Introduction to Algebraic Geometry

(Notes on lectures based on Fulton's book)

Ronnie Sebastian

May 5, 2026

These are the notes I used for my course in Spring 2026. They are essentially a copy of Fulton's really nice book on algebraic curves, except that at few places I have added some more details. The solutions to exercises were submitted by students taking this course. If you find any mistakes, or have any comments, questions or suggestions, please write to me at ronnie@iitb.ac.in.

Throughout these notes, we assume that the characteristic of the underlying field k is zero. In fact, it is safe, and also recommended, to simply assume that $k = \mathbb{C}$.

Ronnie Sebastian

Contents

1 Affine Algebraic Sets **1**

1.1 Algebraic Preliminaries 1
1.2 Affine Space and Algebraic Sets 4
1.3 Ideal of a Subset of $\mathbb{A}^n(k)$ 4
1.4 Hilbert Basis Theorem 5
1.5 Irreducible Components of an Algebraic Set 6
1.6 Algebraic Subsets of the Plane $\mathbb{A}^2(k)$ 7
1.7 Modules; Finiteness conditions 9
1.8 Integral Elements 9
1.9 Finiteness of Field Extensions 10
1.10 Hilbert's Nullstellensatz 11
1.11 Exercises 12

2 Affine Varieties **37**

2.1 Coordinate Ring of a Variety 37
2.2 Polynomial Functions and Maps 38
2.3 Coordinate Change 40
2.4 Rational Functions and Local Rings 41
2.5 Discrete Valuation Rings 43
2.6 Homogenization and Dehomogenization 44
2.7 Operations with Ideals 45
2.8 Ideals with a Finite Number of Zeros 45
2.9 Modules; Exact Sequences 47
2.10 Exercises 47

3 Local Properties of Plane Curves **95**

3.1 Multiplicities and Tangent Lines 95
3.2 Multiplicities and Local Rings 96

3.3 Intersection Numbers . . . 98
3.4 Exercises . . . 104

4 Projective Varieties **117**
4.1 Projective n-space . . . 117
4.2 Projective Algebraic Sets . . . 118
4.3 Affine and Projective Varieties . . . 121
4.4 Exercises . . . 124

5 Projective Plane Curves **135**
5.1 Intersection Multiplicity in $\mathbb{P}^2$ . . . 135
5.2 Linear System of Curves . . . 136
5.3 Multiple Points . . . 143
5.4 Max Noether's Fundamental Theorem . . . 144
5.5 Applications of Noether's Theorem . . . 146
5.6 Exercises . . . 148

6 Varieties, morphisms and rational maps **177**
6.1 Zariski Topology . . . 177
6.2 Quasi-projective varieties . . . 178
6.3 Morphisms of Varieties . . . 179
6.4 Products and Graphs . . . 185
6.5 Algebraic Function Fields and Dimension of Varieties . . . 194
6.6 Rational Maps . . . 196

Chapter 1

Affine Algebraic Sets

1.1 Algebraic Preliminaries

Definition 1.1.1 (Ring)**.** *By a* ***Ring****, we mean a commutative ring with* $1 \neq 0$*. By a homomorphism of rings, we mean a ring homomorphism that sends* 1 *to* 1*.*

In this context, a typical example is the polynomial ring in n variables, denoted $\mathbb{C}[X_1, \ldots, X_n]$. Other rings can be formed from this, for example, by taking the quotient modulo a proper ideal or by localization (see Chapter 3 in Atiyah and MacDonald for the definition and properties of localization). We may also replace the field $\mathbb{C}$ by another field or any other commutative ring with 1.

Definition 1.1.2 (Integral Domain)**.** *An* ***Integral Domain*** *(or simply Domain) is a ring where there are no zero divisors. That is,*

$$xy = 0 \implies x = 0 \quad or \quad y = 0.$$

Definition 1.1.3 (Polynomial Ring)**.** *Let R be a ring. The* ***polynomial ring*** *in n variables is the ring $R[X_1, \ldots, X_n]$. Let $\underline{i} = (i_1, \ldots, i_n)$ be a "multi-index" where each $i_j \geqslant 0$. Then any $F \in R[X_1, \ldots, X_n]$ has a unique expression:*

$$F = \sum_{\underline{i}} c_{(\underline{i})} x^{(\underline{i})}$$

where $x^{(\underline{i})} = x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$. An element of the form $x_1^{i_1} \ldots x_n^{i_n}$ is called a ***monomial****.*

Definition 1.1.4 (Homogeneous Polynomials)**.** *The* ***degree*** *of a monomial is $|\underline{i}| = i_1 + i_2 + \ldots + i_n$. A polynomial F is called* ***homogeneous*** *of degree d if $c_{(\underline{i})} = 0$ unless $|\underline{i}| = d$. Homogeneous polynomials will also be called* ***forms****.*

Given any polynomial F, clearly we may write it as the sum of its homogeneous components:

$$F = F_0 + F_1 + F_2 + \ldots + F_d$$

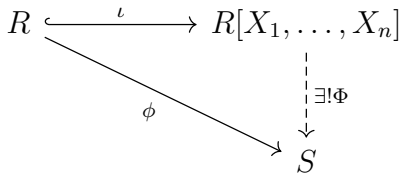
where F_i are homogeneous polynomials of degree i and $F_d \neq 0$. We say $\deg(F) = d$.

Lemma 1.1.5. *If R is a domain, then for the product of two polynomials F and G in $R[X_1, \ldots, X_n]$:*

$$\deg(FG) = \deg(F) + \deg(G).$$

Proposition 1.1.6 (Universal Property of Polynomial Rings)**.** *Let S be a ring and let $\phi : R \to S$ be a ring homomorphism. Given n elements $s_1, \ldots, s_n \in S$, there is a **unique** extension of ϕ, denoted $\tilde{\phi} : R[X_1, \ldots, X_n] \to S$, such that:*

1. *$\tilde{\phi}$ agrees with ϕ on R.*
2. *$\tilde{\phi}(x_i) = s_i$ for all $i = 1, \ldots, n$.*



Definition 1.1.7 (Prime Ideal)**.** *An ideal $I \subsetneq R$ is called **prime** if $I \neq R$ and if $xy \in I \implies x \in I$ or $y \in I$. Equivalently, I is prime if R/I is a domain. An element a is called prime if (a) is a prime ideal.*

Definition 1.1.8 (Irreducible Element)**.** *An element $a \in R$ is called **irreducible** if:*

1. *$a \neq 0$ and a is not a unit.*
2. *If $a = bc$ for $b, c \in R$, then either b or c is a unit.*

Lemma 1.1.9. *Let R be a domain. A prime element is always irreducible.*

Proof. Left as an exercise. □

Definition 1.1.10 (Unique Factorization Domain)**.** *We say R is a **Unique Factorization Domain (UFD)** if every irreducible element is prime. In a UFD, every non-zero, non-unit element has a unique factorization into a product of primes.*

Theorem 1.1.11 (Gauss's Lemma)**.** *If R is a UFD, then the polynomial ring $R[X]$ is also a UFD. Furthermore, if $F \in R[X]$ is irreducible in $R[X]$, then F is also irreducible in $K[X]$, where K is the quotient field of R.*

Corollary 1.1.12. *The ring $k[X_1, \ldots, X_n]$ is a UFD for any field k.*

Throughout these notes, standard notions such as the Kernel of a ring homomorphism, ideals generated by a subset $S \subset R$, finitely generated ideals, the characteristic of a ring, and algebraically closed fields are assumed.

Proposition 1.1.13 (Roots and Expansion)**.** *Let $F \in R[X]$ and let $a \in R$ be such that $F(a) = 0$. By writing $X = X - a + a$ and using binomial expansion, we obtain:*

$$F(X) = (X - a)G(x) + F(a) = (X - a)G(X).$$

Consequently, if a is a root of $F(X)$ then $(X - a)$ divides $F(X)$.

Definition 1.1.14 (Formal Derivative)**.** *If $F \in R[X]$ given by $F = \sum_{i=0}^{d} a_i X^i$, the derivative F_X is defined as:*

$$F_X = \sum_{i=1}^{d} i a_i X^{i-1}.$$

For multivariable polynomials, F_{X_i} is defined by treating F as a polynomial in X_i with coefficients in the other variables.

Considering coefficients in $R[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$, let F_X denote the partial derivative of F with respect to X (formally defined). We have the following identities:

1. **Linearity:** $(aF + bG)_X = aF_X + bG_X$ for constants a, b.
2. **Constant Rule:** $F_X = 0 \iff F$ is a constant (independent of X).
3. **Product Rule:** $(FG)_X = F_X G + F G_X$ and $(F^n)_X = n F^{n-1} F_X$.
4. **Chain Rule:** If $F \in R[X_1, \ldots, X_n]$ and $G_1, \ldots, G_n \in R[X]$, then for the composite polynomial:
$$\frac{\partial}{\partial X} F(G_1, \ldots, G_n) = \sum_{i=1}^{n} F_{X_i}(G_1, \ldots, G_n) \cdot (G_i)_X$$
5. **Commutativity:** $(F_{X_i})_{X_j} = (F_{X_j})_{X_i}$.

Theorem 1.1.15 (Euler's Theorem on Homogeneous Functions)**.** *If F is a form (homogeneous polynomial) of degree m, then:*

$$mF = \sum_{i=1}^{n} X_i F_{X_i}$$

1.2 Affine Space and Algebraic Sets

Definition 1.2.1 (Affine Space)**.** *Let k be a field. We define affine n-space over k as:*

$$\mathbb{A}^n(k) = \{(a_1, \ldots, a_n) \mid a_i \in k\}.$$

Let $P \in \mathbb{A}^n(k)$ and let $F \in k[X_1, \ldots, X_n]$. Then we may evaluate F at P. If $F(P) = 0$, we say that P is a zero of F. The set of zeros of F is denoted $V(F) \subset \mathbb{A}^n(k)$.

If F is not a constant, then $V(F)$ is called a **hypersurface**. If F has degree 1, then $V(F)$ is called a **hyperplane**.

Let $S \subset k[X_1, \ldots, X_n]$ be any set of polynomials. We let

$$V(S) := \{P \in \mathbb{A}^n(k) \mid F(P) = 0 \text{ for all } F \in S\} = \bigcap_{F \in S} V(F). \tag{1.2.2}$$

Definition 1.2.3 (Affine Algebraic Set)**.** *A subset $X \subset \mathbb{A}^n(k)$ is called an **affine algebraic set** if $X = V(S)$ for some S.*

Proposition 1.2.4 (Properties of Algebraic Sets)**.** *Let I and J be ideals. The following properties hold:*

1. *If I is the ideal generated by S, then $V(S) = V(I)$.*
2. *If $\{I_\alpha\}$ is a collection of ideals, then $V(\bigcup_\alpha I_\alpha) = \bigcap_\alpha V(I_\alpha)$.*
3. *If $I \subset J$, then $V(I) \supset V(J)$.*
4. *$V(FG) = V(F) \cup V(G)$; furthermore $V(I) \cup V(J) = V(\{FG \mid F \in I \text{ and } G \in J\})$.*
5. *$V(0) = \mathbb{A}^n(k)$; $\quad V(1) = \emptyset$; $\quad V((X_1 - a_1, \ldots, X_n - a_n)) = \{(a_1, \ldots, a_n)\}$.*

All the assertions are easy and left to the reader. To see the second assertion of (4), assume that $P \notin V(I)$ and show that $P \in V(J)$.

1.3 Ideal of a Subset of $\mathbb{A}^n(k)$

Let $X \subset \mathbb{A}^n(k)$ be a subset. We define the ideal of X as:

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

Proposition 1.3.1 (Properties of the Ideal operator)**.** *We have the following properties:*

6. *If $X \subset Y$ then $I(X) \supset I(Y)$.*

7. *$I(\emptyset) = k[X_1, \ldots, X_n]$; $I(\mathbb{A}^n(k)) = 0$ (if k is infinite).*
   If $P = (a_1, \ldots, a_n)$, then $I(\{P\}) = (X_1 - a_1, \ldots, X_n - a_n)$.

8. *$I(V(S)) \supset S$ and $V(I(X)) \supset X$.*

9. *$V(I(V(S))) = V(S)$ and $I(V(I(X))) = I(X)$.*

Proof of 7. If $F \in I(\{(a_1, \ldots, a_n)\})$, then write $F = F(P) + G$, where $G \in (X_1 - a_1, \ldots, X_n - a_n)$. One checks that $(X_1 - a_1, \ldots, X_n - a_n) \subset I(\{(a_1, \ldots, a_n)\})$, and since $I(\{(a_1, \ldots, a_n)\}) \neq (1)$ and $(X_1 - a_1, \ldots, X_n - a_n)$ is maximal, equality follows. □

Proof of 9. Let S be a set of polynomials. We want to show that $V(I(V(S))) = V(S)$. It is clear that $I(V(S)) \supset S$ (from property 8), and so $V(I(V(S))) \subset V(S)$ (from property 3). Conversely, put $X = V(S)$ in property (8). This shows that $V(I(V(S))) = V(S)$. The proof of $I(V(I(X))) = I(X)$ is similar and left to the reader. □

Definition 1.3.2 (Radical Ideal)**.** *Let $J \subset k[X_1, \ldots, X_n]$ be an ideal. We define the **radical** of J to be:*

$$Rad(J) = \{F \in k[X_1, \ldots, X_n] \mid F^n \in J \text{ for some } n \geqslant 1\}.$$

*An ideal J is called a **radical ideal** if $J = Rad(J)$.*

Corollary 1.3.3. *Let $X \subset \mathbb{A}^n(k)$ be a subset. Then $I(X)$ is a radical ideal.*

Proof. This is clear as if $F^n \in I(X)$, then it follows that for $p \in X$ we have $F(p)^n = 0$ and so $F(p) = 0$, that is, $F \in I(X)$. □

1.4 Hilbert Basis Theorem

Theorem 1.4.1. *Every algebraic set is the intersection of finitely many hypersurfaces.*

Since every algebraic set is of the type $V(I)$ for some ideal I, using (1.2.2) and Proposition 1.2.4 (1), It suffices to show that every ideal is finitely generated.

Definition 1.4.2 (Noetherian Ring)**.** *Let R be a ring. If every ideal in R is finitely generated, then we say R is **Noetherian**.*

Theorem 1.4.3 (Hilbert's Basis Theorem)**.** *Let R be Noetherian. Then $R[X]$ is Noetherian.*

Proof. Let $I \subset R[X]$ be an ideal. If $F \in R[X]$ and $F = a_0 + \ldots + a_d X^d$, then we let $\text{lead}(F) = a_d$. It is easily checked that the set

$$J = \{\text{lead}(F) \mid F \in I\} \subset R$$

is an ideal of R. Since R is Noetherian, J is finitely generated. Let $F_1, \ldots, F_r$ be such that $\text{lead}(F_i)$ generate J.

Let $N = \max\{\deg(F_i)\}$. For each $m \leqslant N$, let J_m be the ideal generated by $\text{lead}(F)$ for $F \in I$ and $\deg(F) \leqslant m$. Each J_m is finitely generated and so there are $F_{mj} \in I$, $\deg(F_{mj}) \leqslant m$ such that $\text{lead}(F_{mj})$ generate J_m.

Let $I' \subset R[X]$ be the ideal generated by F_i and F_{mj}. As each of these is in I, it is clear $I' \subset I$. We claim that $I' = I$.

If not, let $G \in I$ be of the smallest possible degree such that $G \notin I'$. Let $G = a_0 + \ldots + a_d X^d$. If $d \geqslant N$, then we can find an expression of the type $\sum b_i X^{d-\deg(F_i)} F_i$ whose leading coefficient is a_d. Thus, $G - \sum b_i x^{d-\deg(F_i)} F_i$ has degree $< \deg(G)$ and is in I and so in I'. But this forces that $G \in I'$, a contradiction.

Thus, we may assume that $d < N$. Then $a_d \in J_d$ and again we may consider a combination involving F_{dj}'s. Again, this gives a contradiction.

This proves that $I' = I$. This completes the proof of the Theorem. □

Corollary 1.4.4. *The ring $k[X_1, \ldots, X_n]$ is Noetherian.*

Theorem 1.4.1 follows trivially from the Corollary 1.4.4.

1.5 Irreducible Components of an Algebraic Set

Definition 1.5.1. *An algebraic set V is called **reducible** if $V = V_1 \cup V_2$, where $V_1 \subsetneq V$ and $V_2 \subsetneq V$ are proper algebraic subsets. If V is not reducible, then we say it is **irreducible**.*

Proposition 1.5.2. *An algebraic set is irreducible iff $I(V)$ is prime.*

Proof. If $I(V)$ is not prime, then there exist $F_1, F_2 \notin I(V)$ such that $F_1 F_2 \in I(V)$. Let $V_1 = V \cap V(F_1)$ and $V_2 = V \cap V(F_2)$. Then $V_1, V_2 \subsetneq V$.

Clearly, $V_1 \cup V_2 \subset V$. If $P \in V$, then $(F_1 F_2)(P) = 0 \implies P \in V(F_1)$ or $V(F_2)$. Thus, $V \subset V_1 \cup V_2$. This shows $V = V_1 \cup V_2$ and so is reducible.

Conversely, suppose V is reducible. Then $V = V_1 \cup V_2$ and $V_1 \subsetneq V$. Then $I(V) \subsetneq I(V_1)$, or else applying Proposition 1.3.1 (9) we will get $V = V_1$, a contradiction. Thus, $I(V) \subset I(V_1) \cap I(V_2)$. It is clear that $I(V_1) \cap I(V_2) \subset I(V)$. Thus, $I(V) = I(V_1) \cap I(V_2)$. This shows that $I(V)$ is not prime. □

Lemma 1.5.3. *Let $\mathcal{S}$ be a collection of ideals in a Noetherian ring. Then $\mathcal{S}$ has a maximal element.*

Proof. Let $I_0 \in \mathcal{S}$ be any ideal. If it is not maximal, then we may find an ideal $I_1 \in \mathcal{S}$ such that $I_0 \subsetneq I_1$. Proceeding in this fashion, we get a chain $I_0 \subsetneq I_1 \subsetneq \ldots$. Let $I = \bigcup_{j=0}^{\infty} I_j$.

Then I is an ideal and so is finitely generated, say by $F_1, \ldots, F_k$. Then there is N such that $F_1, \ldots, F_k \in I_N$. This proves that $I = I_N$, which is a contradiction. Thus, we cannot get a chain of proper inclusions, and so $\mathcal{S}$ has maximal elements. □

Corollary 1.5.4. *Let $\{V_\alpha\}$ be a collection of algebraic sets of $\mathbb{A}^n(k)$. Then $\{V_\alpha\}$ has minimal elements.*

Theorem 1.5.5. *Let V be an algebraic subset of $\mathbb{A}^n(k)$. Then there are unique irreducible algebraic subsets $V_1, \ldots, V_m$ such that $V = V_1 \cup \ldots \cup V_m$ and $V_i \not\subset V_j$ for $i \neq j$.*

Proof. First, we claim that every algebraic subset can be written as a finite union of irreducible algebraic subsets. If not, let $\mathcal{S}$ be the collection of algebraic subsets that do not have this property. Then $\mathcal{S}$ has a minimal element, say V. If V were irreducible, then we could write $V = V$ as a finite union of irreducible algebraic sets, which is a contradiction. Thus, V is reducible. $V = V_1 \cup V_2$. Since $V_1 \subsetneq V$ and V is minimal in $\mathcal{S}$, it follows that $V_1 \notin \mathcal{S}$ and so they can be written as a finite union of irreducible algebraic subsets. Thus, V is also a finite union of irreducible algebraic subsets, a contradiction. Thus, $\mathcal{S} = \emptyset$.

Thus, given an algebraic subset V, we may write $V = V_1 \cup \ldots \cup V_m$ as a finite union of irreducible algebraic subsets. If $V_i \subset V_j$ for some j, then we may remove V_i. Thus, we may assume that $V_i \not\subset V_j$ for $i \neq j$.

Suppose $V = V_1 \cup \ldots \cup V_m = W_1 \cup \ldots \cup W_k$. Then intersecting both sides with V_1, we get $V_1 = (V_1 \cap W_1) \cup \ldots \cup (V_1 \cap W_k)$. As V_1 is irreducible, this forces that $V_1 = V_1 \cap W_i$ for some i. Thus, $V_1 \subset W_i$. Similarly, $W_i \subset V_j$ for some j. Thus, $j = 1$ and $V_1 = W_i$. Proceeding in this way, it can be shown that $l = m$ and $V_i = W_{\sigma(i)}$ for some permutation σ. We leave this to the reader.

This completes the proof of the Theorem. □

The algebraic sets V_i are called the **irreducible components** of V.

1.6 Algebraic Subsets of the Plane $\mathbb{A}^2(k)$

Proposition 1.6.1. *Let F, G be polynomials in $k[X, Y]$ with no common factors. Then $V(F, G) = V(F) \cap V(G)$ is a finite set of points.*

Proof. F and G have no common factors in $k[X][Y]$, so they also have no common factors in $k(X)[Y]$ (see Theorem 1.1.11). Since $k(X)[Y]$ is a PID, $(F, G) = (1)$ in $k(X)[Y]$. Therefore $AF + BG = 1$ for some $R, S \in k(X)[Y]$. There is a nonzero $D \in k[X]$ such that $DR = A$, $DS = B \in k[X, Y]$. Therefore $AF + BG = D$.

If $(a, b) \in V(F, G)$, then $D(a) = 0$. But D has only a finite number of zeros. This shows that only a finite number of X-coordinates appear among the points of $V(F, G)$. Since the same reasoning applies to the Y-coordinates, there can be only a finite number of points. □

Corollary 1.6.2. *Let $F \in k[X, Y]$ be irreducible and assume that $V(F)$ is infinite. Then $I(V(F)) = (F)$ and $V(F)$ is irreducible.*

Proof. Since F is irreducible and $k[X, Y]$ is a UFD, it follows that F is prime. Thus, it follows that $V(F)$ Clearly, $(F) \subset I(V(F))$. Suppose $G \in I(V(F))$ and $G \notin (F)$. Since F is irreducible, this means F and G have no common factors. The previous Proposition then shows that $V(F, G)$ is a finite set. Since $(F, G) \subset I(V(F))$ it follows that $V(I(V(F)))$ is finite. But as $V(I(V(F))) = V(F)$, it follows that $V(F)$ is finite, which is a contradiction. This shows that $I(V(F)) = (F)$, which in turn shows, using Proposition 1.5.2, that $V(F)$ is irreducible. □

Corollary 1.6.3. *Let k be infinite. Then the irreducible algebraic sets of $\mathbb{A}^2(k)$ are: $\mathbb{A}^2(k)$, $\emptyset$, points, and irreducible plane curves $V(F)$, where F is irreducible and $V(F)$ is infinite.*

Proof. Let $V \neq \emptyset$ be an irreducible set which is infinite. If $I(V) = (0)$, then $V = \mathbb{A}^2(k)$. So assume $I(V) \neq (0)$. Let $F \in I(V)$ be a nonzero element. Since $I(V)$ is prime, it follows that it contains an irreducible factor of F, and so we may assume that F is irreducible.

If $(F) \subsetneq I(V)$ then let $G \in I(V)$ such that $G \notin (F)$. Then $(F, G) \subset I(V)$ and so $V \subset V(F, G)$, which is finite, a contradiction. Thus, $(F) = I(V)$ and $V = V(F)$.

If $p \in \mathbb{A}^2(k)$ is a point, then we saw earlier that $\{p\}$ is an algebraic set. This is an irreducible algebraic set. It is also clear that an algebraic set which is finite is irreducible iff it consists of only one point. This completes the proof of the Proposition. □

Corollary 1.6.4. *Assume k is algebraically closed, F a non-constant polynomial in $k[X, Y]$. Let $F = F_1^{n_1} \dots F_r^{n_r}$ be the decomposition of F into irreducible factors. Then $V(F) = V(F_1) \cup \dots \cup V(F_r)$ is the decomposition of $V(F)$ into irreducible components and $I(V(F)) = (F_1 \dots F_r)$.*

Proof. Since k is algebraically closed, by Prob 1.14, each $V(F_i)$ is infinite and so irreducible. It is clear that $V(F_i) \not\subset V(F_j)$ if $i \neq j$, or else applying Proposition 1.3.1 (9) we

get a contradiction. It is also clear that $V(F) = V(F_1) \cup \ldots \cup V(F_r)$. Thus, it follows that this is the decomposition into irreducible components.

Clearly, $I(V(F)) = \bigcap I(V(F_i)) = \bigcap (F_i) = (F_1 F_2 \ldots F_r)$. □

1.7 Modules; Finiteness conditions

Let R and S be rings and let $\phi : R \to S$ be a ring homomorphism. This makes S into an R-algebra (this is the definition of an R-algebra) and also an R-module.

We say that S is a **finitely generated R-algebra** if there exist elements $s_1, \ldots, s_n \in S$ such that the extension of ϕ,

$$\tilde{\phi} : R[X_1, \ldots, X_n] \to S \quad \text{defined by } x_i \mapsto s_i$$

is surjective.

We say that S is a **finitely generated R-module** if there exist $s_1, \ldots, s_n \in S$ such that

$$S = \sum_{i=1}^{n} R s_i.$$

Note that $a \cdot s := \phi(a)s$ for $a \in R$.

Note that being finitely generated as a module is a much stronger condition than being finitely generated as an algebra. Often "finitely generated as a module" will be simply shortened to "finite".

1.8 Integral Elements

Let S be a domain and let $R \subset S$ be a subring. This implies that R is also a domain.

Definition 1.8.1 (Integral Element)**.** *An element $s \in S$ is said to be **integral over** R if there exists a monic polynomial $P(X) = X^n + a_1 X^{n-1} + \ldots + a_n$, with $a_i \in R$, such that $P(s) = 0$.*

Proposition 1.8.2. *Let R be a subring of a domain S. The following are equivalent:*

1. *$v \in S$ is integral over R.*
2. *The ring $R[v] \subset S$ is module finite over R.*
3. *There is a subring $R' \subset S$ such that $R[v] \subset R'$ and R' is module finite over R.*

Proof. (1) $\implies$ (2) $\implies$ (3) is clear. Let us prove (3) $\implies$ (1).

Let $\alpha_1, \ldots, \alpha_n \in R'$ be generators of R' as an R-module. Consider the map $R' \to R'$, defined by $x \mapsto xv$. Let $\alpha_i v = \sum a_{ji}\alpha_j$. If we write this as a matrix, we get

$$A \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = \begin{bmatrix} a_{11} - v & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} - v & \ldots & a_{2n} \\ \vdots & & \ddots & \vdots \\ a_{n1} & \ldots & & a_{nn} - v \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = 0$$

where $a_{ji} \in R$ and A is an $n \times n$ matrix with entries in R'.

We think of all the coefficients being in the ring R'. Multiplying with the adjoint, we get that $\det(A)\alpha_i = 0$ for all i. As R' is a domain and not all α_i are zero, it follows that $\det(A) = 0$. It is easily seen that this is equivalent to saying that v is the zero of a monic polynomial with coefficients in R. □

Corollary 1.8.3. *Let S be a domain and let $R \subset S$ be a subring. The set R' consisting of elements of S which are integral over R is a subring of S.*

Proof. Let $a, b \in S$ be integral over R. Then $R[a]$ is finite over R and $R[a, b]$ is finite over $R[a]$. Thus, $R[a, b]$ is finite over R. It follows that $a \pm b$ and ab are integral over R. □

1.9 Finiteness of Field Extensions

Next, we want to prove the following Proposition.

Proposition 1.9.1. *Let $k \subset L$ be fields. If L is finitely generated as a k-algebra, then it is finitely generated as a k-module.*

Proof. Suppose $L = k[v]$ is generated by only one element as a k-algebra. If $v = 0$ then $L = k$. If $v \neq 0$, then it has an inverse, $g(v)$. Thus, $g(v)v = 1$ and this shows that v is integral over k. Thus, $k[v]$ is a finite module over k.

We will prove the Proposition by induction on the number of generators of L as a k-algebra. The base case is $n = 1$, which is proved above. Let us assume the proposition is true when L is generated as a k-algebra by $n - 1$ elements.

Let $L = k[v_1, \ldots, v_n]$ and let $k_1 = k(v_1)$. Then $k \subset k_1 \subset L$ and $L = k_1[v_2, \ldots, v_n]$. Thus, by induction, L is finite over k_1. If $k(v_1) = k[v_1]$ then we are done. Thus, we may assume that this is not the case, which shows that $k[v_1]$ is isomorphic to the polynomial ring over k in one variable. L being finite over k_1 means that each of $v_2, \ldots, v_n$ satisfy a monic polynomial $v_i^{n_i} + a_{i,1}v_i^{n_i-1} + \ldots + a_{i,n_i} = 0$ where $a_{i,j} \in k_1 = k(v_1)$.

Letting a to be the product of denominators of a_{ij}, we see that $av_2, \ldots, av_n$ is integral over $k[v_1]$. Obviously v_1, and so av_1, is also integral over $k[v_1]$. It follows that every polynomial in $av_1, av_2, \ldots, av_n$ is integral over $k[v_1]$. Since $L = k[v_1, \ldots, v_n]$, for any $z \in L$, there is an N such that $a^N z$ is a polynomial in $av_1, av_2, \ldots, av_n$, and so integral over $k[v_1]$. In particular, we may take $z \in k(v_1)$.

Since $k[v_1]$ is a polynomial ring over k, it is an easy exercise to check that an element of $k(v_1)$ integral over $k[v_1]$ is in $k[v_1]$. Thus, this shows that for any $z \in k(v_1)$, there is an N such that $a^N z \in k[v_1]$. Clearly, this is not possible. Thus, it follows that $k[v_1] = k(v_1)$ is finite over k.

It follows that L is also finite over k. □

1.10 Hilbert's Nullstellensatz

We assume that k is algebraically closed.

Theorem 1.10.1 (Weak Nullstellensatz)**.** *If I is a proper ideal in $k[X_1, \ldots, X_n]$, then $V(I) \neq \emptyset$.*

Proof. Let $J \supset I$ be a maximal ideal. Then $V(J) \subset V(I)$. Thus, it suffices to show that $V(J) \neq \emptyset$. Consider the extension of fields $k \subset k[X_1, \ldots, X_n]/J$. Since this is finitely generated, it follows that this is a finite extension. Since k is algebraically closed, this map is an isomorphism. Thus, for each X_i, $\exists a_i \in k$ such that $X_i - a_i \in J$.

It follows that $(X_1 - a_1, \ldots, X_n - a_n) \subset J$. Since both are maximal, it follows that $J = (X_1 - a_1, \ldots, X_n - a_n)$. Thus, $V(J) = \{(a_1, \ldots, a_n)\} \neq \emptyset$. □

Remark 1.10.2. The above proof shows that the maximal ideals of $k[X_1, \ldots, X_n]$ are precisely $(X_1 - a_1, \ldots, X_n - a_n)$, for some $a_i \in k$. □

Theorem 1.10.3 (Nullstellensatz)**.** *Let $J \subset k[X_1, \ldots, X_n]$ be an ideal. Then $I(V(J)) = Rad(J)$.*

Proof. It is clear that $\mathrm{Rad}(J) \subset I(V(J))$. Let $J = (F_1, \ldots, F_r)$ and suppose that $G \in I(V(J))$. Consider the ideal $\tilde{J} = (F_1, \ldots, F_r, X_{n+1}G - 1) \subset k[X_1, \ldots, X_n, X_{n+1}]$.

Suppose $(a_1, \ldots, a_n, a_{n+1}) \in V(\tilde{J})$. Then $(a_1, \ldots, a_n) \in V(J)$. Since $G \in I(V(J))$, we get $G(a_1, \ldots, a_n) = 0$. This gives $(X_{n+1}G - 1)(P) = 0$, that is, $-1 = 0$, which is not possible. Thus, $V(\tilde{J}) = \emptyset$ and so $\tilde{J} = (1)$. Thus, there is an equality

$$\sum_{i=1}^{r} A_i(X_1, \ldots, X_{n+1})F_i + B(X_1, \ldots, X_{n+1})(X_{n+1}G - 1) = 1$$

Letting $X_{n+1} = \frac{1}{G}$, and clearing denominators, we get $G^N \in (F_1, \ldots, F_r)$. Equivalently, we can think of this as going modulo the ideal $(X_{n+1}G - 1)$ and then multiplying both sides of the resulting equation by a high enough power of G so that all the X_{n+1} can be removed using the relation $X_{n+1}G = 1$. □

Corollary 1.10.4. *If J is a radical ideal in $k[X_1, \ldots, X_n]$ then $I(V(J)) = J$. Thus, there is a bijective 1-1 correspondence between radical ideals and algebraic sets.*

Corollary 1.10.5. *There is a 1-1 correspondence between irreducible algebraic sets and prime ideals. There is a 1-1 correspondence between points and maximal ideals.*

Corollary 1.10.6. *Let I be an ideal in $k[X_1, \ldots, X_n]$. Then $V(I)$ is a finite set if and only if $k[X_1, \ldots, X_n]/I$ is a finite-dimensional k-vector space. If this occurs the number of points in $V(I)$ is at most* $\dim_k(k[X_1, \ldots, X_n]/I)$.

Proof. Suppose that $\dim_k(k[X_1, \ldots, X_n]/I) < \infty$. Let $P_1, \ldots, P_r$ be distinct points in $V(I)$. Choose $F_1, \ldots, F_r \in k[X_1, \ldots, X_n]$ such that $F_i(P_j) = 0$ if $i \neq j$ and $F_i(P_i) = 1$.

Let $\bar{F_i}$ be the residue in $k[X_1, \ldots, X_n]/I$. If $\sum \lambda_i \bar{F_i} = 0$, then evaluating at P_i (which we can do as $I(P_i) \supset I(V(I)) \supset I$) we get that $\lambda_i = 0$. Thus, $\bar{F_i}$ are linearly independent. Thus, $r \leqslant \dim_k(k[X_1, \ldots, X_n]/I)$. This shows $V(I)$ is finite.

Conversely, suppose $V(I) = \{P_1, \ldots, P_r\}$. Let $P_i = (a_{i1}, \ldots, a_{in})$. Define $F_j = \prod_{i=1}^{r}(X_j - a_{ij})$. Then $F_j \in I(V(I))$ and so $F_j^N \in I$ for some $N > 0$. Choose N which works for all j. Clearly $k[X_1, \ldots, X_n]/(F_1^N, \ldots, F_n^N)$ is a finite dimensional k-vector space as each X_i satisfies a monic polynomial $F_i^N = 0$. Thus, $k[X_1, \ldots, X_n]/I$ being a further quotient of this is also finite dimensional. The first part of the proof also shows that the number of points is at most $\dim_k(k[X_1, \ldots, X_n]/I)$. □

1.11 Exercises

Exercise 1.11.1. Let R be a domain.

(a) If F, G are forms of degree r, s respectively in $R[X_1, \ldots, X_n]$, show that FG is a form of degree $r + s$.

(b) Show that any factor of a form in $R[X_1, \ldots, X_n]$ is also a form.

Solution.

(a) Note that any monomial in the product is obtained by multiplying an r-form with an s-form, thus giving an $r + s$-form. Hence, the resultant product, if non-zero, must be an $r + s$-form. Since R is a domain, $R[X]$ is also a domain, and thus the product polynomial is indeed non-zero.

(b) Let F be a form of degree d such that it factors as $F = AB$. Write A, B in terms of their homogenous components,

$$A = A_a + A_{a+1} + \cdots A_{a+\delta_1}, \quad B = B_b + B_{b+1} + \cdots + B_{b+\delta_2}$$

where $A_a \neq 0, A_{a+\delta_1} \neq 0, B_b \neq 0, B_{b+\delta_2} \neq 0$. Then the component of lowest non-zero order in the product is $A_a B_b$ (order $a+b$), and the component of highest non-zero order in the product is $A_{a+\delta_1} B_{b+\delta_2}$ (order $a+b+\delta_1+\delta_2$). Since the product is a form, we must have $a+b = a+b+\delta_1+\delta_2 \implies \delta_1+\delta_2 = 0$. Since $\delta_1, \delta_2 \geq 0$, we must have $\delta_1 = \delta_2 = 0$. Thus, $A = A_a$ and $B = B_b$, and hence any factor of a form is also a form.

□

Exercise 1.11.2. Let R be a UFD, K the quotient field of R. Show that every element z of K may be written as $z = a/b$, where $a, b \in R$ have no common factors; this representative is unique up to units of R.

Solution. Let $z = p/q$ for some $p, q \in R$. Let $d = \gcd(p, q)$ and $p = dp', q = dq'$. Then $z = p'/q'$ where $\gcd(p', q') = 1$. Assume there was another such representation $z = a/b$ with $\gcd(a, b) = 1$. Since $p'/q' = a/b$, we have that $bp' = aq'$ Now $b|aq'$ and $\gcd(b, a) = 1$, so $b|q'$. Similarly, we see that $q'|b$. Thus b and q' are associates, say $b = uq'$ for some unit $u \in R$. We have $uq'p' = aq' \implies up' = a$ which shows that a and p are associates too and $a = up', b = uq'$ for some unit u. Thus, the representative is unique up to units. □

Exercise 1.11.3. Let R be a PID. Let P be a non-zero, proper, prime ideal in R.

(a) Show that P is generated by an irreducible element.

(b) Show that P is maximal.

Solution.

(a) Let P be generated by an element $p \neq 0$, that is, $P = (p)$. Suppose $p = bc$ for some $b, c \in R$. Since P is prime and $bc \in P$, we have either $b \in P$ or $c \in P$. WLOG, assume $b \in P = (bc)$. Thus, $\exists k \in R$ such that $b = kbc \implies b(1-kc) = 0$. Since $b \neq 0$, we have $kc = 1$ which shows that c is a unit. Thus, p is irreducible and P is generated by an irreducible element.

(b) Say $P = (p)$ for some $0 \neq p \in R$. Let $I = (q)$ be an ideal containing P, where $q \in R$. Then $P \subseteq I \implies (p) \subseteq (q)$ which means that $p = kq$ for some $k \in R$. This means that $kq \in P$, and since P is prime, either $q \in P$ or $k \in P$. If $q \in P$, then

$(q) \subseteq P = (p)$, and thus $(p) = (q) \implies P = I$. Else if $k \in P = (p)$, $\exists k' \in R$ such that $k = k'p$. Then $p = k'pq \implies p(1 - k'q) = 0$. Since $p \neq 0$, we have that $k'q = 1$ and thus q is a unit. Hence, $(q) = 1 \implies I = R$. Thus the only ideals containing P are P and R, and thus P is a maximal ideal.

□

Exercise 1.11.4. Let k be an infinite field, $F \in k[X_1, \ldots, X_n]$. Suppose $F(a_1, \ldots, a_n) = 0$ for all $a_1, \ldots, a_n \in k$. Show that $F = 0$.

Solution. We proceed via induction. For $n = 1$, let $F \in k[X_1]$ be such that $F(a_1) = 0$ for all $a_1 \in k$. Then $F = 0$ since if it has a positive degree n, it could have had at most n roots, but k is infinite.
Now, say we have proved the statement for all polynomials in $k[X_1, \ldots, X_{n-1}]$. Assume that $F \in k[X_1, \ldots, X_n]$ such that $F(a_1, \ldots, a_n) = 0$ for all $a_1, \ldots, a_n \in k$. Consider the polynomial $G(X_n) = F(a_1, \ldots, a_{n-1}, X_n)$ for some fixed $a_1, \ldots, a_{n-1} \in k$. Now $G(a_n) = 0$ for all $a_n \in k$, so $G = 0$. Hence $F(a_1, \ldots, a_n) = 0$ for all $a_1, \ldots, a_n \in k$. Thus, $F = 0$. □

Exercise 1.11.5. Let k be any field. Show that there are an infinite number of irreducible monic polynomials in $k[X]$.

Solution. Assume to the contrary only finite manly irreducible monic polynomials existed in $k[X]$. Let $F_1, \ldots, F_n$ be an enumeration of all of them. Consider the polynomial $k[X] \ni G = F_1 \cdots F_n + 1$. If G is reducible, then one of $F_1, \ldots, F_n$ must divide G. But each F_i, $1 \leq i \leq n$, leaves a remainder of 1 on dividing G. Hence, G must be irreducible contradicting the assumption that $F_1, \ldots, F_n$ were the only irreducible polynomials in $k[X]$. Hence, there are infinitely many irreducible polynomials in $k[X]$. □

Exercise 1.11.6. Show that any algebraically closed field is infinite.

Solution. Let k be an algebraically closed field with finitely many elements $a_1, \ldots, a_n$. Consider the polynomial $f \in k[X]$ defined as $f(X) = (X - a_1) \cdots (X - a_n) + 1$. Since k is algebraically closed, f must admit a root in k, however $f(a) = 1$ for all $a \in k$. We arrive at a contradiction! Thus, any algebraically closed field is infinite. □

Exercise 1.11.7. Let k be a field, $F \in k[X_1, \ldots, X_n]$, $a_1, \ldots, a_n \in k$.

(a) Show that
$$F = \sum \lambda_{(i)} (X_1 - a_1)^{i_1} \cdots (X_n - a_n)^{i_n}, \quad \lambda_{(i)} \in k.$$

(b) If $F(a_1, \ldots, a_n) = 0$, show that $F = \sum_{i=1}^{n} (X_i - a_i) G_i$ for some (not unique) G_i in $k[X_1, \ldots, X_n]$.

Solution.

(a) Let $Y_i = X_i - a_i$ for $1 \leq i \leq n$. Then expand $F(X_1, \ldots, X_n)$ in terms of Y_i by substituting each occurrence of X_i by $Y_i + a_i$. Say

$$F(X_1, \ldots, X_n) = \sum \lambda_{(i)} Y_1^{i_1} \cdots Y_n^{i_n}, \quad \lambda_{(i)} \in k.$$

Then substituting $Y_i = X_i - a_i$ back gives us our required expression.

(b) Take the representation of F as in (a). Take $(X_1 - a_1)$ in common from as many terms as possible and let G_1 be the other factor multiplying it. From the remaining expression, factor out $(X_2 - a_2)$ in common with G_2 representing the other factor. Continuing this process, we end up at

$$F(X_1, \ldots, X_n) = \sum_{i=1}^{n} (X_i - a_i) G_i(X_1, \ldots, X_n) + \lambda$$

for some $\lambda \in k$. But $0 = F(a_1, \ldots, a_n) = \lambda$. Thus, we end up with

$$F = \sum_{i=1}^{n} (X_i - a_i) G_i.$$

□

Exercise 1.11.8. Show that the algebraic subsets of $\mathbb{A}^1(k)$ are just the finite subsets, together with $\mathbb{A}^1(k)$ itself.

Solution. The common zeroes of a set of polynomials of $k[X]$ is contained in the set of zeroes of a single polynomial. Hence $V(F)$ as $F \in k[X]$ varies generates all the algebraic subsets of $\mathbb{A}^1(k)$. If $F = 0$, we have $V(0) = \mathbb{A}^1(k)$. For $F \neq 0$, we get that $V(F)$ is a finite subset corresponding to the roots of F. Conversely, corresponding to any finite subset $a_1, \ldots, a_n$ of $\mathbb{A}^1(k)$, it is equal to $V(F)$ for $F = (X - a_1) \cdots (X - a_n)$. □

Exercise 1.11.9. If k is a finite field, show that every subset of $\mathbb{A}^n(k)$ is algebraic.

Solution. Note that $\emptyset = V(1)$. Now for any subset $S \subseteq k$, define the polynomial

$$F_S(X) = \prod_{s \in S} (X - s)$$

Clearly, $F_S(X) \in k[X]$ and $V(F_S) = S$. □

Exercise 1.11.10. Give an example of a countable collection of algebraic sets whose union is not algebraic.

Solution. Consider $\mathbb{A}^1(\mathbb{R})$. Then the set $\{n\}$ where $n \in \mathbb{Z}$ is an algebraic set. But the set

$$\mathbb{Z} = \bigcup_{n \in \mathbb{Z}} \{n\}$$

is a countable collection of algebraic sets but is not algebraic (since it is neither finite nor the whole space $\mathbb{A}^1(\mathbb{R})$ itself). □

Exercise 1.11.11. Show that the following are algebraic sets:

(a) $\{(t, t^2, t^3) \in \mathbb{A}^3(k) | t \in k\}$;

(b) $\{(\cos(t), \sin(t)) \in \mathbb{A}^2(\mathbb{R}) | t \in \mathbb{R}\}$;

(c) the set of points in $\mathbb{A}^2(\mathbb{R})$ whose polar coordinates (r, θ) satisfy the equation $r = \sin(\theta)$.

Solution.

(a) The given set is $V(Y - X^2, Z - X^3)$.

(b) The given set is $V(X^2 + Y^2 - 1)$.

(c) The given set is $V(X^2 + Y^2 - Y)$.

□

Exercise 1.11.12. Suppose C is an affine plane curve, and L is a line in $\mathbb{A}^2(k)$, $L \not\subset C$. Suppose $C = V(F)$, $F \in k[X, Y]$ a polynomial of degree n. Show that $L \cap C$ is a finite set of no more than n points.

Solution. Suppose $L = (Y - aX - b)$ for some $a, b \in k$. If a point $(x, y) \in L \cap C$, then $F(x, y) = 0$ and $y = ax + b$. Hence, we must have that $F(x, ax + b) = 0$. Now $f(x, ax + b)$ is a degree n polynomial in x and can thus admit at most n roots. Corresponding to each such root x_0, there is a unique $y_0 = ax_0 + b$ such that $(x_0, y_0) \in L \cap C$. Thus, $L \cap C$ can have at most n points. □

Exercise 1.11.13. Let F be a nonconstant polynomial in $k[X_1, \ldots, X_n]$, k algebraically closed. Show that $\mathbb{A}^n(k) \setminus V(F)$ is infinite if $n \geq 1$, and $V(F)$ is infinite if $n \geq 2$. Conclude that the complement of any proper algebraic set is infinite.

Solution. Assume $n \geq 1$. Since F is nonconstant, there exists at least one variable, say X_1 without loss of generality, such that F has positive degree in X_1. Say

$$F = \sum_{i=0}^{d} a_i(X_2, \ldots, X_n)X_1^i, \quad d \geq 1, a_d \neq 0.$$

Since k is infinite, there exists some $(b_2, \ldots, b_n) \in \mathbb{A}^{n-1}(k)$ such that $a_d(b_2, \ldots, b_n) \neq 0$ (since if a_d were to vanish on all of $\mathbb{A}^{n-1}(k)$, then $a_d = 0$). Define the univariate polynomial

$$f(X_1) = F(X_1, b_2, \ldots, b_n) \in k[X_1].$$

Now $\deg f = d \geq 1$. A non-zero univariate polynomial f has only finitely many zeroes. Hence the set $S = \{x_1 \in k | f(x_1) \neq 0\}$ is infinite. For each $x_1 \in S$, the point $(x_1, b_2, \ldots, b_n) \in \mathbb{A}^n(k)$ satisfies $F(x_1, b_2, \ldots, b_n) = f(x_1) \neq 0$ and hence is in $\mathbb{A}^n(k) \backslash V(F)$. Hence, $\mathbb{A}^n(k) \setminus V(F)$ is infinite.

Assume $n \geq 2$. Since F is nonconstant, without loss of generality, we can assume that F has positive degree in X_1, say

$$F = \sum_{i=0}^{d} a_i(X_2, \ldots, X_n)X_1^i, \quad d \geq 1, a_d \neq 0.$$

For any $b = (b_2, \ldots, b_n) \in \mathbb{A}^{n-1}(k)$, the univariate polynomial

$$f_b(X_1) = F(X_1, b_2, \ldots, b_n)$$

is the zero polynomial if and only if $a_d(b_2, \ldots, b_n) = 0$. Hence $\{b \in \mathbb{A}^{n-1}(k) | f_b = 0\} = V(a_d) \subseteq \mathbb{A}^{n-1}(k)$. Since $a_d \neq 0$ and k is infinite, $\mathbb{A}^{n-1}(k) \setminus V(a_d)$ is infinite as we have shown. For each f_b where $b \in \mathbb{A}^{n-1}(k) \setminus V(a_d)$, we have at least one root α, hence $(\alpha, b_2, \ldots, b_n) \in V(F)$. Since the number of b such that $f_b \neq 0$ is infinite, we have that $V(F)$ is infinite.

Let $W \subsetneq \mathbb{A}^n(k)$ be a proper algebraic set for an infinite k. Then $W = V(I)$ for some ideal $I \neq (0)$. Chose $0 \neq F \in I$, then

$$\mathbb{A}^n(k) \setminus W \supseteq \mathbb{A}^n(k) \setminus V(F),$$

which is infinite. □

Exercise 1.11.14. Let $V \subseteq \mathbb{A}^n(k), W \subseteq \mathbb{A}^m(k)$ be algebraic sets. Show that

$$V \times W = \{(a_1, \ldots, a_n, b_1, \ldots, b_m) | (a_1, \ldots, a_n) \in V, (b_1, \ldots, b_m) \in W\}$$

is an algebraic set in $\mathbb{A}^{n+m}(k)$. It is called the *product* of V and W.

Solution. Let $V = V(I)$ and $W = V(J)$ where $I \subseteq k[X_1, \ldots, X_n]$ and $J \subseteq k[Y_1, \ldots, Y_m]$ are ideals. Define the ideals of $k[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$:

$$I^e = k[X_1, \ldots, X_n, Y_1, \ldots, Y_m] \cdot I, \quad J^e = k[X_1, \ldots, X_n, Y_1, \ldots, Y_m] \cdot J.$$

Let $K = I^e + J^e$. Then, we claim that $V(K) = V \times W$.
A point $(a, b) = (a_1, \ldots, a_n, b_1, \ldots, b_m) \in \mathbb{A}^{n+m}(k)$ lies in $V(K)$ iff every polynomial in K vanishes at (a, b), which in particular, holds iff every $f \in I$ vanishes at a and every $g \in J$ vanishes at b. Hence $V(K) = V \times W$, and hence $V \times W$ is an algebraic set in $\mathbb{A}^{n+m}(k)$. □

Exercise 1.11.15. Let V, W be algebraic sets in $\mathbb{A}^n(k)$. Show that $V = W$ if and only if $I(V) = I(W)$.

Solution. If $V = W$, clearly $I(V) = I(W)$.
Conversely, since V, W are algebraic sets, $V(I(V)) = V$ and $V(I(W)) = W$. Since $I(V) = I(W) \implies V(I(V)) = V(I(W)) \implies V = W$. □

Exercise 1.11.16.

