For definiteness let C_j be an affine variety in $\mathbb{A}^{k_j}$, and let $\overline{C}_1, \ldots, \overline{C}_n$ be the respective projective closures of $C_1, \ldots, C_m$ in $\mathbb{P}^{k_j}$. For any point P in $\overline{C}_j$, let M_P be the maximal ideal of the local ring $\mathcal{O}_P(\overline{C}_j)$.

Theorem 10.53 gives us for each j a well-defined function $\gamma_j : \mathbb{V}_{\mathbb{K}} \to \overline{C}_j$, and Corollary 10.58 says that γ_j is onto $\overline{C}_j$. The defining property of $\gamma_j(v)$ is that $M_{\gamma_j(v)} \subseteq \mathfrak{p}_v$, and it follows that $\mathcal{O}_{\gamma_j(v)}(\overline{C}_j) \subseteq R_v$. Corollary 10.51 shows that the inverse image under γ_j of any point in C_j is a singleton set, and Corollary 10.60 shows that the inverse image of any point of the complementary set $\overline{C}_j - C_j$ is a finite set. Let F be the finite subset $F = \bigcup_{j=1}^m \gamma_j^{-1}(\overline{C}_j - C_j)$ of $\mathbb{V}_{\mathbb{K}}$. For $v \notin F$, $\gamma_j(v)$ is a nonsingular point of C_j, and Corollary 10.51 shows that $\mathcal{O}_{\gamma_j(v)}(C_j) = R_v$. Hence also $M_{\gamma_j(v)} = \mathfrak{p}_v$. The construction of the curves $C_1, \ldots, C_m$ was arranged in such a way that

$$\text{each } v \in \mathbb{V}_{\mathbb{K}} \text{ has } \gamma_j(v) \text{ in } C_j \text{ for some } j. \tag{$*$}$$

Let U_j be the open set of C_j given by $U_j = \gamma_j(\mathbb{V}_{\mathbb{K}} - F)$. The curves $\overline{C}_j$ are birationally equivalent because they all have $\mathbb{K}$ as function field, and Corollary 10.54 shows that the largest domain on which the birational map from $\overline{C}_j$ to $\overline{C}_1$ is a morphism includes all the nonsingular points of $\overline{C}_j$. In particular, it contains $U_j = \gamma_j(\mathbb{V}_{\mathbb{K}} - F)$. If φ_j is the morphism from U_j into $\overline{C}_1$, then Proposition 10.42 shows that φ_j induces a homomorphism $\varphi_{j,P}^* : \mathcal{O}_{\varphi_j(P)}(\overline{C}_1) \to \mathcal{O}_P(C_j)$ for $P \in U_j$. By assumption, the isomorphism $\widetilde{\varphi}_j : \Bbbk(C_1) \to \Bbbk(C_j)$ is normalized to be the identity. Since $\widetilde{\varphi}_j$ is the field mapping corresponding to the birational map φ_j, $\widetilde{\varphi}_j$ is an extension of $\varphi_{j,P}^*$. Thus $\varphi_{j,P}^*$ is the identity under our identifications: $\mathcal{O}_{\varphi_j(P)}(\overline{C}_1) = \mathcal{O}_P(C_j)$ for $P \in U_j$. Let $P = \gamma_j(v)$ with v in $\mathbb{V}_{\mathbb{K}} - F$, and let $\varphi_j(P) = \gamma_1(v')$ with v' in $\mathbb{V}_{\mathbb{K}}$. Then $R_v = \mathcal{O}_{\gamma_j(v)}(C_j) = \mathcal{O}_{\varphi_j(P)}(\overline{C}_1) \subseteq R_{v'}$, and

it follows that $v' = v$. In particular, v' is in $\mathbb{V}_{\mathbb{K}} - F$, and $\gamma_1(v) = \varphi_j(\gamma_j(v))$. Hence

$$\varphi_j \circ \gamma_j : \mathbb{V}_{\mathbb{K}} - F \to U_1 \qquad \text{is independent of } j,$$
$$\text{and} \qquad \varphi_j : U_j \to U_1 \qquad \text{is an isomorphism.}$$

The product $W = \overline{C}_1 \times \cdots \times \overline{C}_m$ is an m-dimensional closed subvariety of $\mathbb{P}^{k_1} \times \cdots \times \mathbb{P}^{k_m}$, which in turn is a projective variety in $\mathbb{P}^N$ for a suitably large N. For $1 \le j \le m$, let $\pi_j : W \to \overline{C}_j$ be the j^{th} projection map; this is a morphism. The set $U_1 \times \cdots \times U_m$ is an open subvariety of W, and the "diagonal"

$$\Delta = \left\{ \delta(P) = \left(P, \varphi_2^{-1}(P), \ldots, \varphi_m^{-1}(P)\right) \;\middle|\; P \in U_1 \right\}$$

of $U_1 \times \cdots \times U_m$ is an irreducible curve isomorphic to U_1. The closure $C = \overline{\Delta}$ is an irreducible projective curve. It is a closed subvariety of W, and it has Δ as an open subvariety. The curve Δ may be identified with U_1 via the projection π_1, and we may therefore identify the function field of Δ, which is the same as the function field of C, with $\mathbb{K}$.

We shall show that C is nonsingular. For each j, the restriction $\pi_j : C \to \overline{C}_j$ is a morphism, and the image contains all points $\pi_j(\delta(P)) = \varphi_j^{-1}(P)$ with $P \in U_1$. Hence it contains U_j, which is an open subset of $\overline{C}_j$. In other words, $\pi_j : C \to \overline{C}_j$ is a dominant morphism. For $P \in U_1$, we have $\pi_j(\delta(P)) = \varphi_j^{-1}(P)$. If $Q = \delta(P)$, this says that $\pi_j(Q) = \varphi_j^{-1}\delta^{-1}(Q)$, from which it follows that $\delta \circ \varphi_j$ is a two-sided inverse of π_j on Δ. Consequently the dominant morphism $\pi_j : C \to \overline{C}_j$ is a birational map. Let (V_j, ψ_j) be a pair in the class of the rational map π_j^{-1}; we may assume that V_j is the largest domain in $\overline{C}_j$ on which π_j^{-1} is a morphism.

Let P be any point of C, and let M_P be the maximal ideal of $\mathcal{O}_P(C)$. Corollary 10.58 shows that there is a member v of $\mathbb{V}_{\mathbb{K}}$ such that $M_P \subseteq \mathfrak{p}_v$. Choose $j = j(P)$ with $1 \le j \le m$ such that $\gamma_j(v)$ is in C_j. Since every point of C_j is a nonsingular point by construction, Corollary 10.54 shows that every point of C_j lies in the domain V_j on which ψ_j is defined as a morphism inverting π_j. Consequently the open subvariety $\pi_j^{-1}(C_j)$ of C is isomorphic to the nonsingular irreducible affine curve C_j, and the point P of C has an open neighborhood of nonsingular points. Since P is arbitrary, C is nonsingular. □

The remainder of this section develops a small theory of products of varieties in projective spaces. Most of the proofs are left to the problems at the end of the chapter. It is enough to handle the product of two varieties because general finite products of varieties can then be treated by induction.

We begin with the product of two projective spaces. Let $m \ge 1$ and $n \ge 1$ be integers, and put $N = (m+1)(n+1) - 1 = mn + m + n$. We shall exhibit

$\mathbb{P}^m \times \mathbb{P}^n$ as a projective variety in $\mathbb{P}^N$. To do so, we coordinatize $\mathbb{P}^m$, $\mathbb{P}^n$, and $\mathbb{P}^N$ by using x_i, y_j, and w_{ij} for $0 \le i \le m$ and $0 \le j \le n$. Then

$$\mathbb{P}^m = \big\{[x_0, \ldots, x_m]\big\}, \qquad \mathbb{P}^n = \big\{[y_0, \ldots, y_n]\big\},$$

and

$$\mathbb{P}^N = \big\{[w_{00}, w_{01}, \ldots, w_{m,n-1}, w_{mn}]\big\}.$$

The **Segre embedding** is the function

$$\sigma\big([x_0, \ldots, x_m], [y_0, \ldots, y_n]\big) = [x_0y_0, x_0y_1, \ldots, x_my_{n-1}, x_my_n],$$

i.e., $w_{ij} = x_iy_j$. Define $\mathfrak{a} \subseteq \Bbbk[W_{00}, \ldots, W_{mn}]$ to be the homogeneous ideal generated by all $W_{ij}W_{kl} - W_{il}W_{kj}$. Problems 17–19 at the end of the chapter show that σ is well defined and one-one, that the image of σ is $V(\mathfrak{a})$, and that $V(\mathfrak{a})$ is irreducible. Thus the Segre embedding exhibits $\mathbb{P}^m \times \mathbb{P}^n$ as a projective variety in $\mathbb{P}^N$. This variety is known as a **Segre variety**.[18]

Let $U \subseteq \mathbb{P}^m$ and $V \subseteq \mathbb{P}^n$ be projective algebraic sets. Then the Segre embedding σ carries $U \times V$ to a subset of $\mathbb{P}^N$, and we wish to see that $\sigma(U \times V)$ is a projective algebraic set in $\mathbb{P}^N$. Let us use the abbreviation $X = (X_0, \ldots, X_m)$. If $\alpha = (\alpha_0, \ldots, \alpha_m)$ is an $(m+1)$-tuple of nonnegative integers, we define $|\alpha| = \alpha_0 + \cdots + \alpha_m$ and $X^\alpha = X_0^{\alpha_0} \cdots X_m^{\alpha_m}$. We define Y, β, $|\beta|$, and Y^β similarly. Any monomial $X^\alpha Y^\beta$ with $|\alpha| = d$ and $|\beta| = e$ is said to be **bihomogeneous** of **bidegree** (d, e). A **bihomogeneous polynomial** of bidegree (d, e) is any linear combination of bihomogeneous monomials of bidegree (d, e).

The first observation is that any projective algebraic set S in $\mathbb{P}^m$ can be described as the locus of common zeros of a vector space of homogeneous polynomials in X of a fixed degree. In fact, we know that S is given by the locus of common zeros of a finite set of homogeneous polynomials $F_1(X), \ldots, F_r(X)$ of various degrees $d_1, \ldots, d_r$. Let us say that $d = \max_j d_j$. The point is that S is given by the locus of common zeros of a finite set of homogeneous polynomials all of degree d. The reason is that the locus of common zeros of $F_j(X)$ is the same as the locus of common zeros of $X_0^{d-d_j}F_j(X), \ldots, X_m^{d-d_j}F_j(X)$. The assertion about describing S follows.

Now let $U \subseteq \mathbb{P}^m$ be the locus of common zeros of homogeneous polynomials $F_1(X), \ldots, F_r(X)$ all of degree d, and let $V \subseteq \mathbb{P}^n$ be the locus of common zeros of homogeneous polynomials $G_1(Y), \ldots, G_r(Y)$ all of degree e. Then $U \times V$ is the locus of common zeros of the bihomogeneous polynomials $F_a(X)G_b(Y)$, all of bidegree (d, e). These cannot immediately be expressed in terms of the polynomials W_{ij} of the Segre embedding. However, if we use the same trick again, we can substitute the W_{ij}'s. Specifically suppose that $d \le e$. Replace

[18] If we form the $(m+1)$-by-$(n+1)$ matrix whose $(i, j)^{\text{th}}$ entry is W_{ij}, then an equivalent description of the Segre variety is as the locus of common zeros of all 2-by-2 minors of this matrix.

$F_1(X), \dots, F_r(X)$ by a family of $r(m+1)$ polynomials $F'_1(X), \dots, F'_{r(m+1)}(X)$ homogeneous of degree e. Then the polynomials $F'_a(X)G_b(Y)$ are bihomogeneous of bidegree (e, e). When such a polynomial is expanded as a linear combination of monomials, each monomial has e factors from among $X_0, \dots, X_m$ and e factors from among $Y_0, \dots, Y_n$. We can pair the factors in whatever fashion we want and replace X_iY_j by W_{ij}. In this way our system of bihomogeneous polynomials can be rewritten as a system of polynomials $H_{ab}(W)$, together with the convention that $W_{ij} = X_iY_j$. Then $\sigma(U \times V)$ is the locus of common zeros in $\mathbb{P}^N$ of the polynomials $H_{ab}(W)$ and the defining polynomials of the Segre variety.

Conversely if we have a projective algebraic set in $\mathbb{P}^N$, then its intersection with the Segre variety can be described as the locus of common zeros in $\mathbb{P}^m \times \mathbb{P}^n$ of a family of bihomogeneous polynomials in (X, Y). We have only to take the defining homogeneous polynomials $H(W)$ and substitute the definition $W_{ij} = X_iY_j$ for W_{ij}. If $H(W)$ is homogeneous of degree e, then the result of the substitution is a polynomial bihomogeneous of bidegree (e, e).

Problems 20–21 at the end of the chapter show that if U and V are irreducible closed sets in $\mathbb{P}^m$ and $\mathbb{P}^n$, respectively, then $\sigma(U \times V)$ is irreducible in $\mathbb{P}^N$. Thus we can meaningfully speak of projective varieties in $\mathbb{P}^m \times \mathbb{P}^n$. The same pair of problems addresses what happens for quasiprojective varieties, showing that σ of any relatively open subset of a projective variety in $\mathbb{P}^m \times \mathbb{P}^n$ is a quasiprojective variety in $\mathbb{P}^N$.

Now that the notion of variety is meaningful in $\mathbb{P}^m \times \mathbb{P}^n$, with an interpretation in $\mathbb{P}^N$, we can similarly translate definitions and facts about morphisms to make them apply in $\mathbb{P}^m \times \mathbb{P}^n$. In particular, the projection of a variety to either factor $\mathbb{P}^m$ or $\mathbb{P}^n$ is a morphism on the variety. If U is a quasiprojective variety and if $\varphi_1 : U \to \mathbb{P}^m$ and $\varphi_2 : U \to \mathbb{P}^n$ are isomorphisms of U onto quasiprojective varieties in $\mathbb{P}^m$ and $\mathbb{P}^n$, then the diagonal $\Delta = \{(\varphi_1(u), \varphi_2(u)) \mid u \in U\}$ is a quasiprojective variety in $\mathbb{P}^m \times \mathbb{P}^n$, and the pair (φ_1, φ_2) is an isomorphism of varieties. These matters are discussed in Problem 22 at the end of the chapter.

9. Affine Algebraic Sets for Monomial Ideals

Sections 9–12 in part address aspects of the question of how much one can make explicit computations with affine and projective varieties. As a general rule, the tool for such computations is the theory of Gröbner bases, which were introduced in Sections VIII.7–VIII.10. The topic is an active area of continuing research.[19] One can think of immediate problems—such as finding the dimension of an algebraic set, determining the radical of an ideal when the ideal is given,

[19]The book edited by Buchberger and Winkler contains a number of expository "tutorials" that give an idea of the breadth of applications of the theory. The book contains also a certain number of research papers.

and deciding whether an ideal is prime. We shall concentrate on just one such problem, that of finding the dimension.[20]

Part of the abstract theory in this case dates back to Hilbert, but in combination with the theory of Gröbner bases it becomes easier to establish and relatively easy to implement computationally.[21] We shall prove in Section 12 as a consequence of this investigation the deep theorem that a system of simultaneous homogeneous polynomial equations having more equations than variables always has a nonzero solution.[22]

Hilbert associated a polynomial in one variable, now known as the "Hilbert polynomial," to each ideal of polynomials over an algebraically closed field. This polynomial encodes certain algebraic information about the ideal, and some features of this polynomial depend only on the geometry of the zero locus. In particular, the degree of the polynomial turns out to equal the geometric dimension of the zero locus, and that will be what interests us.

The theory behind Gröbner bases enables one to reduce the theory of the Hilbert polynomial to the case of a monomial ideal, for which it is relatively easy to understand.[23] We begin with that case in this section.

Let $\Bbbk$ be an algebraically closed field, consider affine space $\mathbb{A}^n$, and let $\mathfrak{a}$ be an ideal in $A = \Bbbk[X_1, \ldots, X_n]$. In this section we shall be interested in the case that $\mathfrak{a}$ is generated by monomials, in which case it is called a **monomial ideal**. The structure of monomial ideals is captured by Lemma 8.17, which says about such an ideal $\mathfrak{a}$ that

- for any polynomial $f \neq 0$ in $\mathfrak{a}$, each monomial term contributing to f lies in $\mathfrak{a}$,
- $\mathfrak{a}$ has a finite set of monomials as generators,
- if $\{M_1, \ldots, M_k\}$ is a set of monomials that generate $\mathfrak{a}$ and if M is any monomial in $\mathfrak{a}$, then some M_j divides M.

