

Advanced Algebra

Final Version, September, 2007
For Publication by Birkhäuser Boston
Along with a Companion Volume *Basic Algebra*
In the Series

Cornerstones

Selected Pages from Chapter X: pp. 558–559, 604–618

Anthony W. Knapp

Copyright © 2007 by Anthony W. Knapp
All Rights Reserved

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, \mathbb{k} denotes a fixed algebraically closed field.

Sections 1–6 establish the definitions and elementary properties of varieties, maps between varieties, and dimension, all over \mathbb{k} . 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 \mathbb{k} . 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 \mathbb{k} 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 \mathbb{k} .

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

$$\mathbb{A}^n = \{(x_1, \dots, x_n) \in \mathbb{k}^n\}$$

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 :

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

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

¹The 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.

Pages 560–603 do not appear in this file.

8. Classification Questions about Irreducible Curves

Sections 1–7 give the fundamentals concerning (quasiprojective) varieties over the algebraically closed field \mathbb{k} . 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 \mathbb{k} 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 \mathbb{k} 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 \mathbb{k} . 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

¹⁶The 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.

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

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 xxiii) 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. \square

Corollary 10.51. Let C be an irreducible quasiprojective curve over \mathbb{k} , and let $\mathbb{k}(C)$ 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 $\mathbb{k}(C)$ defined over \mathbb{k} ,
- (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 $\dim_{\mathbb{k}} M_P/M_P^2 = 1$. 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 \mathbb{k}^\times . \square

Corollary 10.52. If C is an irreducible affine curve over \mathbb{k} 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 $\mathbb{k}(C)$ 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. \square

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 \mathbb{k} . If C is any irreducible quasiprojective curve with $\mathbb{k}(C) = \mathbb{K}$, then Corollary 10.51 associates a discrete valuation of \mathbb{K} over \mathbb{k} 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 \mathbb{k} .

Theorem 10.53. Let C be an irreducible projective curve with function field $\mathbb{k}(C)$ equal to \mathbb{K} , and let v be a discrete valuation of \mathbb{K} defined over \mathbb{k} . 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 $\mathbb{k}(C)$ 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 $0 = v(h(Q)) \geq \min(v(h(Q) - h), v(h)) \geq 1$, contradiction. \square

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 $\{[x_0, \dots, x_n] \mid x_j = 0\}$

with $0 \leq j \leq n$. That being so, we may assume that C is a projective variety in \mathbb{P}^n and that $C \cap \beta_j(\mathbb{A}^n) \neq \emptyset$ for $0 \leq j \leq n$, where $\beta_j : \mathbb{A}^n \rightarrow \mathbb{P}^n$ is the embedding defined after Proposition 10.18. Let $\tilde{A}(C) = \mathbb{k}[X_0, \dots, X_n]/I(C)$ be the homogeneous coordinate ring of C , and for each j , let x_j be the image of X_j in $\tilde{A}(C)$. Since $I(C)$ does not contain X_j , x_j is not the 0 element of $\tilde{A}(C)$. 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 $\mathbb{k}(C)$.

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 $v(x_i/x_0) = v(x_{i_0}/x_0) + v(x_i/x_{i_0}) = N - v(x_{i_0}/x_i) \geq 0$ for all i . Consequently each function x_i/x_0 lies in the subring R_v of $\mathbb{k}(C)$.

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 $I(C_0) = \beta_0'(I(C))$. Consequently the substitution homomorphism $\beta_0' : \mathbb{k}[X_0, \dots, X_n] \rightarrow \mathbb{k}[X_1, \dots, X_n]$ descends to a homomorphism of $\tilde{A}(C) = \mathbb{k}[X_0, \dots, X_n]/I(C)$ onto $A(C_0) = \mathbb{k}[X_1, \dots, X_n]/I(C_0)$ that carries x_0 in $\tilde{A}(C)$ to 1 and carries the members x_1, \dots, x_n of $\tilde{A}(C)$ to the generators of $A(C_0)$. The members x_i/x_0 of $\mathbb{k}(C)$ 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 $\mathbb{k}[X_1, \dots, X_n] \rightarrow A(C_0)$ to a prime ideal $\tilde{\mathfrak{q}}$ containing $I(C_0)$. Then $V(\tilde{\mathfrak{q}})$ is an affine subvariety of C_0 . Since $\dim C_0 = 1$, there are only two possibilities. One is that $\dim V(\tilde{\mathfrak{q}}) = 1$, in which case $V(\tilde{\mathfrak{q}}) = C_0$, $\tilde{\mathfrak{q}} = I(C_0)$, and $\mathfrak{q} = 0$. The other is that $\dim V(\tilde{\mathfrak{q}}) = 0$, in which case $V(\tilde{\mathfrak{q}}) = \{P\}$ 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 $\mathbb{k}(C)^\times$, contradiction. Thus we are in the second case. Then $\tilde{\mathfrak{q}}$ is maximal in $\mathbb{k}[X_1, \dots, X_n]$, \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 $A(C_0)/\mathfrak{q} \cong \mathbb{k}$. 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 $\mathfrak{q} + \mathbb{k}1 = A(C_0)$ would be in \mathfrak{p}_v , contradiction. Thus $v(s) = 0$ for all $s \in S$, and $M_P = S^{-1}\mathfrak{m}_P \subseteq \mathfrak{p}_v$. \square

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 $\tilde{\varphi} : \mathbb{k}(C) \rightarrow \mathbb{k}(C')$ be the associated field map of function fields.