(a) Let V be an algebraic set in $\mathbb{A}^n(k)$, $P \in \mathbb{A}^n(k)$ a point not in V. Show that there is a polynomial $F \in k[X_1, \ldots, X_n]$ such that $F(Q) = 0$ for all $Q \in V$, but $F(P) = 1$.

(b) Let $P_1, \ldots, P_r$ be distinct points in $\mathbb{A}^n(k)$, not in an algebraic set V. Show that there are polynomials $F_1, \ldots, F_r \in I(V)$ such that $F_i(P_j) = 0$ if $i \neq j$, and $F_i(P_i) = 1$.

(c) With $P_1, \ldots, P_r$ and V as in (b), and $a_{ij} \in k$ for $1 \leq i, j \leq r$, show that there are $G_i \in I(V)$ with $G_i(P_j) = a_{ij}$ for all i and j.

Solution.

(a) Since $V \subset V \cup \{P\}$, we have that $I(V) \supseteq I(V \cup \{P\})$. If $I(V) = I(V \cup \{P\})$, then $V(I(V)) = V(I(V \cup \{P\}))$ which would imply that $V \supseteq V \cup \{P\}$, which is absurd Hence $I(V) \supset I(V \cup \{P\})$. Hence, choose a $\tilde{F} \in I(V) \setminus I(V \cup \{P\})$. Thus, $\tilde{F}(P) \neq 0$. Define $F = \tilde{F}/\tilde{F}(P)$. Then $F(Q) = 0$ for all $Q \in V$ and $F(P) = 1$.

(b) Define the algebraic set

$$V_i = V \cup \bigcup_{j \neq i} \{P_j\}$$

Using (a), we can find an $F_i \in k[X_1, \ldots, X_n]$ such that $F_i(V_i) = 0$ but $F_i(P_j) = 1$. Thus $F_i \in I(V)$, $F_i(P_j) = \delta_{ij}$.

(c) With $F_1, \ldots, F_r \in k[X_1, \ldots, X_n]$ as defined in (b), define

$$G_i = \sum_{j=1}^{r} a_{ij} F_j$$

Then $G_i \in I(V)$ with $G_i(P_j) = a_{ij}$.

□

Exercise 1.11.17. Let I be an ideal in a ring R. If $a^n \in I, b^m \in I$, show that $(a+b)^{n+m} \in I$. Show that rad$I$ is an ideal, in fact a radical ideal. Show that any prime is a radical ideal.

Solution. Note that

$$(a+b)^m = \sum_{i=0}^{n+m} \binom{n+m}{i} a^i b^{n+m-i}$$

Each term above is contained in I and hence the entire sum is in I. In particular, if $a, b \in \text{rad}I$, then $a+b \in \text{rad}I$. Clearly, for any $r \in R$, $ra \in \text{rad}I$ since $(ra)^n = r^n a^n \in I$ if $a^n \in I$. Thus rad$I$ is an ideal. If $a^n \in \text{rad}I$ for some n, then $(a^n)^m \in I$ for some m. This means that $a^{nm} \in I \implies a \in \text{rad}I$. Thus rad$I$ is a radical ideal.
Let P be a prime ideal. We show by induction on n that if $a^n \in P$, then $a \in P$. For $n = 1$, the case is clear. At the inductive step, assume $a^n \in P$ which means that $a \cdot a^{n-1} \in P$. Since P is prime, either $a \in P$ or $a^{n-1} \in P$ and hence $a \in P$ by induction. Thus $a \in P$. This shows that P is radical. □

Exercise 1.11.18. Show that $I = (X^2+1) \subset \mathbb{R}[X]$ is a radical (even a prime) ideal, but I is not the ideal of any set in $\mathbb{A}^1(\mathbb{R})$.

Solution. Since X^2+1 is a quadratic with no roots in $\mathbb{R}$, it is irreducible in $\mathbb{R}[X]$. Thus (X^2+1) is a prime ideal, and hence a radical ideal.
Assume to the contrary that $I = I(S)$ for some $S \subseteq \mathbb{A}^1(\mathbb{R})$. Since $V(I(S)) \supseteq S$, we must have $S \subseteq V(X^2+1)$. But $V(X^2+1) = \emptyset$, and hence $S = \emptyset$. But then $I(S) = I(\emptyset) = \mathbb{R}[X] \neq (X^2+1)$, which is a contradiction! Thus I is not the ideal of any set in $\mathbb{A}^1(\mathbb{R})$. □

Exercise 1.11.19. Show that for any ideal I in $k[X_1, \ldots, X_n]$, $V(I) = V(\text{rad}I)$, and $\text{rad}I \subseteq I(V(I))$.

Solution. Since $I \subseteq \text{rad}I$, is clear that $V(\text{rad}I) \subseteq V(I)$. For the converse inclusion, let $P \in V(I)$. Then, for any $f \in \text{rad}I$, we have $f^n \in I$ for some $n \in \mathbb{N}$, and thus $f^n(P) = 0$ which implies that $f(P) = 0$. Thus, $P \in V(\text{rad}I)$, establishing that $V(I) \subseteq V(\text{rad}I)$.
Let $f \in \text{rad}I$. Then $f^n \in I$ for some $n \in \mathbb{N}$. Thus, for any point $P \in V(I)$, we have that $f^n(P) = 0 \implies f(P) = 0$. This shows that any element of $\text{rad}I$ vanishes on all of $V(I)$, and hence $\text{rad}I \subseteq I(V(I))$. □

Exercise 1.11.20. Show that $I = (X_1 - a_1, \ldots, X_n - a_n) \subseteq k[X_1, \ldots, X_n]$ is a maximal ideal, and that the natural homomorphism from k to $k[X_1, \ldots, X_n]/I$ is an isomorphism.

Solution. Define the evaluation map $\text{ev}_a : k[X_1, \ldots, X_n] \to k$ given by $f(X_1, \ldots, X_n) \mapsto f(a_1, \ldots, a_n)$. Then ev_a is surjective since $\text{ev}_a(c) = c$ for all $c \in k$. Thus, by the First Isomorphism Theorem,

$$\frac{k[X_1, \ldots, X_n]}{\ker \text{ev}_a} \cong k.$$

We show that $I = \ker \text{ev}_a$. Clearly, $X_i - a_i \in \ker \text{ev}_a$ for all $i \in [n]$, so $I \subseteq \ker \text{ev}_a$. For the reverse inclusion, take $f \in k[X_1, \ldots, X_n]$ such that $f(a_1, \ldots, a_n) = 0$. Then $f = \sum_{i=1}^{n} (X_i - a_i) g_i$ for some $g_i \in k[X_1, \ldots, X_n]$ and hence $f \in I$, which shows that $\ker \text{ev}_a \subseteq I$. Thus,

$$k[X_1, \ldots, X_n]/I \cong k.$$

Note that the isomorphism sends an element $c + I \in k[X_1, \ldots, X_n]$ to $c \in k$ for any $c \in k$. Hence, the natural homomorphism from k to $k[X_1, \ldots, X_n]/I$ is indeed an isomorphism. □

Exercise 1.11.21. Let I be an ideal in a ring R, $\pi : R \to R/I$ the natural homomorphism.

(a) Show that for every ideal J' of R/I, $\pi^{-1}(J') = J$ is an ideal of R containing I, and for every ideal J of R containing I, $\pi(J) = J'$ is an ideal of R/I. This sets up a natural one-to-one correspondence between $\{\text{ideals of } R/I\}$ and $\{\text{ideals of } R \text{ that contain } I\}$.

(b) Show that J' is a radical ideal if and only if J is radical. Similarly for prime and maximal ideals.

(c) Show that J' is finitely generated if J is. Conclude that R/I is Noetherian if R is Noetherian. Any ring of the form $k[X_1, \ldots, X_n]/I$ is Noetherian.

Solution.

(a) Let J' be an ideal of R/I, and let $J = \pi^{-1}(J')$. Being the (additive-group) homomorphic preimage of an additive subgroup, J is clearly an additive subgroup of R. Let $r \in R$ and $x \in J$. Then $\pi(rx) = \pi(r)\pi(x) \in J'$, and hence $rx \in \pi^{-1}(J') = J$, which shows that J is an ideal of R.
Now let J be an ideal of R containing I, and let $J' = \pi(J)$. Being the homomorphic image of an additive subgroup, J' is an additive subgroup of R/I. Let $\overline{r} \in R/I$ and $\overline{x}' \in J'$, say $\pi(x) = x' + I$ for some $x \in J$. Then $\pi(rx) = \pi(r)\pi(x) = \overline{rx'}$ and hence $\overline{rx'} \in J'$, which shows that J' is an ideal of R/I.

(b) Assume that J' is radical. Hence if $\overline{f}^n \in J' \implies \overline{f} \in J'$. Now assume that $f^n \in J$, then $\pi(f^n) \in J' \implies \pi(f)^n \in J' \implies \pi(f) \in J' \implies f \in J$. Thus, J is radical.
Conversely, assume that J is radical. Then $f^n \in J \implies f \in J$. Assume that $\pi(f)^n \in J'$. Then $\pi(f^n) \in J' \implies f^n \in J \implies f \in J \implies \pi(f) \in J'$. Hence J' is radical.

Let J' be a prime ideal. Let $xy \in J$. Then $\pi(xy) \in J' \implies \pi(x)\pi(y) \in J'$ and hence at least one of $\pi(x), \pi(y)$ is in J', which means that at least one of x, y is in J. Hence, J is a prime ideal.
Conversely, assume that J is a prime ideal. Let $\pi(x)\pi(y) \in J'$. Then, $xy \in J$ which implies that at least one of x, y is in J, which means that at least one of $\pi(x), \pi(y)$ is in J, which shows that J' is a prime ideal.

By the lattice correspondence set up in part (a), an ideal J is maximal in R if and only if J' is maximal in R/I.

(c) Say $J = (x_1, \ldots, x_n)$. Then we claim that $J' = (\pi(x_1), \ldots, \pi(x_n))$. This is true since for any $\pi(x) \in J'$, we can write $x = \sum_{i=1}^n r_i x_i$ for some $r_i \in R$, and thus

$$\pi(x) = \pi\left(\sum_{i=1}^n r_i x_i\right) = \sum_{i=1}^n \pi(r_i)\pi(x_i).$$

Now assume that R is Noetherian. Take any ideal J' of R/I, and let $J = \pi^{-1}(J')$. Since J is finitely generated (since R is Noetherian), it must be the case that J' is finitely generated. Hence, R/I is Noetherian.

□

Exercise 1.11.22. Give an example of a collection $\mathscr{S}$ of ideals in a Noetherian ring such that no maximal member of $\mathscr{S}$ is a maximal ideal.

Solution. Consider the ring $\mathbb{Z}$ and the collection $\mathscr{S} = \{(0)\}$. The zero ideal is the only maximal member of $\mathscr{S}$ but is not a maximal ideal. □

Exercise 1.11.23. Show that every proper ideal in a Noetherian ring is contained in a maximal ideal.

Solution. Let our proper ideal in consideration be I. Let $\mathscr{S}$ denote the set of proper ideals containing I. Then $\mathscr{S}$ is non-empty since $I \in \mathscr{S}$. Thus, $\mathscr{S}$ must have a maximal element, say $\mathfrak{m}$. $\mathfrak{m}$ must be a maximal ideal since if it were contained in some other ideal $\mathfrak{m}'$, then $\mathfrak{m}' \supset \mathfrak{m} \supseteq I \implies \mathfrak{m}' \in \mathscr{S}$ contradicting maximality of $\mathfrak{m}$ in $\mathscr{S}$. □

Exercise 1.11.24.

(a) Show that $V(Y - X^2) \subseteq \mathbb{A}^2(\mathbb{C})$ is irreducible; in fact, $I(V(Y - X^2)) = (Y - X^2)$.

(b) Decompose $V(Y^4 - X^2, Y^4 - X^2Y^2 + XY^2 - X^3) \subseteq \mathbb{A}^2(\mathbb{C})$ into irreducible components.

Solution. We shall make use of results from future parts of the chapter to offer a simpler solution.

(a) Note that $Y - X^2$ is irreducible in $\mathbb{C}[X, Y]$ since it is linear in Y. Thus $(Y - X^2)$ is prime, hence radical, and hence $I(V(Y - X^2)) = (Y - X^2)$ by Hilbert's Nullstellensatz. Since $\mathbb{C}$ is algebraically closed, $V(Y - X^2)$ is also irreducible.

(b) Let $F_1 = Y^4 - X^2$ and $F_2 = Y^4 - X^2Y^2 + XY^2 - X^3$. Note that $F_2 - F_1 = X(1 - X)(Y^2 + X)$, and $F_1 = (Y^2 - X)(Y^2 + X)$. So,

$$W = V(F_1, F_2) = V((Y^2 - X)(Y^2 + X), X(1 - X)(Y^2 + X)).$$

If $Y^2 + X = 0$, then both equations vanish simultaneously, so, $V(Y^2 + X) \subseteq W$. Note that $Y^2 + X$ is irreducible, and hence $V(Y^2 + X)$ is an irreducible component. If $Y^2 + X \neq 0$, then the first equation forces $X = Y^2$. Plugging the same into the second equation gives us that $2Y^4(1 - Y)(1 + Y) = 0$. So $Y \in \{-1, 0, 1\}$. This gives us points $(0, 0), (1, 1), (1, -1)$. Hence, the irreducible decomposition is

$$W = V(Y^2 + X) \cup \{(1, -1), (1, 1), (0, 0)\}.$$

□

Exercise 1.11.25. Show that $F = Y^2 + X^2(X - 1)^2 \in \mathbb{R}[X, Y]$ is an irreducible polynomial, but $V(F)$ is reducible.

Solution. Note that $F \in \mathbb{R}[X][Y]$ is a degree 2 polynomial in Y. If it is reducible, then we must have $F = (Y+f)(Y+g)$ for some $f, g \in \mathbb{R}[X]$. Expanding, we get that $F = Y^2+(f+g)Y+fg$. Comparing coefficients, we must have that $f+g = 0 \implies g = -f$ and $fg = X^2(X-1)^2 \implies f^2 = -X^2(X-1)^2$ which is not possible. Hence, F must be an irreducible polynomial.
Note that $V(F)$ is all $(x, y) \in \mathbb{A}^2(\mathbb{R})$ such that $y^2 + x^2(x-1)^2 = 0$ which means that $y^2 = 0$ and $x^2(x-1)^2 = 0$. Thus,

$$V(F) = \{(0,0),(1,0)\} = \{(0,0)\} \cup \{(1,0)\} = V(X,Y) \cup V(X-1,Y)$$

and hence, $V(F)$ is reducible. □

Exercise 1.11.26. Let V, W be algebraic sets in $\mathbb{A}^n(k)$, with $V \subseteq W$. Show that each irreducible component of V is contained in some irreducible component of W.

Solution. Let V_c be an irreducible component of V and let $W_1 \cup \cdots \cup W_m$ be an irreducible decomposition of W. Then $V_c \subseteq V \subseteq W = W_1 \cup \cdots \cup W_m$. Hence, $V_c = (V_c \cap W_1) \cup \cdots \cup (V_c \cap W_m)$. Since V_c is irreducible, we must have $V_c = V_c \cap W_j$ for some $j \in [m]$, which implies that $V_c \subseteq W_j$. □

Exercise 1.11.27. If $V = V_1 \cup \cdots \cup V_r$ is the decomposition of an algebraic set into irreducible components, show that $V_i \not\subseteq \bigcup_{j \neq i} V_j$.

Solution. Without loss of generality, we may assume $i = 1$. Assume to the contrary that $V_1 \subseteq V_2 \cup \cdots \cup V_r$. Then $V_1 = (V_1 \cap V_2) \cup \cdots \cup (V_1 \cap V_r)$. Since V_1 is irreducible, $V_1 = V_1 \cap V_j$ for some $j \in \{2, \ldots, r\}$. Thus, $V_1 \subseteq V_j$ which contradicts the minimality of the decomposition of V. □

Exercise 1.11.28. Show that $\mathbb{A}^n(k)$ is irreducible if k is infinite.

Solution. Note that if $F \in k[X_1, \ldots, X_n]$ such that $F(a_1, \ldots, a_n) = 0$ for all $(a_1, \ldots, a_n) \in \mathbb{A}^n(k)$, then $F = 0$ since k is infinite. Hence, $I(\mathbb{A}^n(k)) = (0)$, which is a prime ideal, and hence $\mathbb{A}^n(k)$ is irreducible. □

Exercise 1.11.29. Let $k = \mathbb{R}$.

(a) Show that $I(V(X^2 + Y^2 + 1)) = (1)$.

(b) Show that every algebraic subset of $\mathbb{A}^2(\mathbb{R})$ is equal to $V(F)$ for some $F \in \mathbb{R}[X, Y]$.

This indicates why we usually require k to be algebraically closed.

Solution.

(a) Note that $V(X^2+Y^2+1) = \emptyset$ since $X^2+Y^2 = -1$ admits no solution in $\mathbb{R}\times\mathbb{R}$. Hence, $I(V(X^2+Y^2+1)) = \mathbb{R}[X,Y] = (1)$.

(b) Let V be an algebraic subset of $\mathbb{A}^2(\mathbb{R})$ given as $V = V(f_1,\ldots,f_n)$ for $f_1,\ldots,f_n \in \mathbb{R}[X,Y]$. Consider $F = f_1^2+\cdots+f_n^2 \in \mathbb{R}[X,Y]$. Then if $P \in V(f_1,\ldots,f_n)$, then $F(P) = \sum_{i=1}^n f_i(P)^2 = 0$, and hence $P \in V(F)$. Conversely, if $P \in V(F)$ then $0 = F(P) = \sum_{i=1}^n f_i(P)^2 \implies f_i(P) = 0\ \forall i \in [n]$, and thus $P \in V(f_1,\ldots,f_n)$. Hence, $V(F) = V(f_1,\ldots,f_n) = V$.

□

Exercise 1.11.30.

(a) Decompose $V(X^2+Y^2-1, X^2-Z^2-1) \subseteq \mathbb{A}^3(\mathbb{C})$ into irreducible components.

(b) Let $V = \{(t,t^2,t^3) \in \mathbb{A}^3(\mathbb{C}) | t \in \mathbb{C}\}$. Find $I(V)$, and show that V is irreducible.

Solution.

(a) Let $f_1 = X^2+Y^2-1$ and $f_2 = X^2-Z^2-1$. Now, $f_1-f_2 = Y^2+Z^2 = (Y+iZ)(Y-iZ)$. Hence,

$$V(f_1,f_2) = V(f_1,f_2,Y+iZ) \cup V(f_1,f_2,Y-iZ).$$

Let us now look at the component $V(f_1,f_2,Y-iZ)$. Here, $Y = iZ \implies Y^2 = -Z^2$. Now $f_2 = 0 \iff X^2-Z^2-1 = 0$ in this component. Similarly, $f_1 = 0 \iff X^2-Z^2-1 = 0$ in this component. Thus

$$V(f_1,f_2,Y-iZ) = V(Y-iZ, X^2-Z^2-1).$$

Similarly, it can be easily seen that

$$V(f_1,f_2,Y+iz) = V(Y+iZ, X^2-Z^2-1).$$

Now, define

$$I_- = (Y-iZ, X^2-Y^2-1), \quad I_+ = (Y+iZ, Y^2-X^2-1).$$

We show that $I_\pm$ are prime, which would then establish that $V(I_+)$ and $V(I_-)$ are the required irreducible components (since $V(I_+) \neq V(I_-)$ and neither is contained in the other).
In $\mathbb{C}[X,Y,Z]/(Y-iZ) \cong \mathbb{C}[X,Z]$, the image of X^2-Y^2-1 is $X^2+(Z^2-1)$. Treating this as a polynomial in X, the discriminant is $4(1-Z^2)$ which is not a square in $\mathbb{C}[Z]$, and hence X^2+Z^2-1 is irreducible in $\mathbb{C}[X,Z]$ and thus (X^2+Z^2-1) is

prime in $\mathbb{C}[X,Y,Z]/(Y-iZ)$, and by pulling back, $I_- = (X^2+Z^2-1, Y-iZ)$ is prime in $\mathbb{C}[X,Y,Z]$.
Similarly, I_+ is seen to be prime in $\mathbb{C}[X,Y,Z]$. Hence, $V(I_+), V(I_-)$ are the required irreducible components.

(b) Let $I = (Y-X^2, Z-X^3)$. Then $\mathbb{C}[X,Y,Z]/I \cong \mathbb{C}[X]$, which is an integral domain, so I is a prime ideal and hence is also a radical ideal. Now, $V(I) = V$, so V is irreducible. Moreover, by Hilbert's Nullstellensatz, $I(V) = I(V(I)) = \text{rad}I = I$, since I is radical. Thus, $I(V) = (Y-X^2, Z-X^3)$.

□

Exercise 1.11.31. Let R be a UFD.

(a) Show that a monic polynomial of degree two or three in $R[X]$ is irreducible if and only if it has no roots in R.

(b) The polynomial $X^2 - a \in R[X]$ is irreducible if and only if a is not a square in R.

Solution.

(a) $\underline{\implies:}$
We show the contrapositive. Let $P \in R[X]$ be a monic polynomial of degree two or three with a root $\alpha \in R$. Then $(X-\alpha)|P$ and hence P is reducible.
$\underline{\impliedby:}$
We prove the contrapositive. If $P \in R[X]$ is a monic reducible polynomial of degree two or three, it must have a linear factor, say $(X-\alpha)$. Then α is a root of P.

(b) $\underline{\implies:}$
We prove the contrapositive. If $a = b^2$ where $b \in R$, then $X^2 - a = X^2 - b^2 = (X-b)(X+b)$ and thus $X^2 - a$ is reducible.
$\underline{\impliedby:}$
We prove the contrapositive. Let $X^2 - a = (X+\alpha)(X+\beta)$ for $\alpha, \beta \in R$. Then $X^2 - a = X^2 + (\alpha+\beta)X + \alpha\beta$. Thus, $\alpha + \beta = 0 \implies \beta = -\alpha$ and $\alpha\beta = -a \implies -\beta^2 = -a \implies a = \beta^2$, which shows that a is a square in R.

□

Exercise 1.11.32. Show that $V(Y^2 - X(X-1)(X-\lambda)) \subseteq \mathbb{A}^2(k)$ is an irreducible curve for any algebraically closed field k, and any $\lambda \in k$.

Solution. We show that $Y^2 - X(X-1)(X-\lambda)$ is irreducible. Since k is algebraically closed, this would establish that $V(Y^2 - X(X-1)(X-\lambda))$ would be an irreducible curve. If a polynomial $Y^2 - f(X)$ is reducible, we show that $f(X)$ must be a square in $k[X]$. To see this, assume that $Y^2 - f(X) = (Y - p(X))(Y - q(X))$ for $p(X), q(X) \in k[X]$. Then

$$Y^2 - f(X) = Y^2 - (p(X) + q(X))Y + p(X)q(X),$$

which shows that $p(X) + q(X) = 0 \implies q(X) = -p(X)$. Hence, $f(X) = -p(X)q(X) = p(X)^2$.
Now, $X(X-1)(X-\lambda)$ has is of degree 3, and hence cannot be a square in $k[X]$. Thus $V(Y^2 - X(X-1)(X-\lambda))$ is an irreducible curve in $\mathbb{A}^2(k)$. □

Exercise 1.11.33. Let $I = (Y^2 - X^2, Y^2 + X^2) \subseteq \mathbb{C}[X, Y]$. Find $V(I)$ and $\dim_{\mathbb{C}}(\mathbb{C}[X, Y]/I)$.

Solution. Let $(x, y) \in V(I)$. Then $x^2 - y^2 = 0 \implies x = \pm y$. Since $x^2 + y^2 = 0$, substituting $x = \pm y$, we get that $2y^2 = 0 \implies y = 0 \implies x = 0$. Thus $V(I) = \{(0, 0)\}$.
Note that $X^2, Y^2 \in I$, so $\overline{X}^2 = \overline{Y}^2 = 0 \in \mathbb{C}[X, Y]/I$. Also any non-zero term in I has degree at least two. Hence, any element of $\mathbb{C}[X, Y]/I$ is of the form $a + b\overline{X} + c\overline{Y} + d\overline{XY}$ for $a, b, c, d \in \mathbb{C}$. Thus, $\{1, \overline{X}, \overline{Y}, \overline{XY}\}$ forms a $\mathbb{C}$-basis of $\mathbb{C}[X, Y]/I$ and hence $\dim_{\mathbb{C}}(\mathbb{C}[X, Y]/I) = 4$. □

Exercise 1.11.34. Let K be any field, $F \in K[X]$ a polynomial of degree $n > 0$. Show that the residues $\overline{1}, \overline{X}, \ldots, \overline{X}^{n-1}$ form a basis of $K[X]/(F)$ over K.

Solution. Let $F = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$ where $a_n \neq 0$. Then

$$\overline{X}^n = -\frac{a_{n-1}}{a_n}\overline{X}^{n-1} - \cdots - \frac{a_0}{a_n}$$

and thus $\overline{1}, \overline{X}, \ldots, \overline{X}^{n-1}$ span $K[X]/(F)$ over K.
Let $G = c_0\overline{1} + c_1\overline{X} + \cdots + c_{n-1}\overline{X}^{n-1} \in K[X]/(F)$. If $G = 0$, then $F | c_0 + c_1 X + \cdots + c_{n-1}X^{n-1}$. But F is a degree-n polynomial, so we must then have $c_0 = c_1 = \cdots = c_{n-1} = 0$, and thus $\overline{1}, \overline{X}, \ldots, \overline{X}^{n-1}$ are linearly independent over K. □

Exercise 1.11.35. Let $R = k[X_1, \ldots, X_n]$, k algebraically closed, $V = V(I)$. Show that there is a natural one-to-one correspondence between algebraic subsets of V and radical ideals in $k[X_1, \ldots, X_n]/I$, and that irreducible algebraic sets (resp. points) correspond to prime ideals (resp. maximal ideals).

Solution. An algebraic subset of V is a subset $W \subseteq V$ of the form $W = V(S) \cap V$, for some set $S \subseteq k[X_1, \ldots, X_n]$. But, $V(S) \cap V(I) = V((S) + I)$, and hence any algebraic subset of V is of the form $V(J)$ for some ideal $J \supseteq I$. Conversely, if $J \supseteq I$, then $V(J) \subseteq V(I)$. Hence, there is a correspondence between algebraic subsets $W \subseteq V$ and ideal J of such that $I \subseteq J$. Define a map

$$\Phi : \{\text{algebraic subsets } W \subseteq V\} \to \{\text{radical ideals in } R/I\}, \quad W \mapsto I(W)/I$$

The map is well-defined since $I(W)$ is radical, and hence $I(W)/I$ is also radical. We also have a map

$$\Psi : \{\text{radical ideals in } R/I\} \to \{\text{algebraic subsets } W \subseteq V\}, \quad J \mapsto V(\pi^{-1}(J)),$$

where $\pi : k[X_1, \ldots, X_n] \twoheadrightarrow k[X_1, \ldots, X_n]/I$ is the natural surjection map. Note that $\Psi(\Phi(W)) = V(\pi^{-1}(I(W)/I)) = V(I(W)) = W$ and $\Phi(\Psi(J)) = I(V(\pi^{-1}(J)))/I = \pi^{-1}(J)/I = J$ since $\pi^{-1}(J)$ is radical as J is radical. This shows that Φ is a bijection.

The correspondence $J \leftrightarrow \pi(J)$ preserves primeness and maximality, and hence the irreducible algebraic subsets of V correspond to prime ideals in $k[X_1, \ldots, X_n]/I$ and the points of V correspond to maximal ideal in $k[X_1, \ldots, X_n]/I$. □

Exercise 1.11.36.

(a) Let R be a UFD, and let $P = (t)$ be a principal, proper, prime ideal. Show that there is no prime ideal Q such that $0 \subset Q \subset P$, $Q \neq 0$, $P \neq Q$.

(b) Let $V = V(F)$ be an irreducible hypersurface in $\mathbb{A}^n$. Show that there is no irreducible algebraic set W such that $V \subset W \subset \mathbb{A}^n$, $W \neq V$, $W \neq \mathbb{A}^n$.

Solution.

(a) Since (t) is a non-zero prime ideal in a UFD, t is also irreducible. Now, assume to the contrary that such a Q exists. Pick any $0 \neq x \in Q$. Since $x \in (t)$, we have that $t|x$. Let $x = t^m u$, where $m \geq 1$ and $t \nmid u$ (this is possible since R is a UFD). Hence $t^m u \in Q$. Since Q is prime, either $u \in Q$ or $t^{m-1}u \in Q$. Continuing this way, we have that either $t \in Q$ or $u \in Q$. Now if $u \in Q \implies u \in (t) \implies t|u$, which is a contradiction. On the other hand, if $t \in Q$, then $(t) \subseteq Q$ which is again a contradiction! Hence, such a prime ideal Q cannot exist.

(b) Assume to the contrary that $V \subset W \subset \mathbb{A}^n$ holds and that $W = V(Q)$ is an irreducible algebraic subset, where Q is a prime ideal. We thus have that $V \subset W \implies I(W) \subset I(V) \implies Q \subset (F)$. But we know from part (a) that it is not possible unless $G = 0$ which would then imply $W = V(0) = \mathbb{A}^n$ which cannot be true.

□

Exercise 1.11.37. Let $I = (X^2 - Y^3, Y^2 - Z^3) \subseteq k[X, Y, Z]$. Define $\alpha : k[X, Y, Z] \to k[T]$ by $\alpha(X) = T^9, \alpha(Y) = T^6, \alpha(Z) = T^4$.

(a) Show that every element of $k[X, Y, Z]/I$ is the residue of an element $A + XB + YC + XYD$, for some $A, B, C, D \in k[Z]$.

(b) If $F = A + XB + YC + XYD$, $A, B, C, D \in k[Z]$, and $\alpha(F) = 0$, compare like powers of T to conclude that $F = 0$.

(c) Show that $\ker(\alpha) = I$, so I is prime, $V(I)$ is irreducible, and $I(V(I)) = I$.

Solution.

(a) Let $R = k[X, Y, Z]/I$. In R, we have that $X^2 = Y^3$ and $Y^2 = Z^3$. Consider a monomial $X^a Y^b Z^c$. Write $a = 2q + r$, where $r \in \{0, 1\}$. Then we have that $X^a Y^b Z^c = X^r Y^{3q+b} Z^c$. Write $3q + b = 2s + t$, where $t \in \{0, 1\}$. Then we have that $X^r Y^{3q+b} Z^c = X^r Y^t Z^{3s+c}$. Thus, $X^a Y^b Z^c = X^r Y^t Z^{3s+c}$ with $r, t \in \{0, 1\}$. Hence, every element of R is a $k[Z]$-linear combination of $1, X, Y, XY$, that is, it has a representative of the form

$$A(Z) + B(Z)X + C(Z)Y + D(Z)XY, \quad A, B, C, D \in k[Z].$$

(b) We have that

$$\begin{aligned} 0 = \alpha(F) &= A(\alpha(Z)) + \alpha(X)B(\alpha(Z)) + \alpha(Y)C(\alpha(Z)) + \alpha(X)\alpha(Y)D(\alpha(Z)) \\ &= A(T^4) + T^9 B(T^4) + T^6 C(T^4) + T^{15} D(T^4). \end{aligned}$$

Now, every term in $A(T^4)$ has degree $0 \pmod 4$. Every term in $T^9 B(T^4)$ has degree $1 \pmod 4$. Every term in $T^6 C(T^4)$ has degree $2 \pmod 4$. Every term in $T^{15} D(T^4)$ has degree $3 \pmod 4$. Hence, there can be no cross-cancellation amidst these terms, and we must have $A = B = C = D = 0$, and hence $F = 0$.

(c) Firstly, $I \subseteq \ker \alpha$ is clear. Thus, it follows that the map α factors as $\bar{\alpha} \circ \pi$, where $\pi : k[X,Y,Z] \twoheadrightarrow k[X,Y,Z]/I$ is the natural surjection. To show $I = \ker \alpha$, it suffices to show that $\bar{\alpha}$ is an inclusion. But this is clear from (b).

Now, $k[T]$ is an integral domain, and hence $\alpha(k[X,Y,Z]) \cong k[X,Y,Z]/\ker \alpha = k[X,Y,Z]/I$ is an integral domain, which implies that I is prime, and hence $V(I)$ is irreducible since k is algebraically closed. As I is prime, it is radical, and hence $I(V(I)) = I$.

□

Exercise 1.11.38. If S is module-finite over R, then S is ring-finite over R.

Solution. Let $\{s_1, \ldots, s_n\}$ be generators of S as an R-module. Then $S = R[s_1, \ldots, s_n]$ too and hence is ring-finite over R. □

Exercise 1.11.39. Show that $S = R[X]$ (the ring of polynomials in one variable) is ring-finite over R, but not module-finite.

Solution. Since $S = R[X]$, by definition, it is ring-finite over R.
Assume to the contrary that S is also module-finite over R. Let $\{s_1, \ldots, s_n\}$ be generators of S as a module over R. Let $N = \max_{i \in [n]}\{\deg s_i\}$. Then the degree of any element $\sum_{i=1}^{n} r_i s_i$ for $r_i \in R$ is at most N. Thus X^{N+1} is not an element of the submodule generated by $\{s_1, \ldots, s_n\}$ but $X^{N+1} \in S$, leading us to a contradiction! □

Exercise 1.11.40. If L is ring-finite over K, (K, L fields) then L is a finitely generated field extension of K.

Solution. Say $L = K[\ell_1, \ldots, \ell_n]$. Since, $K[\ell_1, \ldots, \ell_n] \subseteq K(\ell_1, \ldots, \ell_n)$, we have that $L \subseteq K(\ell_1, \ldots, \ell_n) \subseteq L \implies L = K(\ell_1, \ldots, \ell_n)$. Thus L is a finitely generated field extension of K. □

Exercise 1.11.41. Show that $L = K(X)$ (the field of rational functions in one variable) is a finitely generated field extension of K, but L is not ring-finite over K.

Solution. Since $L = K(X)$, L is a finitely generated field extension of K by definition.
Assume to the contrary that L is ring-finite over K, say $L = K[Q_1, \ldots, Q_n]$. Let $B \in K[X]$ denote the lowest common multiple of all the denominators of Q_i. Then for every element $Q \in L$, there exists an $n \in \mathbb{N}$ such that $B^n Q \in K[X]$. Since $K[X]$ has infinitely many monic irreducible polynomials, choose one such monic irreducible $C \in K[X]$ which does not divide B (since B can have at most finitely many irreducible factors) and let $Q = 1/C$. Now there exists an $n \in \mathbb{N}$ such that $B^n Q \in k[X]$, say $B^n Q = G$. Then $B^n = CG \implies C | B^n$. But C is irreducible, so $C|B$, which is a contradiction. □

Exercise 1.11.42. Let R be a subring of S, S a subring of T.

(a) If $S = \sum Rv_i$, $T = \sum Sw_j$, show that $T = \sum Rv_iw_j$.

(b) If $S = R[v_1, \ldots, v_n]$, $T = S[w_1, \ldots, w_m]$, show that $T = R[v_1, \ldots, v_n, w_1 \ldots, w_m]$.

(c) If R, S, T are fields, and $S = R(v_1, \ldots, v_n)$, $T = S(w_1, \ldots, w_n)$, show that $T = R(v_1, \ldots, v_n, w_1, \ldots, w_m)$.

So each of the three finiteness conditions is a transitive relation.

Solution.

(a) Clearly, $\sum Rv_iw_j \subseteq T$. Now, let $x \in T$. Then $x = \sum_{j=1}^{m} s_jw_j$ for some $s_j \in S$. Furthermore, we must have that $s_j = \sum_{i=1}^{n_j} r_{ji}v_i$ for some $r_{ji} \in R$. Hence,

$$x = \sum_{j=1}^{m}\sum_{i=1}^{n_j} r_{ji}v_i \implies T \subseteq \sum Rv_iw_j.$$

(b) Clearly, $R[c_1, \ldots, v_n, w_1, \ldots, w_m] \subseteq T$. Now, let $f \in T$. Then f is a polynomial in $w_1, \ldots, w_m$ with coefficients from S. But each coefficient of S is a polynomial in $v_1, \ldots, v_n$ with coefficients from R. Expanding out, we get that f must be a polynomial in $v_1, \ldots, v_n, w_1, \ldots, w_m$ with coefficients in R. Hence $T \subseteq R[v_1, \ldots, v_n, w_1, \ldots, w_m]$.

(c) Clearly, $R(v_1, \ldots, v_m, w_1, \ldots, w_n) \subseteq T$. Now, let $f \in T$. Then f can be expressed as a quotient of two polynomials in $w_1, \ldots, w_m$ with coefficients from S. But each coefficient of S is a quotient of polynomials in $v_1, \ldots, v_n$ with coefficients from R. Clearing out denominators in both the numerator and denominator in the expression of f, we obtain that f can be expressed as a quotient of polynomials in $v_1, \ldots, v_n, w_1, \ldots, w_m$ with coefficients from R. Hence, $T \subseteq R(v_1, \ldots, v_n, w_1, \ldots, w_m)$.

□

Exercise 1.11.43. Let R be a subring of S, S a subring of (a domain) T. If S is integral over R, and T is integral over S, show that T is integral over R.

Solution. Let $t \in T$. Since t is integral over S, we have that $t^n + s_1t^{n-1} + \cdots s_n = 0$ for some $n \in \mathbb{N}$ and $s_1, \ldots, s_n \in S$. Consider the ring $R[s_1, \ldots, s_n][t]$ which is module-finite over $R[s_1, \ldots, s_n]$ since t is integral over $R[s_1, \ldots, s_n]$. Thus $R[s_1, \ldots, s_n, t]$ is module-finite over R and since $t \in R[s_1, \ldots, s_n, t]$, we must have t is integral over R. Since $t \in T$ was arbitrary, T is integral over R. □

Exercise 1.11.44. Suppose (a domain) S is ring-finite over R. Show that S is module-finite over R if and only if S is integral over R.

Solution. For the forward direction, assume that S is module-finite over R. Take any $s \in S$. Since s is contained in a module finite extension of R, namely S, it must be the case that s is integral over R. Since $s \in S$ was arbitrary, this shows that S is integral over R.
Conversely, let $S = R[s_1, \ldots, s_m]$ be ring-finite over R and integral over R. Take $S_1 = R[s_1]$, and let

$$s_1^n + r_1 s_1^{n-1} + \cdots + r_n = 0 \implies s_1^n = -r_1 s_1^{n-1} - \cdots - r_n,$$

and multiplying by suitable powers of s_1, shows that $R[s_1]$ is generated as module finite extension with generators $s_1, \ldots, s_1^{n-1}$. Hence $R[s_1]$ is module-finite over R. Similarly, $R[s_1, s_2] = R[s_1][s_2]$ is module-finite over $R[s_1]$, and hence over R. Continuing this way, we obtain that $R[s_1, \ldots, s_m]$ is module-finite over R. □

Exercise 1.11.45. Let L be a field, k an algebraically closed subfield of L.

(a) Show that any element of L that is algebraic over k is already in k.

(b) An algebraically closed field has no module-finite field extensions except itself.

Solution.

(a) Let $x \in L$ be algebraic over k. Since x is algebraic over k, it is integral over k. Hence, we have an equation

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

Since k is algebraically closed, it contains all roots of polynomials of $k[X]$, and thus $x \in k$.

(b) Let M/k be a module-finite field extension such that $M \neq k$. Let $x \in M \setminus k$. Consider the ring $k[x]$. Now, $k[x]$ is module-finite over k since x is contained in M, which is a module-finite extension of k. Hence, $k[x]$ must be integral over k. That would imply that x is a root of some monic polynomial with coefficients in k, that is, x is algebraic over k, but that would imply that $x \in k$ since k is algebraically closed, which is a contradiction! Hence, an algebraically closed field has no module-finite field extensions except itself.

□

Exercise 1.11.46. Let K be a field, $L = K(X)$ the field of rational functions in one variable over K.

(a) Show that any element of L that is integral over $K[X]$ is already in $K[X]$.

(b) Show that there is no nonzero element $F \in K[X]$ such that for every $z \in L$, $F^n z$ is integral over $K[X]$ for some $n > 0$.

Solution.

(a) Since, K is a field, $K[X]$ is a UFD, and $L = K(X)$ is the fraction field of $K[X]$. Let $f/g \in L$, where $f, g \in K[X]$ and f, g have no irreducible factors in common. Suppose that f/g is integral over $K[X]$. If g is a unit of $K[X]$, then $f/g \in K[X]$. If not, let π denote an irreducible element of $K[X]$ which divides g but not f. Since f/g is integral over $K[X]$, we have an equation

$$\left(\frac{f}{g}\right)^n + p_1 \left(\frac{f}{g}\right)^{n-1} + \cdots + p_n = 0, \quad p_i \in K[X].$$

Multiplying by g^n, we get that

$$f^n + p_1 g f^{n-1} + \cdots + p_n n g^n = 0.$$

But π divides the RHS, and hence must divide the LHS. However, π does not divide f^n, but divides every other term on the LHS, hence it cannot divide the LHS. This leads to a contradiction, and hence g cannot be a non-unit.

(b) We fill find a z such that $F^n z$ is not integral over $K[X]$ for any $n > 0$, which will yield to us a contradiction on the assumption that such an $F \in K[X]$ exists. Note that $F^n z$ being integral over $K[X]$ is equivalent to $F^n z \in K[X]$ by part (a). If F is a constant polynomial, then $F^n z \in K[X] \implies z \in K[X]$, and hence taking any $z \in L \setminus K[X]$ would gives us the required contradiction.
Now assume that F is non-constant. Then $F + 1$ is also non-constant, and admits an irreducible factor π. Now $\pi \nmid F$, since if $\pi \mid F$, then $\pi | (F + 1) - F \implies \pi | 1$, which is not possible. Let $z = 1/\pi$. Say that $F^n z \in K[X]$ for some $n > 0$. Now, $F^n z = F^n/\pi$ and since $\pi \nmid F$ and π is irreducible, we have that $\pi \nmid F^n$, and hence $F^n/\pi \notin K[X]$, which immediately results in a contradiction.

□

Exercise 1.11.47. Let K be a subfield of a field L.

(a) Show that the set of elements of L that are algebraic over K is a subfield of L containing K.

(b) Suppose L is module-finite over K, and $K \subseteq R \subseteq L$. Show that R is a field.

Solution.

(a) Since the set of elements of L that are algebraic over K is the set of elements of L integral over K, and the set of elements of L integral over K form a ring, we have that the set of elements of L algebraic over K forms a ring containing K. Now let α be a non-zero element of L algebraic over K. We now show that α^{-1} is also algebraic over K, and hence this will establish that the set of elements of L algebraic over K forms a field.
Since α is algebraic over K, we have an equation

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

Dividing throughout by $a_n\alpha^n$ gives us that

$$\left(\frac{1}{\alpha}\right)^n + \frac{a_{n-1}}{a_n}\left(\frac{1}{\alpha}\right)^{n-1} + \cdots + \frac{1}{a_n} = 0,$$

which shows that a^{-1} is also algebraic over K.

(b) Since R is contained in L, which is module-finite over K, it must be the case that R is integral over K. Take any $0 \neq r \in R$. Since r is integral over K, we have an equation

$$r^n + a_1 r^{n-1} + \cdots + a_n = 0, \quad a_i \in K, a_n \neq 0.$$

Now, note that

$$r(r^{n-1} + a_1 r^{n-2} + \cdots + a_1) + a_n = 0 \implies r^{-1} = -(a_n^{-1}r^{n-1} + \cdots + a_n^{-1}a_1)$$

and since K is a field and $0 \neq a_n \in K$, we have that $a_n^{-1} \in K \subseteq R$. Thus, $r^{-1} \in R$ and hence R is a field.

□

Exercise 1.11.48. Let K be a field, $F \in K[X]$ an irreducible monic polynomial of degree $n > 0$.

(a) Show that $L = K[X]/(F)$ is a field, and if x is the residue of X in L, then $F(x) = 0$.

(b) Suppose L' is a field extension of K, $y \in L'$ such that $F(y) = 0$. Show that the homomorphism from $K[X]$ to L' that takes X to y induces an isomorphism of L with $K(y)$.

(c) With L', y as in (b), suppose $G \in K[X]$ and $G(y) = 0$. Show that F divides G.

(d) Show that $F = (X - x)F_1$, $F_1 \in L[X]$.

Solution.

(a) Since $K[X]$ is a PID, since F is irreducible, (F) is a non-zero prime ideal, and hence a maximal ideal (since every non-zero prime ideal in a PID is maximal). Thus, $L = K[X]/F$ is a field. Let $\pi : K[X] \twoheadrightarrow L$ be the natural quotient map. Then $\pi(F) = F(\pi(X)) = F(x)$. But $\pi(F) = 0$ since $F \in (F)$, and hence $F(x) = 0$.

(b) Define the evaluation homomorphism $\mathrm{ev}_y : K[X] \to L'$ by $\mathrm{ev}_y : G(X) \mapsto G(y)$. Since $F(y) = 0$, $(F) \subseteq \ker \mathrm{ev}_y$. Hence ev_y factors through the quotient $K[X]/(F)$ giving a map

$$\overline{\mathrm{ev}_y} : K[X]/(F) \to L', \quad \overline{G} \mapsto G(y).$$

Since $\overline{\mathrm{ev}_y}$ is a homomorphism of fields, it is injective and the image of $\overline{\mathrm{ev}_y}$ is $K[y]$. But y is algebraic over K (since $F(y) = 0$), so $K[y] = K(y)$. This shows that $L \cong K(y)$ sending $\overline{X} \mapsto y$.

(c) Let d be the GCD of F and G in the PID $K[X]$. If $F|G$, we are done. If not, then since F is irreducible, we have that $\gcd(F, G) = 1$. Hence, we can find $A, B \in K[X]$ such that $AF + BG = 1$. Evaluating at y, we have that $A(y)F(y) + B(y)G(y) = 1 \implies 0 = 1$, which is absurd. Hence $F|G$ must have been the case.

(d) Consider F as a polynomial in $L[X]$ via the standard inclusion $K \hookrightarrow L$. We have $F(x) = 0$ in L. Hence, via the division algorithm, there must be an $F_1 \in L[X]$ such that $F = (X - x)F_1$.

□

Exercise 1.11.49. Let K be a field, $F \in K[X]$ be monic. Show that there is a field L containing K such that $F = \prod_{i=1}^{n}(X - x_i) \in L[X]$. L is called a *splitting field* of F.

Solution. Let $n = \deg F$. We proceed by induction on n.
If $n = 0$, then Fs splits trivially in K, and hence $L = K$ suffices. If $n = 1$, then say $F = X + b$, then $F = (X - (-b))$, and we can take $L = K$.
Now assume that $\deg F = n \geq 2$ and assume that the statement holds true for all

polynomials of degree less than n. Choose a monic irreducible factor f of F with $\deg f \geq 1$, and let $F = f \cdot G$ for some $G \in K[X]$. Let $L_1 = K[X]/(f)$. Then, we can find an $x_1 \in L_1[X]$ such that $F = (X - x_1)H(x)$ in $L_1[X]$ for some $H \in L_1[X]$. Since $\deg H = n - 1$, by the induction hypothesis there is a field $L \supseteq L_1$ where $H = \prod_{i=2}^{n}(X - x_i)$. Thus, in L, we have that $F = \prod_{i=1}^{n}(X - x_i) \in L[X]$. □

Exercise 1.11.50. Suppose K is a field of characteristic zero, F an irreducible monic polynomial in $K[X]$ of degree $n > 0$. Let L be a splitting field of F, so $F = \prod_{i=1}^{n}(X - x_i)$, $x_i \in L$. Show that the x_i are distinct.

Solution. When $\mathrm{char}F = 0$, note that if F has a repeated root, say x, then F' also has x as a root. Thus $(X - x)|\gcd(F, F')$. In particular, if $\gcd(F, F') = 1$, F cannot admit a repeated root. Let $\deg F > 1$, then $\deg F' = n - 1$ (this is where we used the fact that $\mathrm{char}K = 0$), and hence it is not possible that $F|F'$. Since F is irreducible, it must be the case that $\gcd(F, F') = 1$. Thus, F does not admit any repeated roots in a splitting field, and thus all the x_i are distinct. □

Exercise 1.11.51. Let R be a domain with quotient field K, and let L be a finite algebraic extension of K.

(a) For any $v \in L$, show that there is a nonzero $a \in R$ such that av is integral over R.

(b) Show that there is a basis $v_1, \ldots, v_n$ for L over K (as a vector space) such that each v_i is integral over R.

Solution.

(a) Since v is algebraic over K, we have an equation

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

Let $a_i = p_i/q_i$ for $p_i, q_i \in R$. Let $a = \prod_{i=1}^{n} q_i$. Then multiplying throughout by a^n, we get an monic polynomial in av with coefficients from R, and hence av is integral over R.

(b) Let $v_1', \ldots, v_n'$ be a basis for L over K. By part (a), we can find $0 \neq a_i \in R$ such that $v_i = a_i v_i'$ is integral over R. Thus, $v_1, \ldots, v_n$ forms a basis for L over K such that each v_i is integral over R.

□

Chapter 2

Affine Varieties

From now on, k will be a fixed algebraically closed field. By a variety we shall mean an irreducible algebraic set in $\mathbb{A}^n(k)$.

2.1 Coordinate Ring of a Variety

Let $V \subset \mathbb{A}^n$ be a non-empty variety. Then $I(V)$ is a prime ideal in $k[X_1, \ldots, X_n]$ and so $k[X_1, \ldots, X_n]/I(V)$ is a domain.

Definition 2.1.1 (Coordinate Ring)**.** *We let* $\Gamma(V) = k[X_1, \ldots, X_n]/I(V)$ *and call this the* ***coordinate ring*** *of* V*.*

For a non-empty set V, we let $\mathcal{F}(V, k)$ denote the set of all maps from $V \to k$. This is a ring in the usual way: if $f, g \in \mathcal{F}(V, k)$ then $(f + g)(P) := f(P) + g(P)$ and $(fg)(P) = f(P)g(P)$. We have the subring $k \subset \mathcal{F}(V, k)$ which consists of all constant functions.