Let $e_1, \ldots, e_n$ be the standard basis of $\mathbb{A}^n$, and let $\langle e_{j_1}, \ldots, e_{j_k}\rangle$ be the linear span of $e_{j_1}, \ldots, e_{j_k}$. The vector space $\langle e_{j_1}, \ldots, e_{j_k}\rangle$ is called a **coordinate subspace** of $\mathbb{A}^n$. The ideal $\mathfrak{p}_k = (X_1, \ldots, X_k)$ in A is prime, and its variety is $V(\mathfrak{p}_k) = \langle e_{k+1}, \ldots, e_n\rangle$. Since $\mathfrak{p}_0 \subseteq \mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$ is a strictly increasing sequence of prime ideals in A and since A has Krull dimension n,

[20] Solutions to the other two problems are known as well. References may be found in Cox–Little–O'Shea. For determining the radical, see p. 177. For deciding whether an ideal is prime, see p. 207.

[21] The exposition in Sections 9–12 is based in part on Chapter 9 of the book by Cox–Little–O'Shea and in part on Chapter I of Hartshorne's book.

[22] For one equation with two variables, this amounts to the Fundamental Theorem of Algebra. For two equations with three variables, it amounts to the existence part of Bezout's Theorem as formulated in Theorem 8.5.

[23] Similarly the computations associated with Gröbner bases make it possible to reduce the computation of the Hilbert polynomial of a general ideal to the computation of the Hilbert polynomial of a monomial ideal.

no strictly increasing sequence of prime ideals containing $\mathfrak{p}_k$ can be longer than $\mathfrak{p}_k \subseteq \mathfrak{p}_{k+1} \subseteq \cdots \subseteq \mathfrak{p}_n$. It follows that the images of these ideals in $A/\mathfrak{p}$ give a strictly increasing sequence of prime ideals of maximal length and that $A/\mathfrak{p}$ has Krull dimension $n-k$. By Theorem 10.7 the geometric dimension of $V(\mathfrak{p}_k) = \langle e_{k+1}, \ldots, e_n \rangle$ is $n-k$. In other words, the geometric dimension of the vector subspace $\langle e_{k+1}, \ldots, e_n \rangle$ is the same as the vector-space dimension. Relabeling indices in this computation, we see that the geometric dimension of $\langle e_{j_1}, \ldots, e_{j_k} \rangle$ is k if the indices $j_1, \ldots, j_k$ are distinct.

Let us compute the geometric dimension of the zero locus of a general proper monomial ideal $(M_1, \ldots, M_k)$. If $\alpha = (\alpha_1, \ldots, \alpha_n)$ is a tuple of integers ≥ 0, we write X^α for $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ and $|\alpha|$ for $\alpha_1 + \cdots + \alpha_n$. Let $H_j = V(X_j)$ be the **coordinate hyperplane** of points in $\mathbb{A}^n$ with j^{th} coordinate 0. This is the linear span of all e_i for $i \neq j$, and it has geometric dimension $n-1$. If a monomial X^α is given, then Proposition 10.1 shows that

$$V(X^\alpha) = \bigcup_{\alpha_j > 0} V(X_j) = \bigcup_{\alpha_j > 0} H_j$$

and then that

$$V(X^\alpha, X^\beta) = \Big(\bigcup_{\alpha_i > 0} H_i \Big) \cap \Big(\bigcup_{\beta_j > 0} H_j \Big) = \bigcup_{\alpha_i > 0,\ \beta_j > 0} (H_i \cap H_j).$$

Similarly $V(M_1, \ldots, M_k)$ is a finite union of k-fold intersections of coordinate hyperplanes. By Theorem 10.7 the geometric dimension of $V(M_1, \ldots, M_k)$ is the maximum dimension of the subspaces $H_i \cap H_j \cap \cdots$ appearing in the appropriate union for $M_1, \ldots, M_k$. To get the maximum dimension, we want as few distinct indices to appear in an intersection $H_i \cap H_j \cap \cdots$. If the smallest possible number of distinct indices is m, then we see that $V(M_1, \ldots, M_k)$ has geometric dimension $n-m$.

The insight is that to study $V(\mathfrak{a})$, one studies $A/\mathfrak{a}$, and that to study the latter, one considers what happens as a function of s to the part of $A/\mathfrak{a}$ that corresponds to degree at most s. In the case of a monomial ideal, this means that one is to study the monomials outside the ideal in question, particularly how the number of these monomials grows with s. Let $\mathcal{M}$ be the set of all monomials in $\Bbbk[X_1, \ldots, X_n]$. For our monomial ideal $\mathfrak{a}$, let $\mathcal{C}(\mathfrak{a})$ be the complementary subset to $\mathfrak{a}$ in $\mathcal{M}$ given by

$$\mathcal{C}(\mathfrak{a}) = \big\{ X^\alpha \mid X^\alpha \notin \mathfrak{a} \big\}.$$

Proposition 10.64. If $\mathfrak{a}$ is a proper monomial ideal in $\Bbbk[X_1, \ldots, X_n]$, then

(a) the vector subspace $V\big(\{X_i \mid i \notin \{j_1, \ldots, j_k\}\}\big)$ is contained in $V(\mathfrak{a})$ if and only if $\big\{X^\alpha \in \mathcal{M} \mid \alpha \in \langle e_{j_1}, \ldots, e_{j_k} \rangle\big\}$ is contained in $\mathcal{C}(\mathfrak{a})$,

(b) the geometric dimension of $V(\mathfrak{a})$ equals the largest vector-space dimension of a coordinate subspace that lies in $\mathcal{C}(\mathfrak{a})$.

REMARK. The hypothesis "proper" is needed for (b), not for (a).

PROOF. For (a), first suppose that $V\big(\{X_i \mid i \notin \{j_1, \dots, j_k\}\}\big)$ is contained in $V(\mathfrak{a})$, and suppose that α is in $\langle e_{j_1}, \dots, e_{j_k}\rangle$. Let $P = (x_1, \dots, x_n)$ be the point with

$$x_i = \begin{cases} 1 & \text{for } i \in \{j_1, \dots, j_k\}, \\ 0 & \text{for } i \notin \{j_1, \dots, j_k\}. \end{cases} \tag{$*$}$$

Then P is on the zero locus of each X_i for $i \notin \{j_1, \dots, j_k\}$, and hence P is in $V(\mathfrak{a})$. On the other hand, the value of the monomial X^α at P is 1. Since the value of every member of $\mathfrak{a}$ at P is 0, X^α cannot be in $\mathfrak{a}$. Thus X^α is in $\mathcal{C}(\mathfrak{a})$.

Next suppose that $E = V\big(\{X_i \mid i \notin \{j_1, \dots, j_k\}\}\big)$ is not contained in $V(\mathfrak{a})$. Say that $P = (x_1, \dots, x_n)$ is in E but not $V(\mathfrak{a})$. The condition for P to be in E is that $x_i = 0$ for all $i \notin \{j_1, \dots, j_k\}$. Since P is not in $V(\mathfrak{a})$, some member of $\mathfrak{a}$ is nonzero at P. The ideal is generated by monomials, and thus some monomial X^{α_0} in $\mathfrak{a}$ is nonzero at P. Let $\alpha_0 = (\alpha_1, \dots, \alpha_n)$. The (nonzero) value of α_0 on P is $\prod_{i \text{ with } \alpha_i > 0} x_i^{\alpha_i}$. Now $x_i = 0$ for all $i \notin \{j_1, \dots, j_k\}$, and consequently no i outside $\{j_1, \dots, j_k\}$ can have $\alpha_i > 0$. Thus α_0 is in $\langle e_{j_1}, \dots, e_{j_k}\rangle$, and α_0 exhibits $\big\{X^\alpha \in \mathcal{M} \mid \alpha \in \langle e_{j_1}, \dots, e_{j_k}\rangle\big\}$ as failing to be contained in $\mathcal{C}(\mathfrak{a})$.

For (b), we saw before the proof that $V(\mathfrak{a})$ is the union of finitely many vector subspaces and that each vector subspace is an affine variety whose geometric dimension equals its vector-space dimension. By Theorem 10.7 the geometric dimension of $V(\mathfrak{a})$, $\mathfrak{a}$ being proper, is the maximum of the dimensions of these subspaces. Taking (a) into account, we conclude that (b) holds. □

We seek a formula for the number of monomials in $\mathcal{C}(\mathfrak{a})$ of total degree $\le s$ when s is large and positive. We begin with a lemma. For a monomial ideal $\mathfrak{a}$, the function carrying each integer $s \ge 0$ to the number of X^α in $\mathcal{C}(\mathfrak{a})$ with $|\alpha| \le s$ is called the **affine Hilbert function** of $\mathfrak{a}$ and is denoted by $\mathcal{H}_a(s, \mathfrak{a})$. For $\mathfrak{a} = \Bbbk[X_1, \dots, X_n]$, the affine Hilbert function is identically 0, and we shall usually not be interested in this case.

EXAMPLE. For $n = 1$ with one indeterminate X, the proper ideals of $\Bbbk[X]$ are 0 and (X^k) with $k > 0$. The monomials X^α with $|\alpha| \le s$ are $1, X, X^2, \dots, X^s$. By inspection, none of these is in $\mathfrak{a}$ if $\mathfrak{a} = 0$, and thus $\mathcal{H}_a(s, 0) = s + 1$. In the case of (X^k) with $k > 0$, the monomials X^α in $\mathcal{C}((X)^k)$ are $1, X, \dots, X^{k-1}$, and thus $\mathcal{H}_a(s, (X^k))$ is $s + 1$ for $s \le k - 1$ and is k for $s \ge k - 1$.

Theorem 10.65. If $\mathfrak{a}$ is a proper monomial ideal in $\Bbbk[X_1, \dots, X_n]$, then the complementary set $\mathcal{C}(\mathfrak{a})$ of monomials is a disjoint union

$$\mathcal{C}(\mathfrak{a}) = C_0 \cup \cdots \cup C_n,$$

where C_k is a finite union of subsets of the form

$$E = \Big\{X^\alpha \in \mathcal{M} \mid \alpha \in \langle e_{j_1}, \dots, e_{j_k}\rangle + \sum_{i \notin \{j_1, \dots, j_k\}} a_i e_i\Big\}.$$

Here it is assumed that $\langle e_{j_1}, \dots, e_{j_k}\rangle$ is a k-dimensional coordinate subspace and the coefficients a_i are particular integers ≥ 0.

REMARKS. The subsets of $\mathcal{M}$ of which the above set E is an example will be called **standard subsets** of $\mathcal{M}$ with k parameters. The member $\sum_{i\notin\{j_1,\dots,j_k\}} a_i e_i$ of $\mathcal{M}$ is called the **associated translation** of E, and $\langle e_{j_1}, \dots, e_{j_k}\rangle$ is called the **associated vector subspace** of E. Standard subsets of $\mathcal{M}$ with 0 parameters are singleton sets $\{X^\alpha\}$. An example of a standard subset of $\mathcal{M}$ with 1 parameter when $n = 2$ is $\{X_1^{\alpha_1}X_2^{\alpha_2} \mid \alpha_1 \geq 0,\ \alpha_2 = 2\} = \{X^\alpha \mid \alpha \in \langle e_1\rangle + 2e_2\}$. It is apparent that the one and only circumstance in which C_n is nonempty is that $\mathcal{C}(\mathfrak{a}) = \mathcal{M}$, in which case $\mathfrak{a} = 0$.

PROOF. We proceed by induction on n, and we may assume that $\mathfrak{a} \neq 0$. The example above shows for $n = 1$ that $\mathcal{C}(\mathfrak{a})$ is a finite set if $\mathfrak{a}$ is a nonzero proper ideal. Thus $\mathcal{C}(\mathfrak{a}) = C_0$ in this case, and the base case of the induction is settled.

Assume inductively that the theorem has been proved for $n-1$ indeterminates, and let $\mathfrak{a}$ be a nonzero ideal in $\Bbbk[X_1, \dots, X_n]$. Let $\mathcal{M}_{n-1}$ and $\mathcal{M}_n$ denote the sets of monomials in $X_1, \dots, X_{n-1}$ and $X_1, \dots, X_n$, respectively. For $j \geq 0$, let $\mathfrak{a}_j$ be the ideal in $\Bbbk[X_1, \dots, X_{n-1}]$ of all polynomials $f(X_1, \dots, X_{n-1})$ such that $X_n^j f(X_1, \dots, X_{n-1})$ is in $\mathfrak{a}$. The ideals $\mathfrak{a}_j$ are monomial ideals because $\mathfrak{a}$ is a monomial ideal, and $\mathfrak{a}_j \subseteq \mathfrak{a}_{j+1}$ for all j. Since $\Bbbk[X_1, \dots, X_{n-1}]$ is Noetherian, there is some index l such that $\mathfrak{a}_j = \mathfrak{a}_l$ for all $j \geq l$. We apply the inductive hypothesis to $\mathfrak{a}_0, \mathfrak{a}_1, \dots, \mathfrak{a}_l$, writing

$$\mathcal{C}(\mathfrak{a}_j) = C_{0,j} \cup \cdots \cup C_{n-1,j} \qquad \text{for } 0 \leq j \leq l.$$

Here each $C_{k,j}$ is a finite union of standard subsets with k parameters in the $n-1$ indeterminates $X_1, \dots, X_{n-1}$.

Let $C_{k,j}X_n^j$ be the set of all products of members of $C_{k,j}$ with X_n^j. We shall show that

$$\mathcal{C}(\mathfrak{a}) = C_0 \cup \cdots \cup C_n, \tag{$*$}$$

where $C_0, \dots, C_n$ are defined by

$$C_{k+1} = \bigcup_{j=0}^{\infty} C_{k,l}X_n^j \ \cup \bigcup_{j=0}^{l-1} C_{k+1,j}X_n^j \qquad \text{for } 0 \leq k \leq n-1$$

and
$$C_0 = \mathcal{C}(\mathfrak{a}) - \bigcup_{k=1}^{n} C_k.$$

But first let us see that each C_{k+1} for $0 \leq k \leq n-1$ is a finite union of standard subsets of $\mathcal{M}_n$ with $k+1$ parameters. Each $C_{k+1,j}$ is a finite union of standard subsets of $\mathcal{M}_{n-1}$ with some associated translation γ such that $\gamma_n = 0$ and with an associated vector subspace $\langle e_{j_1}, \dots, e_{j_{k+1}}\rangle$ such that $j_1 < \cdots < j_{k+1} < n$. Then each $C_{k+1,j}X_n^j$ is a finite union of standard subsets of $\mathcal{M}$ of the form X^α

with associated translation $\gamma + je_n$ and with the same associated vector space $\langle e_{j_1}, \ldots, e_{j_{k+1}} \rangle$. Similarly the set $\bigcup_{j=0}^{\infty} C_{k,l} X_n^j$ is a finite union of standard subsets of $\mathcal{M}$ with associated translation $\gamma + 0e_n$ and with associated vector space of the form $\langle e_{j_1}, \ldots, e_{j_k}, e_n \rangle$. Thus C_{k+1} is a finite union of standard subsets of $\mathcal{M}_n$ with $k+1$ parameters.