Since $\mathbb{k}(C)$ and $\mathbb{k}(C')$ both have transcendence degree 1 over \mathbb{k} and since $\mathbb{k}(C)$ is finitely generated as a field over \mathbb{k} , the field $\mathbb{k}(C')$ is a finite algebraic extension of the field $\tilde{\varphi}(\mathbb{k}(C))$. If v is any discrete valuation of $\mathbb{k}(C')$, then it follows from the finiteness of this extension that v cannot be identically 0 on $\tilde{\varphi}(\mathbb{k}(C))^\times$; 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 $\mathbb{k}(C')$ in terms of a vector-space basis $\{x_1, \dots, x_m\}$ of $\mathbb{k}(C')$ over $\tilde{\varphi}(\mathbb{k}(C))$ 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 $\mathbb{k}(C')$ over \mathbb{k} . 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 $\tilde{\varphi}(\mathbb{k}(C))^\times$ is not identically 0, the restriction comes from some positive multiple e of a discrete valuation on $\tilde{\varphi}(\mathbb{k}(C))$. Let v_0 be the corresponding discrete valuation of $\mathbb{k}(C)$; this is given by $v_0(f) = e^{-1}v(\tilde{\varphi}(f))$. Let R_0 be its valuation ring and \mathfrak{p}_0 be its valuation ideal in $\mathbb{k}(C)$; the latter is given by $\mathfrak{p}_0 = \tilde{\varphi}^{-1}(\mathfrak{p}_v)$. 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, $M_Q \subseteq \mathfrak{p}_0 = \tilde{\varphi}^{-1}(\mathfrak{p}_v)$. Application of $\tilde{\varphi}$ gives $\tilde{\varphi}(M_Q) \subseteq \tilde{\varphi}\tilde{\varphi}^{-1}(\mathfrak{p}_v) \subseteq \mathfrak{p}_v = M_P$. Theorem 10.45 shows that consequently P is in the largest domain on which φ is a morphism and that $\varphi(P) = Q$. \square

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. \square

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

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

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 $\mathbb{K} = \mathbb{k}(C)$, 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 \mathbb{k} 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 \mathbb{k} 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 \mathbb{k} . 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 $R = k[x_1, \dots, x_n]$ 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 $\mathbb{K} = \mathbb{k}(C)$, 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 \mathbb{k} 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 \mathbb{k} 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 $A(C) = \mathfrak{m}_P + \mathbb{k}1$. In other words, \mathfrak{m}_P and any element of S together generate $A(C)$ as a \mathbb{k} 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 $\mathfrak{m}_P + \mathbb{k}s$ 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 $M_P = S^{-1}\mathfrak{m}_P \subseteq \mathfrak{p}_v$. \square

Corollary 10.59. If \mathbb{K} is a function field in one variable over \mathbb{k} and if v is a discrete valuation of \mathbb{K} defined over \mathbb{k} with valuation ring R_v , then there exists an irreducible nonsingular *affine* curve C over \mathbb{k} 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 $R = \mathbb{k}[x]$. Since $v(x) \neq 0$, x is transcendental over \mathbb{k} , and \mathbb{K} is a finite algebraic extension of the field of fractions $\mathbb{k}(x)$ 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 $T = \mathbb{k}[x_1, \dots, x_n]$ with $x_1 = x$. The substitution homomorphism with $X_j \mapsto x_j$ for all j carries $\mathbb{k}[X_1, \dots, X_n]$ 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 \mathbb{k} , 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 $R = \mathbb{k}[x]$, 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 \mathbb{k} 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 $\mathcal{O}_P(C) = R_v$. \square

Corollary 10.60. Let C be the irreducible nonsingular affine curve constructed in Corollary 10.59 and having function field $\mathbb{K} = \mathbb{k}(C)$, 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 \mathbb{k} 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 \mathbb{k} such that $v'(x) \geq 0$. This inequality implies that v' is ≥ 0 on $\mathbb{k}[x]$, 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 \mathbb{k} 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. \square

Let us prove Theorem 10.57, but only under the assumption that k is algebraically closed. 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. \square

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 $0 \leq d \leq n$, 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 $k[X_1, \dots, X_n] \rightarrow k[x_1, \dots, x_n]$. 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 $1 \leq j \leq n-1$. The equation $f(x_1, \dots, x_n) = 0$ becomes