Lemma 2.1.2. *The map that associates to each* $F \in k[X_1, \ldots, X_n]$ *a polynomial function in* $\mathscr{F}(V, k)$ *is a ring homomorphism whose kernel is* $I(V)$*.*

Proof. Define the map $\Phi : k[X_1, \ldots, X_n] \longrightarrow \mathscr{F}(V, k)$ by sending a polynomial F to the function $\Phi(F) : V \to k$, such that $\Phi(F)(a_1, \ldots, a_n) = F(a_1, \ldots, a_n)$. We first show that Φ is a ring homomorphism. For $F, G \in k[X_1, \ldots, X_n]$ and $a \in V$, we have

$$\Phi(F + G)(a) = (F + G)(a) = F(a) + G(a) = \Phi(F)(a) + \Phi(G)(a),$$

so $\Phi(F + G) = \Phi(F) + \Phi(G)$. Similarly,

$$\Phi(FG)(a) = (FG)(a) = F(a)G(a) = \Phi(F)(a)\Phi(G)(a),$$

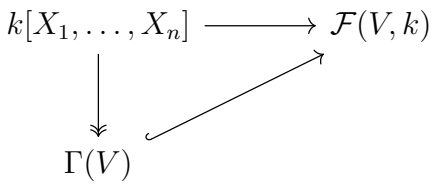
hence $\Phi(FG) = \Phi(F)\Phi(G)$. Finally, $\Phi(1)$ is the constant function 1. Thus Φ is a ring homomorphism. Next, we determine the kernel of Φ. By definition,

$$F \in \ker(\Phi) \iff \Phi(F)(a) = 0 \text{ for all } a \in V \iff F(a) = 0 \text{ for all } a \in V.$$

This is precisely the definition of the ideal $I(V)$ of polynomials vanishing on V. Therefore, $\ker(\Phi) = I(V)$. Hence, the map $I(V)$ is the kernel of the ring homomorphism Φ. □

2.2 Polynomial Functions and Maps

A function $f \in \mathcal{F}(V, k)$ is called a **polynomial function** if there is a polynomial $F \in k[X_1, \ldots, X_n]$ such that $F(P) = f(P)$ for all $P \in V$. In other words, given a polynomial, it defines a function from $\mathbb{A}^n$ to k. We may restrict this function to V. This defines a ring homomorphism $k[X_1, \ldots, X_n] \to \mathcal{F}(V, k)$ whose image is exactly the set of polynomial functions. If $F, G \in k[X_1, \ldots, X_n]$ then they agree on V iff $F - G \in I(V)$. Thus, we have a commutative diagram:



Note that $\Gamma(V) \subset \mathcal{F}(V, k)$ is a subring. We will use this later.

Definition 2.2.1 (Polynomial Map)**.** *Let $V \subset \mathbb{A}^n$ and $W \subset \mathbb{A}^m$ be algebraic subsets. A map of sets $\phi : V \to W$ is called a **polynomial map** if there exist polynomials $T_1, \ldots, T_m \in k[X_1, \ldots, X_n]$ such that*

$$\phi(a_1, \ldots, a_n) = (T_1(a_1, \ldots, a_n), \ldots, T_m(a_1, \ldots, a_n)).$$

Any map of sets $\phi : V \to W$ induces a map $\tilde{\phi} : \mathcal{F}(W, k) \to \mathcal{F}(V, k)$, which is given by $(f : W \to k) \mapsto (f \circ \phi : V \to k)$. It is easily seen that $\tilde{\phi}$ is a ring homomorphism.

We claim that if ϕ is a polynomial map, then $\tilde{\phi} : \mathcal{F}(W, k) \to \mathcal{F}(V, k)$ maps the subset $\Gamma(W)$ to $\Gamma(V)$, that is, $\tilde{\phi}(\Gamma(W)) \subset \Gamma(V)$.

Suppose $f \in \Gamma(W)$. Then there is a polynomial $F(Y_1, \ldots, Y_m) \in k[Y_1, \ldots, Y_m]$ such that $f(b_1, \ldots, b_m) = F(b_1, \ldots, b_m)$. Since ϕ is polynomial, it follows there exist $T_1, \ldots, T_m \in k[X_1, \ldots, X_n]$ such that

$$\phi(a_1, \ldots, a_n) = (T_1(a_1, \ldots, a_n), \ldots, T_m(a_1, \ldots, a_n)).$$

Thus,

$$f \circ \phi(a_1, \ldots, a_n) = F(T_1(a_1, \ldots, a_n), \ldots, T_m(a_1, \ldots, a_n)) .$$

This shows that $f \circ \phi$ is a polynomial map.

Proposition 2.2.2. *Let $V \subset \mathbb{A}^n$ and $W \subset \mathbb{A}^m$ be algebraic sets. Then there is a bijective correspondence between the set of polynomial maps $\phi : V \to W$ and the set of ring homomorphisms $\Gamma(W) \to \Gamma(V)$. Any polynomial map $\phi : V \to W$ is the restriction of a polynomial map from $\mathbb{A}^n \to \mathbb{A}^m$.*

Proof. Let $\mathcal{P}$ denote the set of polynomial maps from $V \to W$. Let $\mathcal{H}$ denote the set of ring homomorphisms from $\Gamma(W) \to \Gamma(V)$. We already have a map $\Psi : \mathcal{P} \to \mathcal{H}$, namely $\Psi(\phi) = \tilde{\phi}$.

Consider the map $\Theta : \mathcal{H} \to \mathcal{P}$ defined as follows. Let $\alpha : \Gamma(W) \to \Gamma(V)$ be a ring homomorphism. Consider the map $k[Y_1, \ldots, Y_m] \to \Gamma(W)$ and let $\bar{Y}_i$ denote the image of Y_i. Define a map $\phi : V \to \mathbb{A}^m$ as follows:

$$\phi(a_1, \ldots, a_n) = (\alpha(\bar{Y}_1)(a_1, \ldots, a_n), \alpha(\bar{Y}_2)(a_1, \ldots, a_n), \ldots, \alpha(\bar{Y}_m)(a_1, \ldots, a_n)).$$

The above map makes sense as $\alpha(\bar{Y}_i)$ are maps on V and so we can evaluate them at points on V to get a number. We claim that the image of ϕ lands inside W. To see this, it suffices to show that $\phi(V) \subset V(I(W))$, as this equals W, by Proposition 1.3.1 (9). Thus, we need to show that if $F \in I(W)$ then $F(\phi(V)) = 0$.

We need the following simple observations. Suppose $f_1, \ldots, f_m$ are m functions on W. Then we get the function $F(f_1, \ldots, f_m)$ on W. Notice that for a point $Q \in W$, the value of the function $F(f_1, \ldots, f_m)$ at the point Q is $F(f_1(Q), \ldots, f_m(Q))$. If the f_i are polynomial functions on W, then $F(f_1, \ldots, f_m)$ is a polynomial function on W. Let us assume that the f_i are polynomial functions. Since α is a ring homomorphism, it is clear that

$$\alpha(F(f_1, \ldots, f_m)) = F(\alpha(f_1), \ldots, \alpha(f_m)) .$$

If $P \in V$ is a point, then using the above, the following is clear

$$\alpha(F(f_1, \ldots, f_m))(P) = F(\alpha(f_1), \ldots, \alpha(f_m))(P) = F(\alpha(f_1)(P), \ldots, \alpha(f_m)(P)) .$$

Now let us put $f_i = \bar{Y}_i$ into the above equation. As $F \in I(W)$, this means that $F(\bar{Y}_1, \ldots, \bar{Y}_m) = 0$ in the ring $\Gamma(W)$. Thus, the function $\alpha(F(\bar{Y}_1, \ldots, \bar{Y}_m))$ equals 0 in $\Gamma(V)$ and so it evaluates to 0 at each point $p \in V$. But this shows that

$$F(\phi(P)) = F(\alpha(\bar{Y}_1)(P), \ldots, \alpha(\bar{Y}_m)(P)) = 0 \qquad \forall\ P \in V .$$

This proves that $\phi(P) \in W$.

Since $\alpha(\bar{Y}_i)$ are restrictions of polynomial functions on V, it follows that ϕ is a polynomial map. This defines the map $\Theta : \mathcal{H} \to \mathcal{P}$.

Let us check that $\Theta \circ \Psi(\phi) = \phi$.

$$\begin{aligned}\Theta \circ \Psi(\phi)(a_1, \ldots, a_n) &= \Theta(\tilde{\phi})(a_1, \ldots, a_n) \\ &= (\tilde{\phi}(\bar{Y}_1)(a_1, \ldots, a_n), \ldots, \tilde{\phi}(\bar{Y}_m)(a_1, \ldots, a_n))\end{aligned}$$

If $\phi(a_1, \ldots, a_n) = (T_1(a_1, \ldots, a_n), \ldots, T_m(a_1, \ldots, a_n))$ then, by the definition of $\tilde{\phi}$, $\tilde{\phi}(\bar{Y}_i)(a_1, \ldots, a_n) = T_i(a_1, \ldots, a_n)$. This shows that $\Theta \circ \Psi(\phi) = \phi$.

Let $\alpha : \Gamma(W) \to \Gamma(V)$ be a ring homomorphism. Let us check that $\Psi \circ \Theta(\alpha) = \alpha$.

$$\Psi(\Theta(\alpha)) = \widetilde{\Theta(\alpha)}.$$

Thus,

$$\Psi(\Theta(\alpha))(\bar{Y}_i) = \widetilde{\Theta(\alpha)}(\bar{Y}_i) = \bar{Y}_i \circ \Theta(\alpha).$$

Since

$$\Theta(\alpha)(a_1, \ldots, a_n) = (\alpha(\bar{Y}_1)(a_1, \ldots, a_n), \ldots, \alpha(\bar{Y}_m)(a_1, \ldots, a_n)),$$

it follows that

$$\bar{Y}_i \circ \Theta(\alpha) = \alpha(\bar{Y}_i).$$

Thus, $\Psi(\Theta(\alpha))(\bar{Y}_i) = \alpha(\bar{Y}_i)$. Since $\bar{Y}_i$ generate $\Gamma(W)$ it follows that $\Psi(\Theta(\alpha)) = \alpha$.

Thus, $\Psi \circ \Theta = Id$ and also $\Theta \circ \Psi = Id$. This completes the proof of the bijective correspondence.

Given a polynomial map $\phi : V \to W$, choose $T_1, \ldots, T_m \in k[X_1, \ldots, X_n]$ such that $\phi(a_1, \ldots, a_n) = (T_1(a_1, \ldots, a_n), \ldots, T_m(a_1, \ldots, a_n))$. Then T_i's define a polynomial map $\phi' : \mathbb{A}^n \to \mathbb{A}^m$ and clearly ϕ is the restriction of ϕ' to V.

This completes the proof of the Proposition. □

Definition 2.2.3 (Isomorphism of Varieties)**.** *Let $\phi : V \to W$ be a polynomial map. We say it is an **isomorphism** if there is a polynomial map $\phi' : W \to V$ such that $\phi \circ \phi' = Id_W$ and $\phi' \circ \phi = Id_V$.*

2.3 Coordinate Change

An **affine change of coordinates** on $\mathbb{A}^n$ is a polynomial map $T = (T_1, \ldots, T_n) : \mathbb{A}^n \to \mathbb{A}^n$ such that each T_i is a polynomial of degree 1.

We may write $T_i = \sum a_{ij} X_j + a_{i0}$. Note that

$$T(b_1, \ldots, b_n) = (a_{11}b_1 + \ldots + a_{1n}b_n + a_{10}, \ldots, a_{n1}b_1 + \ldots + a_{nn}b_n + a_{n0}).$$

We may write this as the composite of two maps:

$$\mathbb{A}^n \xrightarrow{T'} \mathbb{A}^n, \quad (b_1, \ldots, b_n) \mapsto (a_{11}b_1 + \ldots + a_{1n}b_n, \ldots, a_{n1}b_1 + \ldots + a_{nn}b_n)$$

and a translation

$$\mathbb{A}^n \xrightarrow{T''} \mathbb{A}^n, \quad (b_1, \ldots, b_n) \mapsto (b_1 + a_{10}, \ldots, b_n + a_{n0}).$$

Then $T = T'' \circ T'$. Since any translation has an inverse, T is an isomorphism iff T' is an isomorphism.

2.4 Rational Functions and Local Rings

Definition 2.4.1 (Zariski Topology)**.** *Let us make the trivial observation that the collection of subsets*

$$\{V(I) \subset \mathbb{A}^n \mid I \subset k[X_1, \ldots, X_n]\}$$

*satisfy the axioms of closed sets in a topology. This topology on $\mathbb{A}^n$ (whose closed subsets are precisely the collection $\{V(I)\}$) is called the **Zariski topology**. Similarly, we check that there is a topology on $\mathbb{P}^n$, where the closed subsets are precisely $V(I)$, with $I \subset k[X_1, \ldots, X_{n+1}]$ a homogeneous ideal.*

Let $V \subset \mathbb{A}^n(k)$ be a nonempty variety. Recall that $\Gamma(V)$ is a domain as $I(V) \subset k[X_1, \ldots, X_n]$ is a prime ideal. Thus, we may form its quotient field, which is called the field of **rational functions** on V and denoted $k(V)$.

Example 2.4.2. *Let $V = V(XW - YZ) \subset \mathbb{A}^4(k)$. Then*

$$\Gamma(V) = k[X, Y, Z, W]/(XW - YZ)\,.$$

Let $\bar{X}, \bar{Y}, \bar{Z}, \bar{W}$ denote the images in $\Gamma(V)$. Let $f \in k(V)$ be

$$f = \frac{\bar{X}}{\bar{Y}} = \frac{\bar{Z}}{\bar{W}}\,.$$

Clearly $\frac{\bar{X}}{\bar{Y}}$ is defined at points P where $\bar{Y}(P) \neq 0$ and $\frac{\bar{Z}}{\bar{W}}$ is defined at points P where $\bar{W}(P) \neq 0$. Thus, f is defined outside the algebraic subset $V \cap V(Y, W)$.

Motivated by the above example, given a rational function $f \in k(V)$, we say that f is **defined at** P if we can write $f = \frac{a}{b}$, for some $a, b \in \Gamma(V)$ such that $b(P) \neq 0$. The set of points where f is not defined is called the **pole set** of f.

Let $P \in V$. We denote by $\mathcal{O}_P(V)$ the set of rational functions which are defined at P. It is easily checked that this is a subring of $k(V)$, and we have $k \subset \Gamma(V) \subset \mathcal{O}_P(V) \subset k(V)$.

Proposition 2.4.3. *1. The pole set of a rational function is an algebraic subset of V.*

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

Proof. (1) Let $f \in k(V)$ be a rational function. For $G \in k[X_1, \ldots, X_n]$, let $\bar{G} \in \Gamma(V)$ denote its image. Consider the set $S = \{G \in k[X_1, \ldots, X_n] \mid \bar{G}f \in \Gamma(V)\}$. We claim that the pole set of f is $V \cap V(S)$.

If P is a pole of f, then if $G \in S$ and $\bar{G}f = a$, then $f = \frac{a}{\bar{G}}$ and $\bar{G}(P)$ has to be 0, or else f will be defined at P. Thus, poles of $f \subset V \cap V(S)$.

Conversely, if $P \in V \cap V(S)$, write $f = \frac{a}{b}$ for $a, b \in \Gamma(V)$. Since $b(P) = 0$ for any such expression of f, it follows that P is a pole of f. This proves (1).

(2) Clearly $\Gamma(V) \subset \bigcap_{P \in V} \mathcal{O}_P(V)$. Conversely, suppose $f \in k(V)$ and $f \in \bigcap_{P \in V} \mathcal{O}_P(V)$. Let $S = \{b \in \Gamma(V) \mid bf \in \Gamma(V)\}$. We will first show that the ideal generated by S in $\Gamma(V)$ is all of $\Gamma(V)$. If not, then there is a maximal ideal $\mathfrak{m}$ in $\Gamma(V)$ containing S. From Remark 1.10.2, every maximal ideal in $\Gamma(V)$ corresponds to a point $P \in V$. But this means that $S \subset \mathfrak{m}_P$, that is, $b(P) = 0 \quad \forall b \in S$, which shows that f is not defined at P, a contradiction as $f \in \mathcal{O}_P(V)$.

Thus, $1 = \sum h_i b_i$ for $h_i \in \Gamma(V)$ and $b_i \in S$. Thus, $f = \sum h_i(b_i f) \in \Gamma(V)$. Since $b_i f \in \Gamma(V)$, it follows that the RHS is in $\Gamma(V)$ and so $f \in \Gamma(V)$. This proves (2). □

Remark 2.4.4. Recall that on a topological space, or a smooth manifold, or a complex manifold, the continuous, smooth, holomorphic functions are defined locally. The above proposition says that the algebraic functions we defined on V are the same as those functions on V that are locally algebraic everywhere on V. □

Remark 2.4.5. In view of Definition 2.4.1 and the above proposition, it follows that every rational function is a genuine "algebraic" function defined on some open subset of V. □

Definition 2.4.6 (Local Ring)**.** *Let R be a ring that has only one maximal ideal. Such a ring is called a* ***local ring****.*

Recall that $\mathcal{O}_P(V)$ is defined as equivalence classes of $\frac{a}{b}, a, b \in \Gamma(V)$ and $b(P) \neq 0$. Consider the following "evaluation": $\frac{a}{b} \mapsto \frac{a(P)}{b(P)}$. Check that this is well-defined on equivalence classes and so gives rise to a ring homomorphism $\mathcal{O}_P(V) \to k$. The kernel of this map is denoted $\mathfrak{m}_P$. Clearly, this map is surjective as $\mathcal{O}_P(V)$ consists of constant functions. Thus, $\mathcal{O}_P(V)/\mathfrak{m}_P \cong k$ and so $\mathfrak{m}_P$ is a maximal ideal.

We claim that this is the only maximal ideal in $\mathcal{O}_P(V)$. If I is any proper ideal, we claim that $I \subset \mathfrak{m}_P$. If not, $\exists f \in I \setminus \mathfrak{m}_P$. Write $f = \frac{a}{b}$, where $b(P) \neq 0$. Since $a(P) \neq 0$, it

follows that $\frac{b}{a} \in \mathcal{O}_P(V)$. This shows that I contains a unit, a contradiction. This proves that $\mathcal{O}_P(V)$ is a local ring.

Proposition 2.4.7. *$\mathcal{O}_P(V)$ is a Noetherian local domain.*

Proof. It only remains to show that $\mathcal{O}_P(V)$ is Noetherian. Let $I \subset \mathcal{O}_P(V)$ be an ideal and let $J = I \cap \Gamma(V)$. Then J is an ideal in $\Gamma(V)$ and suppose it is generated by $(f_1, \ldots, f_r)$.

Suppose $f \in I$. Then $\exists b \in \Gamma(V)$ such that $b(P) \neq 0$, $bf \in \Gamma(V)$ and so $bf \in J$. Thus, $bf = \sum_{i=1}^{r} a_i f_i$. As b is a unit in $\mathcal{O}_P(V)$, it follows that each $\frac{f_i}{b} \in I$. Thus, I is also finitely generated by $f_1, \ldots, f_r$ in the ring $\mathcal{O}_P(V)$. □

2.5 Discrete Valuation Rings

Proposition 2.5.1. *Let R be a domain that is not a field. Then the following are equivalent:*

1. *R is Noetherian and local, and the maximal ideal is principal.*
2. *There is an irreducible element $t \in R$ such that every nonzero $z \in R$ may be written uniquely in the form $z = ut^n$, u a unit in R, $n \geqslant 0$ an integer.*

Proof. (1) $\implies$ (2). Let $\mathfrak{m} = (t)$. Clearly, since (t) is prime, it follows that t is irreducible.

First, we claim that if $z \in R$ then we can write $z = ut^n$ for some unit u and integer $n \geqslant 0$. If z is a unit, then we are done. If not, then $z \in \mathfrak{m}$ (as R is local) and so $z = z_1 t$. If z_1 is a unit, then we are done, or else $z_1 = z_2 t$. Proceeding in this fashion, we get a chain $(z) \subset (z_1) \subset (z_2) \subset \ldots$. As R is Noetherian, this chain stabilizes and so $(z_n) = (z_{n+1}) = (z_{n+2}) = \ldots$. Thus, $z_{n+1} = z_n \alpha = z_{n+1} t\alpha$. This shows $z_{n+1}(1 - t\alpha) = 0$. As R is a domain, this shows that t is a unit (since $z_{n+1} \neq 0$ implies $1 = t\alpha$), which is a contradiction. Thus, for some n, we get z_n is a unit.

And so $z = ut^n$. Suppose there are two such expressions for z:

$$z = ut^n = vt^m \,.$$

Let us assume that $m \geqslant n$. Then $uv^{-1} = t^{m-n}$. If $m > n$ then this implies that a unit is in $\mathfrak{m}$, a contradiction. Thus, $m = n$ and $u = v$.

(2) $\implies$ (1). Since t is irreducible, it is nonzero and not a unit. If $z \notin (t)$ then $z = ut^0$, which is a unit. Thus, every proper ideal is contained in (t) and so $(t) = \mathfrak{m}$ is the unique maximal ideal, which is principal. It remains to show that R is Noetherian. Let $I \subset R$ be an ideal. Let n be the smallest such that $z = ut^n \in I$. We claim $(t^n) = I$. Since u is a unit we get $t^n \in I \implies (t^n) \subseteq I$. Conversely, if $z' \in I$ then $z' = u' t^m$ where $m \geqslant n$. Thus, $z' \in (t^n)$. This shows that $I = (t^n)$. Thus, every ideal is principal. □

A ring satisfying the above conditions is called a **Discrete Valuation Ring (DVR)**.

In a DVR R, an element t such that $\mathfrak{m} = (t)$ is called a **uniformizing parameter**. Any two uniformizing parameters differ by a unit. Let K be the quotient field of R. Any $f \in K \setminus \{0\}$ can be uniquely written as ut^n for some unit u and integer n. The integer n is called the **order** of f and denoted $\mathrm{ord}(f)$.

Clearly, $R = \{f \in K \mid \mathrm{ord}(f) \geqslant 0\}$ and $\mathfrak{m} = \{f \in K \mid \mathrm{ord}(f) > 0\}$. We set $\mathrm{ord}(0) = \infty$.

2.6 Homogenization and Dehomogenization

Let R be a ring. Let $F \in R[X_1, \ldots, X_{n+1}]$ be a form of degree d.

Definition 2.6.1. *Define $F_* = F(X_1, \ldots, X_n, 1)$. Conversely, for a polynomial $f \in R[X_1, \ldots, X_n]$ of degree d, define*

$$f^* = X_{n+1}^d f\left(\frac{X_1}{X_{n+1}}, \ldots, \frac{X_n}{X_{n+1}}\right).$$

If we write $f = f_0 + \ldots + f_d$, then

$$f^* = X_{n+1}^d f_0 + X_{n+1}^{d-1} f_1 + \ldots + f_d.$$

Note $f^* \in R[X_1, \ldots, X_{n+1}]$ is a form of degree d.

Proposition 2.6.2. *1. $(FG)_* = F_* G_*$; $\quad f^* g^* = (fg)^*$.*

2. If $F \neq 0$ and X_{n+1}^r is the highest power of X_{n+1} which divides F, then $X_{n+1}^r (F_*)^* = F$.

3. $(F+G)_* = F_* + G_*$; $\quad X_{n+1}^t (f+g)^* = X_{n+1}^r f^* + X_{n+1}^s g^*$, where $r = \deg(g)$, $s = \deg(f)$ and $t = r + s - \deg(f+g)$.

Corollary 2.6.3. *Up to powers of X_{n+1}, factoring a form $F \in k[X_1, \ldots, X_{n+1}]$ is the same as factoring F_* in $k[X_1, \ldots, X_n]$. In particular, if $F \in k[X, Y]$ is a form and k is algebraically closed, then*

$$F = cY^r \prod_{i=1}^{n} (X - \lambda_i Y).$$

Proof. We may write $F = X_{n+1}^d F_*\left(\frac{X_1}{X_{n+1}}, \ldots, \frac{X_n}{X_{n+1}}\right)$. Then the first claim follows by viewing $\frac{X_1}{X_{n+1}}, \ldots, \frac{X_n}{X_{n+1}}$ as indeterminates. The second claim is left as an exercise. □

2.7 Operations with Ideals

Let $I_1, \ldots, I_n$ be ideals in R. Then $I_1 \cdot I_2 \cdots I_n$ is defined as the ideal generated by $a_1 a_2 \ldots a_n$, where $a_j \in I_j$. In particular, we may define I^n in this way. Clearly,

$$R = I^0 \supset I^1 \supset I^2 \supset \ldots$$

Let $I, J \subset R$ be ideals. Then $I + J = \{a + b \mid a \in I, b \in J\}$. This is the smallest ideal that contains I and J.

I and J are said to be **comaximal** if $I + J = R$.

If $R \subset S$ is a subring and $I \subset R$ is an ideal, then IS is the ideal of S generated by I. Easy to check that $I^n S = (IS)^n$.

Lemma 2.7.1. *1. $IJ \subset I \cap J$*

2. If I and J are comaximal then $IJ = I \cap J$.

Proof. (1) is clear. If I and J are comaximal, then $\exists a \in I, b \in J$ such that $a + b = 1$. If $x \in I \cap J$ then $xa + xb = x$. Note that $xa, xb \in IJ$ and so $I \cap J \subset IJ$. This proves (2). □

2.8 Ideals with a Finite Number of Zeros

Proposition 2.8.1. *Let $I \subset k[X_1, \ldots, X_n]$ be an ideal such that $V(I) = \{P_1, \ldots, P_N\}$ is finite. Let $\mathcal{O}_i = \mathcal{O}_{P_i}(\mathbb{A}^n)$. Then there is a natural isomorphism of rings:*

$$k[X_1, \ldots, X_n]/I \cong \prod_{i=1}^{N} \mathcal{O}_i / I\mathcal{O}_i.$$

Proof. Let $R_i = \mathcal{O}_i / I\mathcal{O}_i$. Consider the natural homomorphism

$$R = k[X_1, \ldots, X_n]/I \xrightarrow{\phi_i} R_i \,.$$

Using this we get a homomorphism $\phi : R \to \prod R_i$, which we will show is an isomorphism.

Since $V(I) = \{P_1, \ldots, P_N\}$, it is clear that

$$I(V(I)) = I(\{P_1, \ldots, P_N\}) = \bigcap_{i=1}^{N} I(\{P_i\}) \,.$$

Let $\mathfrak{m}_i = I(\{P_i\})$. By Nullstellensatz we get that $\mathrm{Rad}(I) = I(V(I)) = \bigcap \mathfrak{m}_i$. In a Noetherian ring, for any ideal I, $\exists d$ such that $\mathrm{Rad}(I)^d \subset I$. Thus, $\exists d$ such that $(\bigcap \mathfrak{m}_i)^d \subset I$.

Further, note that $\mathfrak{m}_1$ and $\cap_{i\geqslant 2}\mathfrak{m}_i$ are comaximal. If not, then $\cap_{i\geqslant 2}\mathfrak{m}_i \subset \mathfrak{m}_1$, which is not possible. Thus, $\bigcap \mathfrak{m}_i = \prod \mathfrak{m}_i$ and so $\prod \mathfrak{m}_i^d \subset I$.

Since $V(I) \setminus \{P_i\} \subsetneq V(I)$, this implies $I(V(I)) \subsetneq I(V(I) \setminus \{P_i\})$. Thus, for each i, there is an $F_i \in k[X_1, \ldots, X_n]$ such that $F_i(P_j) = 0$ for $j \neq i$ and $F_i(P_i) \neq 0$ (and so we may assume it equals 1). Consider the polynomial

$$E_i = 1 - (1 - F_i^d)^d = F_i^d D \quad \text{for some } D.$$

Since $F_i \in \mathfrak{m}_j$ if $j \neq i$, it follows that $F_i^d \in \mathfrak{m}_j^d$ for $j \neq i$. Thus, $E_i \in \mathfrak{m}_j^d$. Note that $1 - F_i^d \in \mathfrak{m}_i$ and so

$$1 - E_i = (1 - F_i^d)^d \in \mathfrak{m}_i^d \,.$$

This shows that $E_i(1 - E_i) \in \bigcap_{j=1}^N \mathfrak{m}_j^d \subset I$. Thus, $\bar{E}_i = \bar{E}_i^2$ in R. Also

$$1 - \sum_i E_i = (1 - E_j) - \sum_{i\neq j} E_i \in \mathfrak{m}_j^d \,.$$

This shows that $1 - \sum E_i \in \bigcap_{j=1}^N \mathfrak{m}_j^d \subset I$. Thus, $\sum \bar{E}_i = 1$ in R.

Claim: If $G \in k[X_1, \ldots, X_n]$ and $G(P_i) \neq 0$, then there is $t \in R$ such that

$$t\bar{G} = \bar{E}_i \,.$$

We may assume that $G(P_i) = 1$. Let $H = 1 - G$. Note that $H \in \mathfrak{m}_i$. Then

$$(1 - H)(1 + H + H^2 + \ldots + H^{d-1})E_i = (1 - H^d)E_i.$$

Since $E_i \in \prod_{j\neq i} \mathfrak{m}_j^d$, we get $H^d E_i \in \prod \mathfrak{m}_j^d \subset I$. Thus, $\overline{(1 - H)(*)} = \bar{E}_i$ in R, that is, $\bar{G}(*) = \bar{E}_i$. This proves the claim.

Recall the map $\phi : R \to \prod_{i=1}^N \mathcal{O}_i/I\mathcal{O}_i$.

ϕ **is 1-1**: If $\phi(\bar{F}) = 0$, then $F \in I\mathcal{O}_{P_i}(\mathbb{A}^n)$, that is, $\exists G_i$ such that $G_i(P_i) \neq 0$ and $FG_i \in I$. Thus, $\exists t_i \in R$ such that $\bar{G}_i t_i = \bar{E}_i$, which shows that $\bar{F}\bar{G}_i t_i = \bar{F}\bar{E}_i$. But as $FG_i \in I$, we get that $\bar{F}\bar{G}_i = 0$ which shows that $\bar{F}\bar{E}_i = 0$. Thus, $\bar{F} = \sum \bar{F}\bar{E}_i = 0$.

ϕ **is onto**: First consider the ring homomorphism $\phi_i : R \to \mathcal{O}_i/I\mathcal{O}_i$. We will abuse notation and denote the image of an element of R by the same element. Since $E_i(P_i) = 1$, it follows that E_i is a unit in $\mathcal{O}_i$ and so $\bar{E}_i$ is a unit in $\mathcal{O}_i/I\mathcal{O}_i$. Since $E_iE_j \in I$, we get $\bar{E}_i\bar{E}_j = 0$, and so $\bar{E}_j = 0$ in $\mathcal{O}_i/I\mathcal{O}_i$. Also note that since $\bar{E}_i^2 = \bar{E}_i$ in R, the same holds in $\mathcal{O}_i/I\mathcal{O}_i$. It follows that $\bar{E}_i = \bar{1}$ in $\mathcal{O}_i/I\mathcal{O}_i$.

An element of $\mathcal{O}_i$ is of the form $\frac{a}{s}$, where $s(P_i) \neq 0$. There is $t \in R$ such that $t\bar{s} = \bar{E}_i$ in R. Thus, given elements $\frac{a_i}{s_i} \in \mathcal{O}_i$, we get $t_i \in R$ such that $t_i \bar{s}_i = \bar{E}_i$ and we may consider the element $\sum \bar{a}_i t_i \bar{E}_i \in R$. The image of this in $\mathcal{O}_j/I\mathcal{O}_j$ equals $\bar{a}_j t_j \bar{E}_j = \bar{a}_j t_j = \frac{\bar{a}_j}{\bar{s}_j}$.

Thus, the image of $\sum \bar{a}_i t_i \bar{E}_i$ in $\prod \mathcal{O}_i/I\mathcal{O}_i$ is $(\frac{\bar{a}_1}{\bar{s}_1}, \ldots, \frac{\bar{a}_N}{\bar{s}_N})$. This proves ϕ is onto. □

Corollary 2.8.2. *If $V(I)$ is finite then*

$$\dim_k(k[X_1, \ldots, X_n]/I) = \sum_{i=1}^{N} \dim_k(\mathcal{O}_i/I\mathcal{O}_i).$$

Corollary 2.8.3. *If $V(I) = \{P\}$, then*

$$k[X_1, \ldots, X_n]/I \cong \mathcal{O}_P(\mathbb{A}^n)/I\mathcal{O}_P(\mathbb{A}^n)\,.$$

2.9 Modules; Exact Sequences

Consider a sequence of maps

$$\ldots M_{i-1} \xrightarrow{\phi_i} M_i \xrightarrow{\phi_{i+1}} M_{i+2} \to \ldots$$

We say that this is a **complex** if $\phi_{j+1} \circ \phi_j = 0$ for all j. This is equivalent to saying that $\mathrm{Im}(\phi_j) \subset \mathrm{Ker}(\phi_{j+1})$. We say a complex is **exact** if $\mathrm{Im}(\phi_j) = \mathrm{Ker}(\phi_{j+1})$ for all j.

For example, if $\phi : M \to M'$ is an R-module homomorphism, then the following two are an exact complexes:

$$0 \to \mathrm{Ker}(\phi) \to M \to \mathrm{Im}(\phi) \to 0$$

and

$$0 \to \mathrm{Im}(\phi) \to M' \to \mathrm{Coker}(\phi) \to 0.$$

2.10 Exercises

Exercise 2.10.1. Show that the map that associates to each $F \in k[X_1, \ldots, X_n]$ a polynomial function in $\mathscr{F}(V, k)$ is a ring homomorphism whose kernel is $I(V)$.

Solution. Define the map $\Phi : k[X_1, \ldots, X_n] \longrightarrow \mathscr{F}(V, k)$ by sending a polynomial F to the function $\Phi(F) : V \to k$, such that $\Phi(F)(a_1, \ldots, a_n) = F(a_1, \ldots, a_n)$. We first show that Φ is a ring homomorphism. For $F, G \in k[X_1, \ldots, X_n]$ and $a \in V$, we have

$$\Phi(F + G)(a) = (F + G)(a) = F(a) + G(a) = \Phi(F)(a) + \Phi(G)(a),$$

so $\Phi(F+G) = \Phi(F) + \Phi(G)$. Similarly,

$$\Phi(FG)(a) = (FG)(a) = F(a)G(a) = \Phi(F)(a)\Phi(G)(a),$$

hence $\Phi(FG) = \Phi(F)\Phi(G)$. Finally, $\Phi(1)$ is the constant function 1. Thus, Φ is a ring homomorphism. Next we determine the kernel of Φ. By definition,

$$F \in \ker(\Phi) \iff \Phi(F)(a) = 0 \text{ for all } a \in V \iff F(a) = 0 \text{ for all } a \in V.$$

This is precisely the definition of the ideal $I(V)$ of polynomials vanishing on V. Therefore, $\ker(\Phi) = I(V)$. Hence, the map $I(V)$ is the kernel of the ring homomorphism Φ. □

Exercise 2.10.2. Let $V \subset \mathbb{A}^n$ be a variety. A subvariety of V is a variety $W \subset \mathbb{A}^n$ that is contained in V. Show that there is a natural one-to-one correspondence between algebraic subsets (resp. subvarieties, resp. points) of V and radical ideals (resp. prime ideals, resp. maximal ideals) of $\Gamma(V)$. (See Problems 1.22, 1.38.)

Solution. Let $V \subset \mathbb{A}^n$ be a variety, and let $\Gamma(V) = k[X_1, \ldots, X_n]/I(V)$ be its coordinate ring. Recall that the algebraic subsets of V are precisely the sets of the form $W = V(J)$, where $J \subset k[X_1, \ldots, X_n]$ is an ideal containing $I(V)$. For such a subset W, define

$$I_V(W) := \{\, f \in \Gamma(V) \mid f|_W = 0 \,\}.$$

Equivalently, if J is an ideal with $I(V) \subset J$, then $I_V(W)$ is the image of J in $\Gamma(V)$.

Algebraic subsets and radical ideals. It is clear that algebraic subsets of V are in bijection with radical ideals containing $I(V)$. It is also easily checked that radical ideals containing $I(V)$ are in bijection with radical ideals in $\Gamma(V)$.

Subvarieties and prime ideals. Similar proof as above.

Points and maximal ideals. Similar proof as above.

Therefore, there is a natural one-to-one correspondence between:

- algebraic subsets of V and radical ideals of $\Gamma(V)$,
- subvarieties of V and prime ideals of $\Gamma(V)$,
- points of V and maximal ideals of $\Gamma(V)$.

□

Exercise 2.10.3. Let W be a subvariety of a variety V, and let $I_V(W)$ be the ideal of $\Gamma(V)$ corresponding to W.

(a) Show that every polynomial function on V restricts to a polynomial function on W.

(b) Show that the map from $\Gamma(V)$ to $\Gamma(W)$ defined in part (a) is a surjective homomorphism with kernel $I_V(W)$, so that $\Gamma(W)$ is isomorphic to $\Gamma(V)/I_V(W)$.

Solution. Let k be an algebraically closed field and let $V \subset k^n$ be an affine variety. Recall that $\Gamma(V) = k[X_1, \ldots, X_n]/I(V)$is the ring of polynomial functions on V. Let $W \subset V$ be a subvariety, so $I(V) \subset I(W)$ and $I_V(W) = \{f \in \Gamma(V) \mid f|_W = 0\}$ is the ideal of functions on V vanishing on W.

(a) Restriction of polynomial functions.
Let $f \in \Gamma(V)$. By definition, f is represented by a polynomial $\tilde{f} \in k[X_1, \ldots, X_n]$, and for $p \in V$ we have

$$f(p) = \tilde{f}(p).$$

Since $W \subset V$, we may restrict this function to W by defining

$$f|_W(p) = \tilde{f}(p), \qquad p \in W.$$

This is again a polynomial function on W, since it is induced by the same polynomial $\tilde{f}$. Hence every polynomial function on V restricts to a polynomial function on W.

(b) Kernel and surjectivity.
Define the restriction map

$$\varphi : \Gamma(V) \longrightarrow \Gamma(W), \qquad \varphi(f) = f|_W.$$

This map is a ring homomorphism since restriction preserves addition and multiplication.

Kernel. We have

$$\ker \varphi = \{f \in \Gamma(V) \mid f|_W = 0\} = I_V(W),$$

by definition of $I_V(W)$.

Surjectivity. Let $g \in \Gamma(W)$. Then g is represented by a polynomial $\tilde{g} \in k[X_1, \ldots, X_n]$, and $g(p) = \tilde{g}(p)$ for all $p \in W$. The polynomial $\tilde{g}$ defines a polynomial function $f \in \Gamma(V)$, and by construction, $\varphi(f) = f|_W = g$. Hence φ is surjective. We have $\Gamma(W) \cong \Gamma(V)/\ker\varphi = \Gamma(V)/I_V(W)$. □

Exercise 2.10.4. Let $V \subset \mathbb{A}^n$ be a nonempty variety. Show that the following are equivalent:

(i) V is a point;

(ii) $\Gamma(V) = k$;

(iii) $\dim_k \Gamma(V) < \infty$.

Solution. (i) $\Rightarrow$ (ii). If V is a point, say $V = \{p\}$ with $p = (a_1, \ldots, a_n)$, then

$$I(V) = (x_1 - a_1, \ldots, x_n - a_n).$$

Hence

$$\Gamma(V) = k[X_1, \ldots, X_n]/(x_1 - a_1, \ldots, x_n - a_n) \cong k.$$

(ii) $\Rightarrow$ (iii).
If $\Gamma(V) = k$, then clearly

$$\dim_k \Gamma(V) = 1 < \infty.$$

(iii) $\Rightarrow$ (i). By Corollary 4 of section 1.7 we have V is a finite set. Now any finite nonempty variety is a point. Thus, V is a point. Thus (i), (ii), and (iii) are equivalent. $\square$

Exercise 2.10.5. Let F be an irreducible polynomial in $k[X, Y]$, and suppose F is monic in Y: $F = Y^n + a_1(X)Y^{n-1} + \cdots + a_n(X)$ with $n > 0$. Let $V = V(F) \subset \mathbb{A}^2$. Show that the natural homomorphism from $k[X]$ to $\Gamma(V) = k[X, Y]/(F)$ is one-to-one, so that $k[X]$ may be regarded as a subring of $\Gamma(V)$; show that the residues $\overline{1}, \overline{Y}, \ldots, \overline{Y}^{n-1}$ generate $\Gamma(V)$ over $k[X]$ as a module.

Solution. The natural homomorphism is $X \mapsto \overline{X}$. Now we have to show that this map is one-one. Let $f_1, f_2 \in k[X]$ such that $\overline{f_1} = \overline{f_2}$ then $f_1 - f_2 \in (F)$, that is, F divides $(f_1 - f_2)$, but this is not possible. Hence $k[X]$ is a subring of $\Gamma(V)$. Since any polynomial in $\Gamma(V)$ can be written as $f_m(X)Y^m + f_{m-1}(X)Y^{m-1} + \cdots + f_0(X)$, where $f_i(X) \in k[X]$, we easily conclude that $\Gamma(V)$ is a finite $k[X]$-module which can be generated by $\overline{1}, \overline{Y}, \ldots, \overline{Y}^{n-1}$. $\square$

Exercise 2.10.6. Let $\varphi : V \to W$, $\psi : W \to Z$. Show that $\overline{\psi \circ \varphi} = \overline{\varphi} \circ \overline{\psi}$. Show that the composition of polynomial maps is a polynomial map.

Solution. Let $V \subset \mathbb{A}^n$, $W \subset \mathbb{A}^m$, and $Z \subset \mathbb{A}^r$ be affine varieties.

A polynomial map $\varphi : V \to W$ induces a k-algebra homomorphism

$$\overline{\varphi} : \Gamma(W) \to \Gamma(V), \qquad f \mapsto f \circ \varphi,$$

and similarly a polynomial map $\psi : W \to Z$ induces

$$\overline{\psi} : \Gamma(Z) \to \Gamma(W), \qquad g \mapsto g \circ \psi.$$

Let $h \in \Gamma(Z)$. Then

$$(\overline{\varphi} \circ \overline{\psi})(h) = \overline{\varphi}(h \circ \psi) = (h \circ \psi) \circ \varphi = h \circ (\psi \circ \varphi) = \overline{\psi \circ \varphi}(h).$$

Since this holds for all $h \in \Gamma(Z)$, we obtain

$$\overline{\psi \circ \varphi} = \overline{\varphi} \circ \overline{\psi}.$$

Now write

$$\varphi = (\varphi_1, \ldots, \varphi_m), \qquad \psi = (\psi_1, \ldots, \psi_r),$$

where each φ_i is a polynomial function on V and each ψ_j is a polynomial function on W. Then

$$\psi \circ \varphi = (\psi_1(\varphi_1, \ldots, \varphi_m), \ldots, \psi_r(\varphi_1, \ldots, \varphi_m)).$$

Since substitution of polynomials into polynomials again yields polynomials, each coordinate function of $\psi \circ \varphi$ is a polynomial function on V.

Hence the composition of polynomial maps is again a polynomial map. □

Exercise 2.10.7. If $\varphi : V \to W$ is a polynomial map, and X is an algebraic subset of W, show that $\varphi^{-1}(X)$ is an algebraic subset of V. If $\varphi^{-1}(X)$ is irreducible, and X is contained in the image of φ, show that X is irreducible.

Solution. Let $V \subset \mathbb{A}^n$ and $W \subset \mathbb{A}^m$ be affine varieties, and let $\varphi : V \to W$ be a polynomial map.

Step 1: Preimages of algebraic sets. Let $X \subset W$ be an algebraic subset. Then there exists an ideal $I \subset \Gamma(W)$ such that

$$X = V(I).$$

By definition,

$$\varphi^{-1}(X) = \{\, p \in V \mid f(\varphi(p)) = 0 \text{ for all } f \in I \,\}.$$

Equivalently, $\varphi^{-1}(X) = V\big(\overline{\varphi}(I)\big)$, where $\overline{\varphi} : \Gamma(W) \to \Gamma(V)$ is the homomorphism induced by φ. Hence $\varphi^{-1}(X)$ is an algebraic subset of V.

Step 2: Irreducibility. Assume that $\varphi^{-1}(X)$ is irreducible and that $X \subset \varphi(V)$. Suppose for the sake of contradiction, that X is reducible. Then we may write $X = X_1 \cup X_2$, where X_1 and X_2 are proper algebraic subsets of X. Taking preimages under φ, we obtain $\varphi^{-1}(X) = \varphi^{-1}(X_1) \cup \varphi^{-1}(X_2)$. Each $\varphi^{-1}(X_i)$ is an algebraic subset of V, and since $X_i \subsetneq X$ and $X \subset \varphi(V)$, we have

$$\varphi^{-1}(X_i) \subsetneq \varphi^{-1}(X) \quad (i = 1, 2).$$

Thus $\varphi^{-1}(X)$ is written as a union of two proper closed subsets, contradicting its irreducibility. Therefore X must be irreducible. □

Exercise 2.10.8. (a) Show that $\{(t, t^2, t^3) \in \mathbb{A}^3(k) \mid t \in k\}$ is an affine variety.

(b) Show that $V(XZ - Y^2, YZ - X^3, Z^2 - X^2Y) \subset \mathbb{A}^3(\mathbb{C})$ is a variety. (Hint: $Y^3 - X^4, Z^3 - X^5, Z^4 - Y^5 \in I(V)$. Find a polynomial map from $\mathbb{A}^1(\mathbb{C})$ onto V.)

Solution. (a) Consider the polynomials in $F = (Y - X^2)$ and $G = (Z - X^3)$ in $k[X, Y, Z]$. Both F and G are irreducible polynomial. The ideal (F, G) is prime ideal of $k[X, Y, Z]$ since $k[X, Y, Z]/(F, G)$ is an integral domain. Thus $V((F, G))$ is an affine variety.

(b) Let

$$V := V(XZ - Y^2,\ YZ - X^3,\ Z^2 - X^2Y) \subset \mathbb{A}^3(\mathbb{C}).$$

Define a polynomial map

$$\psi : \mathbb{A}^1(\mathbb{C}) \longrightarrow \mathbb{A}^3(\mathbb{C}), \qquad t \longmapsto (t^3, t^4, t^5).$$

A straightforward calculation shows that

$$XZ - Y^2 = t^3 \cdot t^5 - t^8 = 0, \quad YZ - X^3 = t^4 \cdot t^5 - t^9 = 0, \quad Z^2 - X^2Y = t^{10} - t^{10} = 0.$$

Hence $\psi(\mathbb{A}^1) \subset V$.

Conversely, it is easily checked that $Y^3 - X^4, Z^3 - X^5, Z^4 - Y^5 \in I(V)$. Let $p \in V$ be a point such that $P \neq (0, 0, 0)$. It follows that one of the coordinates is nonzero and so all coordinates are nonzero. Let t be the ratio $Y(P)/X(P)$. Then it is easily checked that

$$X(P) = t^3, \qquad Y(P) = t^4, \qquad Z(P) = t^5\,.$$

So every point of V lies in the image of ψ. Thus $\psi(\mathbb{A}^1) = V$.

Since $\mathbb{A}^1$ is irreducible and ψ is a polynomial map whose image is V, it follows that V is irreducible. Being defined by polynomial equations, V is therefore an affine variety. □

Exercise 2.10.9. Let $\varphi : V \to W$ be a polynomial map of affine varieties, $V' \subset V$, $W' \subset W$ subvarieties. Suppose $\varphi(V') \subset W'$.

(a) Show that $\tilde{\varphi}(I_W(W')) \subset I_V(V')$ (see Problems 2.3).

(b) Show that the restriction of φ gives a polynomial map from V' to W'.

Solution. Let $\varphi : V \to W$ be a polynomial map of affine varieties, and let $V' \subset V$, $W' \subset W$ be subvarieties such that $\varphi(V') \subset W'$.

(a) Let $f \in I_W(W')$. By definition, f vanishes on W', that is, $f(w) = 0$ for all $w \in W'$. Consider the induced homomorphism

$$\tilde{\varphi} : \Gamma(W) \longrightarrow \Gamma(V), \qquad f \longmapsto f \circ \varphi.$$

For any $v \in V'$, we have $\varphi(v) \in W'$, hence

$$(\tilde{\varphi}(f))(v) = f(\varphi(v)) = 0.$$

Thus $\tilde{\varphi}(f)$ vanishes on V', which means

$$\tilde{\varphi}(f) \in I_V(V').$$

Therefore,

$$\tilde{\varphi}(I_W(W')) \subset I_V(V').$$

(b) By part (a), the homomorphism $\tilde{\varphi} : k[W] \to k[V]$ sends $I_W(W')$ into $I_V(V')$. Hence it induces a well-defined k-algebra homomorphism on the quotients:

$$\tilde{\varphi}' : \Gamma(W)/I_W(W') \longrightarrow \Gamma(V)/I_V(V').$$

Identifying these quotients with the coordinate rings $\Gamma(W')$ and $\Gamma(V')$, respectively, we obtain a k-algebra homomorphism

$$\tilde{\varphi}' : \Gamma(W') \to \Gamma(V').$$

By definition of morphisms of affine varieties, this homomorphism corresponds to a polynomial map

$$\varphi|_{V'} : V' \to W',$$

which is precisely the restriction of φ to V'.

Hence the restriction of φ defines a polynomial map from V' to W'. □

Exercise 2.10.10. Show that the projection map $pr : \mathbb{A}^n \to \mathbb{A}^r$, $n \geq r$, defined by $pr(a_1, \ldots, a_n) = (a_1, \ldots, a_r)$ is a polynomial map.

Solution. Let $\mathbb{A}^n$ have coordinates $(X_1, \ldots, X_n)$ and $\mathbb{A}^r$ have coordinates $(Y_1, \ldots, Y_r)$. Define

$$pr : \mathbb{A}^n \longrightarrow \mathbb{A}^r, \qquad (a_1, \ldots, a_n) \longmapsto (a_1, \ldots, a_r).$$

Then

$$pr = (X_1, \ldots, X_r),$$

that is, the i-th coordinate function of pr is the polynomial X_i for $1 \leq i \leq r$. Since each coordinate function of pr is a polynomial function on $\mathbb{A}^n$, it follows by definition that pr is a polynomial map. Equivalently, on coordinate rings pr induces the k-algebra homomorphism

$$\widetilde{pr} : k[Y_1, \ldots, Y_r] \longrightarrow k[X_1, \ldots, X_n], \qquad Y_i \longmapsto X_i,$$

which is well defined and polynomial. Hence pr is a polynomial map. □

Exercise 2.10.11. Let $f \in \Gamma(V)$, V a variety $\subset \mathbb{A}^n$. Define

$$G(f) = \{(a_1, \ldots, a_n, a_{n+1}) \in \mathbb{A}^{n+1} \mid (a_1, \ldots, a_n) \in V \text{ and } a_{n+1} = f(a_1, \ldots, a_n)\},$$

the graph of f. Show that $G(f)$ is an affine variety, and that the map $(a_1, \ldots, a_n) \to (a_1, \ldots, a_n, f(a_1, \ldots, a_n))$ defines an isomorphism of V with $G(f)$. (Projection gives the inverse.)