Let us verify $(*)$. The most general monomial in $\Bbbk[X_1, \ldots, X_n]$ is $X^\beta X_n^j$ with X^β in $\Bbbk[X_1, \ldots, X_{n-1}]$, and this monomial is in $\mathfrak{a}$ if and only if X^β is in $\mathfrak{a}_j$. Hence $X^\beta X_n^j$ is in $\mathcal{C}(\mathfrak{a})$ if and only if X^β is in $\mathcal{C}(\mathfrak{a}_j)$. Since $\mathfrak{a}_j = \mathfrak{a}_l$ for $j \geq l$, $\mathcal{C}(\mathfrak{a}_j) = \mathcal{C}(\mathfrak{a}_l)$ for $j \geq l$. Thus

$$\mathcal{C}(\mathfrak{a}) = \Big(\bigcup_{j=l}^{\infty} \mathcal{C}(\mathfrak{a}_l) X_n^j \Big) \cup \Big(\bigcup_{j=0}^{l-1} \mathcal{C}(\mathfrak{a}_j) X_n^j \Big). \tag{$**$}$$

If $j \leq l$, then $X^\beta X_n^l \in \mathcal{C}(\mathfrak{a})$ implies $X^\beta X_n^j \in \mathcal{C}(\mathfrak{a})$, since $X_n^{l-j} \mathfrak{a} \subseteq \mathfrak{a}$. Therefore $\mathcal{C}(\mathfrak{a}_j) \supseteq \mathcal{C}(\mathfrak{a}_l)$ for all $j \leq l$, and we see that $j \leq l$ implies that $\mathcal{C}(\mathfrak{a}_j) = \mathcal{C}(\mathfrak{a}_j) \cup \mathcal{C}(\mathfrak{a}_l)$. Substituting into $(**)$ and rearranging terms gives

$$\mathcal{C}(\mathfrak{a}) = \Big(\bigcup_{j=0}^{\infty} \mathcal{C}(\mathfrak{a}_l) X_n^j \Big) \cup \Big(\bigcup_{j=0}^{l-1} \mathcal{C}(\mathfrak{a}_j) X_n^j \Big). \tag{$\dagger$}$$

For $j \leq l$, X^β is in $\mathcal{C}(\mathfrak{a}_j)$ if and only if X^β is in one of $C_{0,j}, \ldots, C_{n-1,j}$. Thus we can rewrite $(\dagger)$ as

$$\begin{aligned} \mathcal{C}(\mathfrak{a}) &= \Big(\bigcup_{j=l}^{\infty} \bigcup_{k=0}^{n-1} C_{k,l} X_n^j \Big) \cup \Big(\bigcup_{j=0}^{l-1} \bigcup_{k=0}^{n-1} C_{k,j} X_n^j \Big) \\ &= \Big(\bigcup_{j=l}^{\infty} \bigcup_{k=0}^{n-1} C_{k,l} X_n^j \Big) \cup \Big(\bigcup_{j=0}^{l-1} \bigcup_{k=0}^{n-2} C_{k+1,j} X_n^j \Big) \cup \Big(\bigcup_{j=0}^{l-1} C_{0,j} X_n^j \Big). \end{aligned}$$

The first term on the right side contributes to C_{k+1}, with e_n to be adjoined to the basis vectors of the associated vector subspace $\langle e_{j_1}, \ldots, e_{j_k} \rangle$. Equating the terms on the two sides that contribute to C_{k+1} therefore yields $(*)$. The set C_0 is the last term on the right side. This is finite because each $C_{0,j}$ is finite, and therefore C_0 has the correct form. □

Lemma 10.66. Let E be a standard subset of $\mathcal{M}$ with k parameters, and let γ be its associated translation. Then the number of monomials X^α with $|\gamma| \leq s$ such that α is in E is equal to the binomial coefficient

$$\binom{k + s - |\gamma|}{s - |\gamma|}$$

if $s > |\gamma|$. This expression is a polynomial function of s of degree k, and the coefficient of s^k is $1/k!$.

PROOF. Let $\langle e_{j_1}, \dots, e_{j_k}\rangle$ be the associated vector subspace for E. The associated translation γ is assumed to have $\gamma_i = 0$ for i in $\{j_1, \dots, j_k\}$. We are to count monomials $X^\alpha = X^\gamma X^\beta$ with β in $\langle e_{j_1}, \dots, e_{j_k}\rangle$ and with $|\gamma + \beta| \le s$. Since $|\gamma| + |\beta| = |\gamma + \beta| \le s$, the latter condition on β is that $|\beta| \le s - |\gamma|$, which by assumption is ≥ 0. The entries of β are allowed to be arbitrary nonzero integers in the k entries $j_1, \dots, j_k$, subject only to the limitation that the sum of the entries is to be $\le s - |\gamma|$. The number of such β's equals the number of homogeneous monomials in $k+1$ variables of total degree equal to $s - |\gamma|$. This number is recalled in a bulleted list in Section 3 and is $\binom{s-|\gamma|+k}{k} = \binom{s-|\gamma|+k}{s-|\gamma|}$. When expanded out, this binomial coefficient equals

$$\tfrac{1}{k!}\,(s + k - |\gamma|)(s + k - 1 - |\gamma|)\cdots(s + 1 - |\gamma|),$$

which is a polynomial function of s of degree k with leading coefficient $1/k!$. □

Lemma 10.67. Let E and F be standard subsets of $\mathcal{M}$ with k and l parameters, respectively. Then $E \cap F$ either is empty or is a standard subset of $\mathcal{M}$ with m parameters, where $m \le \min(k, l)$. Moreover, the only way that m can equal $\max(k, l)$ is for E to equal F.

PROOF. Denote the respective associated translations for E and F by γ_E and γ_F, and let S_E and S_F be the subsets of $\{1, \dots, n\}$ such that $\langle e_i \mid i \in S_E\rangle$ and $\langle e_i \mid i \in S_F\rangle$ are the associated vector spaces for E and F, respectively. Let T_E be the subset of indices

$$T_E = \big\{i \in \{1, \dots, n\} \mid (\gamma_E)_i > 0\big\},$$

and define T_F similarly. We are given that $|S_E| = k$ and $|S_F| = l$. Also, we are given that $S_E \cap T_E = \varnothing$ and $S_F \cap T_F = \varnothing$, i.e., that $T_E \subseteq S_E^c$ and $T_F \subseteq S_F^c$. If $E \cap F \ne \varnothing$, then there exist x and y with

$$\gamma_E + x = \gamma_F + y \qquad \text{such that } x_i = 0 \text{ for } i \notin S_E \text{ and } y_j = 0 \text{ for } j \notin S_F. \quad (*)$$

Then $x_i = y_i = 0$ for $i \in S_E^c \cap S_F^c$, and we see that a necessary condition to have $E \cap F \ne \varnothing$ is that $(\gamma_E)_i = (\gamma_F)_i$ for $i \in S_E^c \cap S_F^c$. In this case the x and y in $(*)$ must have $x_i = (\gamma_F)_i$ for $i \in S_E \cap S_F^c$ and $y_i = (\gamma_E)_i$ for $i \in S_E^c \cap S_F$.

Conversely if $(\gamma_E)_i = (\gamma_F)_i$ for $i \in S_E^c \cap S_F^c$, then we can define $x_i = (\gamma_F)_i$ for $i \in S_E \cap S_F^c$, $y_i = (\gamma_E)_i$ for $i \in S_E^c \cap S_F$, and $x_i = y_i$ to be arbitrary for $i \in S_E \cap S_F$, and we obtain solutions of $(*)$. It is evident that all solutions of $(*)$ are obtained this way. Consequently $E \cap F$ is the standard subset of $\mathcal{M}$ with $|S_E \cap S_F|$ parameters; with associated translation γ having γ_i equal to γ_E on S_E^c, equal to γ_F on S_F^c, and equal to 0 on $S_E \cap S_F$; and with associated vector space $\langle e_i \mid i \in S\rangle$, where $S = S_E \cap S_F$.

The inequality $\dim_{\Bbbk}(S_E \cap S_F) \le \min(\dim_{\Bbbk} S_E, \dim_{\Bbbk} S_F)$ is the inequality $m \le \min(k, l)$ of the lemma. If $m = \max(k, l)$, then we must have $S = S_E = S_F$ and an equality $(\gamma_E)_i = (\gamma_F)_i$ for $i \in S_E^c \cap S_F^c$, i.e., for $i \notin S$. The latter equality implies that $\gamma_E = \gamma_F$. Hence $E = F$. □

Theorem 10.68. If $\mathfrak{a}$ is a monomial ideal in $\Bbbk[X_1, \ldots, X_n]$ such that $V(\mathfrak{a})$ has geometric dimension d, then there exists a polynomial $H_a(s, \mathfrak{a})$ in one variable of degree d such that the affine Hilbert function $\mathcal{H}_a(s, \mathfrak{a})$ is equal to $H_a(s, \mathfrak{a})$ for all positive s sufficiently large. The leading coefficient of $H_a(s, \mathfrak{a})$ is positive.

REMARK. The polynomial $H_a(s, \mathfrak{a})$ is called the **affine Hilbert polynomial** of the monomial ideal $\mathfrak{a}$. It is of course uniquely determined.

PROOF. For s sufficiently large, we are to count the number of monomials X^α with $|\alpha| \le s$ lying in the complementary set $\mathcal{C}(\mathfrak{a})$ to $\mathfrak{a}$. Proposition 10.64b and Theorem 10.65 together show that $\mathcal{C}(\mathfrak{a}) = C_0 \cup \cdots \cup C_d$ disjointly, with C_k equal to a finite union of standard subsets of $\mathcal{M}$ with k parameters and with C_d nonempty. The sets C_k being disjoint, it is enough to show that the number of such monomials in C_k is a function equal for large s to a polynomial of degree k, provided C_k is nonempty.

According to Lemma 10.66, if E is a standard subset of $\mathcal{M}$ with k parameters, if $s > 0$ is sufficiently large, and if γ is the translation parameter, then the number of monomials X^α in E with $|\alpha| \le s$ is $\binom{k+s-|\gamma|}{s-|\gamma|}$ if $s > |\gamma|$, which is a polynomial of degree k with positive leading coefficient.

Because the sets E of this kind whose finite union is C_k may not be disjoint and because we seek an exact answer for the cardinality $|C_k|$ when s is large, we cannot simply add finitely many such expressions to obtain a value for $|C_k|$. We have to take into account the overlaps of the various sets E. Thus suppose that $C_k = E_1 \cup \cdots \cup E_r$ for standard subsets $E_1, \ldots, E_r$ of $\mathcal{M}$ with k parameters. Without loss of generality, we may assume that no two of the sets $E_1, \ldots, E_r$ are equal to one another. Let $E_1(s), \ldots, E_r(s)$ be the respective subsets of elements α with $|\alpha| \le s$. We use the inclusion–exclusion formula, namely

$$\Big|\bigcup_{i=1}^{r} E_i(s)\Big| = \sum_i |E_i(s)| - \sum_{i_1<i_2} |E_{i_1}(s)\cap E_{i_2}(s)| + \sum_{l=3}^{r} (-1)^{l+1} \sum_{i_1<\cdots<i_l} \Big|\bigcap_{j=1}^{l} E_{i_j}(s)\Big|;$$

this is a formula in Boolean algebra that is readily proved by induction on r starting from the formula $|E \cup F| = |E| + |F| - |E \cap F|$.

Lemma 10.66 shows that $\sum_i |E_i(s)|$ is a sum of functions equal for large $s > 0$ to polynomials of degree d with positive leading coefficient. The leading coefficients cannot cancel, and thus the sum is for large $s > 0$ equal to a polynomial of degree d with positive leading coefficient. Each of the remaining terms on the right side of the inclusion–exclusion formula, according to Lemma 10.67, is plus or minus the number of monomials α with $|\alpha| \le s$ in some standard subset E of $\mathcal{M}$ whose number of parameters is $< d$. Hence the sum of all those terms is a function equal for large s to a polynomial that is 0 or has degree $< d$. The theorem follows. □

Proposition 10.69. A polynomial $P(s)$ in one variable of degree d takes integer values for s sufficiently large and positive if and only if it is an integer linear combination of the polynomials $s \mapsto \binom{s}{j}$ for $0 \le j \le d$.

PROOF. The sufficiency is immediate because $\binom{s}{j}$ is an integer for each j and s. For necessity, suppose that $P(s)$ is integer-valued and has degree d. Since $s \mapsto \binom{s}{j}$ is integer-valued of degree j with leading coefficient $1/j!$, $P(s)$ is certainly a rational linear combination of the polynomials $s \mapsto \binom{s}{j}$. We prove by induction on d that the coefficients are integers. For $\deg P(s) = 0$, we have $\binom{s}{0} = 1$, and there is nothing to prove. Given an integer-valued $P(s)$ of degree d, write $P(s) = \sum_{j=0}^{d} a_j \binom{s}{j}$. Form

$$\Delta P(s) = P(s+1) - P(s) = \sum_{j=0}^{d} a_j \Big[\tbinom{s+1}{j} - \tbinom{s}{j} \Big] = \sum_{j=1}^{d} a_j \tbinom{s}{j-1} = \sum_{j=0}^{d-1} a_{j+1} \tbinom{s}{j},$$

the third equality holding by Pascal's triangle. Since $\Delta P(s)$ is integer-valued and has degree $d-1$, the inductive hypothesis shows that a_{j+1} is an integer for $0 \le j \le d-1$; i.e., a_j is an integer for $1 \le j \le d$. Therefore $Q(s) = \sum_{j=1}^{d} a_j \binom{s}{j}$ is integer-valued. Since $P(s) - Q(s) = a_0$ is integer-valued and constant, a_0 is an integer. □

Corollary 10.70. If $\mathfrak{a}$ is a monomial ideal in $\Bbbk[X_1, \dots, X_n]$ such that $V(\mathfrak{a})$ has geometric dimension d, then the affine Hilbert polynomial $H_a(s, \mathfrak{a})$ of $\mathfrak{a}$ is of the form $H_a(s, \mathfrak{a}) = \sum_{j=0}^{d} a_j \binom{s}{d-j}$ with integer coefficients a_j and with $a_0 > 0$.

PROOF. This follows by combining Theorem 10.68 and Proposition 10.69. □

10. Hilbert Polynomial in the Affine Case

We continue with an algebraically closed field $\Bbbk$ and with the polynomial ring $A = \Bbbk[X_1, \dots, X_n]$. Let $\mathfrak{a}$ be an ideal in A. For each integer $s \ge 0$, let $A_{\le s}$ be the vector subspace of A consisting of 0 and all elements of degree at most s, and put $\mathfrak{a}_{\le s} = \mathfrak{a} \cap A_{\le s}$. The inclusion of $A_{\le s}$ into A descends to a $\Bbbk$ linear mapping $A_{\le s}/\mathfrak{a}_{\le s} \to A/\mathfrak{a}$, and this is one-one because $A_{\le s} \cap \mathfrak{a} \subseteq \mathfrak{a}_{\le s}$. Thus we can regard $A_{\le s}/\mathfrak{a}_{\le s}$, as s varies, as a sequence of successively better approximations to $A/\mathfrak{a}$. We define the **affine Hilbert function** $\mathcal{H}_a(s, \mathfrak{a})$ of $\mathfrak{a}$ by

$$\mathcal{H}_a(s, \mathfrak{a}) = \dim_{\Bbbk} A_{\le s}/\mathfrak{a}_{\le s} \qquad \text{for } s \ge 0.$$

When $\mathfrak{a}$ is a monomial ideal, this function is the one that was investigated in the previous section. In fact, the monomials of degree $\le s$ form a vector-space

basis of $A_{\le s}$, and the monomials in $\mathfrak{a}$ of degree $\le s$ form a basis of $\mathfrak{a}_{\le s}$ because $\mathfrak{a}$ is spanned by monomials. If $\mathcal{C}(\mathfrak{a})$ denotes the set of monomials not in $\mathfrak{a}$, then the monomials of degree $\le s$ within $\mathcal{C}(\mathfrak{a})$ descend to a basis of $A_{\le s}/\mathfrak{a}_{\le s}$. The number of such monomials gives the value of the affine Hilbert function as defined in the previous section, and thus the new definition is consistent with the old one in the case of monomial ideals.

When $\mathfrak{a}$ is a proper monomial ideal, we found in Theorem 10.68 that $\mathcal{H}_a(s, \mathfrak{a})$ equals a polynomial function of s for s sufficiently large and that the degree of this polynomial function equals the geometric dimension of the zero locus $V(\mathfrak{a})$ in the affine space $\mathbb{A}^n$. Our goal in this section is to show that these conclusions remain valid for all proper ideals $\mathfrak{a}$. The polynomial function that results for such an $\mathfrak{a}$ will be called the affine Hilbert polynomial of $\mathfrak{a}$.

We shall make the connection between general ideals $\mathfrak{a}$ and monomial ideals by means of the theory of Sections VIII.7–VIII.10. We recall the notion of a monomial ordering as defined in Section VIII.7. A monomial ordering $\le$ is said to be a **graded monomial ordering** if $|\beta| < |\alpha|$ implies $X^\beta \le X^\alpha$. The graded lexicographic ordering and the graded reverse lexicographic ordering (Examples 2 and 3 in Section VIII.7) are examples of graded monomial orderings, but the lexicographic ordering in Example 1 in that section is *not* a graded monomial ordering.

Fix a graded monomial ordering. As in Section VIII.7, $\mathrm{LT}(f)$ denotes the leading monomial term of the polynomial f. By convention, $\mathrm{LT}(0) = 0$. For our ideal $\mathfrak{a}$, we let $\mathrm{LT}(\mathfrak{a})$ be the vector space of all linear combinations of polynomials $\mathrm{LT}(f)$ for $f \in \alpha$. This is an ideal in A, and it is a monomial ideal. The connection between the goal of this section and the results of the previous section rests on the following remarkable theorem.

Theorem 10.71 (Macaulay). Let a graded monomial ordering be imposed on $\Bbbk[X_1, \dots, X_n]$. If $\mathfrak{a}$ is any ideal in $\Bbbk[X_1, \dots, X_n]$, then the affine Hilbert functions of $\mathfrak{a}$ and $\mathrm{LT}(\mathfrak{a})$ coincide: $\mathcal{H}_a(s, \mathfrak{a}) = \mathcal{H}_a(s, \mathrm{LT}(\mathfrak{a}))$.