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

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

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

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 $n-1 \geq 1$, d being an integer with $0 \leq d \leq n-1$. 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 $1 \leq j \leq n$. If $I \neq 0$, fix $f \neq 0$ 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 $0 \leq d \leq n-1$ 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 $\deg g \leq r-1$ (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 $h_r(c_1, \dots, c_{n-1}, 1) \neq 0$. 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 $I \neq 0$, 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

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

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

$$f_n(x_1, \dots, x_{n-1}, x_n) + c_1 f_1(x_1, \dots, x_{n-1}, x_n) + \dots + c_{n-1} f_{n-1}(x_1, \dots, x_{n-1}, x_n) \neq 0. \quad (\dagger\dagger)$$

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. \square

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 $\{z_1, \dots, z_r\}$ of L over K consisting of elements integral over R ; this is possible by Proposition 8.42 of *Basic Algebra*. Put $S = R[z_1, \dots, z_r]$. 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 $R = k[x_1, \dots, x_n]$ 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, \dots, y_d of x_1, \dots, x_n over k such that the subring $S = k[y_1, \dots, y_d]$ of R is a full polynomial ring, every element of R is integral over S , and K is a separable extension of the field $k(y_1, \dots, y_d)$. 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. \square

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 \mathbb{k} , take any discrete valuation v of \mathbb{K} defined over \mathbb{k} (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 \mathbb{k} . 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 \mathbb{k} 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, \dots, 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 \mathbb{k} . 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 $\overline{C}_1, \dots, \overline{C}_n$ be the respective projective closures of C_1, \dots, 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 $\gamma_j : \mathbb{V}_{\mathbb{K}} \rightarrow \overline{C}_j$, 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, \dots, C_m was arranged in such a way that

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

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 $\varphi_{j,P}^* : \mathcal{O}_{\varphi_j(P)}(\overline{C}_1) \rightarrow \mathcal{O}_P(C_j)$ for $P \in U_j$. By assumption, the isomorphism $\tilde{\varphi}_j : \mathbb{k}(C_1) \rightarrow \mathbb{k}(C_j)$ is normalized to be the identity. Since $\tilde{\varphi}_j$ is the field mapping corresponding to the birational map φ_j , $\tilde{\varphi}_j$ 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

$$\varphi_j \circ \gamma_j : \mathbb{V}_{\mathbb{K}} - F \rightarrow U_1 \quad \text{is independent of } j,$$

and $\varphi_j : U_j \rightarrow U_1$ 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 $1 \leq j \leq m$, let $\pi_j : W \rightarrow \overline{C}_j$ 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”

$$\Delta = \{ \delta(P) = (P, \varphi_2^{-1}(P), \dots, \varphi_m^{-1}(P)) \mid P \in U_1 \}$$

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 $\pi_j : C \rightarrow \overline{C}_j$ 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, $\pi_j : C \rightarrow \overline{C}_j$ 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 $\pi_j : C \rightarrow \overline{C}_j$ 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 $1 \leq j \leq m$ 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. \square

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 $m \geq 1$ and $n \geq 1$ 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 $0 \leq i \leq m$ and $0 \leq j \leq n$. Then

$$\mathbb{P}^m = \{[x_0, \dots, x_m]\}, \quad \mathbb{P}^n = \{[y_0, \dots, y_n]\},$$

and

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

The **Segre embedding** is the function

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

i.e., $w_{ij} = x_iy_j$. Define $\mathfrak{a} \subseteq \mathbb{k}[W_{00}, \dots, W_{mn}]$ 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 $X = (X_0, \dots, X_m)$. If $\alpha = (\alpha_0, \dots, \alpha_m)$ is an $(m+1)$ -tuple of nonnegative integers, we define $|\alpha| = \alpha_0 + \dots + \alpha_m$ and $X^\alpha = X_0^{\alpha_0} \dots X_m^{\alpha_m}$. We define $Y, \beta, |\beta|$, 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 $F_1(X), \dots, F_r(X)$ of various degrees d_1, \dots, 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 $X_0^{d-d_j} F_j(X), \dots, X_m^{d-d_j} F_j(X)$. The assertion about describing S follows.

Now let $U \subseteq \mathbb{P}^m$ be the locus of common zeros of homogeneous polynomials $F_1(X), \dots, F_r(X)$ all of degree d , and let $V \subseteq \mathbb{P}^n$ be the locus of common zeros of homogeneous polynomials $G_1(Y), \dots, G_r(Y)$ 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 $d \leq e$. Replace

¹⁸If we form the $(m+1)$ -by- $(n+1)$ matrix whose (i, j) 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 $\varphi_1 : U \rightarrow \mathbb{P}^m$ and $\varphi_2 : U \rightarrow \mathbb{P}^n$ 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,

¹⁹The 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.