Solution. Let $V \subset \mathbb{A}^n$ be an affine variety and let $f \in \Gamma(V)$ be a regular (polynomial) function on V.

Step 1: $G(f)$ is an affine variety. Let $X_1, \ldots, X_n, X_{n+1}$ be the coordinate functions on $\mathbb{A}^{n+1}$. Since $f \in \Gamma(V)$, there exists a polynomial $F \in k[X_1, \ldots, X_n]$ whose restriction to V equals f. Then the graph of f is

$$G(f) = \{(a_1, \ldots, a_n, a_{n+1}) \in \mathbb{A}^{n+1} \mid (a_1, \ldots, a_n) \in V,\ a_{n+1} - F(a_1, \ldots, a_n) = 0\}.$$

Hence

$$G(f) = V\big(I(V),\ X_{n+1} - F(X_1, \ldots, X_n)\big),$$

which is a closed algebraic subset of $\mathbb{A}^{n+1}$. Therefore $G(f)$ is an affine variety.

Step 2: The graph map is a polynomial map. Define

$$\Phi : V \longrightarrow G(f), \qquad (a_1, \ldots, a_n) \longmapsto (a_1, \ldots, a_n, f(a_1, \ldots, a_n)).$$

Each coordinate function of Φ is a polynomial function on V, so Φ is a polynomial map.

Step 3: Φ is an isomorphism. Consider the projection map

$$\pi : G(f) \longrightarrow V, \qquad (a_1, \ldots, a_n, a_{n+1}) \longmapsto (a_1, \ldots, a_n).$$

This is the restriction of the standard projection $\mathbb{A}^{n+1} \to \mathbb{A}^n$, hence is a polynomial map. For any $(a_1, \ldots, a_n) \in V$,

$$\pi(\Phi(a_1, \ldots, a_n)) = (a_1, \ldots, a_n),$$

and for any $(a_1, \ldots, a_n, a_{n+1}) \in G(f)$ we have $a_{n+1} = f(a_1, \ldots, a_n)$, so

$$\Phi(\pi(a_1, \ldots, a_n, a_{n+1})) = (a_1, \ldots, a_n, a_{n+1}).$$

Thus Φ and π are inverse polynomial maps. $\square$

Exercise 2.10.12. (a) Let $\varphi : \mathbb{A}^1 \to V = V(Y^2 - X^3) \subset \mathbb{A}^2$ be defined by $\varphi(t) = (t^2, t^3)$. Show that although φ is a one-to-one, onto polynomial map, φ is not an isomorphism. (Hint: $\overline{\varphi}(\Gamma(V)) = k[T^2, T^3] \subset k[T] = \Gamma(\mathbb{A}^1)$.)

(b) Let $\varphi : \mathbb{A}^1 \to V = V(Y^2 - X^2(X+1))$ be defined by $\varphi(t) = (t^2 - 1, t(t^2 - 1))$. Show that φ is one-to-one and onto, except that $\varphi(\pm 1) = (0, 0)$.

Solution. (a) Consider the map

$$\varphi : \mathbb{A}^1 \longrightarrow V \subset \mathbb{A}^2, \qquad t \longmapsto (t^2, t^3),$$

where $V = V(Y^2 - X^3)$.

First note that φ is a polynomial map. It is injective since

$$t^2 = s^2 \text{ and } t^3 = s^3 \implies t = s,$$

and it is surjective because every point $(x, y) \in V$, with $(x, y) \neq (0, 0)$ satisfies $y^2 = x^3$, hence $x = t^2$, $y = t^3$ for $t = y/x \in k$. Note that this is well defined since $x \neq 0$. Now consider the induced homomorphism on coordinate rings:

$$\overline{\varphi} : \Gamma(V) = k[X, Y]/(Y^2 - X^3) \longrightarrow \Gamma(\mathbb{A}^1) = k[T],$$

given by

$$\overline{\varphi}(\overline{X}) = T^2, \qquad \overline{\varphi}(\overline{Y}) = T^3.$$

Hence

$$\overline{\varphi}(\Gamma(V)) = k[T^2, T^3] \subset k[T].$$

This inclusion is strict, since for example $T \notin k[T^2, T^3]$. Therefore $\overline{\varphi}$ is not surjective, so it is not an isomorphism of k-algebras. Since an isomorphism of affine varieties must induce an isomorphism of coordinate rings, φ is not an isomorphism, despite being bijective as a set map.

(b) Let

$$\varphi : \mathbb{A}^1 \longrightarrow V = V(Y^2 - X^2(X+1)), \qquad t \longmapsto (t^2 - 1,\ t(t^2 - 1)).$$

A direct computation shows

$$Y^2 - X^2(X+1) = t^2(t^2-1)^2 - (t^2-1)^2(t^2) = 0,$$

so $\varphi(\mathbb{A}^1) \subset V$.

Suppose $\varphi(t_1) = \varphi(t_2)$. Then

$$t_1^2 - 1 = t_2^2 - 1 \quad \text{and} \quad t_1(t_1^2 - 1) = t_2(t_2^2 - 1).$$

From the first equation, $t_1^2 = t_2^2$. If $t_1^2 \neq 1$, then $t_1^2 - 1 \neq 0$ and dividing the second equation by $t_1^2 - 1$ yields $t_1 = t_2$. Thus φ is injective away from $t = \pm 1$. Moreover,

$$\varphi(1) = \varphi(-1) = (0, 0).$$

Conversely, let $(x, y) \in V$ with $(x, y) \neq (0, 0)$. Then $x \neq 0$. Let $y/x = t$. Then from $y^2 = x^2(x+1)$ we obtain $x+1 = (y/x)^2 = t^2$. Hence $x = t^2 - 1$ and $y = (y/x)x = t(t^2 - 1)$. Thus every point of V except $(0, 0)$ is the image of a unique point and $(0, 0)$ has exactly two preimages ± 1. Therefore φ is one-to-one on $\varphi^{-1}(V \setminus \{(0, 0)\})$ and onto. □

Exercise 2.10.13. Let $V = V(X^2 - Y^3, Y^2 - Z^3) \subset \mathbb{A}^3$ as in Problem 1.40, $\overline{\alpha}$ induced by the homomorphism α of that problem.

(a) What is the polynomial map f from $\mathbb{A}^1$ to V such that $\tilde{f} = \overline{\alpha}$?

(b) Show that f is one-to-one and onto, but not an isomorphism.

Solution. Let

$$V = V(X^2 - Y^3,\ Y^2 - Z^3) \subset \mathbb{A}^3.$$

(a) From Problem 1.40, the homomorphism

$$\alpha : k[X, Y, Z]/(X^2 - Y^3,\ Y^2 - Z^3) \longrightarrow k[T]$$

is given by

$$\alpha(\overline{X}) = T^9, \qquad \alpha(\overline{Y}) = T^6, \qquad \alpha(\overline{Z}) = T^4,$$

which indeed satisfies

$$(T^9)^2 = T^{18} = (T^6)^3, \qquad (T^6)^2 = T^{12} = (T^4)^3.$$

The corresponding polynomial map

$$f : \mathbb{A}^1 \longrightarrow V$$

such that $\widetilde{f} = \overline{\alpha}$ is therefore

$$f(t) = (t^9,\ t^6,\ t^4).$$

(b) First, f is a polynomial map and its image lies in V by the above relations. Let us show this is surjective. Let $(x, y, z) \neq (0, 0, 0)$ be any point. Note that this forces that

all the three coordinates are nonzero. Define $t = (x/z^2)$. Note that $x^4 = y^6 = z^9$. Thus, $t^4 = x^4/z^8 = z$. Similarly, $t^9 = x^9/z^{18} = x$ and $t^6 = x^6/z^{12} = x^2/z^3 = yy^2/z^3 = y$. This proves that f is surjective. To see that f is injective, suppose

$$f(t_1) = f(t_2).$$

Then $t_1^4 = t_2^4$ and $t_1^9 = t_2^9$ imply $t_1 = t_2$.

Now consider the induced homomorphism on coordinate rings:

$$\widetilde{f} : \Gamma(V) = k[X, Y, Z]/(X^2 - Y^3,\ Y^2 - Z^3) \longrightarrow k[T],$$

whose image is

$$\widetilde{f}(\Gamma(V)) = k[T^4, T^6, T^9] \subset k[T].$$

This inclusion is strict, since $T \notin k[T^4, T^6, T^9]$. Hence $\widetilde{f}$ is not surjective and therefore not an isomorphism.

Consequently, although f is a bijective polynomial map from $\mathbb{A}^1$ onto V, it is not an isomorphism of affine varieties. □

Exercise 2.10.14. A set $V \subset \mathbb{A}^n(k)$ is called a linear subvariety of $\mathbb{A}^n(k)$ if $V = V(F_1, \ldots, F_r)$ for some polynomials F_i of degree 1.

(a) Show that if T is an affine change of coordinates on $\mathbb{A}^n$, then V^T is also a linear subvariety of $\mathbb{A}^n(k)$.

(b) If $V \neq \emptyset$, show that there is an affine change of coordinates T of $\mathbb{A}^n$ such that $V^T = V(X_{m+1}, \ldots, X_n)$. (Hint: use induction on r.) So V is a variety.

(c) Show that the m that appears in part (b) is independent of the choice of T. It is called the dimension of V. Then V is isomorphic (as a variety) to $\mathbb{A}^m(k)$. (Hint: Suppose there were an affine change of coordinates T such that $V(X_{m+1}, \ldots, X_n)^T = V(X_{s+1}, \ldots, X_n)$, $m < s$; show that $T_{m+1}, \ldots, T_n$ would be dependent.)

Solution. Let $V \subset \mathbb{A}^n(k)$ be a linear subvariety, so

$$V = V(F_1, \ldots, F_r),$$

where each F_i is a polynomial of degree 1.

(a) An affine change of coordinates on $\mathbb{A}^n$ has the form

$$T(x) = Ax + b,$$

where $A \in \mathrm{M}_n(k)$ and $b \in k^n$. If F is a linear polynomial, then $F \circ T$ is again a linear polynomial, since composition with T preserves degree.

Now

$$V^T = \{x \in \mathbb{A}^n \mid T(x) \in V\} = V(F_1 \circ T, \ldots, F_r \circ T),$$

and each $F_i \circ T$ has degree 1. Hence V^T is again a linear subvariety of $\mathbb{A}^n(k)$.

(b) Assume $V \neq \varnothing$. We argue by induction on r, the number of defining linear equations.

If $r = 1$, then $V = V(F)$ for some nonzero linear polynomial F. By an affine change of coordinates, we may assume $F = X_n$, so

$$V = V(X_n).$$

Assume the statement holds for $r - 1$ equations. Write

$$V = V(F_1, \ldots, F_{r-1}, F_r).$$

By the induction hypothesis, there exists an affine change of coordinates T such that

$$V(F_1, \ldots, F_{r-1})^T = V(X_{m+1}, \ldots, X_n)$$

for some m. Replacing V by V^T, we may assume

$$V = V(X_{m+1}, \ldots, X_n, F_r),$$

where F_r is linear. If F_r is a linear combination of $X_{m+1}, \ldots, X_n$, then it adds no new condition and can be discarded. Otherwise, F_r has a nonzero component in the variables $X_1, \ldots, X_m$, and by a further affine change of coordinates among those variables we may assume $F_r = X_m$.

Thus, after an affine change of coordinates,

$$V = V(X_m, X_{m+1}, \ldots, X_n),$$

which proves the claim. In particular, V is an affine variety.

(c) Suppose there are affine changes of coordinates T and T' such that

$$V^T = V(X_{m+1}, \ldots, X_n), \qquad V^{T'} = V(X_{s+1}, \ldots, X_n),$$

with $m < s$. Then

$$V(X_{m+1}, \ldots, X_n)^{T^{-1}T'} = V(X_{s+1}, \ldots, X_n).$$

This means that under the affine transformation $T^{-1}T'$, the linear forms $X_{m+1}, \ldots, X_n$ are sent to linear combinations of $X_{s+1}, \ldots, X_n$. Since $s > m$, this forces $T_{m+1}, \ldots, T_n$ to be linearly dependent, contradicting the invertibility of the linear part of $T^{-1}T'$.

Hence m is independent of the choice of affine coordinates. This integer m is called the dimension of V.

Finally, the projection

$$(X_1, \ldots, X_n) \longmapsto (x_1, \ldots, x_m)$$

induces an isomorphism of varieties

$$V(X_{m+1}, \ldots, X_n) \cong \mathbb{A}^m(k).$$

Therefore V is isomorphic, as a variety, to $\mathbb{A}^m(k)$. □

Exercise 2.10.15. Let $P = (a_1, \ldots, a_n), Q = (b_1, \ldots, b_n)$ be distinct points of $\mathbb{A}^n$. The line through P and Q is defined to be $\{(a_1 + t(b_1 - a_1), \ldots, a_n + t(b_n - a_n)) \mid t \in k\}$.

(a) Show that if L is the line through P and Q, and T is an affine change of coordinates, then $T(L)$ is the line through $T(P)$ and $T(Q)$.

(b) Show that a line is a linear subvariety of dimension 1, and that a linear subvariety of dimension 1 is the line through any two of its points.

(c) Show that, in $\mathbb{A}^2$, a line is the same thing as a hyperplane.

(d) Let $P, P' \in \mathbb{A}^2$, L_1, L_2 two distinct lines through P, L_1', L_2' distinct lines through P'. Show that there is an affine change of coordinates T of $\mathbb{A}^2$ such that $T(P) = P'$ and $T(L_i) = L_i'$, $i = 1, 2$.

Solution. Let $P = (a_1, \ldots, a_n)$ and $Q = (b_1, \ldots, b_n)$ be distinct points of $\mathbb{A}^n$, and let L be the line through P and Q:

$$L = \{\, P + t(Q - P) \mid t \in k \,\}.$$

(a) Let $T(x) = Ax + c$ be an affine change of coordinates, with $A \in \mathrm{M}_n(k)$. For $x = P + t(Q - P) \in L$ we have

$$T(x) = A(P + t(Q - P)) + c = (AP + c) + tA(Q - P) = T(P) + t(T(Q) - T(P)).$$

Hence

$$T(L) = \{\, T(P) + t(T(Q) - T(P)) \mid t \in k \,\},$$

which is exactly the line through $T(P)$ and $T(Q)$.

(b) By an affine change of coordinates, any line $L \subset \mathbb{A}^n$ can be sent to

$$V(X_2, \ldots, X_n),$$

which is a linear subvariety of dimension 1. Hence every line is a linear subvariety of dimension 1.

Conversely, let $V \subset \mathbb{A}^n$ be a linear subvariety of dimension 1. By Problem 2.14, there exists an affine change of coordinates T such that

$$V^T = V(X_2, \ldots, X_n).$$

The set $V(X_2, \ldots, X_n)$ is the line through $(0, \ldots, 0)$ and $(1, 0, \ldots, 0)$, so V itself is the line through any two distinct of its points.

(c) In $\mathbb{A}^2$, a hyperplane is the zero set of a single nonzero linear polynomial, hence has dimension 1. By part (b), linear subvarieties of dimension 1 are exactly lines. Therefore, in $\mathbb{A}^2$, lines and hyperplanes coincide.

(d) Let $P, P' \in \mathbb{A}^2$, and let L_1, L_2 be two distinct lines through P, and L_1', L_2' two distinct lines through P'.

First translate $\mathbb{A}^2$ so that P is sent to the origin and P' is also sent to the origin. Thus we may assume

$$P = P' = (0, 0).$$

Each line through the origin is determined by a one-dimensional linear subspace of k^2. Since $L_1 \neq L_2$, their direction vectors form a basis of k^2, and similarly for L_1', L_2'.

Hence there exists a linear automorphism $A \in \mathrm{GL}_2(k)$ sending the direction of L_i to that of L_i', for $i = 1, 2$. Extending A to an affine transformation $T(x) = Ax$, we obtain

$$T(P) = P', \qquad T(L_i) = L_i', \quad i = 1, 2.$$

Thus there exists an affine change of coordinates of $\mathbb{A}^2$ sending P to P' and each L_i to L_i'. □

Exercise 2.10.16. Let $k = \mathbb{C}$. Give $\mathbb{A}^n(\mathbb{C}) = \mathbb{C}^n$ the usual topology. Recall that a topological space X is path-connected if for any $P, Q \in X$, there is a continuous mapping $\gamma : [0, 1] \to X$ such that $\gamma(0) = P, \gamma(1) = Q$.

(a) Show that $\mathbb{C} \setminus S$ is path-connected for any finite set S.

(b) Let V be an algebraic set in $\mathbb{A}^n(\mathbb{C})$. Show that $\mathbb{A}^n(\mathbb{C}) \setminus V$ is path-connected. (Hint: If $P, Q \in \mathbb{A}^n(\mathbb{C}) \setminus V$, let L be the line through P and Q. Then $L \cap V$ is finite, and L is isomorphic to $\mathbb{A}^1(\mathbb{C})$.)

Solution. Throughout let $k = \mathbb{C}$ and give $\mathbb{A}^n(\mathbb{C}) = \mathbb{C}^n$ the usual (Euclidean) topology.

(a) This is clear.

(b) Let $V \subset \mathbb{A}^n(\mathbb{C})$ be an algebraic set, and let $P, Q \in \mathbb{A}^n(\mathbb{C}) \setminus V$. Let L be the line through P and Q. Note that L is not contained in V, or else we would have $P, Q \in V$.

Then, $L \cap V$ is a finite set. We may identify L with $\mathbb{C}$. By part (a), $L \setminus (L \cap V)$ is path-connected, so there exists a continuous path in $L \setminus (L \cap V)$ joining P and Q. Since

$$L \setminus (L \cap V) \subset \mathbb{A}^n(\mathbb{C}) \setminus V,$$

this path is also a path in $\mathbb{A}^n(\mathbb{C}) \setminus V$. Therefore $\mathbb{A}^n(\mathbb{C}) \setminus V$ is path-connected. □

Exercise 2.10.17. Let $V = V(Y^2 - X^2(X+1)) \subset \mathbb{A}^2$, and $\overline{X}, \overline{Y}$ the residues of X, Y in $\Gamma(V)$; let $z = \overline{Y}/\overline{X} \in k(V)$. Find the pole sets of z and of z^2.

Solution. Let

$$V = V\big(Y^2 - X^2(X+1)\big) \subset \mathbb{A}^2_k,$$

and let $\Gamma(V) = k[X,Y]/(Y^2 - X^2(X+1))$. Denote by $\overline{X}, \overline{Y}$ the residue classes of X, Y in $\Gamma(V)$, and set

$$z = \frac{\overline{Y}}{\overline{X}} \in k(V).$$

Step 1: Simplification of z^2. In $\Gamma(V)$ we have the relation

$$\overline{Y}^2 = \overline{X}^2(\overline{X}+1).$$

Hence in the function field $k(V)$,

$$z^2 = \frac{\overline{Y}^2}{\overline{X}^2} = \overline{X} + 1.$$

Thus z^2 is a regular function on V, namely the image of $X + 1 \in k[X,Y]$.

Step 2: Pole set of z^2. Since $z^2 = \overline{X} + 1 \in \Gamma(V)$ is regular everywhere on V, it has no poles. Therefore

$$\mathrm{Pole}(z^2) = \varnothing.$$

Step 3: Pole set of z. By definition,

$$z = \frac{\overline{Y}}{\overline{X}},$$

so possible poles of z occur at points of V where $\overline{X} = 0$. On V, the equation $\overline{X} = 0$ forces $\overline{Y}^2 = 0$, hence $\overline{Y} = 0$. Thus, there is a unique point $P = (0,0) \in V$ with $X = 0$. To determine whether z actually has a pole at P, note that in the local ring $\mathcal{O}_{V,P}$ we have

$$z^2 = \overline{X} + 1,$$

which is a unit since $\overline{X}+1$ evaluates to 1 at P. Suppose z is regular at 0. This would mean that z is in the local ring of P, and since its square is a unit, it would follow that z is also a unit. Thus, we would have elements $\alpha, \beta \in \Gamma(V)$ such that $z = \alpha/\beta$, $\alpha(P) \neq 0$ and $\beta(P) \neq 0$. It follows that in this local ring, $\overline{Y}$ is in the ideal generated by $\overline{X}$, and so this local ring would be a DVR, which would imply that the multiplicity of P is 1. However, it is clear that the multiplicity at P is 2. This is a contradiction. Thus, z has a pole at $(0,0)$.

Conclusion.

$$\text{Pole}(z) = \{(0,0)\}, \qquad \text{Pole}(z^2) = \varnothing.$$

□

Exercise 2.10.18. Let $\mathcal{O}_P(V)$ be the local ring of a variety V at a point P. Show that there is a natural one-to-one correspondence between the prime ideals in $\mathcal{O}_P(V)$ and the subvarieties of V that pass through P. (Hint: If I is prime in $\mathcal{O}_P(V)$, $I \cap \Gamma(V)$ is prime in $\Gamma(V)$, and I is generated by $I \cap \Gamma(V)$; use Problem 2.10.2.)

Solution. Similar to solution of Problem 2.10.2. □

Exercise 2.10.19. Let f be a rational function on a variety V. Let $U = \{P \in V \mid f \text{ is defined at } P\}$. Then f defines a function from U to k. Show that this function determines f uniquely.

Solution. Suppose g is another rational function. Let us write $f = a/b$, and $g = c/d$ where $a, b, c, d \in \Gamma(V)$ and $b \neq 0, d \neq 0$. Then we may write $f = ad/bd$ and $g = bc/bd$. This shows that both f and g are defined on the subset $U' = V \setminus V(bd)$. Let us assume that both these are equal on this subset. Then we have that as functions on U', $ad - bc = 0$. We claim that $ad - bc$ is 0 as a function on all of V. Consider the function $(ad - bc)bd$. Given a point $P \in V$, it is either in $V(bd)$ or it is in U'. In either case, this function vanishes. As $\Gamma(V)$ is a domain and $bd \neq 0$, it follows that $ad - bc = 0$. It follows that f and g are equal in $k(V)$. This shows that a rational function is determined by its restriction to any open subset where it is defined. □

Exercise 2.10.20. In the example given in this section, show that it is impossible to write $f = a/b$, where $a, b \in \Gamma(V)$, and $b(P) \neq 0$ for every P where f is defined. Show that the pole set of f is exactly $\{(x, y, z, w) \mid y = 0 \text{ and } w = 0\}$.

Solution. We summarize the structure of the example.

The rational function f in the text has the form

$$f = \frac{A}{B},$$

where $A, B \in \Gamma(V)$ but B vanishes along a codimension-2 subset of V. If f could be written as a/b with $b(P) \neq 0$ for every point where f is defined, then the pole set would be contained in the zero locus of b, which would be a hypersurface. But the example shows that the true pole set is

$$Y = 0, \quad W = 0,$$

which is the intersection of two hypersurfaces, not itself a hypersurface.

Thus no single $b \in \Gamma(V)$ can vanish exactly on this set, so f cannot be written in the form a/b with b regular and nonvanishing on its domain of definition.

Therefore the pole set of f is exactly

$$\mathrm{Pole}(f) = \{y = 0,\ w = 0\}.$$

□

Exercise 2.10.21. Let $\varphi : V \to W$ be a polynomial map of affine varieties, $\tilde{\varphi} : \Gamma(W) \to \Gamma(V)$ the induced map on coordinate rings. Suppose $P \in V$, $\varphi(P) = Q$. Show that $\tilde{\varphi}(\mathfrak{m}_Q(W)) \subset \mathfrak{m}_P(V)$. Show that $\tilde{\varphi}$ extends uniquely to a ring homomorphism from $\mathcal{O}_Q(W)$ to $\mathcal{O}_P(V)$. Show that $\tilde{\varphi}(\mathfrak{m}_Q(W)) \subset \mathfrak{m}_P(V)$.

Solution. Let $f \in \mathfrak{m}_Q(W)$. Then $\tilde{\varphi}(f) = f \circ \varphi$. Clearly, $\tilde{\varphi}(f)(P) = f(Q) = 0$. Thus, $\tilde{\varphi}(f) \in \mathfrak{m}_P(V)$. It follows that $\mathfrak{m}_Q(W) \subset \tilde{\varphi}^{-1}(\mathfrak{m}_P(V))$. However, note that $\mathfrak{m}_Q(W)$ is a maximal ideal of $\Gamma(W)$ and so this forces that either $\mathfrak{m}_Q(W) = \tilde{\varphi}^{-1}(\mathfrak{m}_P(V))$, or $\tilde{\varphi}^{-1}(\mathfrak{m}_P(V)) = \Gamma(W)$. The latter is not possible as $1 \notin \tilde{\varphi}^{-1}(\mathfrak{m}_P(V))$ since $\tilde{\varphi}(1) = 1 \notin \mathfrak{m}_P(V)$.

We use the universal property of localization. The local rings are

$$\mathscr{O}_Q(W) = \Gamma(W)_{\mathfrak{m}_Q(W)}, \qquad \mathscr{O}_P(V) = \Gamma(V)_{\mathfrak{m}_P(V)}.$$

Since $\tilde{\varphi} : \Gamma(W) \to \Gamma(V)$ and

$$\mathfrak{m}_Q(W) = \tilde{\varphi}^{-1}(\mathfrak{m}_P(V))$$

every element of $\Gamma(W) \setminus \mathfrak{m}_Q(W)$ maps into $\Gamma(V) \setminus \mathfrak{m}_P(V)$. Thus $\tilde{\varphi}$ satisfies the universal condition to extend uniquely to a homomorphism of localizations:

$$\tilde{\varphi} : \Gamma(W)_{\mathfrak{m}_Q(W)} \to \Gamma(V)_{\mathfrak{m}_P(V)}.$$

This is the desired extension to local rings. □

Exercise 2.10.22. Let $T : \mathbb{A}^n \to \mathbb{A}^n$ be an affine change of coordinates, $T(P) = Q$. Show that $\tilde{T} : \mathcal{O}_Q(\mathbb{A}^n) \to \mathcal{O}_P(\mathbb{A}^n)$ is an isomorphism. Show that $\tilde{T}$ induces an isomorphism from $\mathcal{O}_Q(V)$ to $\mathcal{O}_P(V^T)$ if $P \in V^T$ for V a subvariety of $\mathbb{A}^n$.

Solution. Affine coordinate changes are isomorphisms of varieties.

On coordinate rings,

$$\tilde{T} : k[X_1, \ldots, X_n] \to k[X_1, \ldots, X_n]$$

is an isomorphism. Localizing at the maximal ideals corresponding to Q and P yields

$$\tilde{T} : \mathscr{O}_Q(\mathbb{A}^n) \xrightarrow{\sim} \mathscr{O}_P(\mathbb{A}^n),$$

which is again an isomorphism.

If $V \subseteq \mathbb{A}^n$ is a subvariety and $P \in V^T = T(V)$, then T restricts to an isomorphism $V \to V^T$. Thus the same coordinate-change argument applied to coordinate rings and their localizations gives

$$\mathscr{O}_Q(V) \xrightarrow{\sim} \mathscr{O}_P(V^T).$$

□

Exercise 2.10.23. Show that the order function on K is independent of the choice of uniformizing parameter.

Solution. Let R be a discrete valuation ring with quotient field K. Let t and t' be two uniformizing parameters of R. Since both t and t' generate the maximal ideal of R, there exists a unit $u \in R^\times$ such that $t' = ut$. Let $z \in K^\times$. Using the uniformizing parameter t, we may write uniquely $z = vt^n$, where $v \in R^\times$ and $n \in \mathbb{Z}$. Rewriting this expression in terms of t', we obtain $z = v(u^{-1}t')^n = (vu^{-n})(t')^n$. Since u and v are units in R, the element vu^{-n} is also a unit in R. Therefore, the exponent of t' appearing in the factorization of z is again n. Hence, $\mathrm{ord}_t(z) = \mathrm{ord}_{t'}(z)$.This shows that the order function on K is independent of the choice of uniformizing parameter. □

Exercise 2.10.24. Let $V = \mathbb{A}^1, \Gamma(V) = k[X], K = k(V) = k(X)$.

(a) For each $a \in k = V$, show that $\mathcal{O}_a(V)$ is a DVR with uniformizing parameter $t = X - a$.

(b) Show that $\mathcal{O}_\infty = \{F/G \in k(X) \mid \deg(G) \geq \deg(F)\}$ is also a DVR, with uniformizing parameter $t = 1/X$.

Solution. Let $V = \mathbb{A}^1$, so that $\Gamma(V) = k[X]$ and $k(V) = k(X)$.
(a) Let $a \in k$. The local ring of V at a is

$$\mathcal{O}_a(V) = \left\{ \frac{f}{g} \in k(X) \mid g(a) \neq 0 \right\}.$$

Its maximal ideal is

$$\mathfrak{m}_a = \left\{ \frac{f}{g} \in \mathcal{O}_a(V) \mid f(a) = 0 \right\}.$$

If $f(a) = 0$, then f is divisible by $X - a$, hence every element of $\mathfrak{m}_a$ is divisible by $X - a$. Therefore, $\mathfrak{m}_a = (X - a)$.

Every nonzero element of $k(X)$ can be written uniquely in the form $z = u(X - a)^n$, where $u \in \mathcal{O}_a(V)^\times$ and $n \in \mathbb{Z}$. Hence $\mathcal{O}_a(V)$ is a discrete valuation ring with uniformizing parameter $t = X - a$.

(b) Define

$$\mathcal{O}_\infty = \left\{ \frac{F}{G} \in k(X) \mid \deg(G) \geq \deg(F) \right\}.$$

This is a subring of $k(X)$ and corresponds to functions having no pole at infinity. The maximal ideal consists of those elements satisfying $\deg(G) > \deg(F)$. We first, observe that $\frac{1}{X} \in \mathcal{O}_\infty$, since $\deg(1) = 0$ and $\deg(X) = 1$. Now, let $z \in \mathcal{O}_\infty$ be nonzero. Write $z = \frac{F(X)}{G(X)}$, with $\deg G \geq \deg F$. Set $n = \deg G - \deg F \geq 0$. Then

$$z = \frac{F(X)X^n}{G(X)} \left(\frac{1}{X} \right)^n.$$

Let $u = \frac{F(X)X^n}{G(X)}$. Since $\deg(FX^n) = \deg(F) + n = \deg(G)$, the numerator and denominator of u have the same degree. Hence $u \in \mathcal{O}_\infty$ and $u^{-1} \in \mathcal{O}_\infty$, so u is a unit of $\mathcal{O}_\infty$.

Therefore, every nonzero element $z \in \mathcal{O}_\infty$ can be written in the form

$$z = u \left(\frac{1}{X} \right)^n,$$

where $u \in \mathcal{O}_\infty^\times$ and $n \geq 0$.

To see that this expression is unique, suppose

$$u \left(\frac{1}{X} \right)^n = v \left(\frac{1}{X} \right)^m$$

with $u, v \in \mathcal{O}_\infty^\times$ and $n \leq m$. Then

$$\frac{u}{v} = \left(\frac{1}{X} \right)^{m-n}.$$

The left-hand side is a unit of $\mathcal{O}_\infty$, while the right-hand side lies in the maximal ideal unless $m - n = 0$. Hence $m = n$ and $u = v$. Thus $\mathcal{O}_\infty$ is a discrete valuation ring with uniformizing parameter $t = \frac{1}{X}$. □

Exercise 2.10.25. Let $p \in \mathbb{Z}$ be a prime number. Show that $R = \{r \in \mathbb{Q} \mid r = a/b, a, b \in \mathbb{Z}, p \text{ doesn't divide } b\}$ is a DVR with quotient field $\mathbb{Q}$.

Solution. Let $p \in \mathbb{Z}$ be a prime number, and define

$$R = \left\{ \frac{a}{b} \in \mathbb{Q} \mid a, b \in \mathbb{Z},\ p \nmid b \right\}.$$

As $R \subset \mathbb{Q}$ thus R is a domain. An element $\frac{a}{b} \in R$ is a unit if and only if its inverse $\frac{b}{a}$ lies in R, which holds precisely when $p \nmid a$. Hence the non-units of R are exactly those fractions whose numerator is divisible by p. Let

$$\mathfrak{m} = \left\{ \frac{a}{b} \in R \mid p \mid a \right\}.$$

Every element of $\mathfrak{m}$ is divisible by p, and clearly $p \in \mathfrak{m}$, so

$$\mathfrak{m} = (p).$$

Thus R is a local ring with principal maximal ideal (p). Now we will show that R has descrete valution property. As every nonzero rational number $q \in \mathbb{Q}$ can be written uniquely as

$$q = p^n \cdot \frac{a}{b},$$

where $a, b \in \mathbb{Z}$, $p \nmid a$, $p \nmid b$, and $n \in \mathbb{Z}$. Then $q \in R$ if and only if $n \geq 0$, and q is a unit of R if and only if $n = 0$. Thus every element of R has the form up^n with u a unit and $n \geq 0$. Therefore R is a discrete valuation ring with uniformizing parameter p.

Let $\frac{a}{b} \in \mathbb{Q}$. Write $b = p^k b'$ with $p \nmid b'$. Then

$$\frac{a}{b} = \frac{a}{b'} \cdot \frac{1}{p^k},$$

where $\frac{a}{b'} \in R$ and $p^k \in R$. Hence every element of $\mathbb{Q}$ is a quotient of two elements of R.

Thus the quotient field of R is $\mathbb{Q}$. □

Exercise 2.10.26. Let R be a DVR with quotient field K; let $\mathfrak{m}$ be the maximal ideal of R.

(a) Show that if $z \in K, z \notin R$ then $z^{-1} \in \mathfrak{m}$.

(b) Suppose $R \subset S \subset K$ and S is also a DVR. Suppose the maximal ideal of S contains $\mathfrak{m}$. Show that $S = R$. (We emphasize that both of them have the same quotient field.)

Solution. Let R be a discrete valuation ring with quotient field K and maximal ideal $\mathfrak{m}$.

(a) Suppose $z \in K$ and $z \notin R$. Since

$$R = \{x \in K \mid \operatorname{ord}(x) \geq 0\},$$

we have $\operatorname{ord}(z) < 0$. Then

$$\operatorname{ord}(z^{-1}) = -\operatorname{ord}(z) > 0,$$

which implies

$$z^{-1} \in \mathfrak{m}.$$

This proves part (a).

(b) Suppose $R \subset S \subset K$, where S is also a discrete valuation ring, and assume that the maximal ideal $\mathfrak{m}_S$ of S contains $\mathfrak{m}$. Let t be a uniformizing parameter of R, so $\mathfrak{m} = tR \subset \mathfrak{m}_S$. Let s be a uniformizing parameter of S, so $\mathfrak{m}_S = sS$. Since $t \in \mathfrak{m}_S$, the element t is not a unit in S. Thus,

$$t = us^n,$$

for some unit $u \in S^\times$ and integer $n \geqslant 1$. If $s \in R$ and if it is a unit in R, then it follows it is a unit in S, which is a contradiction. Thus, $s = vt^m$ for some $m \geqslant 1$ and a unit $v \in R$. Since v is a unit in R, it follows it is a unit in S. Thus, we get

$$t = uv^n t^{mn}\,.$$

It follows that t^{mn-1} is a unit in S, and so $m = n = 1$. From this it follows that u is a unit in R. Let $f \in K$ and write $f = u't^n$, where u' is a unit in R. Then $\operatorname{ord}_R(f) = n$. Note that $f = u'(us)^n$, where u, u' are units in S. Thus, $\operatorname{ord}_S(f) = n$. It follows that both the order functions are the same, and since R is the set of elements f such that $\operatorname{ord}_R(f) \geqslant 0$, it follows that $R = S$.

If $s \notin R$, then $s^{-1} \in R$, which shows that $s^{-1} \in S$, which is a contradiction as $s \in \mathfrak{m}_S$.

Thus, $R = S$. This completes the proof of (b). □

Exercise 2.10.27. Show that the DVR's of Problem 2.10.24 are the only DVR's with quotient field $k(X)$ that contain k. Show that those of Problem 2.10.25 are the only DVR's with quotient field $\mathbb{Q}$.

Solution. (a) DVRs of $k(X)$ containing k.

Let R be a DVR with quotient field $k(X)$, and suppose $k \subset R$. Let ord be the associated order function on $k(X)$.

Since $k^\times \subset R^\times$, we have

$$\operatorname{ord}(c) = 0 \quad \text{for all } c \in k^\times.$$

We will consider $\mathrm{ord}(X)$.
Case 1: $\mathrm{ord}(X) > 0$. Then X lies in the maximal ideal of R, hence is not a unit. Clearly, $k[X] \subset R$. The maximal ideal of R intersected with $k[X]$ is nonzero since it contains X. Moreover, this is a nonzero prime ideal in a PID and so is maximal. Thus, it is forced to be (X). It follows that if $f(X) \in k[X]$ is such that $f(X) \notin (X)$, then $f(X)$ is a unit in R. Thus, we have an inclusion of DVR's

$$k[X]_{(X)} \subset R \subset k(X)\,.$$

From Problem 2.10.26 it follows that $k[X]_{(X)} = R$.

Case 2: $\mathrm{ord}(X) = 0$. Then X is a unit in R. Again $k[X] \subset R$. If $\mathfrak{m}_R \cap k[X] = 0$, then since all nonzero constants are also units, every polynomial is a unit, forcing R to be equal to $k(X)$, a field. This contradicts the assumption that R is a DVR, so this case is impossible. As before, since $\mathfrak{m}_R \cap k[X] \neq 0$, it is a maximal ideal, $(X - a)$. Thus, as before, it follows that $k[X]_{(X-a)} = R$.

Case 3: $\mathrm{ord}(X) < 0$. Then $1/X$ lies in the maximal ideal of R. Let $Y = 1/X$. Then note that $k(X) = k(Y)$ and $\mathrm{ord}(Y) > 0$, so we reduce to case 1. It follows that $R = k[Y]_{(Y)}$. Let us check that this equals $\mathcal{O}_\infty$. Note that $f(Y)/g(Y) \in k[Y]_{(Y)}$ iff $g(Y) \neq 0$, that is, iff $g(Y) = a_0 + a_1 Y + \ldots + a_n Y^n$ with $a_0 \neq 0$. Let us write $f(Y) = b_0 + \ldots + b_m Y^m$, $b_m \neq 0$. Then

$$\frac{f(Y)}{g(Y)} = \frac{X^n(b_0 X^m + b_1 X^{m-1} + \ldots + b_m)}{X^m(a_0 X^n + a_1 X^{n-1} + \ldots + a_n)}\,.$$

Since $a_0 \neq 0$, it follows that $f(Y)/g(Y) \in \mathcal{O}_\infty$. Conversely, suppose $f(X)/g(X) \in \mathcal{O}_\infty$, then

$$\frac{f(X)}{g(X)} = \frac{b_n X^n + \ldots + b_0}{a_m X^m + \ldots + a_0}\,,$$

with $b_n \neq 0$, $a_m \neq 0$ and $m \geqslant n$. Then

$$\frac{f(X)}{g(X)} = \frac{Y^m(b_n + \ldots + b_0 Y^n)}{Y^n(a_m + \ldots + a_0 Y^m)} = \frac{Y^{m-n}(b_n + \ldots + b_0 Y^n)}{a_m + \ldots + a_0 Y^m}\,.$$

Clearly, the denominator does not vanish when we put $Y = 0$. It follows that $k[Y]_{(Y)} = \mathcal{O}_\infty$.

(b) DVRs of $\mathbb{Q}$.

Let R be a DVR with quotient field $\mathbb{Q}$, and let $\mathfrak{m}$ be its maximal ideal. Since R is not a field, $\mathfrak{m}$ contains a nonzero integer. Let n be the smallest positive integer in $\mathfrak{m}$.

If $n = ab$ with $1 < a, b < n$, then

$$\mathrm{ord}(n) = \mathrm{ord}(a) + \mathrm{ord}(b) > 0,$$

so at least one of a or b lies in $\mathfrak{m}$, contradicting the minimality of n. Hence n is prime, say $n = p$.

Every element of $\mathbb{Q}$ can be written uniquely in the form $p^l u$, where u is a unit of R and $l \in \mathbb{Z}$. Therefore,

$$R = \left\{ \frac{a}{b} \in \mathbb{Q} \mid p \nmid b \right\},$$

which is exactly the DVR described in Problem 2.25. □

Exercise 2.10.28. An order function on a field K is a function φ from $K \setminus \{0\}$ onto $\mathbb{Z}$, satisfying:

(i) $\varphi(a) = \infty$ if and only if $a = 0$;

(ii) $\varphi(ab) = \varphi(a) + \varphi(b)$;

(iii) $\varphi(a + b) \geq \min(\varphi(a), \varphi(b))$.

Show that $R = \{z \in K \mid \varphi(z) \geq 0\}$ is a DVR with maximal ideal $\mathfrak{m} = \{z \mid \varphi(z) > 0\}$, and quotient field K. Conversely, show that if R is a DVR with quotient field K, then the function ord: $K \to \mathbb{Z} \cup \{\infty\}$ is an order function on K.

Solution. Define

$$R = \{z \in K \mid \varphi(z) \geq 0\}, \qquad \mathfrak{m} = \{z \in K \mid \varphi(z) > 0\}.$$

It is clear that R is a ring and since $R \subset K$ and K is a field, R is an integral domain. As $\varphi(1) = \varphi(1 \cdot 1) = 2\varphi(1) \implies \varphi(1) = 0$. If $\varphi(z) = 0$, then $\varphi(z^{-1}) = 0$, so z is a unit of R. Conversely, if z is a unit then $\varphi(zz^{-1}) = \varphi(z) + \varphi(z^{-1}) = \varphi(1) = 0$. Since both $\varphi(z), \varphi(z^{-1})$ are $\geqslant 0$, it follows that both are equal to 0. Thus, z is a unit iff $\varphi(z) = 0$. It follows that $\mathfrak{m}$ is the unique maximal ideal of R, and R is a local ring.

Since φ maps onto $\mathbb{Z}$, there exists $t \in K$ such that $\varphi(t) = 1$. For any nonzero $z \in R$, let $\varphi(z) = n \geq 0$. Then

$$\varphi(zt^{-n}) = 0,$$

so zt^{-n} is a unit of R. Thus, every element of R can be written uniquely in the form $z = ut^n$, where u is a unit of R. In particular, $\mathfrak{m} = (t)$, and R is a discrete valuation ring with quotient field K.

Now we will prove the converse. Assume R is a DVR with quotient field K, then the function ord: $K \to \mathbb{Z} \cup \{\infty\}$ is an order function on K.

(i) By definition, $\text{ord}(0) = \infty$. If $z \neq 0$, then $z = ut^n$ for some $n \in \mathbb{Z}$, so $\text{ord}(z) = n < \infty$. Thus $\text{ord}(z) = \infty$ if and only if $z = 0$.

(ii) Let $a, b \in K^\times$, and write

$$a = ut^m, \qquad b = vt^n,$$

with $u, v \in R^\times$. Then

$$ab = (uv)t^{m+n}.$$

Since uv is a unit of R, it follows that

$$\operatorname{ord}(ab) = m + n = \operatorname{ord}(a) + \operatorname{ord}(b).$$

(iii) Let $a, b \in K$. If $a + b = 0$, then $\operatorname{ord}(a + b) = \infty$, and the inequality is trivial. Assume $a + b \neq 0$, and write

$$a = ut^m, \qquad b = vt^n,$$

with $u, v \in R^\times$ and $m \leq n$. Then

$$a + b = t^m\big(u + vt^{n-m}\big).$$

Since $t^{n-m} \in \mathfrak{m}$ and u is a unit, the element $u + vt^{n-m}$ is a unit of R. Hence

$$\operatorname{ord}(a + b) = m = \min(m, n) = \min\big(\operatorname{ord}(a), \operatorname{ord}(b)\big).$$

In particular,

$$\operatorname{ord}(a + b) \geq \min\big(\operatorname{ord}(a), \operatorname{ord}(b)\big).$$

Therefore, ord satisfies all the axioms of an order function.

Therefore, giving a DVR with quotient field K is equivalent to giving an order function on K. □

Exercise 2.10.29. Let R be a DVR with quotient field K, ord the order function on K.

(a) If $\operatorname{ord}(a) < \operatorname{ord}(b)$, show that $\operatorname{ord}(a + b) = \operatorname{ord}(a)$.

(b) If $a_1, \ldots, a_n \in K$, and for some i, $\operatorname{ord}(a_i) < \operatorname{ord}(a_j)$ (all $j \neq i$), then $a_1 + \cdots + a_n \neq 0$.

Solution. (a) Assume $\operatorname{ord}(a) < \operatorname{ord}(b)$.

If $a + b = 0$, then $a = -b$, so $\operatorname{ord}(a) = \operatorname{ord}(b)$, which contradicts the hypothesis. Hence $a + b \neq 0$.

Write

$$a = ut^m, \qquad b = vt^n,$$

where $u, v \in R^\times$, t is a uniformizing parameter, and $m = \operatorname{ord}(a)$, $n = \operatorname{ord}(b)$ with $m < n$.

Then

$$a + b = t^m\big(u + vt^{n-m}\big).$$

Since $n - m > 0$, we have $t^{n-m} \in \mathfrak{m}$, so $vt^{n-m} \in \mathfrak{m}$. As u is a unit, the element $u + vt^{n-m}$ is also a unit of R.

Therefore,

$$\operatorname{ord}(a + b) = m = \operatorname{ord}(a).$$

(b) Suppose $a_1, \ldots, a_n \in K$ and that for some index i,

$$\operatorname{ord}(a_i) < \operatorname{ord}(a_j) \quad \text{for all } j \neq i.$$

Without loss of generality, assume $i = 1$. Suppose, for contradiction, that

$$a_1 + a_2 + \cdots + a_n = 0.$$

Then

$$a_1 = -(a_2 + \cdots + a_n).$$

By the valuation inequality,

$$\operatorname{ord}(a_2 + \cdots + a_n) \;\geq\; \min_{j \geq 2} \operatorname{ord}(a_j).$$

By hypothesis,

$$\min_{j \geq 2} \operatorname{ord}(a_j) \;>\; \operatorname{ord}(a_1).$$

Hence,

$$\operatorname{ord}(a_2 + \cdots + a_n) \;>\; \operatorname{ord}(a_1).$$

But from $a_1 = -(a_2 + \cdots + a_n)$, we must have

$$\operatorname{ord}(a_1) = \operatorname{ord}(a_2 + \cdots + a_n),$$

a contradiction.

Therefore,

$$a_1 + a_2 + \cdots + a_n \neq 0.$$

□

Exercise 2.10.30. Let R be a DVR with maximal ideal $\mathfrak{m}$, and quotient field K, and suppose a field k is a subring of R, and that the composition $k \to R \to R/\mathfrak{m}$ is an isomorphism of k with $R/\mathfrak{m}$.

(a) For any $z \in R$, there is a unique $\lambda \in k$ such that $z - \lambda \in \mathfrak{m}$.

(b) Let t be a uniformizing parameter for $R, z \in R$. Then for any $n \geq 0$ there are unique $\lambda_0, \lambda_1, \ldots, \lambda_n \in k$ and $z_n \in R$ such that $z = \lambda_0 + \lambda_1 t + \cdots + \lambda_n t^n + z_n t^{n+1}$.

Solution. Let R be a DVR with maximal ideal $\mathfrak{m}$, quotient field K, and let $k \subset R$ be a subfield such that the natural composition

$$k \longrightarrow R \longrightarrow R/\mathfrak{m}$$

is an isomorphism.

(a) Let $z \in R$. Its image $\overline{z}$ in $R/\mathfrak{m}$ corresponds, via the given isomorphism, to a unique element $\lambda \in k$. Hence

$$\overline{z} = \overline{\lambda} \quad \text{in } R/\mathfrak{m},$$

which means

$$z - \lambda \in \mathfrak{m}.$$

Uniqueness is immediate due to the fact that if $z-\lambda, z-\mu \in \mathfrak{m}$, then $\lambda-\mu \in \mathfrak{m} \cap k = \{0\}$ since k is a field. Hence $\lambda = \mu$.

(b) Let t be a uniformizing parameter of R, so $\mathfrak{m} = (t)$. We proceed by induction on n.

Base case $n = 0$. By part (a), there exists a unique $\lambda_0 \in k$ such that

$$z - \lambda_0 \in \mathfrak{m} = (t).$$

Thus $z = \lambda_0 + z_0 t$ for some $z_0 \in R$.

Inductive step. Assume that for some $n \geq 0$ we have

$$z = \lambda_0 + \lambda_1 t + \cdots + \lambda_n t^n + z_n t^{n+1}, \qquad z_n \in R,$$

with $\lambda_0, \ldots, \lambda_n \in k$ uniquely determined.

Apply part (a) to z_n: there exists a unique $\lambda_{n+1} \in k$ such that

$$z_n - \lambda_{n+1} \in \mathfrak{m} = (t).$$

Thus $z_n = \lambda_{n+1} + z_{n+1} t$ with $z_{n+1} \in R$, and substituting gives

$$z = \lambda_0 + \lambda_1 t + \cdots + \lambda_{n+1} t^{n+1} + z_{n+1} t^{n+2}.$$

Uniqueness follows from the fact that at each step, λ_i is uniquely determined by reducing modulo $\mathfrak{m}$, so the entire expansion is unique. Thus every element $z \in R$ admits a unique truncated expansion in powers of the uniformizer t with coefficients in the residue field k, to arbitrary finite order. This is the algebraic shadow of power series expansions in a DVR. $\square$

Exercise 2.10.31. Let k be a field. Show that $k[[X]]$ is a ring containing $k[X]$ as a subring. Show that $k[[X]]$ is a DVR with uniformizing parameter X.

Solution. Let k be a field and let $k[[X]]$ denote the ring of formal power series

$$\sum_{i=0}^{\infty} a_i X^i \qquad (a_i \in k).$$

$k[[X]]$ is a ring containing $k[X]$ is obvious from the definition of the ring $k[[x]]$.

Let

$$f(X) = \sum_{i=0}^{\infty} a_i X^i \in k[[X]].$$

Then $f(X)$ is a unit in $k[[X]]$ if and only if $a_0 \neq 0$.

Indeed, if $a_0 \neq 0$, one constructs an inverse recursively by solving

$$f(X)g(X) = 1,$$

coefficient by coefficient. Conversely, if $a_0 = 0$, then $f(X)$ is divisible by X and cannot be invertible.