PROOF. Fix $s \ge 0$. It is enough to prove that $\mathfrak{a}_{\le s}$ and $\mathrm{LT}(\mathfrak{a})_{\le s}$ have the same $\Bbbk$ dimension. Since there are only finitely many monomials of degree $\le s$, we can choose $f_1, \dots, f_m$ in $\mathfrak{a}$ such that their leading monomials $\mathrm{LM}(f_1), \dots, \mathrm{LM}(f_k)$ are distinct and form a vector-space basis of $\mathrm{LT}(\mathfrak{a})_{\le s}$. Without loss of generality, we may assume that $\mathrm{LM}(f_1) > \cdots > \mathrm{LM}(f_k)$. Certainly $\dim \mathrm{LT}(\mathfrak{a})_{\le s} = k$, and thus it is enough to show that $f_1, \dots, f_k$ lie in $\mathfrak{a}_{\le s}$ and form a vector-space basis of $\mathfrak{a}_{\le s}$.

For each j, $\mathrm{LM}(f_j - \mathrm{LT}(f_j)) < \mathrm{LM}(f_j)$. Since the monomial ordering is graded, this inequality implies that $\deg(f_j - \mathrm{LT}(f_j)) \le s$. But we know that $\deg(\mathrm{LT}(f_j)) \le s$, and therefore $\deg f_j \le s$. Consequently f_j lies in $\mathfrak{a}_{\le s}$.

To prove that $\{f_1, \dots, f_k\}$ is linearly independent, suppose that $\sum_{j=1}^k c_j f_j = 0$ with all c_j in $\Bbbk$. Arguing by contradiction, suppose that not all c_j are 0. Let i be the

least index j for which $c_j \neq 0$; then $\text{LM}(f_i) = \text{LM}(c_i f_i) = \text{LM}\left(-\sum_{j>i} c_j f_j\right) \leq \max_{j>i} \text{LM}(f_j)$, and we arrive at a contradiction. We conclude that $\{f_1, \ldots, f_k\}$ is linearly independent.

To prove that $\{f_1, \ldots, f_k\}$ spans $\mathfrak{a}_{\leq s}$, we again argue by contradiction. Among all g in $\mathfrak{a}_{\leq s}$ with g not in the linear span of $\{f_1, \ldots, f_k\}$, choose one for which $\text{LM}(g)$ is the smallest. Certainly $\text{LM}(g)$ is one of $\text{LM}(f_1), \ldots, \text{LM}(f_k)$. Say that $\text{LM}(g) = \text{LM}(f_i)$. For some scalar $c \neq 0$, we must have $\text{LT}(g) = \text{LT}(cf_i)$. Then $\text{LM}(g - cf_i) < \text{LM}(g)$, and the minimality of $\text{LM}(g)$ forces $g - cf_i$ to be in the linear span of $\{f_1, \ldots, f_k\}$. Since cf_i is in the linear span, so is g, contradiction. Thus $\{f_1, \ldots, f_k\}$ is a spanning set of $\mathfrak{a}_{\leq s}$. □

Corollary 10.72. If $\mathfrak{a}$ is an ideal in $\Bbbk[X_1, \ldots, X_n]$, then for all s sufficiently large, the affine Hilbert function $\mathcal{H}_a(s, \mathfrak{a})$ of $\mathfrak{a}$ equals a polynomial in s of the form $\sum_{j=0}^{d} a_j \binom{s}{d-j}$ with integer coefficients a_j and with $a_0 > 0$.

REMARKS. The polynomial in the statement of the corollary is called the **affine Hilbert polynomial** of $\mathfrak{a}$ and is denoted by $H_a(s, \mathfrak{a})$. It is the 0 polynomial if and only if $\mathfrak{a} = \Bbbk[X_1, \ldots, X_n]$.

PROOF. Theorem 10.71 says that $\mathcal{H}_a(s, \mathfrak{a}) = \mathcal{H}_a(s, \text{LT}(\mathfrak{a}))$. Consequently the result follows immediately by applying Corollary 10.70 to $\text{LT}(\mathfrak{a})$. □

Corollary 10.73. If a graded monomial ordering is imposed on $\Bbbk[X_1, \ldots, X_n]$ and if $\mathfrak{a}$ is any ideal in $\Bbbk[X_1, \ldots, X_n]$, then the affine Hilbert polynomials of $\mathfrak{a}$ and $\text{LT}(\mathfrak{a})$ coincide: $H_a(s, \mathfrak{a}) = H_a(s, \text{LT}(\mathfrak{a}))$.

PROOF. This is immediate from Theorem 10.71 and the definition of the affine Hilbert polynomial given in the remarks with Corollary 10.72. □

Corollary 10.74. If $\mathfrak{a}$ and $\mathfrak{b}$ are proper ideals of $\Bbbk[X_1, \ldots, X_n]$ such that $\mathfrak{a} \subseteq \mathfrak{b}$, then $\deg H_a(s, \mathfrak{a}) \geq \deg H_a(s, \mathfrak{b})$.

PROOF. Introduce a graded monomial ordering. The inclusion $\mathfrak{a} \subseteq \mathfrak{b}$ implies that $\text{LT}(\mathfrak{a}) \subseteq \text{LT}(\mathfrak{b})$. Therefore $\mathcal{C}(\text{LT}(\mathfrak{a})) \supseteq \mathcal{C}(\text{LT}(\mathfrak{b}))$. Proposition 10.64b shows that the geometric dimension of $V(\text{LT}(\mathfrak{a}))$ is the largest vector-space dimension of a coordinate subspace that lies in $\mathcal{C}(\text{LT}(\mathfrak{a}))$, and the same thing is true for $\text{LT}(\mathfrak{b})$. Thus the geometric dimension of $V(\text{LT}(\mathfrak{a}))$ is $\geq$ the geometric dimension of $V(\text{LT}(\mathfrak{b}))$. By Theorem 10.68, $\deg H_a(s, \text{LT}(\mathfrak{a})) \geq \deg H_a(s, \text{LT}(\mathfrak{b}))$. The result now follows immediately from Corollary 10.73. □

The affine Hilbert polynomial $H_a(s, \mathfrak{a})$ of $\mathfrak{a}$ depends on $\mathfrak{a}$, not just $V(\mathfrak{a})$, but we shall be interested mainly in the degree of $H_a(s, \mathfrak{a})$. Proposition 10.76, as amplified in Corollary 10.77, implies that the degree depends only on $V(\mathfrak{a})$. It requires a lemma.

Lemma 10.75. If $\mathfrak{a}$ is a monomial ideal in $\Bbbk[X_1, \dots, X_n]$, then so is $\sqrt{\mathfrak{a}}$.

PROOF. The preliminary remarks in Section 9 show that $V(\mathfrak{a})$ is a finite union of coordinate subspaces. Let us write $V(\mathfrak{a}) = \bigcup_j E_j$ accordingly. By Proposition 10.2b, $\sqrt{\mathfrak{a}} = I(V(\mathfrak{a})) = I\big(\bigcup_j E_j\big) = \bigcap_j I(E_j)$. Since E_j is an affine variety and is equal to $V(X_{i_1}, \dots, X_{i_k})$ for suitable $X_{i_1}, \dots, X_{i_k}$, the Nullstellensatz shows that $I(E_j)$ is an ideal of the form $I(E) = (X_{i_1}, \dots, X_{i_k})$. This is a monomial ideal, and it is therefore enough to show that the finite intersection of monomial ideals is a monomial ideal. By induction it is enough to show that $\mathfrak{b} \cap \mathfrak{c}$ is a monomial ideal if $\mathfrak{b}$ and $\mathfrak{c}$ are monomial ideals. If an element of $\mathfrak{b} \cap \mathfrak{c}$ is given, then that element is a linear combination of the monomials in $\mathfrak{b}$ and is also a linear combination of the monomials in $\mathfrak{c}$. Since $\mathcal{M}$ is linearly independent, the element is a linear combination of monomials lying in $\mathfrak{b} \cap \mathfrak{c}$. Therefore $\mathfrak{b} \cap \mathfrak{c}$ is a monomial ideal. □

Proposition 10.76. If $\mathfrak{a}$ is a proper ideal in $\Bbbk[X_1, \dots, X_n]$, then the degrees of the affine Hilbert polynomials $H_a(s, \mathfrak{a})$ and $H_a(s, \sqrt{\mathfrak{a}})$ are equal.

PROOF. Fix a graded monomial ordering. We begin by proving that

$$\mathrm{LT}(\mathfrak{a}) \subseteq \mathrm{LT}(\sqrt{\mathfrak{a}}) \subseteq \sqrt{\mathrm{LT}(\mathfrak{a})}. \tag{$*$}$$

The left-hand inclusion is immediate because $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$. For the right-hand inclusion, let $f \neq 0$ be in $\sqrt{\mathfrak{a}}$, and let $X^\alpha = \mathrm{LM}(f)$ be the leading monomial of f. Since f is in $\sqrt{\mathfrak{a}}$, f^r is in $\mathfrak{a}$ for some $r > 0$. Since the leading monomial of a product is the product of the leading monomials, $\mathrm{LM}(f^r) = X^{r\alpha}$. Thus a power of X^α is exhibited as in $\mathrm{LT}(\mathfrak{a})$, and X^α is in $\sqrt{\mathrm{LT}(\mathfrak{a})}$. This proves $(*)$.

Applying Corollary 10.74 to $(*)$, we obtain

$$\deg H_a(s, \mathrm{LT}(\mathfrak{a})) \geq \deg H_a(s, \mathrm{LT}(\sqrt{\mathfrak{a}})) \geq \deg H_a(s, \sqrt{\mathrm{LT}(\mathfrak{a})}). \tag{$**$}$$

The ideal $\mathrm{LT}(\mathfrak{a})$ is a monomial ideal, and Lemma 10.75 shows that $\sqrt{\mathrm{LT}(\mathfrak{a})}$ is a monomial ideal. Then $\mathrm{LT}(\mathfrak{a})$ and $\sqrt{\mathrm{LT}(\mathfrak{a})}$ are monomial ideals with $V(\mathrm{LT}(\mathfrak{a})) = V(\sqrt{\mathrm{LT}(\mathfrak{a})})$, and Theorem 10.68 shows that

$$\deg H_a(s, \mathrm{LT}(\mathfrak{a})) = \deg H_a(s, \sqrt{\mathrm{LT}(\mathfrak{a})}).$$

Comparing this conclusion with $(**)$, we see that

$$\deg H_a(s, \mathrm{LT}(\mathfrak{a})) = \deg H_a(s, \mathrm{LT}(\sqrt{\mathfrak{a}})). \tag{$\dagger$}$$

In combination with the equalities $H_a(s, \mathfrak{a}) = H_a(s, \mathrm{LT}(\mathfrak{a}))$ and $H_a(s, \sqrt{\mathfrak{a}}) = H_a(s, \mathrm{LT}(\sqrt{\mathfrak{a}}))$ given by Corollary 10.73, $(\dagger)$ completes the proof. □

Corollary 10.77. If $\mathfrak{a}$ and $\mathfrak{b}$ are proper ideals in $\Bbbk[X_1, \ldots, X_n]$ with $V(\mathfrak{a}) \subseteq V(\mathfrak{b})$, then $\deg H_a(s, \mathfrak{a}) \le \deg H_a(s, \mathfrak{b})$.

PROOF. Application of $I(\cdot)$ to the inclusion $V(\mathfrak{a}) \subseteq V(\mathfrak{b})$ gives $\sqrt{\mathfrak{a}} = I(V(\mathfrak{a})) \supseteq I(V(\mathfrak{b})) = \sqrt{\mathfrak{b}}$. Then Corollary 10.74 and Proposition 10.76 together yield $\deg H_a(s, \mathfrak{a}) = \deg H_a(s, \sqrt{\mathfrak{a}}) \le \deg H_a(s, \sqrt{\mathfrak{b}}) = \deg H_a(s, \mathfrak{b})$. □

Theorem 10.78. If $\mathfrak{a}$ is a prime ideal in $\Bbbk[X_1, \ldots, X_n]$, then the degree of the affine Hilbert polynomial $H_a(s, \mathfrak{a})$ equals the geometric dimension of the affine variety $V(\mathfrak{a})$.

PROOF. Define $d = \deg H_a(s, \mathfrak{a})$ and $V = V(\mathfrak{a})$, and let $A(V)$ be the affine coordinate ring $A(V) = \Bbbk[X_1, \ldots, X_n]/\mathfrak{a}$. Theorem 10.7 shows that $\dim V$ equals the Krull dimension of $A(V)$, and Theorem 7.22 shows that the latter equals the transcendence degree over $\Bbbk$ of the field of fractions $\Bbbk(V)$ of $A(V)$. Thus the theorem will follow if we show that $\Bbbk(V)$ has transcendence degree d over $\Bbbk$.

Let $\varphi : \Bbbk[X_1, \ldots, X_n] \to A(V)$ be the quotient homomorphism, and put $x_i = \varphi(X_i)$ for $1 \le i \le n$. Introduce a graded monomial ordering on $\mathcal{M}$. Corollary 10.73 shows that $H_a(s, \mathfrak{a}) = H_a(s, \mathrm{LT}(\mathfrak{a}))$, and Theorem 10.68 shows that $V(\mathrm{LT}(\mathfrak{a}))$ has geometric dimension d. We saw in Section 9 that the zero locus of a monomial ideal is the finite union of coordinate subspaces, and it follows that $V(\mathrm{LT}(\mathfrak{a})) \subseteq \mathbb{A}^n$ contains a coordinate subspace E of dimension d. Let E have as basis the standard vectors $e_{j_1}, \ldots, e_{j_d}$, so that

$$E = V\big(\{X_i \mid i \notin \{j_1, \ldots, j_d\}\}\big).$$

The set E is a variety, and thus $I(E) = \big(\{X_i \mid i \notin \{j_1, \ldots, j_d\}\big)$. Also, $E \subseteq V(\mathrm{LT}(\mathfrak{a}))$, and hence $I(E) \supseteq I(V(\mathrm{LT}(\mathfrak{a}))) \supseteq \mathrm{LT}(\mathfrak{a})$. If X^α is a monomial in $\mathrm{LT}(\mathfrak{a})$, then it follows that X^α lies in the ideal generated by the X_i for $i \notin \{j_1, \ldots, j_d\}$. We can summarize this fact as follows: if we write $\Bbbk[X_{j_1}, \ldots, X_{j_d}]$ for the subring of $\Bbbk[X_1, \ldots, X_n]$ of polynomials involving only $X_{j_1}, \ldots, X_{j_d}$, then

$$\mathrm{LT}(\mathfrak{a}) \cap \Bbbk[X_{j_1}, \ldots, X_{j_d}] = 0. \tag{$*$}$$

If f is any nonzero member of $\Bbbk[X_{j_1}, \ldots, X_{j_d}]$, then its leading monomial $\mathrm{LM}(f)$ has to lie in $\Bbbk[X_{j_1}, \ldots, X_{j_d}]$, and thus $(*)$ implies that

$$\mathfrak{a} \cap \Bbbk[X_{j_1}, \ldots, X_{j_d}] = 0. \tag{$**$}$$

Using $(**)$ and notation introduced at the beginning of Section VII.4, we shall show that $x_{j_1}, \ldots, x_{j_d}$ are algebraically independent over $\Bbbk$, and then it follows that $d \le \mathrm{tr.deg}\, A(V)$. Thus suppose that $g(Y_1, \ldots, Y_d)$ is a polynomial in $\Bbbk[Y_1, \ldots, Y_d]$ such that $g(x_{j_1}, \ldots, x_{j_d}) = 0$. We can identify $\Bbbk[Y_1, \ldots, Y_d]$

with $\Bbbk[X_{j_1}, \ldots, X_{j_d}] \subseteq \Bbbk[X_1, \ldots, X_n]$, and then the equality $g(x_{j_1}, \ldots, x_{j_d}) = 0$ means that $\varphi(g) = 0$, i.e., g is in $\mathfrak{a}$. Hence g is a member of $\mathfrak{a} \cap \Bbbk[X_{j_1}, \ldots, X_{j_d}]$, and $g = 0$ by $(**)$. Therefore $x_{j_1}, \ldots, x_{j_d}$ are algebraically independent over $\Bbbk$.

For the reverse inequality, we are to prove that $d \geq \text{tr. deg } A(V)$. Let $r = \text{tr. deg } A(V)$. The elements $x_j = \varphi(X_j)$ generate $A(V)$ as a $\Bbbk$ algebra, and therefore they generate $\Bbbk(V)$ over $\Bbbk$ as a field. By Lemma 7.6b some subset $\{x_{j_1}, \ldots, x_{j_d}\}$ of $\{x_1, \ldots, x_n\}$ is algebraically independent. Consider the substitution homomorphism

$$\psi(h) = h(x_{j_1}, \ldots, x_{j_r})$$

of $\Bbbk[Y_1, \ldots, Y_r]$ into $A(V)$. This is one-one because the elements $x_{j_1}, \ldots, x_{j_d}$ by assumption are algebraically independent. Fix $s \geq 0$, and consider the restriction of ψ to $\Bbbk[Y_1, \ldots, Y_r]_{\leq s}$. If $h(Y_1, \ldots, Y_r)$ is a monomial Y^α in $\Bbbk[Y_1, \ldots, Y_r]_{\leq s}$ with $\alpha = (\alpha_1, \ldots, \alpha_r)$ and $|\alpha| \leq s$, then we see that

$$\psi(Y^\alpha) = \prod_{i=1}^{r} {x_{j_i}}^{\alpha_i} = \varphi\Big(\prod_{i=1}^{r} {X_{j_i}}^{\alpha_i}\Big).$$

In other words, $\psi(Y^\alpha)$ is the image under φ of a member of $\Bbbk[X_1, \ldots, X_n]$ of degree $\leq s$. Taking linear combinations of such monomials, we see that $\psi(h)$ is a one-one $\Bbbk$ linear mapping

$$\psi : \Bbbk[Y_1, \ldots, Y_r]_{\leq s} \to \Bbbk[X_1, \ldots, X_n]_{\leq s}/\mathfrak{a}_{\leq s} \subseteq A(V).$$

Therefore

$$H_a(s, \mathfrak{a}) = \dim_{\Bbbk}\big(\Bbbk[X_1, \ldots, X_n]_{\leq s}/\mathfrak{a}_{\leq s}\big) \geq \dim_{\Bbbk} \Bbbk[Y_1, \ldots, Y_r]_{\leq s} = \tbinom{r+s}{r}.$$

The binomial coefficient on the right side is a polynomial of degree r in s with positive leading coefficient. The left side is a polynomial in s of degree d. The inequality forces $d \geq r$, and the proof is complete. □

Proposition 10.79. If $\mathfrak{a}$ and $\mathfrak{b}$ are proper ideals in $\Bbbk[X_1, \ldots, X_n]$, then $\deg H_a(s, \mathfrak{ab}) = \max\big(\deg H_a(s, \mathfrak{a}), \deg H_a(s, \mathfrak{b})\big)$.

REMARKS. Proposition 10.1 points out that $V(\mathfrak{ab}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$. Since the degree of the affine Hilbert polynomial of $\mathfrak{a}$ depends only on $V(\mathfrak{a})$, this proposition says that the degree associated with the union of two affine algebraic sets is the larger of the degrees associated with each of the sets.

PROOF. Impose a graded monomial ordering on $\mathcal{M}$. Let us check that

$$\big(\text{LT}(\mathfrak{a})\big)\big(\text{LT}(\mathfrak{b})\big) \subseteq \text{LT}(\mathfrak{ab}) \subseteq \text{LT}(\mathfrak{a} \cap \mathfrak{b}) \subseteq \sqrt{\big(\text{LT}(\mathfrak{a})\big)\big(\text{LT}(\mathfrak{b})\big)}\,. \qquad (*)$$

In fact, let f be in $\mathfrak{a}$ and g be in $\mathfrak{b}$, and define $X^\alpha = \text{LM}(f)$ and $X^\beta = \text{LM}(g)$ to be the leading monomials of f and g. Then $X^{\alpha+\beta} = \text{LM}(fg)$, and hence the product of any generator of $\text{LT}(\mathfrak{a})$ and any generator of $\text{LT}(\mathfrak{b})$ lies in $\text{LT}(\mathfrak{ab})$.

This proves the first inclusion of $(*)$. The second inclusion is immediate because $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$. If $X^\alpha = \operatorname{LM}(f)$ with $f \in \mathfrak{a} \cap \mathfrak{b}$, then $(X^\alpha)^2 = \operatorname{LM}(f)\operatorname{LM}(f)$ is in $\operatorname{LT}(\mathfrak{a})\operatorname{LT}(\mathfrak{b})$. Hence X^α is in $\sqrt{\big(\operatorname{LT}(\mathfrak{a})\big)\big(\operatorname{LT}(\mathfrak{b})\big)}$. Thus a generating set of $\operatorname{LT}(\mathfrak{a}\cap\mathfrak{b})$ lies in $\sqrt{\big(\operatorname{LT}(\mathfrak{a})\big)\big(\operatorname{LT}(\mathfrak{b})\big)}$, and the third inclusion of $(*)$ follows.

In $(*)$, the values of $V(\,\cdot\,)$ on the end two members are the same, according to Proposition 10.3c, and therefore

$$V\big(\operatorname{LT}(\mathfrak{a})\operatorname{LT}(\mathfrak{b})\big) = V(\operatorname{LT}(\mathfrak{ab})). \tag{$**$}$$

The proposition now follows from the computation

$$\begin{aligned}
&\max(\deg H_a(s,\mathfrak{a}), \deg H_a(s,\mathfrak{b}))\\
&\qquad = \max(\deg H_a(s, \operatorname{LT}(\mathfrak{a})), \deg H_a(s, \operatorname{LT}(\mathfrak{b}))) && \text{by Corollary 10.73}\\
&\qquad = \max(\dim V(\operatorname{LT}(\mathfrak{a})), \dim V(\operatorname{LT}(\mathfrak{b}))) && \text{by Theorem 10.68}\\
&\qquad = \dim\big(V(\operatorname{LT}(\mathfrak{a})) \cup V(\operatorname{LT}(\mathfrak{b}))\big) && \text{by Theorem 10.7}\\
&\qquad = \dim(V(\operatorname{LT}(\mathfrak{a})\operatorname{LT}(\mathfrak{b})) && \text{by Proposition 10.1c}\\
&\qquad = \dim V(\operatorname{LT}(\mathfrak{ab})) && \text{by } (**)\\
&\qquad = \deg H_a(s, \operatorname{LT}(\mathfrak{ab})) && \text{by Theorem 10.68}\\
&\qquad = \deg H_a(s, \mathfrak{ab}) && \text{by Corollary 10.73. } \square
\end{aligned}$$

Corollary 10.80. If $\mathfrak{a}$ is any ideal in $\Bbbk[X_1, \dots, X_n]$, then the geometric dimension of the affine algebraic set $V(\mathfrak{a})$ equals the degree of the affine Hilbert polynomial $H_a(s, \mathfrak{a})$.

PROOF. Write $V(\mathfrak{a}) = \bigcup_{j=1}^k V_j$ as a finite union of affine varieties V_j, and define $\mathfrak{p}_j = I(V_j)$. Since V_j is irreducible, $\mathfrak{p}_j$ is prime. Moreover, $V_j = V(I(V_j)) = V(\mathfrak{p}_j)$. Then Proposition 10.1c shows that $V(\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_k) = \bigcup_{j=1}^k V(\mathfrak{p}_j) = \bigcup_{j=1}^k V_j = V(\mathfrak{a})$. Proposition 10.79 and induction give

$$\deg H_a(s, \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_k) = \max_{1\le j\le n} \deg H_a(s, \mathfrak{p}_j),$$

and Theorem 10.78 shows that the right side equals $\max_{1\le j\le k} \dim V(\mathfrak{p}_j) = \max_{1\le j\le k} \dim V_j$, which equals $\dim V(\mathfrak{a})$ by Theorem 10.7. $\square$

As a consequence of Corollary 10.80, we obtain an algorithm for computing the dimension of an affine algebraic set V when given an ideal $\mathfrak{a}$ whose locus of common zeros $V(\mathfrak{a})$ is V: We introduce any graded monomial ordering and compute $\operatorname{LT}(\mathfrak{a})$, using a Gröbner basis. Corollaries 10.73 and 10.80 together say that $\dim V(\mathfrak{a}) = \dim V(\operatorname{LT}(\mathfrak{a}))$. The remarks before Proposition 10.64 show how to compute $\dim V(\operatorname{LT}(\mathfrak{a}))$, and Proposition 10.64b gives an alternative method of computation.

11. Hilbert Polynomial in the Projective Case

In this section we consider the analog for projective space of the theory of Section 10. We continue with $\Bbbk$ as an algebraically closed field, and we let $\widetilde{A} = \Bbbk[X_0, \ldots, X_n]$. Our interest is in the zero locus $V(\mathfrak{a})$ in $\mathbb{P}^n$, as defined in Section 3, of a homogeneous ideal $\mathfrak{a}$ in $\widetilde{A}$. To relate matters to Section 10, we shall make use of the **cone** $C(V(\mathfrak{a}))$ over $V(\mathfrak{a})$, which was defined in Section 3 as

$$C(V(\mathfrak{a})) = (0, \ldots, 0) \cup \big\{(x_0, \ldots, x_n) \in \mathbb{A}^{n+1} \mid [x_0, \ldots, x_n] \in V(\mathfrak{a})\big\}.$$

The homogeneous ideal $\mathfrak{a}$ is in particular an ideal in $n+1$ variables, and its associated affine algebraic set is the subset $C(V(\mathfrak{a}))$ of $\mathbb{A}^{n+1}$. An affine Hilbert polynomial $H_a(s, \mathfrak{a})$ is therefore associated to $C(V(\mathfrak{a}))$, and its degree matches the geometric dimension of $C(V(\mathfrak{a}))$.

To get something directly related to the projective algebraic set $V(\mathfrak{a})$ in projective space $\mathbb{P}^n$, we make a new definition of Hilbert function. Let $\widetilde{A}_s = \Bbbk[X_0, \ldots, X_n]_s$ be the subspace $\widetilde{A}$ of all polynomials homogeneous of degree s. If $\mathfrak{a}$ is a homogeneous ideal in $\widetilde{A}$, let $\mathfrak{a}_s = \mathfrak{a} \cap \widetilde{A}_s$. The **Hilbert function**[24] of $\mathfrak{a}$ is the integer-valued function of $s \geq 0$ defined by

$$\mathcal{H}(s, \mathfrak{a}) = \dim_{\Bbbk} \widetilde{A}_s/\mathfrak{a}_s \qquad \text{for } s \geq 0.$$

We have $\widetilde{A}_{\leq s} = \widetilde{A}_s \oplus \widetilde{A}_{\leq s-1}$, and the fact that $\mathfrak{a}$ is homogeneous implies that $\mathfrak{a}_{\leq s} = \mathfrak{a}_s \oplus \mathfrak{a}_{\leq s-1}$. Consequently $\widetilde{A}_{\leq s}/\mathfrak{a}_{\leq s} \cong \widetilde{A}_s/\mathfrak{a}_s \oplus \widetilde{A}_{\leq s-1}/\mathfrak{a}_{\leq s-1}$. Therefore

$$\mathcal{H}(s, \mathfrak{a}) = \mathcal{H}_a(s, \mathfrak{a}) - \mathcal{H}_a(s-1, \mathfrak{a}).$$

This is the fundamental formula by which the algebraic part of the theory of the Hilbert function in the projective case can be reduced to the corresponding theory in the affine case.

We know that the affine Hilbert function is a polynomial for large s. Since

$$s^d - (s-1)^d = s^{d-1} - s^{d-2} + s^{d-3} - \cdots + (-1)^{d+1}$$

is a polynomial of one lower degree and with positive leading coefficient, it follows that the Hilbert function of $\mathfrak{a}$ is a polynomial for large s, that its degree is $\dim C(V(\mathfrak{a})) - 1$, and that its leading coefficient is positive. This polynomial is called the **Hilbert polynomial** of $\mathfrak{a}$ and is denoted by $H(s, \mathfrak{a})$. To connect the geometric part of the theory of the Hilbert function in the projective case to the corresponding theory in the affine case, we use the following proposition.

[24] It is traditional not to include the word "projective" or any subscript, even though the terminology is meant to refer to the projective case.

Proposition 10.81. If $\mathfrak{a}$ is a homogeneous ideal in $\Bbbk[X_0, \dots, X_n]$ and if the corresponding projective algebraic set $V(\mathfrak{a})$ is nonempty, then

$$\dim C(V(\mathfrak{a})) = \dim V(\mathfrak{a}) + 1.$$

PROOF. The proof of Corollary 10.13 shows that $C(V(\mathfrak{a}))$ is irreducible in $\mathbb{A}^{n+1}$ if and only if $V(\mathfrak{a})$ is irreducible in $\mathbb{P}^n$. Since the dimension in both cases for a general $\mathfrak{a}$ is the maximum of the dimensions of irreducible closed subsets, it is enough to prove the dimensional equality in the irreducible case.

If we have a strictly increasing sequence of irreducible closed subsets $E_0 \subsetneqq E_1 \subsetneqq \cdots \subsetneqq E_d$ in $\mathbb{P}^n$, then each $C(E_j)$ is irreducible in $\mathbb{A}^{n+1}$, and the sequence $C(E_0) \subsetneqq C(E_1) \subsetneqq \cdots \subsetneqq C(E_d)$ in $\mathbb{A}^{n+1}$ consists of Zariski closed sets that are irreducible. Since the subset $\{0\}$ of $\mathbb{A}^{n+1}$ is irreducible and can be adjoined at the beginning of the latter sequence, we conclude that $\dim C(V(\mathfrak{a})) \geq \dim V(\mathfrak{a}) + 1$.

We need to prove the reverse inequality in the irreducible case. Since $V(\mathfrak{a})$ is assumed irreducible (and hence nonempty), we may assume that $\mathfrak{a}$ is prime and omits at least one of $X_0, \dots, X_n$. To fix the notation, say that X_0 is not in $\mathfrak{a}$. Recall from Section 3 the substitution homomorphism $\beta_0^t : \Bbbk[X_0, \dots, X_n] \to \Bbbk[X_1, \dots, X_n]$ formed by setting $X_0 = 1$. Let $\mathfrak{b} = \beta_0^t(\mathfrak{a})$. This is a prime ideal in $\Bbbk[X_1, \dots, X_n]$, according to Theorem 10.20. Let $A(C(V(\mathfrak{a}))) = \Bbbk[X_0, \dots, X_n]/\mathfrak{a}$ and $A(V(\mathfrak{b})) = \Bbbk[X_1, \dots, X_n]/\mathfrak{b}$. The homomorphism β_0^t descends to a homomorphism of $A(C(V(\mathfrak{a}))$ onto $A(V(\mathfrak{b}))$, which we denote by $\bar{\beta}_0^t$.

Let $x_0, \dots, x_n$ be the images of $X_0, \dots, X_n$ in $A(C(V(\mathfrak{a})))$. The element x_0 is transcendental over $\Bbbk$. In fact, the only alternative is that it is a scalar c, since $\Bbbk$ is algebraically closed; the equality $x_0 = c$ would imply that $X_0 - c$ is in $\mathfrak{a}$, and the fact that $\mathfrak{a}$ is homogeneous would imply that X_0 and c are separately in $\mathfrak{a}$, in contradiction to our choice of X_0. Consequently $\Bbbk(x_0)(x_1, \dots, x_n)$ has transcendence degree $r = \dim C(V(\mathfrak{a})) - 1$ over $\Bbbk(x_0)$. Since $x_1, \dots, x_n$ generate $\Bbbk(x_0)(x_1, \dots, x_n)$ as a field over $\Bbbk(x_0)$, some subset $\{x_{j_1}, \dots, x_{j_r}\}$ of $\{x_1, \dots, x_n\}$ is a transcendence basis of $\Bbbk(x_0)(x_1, \dots, x_n)$ as a field over $\Bbbk(x_0)$. Thus $\{x_0, x_{j_1}, \dots, x_{j_r}\}$ is a transcendence basis of $\Bbbk(x_0, \dots, x_n)$ over $\Bbbk$.