Hence the set

$$\mathfrak{m} = (X) = \{f(X) \in k[[X]] \mid a_0 = 0\}$$

is precisely the set of nonunits. Therefore (X) is the unique maximal ideal of $k[[X]]$, and $k[[X]]$ is a local ring.

We will now prove that $k[[x]]$ is a DVR. Every nonzero power series $f(X)$ can be written uniquely as

$$f(X) = X^n u(X),$$

where $n \geq 0$ and $u(X)$ is a unit in $k[[X]]$ (namely, $u(0) \neq 0$). Thus every ideal of $k[[X]]$ is of the form (X^n) (We have used the fact that $k[[x]]$ is a pid). Hence the ring $k[[X]]$ contains $k[X]$ as a subring and is a discrete valuation ring with uniformizing parameter X.

□

Exercise 2.10.32. Factor $Y^3 - 2XY^2 + 2X^2Y + X^3$ into linear factors in $\mathbb{C}[X, Y]$.

Solution. Let $F(X, Y) = Y^3 - 2XY^2 + 2X^2Y + X^3$. Each term has degree 3, hence F is a homogeneous polynomial of degree 3. Dehomogenizing F by setting $Y = 1$:

$$F_*(X) = F(X, 1) = 1 - 2X + 2X^2 + X^3 = X^3 + 2X^2 - 2X + 1.$$

Since $\mathbb{C}$ is algebraically closed, the polynomial $F_*(X)$ has three roots $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$, and hence

$$F_*(X) = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3) \quad \text{in } \mathbb{C}[X].$$

We factor $F_*(X)$ in $\mathbb{C}[X]$. By the homogenization process, we obtain

$$F(X, Y) = Y^3 F_*(X/Y) = (X - \alpha_1 Y)(X - \alpha_2 Y)(X - \alpha_3 Y)$$

Hence the factorization. □

Exercise 2.10.33. Suppose $F, G \in k[X_1, \ldots, X_n]$ are forms of degree $r, r+1$ respectively, with no common factors (k a field). Show that $F + G$ is irreducible.

Solution. Let $F, G \in k[X_1, \ldots, X_n]$ be forms of degrees r and $r+1$ respectively, with no common factors.

Suppose, for contradiction, that $F + G$ is reducible. Then there exist non-constant polynomials $A, B \in k[X_1, \ldots, X_n]$ such that

$$F + G = AB.$$

By writing A and B as sums of forms, and comparing homogeneous parts we easily conclude that $A = A_a + A_{a-1}$ and $B = B_b$. If we write $G = G_{r+1}$ and $F = F_r$, then it follows that $G_{r+1} = A_a B_b$ and $F_r = A_{a-1} B_b$. But this contradicts the fact that F and G have no common factor. □

Exercise 2.10.34. (a) Show that there are $d + 1$ monomials of degree d in $R[X, Y]$, and $(d + 1)(d + 2)/2$ monomials of degree d in $R[X, Y, Z]$.

(b) Let $V(d, n) = \{\text{forms of degree } d \text{ in } k[X_1, \ldots, X_n]\}$. Show that $V(d, n)$ is a vector space over k, and that the monomials of degree d form a basis.

(c) Let $L_1, L_2, \ldots$ and $M_1, M_2, \ldots$ be sequences of nonzero linear forms in $k[X, Y]$, and assume no $L_i = \lambda M_j, \lambda \in k$. Let $A_{ij} = L_1 \ldots L_i M_1 \ldots M_j$. Show that $\{A_{ij} \mid i + j = d\}$ forms a basis for $V(d, 2)$.

Solution. (a) A monomial of degree d in $R[X, Y]$ has the form $X^a Y^b$ with $a, b \geq 0$ and $a + b = d$. The number of nonnegative integer solutions of $a + b = d$ is $d + 1$. Hence there are $d + 1$ monomials of degree d in $R[X, Y]$.

A monomial of degree d in $R[X, Y, Z]$ has the form $X^a Y^b Z^c$ with $a, b, c \geq 0$ and $a + b + c = d$.

The number of such triples is given by bar and star formula giving number of solution to $x_1 + \cdots + x_k = n$

$$\binom{n+k-1}{k-1} = \binom{d+2}{2} = \frac{(d+1)(d+2)}{2} = 1 + 2 + \cdots + (d+1).$$

(b) Clear.
(c) Let $L_1, L_2, \ldots$ and $M_1, M_2, \ldots$ be sequences of nonzero linear forms in $k[X, Y]$ such that $L_i \neq \lambda M_j$ for all $\lambda \in k$. Define

$$A_{ij} = L_1 \cdots L_i \, M_1 \cdots M_j, \qquad i, j \geq 0,$$

with $A_{00} = 1$. If $i + j = d$, then A_{ij} is a homogeneous polynomial of degree d, so $A_{ij} \in V(d, 2)$.
There are $d + 1$ such polynomials. Suppose that

$$\sum_{i+j=d} c_{ij} A_{ij} = 0.$$

Note that except for A_{0d}, L_1 divides every A_{ij}. Thus, we get a contradiction if $c_{0d} \neq 0$. So $c_{0d} = 0$ and we may divide the entire equation by L_1. Next note that except for $A_{1,d-1}/L_1$, L_2 divides every A_{ij} in this new equation. This shows that $c_{1,d-1} = 0$. Proceeding in this way we see that all the coefficients are 0. This proves that the A_{ij} are linearly independent. □

Exercise 2.10.35. With the above notation, show that $\dim_k V(d, n) = \binom{d+n-1}{n-1}$.

Solution. Recall from Problem 2.35 that $V(d, n)$ has as a basis the set of monomials

$$X_1^{a_1} \cdots X_n^{a_n} \quad \text{with} \quad a_1 + \cdots + a_n = d, \quad a_i \geq 0.$$

Therefore, $\dim V(d, n)$ is equal to the number of nonnegative integer solutions of the equation $a_1 + \cdots + a_n = d$. This number is the coefficient of x^d in the series expansion of $(1 - x)^{-n}$. □

Exercise 2.10.36. What are the additive and multiplicative identities in $\prod R_i$? Is the map $R_i \to \prod R_j$ sending a_i to $(0, \ldots, a_i, \ldots, 0)$ a ring homomorphism?

Solution. Left to the reader. □

Exercise 2.10.37. Show that if $k \subset R_i$, and each R_i is finite-dimensional over k, then $\dim(\prod R_i) = \sum \dim R_i$.

Solution. This is clear. □

Exercise 2.10.38. Prove the following relations among ideals I_i, J, in a ring R:

(a) $(I_1 + I_2)J = I_1J + I_2J$.

(b) $(I_1 \cdots I_N)^n = I_1^n \cdots I_N^n$.

Solution. (a) is proved by showing both inclusions. (b) is clear as $IJ = JI$. □

Exercise 2.10.39. (a) Suppose I, J are comaximal ideals in R. Show that $I + J^2 = R$. Show that I^m and J^n are comaximal for all m, n.

(b) Suppose $I_1, \ldots, I_N$ are ideals in R, and I_i and $J_i = \bigcap_{j \neq i} I_j$ are comaximal for all i. Show that $I_1^n \cap \cdots \cap I_N^n = (I_1 \cdots I_N)^n = (I_1 \cap \cdots \cap I_N)^n$ for all n.

Solution. (a) Suppose I, J are comaximal.

(i) Show that $I + J^2 = R$.

Since $I + J = R$, there exist $a \in I$ and $b \in J$ such that

$$a + b = 1.$$

Squaring, we obtain

$$1 = (a + b)^2 = a^2 + 2ab + b^2.$$

Here $a^2, 2ab \in I$ and $b^2 \in J^2$. Hence

$$1 \in I + J^2,$$

so $I + J^2 = R$.

(ii) Show that I^m and J^n are comaximal for all m, n.

Since $a + b = 1$ with $a \in I$ and $b \in J$, we have

$$1 = (a + b)^{m+n}.$$

By the binomial theorem, each term in the expansion contains either at least m factors of a or at least n factors of b. Therefore, every term lies in I^m or J^n.

Hence,

$$1 \in I^m + J^n,$$

so

$$I^m + J^n = R.$$

(b) Suppose $I_1, \ldots, I_N$ are ideals and $I_i + J_i = R$, where $J_i = \bigcap_{j \neq i} I_j$.

Show that

$$I_1^n \cap \cdots \cap I_N^n = (I_1 \cdots I_N)^n = (I_1 \cap \cdots \cap I_N)^n.$$

Since $I_i + J_i = R$, by the lemma we have

$$I_i J_i = I_i \cap J_i.$$

But

$$J_i = \bigcap_{j \neq i} I_j,$$

so

$$I_i J_i = I_1 \cdots I_N.$$

Hence,

$$I_1 \cdots I_N = I_1 \cap \cdots \cap I_N.$$

By Problem 2.39(b),

$$(I_1 \cdots I_N)^n = I_1^n \cdots I_N^n.$$

Therefore,

$$(I_1 \cap \cdots \cap I_N)^n = (I_1 \cdots I_N)^n.$$

By part (a), the ideals I_i^n remain comaximal. Applying the lemma again, we obtain

$$I_1^n \cap \cdots \cap I_N^n = I_1^n \cdots I_N^n.$$

Combining the above equalities gives the desired result.

□

Exercise 2.10.40. Let I, J be ideals in a ring R. Suppose I is finitely generated and $I \subset \mathrm{Rad}(J)$. Show that $I^n \subset J$ for some n.

Solution. Since I is finitely generated, there exist elements

$$f_1, \ldots, f_m \in R$$

such that

$$I = (f_1, \ldots, f_m).$$

Since $I \subset \mathrm{Rad}(J)$, we have $f_i \in \mathrm{Rad}(J)$ for each i. By definition of the radical, for each i there exists a positive integer n_i such that

$$f_i^{n_i} \in J.$$

Let

$$N = n_1 + \cdots + n_m.$$

We claim that $I^N \subset J$.

An arbitrary element of I^N is a finite sum of monomials of the form

$$f_1^{a_1} \cdots f_m^{a_m},$$

where

$$a_1 + \cdots + a_m = N.$$

By the pigeonhole principle, there exists an index i such that

$$a_i \geq n_i.$$

Hence,

$$f_1^{a_1} \cdots f_m^{a_m} = f_i^{n_i} \cdot \left(f_1^{a_1} \cdots f_i^{a_i - n_i} \cdots f_m^{a_m} \right).$$

Since $f_i^{n_i} \in J$ and J is an ideal, the above product lies in J.

Therefore every generator of I^N lies in J, and hence

$$I^N \subset J.$$

□

Exercise 2.10.41. (a) Let $I \subset J$ be ideals in a ring R. Show that there is a natural ring homomorphism from R/I onto R/J.

(b) Let I be an ideal in a ring R, and let R be a subring of a ring S. Show that there is a natural ring homomorphism from R/I to S/IS.

Solution. (a) Let $I \subset J$ be ideals in a ring R.

Show that there is a natural ring homomorphism from R/I onto R/J.

Define a map

$$\varphi : R/I \to R/J$$

by

$$\varphi(r + I) = r + J.$$

We first show that φ is well-defined. Suppose

$$r + I = s + I.$$

Then $r - s \in I \subset J$, so $r + J = s + J$. Hence φ is well-defined.

Next, for $r, s \in R$,

$$\varphi((r+I)+(s+I)) = \varphi(r+s+I) = r+s+J,$$

and

$$\varphi(r+I)+\varphi(s+I) = (r+J)+(s+J) = r+s+J.$$

Thus φ preserves addition. Similarly,

$$\varphi((r+I)(s+I)) = \varphi(rs+I) = rs+J = (r+J)(s+J),$$

so φ preserves multiplication.

Hence φ is a ring homomorphism.

Finally, for any $r+J \in R/J$, we have

$$\varphi(r+I) = r+J,$$

so φ is surjective.

(b) Let I be an ideal of R, and let $R \subset S$ be a subring.

Show that there is a natural ring homomorphism from R/I to S/IS.

Define a map

$$\psi : R/I \to S/IS$$

by

$$\psi(r+I) = r+IS.$$

NOTE:

In general, I is not an ideal of S, so the quotient S/I is not defined.

The *extension* of I to S is the ideal

$$IS = \left\{ \sum a_i b_i \mid a_i \in I,\ b_i \in S \right\},$$

which is the smallest ideal of S containing I.

We show that ψ is well-defined. Suppose

$$r+I = s+I.$$

Then $r-s \in I$, hence $r-s \in IS$. Therefore,

$$r+IS = s+IS,$$

so ψ is well-defined.

For $r, s \in R$, we have

$$\psi((r+I)+(s+I)) = \psi(r+s+I) = r+s+IS,$$

and

$$\psi(r+I)+\psi(s+I) = (r+IS)+(s+IS) = r+s+IS.$$

Similarly,

$$\psi((r+I)(s+I)) = \psi(rs+I) = rs+IS = (r+IS)(s+IS).$$

Thus ψ is a ring homomorphism.

Hence there is a natural ring homomorphism from R/I to S/IS.

□

Exercise 2.10.42. Let $P = (0,\dots,0) \in \mathbb{A}^n$, $\mathscr{O} = \mathscr{O}_P(\mathbb{A}^n)$, $\mathfrak{m} = \mathfrak{m}_P(\mathbb{A}^n)$. Let $I \subset k[X_1,\dots,X_n]$ be the ideal generated by $X_1,\dots,X_n$. Show that $I\mathscr{O} = \mathfrak{m}$, so $I^r\mathscr{O} = \mathfrak{m}^r$ for all r.

Solution. By definition,

$$\mathcal{O} = \left\{ \frac{f}{g} \;\middle|\; f,g \in k[X_1,\dots,X_n],\ g(P) \neq 0 \right\},$$

and

$$\mathfrak{m} = \left\{ \frac{f}{g} \in \mathcal{O} \mid f(P) = 0 \right\}.$$

Since $X_i(P) = 0$ for all i, every element of $I\mathcal{O}$ vanishes at P. Hence,

$$I\mathcal{O} \subset \mathfrak{m}.$$

Conversely, let $f/g \in \mathfrak{m}$. Then $f(P) = 0$, so f has no constant term. Therefore,

$$f \in (X_1,\dots,X_n),$$

and there exist polynomials $h_1,\dots,h_n$ such that

$$f = \sum_{i=1}^{n} X_i h_i.$$

Hence,

$$\frac{f}{g} = \sum_{i=1}^{n} X_i \frac{h_i}{g} \in I\mathcal{O}.$$

Thus,

$$\mathfrak{m} \subset I\mathcal{O}.$$

We conclude that $I\mathcal{O} = \mathfrak{m}$.

Finally, since $(AB)\mathcal{O} = (A\mathcal{O})(B\mathcal{O})$ for ideals $A, B \subset R$, it follows by induction that

$$I^r\mathcal{O} = (I\mathcal{O})^r = \mathfrak{m}^r.$$

for all $r \geq 1$.

□

Exercise 2.10.43. Let V be a variety in $\mathbb{A}^n$, $I = I(V) \subset k[X_1, \ldots, X_n]$, $P \in V$, and let J be an ideal of $k[X_1, \ldots, X_n]$ that contains I. Let J' be the image of J in $\Gamma(V)$. Show that there is a natural homomorphism φ from $\mathscr{O}_P(\mathbb{A}^n)/J\mathscr{O}_P(\mathbb{A}^n)$ to $\mathscr{O}_P(V)/J'\mathscr{O}_P(V)$, and that φ is an isomorphism. In particular, $\mathscr{O}_P(\mathbb{A}^n)/I\mathscr{O}_P(\mathbb{A}^n)$ is isomorphic to $\mathscr{O}_P(V)$.

Solution. Recall that

$$\mathcal{O}_P(\mathbb{A}^n) = \left\{ \frac{f}{g} \;\middle|\; f, g \in k[X_1, \ldots, X_n],\ g(P) \neq 0 \right\},$$

and

$$\mathcal{O}_P(V) = \left\{ \frac{\overline{f}}{\overline{g}} \;\middle|\; f, g \in k[X_1, \ldots, X_n],\ g(P) \neq 0 \right\},$$

where $\overline{f}$ denotes the image of f in $\Gamma[V] = k[X_1, \ldots, X_n]/I$.

Define a map

$$\Phi : \mathcal{O}_P(\mathbb{A}^n) \to \mathcal{O}_P(V)$$

by

$$\Phi\left(\frac{f}{g}\right) = \frac{\overline{f}}{\overline{g}}.$$

Step 1: Φ is well-defined.

Suppose

$$\frac{f}{g} = \frac{f'}{g'}$$

in $\mathcal{O}_P(\mathbb{A}^n)$. Then

$$fg' - f'g = 0.$$

Passing to $\Gamma[V]$, we obtain

$$\overline{f}\,\overline{g'} - \overline{f'}\,\overline{g} = 0.$$

It follows that

$$\frac{\overline{f}}{\overline{g}} = \frac{\overline{f'}}{\overline{g'}}$$

in $\mathcal{O}_P(V)$. Hence Φ is well-defined.

Step 2: Φ is a ring homomorphism.
For $f/g, f'/g' \in \mathcal{O}_P(\mathbb{A}^n)$, we have

$$\Phi\left(\frac{f}{g} + \frac{f'}{g'}\right) = \frac{\overline{fg' + f'g}}{\overline{gg'}} = \frac{\overline{f}}{\overline{g}} + \frac{\overline{f'}}{\overline{g'}},$$

and

$$\Phi\left(\frac{f}{g} \cdot \frac{f'}{g'}\right) = \frac{\overline{ff'}}{\overline{gg'}} = \frac{\overline{f}}{\overline{g}} \cdot \frac{\overline{f'}}{\overline{g'}}.$$

Thus Φ is a ring homomorphism.

Step 3: Image of $J\mathcal{O}_P(\mathbb{A}^n)$.
Let $j \in J$ and $h/g \in \mathcal{O}_P(\mathbb{A}^n)$. Then

$$\Phi\left(j \cdot \frac{h}{g}\right) = \overline{j} \cdot \frac{\overline{h}}{\overline{g}} \in J'\mathcal{O}_P(V).$$

Hence,

$$\Phi(J\mathcal{O}_P(\mathbb{A}^n)) = J'\mathcal{O}_P(V).$$

Step 4: Induced map on quotients.
By the universal property of quotients, Φ induces a homomorphism

$$\varphi : \mathcal{O}_P(\mathbb{A}^n)/J\mathcal{O}_P(\mathbb{A}^n) \to \mathcal{O}_P(V)/J'\mathcal{O}_P(V).$$

Step 5: φ is surjective.
Let $\overline{f}/\overline{g} \in \mathcal{O}_P(V)$. Then

$$\varphi\left(\frac{f}{g} + J\mathcal{O}_P(\mathbb{A}^n)\right) = \frac{\overline{f}}{\overline{g}} + J'\mathcal{O}_P(V),$$

so every element of the target is in the image. Hence φ is surjective.

Step 6: φ is injective.
Suppose

$$\varphi\left(\frac{f}{g} + J\mathcal{O}_P(\mathbb{A}^n)\right) = 0.$$

Then

$$\frac{\overline{f}}{\overline{g}} \in J'\mathcal{O}_P(V).$$

So there exist $\overline{j} \in J'$ and $\overline{h}/\overline{k} \in \mathcal{O}_P(V)$ such that

$$\frac{\overline{f}}{\overline{g}} = \overline{j} \cdot \frac{\overline{h}}{\overline{k}}.$$

This implies that $\overline{fk - gjh} \in I$ and so $\overline{fk} \in J$. Lifting to $k[X_1, \ldots, X_n]$, this implies

$$\frac{f}{g} \in J\mathcal{O}_P(\mathbb{A}^n).$$

Hence the kernel is zero, and φ is injective.

Therefore, φ is an isomorphism.

Finally, taking $J = I$, we obtain

$$\mathcal{O}_P(\mathbb{A}^n)/I\mathcal{O}_P(\mathbb{A}^n) \cong \mathcal{O}_P(V).$$

□

Exercise 2.10.44. Show that ideals $I, J \subset k[X_1, \ldots, X_n]$ (k algebraically closed) are comaximal if and only if $V(I) \cap V(J) = \varnothing$.

Solution. Suppose first that I and J are comaximal.
Then $I + J = R$, so there exist $f \in I$ and $g \in J$ such that $f + g = 1$.

If $P \in V(I) \cap V(J)$, then $f(P) = g(P) = 0$, hence

$$1 = (f + g)(P) = 0,$$

a contradiction.
Therefore $V(I) \cap V(J) = \emptyset$.

Conversely, suppose that $V(I) \cap V(J) = \emptyset$. Then

$$V(I + J) = V(I) \cap V(J) = \emptyset.$$

By the Weak Nullstellensatz, $\sqrt{I + J} = (1)$, so $1 \in I + J$.
Hence $I + J = R$, and I, J are comaximal.

□

Exercise 2.10.45. Let $I = (X, Y) \subset k[X, Y]$. Show that

$$\dim_k\big(k[X, Y]/I^n\big) = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Solution. Let $I = (X, Y) \subset k[X, Y]$. Then

$$I^n = (X, Y)^n = (X^a Y^b \mid a + b \geq n).$$

Hence in the quotient $k[X, Y]/I^n$, every monomial $X^a Y^b$ with $a + b \geq n$ is zero.

Therefore the nonzero monomials in $k[X, Y]/I^n$ are exactly those with $a + b < n$, namely

$$1, X, Y, X^2, XY, Y^2, \ldots$$

up to total degree $n - 1$.

For each $d < n$, there are $d + 1$ monomials with $a + b = d$. Thus

$$\dim_k(k[X, Y]/I^n) = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

□

Exercise 2.10.46. Suppose R is a ring containing k, and R is finite dimensional over k. Show that R is isomorphic to a direct product of local rings.

Solution. R is a $k-$Algebra, So we can see R as Vector Space over k. Since R is finite-dimensional over k, it has a finite basis $r_1, \ldots, r_n$ which generates R as a k-algebra. Hence by the universal property of polynomial rings, there exists a surjective homomorphism

$$\varphi : k[X_1, \ldots, X_n] \longrightarrow R$$

such that $\varphi(X_i) = r_i$ for some n. Let

$$I = \ker(\varphi).$$

Then

$$R \cong k[X_1, \ldots, X_n]/I.$$

Since R is finite dimensional over k, it follows that

$$\dim_k(k[X_1, \ldots, X_n]/I) < \infty.$$

By Corollary 4 in section 1.7, $V(I) \subset \mathbb{A}^n$ is finite. Let

$$V(I) = \{P_1, \ldots, P_N\}.$$

By Proposition 6 in the text, since $V(I)$ is finite, we obtain a natural isomorphism

$$k[X_1, \ldots, X_n]/I \cong \prod_{i=1}^{N} \mathcal{O}_{P_i}(\mathbb{A}^n)/I\mathcal{O}_{P_i}(\mathbb{A}^n).$$

Therefore,

$$R \cong \prod_{i=1}^{N} R_i, \quad \text{where } R_i = \mathcal{O}_{P_i}(\mathbb{A}^n)/I\mathcal{O}_{P_i}(\mathbb{A}^n).$$

For each point P_i, the ring $\mathcal{O}_{P_i}(\mathbb{A}^n)$ is the local ring at P_i. It has a unique maximal ideal consisting of functions vanishing at P_i.

Hence it is a local ring.

The quotient

$$R_i = \mathcal{O}_{P_i}(\mathbb{A}^n)/I\mathcal{O}_{P_i}(\mathbb{A}^n)$$

is also a local ring.

We have shown that

$$R \cong \prod_{i=1}^{N} R_i,$$

where each R_i is a local ring.

Thus R is isomorphic to a finite direct product of local rings.

□

Exercise 2.10.47. Verify that for any R-module homomorphism $\varphi : M \to M'$, $\ker(\varphi)$ and $\mathrm{Im}(\varphi)$ are submodules of M and M' respectively. Show that

$$0 \longrightarrow \ker(\varphi) \longrightarrow M \xrightarrow{\varphi} \mathrm{Im}(\varphi) \longrightarrow 0$$

is exact.

Solution. For any R-linear map φ it is clear that $\ker(\varphi)$ is a submodule of M and $\mathrm{Im}(\varphi)$ is a submodule of M'. The only thing remained to show is that the sequence

$$0 \longrightarrow \ker(\varphi) \xrightarrow{\iota} M \xrightarrow{\varphi} \mathrm{Im}(\varphi) \longrightarrow 0$$

is exact. The map ι is injective, so the sequence is exact at 0 and $\ker(\varphi)$. By definition of kernel, $\mathrm{Im}(\iota) = \ker(\varphi)$, hence the sequence is exact at M. The map $\varphi : M \to \mathrm{Im}(\varphi)$ is surjective by definition of $\mathrm{Im}(\varphi)$, and $\ker(\varphi : M \to \mathrm{Im}(\varphi)) = \ker(\varphi)$. Therefore the sequence is exact at every term. □

Exercise 2.10.48. (a) Let N be a submodule of M, $\pi : M \to M/N$ the natural homomorphism. Suppose $\varphi : M \to M'$ is a homomorphism of R-modules, and $\varphi(N) = 0$. Show that there is a unique homomorphism $\bar{\varphi} : M/N \to M'$ such that $\bar{\varphi} \circ \pi = \varphi$.

(b) If N and P are submodules of a module M, with $P \subset N$, then there are natural homomorphisms from M/P onto M/N and from N/P into M/P. Show that the resulting sequence

$$0 \longrightarrow N/P \longrightarrow M/P \longrightarrow M/N \longrightarrow 0$$

is exact (*Second Noether Isomorphism Theorem*).

(c) Let $U \subset W \subset V$ be vector spaces, with V/U finite-dimensional. Show that

$$\dim(V/U) = \dim(V/W) + \dim(W/U).$$

(d) If $J \subset I$ are ideals in a ring R, show that there is a natural exact sequence of R-modules

$$0 \longrightarrow I/J \longrightarrow R/J \longrightarrow R/I \longrightarrow 0.$$

(e) If $\mathcal{O}$ is a local ring with maximal ideal $\mathfrak{m}$, show that there is a natural exact sequence of $\mathcal{O}$-modules

$$0 \longrightarrow \mathfrak{m}^n/\mathfrak{m}^{n+1} \longrightarrow \mathscr{O}/\mathfrak{m}^{n+1} \longrightarrow \mathscr{O}/\mathfrak{m}^n \longrightarrow 0.$$

Solution. We address each part.

(a) Define $\bar{\varphi}(m + N) = \varphi(m)$. If $m + N = m' + N$, then $m - m' \in N$ and hence $\varphi(m - m') = 0$, so $\varphi(m) = \varphi(m')$. Thus the definition is well-defined. It is R-linear, satisfies $\bar{\varphi} \circ \pi = \varphi$, and uniqueness follows from surjectivity of π.

(b) The map $N/P \to M/P$ is injective. Exactness at M/P requires the kernel of $M/P \to M/N$ to be N/P:

$$m + P \mapsto m + N \text{ equals } 0 \iff m \in N.$$

Surjectivity of $M/P \to M/N$ is clear. Thus the sequence is exact.

(c) Applying dimensions to part (b) for vector spaces gives:

$$\dim(M/P) = \dim(N/P) + \dim(M/N).$$

Replace (M, N, P) by (V, W, U) to obtain the stated identity.

(d) The maps are the natural ones:

$$I/J \hookrightarrow R/J, \qquad R/J \to R/I.$$

Exactness at I/J and R/I is clear. Exactness at R/J follows because $r + J$ maps to 0 in R/I iff $r \in I$, i.e. $r + J \in I/J$.

(e) The map $\mathscr{O}/\mathfrak{m}^{n+1} \to \mathscr{O}/\mathfrak{m}^n$ is the natural projection. Its kernel is

$$\{a + \mathfrak{m}^{n+1} : a \in \mathfrak{m}^n\} = \mathfrak{m}^n/\mathfrak{m}^{n+1},$$

giving exactness at the middle term. Injectivity and surjectivity at the ends are automatic.

Thus all sequences are exact. □

Exercise 2.10.49. Let R be a DVR satisfying the conditions of Problem 2.30. Then $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ is an R-module, and hence also a k-module, since $k \subset R$.

(a) Show that $\dim_k(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = 1$ for all $n \geq 0$.

(b) Show that $\dim_k(R/\mathfrak{m}^n) = n$ for all $n > 0$.

(c) Let $z \in R$. Show that $\operatorname{ord}(z) = n$ if $(z) = \mathfrak{m}^n$, and hence that $\operatorname{ord}(z) = \dim_k(R/(z))$.

Solution. We use the uniformizer t of the DVR R.

(a) Define an R-module homomorphism $\phi : \mathfrak{m}^n \to R/\mathfrak{m}$ as follows. Every element $x \in \mathfrak{m}^n$ is $t^n u$ for some $u \in R$. First consider the isomorphism $\mathfrak{m}^n \to R$ defined by $x \mapsto x/t^n$. Define ϕ to be the composite of this isomorphism with the natural map $R \to R/\mathfrak{m}$. It is easy to check that this map is surjective and that the kernel is exactly $\mathfrak{m}^{n+1}$.

(b) Use the filtration

$$R \supset \mathfrak{m} \supset \mathfrak{m}^2 \supset \cdots \supset \mathfrak{m}^n.$$

Problem 2.49(e) gives short exact sequences

$$0 \to \mathfrak{m}^i/\mathfrak{m}^{i+1} \to R/\mathfrak{m}^{i+1} \to R/\mathfrak{m}^i \to 0.$$

Taking dimensions and using (a),

$$\dim_k(R/\mathfrak{m}^{i+1}) = \dim_k(R/\mathfrak{m}^i) + 1.$$

Induction yields $\dim_k(R/\mathfrak{m}^n) = n$.

(c) If $z = t^n u$ with u a unit, then $(z) = (t^n) = \mathfrak{m}^n$. Conversely, if $(z) = \mathfrak{m}^n$, the generator of $\mathfrak{m}^n$ has order n, forcing $\operatorname{ord}(z) = n$.

Since $(z) = \mathfrak{m}^n$, we have

$$R/(z) \cong R/\mathfrak{m}^n,$$

so $\dim_k(R/(z)) = n = \operatorname{ord}(z)$. □

Exercise 2.10.50. Let

$$0 \longrightarrow V_1 \longrightarrow \cdots \longrightarrow V_n \longrightarrow 0$$

be an exact sequence of finite-dimensional vector spaces. Show that

$$\sum (-1)^i \dim(V_i) = 0.$$

Solution. Consider the exact sequence

$$0 \longrightarrow V_1 \xrightarrow{d_1} V_2 \xrightarrow{d_2} \cdots \xrightarrow{d_{n-1}} V_n \longrightarrow 0$$

of finite-dimensional vector spaces.

Exactness gives, for each i,

$$\operatorname{Im}(d_{i-1}) = \ker(d_i).$$

Hence we have short exact sequences

$$0 \longrightarrow \ker(d_i) \longrightarrow V_i \longrightarrow \operatorname{Im}(d_i) \longrightarrow 0,$$

which imply

$$\dim V_i = \dim \ker(d_i) + \dim \operatorname{Im}(d_i).$$

Substituting $\ker(d_i) = \operatorname{Im}(d_{i-1})$, we obtain

$$\dim V_i = \dim \operatorname{Im}(d_{i-1}) + \dim \operatorname{Im}(d_i).$$

Taking the alternating sum yields

$$\sum_{i=1}^{n} (-1)^i \dim V_i = \sum_{i=1}^{n} (-1)^i \big(\dim \operatorname{Im}(d_{i-1}) + \dim \operatorname{Im}(d_i)\big).$$

The two sums cancel term-by-term, since each $\dim \operatorname{Im}(d_i)$ appears once with sign $(-1)^i$ and once with sign $(-1)^{i+1}$. Therefore,

$$\sum_{i=1}^{n} (-1)^i \dim V_i = 0.$$

□

Exercise 2.10.51. Let N, P be submodules of a module M. Show that the subgroup

$$N + P = \{\, n + p \mid n \in N,\, p \in P \,\}$$

is a submodule of M. Show that there is a natural R-module isomorphism

$$N/(N \cap P) \cong (N + P)/P$$

(*First Noether Isomorphism Theorem*).

Solution. Let N and P be submodules of an R-module M.

Step 1: $N + P$ is a submodule of M.
We verify the submodule axioms.

(i) *Nonempty.* Since $0 \in N$ and $0 \in P$, we have $0 = 0 + 0 \in N + P$.

(ii) *Closed under addition.* If $n_1 + p_1, n_2 + p_2 \in N + P$, then

$$(n_1 + p_1) + (n_2 + p_2) = (n_1 + n_2) + (p_1 + p_2) \in N + P,$$

because N and P are submodules.

(iii) *Closed under scalar multiplication.* For $r \in R$ and $n + p \in N + P$,

$$r(n + p) = rn + rp \in N + P,$$

since $rn \in N$ and $rp \in P$.

Hence $N + P$ is a submodule of M.

Step 2: Construction of the isomorphism.
Define a map

$$\varphi : N \longrightarrow (N + P)/P \quad \text{by} \quad \varphi(n) = n + P.$$

This map is R-linear.

Step 3: Kernel and image.
The kernel of φ is

$$\ker(\varphi) = \{\, n \in N \mid n \in P \,\} = N \cap P.$$

The image of φ is all of $(N + P)/P$, since every element of $N + P$ has the form $n + p$ with $n \in N$, $p \in P$, and

$$(n + p) + P = n + P.$$

Thus φ is surjective.

Step 4: Conclusion.
By the First Noether Isomorphism Theorem,

$$N/(N \cap P) \cong (N + P)/P.$$

□

Exercise 2.10.52. Let V be a vector space, W a subspace, and $T : V \to V$ a one-to-one linear map such that $T(W) \subset W$, and assume V/W and $W/T(W)$ are finite-dimensional.

(a) Show that T induces an isomorphism of V/W with $T(V)/T(W)$.

(b) Construct an isomorphism between $T(V)/(W \cap T(V))$ and $(W + T(V))/W$, and an isomorphism between $W/(W \cap T(V))$ and $(W + T(V))/T(V)$.

(c) Use Problem 2.49(c) to show that

$$\dim(V/(W + T(V))) = \dim((W \cap T(V))/T(W)).$$

(d) Conclude finally that

$$\dim(V/T(V)) = \dim(W/T(W)).$$

Solution. (a) Define

$$\bar{T} : V/W \to T(V)/T(W), \qquad \bar{T}(v + W) = T(v) + T(W).$$

This is well-defined because $T(W) \subset W$. Injectivity follows from injectivity of T. Surjectivity is clear since every element of $T(V)$ is $T(v)$ for some v. Thus it is an isomorphism.

(b) Define

$$T(V) \ni T(v) \mapsto v + W \in (W + T(V))/W.$$

Kernel consists of those $T(v) \in T(V)$ lying in W, i.e. $T(v) \in W \cap T(V)$. This gives the first isomorphism:

$$T(V)/(W \cap T(V)) \cong (W + T(V))/W.$$

Similarly restrict the projection

$$W \to (W + T(V))/T(V), \qquad w \mapsto w + T(V),$$

whose kernel is $W \cap T(V)$, giving

$$W/(W \cap T(V)) \cong (W + T(V))/T(V).$$

(c) Apply Problem 2.49(c) to the pair of subspaces

$$W \subset W + T(V) \subset V.$$

We obtain

$$\dim(V/W) = \dim(V/(W + T(V))) + \dim((W + T(V))/W).$$

Replace $((W + T(V))/W)$ by $T(V)/(W \cap T(V))$ from part (b), and note from part (a) that

$$\dim(V/W) = \dim(T(V)/T(W)).$$

Rearranging gives

$$\dim V/(W + T(V)) = \dim(W \cap T(V))/T(W).$$

(d) Apply Problem 2.49(c) again to the inclusion

$$T(V) \subset V.$$

We have

$$\dim(V/T(V)) = \dim(V/(W + T(V))) + \dim((W + T(V))/T(V)).$$

Using part (b),

$$(W + T(V))/T(V) \cong W/(W \cap T(V)).$$

Using part (c),

$$\dim(V/(W + T(V))) = \dim((W \cap T(V))/T(W)).$$

Add the two contributions:

$$\dim(V/T(V)) = \dim(W/(W \cap T(V))) + \dim((W \cap T(V))/T(W)) = \dim(W/T(W)).$$

□

Exercise 2.10.53. What does M being free on $m_1, \ldots, m_n$ say in terms of the elements of M?

Solution. Let M be an R-module and let $m_1, \ldots, m_n \in M$.

We say that M is free on $m_1, \ldots, m_n$ if the natural homomorphism

$$\phi : M_X \longrightarrow M, \quad \phi\left(\sum_{i=1}^{n} a_i x_i\right) = \sum_{i=1}^{n} a_i m_i,$$

is an isomorphism, where $X = \{m_1, \ldots, m_n\}$.

This condition is equivalent to the following two properties:

(1) Generating Property. Every element $m \in M$ can be written in the form

$$m = a_1 m_1 + \cdots + a_n m_n \quad \text{for some } a_1, \ldots, a_n \in R.$$

Thus, $\{m_1, \ldots, m_n\}$ generates M.

(2) Linear Independence. If

$$a_1 m_1 + \cdots + a_n m_n = 0,$$

then

$$a_1 = a_2 = \cdots = a_n = 0.$$

Hence, the representation of elements of M is unique.

Combining (1) and (2), every element of M can be written uniquely as a linear combination of $m_1, \ldots, m_n$. Therefore, $m_1, \ldots, m_n$ form a basis of M.

Consequently,

$$M \cong R^n,$$

and M is a free R-module of rank n.

□

Exercise 2.10.54. Let $F = X^n + a_1 X^{n-1} + \cdots + a_n$ be a monic polynomial in $R[X]$. Show that $R[X]/(F)$ is a free R-module with basis $1, \overline{X}, \ldots, \overline{X}^{n-1}$, where $\overline{X}$ is the residue of X.

Solution. Let

$$F = X^n + a_1 X^{n-1} + \cdots + a_n \in R[X]$$

be a monic polynomial.

Step 1. Division Algorithm. Since F is monic of degree n, for every $G(X) \in R[X]$ there exist polynomials $Q(X), R(X) \in R[X]$ such that

$$G(X) = Q(X)F(X) + R(X),$$

where $\deg R < n$.

Thus,

$$R(X) = b_0 + b_1 X + \cdots + b_{n-1} X^{n-1}.$$

Step 2. Generation. In the quotient $R[X]/(F)$ we have

$$\overline{G} = \overline{R} = b_0 \bar{1} + b_1 \bar{X} + \cdots + b_{n-1} \overline{X^{n-1}}.$$

Hence, every element of $R[X]/(F)$ is an R-linear combination of

$$\bar{1}, \bar{X}, \ldots, \overline{X^{n-1}}.$$

Therefore, these elements generate $R[X]/(F)$.

Step 3. Linear Independence. Suppose that

$$b_0 \bar{1} + b_1 \bar{X} + \cdots + b_{n-1} \overline{X^{n-1}} = 0.$$

Then

$$\overline{b_0 + b_1 X + \cdots + b_{n-1} X^{n-1}} = 0,$$

which implies

$$b_0 + b_1 X + \cdots + b_{n-1} X^{n-1} \in (F).$$

Thus,

$$b_0 + b_1 X + \cdots + b_{n-1} X^{n-1} = H(X) F(X)$$

for some $H(X) \in R[X]$.

Since the left-hand side has degree $< n$ and F has degree n, we must have $H(X) = 0$. Hence,

$$b_0 = b_1 = \cdots = b_{n-1} = 0.$$

Therefore, the elements are linearly independent.

Step 4. Conclusion. The elements $\bar{1}, \bar{X}, \ldots, \overline{X^{n-1}}$ generate $R[X]/(F)$ and are linearly independent. Hence, they form a basis.

Thus,

$$R[X]/(F) \cong R^n,$$

and $R[X]/(F)$ is a free R-module of rank n.

□

Exercise 2.10.55. Show that a subset X of a module M generates M if and only if the homomorphism $M_X \to M$ is onto. Every module is isomorphic to a quotient of a free module.

Solution. Let X be a subset of an R-module M, and let M_X be the free R-module on X. Define the homomorphism

$$\phi : M_X \longrightarrow M, \quad \phi\left(\sum a_i x_i\right) = \sum a_i x_i.$$

Assume that X generates M. Then for every $m \in M$, there exist $a_i \in R$ and $x_i \in X$ such that

$$m = \sum a_i x_i.$$

Hence,

$$m = \phi\left(\sum a_i x_i\right),$$

so ϕ is surjective.

Conversely, assume that ϕ is surjective. Then for every $m \in M$, there exists $u = \sum a_i x_i \in M_X$ such that

$$\phi(u) = m.$$

Thus,

$$m = \sum a_i x_i,$$

and X generates M.

Therefore,

$$X \text{ generates } M \iff \phi \text{ is surjective.}$$

Let M be any R-module and take $X = M$. Then X generates M, and the map $\phi : M_M \to M$ is surjective. By the First Isomorphism Theorem, $M_M/\ker(\phi) \cong M$. Since M_M is free, it follows that every module is isomorphic to a quotient of a free module.

□

Chapter 3

Local Properties of Plane Curves

3.1 Multiplicities and Tangent Lines

In the previous chapter, we considered the zero locus of a polynomial $F \in k[x, y]$. If we write $F = F_1^{e_1} \dots F_r^{e_r}$, then we saw that $V(F) = V(F_1 \dots F_r)$. Thus, from the zero locus we may determine the irreducible components of $V(F)$, but not the "multiplicities" e_i. In this chapter we want to keep track of the multiplicities as well and so by a **plane curve** we will mean a polynomial $F \in k[x, y]$.

The **degree** of a plane curve is simply the degree of F. If $F = F_1^{e_1} \dots F_r^{e_r}$, then the F_i are components of F. The multiplicity of the component F_i is e_i. The component F_i is said to be **simple** if $e_i = 1$, otherwise it is called a **multiple component**. Note that the components of F can be recovered from $V(F)$, but not their multiplicities.

If F is irreducible then $V(F)$ is a variety in $\mathbb{A}^2(k)$. We will write $\Gamma(F)$, $k(F)$ and $\mathcal{O}_P(F)$ instead of $\Gamma(V(F))$, $k(V(F))$ and $\mathcal{O}_P(V(F))$.

Definition 3.1.1 (Simple Point and Tangent Line)**.** *Let F be a plane curve, $P = (a, b) \in F$. The point P is called a **simple point** of F if either $F_x(P) \neq 0$ or $F_y(P) \neq 0$. If P is simple, the line*

$$F_x(P)(X - a) + F_y(P)(Y - b) = 0$$

*is called the **tangent line** to F at P.*

A point of F which is not simple is called a **multiple point**, or a **singular point**. If every point is simple then the curve is called **non-singular** or **smooth**.

Definition 3.1.2 (Multiplicity of a Point)**.** *Let F be any curve, $P = (0, 0)$. Write $F = F_m + F_{m+1} + \dots + F_d$, where $F_m \neq 0$, $F_d \neq 0$ and F_i is a form of degree i. We define m to be the **multiplicity** of F at P and denote this by $m_P(F)$.*

It is easily checked that $P \in V(F) \iff m_P(F) \geqslant 1$. If $P \in V(F)$ then it is easily checked that P is a simple point $\iff m_P(F) = 1$.

Assume $m_P(F) > 0$, that is, $P \in V(F)$. Since F_m is a form in two variables, we may factor it as $F_m = \prod L_i^{r_i}$, where L_i's are linear forms. The L_i are called **tangent lines** to F at P and r_i is the multiplicity of the tangent. The line L_i is a **simple tangent** if $r_i = 1$.

Let $F = \prod F_i^{e_i}$. Then it is clear that

$$m_P(F) = \sum e_i m_P(F_i).$$

In particular, P is a simple point of F if P belongs to exactly one component F_i, which is a simple component of F and such that P is a simple point of F_i.

To extend these definitions to a point $P = (a, b) \neq (0, 0)$, apply a linear change of coordinates $X' = X - a$ and $Y' = Y - b$.

3.2 Multiplicities and Local Rings

Let F be an irreducible plane curve and let $P \in V(F)$. Our aim is to find $m_P(F)$ in terms of the local ring $\mathcal{O}_P(F) = \{\frac{a}{b} \mid a, b \in \Gamma(F), b(P) \neq 0\}$.

Theorem 3.2.1. *Let P be a point on an irreducible curve F. Let $\mathcal{O} = \mathcal{O}_P(F)$ and $\mathfrak{m} \subset \mathcal{O}$ be the maximal ideal. Then for all sufficiently large n,*

$$m_P(F) = \dim_k(\mathfrak{m}^n/\mathfrak{m}^{n+1}).$$

Proof. Consider the short exact sequence of vector spaces

$$0 \to \mathfrak{m}^n/\mathfrak{m}^{n+1} \to \mathcal{O}/\mathfrak{m}^{n+1} \to \mathcal{O}/\mathfrak{m}^n \to 0.$$

It suffices to show that $\dim_k(\mathcal{O}/\mathfrak{m}^n) = nm_P(F) + s$ for some constant s and all $n \gg 0$. We will first write the ring $\mathcal{O}/\mathfrak{m}^n$ in terms of the polynomial ring $k[X, Y]$. As before, after a translation, we may assume that $P = (0, 0)$ and so the maximal ideal is $I_P = (X, Y)$. It follows that for any integer $n \geqslant 0$ we have $V(I_P^n) = \{P\}$.

Thus, we also have $V(I_P^n, F) = \{P\}$. Recall that we saw that if $V(I) = \{P\}$, then $k[X_1, \ldots, X_n]/I \cong \mathcal{O}_P(\mathbb{A}^n)/I\mathcal{O}_P(\mathbb{A}^n)$, see Corollary 2.8.3. Thus, we get

$$k[X, Y]/(I_P^n, F) \cong \mathcal{O}_P(\mathbb{A}^n)/(I_P^n, F)\mathcal{O}_P(\mathbb{A}^n) \cong \mathcal{O}/\mathfrak{m}^n.$$

Thus, we need to compute the dimension of $k[X, Y]/(I_P^n, F)$.

Consider the multiplication by F map:

$$k[X,Y] \to k[X,Y], \quad G \mapsto GF.$$

Let $F = F_m + \ldots + F_d$, with $F_m \neq 0$. It is clear that $FI_P^k \subset I_P^{k+m}$. Conversely, if $GF \in I_P^{k+m}$, then writing $G = G_l + \ldots + G_t$, we see that $l \geqslant k$, that is, $G \in I_P^k$. This shows that we have an inclusion

$$k[X,Y]/I_P^k \hookrightarrow k[X,Y]/I_P^{k+m}, \quad \bar{G} \mapsto \overline{GF}.$$

Thus, for every $k \geqslant 0$, we have a short exact sequence

$$0 \to k[X,Y]/I_P^k \to k[X,Y]/I_P^{k+m} \to k[X,Y]/(I_P^{k+m}, F) \to 0.$$

Exactness of the above sequence in the middle is obvious as if $A \in k[X,Y]$ maps to 0 on the right, then it follows that $A \in FG + I_P^{k+m}$, but this obviously implies that in $k[X,Y]/I_P^{k+m}$, A is the image of an element from the left. This shows that

$$\begin{aligned}\dim\left(\frac{k[X,Y]}{(I_P^{k+m}, F)}\right) &= \dim\left(\frac{k[X,Y]}{I_P^{k+m}}\right) - \dim\left(\frac{k[X,Y]}{I_P^k}\right)\\ &= \frac{(k+m)(k+m+1)}{2} - \frac{k(k+1)}{2}\\ &= (k+m)m - \frac{m(m-1)}{2}.\end{aligned}$$

Thus, for all $n \gg 0$ (setting $n = k+m$) we have

$$\dim\left(\frac{k[X,Y]}{(I_P^n, F)}\right) = nm - \frac{m(m-1)}{2}.$$

This completes the proof of the Theorem. □

Theorem 3.2.2. *P is a simple point of F iff $\mathcal{O}_P(F)$ is a DVR. In this case, if $L = aX + bY + c$ is any line through P that is not tangent to F, then the image of L in $\mathcal{O}_P(F)$ is a uniformizing parameter for $\mathcal{O}_P(F)$.*

Proof. After doing a translation, we may assume that $P = (0,0)$. Let us assume that P is a simple point. Then $F = L_1 +$ higher degree terms. Since L is not tangent to F at P, it follows that L is not a scalar multiple of L_1. Thus, L and L_1 are linearly independent.

After doing a linear change of coordinates, we may assume that $F = Y +$ higher degree terms and $L = X$. Since $\mathcal{O}_P(F)$ is a domain and Noetherian, it follows that to show it

is a DVR, it suffices to show that the maximal ideal is generated by $\bar{X}$, the image of L in $\mathcal{O}_P(F)$. Note that the maximal ideal of P in $\mathcal{O}_P(F)$ is generated by $(\bar{X}, \bar{Y})$. Thus, it suffices to show that $\bar{Y}$ is in the ideal generated by $\bar{X}$.

Write $F = YG + X^2H$, where $G = 1+$ higher degree terms. Going modulo (F) we get $\bar{Y}\bar{G} = -\bar{X}^2\bar{H}$. But note that $\bar{G}$ is a unit in $\mathcal{O}_P(F)$ and so we get $\bar{Y} \in (\bar{X})$ in $\mathcal{O}_P(F)$. This shows that if P is simple then the maximal ideal is generated by one element and so $\mathcal{O}_P(F)$ is a DVR.

Conversely, if $\mathcal{O}_P(F)$ is a DVR, then the maximal ideal $\overline{I_P^n} = (t^n)$ for some uniformizing parameter t. This shows that $\dim_k(\overline{I_P^n}/\overline{I_P^{n+1}}) = 1$ for all n, and so using Theorem 3.2.1 we get that $m_P(F) = 1$. This shows that P is a simple point. □

3.3 Intersection Numbers

Let F and G be plane curves and let $P \in \mathbb{A}^2$ be a point. We want to define the intersection number of F and G at P, and we will denote it by $I(P, F \cap G)$.

We say that F and G **intersect properly** at P if F and G have no common component which passes through P. We would want the intersection number $I(P, F \cap G)$ to satisfy the following conditions:

1. $I(P, F \cap G) \in \mathbb{Z}_{\geqslant 0}$ if F and G intersect properly at P. $I(P, F \cap G) = \infty$ if F and G do not intersect properly at P.