The elements $x_0, x_{j_1}, \dots, x_{j_r}$ all lie in $A(C(V(\mathfrak{a})))$, and we consider their images $1, \bar{\beta}_0^t(x_{j_1}), \dots, \bar{\beta}_0^t(x_{j_r})$ in $A(V(\mathfrak{b}))$. Suppose that $h(Y_1, \dots, Y_r)$ is a polynomial in r variables exhibiting the last r of these images as algebraically dependent. That is, suppose that

$$h\big(\bar{\beta}_0^t(x_{j_1}), \dots, \bar{\beta}_0^t(x_{j_r})\big) = 0. \tag{$*$}$$

Let h have degree d. We regard h as a member of $\Bbbk[X_1, \dots, X_n]_{\leq d}$ that depends only on $X_{j_1}, \dots, X_{j_n}$. With this notational change, $(*)$ reads

$$h(X_1, \dots, X_n) \qquad \text{is in } \mathfrak{b}. \tag{$**$}$$

We now refer to the details of the proof of Theorem 10.20 that are summarized before Proposition 10.33. The linear mapping φ_d with $\varphi_d(f)(X_0, \ldots, X_n) = X_0^d f(X_1/X_0, \ldots, X_n/X_0)$ is a two-sided inverse to $\beta_0^t : \Bbbk[X_0, \ldots, X_n]_d \to \Bbbk[X_1, \ldots, X_n]_{\le d}$. Put $H = \varphi_d(h)$, so that $h = \beta_0^t(H)$. The detail in question is that

$$\mathfrak{a} \cap \Bbbk[X_0, \ldots, X_n]_d = \varphi_d\big(\mathfrak{b} \cap \Bbbk[X_1, \ldots, X_n]_{\le d}\big). \tag{$\dagger$}$$

By $(**)$, $\varphi_d(h)$ is in the right side of $(\dagger)$. Since $(\dagger)$ is a valid identity, $\varphi_d(h)$ is in the left side. So H is in $\mathfrak{a}$. This means that $H(x_0, \ldots, x_n) = 0$. Remembering that H depends only on $X_0, X_{j_1}, \ldots, X_{j_r}$ and that $\{x_0, x_{j_1}, \ldots, x_{j_r}\}$ is a transcendence set, we see that $H = 0$. Therefore $h = 0$, and $\{\bar\beta_0^t(x_{j_1}), \ldots, \bar\beta_0^t(x_{j_r})\}$ is a transcendence set in $A(V(\mathfrak{b}))$. Thus

$$\dim V(\mathfrak{b}) = \text{tr. deg } A(V(\mathfrak{b})) \ge r = \text{tr. deg } A(C(V(\mathfrak{a})) - 1 = \dim C(V(\mathfrak{a})) - 1.$$

By Corollary 10.19, $\dim V(\mathfrak{b}) = \dim V(\mathfrak{a})$. Hence $\dim C(V(\mathfrak{a})) \le \dim V(\mathfrak{a}) + 1$, and the proof is complete. □

Corollary 10.82. If $\mathfrak{a}$ is a homogeneous ideal in $\Bbbk[X_0, \ldots, X_n]$ and if the corresponding projective algebraic set $V(\mathfrak{a})$ is nonempty, then $\dim V(\mathfrak{a})$ equals the degree of the Hilbert polynomial $H(s, \mathfrak{a})$.

PROOF. This is immediate from Proposition 10.81 because $\dim C(V(\mathfrak{a})) = \dim H_a(s, \mathfrak{a})$ and because $\deg H(s, \mathfrak{a}) = \deg H_a(s, \mathfrak{a}) - 1$. □

We could also obtain a corollary relating $H(s, V(\mathfrak{a}))$ and $H(s, V(\text{LT}(\mathfrak{a})))$ when a graded monomial ordering is imposed, and we could then give a geometric way of visualizing the dimension in terms of the projective case. But we shall not need these details, and we omit them.

12. Intersections in Projective Space

Hilbert polynomials are an appropriate tool for dealing with how a projective algebraic set intersects a lower-dimensional projective space. In this section we consider such intersections, and we obtain as a corollary the deep result that a system of homogeneous polynomial equations over an algebraically closed field $\Bbbk$ always has a nonzero solution if there are more variables than equations.

It will be convenient in this section to adopt the convention that the empty projective algebraic set has dimension -1 and that the 0 Hilbert polynomial has degree -1. To make use of this convention, we recall from the homogeneous Nullstellensatz (Proposition 10.12a) that a homogeneous ideal $\mathfrak{a}$ in $\Bbbk[X_0, \ldots, X_n]$ has $V(\mathfrak{a})$ empty in $\mathbb{P}^n$ if and only if there is an integer N such that $\mathfrak{a}$ contains $\Bbbk[X_0, \ldots, X_n]_k$ for $k \ge N$. In this case our definition makes $C(V(\mathfrak{a}))$ consist

of $\{0\}$ alone.[25] With the convention that such ideals have $\dim V(\mathfrak{a}) = -1$ and $C(V(\mathfrak{a})) = \{0\}$, the formula of Proposition 10.81 remains valid, and we can therefore drop the assumption that $V(\mathfrak{a})$ is nonempty. As to Corollary 10.82, the definition of the Hilbert function when $\mathfrak{a}$ contains $\Bbbk[X_0, \dots, X_n]_k$ for all sufficiently large k makes $\mathcal{H}(k, \mathfrak{a}) = 0$ for such k; therefore the Hilbert polynomial in this case is the 0 polynomial, and Corollary 10.82 continues to be valid even when $V(\mathfrak{a})$ is empty.

Theorem 10.83. If $\mathfrak{a}$ is any homogeneous ideal in $\Bbbk[X_0, \dots, X_n]$ and if F is a homogeneous polynomial, then

$$\dim V(\mathfrak{a}) \geq \dim V(\mathfrak{a} + (F)) \geq \dim V(\mathfrak{a}) - 1.$$

In particular, $V(\mathfrak{a} + (F))$ is nonempty if $\dim V(\mathfrak{a}) \geq 1$.

PROOF. Since $\mathfrak{a} \subseteq \mathfrak{a} + (F)$ and since $V(\,\cdot\,)$ is inclusion reversing, we know that

$$\dim V(\mathfrak{a}) \geq \dim V(\mathfrak{a} + (F)).$$

To obtain the second inequality of the theorem, we shall compare the Hilbert polynomials $H(s, \mathfrak{a})$ and $H(s, \mathfrak{a} + (F))$, taking advantage of Corollary 10.82. Let $d = \deg F$, and suppose that $s > d$. The identity mapping on $\Bbbk[X_0, \dots, X_n]_s$ descends to a $\Bbbk$ linear mapping

$$\varphi : \Bbbk[X_0, \dots, X_n]_s/\mathfrak{a}_s \to \Bbbk[X_0, \dots, X_n]_s\big/(\mathfrak{a} + (F))_s,$$

and φ is onto, being formed from an onto map. To understand $\ker \varphi$, we shall use the $\Bbbk$ linear map

$$\psi : \Bbbk[X_0, \dots, X_n]_{s-d}/\mathfrak{a}_{s-d} \to \Bbbk[X_0, \dots, X_n]_s/\mathfrak{a}_s$$

induced by multiplication by F, which we view as carrying $\Bbbk[X_0, \dots, X_n]_{s-d}$ into $\Bbbk[X_0, \dots, X_n]_s/\mathfrak{a}_s$. Observe that if G is in $\Bbbk[X_0, \dots, X_n]_{s-d}$, then FG is in $(\mathfrak{a} + (F))_s$, and therefore $\varphi \circ \psi = 0$, i.e., image $\psi \subseteq \ker \varphi$.

We shall prove that equality holds. Thus suppose that G is a member of $\Bbbk[X_0, \dots, X_n]_s$ such that $G + \mathfrak{a}_s$ is in $\ker \varphi$, i.e., that G is in $(\mathfrak{a} + (F))_s$. Then we can write $G = G_1 + HF$ with G_1 in $\mathfrak{a}_s$ and H in $\Bbbk[X_0, \dots, X_n]_{s-d}$. So $G - G_1 = HF$, and the coset $G + \mathfrak{a}_s = G - G_1 + \mathfrak{a}_s$ is ψ of $H + \mathfrak{a}_{s-d}$. We conclude that image $\psi = \ker \varphi$.

Now we compute

$$\begin{aligned}
&\dim_{\Bbbk} \Bbbk[X_0, \dots, X_n]_s/\mathfrak{a}_s \\
&\qquad = \dim_{\Bbbk}(\text{domain}\,\varphi) = \dim_{\Bbbk}(\ker \varphi) + \dim_{\Bbbk}(\text{image}\,\varphi) \\
&\qquad = \dim_{\Bbbk}(\text{image}\,\psi) + \dim_{\Bbbk} \Bbbk[X_0, \dots, X_n]_s\big/(\mathfrak{a} + (F))_s \\
&\qquad \leq \dim_{\Bbbk} \Bbbk[X_0, \dots, X_n]_{s-d}/\mathfrak{a}_{s-d} + \dim_{\Bbbk} \Bbbk[X_0, \dots, X_n]_s\big/(\mathfrak{a} + (F))_s.
\end{aligned}$$

[25] Admittedly the inclusion of $\{0\}$ in the cone might seem unnatural if $\mathfrak{a} = \Bbbk[X_0, \dots, X_n]$, but that is the definition that makes this particular $\mathfrak{a}$ behave like all other ideals.

In terms of Hilbert functions, this says that

$$\mathcal{H}(s, \mathfrak{a}) \leq \mathcal{H}(s - d, \mathfrak{a}) + \mathcal{H}(s, \mathfrak{a} + (F)).$$

For large s, this is an inequality of polynomials:

$$H(s, \mathfrak{a}) \leq H(s - d, \mathfrak{a}) + H(s, \mathfrak{a} + (F)).$$

Since $H(s, \mathfrak{a}) - H(s - d, \mathfrak{a})$ is a polynomial of one lower degree than $H(s, \mathfrak{a})$ with leading coefficient positive, we obtain

$$\deg H(s, \mathfrak{a}) - 1 \leq \deg H(s, \mathfrak{a} + (F)).$$

The second inequality of the theorem now follows from Corollary 10.82. The final assertion in the theorem takes into account the remarks in the paragraph preceding the statement of the theorem. □

Corollary 10.84. If $\mathfrak{a}$ is any homogeneous ideal in $\Bbbk[X_0, \ldots, X_n]$ and if $F_1, \ldots, F_r$ are homogeneous polynomials, then

$$\dim V(\mathfrak{a}) \geq \dim V(\mathfrak{a} + (F_1, \ldots, F_r)) \geq \dim V(\mathfrak{a}) - r.$$

In particular, $V(\mathfrak{a} + (F_1, \ldots, F_r))$ is nonempty if $\dim V(\mathfrak{a}) \geq r$.

PROOF. We use Theorem 10.83 inductively, first applying it to the ideal $\mathfrak{a}$ with $F = F_1$, then applying it to the ideal $\mathfrak{a} + (F_1)$ with $F = F_2$, and so on. This proves the first conclusion, and the second conclusion follows because of the convention that the empty set has dimension -1. □

Corollary 10.85. Over an algebraically closed field any system of homogeneous polynomial equations with more variables than equations has a nonzero solution.

PROOF. Let there be r equations and $n + 1$ variables with $n + 1 > r$, the equations being $F_1 = 0, \ldots, F_r = 0$. The zero locus for each equation is a subset of $\mathbb{P}^n$. Applying Corollary 10.84 with $\mathfrak{a} = 0$ shows that $\dim V(F_1, \ldots, F_r) \geq n - r \geq 0$ and that $V(F_1, \ldots, F_r)$ is not empty as long as $n \geq r$. □

Corollary 10.85 is the result in the present chapter that was anticipated in Problem 23 at the end of Chapter VIII.

13. Schemes

We conclude with some commentary about "schemes." The subject of algebraic geometry studied along the lines of Sections 1–12 suffers from at least two shortcomings. One concerns the coefficients that are involved. The original impetus for the subject came from systems of polynomial equations in several variables. These equations involve addition, subtraction, and multiplication, and the requirement that division be allowable is unnatural and cuts down the scope of the subject. It immediately cuts out Diophantine equations, for example, to say nothing of congruences modulo prime powers. It would be more natural to allow the coefficients to lie in any commutative ring with identity. The other shortcoming is that the definition of variety depends on an embedding whose chief role is to get past the stage of making definitions; soon the embedding is stripped away, and the interest is in varieties up to isomorphism. The situation is similar to the historical treatment of groups and of manifolds. Groups were for the most part originally conceived in terms of group actions, but eventually the groups were separated from the actions. Manifolds at first were defined as certain subsets of Euclidean space, but eventually they were given an intrinsic definition. It would be more in keeping with the wisdom gained from other areas of mathematics if varieties could be defined intrinsically right away.

Schemes, introduced and developed by A. Grothendieck in the late 1950s and early 1960s, accomplish both these objectives. The theory of schemes borrows ideas and techniques from many areas of mathematics, as will be apparent shortly. This section will briefly present some of the definitions, offer some examples, and show the sense in which varieties may be regarded as schemes.[26] The interested reader may want to read more, and this section will therefore conclude with some bibliographical remarks.

1. Spectrum. One preliminary remark is necessary. To isolate an affine variety from its ambient space $\mathbb{A}^n$, we can take advantage of Proposition 10.23, which says that the points of the variety correspond exactly to the maximal ideals of the affine coordinate ring.[27] The set of maximal ideals in a ring, however, is usually not an object that lends itself to use with mappings. For example the canonical inclusion of $\mathbb{Z}$ into $\mathbb{Q}$ is not reflected in any of the mappings of the singleton set $\{(0)\}$ of maximal ideals of $\mathbb{Q}$ into the set of maximal ideals of $\mathbb{Z}$. Instead, the theory of schemes works with *prime* ideals. These behave nicely in that the inverse image of a prime ideal under a homomorphism of rings with identity is a prime ideal.

[26] The material in this section is based in part on lectures by V. Schechtman given in 1991–92 and in part on the books by Gunning, Hartshorne, and Shafarevich in the Selected References.

[27] Readers familiar with some functional analysis will recognize that a similar thing happens with compact Hausdorff spaces; by a theorem of M. Stone, the points of the space correspond exactly to the maximal ideals of the algebra of continuous complex-valued functions on the space.

Thus we work with the category of commutative rings with identity, the motivating example being the affine coordinate ring of an affine variety over an algebraically closed field. If A is a ring in this category, the **spectrum** of A is the set Spec A of prime ideals of A. For example the spectrum of a field consists of the one element (0), that of a discrete valuation ring consists of 0 and the unique maximal ideal, that of a principal ideal domain consists of 0 and the principal ideals (f) such that f is an irreducible element, and that of $\mathbb{C}[X, Y]$ consists of the ideal (0), the maximal ideals corresponding to one-point sets in $\mathbb{C}^2$, and all prime ideals $(f(X, Y))$ of irreducible affine plane curves over $\mathbb{C}$.

The spectrum of A is understood to carry along with it two additional pieces of structure. The first piece of structure is an analog for Spec A of the Zariski topology.[28] To each ideal $\mathfrak{a}$ of A, we associate the subset $V(\mathfrak{a}) \subseteq$ Spec A of all prime ideals $\mathfrak{p}$ with $\mathfrak{a} \subseteq \mathfrak{p}$. The sets $V(\mathfrak{a})$ are easily seen to have the defining properties of the closed sets of a topology, and this topology will always be understood to be in place. It is immediate from the definition that $V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}})$ for every ideal $\mathfrak{a}$. One checks for any prime ideal $\mathfrak{p}$ that $V(\mathfrak{p}) = \overline{\{\mathfrak{p}\}}$; consequently the one-point set $\{\mathfrak{p}\}$ is closed if and only if $\mathfrak{p}$ is a maximal ideal.

At least when A is Noetherian, Spec A is a Noetherian space, and a notion of dimension (not necessarily finite) is defined for each closed set in the usual way[29] as in Section 2; for A itself this coincides with the Krull dimension of A. In this situation the irreducible closed sets are the sets $V(\mathfrak{p})$ with $\mathfrak{p}$ prime. The fact that such a set is irreducible follows from the identity $V(\mathfrak{p}) = \overline{\{\mathfrak{p}\}}$; the converse assertion follows from the identity $V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}})$ and the Lasker–Noether Decomposition Theorem (Problem 14 at the end of Chapter VII). By Proposition 10.5 every closed set is a finite union of irreducible closed sets, and thus we have a complete description of the closed sets. For example, in a principal ideal domain the closed sets consist of the finite sets of nonzero prime ideals, as well as the set of all prime ideals. For the ring $A = \mathbb{C}[X, Y]$, every proper closed set of Spec A is a finite union of singleton sets $\{(X - x_0, Y - y_0)\}$ and of sets

$$\{(f(X, Y))\} \cup \bigcup_{f(x_0, y_0)=0} \{(X - x_0, Y - y_0)\}$$

with $f(X, Y)$ irreducible.