2. $I(P, F \cap G) = 0 \iff P \notin F \cap G$. $I(P, F \cap G)$ depends only on the components of F and G which contain P. That is, if we write $F = F_1F_2$ where $F_1(P) = 0$ and $F_2(P) \neq 0$, and write $G = G_1G_2$ where $G_1(P) = 0$ and $G_2(P) \neq 0$, then $I(P, F \cap G) = I(P, F_1 \cap G_1)$. $I(P, F \cap G) = 0$ if F or G is a nonzero constant.

3. $I(P, F \cap G)$ is invariant under affine change of coordinates.

4. $I(P, F \cap G) = I(P, G \cap F)$.

   Two curves F and G are said to **intersect transversally** at P if P is a simple point of F and G and the tangent lines at P to F and G are different.

5. $I(P, F \cap G) \geqslant m_P(F)m_P(G)$. Equality holds iff F and G have no common tangent lines at P. For example, if F and G meet transversally at P then we want $I(P, F \cap G) = 1$.

6. If $F = \prod F_i^{r_i}$ and $G = \prod G_j^{s_j}$ then $I(P, F \cap G) = \sum_{i,j} r_i s_j I(P, F_i \cap G_j)$.

7. $I(P, F \cap G) = I(P, F \cap (G + AF))$ for any $A \in k[X, Y]$.

Theorem 3.3.1. *There is a unique intersection number $I(P, F \cap G)$, defined for all plane curves F, G and all points $P \in \mathbb{A}^2$ satisfying properties (1)–(7). It is given by the formula*

$$I(P, F \cap G) = \dim_k \left(\mathcal{O}_P(\mathbb{A}^2)/(F, G)\right).$$

Proof. **Proof of Uniqueness**. Assume that we have a number $I(P, F \cap G)$ defined for all F, G and $P \in \mathbb{A}^2$ satisfying (1)–(7). Suppose $J(P, F \cap G)$ is another such number, then we need to show that $I(P, F \cap G) = J(P, F \cap G)$.

(a) If F or G is a nonzero constant, then by (2) both are 0 and so equal. So we may assume that neither F nor G is a nonzero constant.

(b) If F and G have a common component and P lies on this component, then by (1), both are ∞ and so they are equal. Thus, we may assume that F and G intersect properly at P.

(c) By (1) both are finite. We will prove by induction on the value of $I(P, F \cap G)$ that $I(P, F \cap G) = J(P, F \cap G)$.

(d) The base case for the induction is when $I(P, F \cap G) = 0$. By (2) this happens iff $P \notin F \cap G$, in which case $J(P, F \cap G)$ is also 0. Thus, equality holds.

(e) Now assume that $I(P, F \cap G) = n > 0$. Consider the polynomials $F(X, 0)$ and $G(X, 0)$ in $k[X]$. Let $r = \deg(F(X, 0))$ and $s = \deg(G(X, 0))$. If $F(X, 0) = 0$ then we take $r = 0$. Similarly, if $G(X, 0) = 0$, we take $s = 0$. By (4) we may assume that $r \leqslant s$.

Case 1: $r = 0$**.** This means that $F = YH$. By (6) we get

$$I(P, F \cap G) = I(P, Y \cap G) + I(P, H \cap G).$$

If $I(P, Y \cap G)$ and $I(P, H \cap G)$ are both positive, then $I(P, Y \cap G) = J(P, Y \cap G)$ and $I(P, H \cap G) = J(P, H \cap G)$ by induction and so $I(P, F \cap G) = J(P, F \cap G)$.

Note that by (2), $I(P, Y \cap G) > 0$. So consider the case $I(P, H \cap G) = 0$. Note that this happens iff $P \notin H \cap G$) and so we also have $J(P, H \cap G) = 0$. Then

$$I(P, F \cap G) = I(P, Y \cap G) = (\text{using (7)})\ I(P, Y \cap G(X, 0))$$

as $G = G(X, 0) + AY$. Writing $G(X, 0) = X^m(a_0 + a_1X + \ldots)$ with $a_0 \neq 0$, and using (6) and (2) we get $I(P, F \cap G) = I(P, Y \cap X^m)$, using (6) and (5) we get $I(P, F \cap G) = m$ and all this also holds for $J(P, F \cap G)$. Thus, $I(P, F \cap G) = J(P, F \cap G)$.

Case 2: $r > 0$**.** We may multiply $F(X,0)$ and $G(X,0)$ by constants and assume they are monic. Let $H = G - X^{s-r}F$. Then $\deg(H(X,0)) = t < s$, and by (7) we have $I(P, F \cap G) = I(P, F \cap H)$. Repeating this process finitely many times, and interchanging the roles of F, H if $t < r$, then we get $I(P, F \cap G) = I(P, A \cap B)$ where A and B are polynomials as in Case 1. Similarly, $J(P, F \cap G) = J(P, A \cap B)$ and by Case 1 we have $I(P, F \cap G) = I(P, A \cap B) = J(P, A \cap B) = J(P, F \cap G)$.

This completes the proof of uniqueness.

Proof of Existence. Define $I(P, F \cap G)$ to be $\dim_k(\mathcal{O}_P(\mathbb{A}^2)/(F,G))$. We must show that (1)–(7) hold. It is clear that (2), (4), and (7) hold. It is also clear that (3) holds, and so we may assume that $P = (0,0)$.

Let us show that (1) holds. First assume that F and G have a common component H which passes through P. Then $(F,G) \subset (H)$ and so $\mathcal{O}_P(\mathbb{A}^2)/(F,G) \twoheadrightarrow \mathcal{O}_P(\mathbb{A}^2)/(H)$ and so

$$\dim \mathcal{O}_P(\mathbb{A}^2)/(F,G) \geqslant \dim \mathcal{O}_P(\mathbb{A}^2)/(H)\,.$$

But $\mathcal{O}_P(\mathbb{A}^2)/(H)$ is isomorphic to $\mathcal{O}_P(H)$, which contains $\Gamma(H)$. By Corollary 1.10.6, as $V(H)$ is infinite, it follows that $\Gamma(H)$ is an infinite dim vector space and so this shows $\dim \mathcal{O}_P(\mathbb{A}^2)/(H)$ is ∞. Thus, $I(P, F \cap G) = \infty$.

Next let us assume that F and G intersect properly at P. Since F and G have no common component, we see that $V(F,G)$ is a finite set. Let $I = (F,G)k[X,Y]$. This implies that $k[X,Y]/I$ is finite by Proposition 1.6.1. Then Proposition 2.8.1 says that there is an isomorphism

$$k[X,Y]/I \xrightarrow{\sim} \prod \mathcal{O}_{P_i}(\mathbb{A}^2)/I\mathcal{O}_{P_i}(\mathbb{A}^2).$$

Thus, there is a surjection $k[X,Y]/I \to \mathcal{O}_P(\mathbb{A}^2)/I\mathcal{O}_P(\mathbb{A}^2)$ and so $\mathcal{O}_P(\mathbb{A}^2)/(F,G)$ is finite dimensional. This proves (1).

To prove (6), it suffices to show that $I(P, F \cap GH) = I(P, F \cap G) + I(P, F \cap H)$. If F and GH have a common component, then both sides are ∞. Thus, we may assume F and G have no common component. Since $(F, GH) \subset (F, G)$ we have the natural map $\mathcal{O}/(F, GH) \twoheadrightarrow \mathcal{O}/(F, G)$.

Consider the map $\mathcal{O} \to \mathcal{O}/(F, GH)$ given by $A \mapsto \overline{AG}$. It is clear that the kernel contains F and H. We claim the kernel is exactly (F, H). Suppose $AG = BF + CGH$, which implies, $G(A - CH) = BF$. Since G and F have no common factors, it follows that G divides B, say $B = B'G$. Then we get $A = B'F + CH$, thus $A \in (F, H)$. This shows that $\mathcal{O}/(F, H) \to \mathcal{O}/(F, GH)$ is an inclusion.

Clearly, we have a complex:

$$0 \to \mathcal{O}/(F,H) \xrightarrow{\cdot G} \mathcal{O}/(F,GH) \to \mathcal{O}/(F,G) \to 0$$

We claim this is exact. It only remains to show exactness in the middle. Suppose $\bar{A} \mapsto 0$, then $A = BF + CG$. This means that $A - BF \in \mathrm{Im}(\mathcal{O}/(F,H))$. Thus, exactness at the middle also holds. This proves that (6) holds.
Caution: In the above argument, we have used the fact that $\mathcal{O}_P(\mathbb{A}^2)$ is a UFD. **Check this!** Alternatively, we could have worked with the rings $k[X,Y]/(F,H)$, $k[X,Y]/(F,GH)$ and $k[X,Y]/(F,G)$, used Proposition 2.8.1 and projected to the local ring of P.

Finally, we prove property (5). Let m = multiplicity of P at F and n = multiplicity of P at G. Let J = maximal ideal of $P = (0,0)$ in $\mathbb{A}^2$, that is, (X,Y). Consider the diagram:

$$\begin{array}{ccccccc} (k[X,Y]/J^n) \times (k[X,Y]/J^m) & \xrightarrow{\psi} & k[X,Y]/J^{m+n} & \xrightarrow{\varphi} & k[X,Y]/(J^{m+n},F,G) & \longrightarrow & 0 \\ & & & & \downarrow \alpha & & \\ & & & & \mathcal{O}/(F,G) \xrightarrow{\pi} \mathcal{O}/(J^{m+n},F,G) & \longrightarrow & 0 \end{array}$$

The map α is an isomorphism by Corollary 2.8.3. The maps φ and π are surjections. The map ψ is given by $\psi(\bar{A},\bar{B}) = \overline{AF+BG}$. We claim that the top row is exact. First note that we may represent an element in $k[X,Y]/J^{m+n}$ by $f = f_0 + f_1 + \ldots + f_{m+n-1}$, where f_i are forms of deg i. Suppose $\varphi(f) = 0$, that is, $f = aF + bG \pmod{J^{m+n}}$. It is clear that the map ψ sends $(\bar{a},\bar{b})$ to f.

Thus, it follows that

$$\dim(k[X,Y]/J^n) + \dim(k[X,Y]/J^m) \geqslant \dim(\mathrm{Ker}(\phi)),$$

and equality holds iff ψ is 1-1. Also note that

$$\dim(k[X,Y]/(J^{m+n},F,G)) = \dim(k[X,Y]/J^{m+n}) - \dim(\mathrm{Ker}(\phi)).$$

Thus,

$$\begin{aligned} I(P,F\cap G) &= \dim(\mathcal{O}/(F,G)) \\ &\geqslant \dim(\mathcal{O}/(J^{m+n},F,G)) \\ &= \dim(k[X,Y]/(J^{m+n},F,G)) \\ &= \dim(k[X,Y]/J^{m+n}) - \dim(\mathrm{Ker}(\phi)) \\ &\geqslant \dim(k[X,Y]/J^{m+n}) - \dim(k[X,Y]/J^n) - \dim(k[X,Y]/J^m) \\ &= mn. \end{aligned}$$

Thus, $I(P,F\cap G) \geqslant mn$. Equality holds iff

1. $\dim(\mathcal{O}/(F,G)) = \dim(\mathcal{O}/(J^{m+n}, F, G))$, that is, $J^{m+n} \subset (F,G)\mathcal{O}$, and
2. ψ is 1-1.

We have already proved the first part of (5), namely, that $I(P, F \cap G) \geqslant mn$. We need to show that equality holds iff F and G have distinct tangent lines at P. Suppose equality holds, then ψ is injective and using Lemma 3.3.3(b), F and G have no common tangents at P. Conversely, suppose F and G have no common tangents at P, then again using Lemma 3.3.3, ψ is injective and $J^{m+n} \subset (F,G)\mathcal{O}$, which shows that equality holds.

This completes the proof of the existence. □

Lemma 3.3.2. *Let $L_1, L_2, \ldots$ and $M_1, M_2, \ldots$ be sequences of nonzero linear forms in $k[X,Y]$, and assume no $L_i = \lambda M_j, \lambda \in k$. Let $A_{ij} = L_1 \ldots L_i M_1 \ldots M_j$. Then $\{A_{ij} \mid i + j = d\}$ forms a basis for the space of forms of degree d.*

Proof. Let $L_1, L_2, \ldots$ and $M_1, M_2, \ldots$ be sequences of nonzero linear forms in $k[X,Y]$ such that $L_i \neq \lambda M_j$ for all $\lambda \in k$. Define

$$A_{ij} = L_1 \cdots L_i \, M_1 \cdots M_j, \qquad i, j \geqslant 0,$$

with $A_{00} = 1$. If $i + j = d$, then A_{ij} is a homogeneous polynomial of degree d, so $A_{ij} \in V(d,2)$.
There are $d+1$ such polynomials. Suppose that

$$\sum_{i+j=d} c_{ij} A_{ij} = 0.$$

Note that except for A_{0d}, L_1 divides every A_{ij}. Thus, we get a contradiction if $c_{0d} \neq 0$. So $c_{0d} = 0$ and we may divide the entire equation by L_1. Next note that except for $A_{1,d-1}/L_1$, L_2 divides every A_{ij} in this new equation. This shows that $c_{1,d-1} = 0$. Proceeding in this way we see that all the coefficients are 0. This proves that the A_{ij} are linearly independent. □

Lemma 3.3.3. *(a) If F and G have no common tangent at P, then $J^t \subset (F,G)\mathcal{O}$ for $t \geqslant m + n - 1$.*

(b) ψ is 1-1 iff F and G have distinct tangents at P.

Proof. Let $L_1, \ldots, L_m$ be the tangents to F at P. For $i > m$ define $L_i = L_m$. Similarly, let $M_1, \ldots, M_n$ be the tangents to G at P. For $j > n$ define $M_j = M_n$. Let $A_{ij} = L_1 \ldots L_i M_1 \ldots M_j$ for all $i, j \geqslant 0$ (take $L_0 = M_0 = 1$). In view of Lemma 3.3.2, to prove (a) it suffices to show that $A_{ij} \subset (F,G)\mathcal{O}$ for all $i + j \geqslant m + n - 1$.

We will first show that there is $N \gg 0$ such that $J^N \subset (F,G)\mathcal{O}$. Let $V(F,G) = \{P, Q_1, \ldots, Q_s\}$. Choose a polynomial H such that $H(Q_i) = 0$ for all i and $H(P) \neq 0$. Then HX and HY are in $I(V(F,H)) = \mathrm{Rad}(F,G)$. Thus, $(HX)^N$ and $(HY)^N$ are in (F,G) for some $N \gg 0$. Since H is a unit in the local ring $\mathcal{O}$, it follows that $X^N, Y^N \in (F,G)\mathcal{O}$. Thus, it follows that $J^{2N} \subset (F,G)\mathcal{O}$. Next we will show that if $t \geqslant m+n-1$ and $J^{t+1} \subset (F,G)\mathcal{O}$ then $J^t \subset (F,G)\mathcal{O}$. This will prove (a).

Let us assume that $i+j = t \geqslant m+n-1$. Assume that we have proved that $J^{t+1} \subset (F,G)\mathcal{O}$. Since $i+j \geqslant m+n-1$, either $i \geqslant m$ or $j \geqslant n$. Let us assume that $i \geqslant m$. Then $A_{ij} = L_1 \ldots L_m B = A_{m0} B$ for some form B. As $A_{m0} = F_m = F - F'$ for some $F' \in J^{m+1}$, it follows that $A_{ij} = BF - BF'$, where $BF' \in J^{(i-m)+(m+1)} = J^{i+j+1} = J^{t+1}$. This completes the proof of (a).

To prove (b), let us first assume that the tangents are distinct. Suppose $\psi(\bar{A}, \bar{B}) = 0$, that is, $AF + BG \in J^{m+n}$. Suppose $(\bar{A}, \bar{B}) \neq (0,0)$. Let us assume that $\bar{A} \neq 0$. We may write $\bar{A} = A_r + A_{r+1} + \ldots$, with $r < n$ and $A_r \neq 0$. Write $\bar{B} = B_s + B_{s+1} + \ldots$. Then

$$AF + BG = A_r F_m + B_s G_n + \text{higher order terms} \in J^{m+n}\,.$$

If $A_r F_m$ and $B_s G_n$ have different degrees, then both of then have to be in J^{m+n}, which is a contradiction as $A_r F_m$ is a form of degree strictly less than $m+n$. If they are of the same degree then we get

$$A_r L_1 \ldots L_m + B_s M_1 \ldots M_n = 0.$$

But this is not possible as the tangents are distinct. Thus, $(\bar{A}, \bar{B}) = (0,0)$. This proves ψ is injective.

Conversely, if L be a common tangent to F and G at P, write $F_m = LF'_{m-1}$ and $G_n = LG'_{n-1}$. Then $\psi(\bar{G}'_{n-1}, -\bar{F}'_{m-1}) = \overline{FG'_{n-1} - GF'_{m-1}} = \overline{F_m G'_{n-1} - G_n F'_{m-1}} = 0$. Thus, ψ is not injective. This completes the proof of the Lemma. □

Proposition 3.3.4. *The intersection number satisfies the further additional properties:*

8. *If P is a simple point of F then $I(P, F \cap G)$ equals the order of G in the DVR $\mathcal{O}_P(F)$.*

9. *If F and G have no common components then*

$$\sum_P I(P, F \cap G) = \dim_k(k[X,Y]/(F,G))\,.$$

Proof. For the first point, using property (6) of the intersection number, We may assume that F is irreducible. Note that

$$\mathcal{O}_P(\mathbb{A}^2)/(F,G) \cong \mathcal{O}_P(F)/(\bar{G})\,.$$

Clearly, the dimension of this vector space equals the order of $\bar{G}$ in the DVR $\mathcal{O}_P(F)$.

The second point is clear from Proposition 1.6.1 and Proposition 2.8.1. □

3.4 Exercises

Exercise 3.4.1. Prove that in the above examples $P = (0, 0)$ is the only multiple point on the curves C, D, E, and F.

Solution. A point P is multiple on a plane curve $F(X, Y) = 0$ if

$$F(P) = F_X(P) = F_Y(P) = 0.$$

In each of the given examples C, D, E, F, one verifies directly:

1. $F(0, 0) = 0$. 2. $F_X(0, 0) = F_Y(0, 0) = 0$. 3. Away from $(0, 0)$, the equations $F_X = F_Y = 0$ have no simultaneous solutions on the curve.

Thus, $(0, 0)$ is the only point where all first derivatives vanish simultaneously on the curve. Hence,e it is the only multiple point. □

Exercise 3.4.2. Find the multiple points and tangent lines at those points for the following curves:

(a) $Y^3 - Y^2 + X^3 - X^2 + 3XY^2 + 3X^2Y + 2XY$

(b) $X^4 + Y^4 - X^2Y^2$

(c) $X^3 + Y^3 - 3X^2 - 3Y^2 + 3XY + 1$

(d) $Y^2 + (X^2 - 5)(4X^4 - 20X^2 + 25)$

Sketch the real part of (d).

Solution. We determine multiple points by solving

$$F = F_X = F_Y = 0.$$

(a) At $(0, 0)$, all first derivatives vanish, so it is a double point. The quadratic part of F is

$$-X^2 - Y^2 + 2XY.$$

Factoring:

$$-(X - Y)^2.$$

Thus, the tangent line is $X = Y$ (double tangent).

(b) $F = X^4+Y^4-X^2Y^2$. At $(0, 0)$, the lowest degree terms are degree 4, so multiplicity 4. The leading form is

$$X^4 + Y^4 - X^2Y^2 = (X^2 - Y^2)^2.$$

Thu,s the tangents are $X = \pm Y$, each with multiplicity 2.

(c) At $(1, 1)$ one checks

$$F(1, 1) = F_X(1, 1) = F_Y(1, 1) = 0.$$

Expanding around $(1, 1)$ shows the quadratic part factors into two distinct linear forms, giving two distinct tangents; hence $(1, 1)$ is a node.

(d) The equation simplifies:

$$Y^2 + (X^2 - 5)^3 = 0.$$

Then, the singular points occur where

$$Y = 0, \quad (X^2 - 5)^3 = 0.$$

So $X = \pm\sqrt{5}$, $Y = 0$ are double points. The real curve consists of two cuspidal branches meeting the x-axis at $\pm\sqrt{5}$.

Sketch description: The curve is symmetric about the x-axis and consists of two real branches touching the axis at $\pm\sqrt{5}$, with no other real points. □

Exercise 3.4.3. If a curve F of degree n has a point P of multiplicity n, show that F consists of n lines through P (not necessarily distinct).

Solution. Translate coordinates so that $P = (0, 0)$.

If P has multiplicity n, then the lowest-degree nonzero homogeneous part of F has degree n. Since $\deg F = n$, the polynomial consists entirely of its homogeneous degree-n part.

Thus F is a homogeneous polynomial of degree n. Over an algebraically closed field, any homogeneous polynomial in two variables factors into linear forms:

$$F = L_1 L_2 \cdots L_n.$$

Each L_i defines a line through $(0, 0)$. Thus F consists of n lines through P. □

Exercise 3.4.4. Let P be a double point of a curve F. Show that P is a node iff

$$F_{XY}(P)^2 \neq F_{XX}(P)F_{YY}(P).$$

Solution. At a double point, the quadratic part determines tangents:

$$Q(X, Y) = \frac{1}{2}(F_{XX}X^2 + 2F_{XY}XY + F_{YY}Y^2).$$

This quadratic form factors into two distinct linear forms iff its discriminant is nonzero:

$$(2F_{XY})^2 - 4F_{XX}F_{YY} \neq 0,$$

i.e.

$$F_{XY}^2 \neq F_{XX}F_{YY}.$$

Thus, P is a node exactly when the quadratic part has two distinct linear factors. □

Exercise 3.4.5. Assume $\mathrm{char}(k) = 0$. Show that $m_P(F)$ is the smallest integer m such that for some $i + j = m$,

$$\frac{\partial^m F}{\partial x^i \partial y^j}(P) \neq 0.$$

Describe the leading form at P in terms of these derivatives.

Solution. Translate so that $P = (0, 0)$.

Expand F in its Taylor series:

$$F(X, Y) = \sum_{i,j} \frac{1}{i!j!} \frac{\partial^{i+j} F}{\partial X^i \partial Y^j}(0, 0) X^i Y^j.$$

The multiplicity $m_P(F)$ is the smallest total degree m such that a coefficient of degree m is nonzero. This occurs exactly when some partial derivative of order m is nonzero at P.

Thus

$$m_P(F) = \min\{\, m : \exists\, i + j = m,\ \partial^m F/\partial X^i \partial Y^j(P) \neq 0 \,\}.$$

The leading form is the homogeneous polynomial of degree m:

$$F_m(X, Y) = \sum_{i+j=m} \frac{1}{i!j!} \frac{\partial^m F}{\partial X^i \partial Y^j}(P) X^i Y^j.$$

This homogeneous form determines the tangent cone at P. □

Exercise 3.4.6. Irreducible curves with given tangent lines L_i of multiplicities r_i may be constructed as follows: if $\sum r_i = m$, let

$$F = \prod L_i^{r_i} + F_{m+1},$$

where F_{m+1} is chosen so that F is irreducible.

Solution. Let $P = (0,0)$ and assume the L_i are distinct linear forms through P. The product

$$F_m = \prod L_i^{r_i}$$

is a homogeneous polynomial of degree m, whose tangent cone at P consists of the lines L_i with multiplicities r_i.

Now define

$$F = F_m + F_{m+1},$$

where F_{m+1} has degree $m+1$.

Then the lowest-degree nonzero homogeneous part of F at P is F_m, so the multiplicity at P is m, and the tangent cone is precisely $\prod L_i^{r_i}$.

Choosing F_{m+1} generically ensures that F does not factor, by Problem 2.34 (a form plus a higher-degree form without common factors is irreducible). Thus F is irreducible with the prescribed tangent lines and multiplicities. □

Exercise 3.4.7. Let $T : \mathbb{A}^2 \to \mathbb{A}^2$ be a polynomial map with $T(Q) = P$.

(a) Show $m_Q(F^T) \geq m_P(F)$.

(b) Show equality holds if $J_Q T$ is invertible.

(c) Show the converse is false using $T = (X^2, Y)$ and $F = Y - X^2$.

Solution. (a) Let us first understand what is meant by F^T. Note that the map T gives rise to a map $\tilde{T} : k[X,Y] \to k[X,Y]$. Then F^T is the image $\tilde{T}(F)$. After a linear change of coordinates on both the domain and codomain, we may assume that both P and Q are the origin. It follows that $\tilde{T}(X), \tilde{T}(Y) \in (X,Y)$. Thus, $\tilde{T}(F) = F(\tilde{T}(X), \tilde{T}(Y))$. If F has multiplicity m at P, then its lowest nonzero homogeneous part at P has degree m. It is clear that $\tilde{T}(F)$ has multiplicity at least m.

(b) Let us write $T = (T_1, T_2)$. The Jacobian matrix is the 2×2 matrix of partial derivatives at the point $(0,0)$. Write $T_i = L_i + M_i$, then the Jacobian matrix depends only on the L_i. The Jacobian matrix is invertible iff L_1 and L_2 are linearly independent. In this case, after a linear change of coordinates, we may assume that $L_1 = X$ and $L_2 = Y$. Then it is clear that the lowest nonzero homogeneous part of $\tilde{T}(F)$ has degree m.

(c) Let $T = (X^2, Y)$, $F = Y - X^2$. Then

$$F^T = Y - (X^2)^2 = Y - X^4.$$

At $(0,0)$, $m_P(F) = 2$ but $m_Q(F^T) = 4$. Thus equality may fail when the Jacobian is not invertible. □

Exercise 3.4.8. Let $F \in k[X_1, \ldots, X_n]$ define a hypersurface $V(F)$.

(a) Define $m_P(F)$.

(b) If $m_P(F) = 1$, define the tangent hyperplane.

(c) Examine $F = X^2 + Y^2 - Z^2$, $P = (0, 0, 0)$.

Solution. (a) $m_P(F)$ is the smallest degree of a nonzero homogeneous term in the Taylor expansion of F at P.

(b) If $m_P(F) = 1$, the linear part is nonzero:

$$\sum F_{X_i}(P)(X_i - P_i) = 0,$$

which defines the tangent hyperplane.

(c) For $F = X^2 + Y^2 - Z^2$, at $(0, 0, 0)$ all first derivatives vanish, so multiplicity is 2. The quadratic part defines a cone. Thus, no unique tangent hyperplane exists at multiple points. □

Exercise 3.4.9. Show that an irreducible plane curve has only finitely many multiple points. Is this true for hypersurfaces?

Solution. Multiple points satisfy

$$F = F_X = F_Y = 0.$$

These are three polynomial equations in two variables. Since F is irreducible, F does not divide both F_X and F_Y, so the system has only finitely many solutions.

For hypersurfaces in higher dimensions, the singular locus may have positive dimension (e.g., a cone), so infinitely many singular points may occur. □

Exercise 3.4.10. Let $V \subset \mathbb{A}^n$ be affine, $P \in V$. The tangent space is

$$T_P(V) = \{(v_1, \ldots, v_n) \mid \sum G_{X_i}(P)v_i = 0 \text{ for all } G \in I(V)\}.$$

If $V = V(F)$ is a hypersurface with F irreducible, show

$$T_P(V) = \{(v_1, \ldots, v_n) \mid \sum F_{X_i}(P)v_i = 0\}.$$

Relate $\dim T_P(V)$ to $m_P(F)$.

Solution. If $V = V(F)$ with F irreducible, then $I(V) = (F)$. Thus every $G \in I(V)$ is HF. Differentiating gives

$$G_{X_i}(P) = H(P)F_{X_i}(P).$$

Hence, the tangent condition reduces to

$$\sum F_{X_i}(P)v_i = 0.$$

If $m_P(F) = 1$, some derivative is nonzero, so the tangent space has codimension 1 (dimension $n-1$). If $m_P(F) > 1$, all first derivatives vanish, so every vector satisfies the condition and

$$T_P(V) = \mathbb{A}^n.$$

Thus

$$\dim T_P(V) = \begin{cases} n-1, & m_P(F) = 1, \\ n, & m_P(F) > 1. \end{cases}$$

□

Exercise 3.4.11. A simple point P on a curve F is called a flex if $\mathrm{ord}_P^F(L) \geq 3$, where L is the tangent at P.

(a) Let $F = Y - X^n$. For which n does F have a flex at $P = (0,0)$, and what kind?

(b) Suppose $P = (0,0)$, $L = Y$ is the tangent line, and $F = Y + aX^2 + \cdots$. Show P is a flex iff $a = 0$. Give a simple criterion for computing $\mathrm{ord}_P^F(Y)$.

Solution. (a) For $F = Y - X^n$, the tangent line at $(0,0)$ is $Y = 0$.

On the curve,

$$Y = X^n.$$

Thus the intersection multiplicity with $Y = 0$ is n:

$$\mathrm{ord}_P^F(Y) = n.$$

Hence,

- If $n = 1$, the point is simple, not a flex.
- If $n = 2$, ord $= 2$ (no flex).
- If $n = 3$, ord $= 3$: ordinary flex.
- If $n > 3$, ord ≥ 4: higher flex.

(b) Write

$$F = Y + aX^2 + (\text{higher terms}).$$

On the curve,

$$Y = -aX^2 + \cdots .$$

Thus, unless $a = 0$,

$$\operatorname{ord}_P^F(Y) = 2\,,$$

in which case the first nonzero term has degree ≥ 3. Hence, P is a flex iff $a = 0$.

Criterion: $\operatorname{ord}_P^F(Y)$ equals the smallest degree of X appearing in the expansion of Y as a function of X along the curve. □

Exercise 3.4.12. Let $\mathfrak{m} = \mathfrak{m}_P(F)$. Show that

$$\dim_k(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = n + 1 \quad \text{for } 0 \leq n < m_P(F).$$

In particular, P is simple iff $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$.

Solution. Near $P = (0, 0)$, write

$$F = F_m + F_{m+1} + \cdots ,$$

where $m = m_P(F)$.

We claim that for $n < m$, the relations defining the curve do not affect monomials of degree $\leq n$. Let $I \subset k[X, Y]$ denote the ideal (X, Y). Then there is a surjection

$$I^n/I^{n+1} \to \mathfrak{m}^n/\mathfrak{m}^{n+1} = I^n/I^n \cap (I^{n+1} + (F))\,.$$

Suppose a nonzero form G of degree n in I^n maps to 0. Then it follows that it is in $I^{n+1} + (F)$. But clearly this is not possible if $n < m$.

Thus monomials

$$X^iY^j, \qquad i + j = n,$$

remain linearly independent in $\mathfrak{m}^n/\mathfrak{m}^{n+1}$.

There are $n + 1$ such monomials, so

$$\dim_k(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = n + 1.$$

For $n = 1$:

$$\dim_k(\mathfrak{m}/\mathfrak{m}^2) = \begin{cases} 1, & m = 1, \\ 2, & m > 1. \end{cases}$$

Thus P is simple iff this dimension equals 1. □

Exercise 3.4.13. Let $V = V(X^2 - Y^3, Y^2 - Z^3) \subset \mathbb{A}^3$, $P = (0,0,0)$, $\mathfrak{m} = \mathfrak{m}_P(V)$. Find $\dim_k(\mathfrak{m}/\mathfrak{m}^2)$.

Solution. The maximal ideal is generated by $\bar{X}, \bar{Y}, \bar{Z}$.

The defining relations begin in degree ≥ 2:

$$X^2 - Y^3, \qquad Y^2 - Z^3.$$

Thus, in degree 1, there are no linear relations among X, Y, Z. Therefore

$$\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 3.$$

Hence, the tangent space has dimension 3. □

Exercise 3.4.14. (a) Let $\mathscr{O} = \mathscr{O}_P(\mathbb{A}^2)$, $\mathfrak{m}$ its maximal ideal. Compute

$$\chi(n) = \dim_k(\mathscr{O}/\mathfrak{m}^n).$$

(b) Let $\mathscr{O} = \mathscr{O}_P(\mathbb{A}^r)$. Show $\chi(n)$ is a polynomial of degree r with leading coefficient $1/r!$.

Solution. (a) Monomials X^iY^j with $i + j < n$ form a basis of $\mathscr{O}/\mathfrak{m}^n$. Their number equals

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Thus

$$\chi(n) = \frac{n(n+1)}{2}.$$

(b) In $\mathbb{A}^r$, monomials of total degree $< n$ correspond to solutions of

$$\alpha_1 + \cdots + \alpha_r < n.$$

Their number equals

$$\binom{n+r-1}{r}.$$

This is a polynomial in n of degree r, with leading term

$$\frac{n^r}{r!}.$$

□

Exercise 3.4.15. Let $F \in k[X_1, \ldots, X_r]$ define a hypersurface, $P = (0, \ldots, 0)$, $m = m_P(F)$. Let $\mathscr{O} = \mathscr{O}_P(V(F))$, $\mathfrak{m}$ its maximal ideal. Show

$$\chi(n) = \dim_k(\mathscr{O}/\mathfrak{m}^n)$$

is a polynomial of degree $r-1$ for large n, with leading coefficient $m/(r-1)!$.

Can you define the multiplicity of a local ring in general?

Solution. Near P, write

$$F = F_m + F_{m+1} + \cdots,$$

with F_m homogeneous of degree m.

Let $I \subset k[X_1, \ldots, X_r] =: R$ denote the ideal $(X_1, \ldots, X_r)$. Then there is a surjection

$$R/I^n \to \mathcal{O}/\mathfrak{m}^n = R/(I^n + (F)).$$

Consider the multiplication by F map:

$$k[X_1, \ldots, X_r] \to k[X_1, \ldots, X_r], \quad G \mapsto GF.$$

Let $F = F_m + \ldots + F_d$, with $F_m \neq 0$. It is clear that $FI^k \subset I^{k+m}$. Conversely, if $GF \in I^{k+m}$, then writing $G = G_l + \ldots + G_t$, we see that $l \geq k$, that is, $G \in I^k$. This shows that we have an inclusion

$$k[X_1, \ldots, X_r]/I^k \hookrightarrow k[X_1, \ldots, X_r]/I^{k+m}, \quad \bar{G} \mapsto \overline{GF}.$$

Thus, for every $k \geq 0$, we have a short exact sequence

$$0 \to k[X_1, \ldots, X_r]/I^k \to k[X_1, \ldots, X_r]/I^{k+m} \to k[X_1, \ldots, X_r]/(I^{k+m}, F) \to 0.$$

It follows that for n large, we have

$$\dim_k(\mathscr{O}/\mathfrak{m}^n) = \dim_k(R/I^n) - \dim_k(R/I^{n-m}).$$

Thus,

$$\chi(n) \sim \frac{m}{(r-1)!} n^{r-1}$$

for large n.

Hence $\chi(n)$ is a polynomial of degree $r-1$, with leading coefficient $m/(r-1)!$.

Multiplicity definition. For a local ring $(R, \mathfrak{m})$ of dimension d, define the multiplicity $e(R)$ to be

$$e(R) = d! \times (\text{leading coefficient of } \dim_k(R/\mathfrak{m}^n)).$$

This agrees with:
- plane curve multiplicity,
- hypersurface multiplicity,
- DVR case ($e = 1$).

Thus, multiplicity is the leading coefficient of the Hilbert–Samuel polynomial. □

Exercise 3.4.16. Find the intersection numbers of various pairs of curves from the examples of Section 1 at $P = (0, 0)$.

Solution. The intersection number is defined by

$$I(P, F \cap G) = \dim_k \mathscr{O}_P/(F, G).$$

In each example from Section 1, one computes by substituting the parametrization of one curve into the other, or by comparing leading forms.

Typical cases:

1. If $F = Y - X^n$ and $G = Y$, then

$$I(0, F \cap G) = n.$$

2. If $F = XY$ and $G = X$, then

$$I(0, F \cap G) = 1.$$

3. If two curves have distinct tangent lines at P, then

$$I(P, F \cap G) = 1.$$

4. If they share a common tangent line, the intersection multiplicity equals the order of contact determined by the lowest-degree terms.

Thus, intersection numbers are computed from the orders of vanishing of one equation along the parametrization of the other. □

Exercise 3.4.17. A line L is tangent to a curve F at P iff

$$I(P, F \cap L) > m_P(F).$$

Solution. Let $m = m_P(F)$.

If L is not tangent, then its defining linear form does not divide the leading homogeneous part F_m. Thus, the intersection multiplicity equals m.

If L is tangent, then its defining linear form divides F_m. Hence the lowest-degree term of F vanishes to order $\geq m + 1$ along L, giving

$$I(P, F \cap L) > m.$$

Thus, the condition characterizes tangency. □

Exercise 3.4.18. If P is simple on F, show

$$I(P, F \cap (G + H)) \geq \min(I(P, F \cap G), I(P, F \cap H)).$$

Give an example where this fails if P is not simple.

Solution. If P is simple, then $\mathscr{O}_P(F)$ is a DVR. Intersection multiplicity becomes the valuation:

$$I(P, F \cap G) = \mathrm{ord}_P^F(G).$$

Since valuations satisfy

$$\mathrm{ord}(G + H) \geq \min(\mathrm{ord}(G), \mathrm{ord}(H)),$$

The inequality follows.

Counterexample. Let $F = Y^2 - X^3$ (a cusp at 0). Let $G = Y^3$ and $H = X^2 - Y^3$. Check using Macaulay2 that the inequality is violated.

Thus, the statement may fail at singular points. □

Exercise 3.4.19. Let F be a plane curve and L a line not a component of F. Parametrize L by

$$(a + tb,\ c + td).$$

Define $G(T) = F(a + Tb, c + Td)$. Factor

$$G(T) = \epsilon \prod (T - \lambda_i)^{e_i}.$$

Show there is a one-to-one correspondence between the λ_i and $P_i \in L \cap F$, and that

$$I(P_i, L \cap F) = e_i.$$

Conclude

$$\sum I(P, L \cap F) \leq \deg F.$$

Solution. Substituting the parametrization of L into F produces a polynomial $G(T)$ of degree $\leq \deg F$.

Each root λ_i gives a point

$$P_i = (a + \lambda_i b,\ c + \lambda_i d) \in L \cap F.$$

Conversely, each intersection point arises from some λ_i.

The multiplicity e_i equals the order of vanishing of F along the parametrization, which equals

$$I(P_i, L \cap F).$$

Since $\deg G \leq \deg F$,

$$\sum e_i \leq \deg F.$$

□

Exercise 3.4.20. Suppose P is a double point on F with only one tangent L.

(a) Show $I(P, F \cap L) \geq 3$.

(b) If $P = (0, 0)$ and $L = Y$, show P is a cusp iff $F_{XXX}(P) \neq 0$.

(c) Show a cusp has only one component through P.

Solution. (a) Since P is double, $m_P(F) = 2$. Having only one tangent means the quadratic form is a square:

$$F_2 = L^2.$$

It is clear that

$$\mathcal{O}_P(\mathbb{A}^2)/(F, L) \cong \mathcal{O}_P(\mathbb{A}^2)/(F_3 + F_4 + \ldots + F_d, L) \cong \mathcal{O}_P(L)/(\bar{F}_3 + \bar{F}_4 + \ldots + \bar{F}_d)\,.$$

Thus,

$$I(P, F \cap L) \geq 3.$$

(b) Let $F = Y^2 + aX^3 + \cdots$ with $L = Y$. Then substituting $Y = 0$,

$$F|_{Y=0} = aX^3 + \cdots\,.$$

Thus

$$I(P, F \cap L) = 3$$

iff the cubic term is nonzero, that is,

$$F_{XXX}(P) \neq 0.$$

(c) If F had two components through P, the quadratic part would factor into two distinct linear forms, giving two tangents. Since a cusp has only one tangent, F must have only one branch through P. □

Exercise 3.4.21. Let F be an irreducible plane curve, $P = (0,0)$, $m = m_P(F) > 1$, and $\mathfrak{m} = \mathfrak{m}_P(F)$. (a) Show that the map

$$\{aX + bY\} \longrightarrow \mathfrak{m}/\mathfrak{m}^2, \quad aX + bY \mapsto \overline{ax + by}$$

is a vector space isomorphism.
(b) Suppose P is an ordinary multiple point with tangents $L_1, \ldots, L_m$. Show $I(P, F \cap L_i) > m$ and $\overline{l_i} \neq \lambda \overline{l_j}$ for $i \neq j$.
(c) Conversely, suppose there are $G_1, \ldots, G_m$ with

$$I(P, F \cap G_i) > m$$

and $\bar{g}_i \neq \lambda \bar{g}_j$. Show P is an ordinary multiple point.
(d) Conclude that P is ordinary multiple iff there exist $g_1, \ldots, g_m \in \mathfrak{m}$ such that

$$\bar{g}_i \neq \lambda \bar{g}_j \quad \text{and} \quad \dim \mathscr{O}_P(F)/(g_i) > m.$$

Solution. (a) From Problem 3.13, for $m > 1$,

$$\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 2.$$

The residue classes of x and y form a basis. Thus, the map sending $aX + bY$ to $\overline{ax + by}$ is linear, injective, and surjective. Hence, it is an isomorphism.

(b) If P is an ordinary multiple point, the leading homogeneous form factors as

$$F_m = L_1 \cdots L_m,$$

with distinct linear forms. Each L_i divides F_m, so

$$I(P, F \cap L_i) > m.$$

Distinct tangents give distinct linear forms, hence their residues in $\mathfrak{m}/\mathfrak{m}^2$ are not proportional.

(c) Write

$$G_i = L_i + (\text{higher terms}).$$

Then $\bar{l}_i = \bar{g}_i \neq 0$, so L_i is the tangent to G_i. Since $I(P, F \cap G_i) > m$, Property (5) implies L_i is tangent to F. The distinctness of $\bar{g}_i$ ensures distinct tangent directions.

Thus F has m distinct tangents at P, so P is an ordinary multiple point.

(d) If P is an ordinary multiple, take $g_i = l_i$ the linear forms defining the tangents. Then $\bar{g}_i$ are distinct and

$$\dim \mathscr{O}_P(F)/(g_i) > m$$

because intersection multiplicity exceeds m.

Conversely, if such g_i exist, part (c) shows P has m distinct tangents, hence is an ordinary multiple. □

Chapter 4

Projective Varieties

The motivation for defining projective space and projective varieties is clear: to get uniform answers to intersection numbers, among many other things. We will see more of these as we progress.

4.1 Projective n-space

Projective n-space over k, denoted $\mathbb{P}^n_k$, or simply $\mathbb{P}^n$, is the set of all lines through the origin in the vector space k^{n+1}. Thus, we may also view this as $(k^{n+1} \setminus \{(0, \ldots, 0)\})/k^*$. That is, we look at the set $k^{n+1} \setminus \{0\}$ with the action of the group k^* given by $\lambda \cdot (X_1, \ldots, X_{n+1}) := (\lambda x_1, \ldots, \lambda x_{n+1})$, and $\mathbb{P}^n$ is the space of orbits for this action.

Then projective space is the space of orbits. We will represent a point $P \in \mathbb{P}^n$ by $[x_1 : \ldots : x_{n+1}]$. In other words, if $\lambda \in k^*$, then $[x_1 : \ldots : x_{n+1}]$ and $[\lambda x_1 : \ldots : \lambda x_{n+1}]$ represent the same point, that is, this is defined only upto multiplication by elements of k^*.

Let $U_i = \{P \in \mathbb{P}^n \mid x_i \neq 0\}$. Note that this is independent of the choice of representative for P and so it is well-defined. Any element of U_i may be uniquely represented as

$$[x_1 : \ldots : x_{i-1} : 1 : x_{i+1} : \ldots : x_{n+1}].$$

Thus, we get a bijection $\mathbb{A}^n \to U_i$ given by $(a_1, \ldots, a_n) \mapsto [a_1 : \ldots : 1 : \ldots : a_n]$. The set $\mathbb{P}^n \setminus U_i$ equals $\{P \in \mathbb{P}^n \mid x_i(P) = 0\}$. Again, notice that the condition $x_i(P) = 0$ is well defined on equivalence classes. The complement is usually called a **hyperplane at infinity**.

4.2 Projective Algebraic Sets

Let $F \in k[X_1, \ldots, X_{n+1}]$ be a homogeneous polynomial. Then we can "evaluate" F at a point $P \in \mathbb{P}^n$ and ask whether the value is 0 or not. Notice that since F is a form, the answer of being 0 or not does not depend on the choice of homogeneous coordinates of P.

Let $S \subset k[X_1, \ldots, X_{n+1}]$ be a subset consisting of forms. We define

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

Let I be the ideal generated by S. Notice that I is a homogeneous ideal, that is, if $F = F_0 + \ldots + F_d \in I$ then each $F_i \in I$. It is clear that $V(I) = V(S)$. It is easy to check that an ideal I is homogeneous iff it can be generated by homogeneous elements.

Let $X \subset \mathbb{P}^n$ be a subset. Define

$$I(X) := \{F \in k[X_1, \ldots, X_{n+1}] \mid F \text{ is a form and } F(P) = 0 \text{ for all } P \in X\}.$$

We define the ideal of the empty set to be (1).

An algebraic set $V \subset \mathbb{P}^n$ is called **irreducible** if it cannot be written as a union of two proper algebraic subsets. A homogeneous ideal is prime iff for all forms F, G, the following condition is satisfied:

$$FG \in I \implies F \in I \text{ or } G \in I.$$

Analogous to what we proved earlier, it follows that V is irreducible $\iff$ $I(V)$ is prime. Similarly, we see that any projective algebraic subset is a finite union of irreducible projective varieties.

Define the **cone** of a projective variety $V \subset \mathbb{P}^n$ to be the set

$$C(V) = \{(a_1, \ldots, a_{n+1}) \in \mathbb{A}^{n+1} \mid [a_1 : \ldots : a_{n+1}] \in V \text{ or } (a_1, \ldots, a_{n+1}) = (0, \ldots, 0)\}.$$

If $V = \emptyset$ then $C(V) = \{(0, \ldots, 0)\}$.

The correspondence between projective algebraic sets and homogeneous ideals satisfies the following relations:

- If I_α is any collection of homogeneous ideals then $V(\bigcup I_\alpha) = \bigcap V(I_\alpha)$.
- If $I \subset J$ are homogeneous ideals then $V(I) \supset V(J)$.
- If F and G are forms then $V(FG) = V(F) \cup V(G)$.
- $V(I) \cup V(J) = V(\{FG \mid F \in I \text{ and } G \in J\})$.

- $V(0) = \mathbb{P}^n$; $V(1) = \emptyset$; if $a_i \neq 0$ then $V(a_i x_1 - a_1 x_i, \ldots, a_i x_{n+1} - a_{n+1} x_i) = \{[a_1 : \ldots : a_{n+1}]\}$. If $[b_1 : \ldots : b_{n+1}] \in V(a_i x_1 - a_1 x_i, \ldots, a_i x_{n+1} - a_{n+1} x_i)$, then $b_i = 0$ would imply that all other b_j equal 0, but then this does not define a point in projective space. Thus, $b_i \neq 0$ and then it is clear that $[b_1 : \ldots : b_{n+1}] = [a_1 : \ldots : a_{n+1}]$. So any finite subset of $\mathbb{P}^n$ is an algebraic subset.

- If $X \subset Y$ then $I(X) \supset I(Y)$.

- $I(\emptyset) = k[X_1, \ldots, X_{n+1}]$; $I(\mathbb{P}^n) = (0)$ if k is infinite.

- $I(\{(a_1 : \ldots : a_{n+1})\}) = (a_i X_1 - a_1 X_i, a_i X_2 - a_2 X_i, \ldots, a_i X_{n+1} - a_{n+1} X_i)$ where $a_i \neq 0$. If F is a form of degree d such that $F(a_1, \ldots, a_{n+1}) = 0$, we may write it follows that
$$F = X_i^d F\left(\frac{X_1}{X_i}, \ldots, 1, \ldots, \frac{X_{n+1}}{X_i}\right).$$
Then since $F\left(\frac{a_1}{a_i}, \ldots, 1, \ldots, \frac{a_{n+1}}{a_i}\right) = 0$, using the "power series expansion around $(\frac{a_1}{a_i}, \ldots, 1, \ldots, \frac{a_{n+1}}{a_i})$" trick,
$$F\left(\frac{X_1}{X_i}, \ldots, 1, \ldots, \frac{X_{n+1}}{X_i}\right) = \sum_{j \neq i} \left(\frac{X_j}{X_i} - \frac{a_j}{a_i}\right) H_j\left(\frac{X_1}{X_i}, \ldots, \frac{X_{n+1}}{X_i}\right).$$
This also shows that $\deg H_j < d$. Multiplying both sides with X_i^d we get that $F \in (a_i X_1 - a_1 X_i, a_i X_2 - a_2 X_i, \ldots, a_i X_{n+1} - a_{n+1} X_i)$.

- $I(V(S)) \supset S$ for any set of homogeneous polynomials. Similarly, $V(I(X)) \supset X$ for any subset X.

- $I(V(S)) \supset S \Rightarrow V(I(V(S))) \subset V(S)$. Putting $X = V(S)$ in $V(I(X)) \supset X$ gives $V(I(V(S))) \supset V(S)$. This proves $V(I(V(S))) = V(S)$.

- $I(V(I(X))) = I(X)$. First $V(I(X)) \supset X \Rightarrow I(V(I(X))) \subset I(X)$. Putting $S = I(X)$ in $I(V(S)) \supset S$ gives $I(V(I(X))) \supset I(X)$. This shows that $I(V(I(X))) = I(X)$.

- $I(X)$ is a homogeneous radical ideal. Note that if I is a homogeneous ideal then $\mathrm{Rad}(I)$ is also homogeneous.

- Given a projective variety V, we may form the cone over it, $C(V) \subset \mathbb{A}^{n+1}$. If $V \neq \emptyset$ then we claim that $\mathrm{Ideal}(C(V)) = \mathrm{Ideal}(V)$. Note that if $V = \emptyset$ then these are not equal as the LHS is $(x_1, \ldots, x_{n+1})$ and the RHS is (1). So assume

$V \neq \emptyset$ and let $F \in \text{Ideal}(V)$. As $V \neq \emptyset$, it follows that F is a homogeneous polynomial of deg $\geqslant 1$. Then it is clear that F vanishes on $C(V)$. Conversely, if F vanishes on $C(V)$, then first note that $F(0,\ldots,0) = 0$ implies that F has no constant term. If $P \in V$, then it is easy to see that each homogeneous component of F vanishes on P (fix $a_1,\ldots,a_{n+1}$, and consider the polynomial $F(\lambda a_1,\ldots,\lambda a_{n+1})$ in λ. If the coefficients are not all zero then this poly vanishes only at finitely many values of λ). Clearly, each homogeneous component vanishes at $(a_1,\ldots,a_{n+1})$. This shows that $\text{Ideal}(C(V))$ is a homogeneous ideal contained in $\text{Ideal}(V)$. This proves $\text{Ideal}(C(V)) = \text{Ideal}(V)$.