If $\varphi : A \to B$ is a homomorphism in our category of rings (always assumed to carry 1 to 1) and if $\mathfrak{p}$ is a prime ideal in B, then $\varphi^{-1}(\mathfrak{p})$ is a prime ideal in A. Thus the definition ${}^a\varphi(\mathfrak{p}) = \varphi^{-1}(\mathfrak{p})$ gives us a function ${}^a\varphi :$ Spec $B \to$ Spec A. If E is a subset of A, then we readily check that

$$({}^a\varphi)^{-1}(V(E)) = ({}^a\varphi)^{-1}(\{\mathfrak{p} \mid \mathfrak{p} \supseteq E\}) = \{\mathfrak{q} \mid {}^a\varphi(\mathfrak{q}) \supseteq E\} = V(\varphi(E)),$$

[28] A little care is needed with the definitions when A is the 0 ring, which has an identity but no prime ideals. Then Spec A is empty, but we will want to allow it as part of the theory. So we need to allow the empty set as a topological space.

[29] The general theory treats dimension as defined even when A is not Noetherian, but it will be enough in this section to consider only the Noetherian case.

from which it follows that ${}^a\varphi$ is continuous. The function ${}^a\varphi$ can be fairly subtle. For example, if φ is the inclusion of $\mathbb{Z}$ into the ring R of algebraic integers in a number field and if P is a nonzero prime ideal in R, then ${}^a\varphi(P) = P \cap \mathbb{Z}$ is the corresponding prime ideal (p) in $\mathbb{Z}$; the continuity of ${}^a\varphi$ implies that each nonzero prime ideal (p) of $\mathbb{Z}$ arises in this way from only finitely many ideals P in R.

2. Structure sheaf. The second piece of additional structure carried by the spectrum of A is its "structure sheaf," which is a certain specific sheaf with base space Spec A. Sheaves were introduced by J. Leray in 1946 in connection with partial differential equations and by K. Oka and H. Cartan about 1950 in connection with the theory of several complex variables. As with vector bundles, sheaves may be viewed as having a base space carrying some topological information and fibers carrying some algebraic information; local sections will be of great interest. The initial example of a sheaf in several complex variables is the "sheaf of germs of holomorphic functions" on an open set in $\mathbb{C}^n$, germs being defined for holomorphic functions on an open set in the same way as they were defined in Section 4 for rational functions on a quasi-affine variety.

We shall define two general notions, "sheaf" and "presheaf," and compare them. The prototype of a presheaf in several complex variables is the collection of vector spaces of holomorphic functions on each nonempty open subset of the given open set; the prototype in classical algebraic geometry is the collection of regular functions on each nonempty open subset of a quasiprojective variety. In the general case, fix a category to describe the allowable structure on each fiber; common choices for the objects in this category are abelian groups, commutative rings with identity (called "rings" hereafter in this section), and unital R modules for some ring. In defining sheaves and presheaves, we shall write the definitions using abelian groups, since it is a simple matter to adjoin the additional structure when the fibers are rings or modules.

Let X be a topological space. A **presheaf** of abelian groups on the **base space** X is a collection $\{\mathcal{O}(U), \rho_{VU}\}$, parametrized by the open subsets U of X and the open subsets V of U, such that each $\mathcal{O}(U)$ is an abelian group, $\mathcal{O}(\varnothing)$ is the 0 group, each $\rho_{VU} : \mathcal{O}(U) \to \mathcal{O}(V)$ is a group homomorphism, each ρ_{UU} is the identity, and $\rho_{WV}\rho_{VU} = \rho_{WU}$ whenever $W \subseteq V \subseteq U$. We are to think of $\mathcal{O}(U)$ as a space of sections of some kind over U and ρ_{VU} as a restriction map carrying sections over U to sections over V. A **sheaf** of abelian groups on the **base space** X is a topological space $\mathcal{O}$ with a mapping $\pi : \mathcal{O} \to X$ such that π is a local homeomorphism onto, $\pi^{-1}(P)$ is an abelian group for each $P \in X$, and the group operations on each $\pi^{-1}(P)$ are continuous in the relative topology from $\mathcal{O}$. We are to think of the elements of a sheaf as germs obtained starting from a presheaf. The individual fibers $\pi^{-1}(P)$ of a sheaf are called **stalks**. One writes $(X, \mathcal{O})$ for the sheaf, sometimes abbreviating the notation to $\mathcal{O}$.

It is possible to construct a presheaf from a sheaf, and vice versa. If we are

given a sheaf $\mathcal{O}$, we define a **section** s of $\mathcal{O}$ over U to be a continuous function $s : U \to \mathcal{O}$ such that $\pi \circ s = 1_U$. If $\mathcal{O}(U)$ denotes the abelian group of sections of $\mathcal{O}$ over U and if ρ_{VU} is the restriction map for sections, then $\{\mathcal{O}(U), \rho_{VU}\}$ is a presheaf. In the reverse direction if we start from a presheaf $\{\mathcal{O}(U), \rho_{VU}\}$ and form the kind of direct limit of abelian groups at each point that is suggested by the passage to germs, then it is possible to topologize the disjoint union of the abelian groups of germs so as to produce a sheaf. Passing from a sheaf to a presheaf and then back to a sheaf reproduces the original sheaf. But passing from a presheaf to a sheaf and then back to a presheaf does not necessarily reproduce the original presheaf. A necessary and sufficient condition on the presheaf $\{\mathcal{O}(U), \rho_{VU}\}$ for $\{\mathcal{O}(U), \rho_{VU}\}$ to result from passing to a sheaf and then back to a presheaf is that the presheaf be **complete** in the sense that both the following conditions hold:

(i) Whenever $\{U_j\}$ is an open covering of an open subset U of X and $f \in \mathcal{O}(U)$ is an element such that $\rho_{U_j,U}(f) = 0$ for all j, then $f = 0$.
(ii) Whenever $\{U_j\}$ is an open covering of an open subset U of X and f_j is given in $\mathcal{O}(U_j)$ for each j in such a way that $\rho_{U_j \cap U_k, U_j}(f_j) = \rho_{U_j \cap U_k, U_k}(f_k)$ for all j and k, then there exists $f \in \mathcal{O}(U)$ such that $\rho_{U_j,U}(f) = f_j$ for all j.

The **structure sheaf** of the spectrum of A is a certain sheaf of rings (Spec A, $\mathcal{O}$) with base space Spec A. Just as in the case of regular (= polynomial) functions on an affine variety, this sheaf will have the property that the ring of global sections is isomorphic to the original ring (cf. Corollary 10.25). We shall describe $\mathcal{O}$ by describing the presheaf. For each prime ideal $\mathfrak{p}$ of A, let $A_\mathfrak{p}$ be the localization of A at $\mathfrak{p}$, i.e., the localization of A relative to the multiplicative system consisting of the set-theoretic complement of $\mathfrak{p}$. This kind of localization is always a local ring. The idea is to define a ring $\mathcal{O}(U)$ of regular functions for each open subset U of Spec A in such a way that the stalk $\mathcal{O}_\mathfrak{p}$ at the point $\mathfrak{p}$ ends up being $A_\mathfrak{p}$ for each $\mathfrak{p}$. With affine varieties we were able to make the definition directly in terms of the function field of the variety, i.e., the field of fractions of A; both $\mathcal{O}(U)$ and the stalk $\mathcal{O}_P(U)$ at each point P ended up being subrings of this function field. The complication for general A is that we do not have a convenient analog of the function field available in which all the localizations are subrings. Thus we proceed by imitating the messier equivalent definition of **regular function** given in Proposition 10.28. Namely, for U open in Spec A, let $\mathcal{O}(U)$ be the set of functions s from U into the product $\prod_{\mathfrak{p} \in U} A_\mathfrak{p}$ such that $s(\mathfrak{p})$ is in the $\mathfrak{p}^{\text{th}}$ factor $A_\mathfrak{p}$ for each $\mathfrak{p}$ and such that s is locally a quotient of members of A in the following sense: for each $\mathfrak{p}$ in U, there is to be an open neighborhood V of $\mathfrak{p}$ within U and there are to be elements a and f in A such that for each $\mathfrak{q}$ in V, the element f is not in $\mathfrak{q}$ and $s(\mathfrak{q})$ equals a/f in $A_\mathfrak{q}$. (Recall that any element of A not in $\mathfrak{q}$ defines an element in the multiplicative system leading to $A_\mathfrak{q}$; f is to be such an element for each $\mathfrak{q}$ in V.) The mappings ρ_{VU} are taken as ordinary restriction mappings, and the result is a presheaf. This presheaf is complete, and the associated sheaf

is the structure sheaf (Spec A, $\mathcal{O}$). An **affine scheme** is any sheaf of rings that is isomorphic in a suitable sense to the structure sheaf of some ring.

3. Scheme. To define "scheme" and the notion that a scheme is defined over some ring or some field, we need to back up and say a few more words about mappings in connection with sheaves. A **ringed space** is a sheaf of rings, (Spec A, $\mathcal{O}$) being an example. Let $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ be two ringed spaces, and let $\{\rho_{V^*U^*}\}$ and $\{\rho'_{VU}\}$ be their respective systems of restriction maps. A **morphism** $(\sigma, \psi) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ **of ringed spaces** consists of a continuous function $\sigma : X \to Y$ and a collection ψ of homomorphisms $\psi_U : \mathcal{O}_Y(U) \to \mathcal{O}_X(\sigma^{-1}(U))$ such that

$$\psi_V \circ \rho_{\sigma^{-1}V, \sigma^{-1}U} = \rho'_{VU} \circ \psi_U$$

whenever U and V are open subsets of Y with $V \subseteq U$. The collection $\psi = \{\psi_U\}$ yields homomorphisms of stalks $\psi_P : \mathcal{O}_{Y,\sigma(P)} \to \mathcal{O}_{X,P}$ for each P in X.

One property of the definition is that if $\varphi : A \to B$ is a homomorphism of rings, then there is an associated morphism $(\sigma, \psi) : (\text{Spec } B, \mathcal{O}_B) \to (\text{Spec } A, \mathcal{O}_A)$ of ringed spaces. The continuous map $\sigma : \text{Spec } B \to \text{Spec } A$ is the map $\sigma = {}^a\varphi$ given by ${}^a\varphi(\mathfrak{p}) = \varphi^{-1}(\mathfrak{p})$ for any prime ideal $\mathfrak{p}$ of B. The mapping ψ on stalks carries $\mathcal{O}_{\text{Spec } A, \sigma(\mathfrak{p})} = \mathcal{O}_{\text{Spec } A, \varphi^{-1}(\mathfrak{p})}$ to $\mathcal{O}_{\text{Spec } B, \mathfrak{p}}$ and is what is induced on the stalk by composition with φ. It is not quite true that every morphism $(\sigma, \psi) : (\text{Spec } B, \mathcal{O}_B) \to (\text{Spec } A, \mathcal{O}_A)$ of ringed spaces arises from a ring homomorphism. The homomorphism (σ, ψ) of ringed spaces resulting from the ring homomorphism φ has the property that ψ carries the maximal ideal $M_{\varphi^{-1}(\mathfrak{p})}$ of the stalk $A_{\varphi^{-1}(\mathfrak{p})}$ into the maximal ideal $M_{\mathfrak{p}}$ of the stalk $B_{\mathfrak{p}}$. A morphism (σ, ψ) of ringed spaces whose stalks are local rings is called a **local morphism** if it has this property. With this definition one can show that every local morphism of ringed spaces $(\sigma, \psi) : (\text{Spec } B, \mathcal{O}_B) \to (\text{Spec } A, \mathcal{O}_A)$ arises from some ring homomorphism $\varphi : A \to B$. This result is to be compared with Corollary 10.40 for affine varieties.

An isomorphism of ringed spaces is automatically local if all the stalks are local rings. The reason is that an isomorphism of one local ring onto another carries the maximal ideal of the first onto the maximal ideal of the second. Thus the earlier definition of **affine scheme** as a ringed space that is isomorphic to some (Spec A, $\mathcal{O}$) concealed only the rather natural definition of isomorphism of ringed spaces, not the more subtle condition "local."

A **morphism of affine schemes** is a local morphism of the affine schemes as ringed spaces. Then the classes of all affine schemes and morphisms of affine schemes together form a category. A **scheme** is a ringed space $(X, \mathcal{O})$ such that each point of X has an open neighborhood for which the restriction of the ringed space to that part of the base is isomorphic to an affine scheme. One can define a natural notion of morphism for schemes, and the classes of all schemes and morphisms of schemes together form a category.

4. Variety as a scheme. Let V be an affine variety over an algebraically closed field, and let $A(V)$ be the affine coordinate ring. We have just seen how Spec $A(V)$ has the natural structure of an affine scheme. Since Spec $A(V)$ includes all prime ideals of $A(V)$, not just the maximal ideals, the continuous inclusion $V \to \text{Spec } A(V)$ is not onto. However, there is a natural relationship between the two, and there is a natural relationship between their rings of regular functions. The reason is that morphisms of affine varieties correspond exactly (in contravariant fashion) to homomorphisms of the affine coordinate rings, which in turn correspond exactly to morphisms of affine schemes. From the point of view of categories, therefore, the categories of affine varieties and affine schemes match perfectly. This description blurs what happens to the underlying algebraically closed field of scalars, and one wants to be able to say that the categories of affine varieties over $\Bbbk$ and affine schemes over $\Bbbk$ match perfectly. Making this statement requires an additional construction, which will be sketched in the next subsection.

This correspondence can be extended suitably from affine varieties to quasiprojective varieties, and the interested reader can find details on page 30 of Volume 2 of Shafarevich's books.

5. Scheme defined over a ring. If A is a ring and $(X, \mathcal{O}_X)$ is a scheme, then a morphism of schemes $(\sigma, \psi) : X \to \text{Spec } A$ defines a homomorphism $A \to \mathcal{O}_X(U)$ of rings for each open subset U of X. Specifically $\psi_{\text{Spec } A}$ carries $\mathcal{O}_{\text{Spec } A}(\text{Spec } A) = A$ into $\mathcal{O}_X(X)$, and hence $\rho_{UX} \circ \psi_{\text{Spec } A}$ carries A into $\mathcal{O}_X(U)$ if $\{\rho_{VU}\}$ is the system of restriction maps for $(X, \mathcal{O}_X)$. The result is that $\mathcal{O}_X$ becomes a sheaf of A algebras.

Conversely if $\mathcal{O}_X$ is a sheaf of A algebras, then one can construct a morphism of schemes $X \to \text{Spec } A$. In this case one says that $(X, \mathcal{O}_X)$ is a **scheme over** A. Every sheaf of abelian groups is a sheaf of $\mathbb{Z}$ algebras, and thus every scheme is a scheme over $\mathbb{Z}$. Schemes over $\mathbb{Z}$ are of special interest in number-theoretic situations, among others. The schemes produced from varieties in the previous subsection are schemes over the underlying field $\Bbbk$. The notion of a scheme over a field that is not algebraically closed is one way of extending the theory of varieties to have it apply when the underlying field is not algebraically closed.

6. Role of homological algebra. The sheaves of abelian groups over a fixed topological space X, with a natural definition of morphism, form a category, and one can define kernels and cokernels in this category. The result turns out to be an abelian category with enough injectives, and the homological algebra of Chapter IV is applicable. If $(X, \mathcal{O})$ is a sheaf over X, then formation of global sections, given by $(X, \mathcal{O}) \mapsto \mathcal{O}(X)$, is a covariant left exact functor. Since there are enough injectives in the category, the derived functors make sense, and the k^{th} derived functor gives what is called the k^{th} **sheaf cohomology** group $H^k(X, \mathcal{O})$ with coefficients in $\mathcal{O}$. This kind of cohomology is easy to use abstractly and hard to use concretely, but it can be shown to be isomorphic to other more concrete kinds of cohomology. In this way the cohomology of sheaves leads to generalizations

of Euler characteristics and Betti numbers that have significance in number theory and geometry.

In applications, there tends to be a ringed space $(X, \mathcal{R})$ (maybe a scheme) in the picture, and the sheaves $(X, \mathcal{O})$ often have the property that each stalk of $\mathcal{O}$ is a module for the corresponding stalk of $\mathcal{R}$. Then the above kind of theory is applicable for sheaves that are $\mathcal{R}$ modules in this sense, not merely sheaves of abelian groups. The interested reader can find details in Chapter III of Hartshorne's book.

BIBLIOGRAPHICAL REMARKS. The topic of schemes assumes knowledge of a certain core of algebraic geometry and commutative algebra, and it builds on more commutative algebra as it goes along. Some books mentioned in the Selected References that include algebraic geometry at the beginning level are those of Hartshorne (Chapter I), Harris, Reid, and Shafarevich (Volume 1). All these books have many geometric examples; this is particularly so for the book by Harris. Some books on commutative algebra are the ones by Atiyah–Macdonald, Eisenbud, Matsumura, and Zariski–Samuel. These lists are by no means exhaustive. There are in fact hundreds of books on the two subjects. To get a list of many of the ones in commutative algebra, one can search in the Library of Congress catalog at `http://catalog.loc.gov`, using the call number QA251.3; a few additional ones are sprinkled in among books with call number QA251. For books on algebraic geometry, one can search using the call number QA564.