Given a homogeneous ideal $I \subset k[X_1,\ldots,X_{n+1}]$, it defines an affine algebraic set in $\mathbb{A}^{n+1}$ and a projective algebraic set in $\mathbb{P}^n$. The affine algebraic set will be denoted $V_a(I)$ and the projective algebraic set by $V_p(I)$.

Theorem 4.2.1 (Projective Nullstellensatz)**.** *Let $I \subset k[X_1,\ldots,X_{n+1}]$ be a homogeneous ideal.*

1. *$V_p(I) = \emptyset$ iff there is an integer N such that I contains all forms of degree $\geqslant N$.*
2. *If $V_p(I) \neq \emptyset$ then $I(V_p(I)) = \text{Rad}(I)$.*

Proof. (1) Assume $V_p(I) = \emptyset$. If $I = (1)$ then there is nothing to prove. So let us assume that I is a proper ideal of $k[X_1,\ldots,X_{n+1}]$. Since I is homogeneous, it follows that $I \subset (X_1,\ldots,X_{n+1})$. Thus, $V_a(I) \supset \{(0,0,\ldots,0)\}$. It does not contain any other point, or else we would get that $V_p(I) \neq \emptyset$. Thus, $V_a(I) = \{(0,\ldots,0)\} \subset \mathbb{A}^{n+1}$. By the affine Nullstellensatz, it follows that $I(V_a(I)) = \text{Rad}(I) = (x_1,\ldots,x_{n+1})$. This shows that $\exists N$ such that $\text{Rad}(I)^N = (x_1,\ldots,x_{n+1})^N \subset I$, that is, I contains all forms of deg $\geqslant N$.

(2) Recall that we saw that if $V \neq \emptyset$ then $I(C(V)) = I(V)$. Putting $V = V_p(I)$, we have $I(C(V_p(I))) = I(V_p(I))$. Let J be a homogeneous ideal not equal to (1). It is easy to check that $C(V_p(J)) = V_a(J)$. Since $V_p(I) \neq \emptyset$, it follows that $I \neq (1)$. Thus, $C(V_p(I)) = V_a(I)$. Thus, $I(C(V_p(I))) = I(V_a(I)) = \text{Rad}(I)$ by affine Nullstellensatz. Thus, $I(V_p(I)) = I(C(V_p(I))) = I(V_a(I)) = \text{Rad}(I)$. □

Projective Coordinate Ring. Let $V \neq \emptyset$ be a projective algebraic variety. Then $I(V)$ is a prime ideal. $\Gamma_h(V) = k[X_1,\ldots,X_{n+1}]/I(V)$ is a domain, which we call the **homogeneous coordinate ring** of V. Recall that there are no non-constant holomorphic functions on a compact complex manifold. Thus, we should expect that on a projective variety there should be no global algebraic functions.

Remark 4.2.2. Recall the Zariski topology on affine algebraic sets, see Definition 2.4.1. In the same way we may define the Zariski topology on projective algebraic sets. The

closed subsets of $\mathbb{P}^n$ are precisely the subsets of the form $V(I)$ for some homogeneous ideal $I \subset k[X_1, \ldots, X_{n+1}]$. □

Note that elements of $\Gamma_h(V)$ do not define functions on V as the evaluation map is not independent of the choice of homogeneous coordinates for P: If $P = [a_1 : \ldots : a_n] = [\lambda a_1 : \ldots : \lambda a_n]$, then $F(\lambda a_1, \ldots, \lambda a_n) = \lambda^d F(a_1, \ldots, a_n)$ (except the ones in degree 0, which are constants).

However, if $F, G \in \Gamma_h(V)$ are homogeneous of the same degree, then $\frac{F}{G}$ makes sense as a function on the set of points $\{P \in V \mid G(P) \neq 0\} = V \setminus V(G)$. The element $\frac{F}{G}$ is an element of $k_h(V) =$ field of fractions of $\Gamma_h(V)$. Note that the degree of elements of $k_h(V)$ is well defined and $\frac{F}{G}$ is an element of degree 0. Clearly, we should define

$$k(V) = \{\frac{F}{G} \in k_h(V) \mid \ F \text{ and } G \text{ homogeneous of same degree}\}$$

as the field of rational functions on V. This is in analogue with our earlier definition of $k(V)$ as the field of functions defined on some non-empty open subset of V, see Remark 2.4.4.

Remark 4.2.3. Similarly, we may define $\mathcal{O}_P(V) = \{\frac{F}{G} \in k(V) \mid G(P) \neq 0\}$. This is a local ring and the maximal ideal is $\{\frac{F}{G} \in \mathcal{O}_P(V) \mid F(P) = 0\}$. □

Linear Change of Coordinates. If $T : \mathbb{A}^{n+1} \to \mathbb{A}^{n+1}$ is a linear isomorphism, then it takes a line through the origin to line through the origin, and so gives rise to an isomorphism $\mathbb{P}^n \to \mathbb{P}^n$. At the level of rings this is the isomorphism $k[X_1, \ldots, X_{n+1}] \to k[X_1, \ldots, X_{n+1}]$ where each X_i is sent to a form of degree 1 determined by T. Such an isomorphism is called a **projective change of coordinates**.

4.3 Affine and Projective Varieties

Recall that we have the natural inclusion $\varphi_{n+1} : \mathbb{A}^n \hookrightarrow \mathbb{P}^n$ given by

$$(a_1, \ldots, a_n) \mapsto [a_1 : \ldots : a_n : 1]\,.$$

Since $\mathbb{P}^n \setminus \mathbb{A}^n$ is the hyperplane $\{X_{n+1} = 0\}$, it follows that this is an open subset in the Zariski topology. Given a closed subset of $\mathbb{A}^n$, we may ask what is its closure in $\mathbb{P}^n$. This question has a simple answer which we now give.

Let V_a be an algebraic subset in $\mathbb{A}^n$ and let $I(V_a) \subset k[X_1, \ldots, X_n]$ be the ideal it defines. Let I^* be the ideal in $k[X_1, \ldots, X_{n+1}]$ generated by $\{F^* \mid F \in I\}$. Then I^* is a homogeneous ideal and we define $V_p^* \subset \mathbb{P}^n$ to be $V_p(I^*)$.

Conversely, let $V_p \subset \mathbb{P}^n$ be a projective algebraic set with ideal $I(V_p) \subset k[X_1, \ldots, X_{n+1}]$. Let I_* be the ideal in $k[X_1, \ldots, X_n]$ generated by $\{F_* \mid F \in I\}$. Define $(V_p)_*$ to be $V_a(I_*) \subset \mathbb{A}^n$.

Proposition 4.3.1. *1. If $V \subset \mathbb{A}^n$, then $\varphi_{n+1}(V) = V^* \cap U_{n+1}$ and $(V^*)_* = V$.*

2. If $V \subset W \subset \mathbb{A}^n$ then $V^* \subset W^* \subset \mathbb{P}^n$. If $V \subset W \subset \mathbb{P}^n$ then $V_* \subset W_* \subset \mathbb{A}^n$.

3. If V is irreducible in $\mathbb{A}^n$, then V^* is irreducible in $\mathbb{P}^n$.

4. If $V = \cup V_i$ is the irreducible decomposition of V in $\mathbb{A}^n$, then $V^* = \cup_i V_i^*$ is the irreducible decomposition of V^* in $\mathbb{P}^n$.

5. If $V \subset \mathbb{A}^n$ then V^* is the closure of $\varphi_{n+1}(V)$ in $\mathbb{P}^n$ in the Zariski topology.

6. If $V \subsetneq \mathbb{A}^n$ is not empty, then no component of V^* lies in or contains $H_\infty = \mathbb{P}^n \backslash U_{n+1}$.

7. If $V \subset \mathbb{P}^n$, and no component of V lies in H_∞ or contains H_∞, then $V_* \subsetneqq \mathbb{A}^n$ and $(V_*)^* = V$.

Proof. (1) It is clear that $\varphi_{n+1}(V) \subset U_{n+1}$. Let us show that $\varphi_{n+1}(V) \subset V^*$. For this, we have to show that if $P \in V$, then $\varphi_{n+1}(P)$ is in the vanishing locus of F^*, for every $F \in I$. But this is obvious. This shows that $\varphi_{n+1}(V) \subset V^* \cap U_{n+1}$. Conversely, suppose $P \in V^* \cap U_{n+1}$, then we may uniquely represent P as $(a_1 : \ldots : a_n : 1)$. Since $P \in V^*$, it follows that $F^*(P) = 0$ for all $F \in I$. It follows that $F(P) = 0$ for all $F \in I$. This proves that $P \in \varphi_{n+1}(V)$. Thus, $V^* \cap U_{n+1} \subset \varphi_{n+1}(V)$ and so $\varphi_{n+1}(V) = V^* \cap U_{n+1}$.

Let $W \subset \mathbb{P}^n$ be an algebraic subset. We claim that $W_* = \varphi_{n+1}^{-1}(W \cap U_{n+1})$. Suppose $Q \in W_*$. Then for every $F \in I(W)$ we have $(F_*)(Q) = 0$, that is,

$$F(a_1, \ldots, a_n, 1) = F(\varphi_{n+1}(Q)) = 0\,.$$

This shows that $\varphi_{n+1}(Q) \in W \cap U_{n+1}$. Thus, $Q \in \varphi_{n+1}^{-1}(W \cap U_{n+1})$ and so we get $W_* \subset \varphi_{n+1}^{-1}(W \cap U_{n+1})$. Conversely, if $\varphi_{n+1}(Q) \in W \cap U_{n+1}$, then, if $Q = (a_1, \ldots, a_n)$, then $(a_1, \ldots, a_n, 1) \in W$. Thus, for any $F \in I(W)$, we have $(F_*)(Q) = F(a_1, \ldots, a_n, 1) = 0$ as $(a_1, \ldots, a_n, 1) \in W$. This proves that $Q \in W_*$, that is, $\varphi_{n+1}^{-1}(W \cap U_{n+1}) \subset W_*$. This completes the proof of the claim.

Using the claim and what we proved earlier we get

$$(V^*)_* = \varphi_{n+1}^{-1}(V^* \cap U_{n+1}) = \varphi_{n+1}^{-1}(\varphi_{n+1}(V)) = V$$

as φ_{n+1} is an inclusion.

(2) If $V \subset W \subset \mathbb{A}^n$, then $I(W) \subset I(V)$. Let $P \in V^*$ and let $f \in I(W)$. We need to show that $f^*(P) = 0$. But $f^* \in I(W)^* \subset I(V)^*$, and since $P \in V^* \Rightarrow f^*(P) = 0$. This shows that $P \in V(I(W)^*) = W^*$. Thus, $V^* \subset W^*$.

Suppose $V \subset W \subset \mathbb{P}^n$, then as we observed above, $V_* = \varphi_{n+1}^{-1}(V \cap U_{n+1})$, and from this it is clear that $V_* \subset W_*$.

(3) If V is empty then $I(V) = (1)$ and so $I(V)^* = (1)^* = (1)$ and so V^* is empty. So assume $V \neq \emptyset$ and irreducible. Then $I(V)$ is prime. We claim $I(V)^*$ is prime.

First we claim that for any ideal $J \subset k[X_1, \ldots, X_n]$, we have $(J^*)_* = J$. Notice that if $f \in J$ then it is clear that $(f^*)_* \in J$. This shows that $J \subset (J^*)_*$. Conversely, a general element of J^* looks like $\sum a_i f_i^*$, where $f_i \in J$. It is clear that $(\sum a_i f_i^*)_* = \sum (a_i)_* f_i$ which is clearly in J. This proves the claim.

Using the above claim we show that $I(V)^*$ is prime. Suppose $FG \in I(V)^*$, then $(FG)_* = F_* G_* \in I(V)$. Thus, one of them is in $I(V)$, say F_*. This shows that $(F_*)^* \in I(V)^*$, which shows that $F \in I(V)^*$ as $F = X_{n+1}^l (F_*)^*$, where l is the largest power of X_{n+1} which divides F. This proves that $I(V)^*$ is prime and so V^* is irreducible.

(5) Let $W \subset \mathbb{P}^n$ be an algebraic subset which contains V. We need to show that $V^* \subset W$. It suffices to show that $I(W) \subset I(V^*)$. Let $F \in I(W)$ be a form. Then $F = X_{n+1}^l (F_*)^*$, and so it suffices to show that $(F_*)^* \in I(V^*)$. First note that it is clear that $F_* \in I(V)$ as $\varphi_{n+1}(V) \subset W$. This shows that

$$(F_*)^* \in I(V^*) \subset I(V(I(V^*))) = I(V^*)\,.$$

This proves that $I(W) \subset I(V^*)$. Thus, it follows from topology that V^* is the closure of $\varphi_{n+1}(V)$ in $\mathbb{P}^n$.

(4) Since $V = \bigcup V_i$ we get $V^* = \bigcup V_i^*$ ($\overline{A \cup B} = \overline{A} \cup \overline{B}$). That this is the decomposition into irreducible components follows from (3) and (2).

(6) Let $V \subsetneq \mathbb{A}^n$ be nonempty. Let V_i be a component of V. Since $V \subsetneq \mathbb{A}^n$, it follows that $V_i \subsetneq \mathbb{A}^n$, and we need to show that V_i^* is not contained in H_∞ and V_i^* does not contain H_∞. Clearly, V_i^* is not contained in H_∞ as it contains $\varphi_{n+1}(V_i)$ which contains points outside H_∞. If V_i^* contained H_∞, then it follows that $I(V_i^*) \subset I(H_\infty) = (X_{n+1})$. But if $0 \neq F \in I(V_i)$, which exist as $V_i \subsetneq \mathbb{A}^n$, then $F^* \in I(V_i)^* \subset I(V_i^*)$ and X_{n+1} does not divide F^* (Write F as a sum of forms, say $F = F_0 + \ldots F_d$ with $F_d \neq 0$. Note that $F^* = F_d + X_{n+1} G$, and so X_{n+1} does not divide F^*).

(7) We have already seen that if $V \subset \mathbb{P}^n$ is an algebraic set then $V_* = \varphi_{n+1}^{-1}(V \cap U_{n+1})$. Moreover, if $W \subset \mathbb{A}^n$ is an algebraic set then W^* is the closure of $\varphi_{n+1}(W)$ in $\mathbb{P}^n$. Let $V \subset \mathbb{P}^n$ be as given. Suppose $V_* = \mathbb{A}^n$, then $(V_*)^* = \overline{\varphi_{n+1}(\mathbb{A}^n)}$. We claim that $\overline{\varphi_{n+1}(\mathbb{A}^n)} = \mathbb{P}^n$. If not, then there is a nonzero form F such that F vanishes on $\varphi_{n+1}(\mathbb{A}^n)$. In other words, $F(a_1, \ldots, a_n, 1) = 0$ for all $(a_1, \ldots, a_n) \in \mathbb{A}^n$. Let us write

$$F(X_1, \ldots, X_{n+1}) = F_0(X_1, \ldots, X_n) X_{n+1}^d + F_1(X_1, \ldots, X_n) X_{n+1}^{d-1} + \ldots\,,$$

where F_i are forms of degree i. This shows that $F(a_1, \ldots, a_n, X_{n+1}) = 0$ vanishes at all nonzero values for X_{n+1}, that this, this has infinitely many solutions and so is forced to be the zero polynomial. Thus, $F_0 = F_1 = \ldots = 0$ and so $F = 0$. This shows that $\overline{\varphi_{n+1}(\mathbb{A}^n)} = \mathbb{P}^n$. Note that $(V_*)^* = \overline{V_*} \subset V$ as $V_* \subset V$ and V is closed. Since $(V_*)^* = \mathbb{P}^n$, we get $\mathbb{P}^n \subset V$. It follows that $H_\infty \subset V$. It follows that H_∞ (being irreducible) is contained in one of the irreducible components of V, which contradicts our hypothesis. Thus, $V_* \subsetneqq \mathbb{A}^n$.

Let us write $V = \bigcup V_i$ as a union of irreducible components. Each V_i satisfies: V_i is not contained in H_∞ nor does it contain H_∞. If we show that $((V_i)_*)^* = V_i$, then it follows that $(V_*)^* = V$. Thus, we may assume V is irreducible.

We have already proved that $(V_*)^* \subset V$. It suffices to show that $V \subset (V_*)^*$, or equivalently $I((V_*)^*) \subset I(V)$. Let $F \in I((V_*)^*)$. Then F vanishes on $(V_*)^*$ and so F_* vanishes on V_*. We will show that $(F_*)^* \in I(V)$, then since $F = X_{n+1}^l (F_*)^*$, it follows that $F \in I(V)$.

Thus, it suffices to show that if $G \in I(V_*)$, then $G^* \in I(V)$. Recall that V_* is the algebraic subset defined by the ideal $I(V)_*$, that is, $V_* = V(I(V)_*)$. Thus, by Nullstellensatz, we have $I(V_*) = I(V(I(V)_*)) = \mathrm{Rad}(I(V)_*)$. Now $G \in \mathrm{Rad}(I(V)_*)$ implies $G^N \in I(V)_*$. If we write $G^N = H_*$, for some $H \in I(V)$, then as $X_{n+1}^l (H_*)^* = H$, it follows that $X_{n+1}^l (G^N)^* \in I(V)$. Note that $(AB)^* = A^* B^*$, and so we get $X_{n+1}^l (G^*)^N \in I(V)$. As $I(V)$ is prime, either $X_{n+1} \in I(V)$ or $G^* \in I(V)$. As $V \not\subset H_\infty$ this shows $G^* \in I(V)$. This completes the proof of (7). □

Remark 4.3.2. Recall the Zariski topology on $\mathbb{A}^n$ from Definition 2.4.1 and the Zariski topology on $\mathbb{P}^n$ from Remark 4.2.2. Clearly, the map $\varphi_{n+1} : \mathbb{A}^n \to \mathbb{P}^n$ is a bijection onto the open subset U_{n+1}. We claim that the Zariski topology on $\mathbb{A}^n$ equals the subspace topology. For a closed subset $V \subset \mathbb{P}^n$, since $V_* = \varphi_{n+1}^{-1}(V \cap U_{n+1})$, and V_* is closed in $\mathbb{A}^n$, it follows that φ_{n+1} is continuous. Since $\varphi_{n+1}(V) = V^* \cap U_{n+1}$, it follows that φ_{n+1} is a closed map. This shows that φ_{n+1} is a homeomorphism onto its image. □

4.4 Exercises

Exercise 4.4.1. What points in $\mathbb{P}^2$ do not belong to two of the three sets U_1, U_2, U_3?

Solution. The set of points missing two of the U_i is exactly the 3 coordinate points: $\{[1:0:0], [0:1:0], [0:0:1]\}$. □

Exercise 4.4.2. Let $F \in k[X_1, \ldots, X_{n+1}]$ (k infinite). Write $F = \sum F_i$, F_i a form of degree i. Let $P \in \mathbb{P}^n(k)$, and suppose $F(x_1, \ldots, x_{n+1}) = 0$ for every choice of homogeneous

coordinates $(x_1, \ldots, x_{n+1})$ for P. Show that each $F_i(x_1, \ldots, x_{n+1}) = 0$ for all homogeneous coordinates for P. (Hint: consider $G(\lambda) = F(\lambda x_1, \ldots, \lambda x_{n+1}) = \sum \lambda^i F_i(x_1, \ldots, x_{n+1})$ for fixed $(x_1, \ldots, x_{n+1})$.

Solution. Choose one set of homogeneous coordinates $(a_1, \ldots, a_{n+1})$ for P. Given that $F(\lambda a_1, \ldots, \lambda a_{n+1}) = 0$ for all $\lambda \in k^*$. We know $F_i(\lambda a) = \lambda^i F_i(a)$. So $F(\lambda a) = \sum_{i=0}^{d} \lambda^i F_i(a) = 0 \quad \forall \lambda \in k^*$. Let $G(\lambda) = \sum_{i=0}^{d} F_i(a)\, \lambda^i$. Then $G(\lambda)$ is a polynomial in λ over k, and $G(\lambda) = 0$ for all $\lambda \in k^*$. Since k is infinite, k^* is infinite. If $G(\lambda)$ vanishes for infinitely many λ, it must be the zero polynomial in $k[\lambda]$. Thus $G(\lambda) \equiv 0$ for all λ in k.
Then $G(\lambda) = \sum_{i=0}^{d} F_i(a)\lambda^i$ is the zero polynomial. Hence each coefficient $F_i(a) = 0$ in k. So $F_i(a) = 0$ for this one choice $(a_1, \ldots, a_{n+1})$ of homogeneous coordinates for P. Thus, for all homogeneous coordinates $(b_1, \ldots, b_{n+1})$ for P, each F_i vanishes on it. □

Exercise 4.4.3. Let I be a homogeneous ideal in $k[X_1, \ldots, X_{n+1}]$. Show that I is prime if and only if the following condition is satisfied; for any forms $F, G \in k[X_1, \ldots, X_{n+1}]$, if $FG \in I$, then $F \in I$ or $G \in I$.

Solution. ($\Rightarrow$) If I is prime, then for any $F, G \in R = k[X_1, \ldots, X_{n+1}]$ (whether homogeneous or not), $FG \in I$ implies $F \in I$ or $G \in I$. So the condition on forms is automatically satisfied.
($\Leftarrow$) Assume that for all forms $F, G \in R$, $FG \in I \implies F \in I$ or $G \in I$. We want to show I is prime.

Let $f, g \in R$ be arbitrary (not necessarily homogeneous) such that $fg \in I$. We need to show $f \in I$ or $g \in I$. Let us assume that $f \notin I$ and $g \notin I$. Write $f = \sum_{i=m}^{M} f_i$ and $g = \sum_{j=n}^{N} g_j$ where f_i, g_j are forms of degree i, j respectively, and m, M, n, N are the smallest and largest degrees appearing in f and g. The product $fg = \sum_k \sum_{i+j=k} f_i g_j$. If $f_M \in I$, then we may replace f with $f - f_M$. Similarly, if $g_N \in I$ then we may replace g with $g - g_N$. Thus, we may assume that $f_M \notin I$ and $g_N \notin I$. Since $fg \in I$ and I is homogeneous, each homogeneous component of fg lies in I. In particular, the component of highest degree $M + N$ is $f_M g_N \in I$. Since f_M and g_N are forms, by our hypothesis, either $f_M \in I$ or $g_N \in I$, which is a contradiction. □

Exercise 4.4.4. If I is a homogeneous ideal, show that $\mathrm{Rad}(I)$ is also homogeneous.

Solution. Let $I \subseteq k[X_1, \ldots, X_{n+1}]$ be a homogeneous ideal. Recall $\mathrm{Rad}(I) = \{f \in k[X_1, \ldots, X_{n+1}] \mid f^m \in I \text{ for some } m \geq 1\}$. To show that $\mathrm{Rad}(I)$ is homogeneous, we need to prove that if $f \in \mathrm{Rad}(I)$, then each homogeneous component of f is also in $\mathrm{Rad}(I)$.
Let $f \in \mathrm{Rad}(I)$. Then there exists a positive integer m such that $f^m \in I$. Write

$f = f_d + f_{d+1} + \cdots + f_D$ where f_i is homogeneous of degree i, and $f_d \neq 0$, $f_D \neq 0$. Here d is the minimum degree and D is the maximum degree among the components.

Now consider f^m. The highest degree term in f^m is $(f_D)^m$, and the lowest degree term is $(f_d)^m$. Since I is homogeneous, each homogeneous component of f^m lies in I. In particular, $(f_D)^m \in I$ and $(f_d)^m \in I$. From $(f_D)^m \in I$, we get that $f_D \in \mathrm{Rad}(I)$. Similarly, from $(f_d)^m \in I$, we get $f_d \in \mathrm{Rad}(I)$.

Now consider $f - f_D$, which has maximum degree less than D. Observe that $(f - f_D)^{2m} \in I \in I$ and so $f - f_D \in \mathrm{Rad}(I)$. We can proceed by induction on the number of homogeneous components. □

Exercise 4.4.5. Show that each irreducible component of a cone is also a cone.

Solution. Let $C \subseteq \mathbb{A}^{n+1}$ be a cone. If C contains only the origin, then C is irreducible. So let us assume that C contains a point which is different from the origin. In other words, there is a nonempty projective algebraic set V such that $C = C(V)$. Recall that we had seen that if $V \neq \emptyset$ then $\mathrm{Ideal}(C(V)) = \mathrm{Ideal}(V)$. Let $V = \cup_{i=1}^{n} V_i$ be the decomposition of V into irreducible components. It is clear that $C(V) = \cup_{i=1}^{n} C(V_i)$. Since $V_i \neq \emptyset$, it follows that $\mathrm{Ideal}(C(V_i)) = \mathrm{Ideal}(V_i)$. As V_i is irreducible, we know that $\mathrm{Ideal}(V_i)$ is a homogenous prime ideal, which shows that $C(V_i)$ is also irreducible. □

Exercise 4.4.6. Let $V = \mathbb{P}^1, \Gamma_h(V) = k[X, Y]$. Let $t = X/Y \in k(V)$, and show that $k(V) = k(t)$. Show that there is a natural one-to-one correspondence between the points of $\mathbb{P}^1$ and the DVR's with quotient field $k(V)$ that contain k (see Problem 2.10.27); which DVR corresponds to the point at infinity?

Solution. Let $V = \mathbb{P}^1$, with homogeneous coordinate ring $\Gamma_h(V) = k[X, Y]$. The function field is $k(V)$. Let $t = X/Y \in k(V)$. Need to show t $k(V) = k(t)$. Define a map $\varphi : k(V) \to k(t)$ by $\varphi(f(X, Y)) = f(t, 1)$, where f is a rational function in $k(V)$. This map is well-defined because for any homogeneous representation $f = g/h$ with $g, h \in k[X, Y]$ of the same degree, $f(t, 1) = g(t, 1)/h(t, 1)$ is a rational function in t. The map φ is clearly a homomorphism of fields.

Any element of $k(t)$ can be written as $p(t)/q(t)$ where $p, q \in k[t]$. We can homogenize p and q to get polynomials $P(X, Y) = Y^{\deg p} p(X/Y)$ and $Q(X, Y) = Y^{\deg q} q(X/Y)$. Then $f = P/Q \in k(V)$ and $\varphi(f) = p(t)/q(t)$.

It is clear that φ is an inclusion. Thus φ is an isomorphism.

The second part is solved in Problem 2.10.27. □

Exercise 4.4.7. Let I be a homogeneous ideal in $k[X_1, \ldots, X_{n+1}]$, and

$$\Gamma = k[X_1, \ldots, X_{n+1}]/I.$$

Show that the forms of degree d in Γ form a finite-dimensional vector space over k.

Solution. Let $S = k[X_1, \ldots, X_{n+1}]$, and let $I \subseteq S$ be a homogeneous ideal. Define $\Gamma = S/I$. Since I is homogeneous, $\Gamma = \bigoplus_{d \geq 0} \Gamma_d$, where Γ_d is the image of the degree d homogeneous polynomials S_d under the quotient map. We need to show $\dim_k \Gamma_d < \infty$.

Let $\pi : S \to \Gamma$ be the projection. The set $\Gamma_d = \pi(S_d)$. Since S_d is a finite-dimensional vector space over k (its basis consists of all monomials of total degree d), its image under a linear map is also finite-dimensional. More formally, $\dim_k \Gamma_d \leq \dim_k S_d$. The dimension of S_d is given by the binomial coefficient:

$$\dim_k S_d = \binom{n+d}{d} = \binom{n+d}{n}.$$

Thus, $\dim_k \Gamma_d$ is bounded by this number and is therefore finite. □

Exercise 4.4.8. Let $R = k[X, Y, Z]$, $F \in R$ an irreducible form of degree n, $V = V(F) \subset \mathbb{P}^2$, and $\Gamma = \Gamma_h(V)$.

(a) Construct an exact sequence $0 \to R \xrightarrow{\psi} R \xrightarrow{\varphi} \Gamma \to 0$, where ψ is multiplication by F.
(b) Show that

$$\dim_k\{\text{forms of degree } d \text{ in } \Gamma\} = dn - \frac{n(n-3)}{2}$$

if $d > n$.

Solution. Let $R = k[X, Y, Z]$, $F \in R$ an irreducible homogeneous polynomial (form) of degree n, $V = V(F) \subset \mathbb{P}^2$, and $\Gamma = \Gamma_h(V) = R/(F)$.

(a) Consider the maps: $0 \to R \xrightarrow{\psi} R \xrightarrow{\varphi} \Gamma \to 0$, where ψ is multiplication by F, i.e., $\psi(G) = F \cdot G$, and φ is the canonical quotient map onto $R/(F)$. ψ is injective because R is a domain and $F \neq 0$, so multiplication by F has no kernel. φ is surjective by definition of a quotient ring. $\operatorname{Im} \psi = (F) = \ker \varphi$, since the kernel of the quotient map is exactly the ideal (F). The maps preserve degree up to a shift: $\psi(R_d) \subseteq R_{d+n}$.

(b) Let Γ_d be the vector space of forms of degree d in Γ. From the exact sequence in part (a), for each degree d, the multiplication by F map gives an injective map $R_d \to R_{d+n}$. When we take the quotient, we have an exact sequence of finite-dimensional vector spaces: $0 \to R_{d-n} \xrightarrow{\cdot F} R_d \to \Gamma_d \to 0$, where we interpret $R_{d-n} = 0$ if $d < n$. This sequence is exact because the original sequence is exact and the maps are homogeneous. Thus,

$$\dim_k \Gamma_d = \dim_k R_d - \dim_k R_{d-n}.$$

We know that for a polynomial ring in three variables:

$$\dim_k R_d = \binom{d+3-1}{3-1} = \binom{d+2}{2} = \frac{(d+2)(d+1)}{2}.$$

Similarly, $\dim_k R_{d-n} = \binom{(d-n)+2}{2} = \frac{(d-n+2)(d-n+1)}{2}$, provided $d \geq n$.

For $d > n$, we get

$$\begin{aligned}
\dim_k \Gamma_d &= \frac{(d+2)(d+1)}{2} - \frac{(d-n+2)(d-n+1)}{2} \\
&= \frac{1}{2}\left[(d^2+3d+2) - ((d-n)^2 + 3(d-n) + 2)\right] \\
&= \frac{1}{2}\left[d^2+3d+2 - (d^2 - 2nd + n^2 + 3d - 3n + 2)\right] \\
&= \frac{1}{2}\left[(d^2+3d+2) - (d^2 - 2nd + n^2 + 3d - 3n + 2)\right] \\
&= \frac{1}{2}\left[2nd - n^2 + 3n\right] \\
&= nd - \frac{n^2 - 3n}{2} \\
&= dn - \frac{n(n-3)}{2}.
\end{aligned}$$

□

Exercise 4.4.9. A set $V \subset \mathbb{P}^n(k)$ is called a *linear subvariety* of $\mathbb{P}^n(k)$ if $V = V(H_1, \ldots, H_r)$, where each H_i is a form of degree 1. (a) Show that if T is a projective change of coordinates, then $V^T = T^{-1}(V)$ is also a linear subvariety. (b) Show that there is a projective change of coordinates T of $\mathbb{P}^n$ such that $V^T = V(X_{m+2}, \ldots, X_{n+1})$, so V is a variety. (c) Show that the m that appears in part (b) is independent of the choice of T. It is called the *dimension* of V ($m = -1$ if $V = \emptyset$).

Solution. (a) Let $V = V(H_1, \ldots, H_r)$ where each H_i is a linear form. Let $T : \mathbb{P}^n \to \mathbb{P}^n$ be a projective change of coordinates, given by an invertible matrix $A = (a_{ij})$. If $X = (X_1, \ldots, X_{n+1})$, then T is given by $X = A\tilde{X}$ where $\tilde{X}$ are the new coordinates. The inverse image $V^T = T^{-1}(V)$ consists of points P such that $T(P) \in V$, i.e., $H_i(T(P)) = 0$ for all i. But $H_i(T(P)) = H_i(A\tilde{P})$ is a linear form in the coordinates $\tilde{P}$ because the composition of a linear form with a linear transformation is linear. Hence V^T is defined by the vanishing of r linear forms in the new coordinates, so it is a linear subvariety.

(b) Since V is linear, it is defined by r independent linear equations (after eliminating redundancies). In projective space, $r \leq n+1$. A set of r independent linear equations defines a subspace of dimension $n-r$ in the vector space k^{n+1}. By a change of basis in k^{n+1}, we can map this subspace to the subspace where the last r coordinates

are zero. More formally, let the equations be $\sum_{j=1}^{n+1} a_{ij}X_j = 0$, $i = 1, \ldots, r$. The coefficient matrix has rank r. Extend these r row vectors to a basis of k^{n+1}. Let T be the projective transformation whose matrix is the inverse of the matrix whose rows are this basis. Then in the new coordinates, the equations become $\tilde{X}_i = 0$ for $i = n + 2 - r, \ldots, n + 1$ (or some set of r coordinates). Relabeling indices, we can write $V^T = V(X_{m+2}, \ldots, X_{n+1})$ where $m = n - r$. The set V is then a variety (a linear subspace) of dimension m.

(c) The number of linearly independent forms of degree 1 required to define V is independent of the change of coordinates (as projective change of coordinates happens using a linear isomorphism). Thus, m is invariant.

□

Exercise 4.4.10. Let $H_1, \ldots, H_m$ be hyperplanes in $\mathbb{P}^n$, $m \leq n$. Show that $H_1 \cap H_2 \cap \cdots \cap H_m \neq \emptyset$.

Solution. A hyperplane in $\mathbb{P}^n$ is given by a linear equation $\sum_{i=1}^{n+1} a_i X_i = 0$. Let $H_i = V(L_i)$ where $L_i = \sum_{j=1}^{n+1} a_{ij}X_j$, $i = 1, \ldots, m$, with $m \leq n$. In the vector space k^{n+1}, each equation $L_i = 0$ defines a codimension 1 subspace (through the origin). The intersection of these subspaces in k^{n+1} has dimension at least $(n + 1) - m \geq (n + 1) - n = 1$. Since the dimension is at least 1, there exists a nonzero vector $(x_1, \ldots, x_{n+1})$ satisfying all m equations. This vector gives a point $[x_1 : \cdots : x_{n+1}] \in \mathbb{P}^n$ that lies in all H_i. Hence the intersection is nonempty. □

Exercise 4.4.11. Let $P = [a_1 : \ldots : a_{n+1}]$, $Q = [b_1 : \ldots : b_{n+1}]$ be distinct points of $\mathbb{P}^n$. The *line* L through P and Q is defined by

$$L = \{[\lambda a_1 + \mu b_1 : \ldots : \lambda a_{n+1} + \mu b_{n+1}] \mid \lambda, \mu \in k, \lambda \neq 0 \text{ or } \mu \neq 0\}.$$

Prove the projective analogue of Problem 2.10.15.

Solution. The projective analogue of Problem 2.10.15 (which states that in affine space, any two distinct points determine a unique line) is: any two distinct points P and Q in $\mathbb{P}^n$, there passes a unique projective line. Given $P = [a_1 : \cdots : a_{n+1}]$ and $Q = [b_1 : \cdots : b_{n+1}]$, the set

$$L = \{[\lambda a_1 + \mu b_1 : \cdots : \lambda a_{n+1} + \mu b_{n+1}] \mid (\lambda, \mu) \neq (0, 0)\}$$

is clearly a projective line (it is the image of $\mathbb{P}^1$ under the map $[\lambda : \mu] \mapsto [\lambda a + \mu b]$). To show uniqueness, suppose L' is any line containing P and Q. A line in $\mathbb{P}^n$ is a linear subvariety of dimension 1. It can be described as the set of points whose coordinates are linear combinations of two independent vectors. Since P and Q are two distinct points

on L', their representing vectors are linearly independent and span the 2-dimensional subspace of k^{n+1} corresponding to L'. Therefore, any point on L' is a linear combination of P and Q, i.e., of the form $[\lambda a + \mu b]$. Hence $L' = L$. □

Exercise 4.4.12. Let P_1, P_2, P_3 (resp. Q_1, Q_2, Q_3) be three points in $\mathbb{P}^2$ not lying on a line. Show that there is a projective change of coordinates $T : \mathbb{P}^2 \to \mathbb{P}^2$ such that $T(P_i) = Q_i$, $i = 1, 2, 3$. Extend this to $n + 1$ points in $\mathbb{P}^n$, not lying on a hyperplane.

Solution. Let P_1, P_2, P_3 be three non-collinear points in $\mathbb{P}^2$. Choose representative vectors $p_1, p_2, p_3 \in k^3$ such that they are linearly independent. This is possible because if they were dependent, the points would lie on a line. Similarly, choose representative vectors q_1, q_2, q_3 for Q_1, Q_2, Q_3 that are linearly independent.

Define a linear map $\tilde{T} : k^3 \to k^3$ by $\tilde{T}(p_i) = q_i$ for $i = 1, 2, 3$. Since the p_i form a basis, $\tilde{T}$ is an invertible linear transformation. It induces a projective transformation $T : \mathbb{P}^2 \to \mathbb{P}^2$ by $T([v]) = [\tilde{T}(v)]$. Then $T(P_i) = Q_i$ by construction. For $n+1$ points in $\mathbb{P}^n$ not lying on a hyperplane, choose representative vectors that form a basis of k^{n+1}. The same construction gives the required projective transformation. □

Exercise 4.4.13. Show that any two distinct lines in $\mathbb{P}^2$ intersect in one point.

Solution. Let L_1 and L_2 be two distinct lines in $\mathbb{P}^2$. A line in $\mathbb{P}^2$ is a hyperplane. By Problem 4.4.10 with $n = 2$ and $m = 2 \leq n$, the intersection $L_1 \cap L_2$ is nonempty. Since they are distinct, they cannot be the same line, so the intersection must be exactly one point. □

Exercise 4.4.14. Let L_1, L_2, L_3 (resp. M_1, M_2, M_3) be lines in $\mathbb{P}^2(k)$ that do not all pass through a point. Show that there is a projective change of coordinates: $T : \mathbb{P}^2 \to \mathbb{P}^2$ such that $T(L_i) = M_i$. (*Hint:* Let $P_i = L_j \cap L_k$, $Q_i = M_j \cap M_k$, i, j, k distinct, and apply Problem 4.4.12.) Extend this to $n + 1$ hyperplanes in $\mathbb{P}^n$, not passing through a point.

Solution. Let L_1, L_2, L_3 be lines in $\mathbb{P}^2$ not all passing through a point. Define $P_1 = L_2 \cap L_3$, $P_2 = L_1 \cap L_3$, $P_3 = L_1 \cap L_2$. Because the lines do not all pass through a point, the points P_1, P_2, P_3 are distinct. Moreover, they are not collinear (If they were, then P_1 would lie on the unique line joining P_2 and P_3, that is, L_1. But this would mean that L_1 contains P_1 and P_2, and so it equals the unique line joining these, that is, L_3). Similarly, define $Q_i = M_j \cap M_k$.

By Problem 4.4.12, there exists a projective transformation T such that $T(P_i) = Q_i$. Since a projective transformation maps lines to lines and preserves incidence, and since L_i is the line through P_j and P_k, we have $T(L_i)$ is the line through $T(P_j)$ and $T(P_k)$, which is M_i. Hence $T(L_i) = M_i$.

For $n+1$ hyperplanes $H_1, \ldots, H_{n+1}$ in $\mathbb{P}^n$ not passing through a point, their intersection points $P_i = \bigcap_{j \neq i} H_j$ are well-defined and form $n+1$ points in general position (not lying on a hyperplane). The same construction using Problem 4.4.12 extended to $n+1$ points yields a projective transformation sending the configuration of hyperplanes to any other such configuration. □

Exercise 4.4.15. Let z be a rational function on a projective variety V. Show that the pole set of z is an algebraic subset of V.

Solution. Let $V \subseteq \mathbb{P}^n$ be a projective variety, and let $z \in k(V)$ be a rational function. Let S be the set of homogeneous elements in $G \in \Gamma_h(V)$ such that $Gz \in \Gamma_h(V)$. Suppose $P \in V$ is not a pole of z. Then we may write $z = F/G$ where F, G are homogeneous elements of $\Gamma_h(V)$ of the same degree such that $G(P) \neq 0$. This shows that $P \notin V(S)$ as $G \in S$. Conversely, if $P \notin V(S)$, then there is $G \in S$ such that $G(P) \neq 0$, which shows that P is not a pole of z. Thus, the pole set is precisely $V(S)$. □

Exercise 4.4.16. Let $H = V(\sum a_i X_i)$ be a hyperplane in $\mathbb{P}^n$. Note that $(a_1, \ldots, a_{n+1})$ is determined by H up to a constant.
(a) Show that assigning $[a_1 : \ldots : a_{n+1}] \in \mathbb{P}^n$ to H sets up a natural one-to-one correspondence between hyperplanes in $\mathbb{P}^n$ and points in $\mathbb{P}^n$. If $P \in \mathbb{P}^n$, let P^* be the corresponding hyperplane; if H is a hyperplane, H^* denotes the corresponding point.
(b) Show that $P^{**} = P$, $H^{**} = H$. Show that $P \in H$ if and only if $H^* \in P^*$.
This is the well-known *duality* of the projective space.

Solution. (a) A hyperplane H in $\mathbb{P}^n$ is defined by a linear form $\sum_{i=1}^{n+1} a_i X_i = 0$. The coefficients $(a_1, \ldots, a_{n+1})$ are determined up to a nonzero scalar multiple because multiplying the equation by a nonzero constant gives the same set of points. Thus, the set of coefficients defines a point $[a_1 : \cdots : a_{n+1}] \in \mathbb{P}^n$. This assignment is bijective: given a point $P = [a] \in \mathbb{P}^n$, the corresponding hyperplane P^* is $V(\sum a_i X_i)$. This is well-defined because scaling a gives the same hyperplane.

(b) Let $P = [a_1 : \cdots : a_{n+1}]$. By definition, $P^* = V(\sum a_i X_i)$ and $P^{**} = P$. Similarly, $H^{**} = H$. Let $P = [a_1 : \ldots, a_{n+1}]$ and $H = V(\sum b_i X_i)$. Then $P \in H$ if and only if $\sum a_i b_i = 0$. But $H^* = [b_1 : \ldots : b_{n+1}]$ and $P^* = V(\sum a_i X_i)$. The condition $H^* \in P^*$ means that $\sum b_i a_i = 0$, which is exactly the same equation. Therefore, $P \in H \iff H^* \in P^*$.

□

Exercise 4.4.17. If $I = (F)$ is the ideal of an affine hypersurface, show that $I^* = (F^*)$.

Solution. – $I^* := \langle G^* \ : \ G \in I \rangle$. As $F \in I$, we have $(F^*) \subseteq I^*$. Now to show that $I^* \subseteq (F^*)$, let $H \in I^*$. Then $H = \sum \alpha_i G_i^*$, where $G_i \in I$. To show $H \in (F^*)$, it is enough to show that $G_i^* \in (F^*)$ for all i. As $G_i \in I = (F)$, we have $G_i = \beta F$, for some $\beta \in k[x_1, \ldots, x_n]$. Suppose $\deg(\beta) = c$ and $\deg(F) = d$.Then

$$\begin{aligned} G_i^* &= X_{n+1}^{c+d} G\left(\frac{X_1}{X_{n+1}}, \ldots, \frac{X_n}{X_{n+1}}\right) \\ &= X_{n+1}^{c+d} \beta\left(\frac{X_1}{X_{n+1}}, \ldots, \frac{X_n}{X_{n+1}}\right) F\left(\frac{X_1}{X_{n+1}}, \ldots, \frac{X_n}{X_{n+1}}\right) \\ &= X_{n+1}^{c} \beta\left(\frac{X_1}{X_{n+1}}, \ldots, \frac{X_n}{X_{n+1}}\right) X_{n+1}^{d} F\left(\frac{X_1}{X_{n+1}}, \ldots, \frac{X_n}{X_{n+1}}\right) \\ &= \beta^* F^*. \end{aligned}$$

So, $G_i^* \in (F^*)$ for all i and hence $H \in (F^*)$. Therefore, $I^* = (F^*)$. □

Exercise 4.4.18. Let $V = V(Y - X^2, Z - X^3) \subset \mathbb{A}^3$. Prove:

(a) $I(V) = (Y - X^2, Z - X^3)$.

(b) $ZW - XY \in I(V)^* \subset k[X, Y, Z, W]$, but $ZW - XY \notin ((Y - X^2)^*, (Z - X^3)^*)$.

So if $I(V) = (F_1, \ldots, F_r)$, it does not follow that $I(V)^* = (F_1^*, \ldots, F_r^*)$.

Solution. (a) Let $\mathfrak{a} = (Y - X^2, Z - X^3)$. By Hilbert Nullstellensatz, $I(V(\mathfrak{a})) = \mathrm{Rad}(\mathfrak{a})$ and hence it is enough to show that $\mathrm{Rad}(\mathfrak{a}) = \mathfrak{a}$. It is clear that $\mathfrak{a}$ is a prime ideal.

(b) Note that $Z - XY \in I(V)$, as

$$Z - XY = (Z - X^3) - X(Y - X^2).$$

$$(Z - XY)^* = W^2\left(\frac{Z}{W} - \frac{X}{W}\frac{Y}{W}\right) = ZW - XY.$$

Therefore, $ZW - XY = (Z - XY)^* \in I(V)^*$.

Now, we will show that $ZW - XY \notin ((Y - X^2)^*, (Z - X^3)^*)$.

$$(Y - X^2)^* = W^2\left(\frac{Y}{W} - \frac{X^2}{W^2}\right) = YW - X^2.$$

$$(Z - X^3)^* = W^3\left(\frac{Z}{W} - \frac{X^3}{W^3}\right) = ZW^2 - X^3.$$

The ideal generated by the above two is a homogeneous ideal whose degree 2 piece is the one dimensional space generated by $YW - X^2$. Thus, this ideal clearly does not contain $ZW - XY$.

□

Exercise 4.4.19. Show that if $V \subset W \subset \mathbb{P}^n$ are varieties, and V is a hypersurface, then $W = V$ or $W = \mathbb{P}^n$ (see Problem 1.11.36).

Solution. After a change of coordinates we may assume that V meets U_{n+1}. Then $V_* \subset W_*$ and by Problem 1.11.36, W_* is either V_* or all of $\mathbb{A}^n$. Thus, W is either V or all of $\mathbb{P}^n$. □

Exercise 4.4.20. Suppose V is a variety in $\mathbb{P}^n$ and $V \supset H_\infty$. Show that $V = \mathbb{P}^n$ or $V = H_\infty$. If $V = \mathbb{P}^n$, $V_* = \mathbb{A}^n$, while if $V = H_\infty$, $V_* = \emptyset$.

Solution. $H_\infty \subset V \subset \mathbb{P}^n$ and H_∞ is a hypersurface as $H_\infty = V(x_{n+1})$. By Exercise 4.4.19, we have $V = \mathbb{P}^n$ or $V = H_\infty$. The rest is clear. □

Exercise 4.4.21. Let $P = [0 : 1 : 0] \in \mathbb{P}^2(k)$. Show that the lines through P consist of the following:

(a) The "vertical" lines $L_\lambda = V(X - \lambda Z) = \{[\lambda : t : 1] \mid t \in k\} \cup \{P\}$.

(b) The line at infinity $L_\infty = V(Z) = \{[x : y : 0] \mid x, y \in k\}$.

Solution. Let $ax + by + cz = 0$ be a line in $\mathbb{P}^2$, where $(a, b, c) \neq (0, 0, 0)$. As it passes through $[0 : 1 : 0]$, we have $b = 0$. Lines in $\mathbb{P}^2$ passing through $[0 : 1 : 0]$ are of the form $ax + cz = 0$. First consider the case $a \neq 0$ Rewriting the equation $ax + cz = 0$ as $x - \lambda z = 0$, we get the line

$$L_\lambda = V(x - \lambda z).$$

When $z = 0$, we get $x = 0$ and $y \in k$. This gives us the point P. When $z = 1$, we get $x = \lambda$ and $y \in k$. This gives us the points $[\lambda : t : 1]$, $t \in k$.

Next consider the case $a = 0$. This gives the line $z = 0$. This line L_∞ has points of the form $[x : y : 0]$, $x, y \in k$. (This is nothing but the hyperplane H_∞). □

Exercise 4.4.22. Let $P = [x : y : z] \in \mathbb{P}^2$.

(a) Show that $\{(a, b, c) \in \mathbb{A}^3 \mid ax + by + cz = 0\}$ is a hyperplane in $\mathbb{A}^3$.

(b) Show that for any finite set of points in $\mathbb{P}^2$, there is a line not passing through any of them.

Solution. (a) This is obvious.

(b) Assume k is infinite. Consider points $P_i = [a_i : b_i : c_i] \in \mathbb{P}^2$, for $1 \leq i \leq n$. We need to find a line $\alpha x + \beta y + \gamma z = 0$ such that $\alpha a_i + \beta b_i + \gamma c_i \neq 0$ for all i. It is enough to show there exist α, β, and γ such that $\alpha a_i + \beta b_i + \gamma c_i \neq 0$ for all i. Suppose this is not true. Consider the polynomial

$$F = \prod_{i=1}^{n} (a_i X + b_i Y + c_i Z) \in k[X, Y, Z].$$

$F \neq 0$ as $P_i \in \mathbb{P}^2 \ \forall \ i$. As such α, β, γ do not exist, we have $V(F) = \mathbb{P}^n$. This is not possible as $F \neq 0$. Therefore, we can find a line not passing through any of the given points.

□

Chapter 5

Projective Plane Curves

Let $F(X,Y,Z) \in k[X,Y,Z]$ be a form of degree d. We are interested in $V(F) \subset \mathbb{P}^2$; however, as in the previous chapters, we also keep track of multiplicities of multiple components. Given any point $P \in \mathbb{P}^2$, after a linear change of coordinates we may assume that $P = (0:0:1)$. Then we may define the local properties of F at P, by viewing P as a point in $\mathbb{A}^2$ and by considering the curve in $\mathbb{A}^2$ defined by F_*. We had defined the local ring of a projective algebraic subset at P, see Remark 4.2.3, and we easily check that $\mathcal{O}_P(F)$ is the same as $\mathcal{O}_P(F_*)$. We also define multiplicity, tangent lines at P by passing to $\mathbb{A}^2$. If F is irreducible and P is a simple point of F, then $\mathcal{O}_P(F)$ is a DVR.