The book by Eisenbud–Harris on schemes is an introductory one written in a style that makes it comparatively easy for the reader to get an overview of the subject. Two older books on schemes are the ones by Macdonald and Mumford. Hartshorne's book introduces schemes in Chapter II, and Volume 2 of Shafarevich's books is on that topic. The end of Volume 2 of Shafarevich's books contains a 20-page historical sketch of algebraic geometry, including discussion of some of the precursors of the subject of schemes.

14. Problems

In all problems, $\Bbbk$ is understood to be an algebraically closed field.

1. If P is in $\mathbb{P}^n$, show that the ideal $I(P)$ of members of $\Bbbk[X_0, \ldots, X_n]$ vanishing at all points $(x_0, \ldots, x_n)$ in $\Bbbk^{n+1} - \{0\}$ with $[x_0, \ldots, x_n] = P$ is homogeneous.
2. Let X be a Noetherian topological space.
   (a) Prove that X is compact.
   (b) Prove that every irreducible closed subset of X is connected.
3. (a) Prove that the image of a quasiprojective variety V under a regular function $f : V \to \mathbb{A}^1$ is connected.
   (b) Prove that if V is a projective variety and $\varphi : V \to \mathbb{A}^n$ is a morphism, then $\varphi(V)$ is a one-point set.

4. Let U be the quasi-affine variety $U = \mathbb{A}^2 - \{(0,0)\}$ in $\mathbb{A}^2$. Prove that $\mathcal{O}(U) = \Bbbk[X, Y]$.
5. Deduce from the previous problem, Corollary 10.25, and Theorem 10.38 that U is not isomorphic to an affine variety.
6. Prove that a rational map of an irreducible curve into an irreducible curve is dominant or is constant.
7. Let $\varphi : U \to V$ be a dominant morphism between quasiprojective varieties. Prove that the induced mapping of local rings $\varphi_P^* : \mathcal{O}_{\varphi(P)}(V) \to \mathcal{O}_P(U)$ given in Proposition 10.42 is one-one.
8. Let V be the affine variety $V = V(WX - YZ)$ in $\mathbb{A}^4$, let $A(V)$ be the affine coordinate ring $\Bbbk[W, X, Y, Z]/(WX - YZ)$, let $\overline{X}$ and $\overline{Y}$ be the images of X and Y in $A(V)$, and let $f = \overline{X}/\overline{Y}$ in the field of fractions of $A(V)$. Prove that there exist no members $\bar{a}$ and $\bar{b}$ of $A(V)$ with $f = \bar{a}/\bar{b}$ and $\bar{b}(w, x, y, z) \neq 0$ whenever $wx = yz$ and one or both of w and y are nonzero.
9. Let U and V be quasiprojective varieties, and let $\varphi : U \to V$ be a function. Suppose that U and V are unions of nonempty open subsets $U = \bigcup_{\alpha \in I} U_\alpha$ and $V = \bigcup_{\alpha \in I} V_\alpha$ such that $\varphi(U_\alpha) \subseteq V_\alpha$ for all α. Prove that φ is a morphism if and only if each $\varphi_\alpha : U_\alpha \to V_\alpha$ is a morphism.
10. This problem concerns local extensions of regular functions from quasiprojective varieties to open sets in the ambient affine or projective space.
    (a) Let V be an affine variety in $\mathbb{A}^n$, let U be a nonempty open subset of V, let f be in $\mathcal{O}(U)$, and let P be a point in U. Prove that there exist an open neighborhood U_0 of U about P in V, an open set $\widetilde{U}_0$ in $\mathbb{A}^n$, and a function F in $\mathcal{O}(\widetilde{U}_0)$ such that $U_0 = V \cap \widetilde{U}_0$ and such that F is an extension of $f\big|_{U_0}$.
    (b) Extend the result of (a) to make it valid for any quasiprojective variety V in $\mathbb{P}^n$.
11. Suppose that X and Y are quasiprojective varieties, that U and V are irreducible closed subsets of X and Y, respectively, and that $\varphi : X \to Y$ is a morphism such that $\varphi(U) \subseteq V$. Prove that $\varphi : U \to V$ is a morphism.
12. Prove that
    (a) the mapping $\varphi : \mathbb{P}^{n-1} \to \mathbb{P}^n$ given by $\varphi([x_0, \ldots, x_{n-1}]) = [x_0, \ldots, x_{n-1}, 0]$ is an isomorphism of $\mathbb{P}^{n-1}$ onto the projective hyperplane H_n corresponding to the homogeneous ideal (X_n) of $\Bbbk[X_0, \ldots, X_n]$,
    (b) any projective variety V in $\mathbb{P}^n$ that lies in H_n is isomorphic to a projective variety in $\mathbb{P}^{n-1}$,
    (c) any projective variety V in $\mathbb{P}^n$ is isomorphic to a projective variety V' in some $\mathbb{P}^r$ with $r \leq n$ that is not contained in any projective hyperplane defined by a homogeneous ideal (X_j) of $\Bbbk[X_0, \ldots, X_r]$.

Problems 13–16 relate the classical condition for detecting a singularity in the affine

case to the corresponding condition in the projective case. The key is an identity traditionally known as Euler's Theorem that is proved as Problem 3 at the end of Chapter VIII. In these problems it is assumed that $F_1, \dots, F_r$ are homogeneous polynomials in $\Bbbk[X_0, \dots, X_n]$, that $P = [x_0, \dots, x_n]$ is a point in $\mathbb{P}^n$ in their common locus of zeros, and that P is in the image of $\mathbb{A}^n$ under β_0, i.e., that $x_0 \neq 0$. Define $f_1, \dots, f_r$ in $\Bbbk[X_1, \dots, X_n]$ by $f_i(X_1, \dots, X_n) = F_i(1, X_1, \dots, X_n)$.

13. Define $J(F)(x_0', \dots, x_n')$ to be the r-by-$(n+1)$ matrix whose $(i, j)^{\text{th}}$ entry is $\frac{\partial F_i}{\partial X_j}(x_0', \dots, x_n')$ for $1 \le i \le r$ and $0 \le j \le n$, and define $J(f)(x_1', \dots, x_n')$ to be the r-by-n matrix whose $(i, j)^{\text{th}}$ entry is $\frac{\partial f_i}{\partial X_j}(x_1', \dots, x_n')$ for $1 \le i \le r$ and $1 \le j \le n$. Prove that $\operatorname{rank} J(F)(x_0', \dots, x_n') = \operatorname{rank} J(F)(\lambda x_0', \dots, \lambda x_n')$ for all $\lambda \in \Bbbk^\times$.

14. With notation as in Problem 13, prove that the r-by-n matrix $J(f)(x_1', \dots, x_n')$ equals the r-by-n matrix obtained by deleting the 0^{th} column of the r-by-$(n+1)$ matrix $J(F)(1, x_1', \dots, x_n')$.

15. Using Euler's Theorem (Problem 3 at the end of Chapter VIII), prove concerning the point P on the locus of common zeros of $F_1, \dots, F_r$ that the 0^{th} column of the matrix $J(F)(x_0, \dots, x_n)$ is a linear combination of the other columns of the matrix.

16. Deduce for the point P on the locus of common zeros of $F_1, \dots, F_r$ that
$$\operatorname{rank} J(F)(x_0, x_1, \dots, x_n) = \operatorname{rank} J(f)(x_1/x_0, \dots, x_n/x_0).$$

Problems 17–22 concern products of quasiprojective varieties. The Segre mapping $\sigma : \mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^N$ with $N = mn + m + n$ was defined in Section 8 by $\sigma\big([x_0, \dots, x_m], [y_0, \dots, y_n]\big) = [w_{00}, \dots, w_{mn}]$ with $w_{ij} = x_i y_j$. Let us abbreviate $[w_{00}, \dots, w_{mn}]$ as $[\{w_{ij}\}]$ and $\Bbbk[W_{00}, \dots, W_{mn}]$ as $\Bbbk[\{W_{ij}\}]$.

17. Prove that σ is well defined and one-one.

18. Every member $[\{w_{ij}\}]$ of image σ has $w_{ij}w_{kl} = w_{il}w_{kj}$ for all i, j, k, l. Prove conversely that every member $[\{w_{ij}\}]$ of $\mathbb{P}^N$ with $w_{ij}w_{kl} = w_{il}w_{kj}$ for all i, j, k, l is in image σ, and deduce that image $\sigma = V(\mathfrak{a})$, where $\mathfrak{a}$ is the ideal in $\Bbbk[\{W_{ij}\}]$ generated by all $W_{ij}W_{kl} - W_{il}W_{kj}$.

19. This problem will prove that $\mathfrak{a}$ is a prime ideal, and in particular it will follow that $V(\mathfrak{a})$ is irreducible. Let $\varphi : \Bbbk[\{W_{ij}\}] \to \Bbbk[X_0, \dots, X_m, Y_0, \dots, Y_n]$ be the substitution homomorphism given by setting $W_{ij} = X_i Y_j$. Then $\ker \varphi$ is an ideal containing $\mathfrak{a}$.
    (a) By introducing a suitable monomial ordering in $\Bbbk[\{W_{ij}\}]$, show that any monomial in $\Bbbk[\{W_{ij}\}]$ of total degree d is congruent modulo $\mathfrak{a}$ to a monomial of total degree d of the form $M = \prod_{i,j} W_{ij}^{a_{ij}}$ having the property that $a_{ij} > 0$ implies that $a_{kl} = 0$ for all (k, l) with $l > j$ and $k > i$. Call a monomial of this form **reduced**.

(b) Suppose that $M = \prod_{i,j} W_{ij}^{a_{ij}}$ and $M' = \prod_{i,j} W_{ij}^{b_{ij}}$ are two distinct reduced monomials. By considering the first W_{ij} for which $a_{ij} \neq b_{ij}$, prove that $\varphi(M) \neq \varphi(M')$.

(c) Deduce that $\ker \varphi = \mathfrak{a}$, and show why it follows that $\mathfrak{a}$ is prime.

20. Let $\mathfrak{p}$ be a prime ideal in $\Bbbk[X_0, \ldots, X_m]$, and let $R = \Bbbk[X_0, \ldots, X_m]/\mathfrak{p}$ be the quotient.

(a) Prove that the ideal $\mathfrak{p}\,\Bbbk[Y_0, \ldots, Y_n]$ in $\Bbbk[X_0, \ldots, X_m, Y_0, \ldots, Y_n]$ generated by all products of members of $\mathfrak{p}$ and polynomials in $Y_0, \ldots, Y_n$ is prime.

(b) By following the substitution homomorphism

$$\Bbbk[\{W_{ij}\}] \to \Bbbk[X_0, \ldots, X_m, Y_0, \ldots, Y_n]$$

with a substitution homomorphism $\Bbbk[X_0, \ldots, X_m, Y_0, \ldots, Y_n] \to R[Z]$, prove that whenever U is a projective variety in $\mathbb{P}^m$ and P is a point in $\mathbb{P}^n$, then $\sigma(U \times \{P\})$ is a projective variety in $\mathbb{P}^N$.

21. Let U and V be projective varieties in $\mathbb{P}^m$ and $\mathbb{P}^n$, respectively. Problem 20 shows that $\sigma(U \times \{v\})$ is a projective variety in $\mathbb{P}^N$ for each $v \in V$. Suppose that $\sigma(U \times V)$ is a union $E_1 \cup E_2$ of two closed sets in $\mathbb{P}^N$.

(a) For i equal to 1 or 2, define $V_i = \{v \in V \mid \sigma(U \times \{v\}) \nsubseteq E_i\}$. Why is $V_1 \cap V_2 = \varnothing$?

(b) Prove that V_1 and V_2 are open by using bihomogeneous polynomials to exhibit each of V_1 and V_2 as a neighborhood of each of its points.

(c) Deduce from (b) that $\sigma(U \times V)$ is a projective variety in $\mathbb{P}^N$.

(d) Show how to deduce from (c) that if U and V are quasiprojective varieties in $\mathbb{P}^m$ and $\mathbb{P}^n$, respectively, then $\sigma(U \times V)$ is a quasiprojective variety in $\mathbb{P}^N$.

22. (a) Prove that if U and V are quasiprojective varieties, then the projections of $U \times V$ to U and V are morphisms. Here the projection of $U \times V$ to U is understood to be the map $\sigma(u, v) \mapsto u$ of $\sigma(U \times V)$ into U, and similarly for the projection to V.

(b) If $\varphi : U \to X$ and $\psi : U \to Y$ are morphisms, prove that $(\varphi, \psi) : U \to X \times Y$ when defined by $(\varphi, \psi)(u) = (\varphi(u), \psi(u))$ is a morphism.

(c) If $\varphi : U \to X$ and $\psi : V \to Y$ are morphisms, prove that $\varphi \times \psi : U \times V \to X \times Y$ when defined by $(\varphi \times \psi)(u, v) = (\varphi(u), \psi(v))$ is a morphism.

Problems 23–25 make some observations about prime ideals and irreducible polynomials.

23. Let $I = (f_1, \ldots, f_r)$ be an ideal in $\Bbbk[X, Y]$ such that the zero locus $V(I)$ is irreducible and such that $f_1, \ldots, f_r$ are irreducible polynomials.

(a) Prove that I is prime if $\dim V(I) = 1$.

(b) Give an example to show that I need not be prime if $\dim V(I) = 0$.

24. Fix a monomial ordering for $\Bbbk[X_1, \ldots, X_n]$, and let I be a nonzero ideal in $\Bbbk[X_1, \ldots, X_n]$. Prove that if I is prime, then the members of any minimal Gröbner basis of I are irreducible polynomials.

25. Suppose that $\mathrm{char}(\Bbbk) \neq 2$. Within $\Bbbk[X, Y, Z]$, let E be the homogeneous subspace $\Bbbk[X, Y, Z]_2$. The six monomials in E form a $\Bbbk$ basis of E and may be used to identify E with $\Bbbk^6$. Under this identification prove that the subset of reducible polynomials in E, including the 0 polynomial, is an affine hypersurface of $\Bbbk^6$.

Problems 26–35 concern elliptic curves. An **elliptic curve** over $\Bbbk$ is a pair (E, O) consisting of a nonsingular irreducible projective curve E of genus 1 and a distinguished point O. These problems use the Riemann–Roch Theorem and its associated notation in Chapter IX in order to exhibit a concrete realization of such a curve in $\mathbb{P}^2$ with O on the line at infinity and with all other points of E in $\mathbb{A}^2$. Such a curve has a remarkable structure; for further information, including further applications of the Riemann–Roch Theorem to these curves, see the book by Silverman. Corollary 10.56 identifies the points of E with the discrete valuations of the function field $\Bbbk(E)$ over E. Let v_O be the discrete valuation corresponding to O.

26. For $n > 0$, prove that $\ell(nv_O) = n$. Use this result to find members x and y of $\Bbbk(E)$ whose divisors satisfy $(x)_\infty = 2v_O$ and $(y)_\infty = 3v_O$.

27. Prove that $[\Bbbk(E) : \Bbbk(x)] = 2$ and $[\Bbbk(E) : \Bbbk(y)] = 3$.

28. Why does it follow from the previous problem that $\Bbbk(E) = \Bbbk(x, y)$?

29. From the fact that $\ell(6v_O) = 6$, deduce a nontrivial linear dependence over $\Bbbk$ among the members $1, x, y, x^2, xy, y^2, x^3$ of $\Bbbk(E)$. Show that the coefficients of y^2 and x^3 are necessarily nonzero, and then scale x and y appropriately to show that the image of the function $\varphi : E - \{0\} \to \mathbb{P}^2$ defined by $\varphi(P) = [x(P), y(P), 1]$ is contained in the projective closure C of the zero locus of the polynomial $f(X, Y) = (Y^2 + a_1XY + a_3Y) - (X^3 + a_2X^2 + a_4X + a_6)$.

30. Prove that $f(X, Y)$ is irreducible and that C is therefore a projective curve.

31. Why is $\varphi : E - \{0\} \to C$ a morphism? Why does it follow that φ extends to a morphism $\Phi : E \to C$?

32. Deduce from Problem 28 that Φ is birational.

33. Show that C is nonsingular at its point at infinity.

34. Show that if C is singular at (x_0, y_0) in $\mathbb{A}^2$, then the member of $\Bbbk(E)$ given by $z = (y - y_0)(x - x_0)^{-1}$ has $v_O(z) = -1$ and $v_P(z) \geq 0$ for all P in $E - \{O\}$.

35. Deduce from Problems 33 and 34 that C is nonsingular, and explain why it follows that $\Phi : E \to Z$ is an isomorphism.