5.1 Intersection Multiplicity in $\mathbb{P}^2$

Let F, G be projective plane curves and let $P \in \mathbb{P}^2$ be a point. We define the intersection multiplicity $I(P, F \cap G) = \dim_k(\mathcal{O}_P(\mathbb{P}^2)/(F_*, G_*))$. This satisfies all properties of the intersection multiplicity defined in the affine case, except that,

(i) in property (3) we need to take a linear automorphism $T : \mathbb{P}^2 \to \mathbb{P}^2$ (that is, one which arises from a linear isomorphism $\mathbb{A}^3 \to \mathbb{A}^3$)

(ii) in property (7) $I(P, F \cap G) = I(P, F \cap (G + AF))$ holds only for homogeneous A such that $\deg(A) = \deg(G) - \deg(F)$.

Assume that we are in the affine situation and $P = (0,0) \in \mathbb{A}^2$ and let $F \in k[X,Y]$ be a polynomial such that $F(P) = 0$. Recall that we had defined the tangent lines at P to F to be the linear factors of F_m, where $m = m_P(F)$. Let L be any line. After a linear change of coordinates we may assume $L = X$. Let $\bar{F} = F(0,Y)$ and write

$\bar{F} = Y^k +$ higher order terms. Note that $k \geqslant m$ and $k > m$ iff X divides F_m. Further note that

$$\dim(\mathcal{O}_P(\mathbb{A}^2)/(F, X)) \cong \dim(\mathcal{O}_P(\mathbb{A}^1)/(Y^k)) = k\,.$$

Thus, $I(P, F \cap L) = m$ iff $k = m$ iff $X \nmid F_m$. Thus, for any line L, we say it is tangent at P if $I(P, F \cap L) > m_P(F)$. A point P is an **ordinary multiple point** of F if F has $m_P(F)$ distinct tangent lines at P.

5.2 Linear System of Curves

Recall that the space of forms of degree d in three variables is a vector space of dimension $\frac{1}{2}(d+1)(d+2)$. Let us denote this vector space by S_d. Let us fix a basis of monomials $M_1, M_2, \ldots, M_N$. A curve of degree d, up to scalars, is given by an equation $\sum a_i M_i = 0$. Thus, a curve is represented uniquely by a line in the vector space of forms, that is, by a point in $\mathbb{P}(S_d) \cong \mathbb{P}^{N-1}$, where $N - 1 = \frac{1}{2}(d+1)(d+2) - 1 = \frac{1}{2}d(d+3)$.

Lemma 5.2.1. *1. Let $P \in \mathbb{P}^2$ be a point. The set of curves passing through P is a hyperplane in $\mathbb{P}^{N-1}$.*

2. If $T : \mathbb{P}^2 \to \mathbb{P}^2$ is a projective change of coordinates (that is, induced by a linear map $\mathbb{A}^3 \to \mathbb{A}^3$) then this induces a projective change of coordinates on $\mathbb{P}^{N-1}$.

Proof. (1) is clear. For (2), consider a linear isomorphism $T : S_1 \to S_1$,

$$\begin{aligned} T(X) &= \alpha_1 X' + \beta_1 Y' + \gamma_1 Z'\,, \\ T(Y) &= \alpha_2 X' + \beta_2 Y' + \gamma_2 Z'\,, \\ T(Z) &= \alpha_3 X' + \beta_3 Y' + \gamma_3 Z'\,. \end{aligned}$$

This linear isomorphism gives rise to a linear map

$$\tilde{T} : S_d \to S_d\,,$$

which we may define on the monomials as

$$M(X, Y, Z) \mapsto M(T(X), T(Y), T(Z))\,.$$

The coefficients of the monomials $M(T(X), T(Y), T(Z))$ are linear in the a_i's, and polynomial in $\alpha_j, \beta_j, \gamma_j$. Note that the map $\tilde{T}$ is an isomorphism, as $\widetilde{T^{-1}}\tilde{T} = Id$. Thus, we see that we get an isomorphism $\mathbb{P}^{N-1} \to \mathbb{P}^{N-1}$. Note that it is important that the map T should be an isomorphism. For example, if $T(X) = X, T(Y) = Y$ and $T(Z) = 0$, then any monomial which is a multiple of Z would map to 0 and this will no more give a point in $\mathbb{P}^{N-1}$. □

Corollary 5.2.2. *Let $Q_1, \ldots, Q_n \in \mathbb{P}^2$ be any set of points in $\mathbb{P}^2$. There exists a curve of degree d passing through these points if $n \leqslant \frac{1}{2}d(d+3)$.*

Proof. Let $Q = (a : b : c) \in \mathbb{P}^2$ be a point. Let F be a form of degree d. The condition that F passes through Q is equivalent to the condition that the coefficients of F satisfy a certain linear equation determined by Q. Thus, if $p_F \in \mathbb{P}(S_d)$ is the point corresponding to the line through F, then F contains Q iff p_F lies on the hyperplane H_Q.

Thus, passing through $Q_1, \ldots, Q_{N-1}$ points is equivalent to lying on $H_{Q_1} \cap \cdots \cap H_{Q_{N-1}}$. The intersection of $N-1$ hyperplanes in $\mathbb{P}^{N-1}$ is never empty. If the hyperplanes are in general position, then this intersection is exactly one point. Thus, if the points are in "general position", then there is exactly one curve through them. □

Let $V(d; r_1P_1 + \cdots + r_nP_n) = \{\text{curves } F \subset \mathbb{P}^2 \text{ of deg } d \mid m_{P_i}(F) \geqslant r_i,\ 1 \leqslant i \leqslant n\}$.

Theorem 5.2.3. *Fix an integer $n > 0$ and n points in $\mathbb{P}^2$, $P_1, \ldots, P_n$. Let $r_1, \ldots, r_n$ be nonnegative integers.*

1. *$V(d; r_1P_1 + \cdots + r_nP_n)$ is a linear subvariety and*

$$\dim V(d; r_1P_1 + \cdots + r_nP_n) \geqslant \frac{d(d+3)}{2} - \sum_{i=1}^{n} \frac{r_i(r_i+1)}{2}.$$

2. *If $d \geqslant (\sum_{i=1}^{n} r_i) - 1$ then*

$$\dim V(d; r_1P_1 + \cdots + r_nP_n) = \frac{d(d+3)}{2} - \sum_{i=1}^{n} \frac{r_i(r_i+1)}{2}.$$

Proof. (1) Let $P = (0 : 0 : 1)$. Let us check that the condition $m_P(F) \geqslant r$ imposes $\frac{r(r+1)}{2}$ linear conditions on the space of curves. Write

$$F(X, Y, Z) = F_0(X, Y)Z^d + F_1(X, Y)Z^{d-1} + \cdots + F_d(X, Y)$$

where F_i is a form of degree i. Restricting to $\mathbb{A}^2$, this gives the function

$$F(X, Y, 1) = F_0(X, Y) + F_1(X, Y) + \cdots + F_d(X, Y).$$

We want this function to satisfy $F_i = 0$ for $i < r$. This imposes $1 + 2 + \cdots + r = \frac{r(r+1)}{2}$ linear conditions on the coefficients in F. Thus, doing this for all points $P_1, \ldots, P_n$ we get that the

$$\dim V(d; r_1P_1 + \cdots + r_nP_n) \geqslant \frac{d(d+3)}{2} - \sum_{i=1}^{n} \frac{r_i(r_i+1)}{2}.$$

(2) Suppose $d = 1$. The given condition implies $\sum r_i \leqslant d + 1 = 2$. This implies one of the following three holds:

- All the $r_i = 0$. In this case the assertion is trivially true.
- Exactly one of the r_i equals one and all the other are 0. In this case too the assertion is trivially true.
- Exactly two of the r_i equal 1, which we may assume to be $r_1 = r_2 = 1$, and the remaining r_i equal 0. Through any two points there is exactly one line, and both these points are simple points of this line. Thus, $\dim V(d; \sum_{i=1}^n r_i P_i) = 0$ and also $0 = \frac{1(1+3)}{2} - 2$.

This proves equality when $d = 1$.

Next assume $d > 1$ and $(\sum_{i=1}^n r_i) - 1 = 1$. Then $\sum r_i = 2$ and again we have $r_1 = r_2 = 1$. Clearly, passing through two distinct points imposes two distinct conditions on the coefficients of F. Thus, $\dim V = \frac{d(d+3)}{2} - 2$, which equals the given formula.

So we may assume that $m = (\sum_{i=1}^n r_i) - 1 > 1$ and $d > 1$.

Case 1: Each $r_i = 1$. The hypothesis implies that $d + 1 \geqslant \sum r_i = n$. Let $V_i = V(d; P_1 + \cdots + P_i)$ and $V_0 = \mathbb{P}^{\frac{d(d+3)}{2}}$. We know from the first part of the Theorem that $\dim V_i \geqslant \frac{d(d+3)}{2} - i$ and $\dim V_n \geqslant \frac{d(d+3)}{2} - n$. Moreover,

$$V_0 = V_1 \supset V_2 \supset \cdots \supset V_n \,.$$

Since $\dim V_0 = \frac{d(d+3)}{2}$, if we show that $V_i \subsetneq V_{i-1}$, then this will show that $\dim V_i = \frac{d(d+3)}{2} - i$, which will prove the Theorem in this case.

Choose a line L_i such that $L_i \cap \{P_1, \ldots, P_n\} = P_i$. Let L_0 be a line such that $L_0 \cap \{P_1, \ldots, P_n\} = \emptyset$. Then $F = L_i \ldots L_1 \ldots L_{i-1} L_0^{d-i+1} \in V_{i-1} \setminus V_i$. Note that for F to be a polynomial, we need that $d - i + 1 \geqslant 0$. This is true as $d - i + 1 \geqslant d - n + 1 \geqslant 0$ by assumption.

Case 2: Fix a tuple $(d, r_1, r_2, \ldots, r_n)$ with $d \geqslant (\sum r_i) - 1$. Let us assume that (2) has been proved for all tuples $(d', r_1', r_2', \ldots, r_n')$ satisfying either one of the following two conditions

- $1 \leqslant d' < d$ and $d' \geqslant (\sum r_i') - 1$
- $d' = d$ and $\sum r_i' < \sum r_i$.

Note that for any $d' \geqslant 1$ we have already proved that if all the r_i' satisfy $0 \leqslant r_i' \leqslant 1$ and $d' \geqslant (\sum r_i') - 1$, then (2) is true. Consider $V(d; r_1 P_1 + r_2 P_2 + \cdots + r_n P_n)$. If all the $r_i \leqslant 1$, then we are done by the previous case. So we may assume some $r_i > 1$, say $r_1 > 1$. Further, we may assume that $P = P_1 = [0 : 0 : 1]$. Let

$$V_0 = V(d; (r_1 - 1)P_1 + r_2 P_2 + \cdots + r_n P_n) \,.$$

Let $F \in V_0$ and write

$$F_* = G_{r_1-1} + G_{r_1} + G_{r_1+1} + \dots .$$

Further, write

$$G_{r_1-1} = \sum_{j=0}^{r_1-1} a_j X^j Y^{r_1-1-j} .$$

Let

$$V_i = \{F \in V_0 \mid a_j = 0 \text{ for } j < i\} .$$

Then

$$V_0 \supset V_1 \supset \cdots \supset V_{r_1} = V(d; r_1P_1 + \cdots + r_nP_n) .$$

Since $(r_1 - 1) + \sum_{i=2}^{n} r_i =< \sum r_i$, it follows by our hypothesis that

$$\dim V_0 = \frac{d(d+3)}{2} - \frac{r_1(r_1-1)}{2} - \sum_{i=2}^{n} \frac{r_i(r_i+1)}{2} .$$

So if we show that $V_i \subsetneqq V_{i-1}$, then

$$\dim V_{r_1} \leqslant \dim V_0 - r_1 = \frac{d(d+3)}{2} - \sum_{i=1}^{n} \frac{r_i(r_i+1)}{2} .$$

By the first part of the Theorem, as

$$\dim V_{r_1} \geqslant \frac{d(d+3)}{2} - \sum_{i=1}^{n} \frac{r_i(r_i+1)}{2} ,$$

we get equality. Thus, it suffices to show that $V_i \subsetneqq V_{i-1}$.

Let

$$W_0 = V(d-1; (r_1-2)P_1 + r_2P_2 + \cdots + r_nP_n) .$$

For $F \in W_0$, write

$$F_* = G_{r_1-2} + G_{r_1-1} + \dots .$$

Write

$$G_{r_1-2} = \sum_{i=0}^{r_1-2} a_i X^i Y^{r_1-2-i} .$$

Define

$$W_i = \{F \in W_0 \mid a_j = 0 \text{ for } j < i\} .$$

Then

$$W_0 \supset W_1 \supset \cdots \supset W_{r_1-1} = V(d-1; (r_1-1)P_1 + r_2P_2 + \cdots + r_nP_n)\,.$$

By our hypothesis, we have that

$$\dim(W_0) - \dim(W_{r_1-1}) = r_1 - 1\,.$$

Each W_i is a linear subspace and it is clear that $\dim(W_i) - \dim(W_{i+1}) \in \{0, 1\}$. Since the dimension can at most drop by 1, it follows that it has to drop by 1. Thus, for $0 \leqslant i \leqslant r_1 - 2$, we see that $W_i \subsetneqq W_{i+1}$. Let $F_i \in W_i \setminus W_{i+1}$. Then

$$(F_i)_* = \sum_{j=i}^{r_1-2} a_j X^j Y^{r_1-2-j} + \text{higher order terms}\,,$$

where $a_i \neq 0$. This shows that

$$(YF_i)_* = \sum_{j=i}^{r_1-2} a_j X^j Y^{r_1-1-j} + \text{higher order terms}\,,$$

with $a_i \neq 0$. Thus, $YF_i \in V_i \setminus V_{i+1}$ for $i = 0, 1, \ldots, r_1 - 2$.

Further note

$$(F_{r_1-2})_* = a_{r_1-2}X^{r_1-2} + \text{higher order terms}\,,$$

where $a_{r_1-2} \neq 0$. Then

$$(XF_{r_1-2})_* = a_{r_1-2}X^{r_1-1} + \text{higher order terms}\,.$$

This shows $XF_{r_1-2} \in V_{r_1-1} \setminus V_{r_1}$. This proves that $V_i \supsetneqq V_{i+1}$ and so completes the proof of (2). □

Theorem 5.2.4 (Bezout's Theorem)**.** *Let F and G be projective plane curves of degree m and n. Assume they have no common components. Then*

$$\sum_P I(P, F \cap G) = mn.$$

Proof. Since F and G have no common components, after a projective change of coordinates, we may assume that none of the points of $F \cap G$ lie on the line $Z = 0$. Then we have already seen that

$$\sum I(P, F \cap G) = \sum I(P, F_* \cap G_*) = \dim_k \left(\frac{k[X, Y]}{(F_*, G_*)} \right)$$

Let $\Gamma_* = k[X,Y]/(F_*, G_*)$ and $\Gamma = k[X,Y,Z]/(F,G)$ and $R = k[X,Y,Z]$. Let Γ_d and R_d be the vector spaces of forms of degree d in Γ and R. Suppose we can find $d \gg 0$ such that $\dim \Gamma_d = mn$ and we can also show that $\dim \Gamma_* = \dim \Gamma_d$, then we would be done.
Step 1: In this step we will prove that $\dim \Gamma_d = mn$ for all $d \geqslant m+n$. Let $\pi : R \to \Gamma$ be the natural map. Let $\psi : R \times R \to R$ be the map $\psi(A,B) = AF + BG$. Let $\phi : R \to R \times R$ be $\phi(C) = (-GC, FC)$. We claim that there is an exact sequence:

$$0 \to R \xrightarrow{\phi} R \times R \xrightarrow{\psi} R \xrightarrow{\pi} \Gamma \to 0$$

This follows easily as F and G have no common factors. We could have defined the same maps on the space of forms of various degrees to get an exact sequence:

$$0 \to R_{d-m-n} \xrightarrow{\phi} R_{d-n} \times R_{d-m} \xrightarrow{\psi} R_d \xrightarrow{\pi} \Gamma_d \to 0$$

Since $\dim R_d = (d+1)(d+2)/2$, it follows that

$$\dim(\Gamma_d) = \dim(R_d) - \dim(R_{d-n}) - \dim(R_{d-m}) + \dim(R_{d-m-n}) = mn$$

for $d \geqslant m+n$.
Step 2: Consider the map $\alpha : \Gamma \to \Gamma$ given by $\alpha(\bar{H}) = \bar{Z}\bar{H}$. We claim that this map is injective. Suppose $\bar{Z}\bar{H} = 0$, then $ZH \in (F,G)$. We claim that the polynomials $F(X,Y,0)$ and $G(X,Y,0)$ have no common factors in $k[X,Y]$. If not, then since both are homogeneous, a common factor would be homogeneous. Since every homogeneous polynomial in $k[X,Y]$ factors as a product of linear forms, it follows that there is a linear form $aX + bY$ which divides both $F(X,Y,0)$ and $G(X,Y,0)$. But this would mean that the point $(b : -a : 0) \in V(F,G) \cap V(Z)$, which we had assumed to be empty. This shows that $F(X,Y,0)$ and $G(X,Y,0)$ have no common factor.

If $ZH = AF + BG$, then putting $Z = 0$, we get

$$A(X,Y,0)F(X,Y,0) + B(X,Y,0)G(X,Y,0) = 0\,.$$

Since $F(X,Y,0)$ and $G(X,Y,0)$ have no common factor, $A(X,Y,0) = CG(X,Y,0)$ and $B(X,Y,0) = -CF(X,Y,0)$ for some $C \in k[X,Y]$. Then

$$ZH = AF + BG = (A - CG)F + (B + CF)G.$$

Since Z divides $A - CG$ and $B + CF$, we get $H = A'F + B'G$, which shows that $\bar{H} = 0$. This proves that α is an inclusion.
Step 3: It is clear that $\alpha(\Gamma_d) \subset \Gamma_{d+1}$. However, we noted that $\dim(\Gamma_d) = mn$ for all $d \geqslant m+n$. Since α is injective, this shows that $\alpha : \Gamma_d \xrightarrow{\sim} \Gamma_{d+1}$ are isomorphisms for $d \geqslant m+n$.

Let $A_1, \ldots, A_{mn} \in R_{m+n}$ be such that their images in Γ_{m+n} is a basis for Γ_{m+n}. Then $Z^r A_1, \ldots, Z^r A_{mn}$ is a basis for Γ_{m+n+r}. Let a_i be the image of A_i in Γ_*. We will next show that a_i forms a basis for Γ_*. This will show $\dim(\Gamma_*) = mn$.

First we show that a_i generate Γ_*. Let $h \in \Gamma_*$ and choose $H \in k[X,Y]$ such that $\bar{H} = h$. Then $H^* \in k[X,Y,Z]$ is a form. Consider the form $G := Z^{m+n}H^*$. This has degree $m+n+r$ and is such that the image of G_* (which is an element of $k[X,Y]$) in Γ_* equals h. We may consider the image of G in Γ_{m+n+r} and use the above basis to write $\bar{G} = \sum \lambda_i Z^r \bar{A}_i$. This means we get $G = \sum \lambda_i Z^r A_i + BF + CG$, for $\lambda_i \in k$ and $B, C \in k[X,Y,Z]$. Putting $Z = 1$ and taking image in Γ_* we get $h = \sum \lambda_i a_i$. This proves that a_i generate Γ_* as a k-vector space.

Next we prove linear independence of a_i. Suppose $\sum \lambda_i a_i = 0$, then this means that

$$\sum \lambda_i (A_i)_* = BF_* + CG_*$$

for $B, C \in k[X,Y]$. Recall from Proposition 2.6.2 that for a form H we have $H = Z^l (H_*)^*$, where l is the largest power of Z which divides H. Writing the above equation as

$$\sum \lambda_i A_i \left(\frac{X}{Z}, \frac{Y}{Z}, 1\right) = BF\left(\frac{X}{Z}, \frac{Y}{Z}, 1\right) + CG\left(\frac{X}{Z}, \frac{Y}{Z}, 1\right)$$

and mutliplying both sides by a sufficiently large power of Z, we get

$$\sum \lambda_i Z^{r_i} A_i = Z^s BF + Z^t CG$$

for some r_i, s, t. This equality holds in R. Let us assume that one of the λ_i is nonzero. The degree of $Z^{r_i} A_i$ equals $r_i + m + n$. Let $r = r_i$. Collecting together polynomials of degree $r + m + n$ on both sides of the equation shows that there is a relation

$$\sum \lambda_i Z^r A_i = B'F + C'G\,.$$

But this shows there is a non-trivial relation $\sum \lambda_i Z^r \bar{A}_i = 0$ in Γ_{r+m+n}, which contradicts the fact that these were linearly independent. This completes the proof of the Theorem. □

Corollary 5.2.5. *If F and G have no common components then $\sum_P m_P(F) m_P(G) \leqslant mn$.*

Proof. As $m_P(F) m_P(G) \leqslant I(P, F \cap G)$, this follows from the Theorem. □

Corollary 5.2.6. *If F and G meet in mn distinct points then each point of intersection is a simple point of F and G.*

Corollary 5.2.7. *If F and G have more than mn points in their intersection, then they have a component in common.*

5.3 Multiple Points

Proposition 5.3.1. *Let F be an irreducible curve of degree n. Then*

$$\sum_P m_P(F)(m_P(F)-1) \leqslant n(n-1)\,.$$

Proof. By Euler's formula, it is clear that one of F_X, F_Y or F_Z is nonzero. Let us assume that $F_X \neq 0$. Thus, it follows that $V(F, F_X)$ is a finite set, from which it follows that the set of points on F which are not simple is a finite set. After a change of coordinates we may assume that none of these points are in $V(Z)$.

Since $F_X \neq 0$, it is a homogeneous polynomial of deg $n-1$. Let G denote F_X. If P is a point on F which is not simple, then it is in the affine open set $\{Z \neq 0\}$, and we may compute the multiplicity by restricting to this open subset. Note that $G_* = \frac{\partial}{\partial X}(F_*)$. It follows easily that $m_P(G) \geqslant m_P(F) - 1$. From Bezout's Theorem it follows that

$$\sum m_P(F)(m_P(F)-1) \leqslant \sum m_P(F)m_P(G) \leqslant n(n-1).$$

□

We may improve the above result to the following.

Theorem 5.3.2. *Let F be an irreducible plane curve. Then*

$$\sum \frac{m_P(F)(m_P(F)-1)}{2} \leqslant \frac{(n-1)(n-2)}{2}\,.$$

Proof. The space of curves of degree $n-1$ has dimension $\frac{(n-1)(n+2)}{2}$. Let $P_1, \ldots, P_k$ be the points of F with multiplicity > 1. The dimension of the space of curves of deg $n-1$ with multiplicity $\geqslant m_{P_i}(F) - 1$ at the point P_i is at least

$$\begin{aligned}\frac{(n-1)(n+2)}{2} - \sum \frac{m_{P_i}(F)(m_{P_i}(F)-1)}{2} \\ = \frac{(n-1)n}{2} - \sum \frac{m_{P_i}(F)(m_{P_i}(F)-1)}{2} + (n-1) \geqslant 0\end{aligned}$$

Let

$$r := \frac{(n-1)(n+2)}{2} - \sum \frac{m_{P_i}(F)(m_{P_i}(F)-1)}{2}\,.$$

We have just proved that $r \geqslant 0$. Choose r simple points on F, say $Q_1, Q_2, \ldots, Q_r$. Then the dimension of the space of curves of degree $n-1$, passing through P_i with multiplicity $\geqslant m_{P_i}(F) - 1$ and passing through Q_i with multiplicity $\geqslant 1$ is at least

$$\frac{(n-1)(n+2)}{2} - \sum \frac{m_{P_i}(F)(m_{P_i}(F)-1)}{2} - \sum_{j=1}^{r} 1 = 0\,.$$

Thus, there is at least one curve G of degree $n-1$ such that $m_{P_i}(G) \geqslant m_{P_i}(F) - 1$ and $m_{Q_j}(G) \geqslant 1$. Then

$$\begin{aligned} n(n-1) = \sum m_P(G) m_P(F) &\geqslant \sum m_{P_i}(F)(m_{P_i}(F)-1) + \sum m_{Q_j}(G) \\ &= \sum m_{P_i}(F)(m_{P_i}(F)-1) + r \end{aligned}$$

It follows that $n(n-1) - r \geqslant \sum m_{P_i}(F)(m_{P_i}(F)-1)$. Substituting for r we get

$$\frac{(n-1)(n-2)}{2} = n(n-1) - \frac{(n-1)(n+2)}{2} \geqslant \sum \frac{m_{P_i}(F)(m_{P_i}(F)-1)}{2}\,.$$

This completes the proof of the Theorem. □

5.4 Max Noether's Fundamental Theorem

Consider the free abelian group on points of $\mathbb{P}^2$, that is,

$$\bigoplus_{P \in \mathbb{P}^2} \mathbb{Z}[P]\,.$$

This is called the group of zero cycles. Thus, a typical element of this group is $\sum a_P[P]$, where all but finitely many a_P are zero. The degree of a zero cycle is defined as

$$\deg(\sum a_P[P]) = \sum a_P\,.$$

We say that $\sum n_P[P] \geqslant \sum m_P[P]$ if $n_P \geqslant m_P$ for all P.

Let F, G be projective plane curves with no common component. Define a zero cycle

$$F \cdot G = \sum_{P \in \mathbb{P}^2} I(P, F \cap G)[P].$$

Consider the following question: let F, G and H be curves and suppose that H and F have no common factor and H and G have no common factor. Assume that $H \cdot F \geqslant G \cdot F$. Does there exist a curve B, with no common factor with F, such that $B \cdot F = H \cdot F - G \cdot F$? If such a curve exists then clearly $\deg(B) = \deg(H) - \deg(G)$.

Suppose we can find forms A and B such that $H = AF + BG$. Note that since H and F have no common factor, it follows that B and F have no common factor. Thus,

$$\begin{aligned} H \cdot F &= \sum_P I(P, F \cap (BG + AF))[P] = \sum_P I(P, F \cap BG)[P] \\ &= \sum_P (I(P, F \cap B) + I(P, F \cap G))[P] = B \cdot F + G \cdot F \end{aligned}$$

Definition 5.4.1. *Let $P \in \mathbb{P}^2$ and let F and G be curves through P, which have no common component through P. Let H be another curve. We say that Noether's conditions are satisfied at P, with respect to F, G and H, if $H_* \in (F_*, G_*) \subset \mathcal{O}_P(\mathbb{P}^2)$.*

Max Noether's fundamental theorem is the following.

Theorem 5.4.2 (Max Noether)**.** *Let F, G and H be projective plane curves. Assume F and G have no common components. Then there is an equation $H = AF + BG$, with A and B forms, iff Noether's conditions are satisfied at every $P \in F \cap G$.*

Proof. If $H = AF + BG$, then $H_* = A_*F_* + B_*G_* \in (F_*, G_*)$ and so this happens for all $P \in F \cap G$. Conversely, after a change of coordinates, we may assume that $V(F, G, Z) = \phi$. Since Noether's conditions are satisfied, it follows that $H_* = 0$ in $\mathcal{O}_P(\mathbb{P}^2)/(F_*, G_*)$ for every $P \in F \cap G$. Recall that we had proved that

$$k[X, Y]/(F_*, G_*) \cong \prod_{P \in F \cap G} \mathcal{O}_P(\mathbb{P}^2)/(F_*, G_*)\,.$$

Thus, it follows that $H_* \in (F_*, G_*)$ in $k[X, Y]$. Thus, there $a, b \in k[X, Y]$ such that $H_* = aF_* + bG_*$. This proves that $Z^r H = AF + BG$ for some forms A, B.

However, recall that we saw in the proof of Bezout's Theorem (5.2.4) that multiplication by Z is an injective map on $k[X, Y, Z]/(F, G)$. This proves that $H \in (F, G)$. Since H, F and G are homogeneous, it follows $\exists$ A, B homogeneous such that $H = AF + BG$. This completes the proof of the Theorem. □

Proposition 5.4.3. *Let F, G and H be plane curves. Assume F and G have no common components. Let $P \in F \cap G$. Then Noether's conditions are satisfied at P (with respect to F, G, H) if any one of the following is true:*

(1) F and G meet transversally at P and $P \in H$

(2) P is a simple point on F and $I(P, H \cap F) \geqslant I(P, G \cap F)$

(3) F and G have distinct tangents at P, and $m_P(H) \geqslant m_P(F) + m_P(G) - 1$.

Proof. (3) follows from Lemma 3.3.3 (a). If P is a simple point on F then $\mathcal{O}_P(F)$ is a DVR and recall that $I(P, G \cap F)$ equals the order of $\bar{G}$ in this DVR. Thus, if $I(P, H \cap F) = \text{ord}(\bar{H}) \geqslant \text{ord}(\bar{G})$ then it follows that $\bar{H} \in (\bar{G})$ in $\mathcal{O}_P(F)$ and so $H_* \in (F_*, G_*)$ in $\mathcal{O}_P(\mathbb{P}^2)$. (1) follows from (2) as P is a simple point of both F and G. □

Corollary 5.4.4. *Assume that all the points of $F \cap G$ are simple points of F, and $H \cdot F \geqslant G \cdot F$. Then there is a curve B such that $B \cdot F = H \cdot F - G \cdot F$.*

Proof. The Corollary follows from the previous Proposition. □

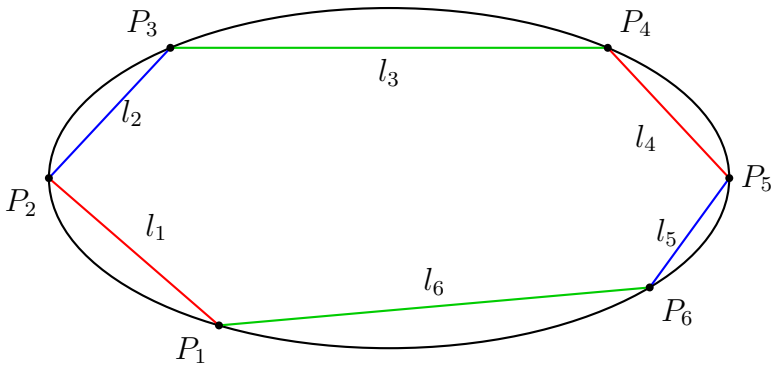
5.5 Applications of Noether's Theorem

Proposition 5.5.1. *Let C and C' be cubics (curves of degree 3) and let $C \cdot C' = \sum_{i=1}^{9} P_i$. Let Q be a quadric (curve of degree 2) and suppose $Q \cdot C = \sum_{i=1}^{6} P_i$. Then P_7, P_8 and P_9 lie on a straight line.*

Proof. Since we assume C and C' meet in 9 distinct points, it follows that the P_i are simple points of both C and C'. Take $F = C, G = Q$ and $H = C'$. Then Corollary 5.4.4 says that there is a line B such that $B \cdot F = P_7 + P_8 + P_9$. □

Corollary 5.5.2 (Pascal)**.** *Let Q be a nonsingular plane curve of degree 2. If a hexagon is inscribed in Q, then the opposite sides meet in collinear points.*

Proof. Consider the following diagram.



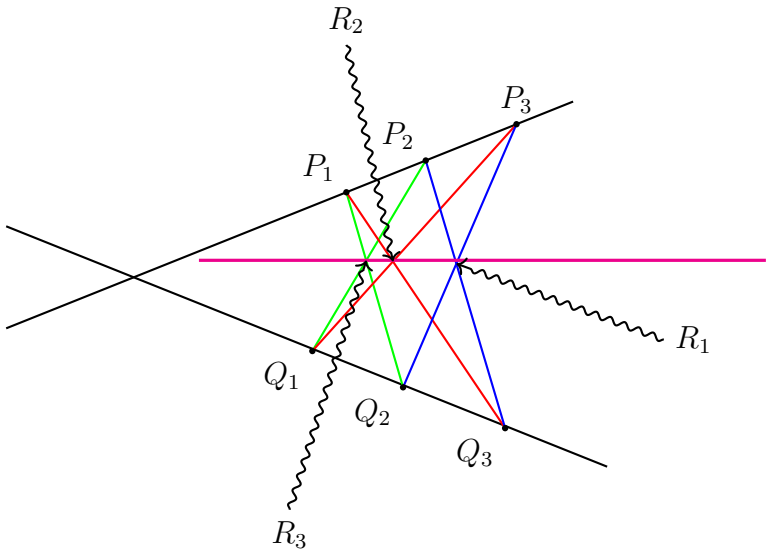
Let C be the cubic obtained as the product $l_1 l_3 l_5$. Let C' be the cubic obtained as the product $l_2 l_4 l_6$. Let $l_1 \cap l_4 = P_7$, $l_2 \cap l_5 = P_8$ and $l_3 \cap l_6 = P_9$. Then

$$C \cdot C' = \sum V(l_i, l_j) = P_1 + \cdots + P_6 + P_7 + P_8 + P_9 = Q \cdot C + P_7 + P_8 + P_9 \,.$$

It follows that P_7, P_8, P_9 are on a line. □

Corollary 5.5.3 (Pappus)**.** *Let L_1, L_2 be two lines. $P_1, P_2, P_3 \in L_1$ and $Q_1, Q_2, Q_3 \in L_2$ (none of these points equals $L_1 \cap L_2$). Let L_{ij} be the line joining P_i and Q_j for $i \neq j$. Let $R_1 = L_{23} \cdot L_{32}$, $R_2 = L_{13} \cdot L_{31}$ and $R_3 = L_{12} \cdot L_{21}$. Then R_1, R_2 and R_3 are collinear.*

Proof. Let $Q = L_1 L_2$.



Let $C = (P_1Q_2)(P_2Q_3)(P_3Q_1)$ and $C' = (P_2Q_1)(P_3Q_2)(P_1Q_3)$. Then

$$C \cdot C' = R_3 + Q_2 + P_1 + P_2 + R_1 + Q_3 + Q_1 + P_3 + R_2.$$

$Q \cdot C = P_1 + P_2 + P_3 + Q_1 + Q_2 + Q_3$. Thus, R_1, R_2 and R_3 are collinear. □

Proposition 5.5.4. *Let C be an irreducible cubic and C', C'' be two cubics. Suppose $C' \cdot C = \sum_{i=1}^{9} P_i$, where P_i are simple points on C (not necessarily distinct). Suppose $C'' \cdot C = \sum_{i=1}^{8} P_i + P'$. Then $P' = P_9$.*

Proof. Let L be a general line which passes through P_9. Then L meets C in distinct points P_9, R, S. Thus,

$$(LC'') \cdot C = \sum_{i=1}^{8} P_i + P' + P_9 + R + S = (C' \cdot C) + P' + R + S\,.$$

It follows that there is a line L' such that $L' \cdot C = P' + R + S$. But there is a unique line through R and S, which is forced to be L. This shows $P' = P_9$. □

5.5.5 **Addition on a cubic**. Let C be a non-singular cubic. Recall that this means that every point on C is a simple point. For any two points $P, Q \in C$, there is a unique line through P and Q (if $P = Q$ then take L to be the unique tangent to C at P). Let this line be L. Then $L \cdot C = P + Q + R$. Define a map of sets $\varphi : C \times C \to C$ by $\varphi(P, Q) = R$.

Now fix any point $O \in C$ and define $m(P,Q) = \varphi(O, \varphi(P,Q))$. We claim that this defines a group law on the points of C with O as identity.

Associativity: We need to show that $m(P, m(Q,R)) = m(m(P,Q),R)$. Let L_1 be the unique line through P and Q. Then $L_1 \cdot C = P+Q+S'$ and $\varphi(P,Q) = S'$. Let M_1 be the unique line through O and S'. Then $M_1 \cdot C = O+S+S'$. Then $m(P,Q) = S$. Let L_2 be the unique line through S and R. Then $L_2 \cdot C = S+R+T'$ and $m(m(P,Q),R) = \varphi(O,T')$.

Let M_2 be the unique line through Q and R, then $M_2 \cdot C = Q+R+U'$. Let L_3 be the unique line through O and U', then $L_3 \cdot C = O+U'+U$ and $m(Q,R) = U$. Let M_3 be the unique line through P and U. Then $M_3 \cdot C = P+U+T''$. Then $m(P, m(Q,R)) = \varphi(O,T'')$. Thus, to prove associativity it suffices to show $T' = T''$. Take $C' = L_1L_2L_3$ and $C'' = M_1M_2M_3$. Then

$$C' \cdot C = P+Q+S'+S+R+T'+O+U'+U$$
$$C'' \cdot C = O+S+S'+Q+R+U'+P+U+T''$$

It follows from the preceding Proposition that $T' = T''$.

Identity: $m(O,P) = m(P,O) = P$. Let L be the unique line through O, P. Then $L \cdot C = O+P+R$. The unique line through O, R is L again and so we get $\varphi(O, \varphi(O,P)) = P$. Similarly, it follows $m(P,O) = P$.

Commutativity: Clearly, $\varphi(P,Q) = \varphi(Q,P)$ implies $m(P,Q) = m(Q,P)$. It is clear the $\varphi(P,Q) = \varphi(Q,P)$.

Inverse: Let L_0 be the tangent line at O. Then $L_0 \cdot C = 2O + R$. Let $P \in C$ be any point. Let L be the unique line through P and R. Then $L \cdot C = P+R+Q$. We claim $m(P,Q) = O$. Note that $\varphi(P,Q) = R$. Clearly, the unique line through R and O is L_0 and so $\varphi(O, \varphi(P,Q)) = O$. Thus, $m(P,Q) = O = m(Q,P)$.

This proves the existence of a group law.

5.6 Exercises

Exercise 5.6.1. Let F be a projective plane curve. Show that a point P is a multiple point of F if and only if $F(P) = F_X(P) = F_Y(P) = F_Z(P) = 0$.

Solution. Suppose $P = [a : b : 1]$ (that is, $P \in U_3$). Assume that P is a multiple point. Then we know that $(F_*)_X(P) = (F_*)_Y(P) = 0$. It is also clear that $(F_*)_X = (F_X)_*$ and $(F_*)_Y = (F_Y)_*$. Thus, it follows that $(F_X)_*(P) = (F_Y)_*(P) = 0$. Recall that

$F_X = Z^l((F_X)_*)^*$, where l is the highest power of Z which divides F_X. Thus, it follows that $F_X(P) = 0$. Similarly, we see that $F_Y(P) = 0$. Let us further assume that $b \neq 0$. Then arguing as above, with Y instead of Z, we see that $F_X(P) = F_Z(P) = 0$. Thus, it follows that if any two coordinates of P are nonzero, then $F_X(P) = F_Y(P) = F_Z(P) = 0$.

Let us consider the case of the three remaining points, that is,

$$P \in \{[1:0:0], [0:1:0], [0:0:1]\}.$$

We will consider the case $P = [0:0:1]$ (case of $P = [0:1:0]$ or $[1:0:0]$ is similar). As $0 = F(P) = F(0,0,\lambda)$ for every $\lambda \in k^\times$, we get $F(0,0,Z) = 0$. So

$$F = \sum_{\substack{p+q+r=n \\ p+q\geqslant 1}} \alpha_{pqr} X^p Y^q Z^r$$

and hence

$$F_Z = \sum_{\substack{p+q+r=n \\ p+q\geqslant 1 \\ r\neq 0}} r\alpha_{pqr} X^p Y^q Z^{r-1}.$$

Thus, $F_Z(P) = 0$. This proves that if P is a multiple point then $F(P) = F_X(P) = F_Y(P) = F_Z(P) = 0$. The converse follows easily by considering P as a point of one of the U_i. □

Exercise 5.6.2. Show that the following curves are irreducible; find their multiple points, and the multiplicities and tangents at the multiple points.

(a) $XY^4 + YZ^4 + XZ^4$.

(b) $X^2Y^3 + X^2Z^3 + Y^2Z^3$.

(c) $Y^2Z - X(X - Z)(X - \lambda Z),\ \lambda \in k$.

(d) $X^n + Y^n + Z^n,\ n > 0$.

Solution. If a form F happens to be irreducible in $k[X,Y,Z]$ then the curve $V(F)$ will also be irreducible. Suppose F is a form in $k[X,Y,Z]$ such that Z is not a factor of F and F_* is irreducible then F is also irreducible. Note that each curve in (a), (b), (c), (d) has no Z factor therefore to show that each of them is an irreducible curve it suffices to show that F_* is irreducible in $k[X,Y]$.

(a) Let $F = XY^4 + YZ^4 + XZ^4$ and we dehomogenize F with respect to Z:

$$F_* = XY^4 + X + Y.$$

Note that $\deg_X F_* = 1$. If $F_* = GH$ (with $\deg(H), \deg(G) \geqslant 1$), we may assume that $\deg_X G = 1$ and $\deg_X H = 0$. So $G = AX + B$ where $A, B \in k[Y]$; $H \in k[Y]$. Hence, $XY^4 + X + Y = (AX + B)H = AHX + BH$, which means $AH = Y^4 + 1$ and $BH = Y$ which further implies that $1 = AH - (BH)^4 = H(A - B^4H^3)$, but this is not possible as $\deg H \geqslant 1$. Hence F_* is irreducible.

We have $F_X = Y^4 + Z^4$, $F_Y = 4XY^3 + Z^4$, $F_Z = 4(X + Y)Z^3$. To find the multiple points (by Exercise 5.6.1), we solve the system $F = F_X = F_Y = F_Z = 0$, which has $P = [1 : 0 : 0]$ as the only solution. Thus, $[1 : 0 : 0]$ is the only multiple point.

(b) Let $F = X^2Y^3 + X^2Z^3 + Y^2Z^3$ and we dehomogenize F with respect to Z:

$$F_* = X^2Y^3 + X^2 + Y^2 = X^2(Y^3 + 1) + Y^2.$$

We view the above as an element of $k(Y)[X]$. This factors in $k[X, Y]$ iff it factors in $k(Y)[X]$, which happens iff the discriminant is a square. But the discriminant is

$$-4Y^2(Y^3 + 1)\,,$$

which is clearly not a square in $k(Y)$. Hence F_* is irreducible.

We have $F_X = 2XY^3 + 2XZ^3$, $F_Y = 3X^2Y^2 + 2YZ^3$, $F_Z = 3(X^2 + Y^2)Z^2$. To find the multiple points, we solve the system $F = F_X = F_Y = F_Z = 0$ which has $[1 : 0 : 0]$, $[0 : 1 : 0]$, $[0 : 0 : 1]$ as the only solutions and hence $[1 : 0 : 0]$, $[0 : 1 : 0]$, $[0 : 0; 1]$ are all the multiple points of F.

When $P = [1 : 0 : 0]$, $m_P(F) = m_{(0,0)}(F(1, Y, Z)) = m_{(0,0)}(Y^3 + Z^3 + Y^2Z^3) = 3$. The tangents are obtained by factoring $Y^3 + Z^3$. Thus, the tangent lines are

$$L = Y + Z, \quad Y - \frac{1 + i\sqrt{3}}{2}Z, \quad Y - \frac{1 - i\sqrt{3}}{2}Z.$$

each of multiplicity 1.

When $P = [0 : 1 : 0]$, $m_P(F) = m_{(0,0)}(F(X, 1, Z)) = m_{(0,0)}(X^2 + X^2Z^3 + Z^3) = 2$. Tangent line is X with multiplicty 2.

When $P = [0 : 0 : 1]$, $m_P(F) = m_{(0,0)}(F(X, Y, 1)) = m_{(0,0)}(X^2Y^3 + X^2 + Y^2) = 2$. Tangent lines: $X + iY$, $X - iY$.

multiple points	tangent lines
$[1 : 0 : 0]$	$Y + Z,\ Y - \frac{1+i\sqrt{3}}{2}Z,\ Y - \frac{1-i\sqrt{3}}{2}Z$
$[0 : 1 : 0]$	X
$[0 : 0 : 1]$	$X + iY,\ X - iY$

(c) Let $F = Y^2Z - X(X-Z)(X-\lambda Z)$ where $\lambda \in k$. Dehomogenize F with respect to Z:

$$F_* = Y^2 - X(X-1)(X-\lambda).$$

By Problem 1.11.32, F_* is irreducible and thus F is irreducible.

We have

$$\begin{aligned} F_X &= -(X-Z)(X-\lambda Z) - X(X-\lambda Z) - X(X-Z), \\ F_Y &= 2YZ, \\ F_Z &= Y^2 + X(X-\lambda Z) + \lambda X(X-Z)\,. \end{aligned}$$

To find the multiple points, we solve the system $F = F_X = F_Y = F_Z = 0$. If $Z = 0$, then $X^3 = 0$, so $X = 0$. Then $Y^2 = 0$, hence the point is $[0:0:0]$, which is not possible. Therefore, $Z \neq 0$ and $Y = 0$. We assume that our point is $[X:0:1]$. Thus, $0 = X(X-1)(X-\lambda)$. Also, we need $(F_X)_*(P) = 0$, which gives that $X(X-1)(X-\lambda)$ has a repeated root. Hence, the only possibilities are $X = \lambda = 0$ or $X = \lambda = 1$. Therefore $[0:0:1]$ is a multiple point if $\lambda = 0$, and $[1:0:1]$ is a multiple point if $\lambda = 1$. Also, F has no multiple points if $\lambda \neq 0, 1$.

(1) $P = [0:0:1]$ if $\lambda = 0$:

$$m_P(F) = m_{(0,0)}(F(X,Y,1)) = m_{(0,0)}(Y^2 + X^2 - X^3) = 2.$$

Tangent lines: $X + iY$, $X - iY$.

(2) $P = [1:0:1]$ if $\lambda = 1$:

$$m_P(F) = m_{(1,0)}(F(X,Y,1)) = m_{(1,0)}(Y^2 - (X-1)^3 - (X-1)^2) = 2.$$

The tangent lines of F_* at $(1,0)$ are $X - Y - 1$, $X + Y - 1$. Therefore the tangent lines of F at P are $X + Y - Z$, $\quad X - Y - Z$.

multiple points	tangent lines
$[0:0:1]$, $\lambda = 0$	$X + iY,\ X - iY$
$[1:0:1]$, $\lambda = 1$	$X + Y - Z,\ X - Y - Z$

(d) Let $F = X^n + Y^n + Z^n$; dehomogenize F with respect to Z:

$$F_* = X^n + Y^n + 1.$$

Note that $Y^n + 1$ has no multiple roots. Thus, using Eisenstein's criterion with any prime factor of $Y^n + 1$, we see that F_* is irreducible.

We have $F_X = nX^{n-1}, F_Y = nY^{n-1}, F_Z = nZ^{n-1}$. To find the multiple points, we solve $F = F_X = F_Y = F_Z = 0$. This does not have a solution in projective space. Hence, F has no multiple points. $\square$

Exercise 5.6.3. Find all points of intersection of the following pairs of curves, and the intersection numbers at these points:

(a) $Y^2Z - X(X-2Z)(X+Z)$ and $Y^2 + X^2 - 2XZ$.

(b) $(X^2+Y^2)Z + X^3 + Y^3$ and $X^3 + Y^3 - 2XYZ$.

Solution. For brevity, we define $I((0,0), F \cap G) = I_O(F \cap G)$.
(a) Let $F = Y^2Z - X(X-2Z)(X+Z)$ and $G = Y^2 + X^2 - 2XZ$. $F = G = 0$ implies $0 = X(X-2Z)(X+2Z)$. If $X = 0$, then $(X,Y,Z) = (0,0,1) \in \mathbb{P}^2$. If $X - 2Z = 0$, then $(X,Y,Z) = (2,0,1) \in \mathbb{P}^2$. If $X + 2Z = 0$, then $(X,Y,Z) = (-2, \sqrt{-8}, 1)$ or $(-2, -\sqrt{-8}, 1) \in \mathbb{P}^2$.
(1) $P_1 = (0,0,1)$: We dehomogenize F and G with respect to Z: $F_* = F(X,Y,1)$, $G_* = G(X,Y,1)$. Hence,

$$\begin{aligned} I(P_1, F \cap G) &= \dim_k(\mathcal{O}_{P_1}(\mathbb{P}^2)/(F_*, G_*)) \\ &= \dim_k(\mathcal{O}_{(0,0)}(\mathbb{A}^2)/(F_*, G_*)) \\ &= I_O(F_* \cap G_*). \end{aligned}$$

So

$$\begin{aligned} I(P_1, F \cap G) = I_O(F_* \cap G_*) &= I_O(G_* \cap (G_* - F_*)) \\ &= I_O((Y^2 + X^2 - 2X) \cap X(X-2)(X+2)) \\ &= I_O((Y^2 + X^2 - 2X) \cap X) + I_O((Y^2 + X^2 - 2X) \cap (X-2)) \\ &\qquad + I_O((Y^2 + X^2 - 2X) \cap (X+2)) \\ &= I_O(Y^2 \cap X) = 2. \end{aligned}$$

Note that $X+2$ and $X-2$ are units in the local ring, and so there are no contributions from the second and third terms.

(2) $P_2 = (2,0,1)$: Similar to (1). So

$$\begin{aligned} I(P_2, F \cap G) &= I((2,0), F_* \cap G_*) \\ &= I_O(F_*(X+2, Y) \cap G_*(X+2, Y)) \\ &= I_O((Y^2 - X(X+2)(X+3)) \cap (Y^2 + X(X+2))) \\ &= I_O((Y^2 - X(X+2)(X+3)) \cap X(X+2)(X+4)) = 2. \end{aligned}$$

(3) $P_3 = (-2, \sqrt{-8}, 1)$ or $P_4 = (-2, -\sqrt{-8}, 1)$:

$$\begin{aligned} I(P_3, F \cap G) &= I(P_3, F - GZ, G) \\ &= I((-2, \sqrt{-8}), X(X-2)(X+2) \cap (Y^2 + X(X-2))) \\ &= I((-2, \sqrt{-8}), (X+2) \cap (Y^2 + X(X-2))) \\ &= I((-2, \sqrt{-8}), (X+2) \cap (Y^2 + 8)) \\ &= 1 \end{aligned}$$

Similarly, $I(P_4, F \cap G) = 1$.

points	intersection numbers
$(0:0:1)$	2
$(2:0:1)$	2
$(-2:\sqrt{-8}:1)$	1
$(-2:-\sqrt{-8}:1)$	1

(b) Let $F = (X^2 + Y^2)Z + X^3 + Y^3$ and $G = X^3 + Y^3 - 2XYZ$. $F = G = 0$ implies $Z(X+Y)^2 = 0$. If $Z = 0$, then $X^3 + Y^3 = 0$, that is,

$$(X, Y, Z) \in \left\{ (-1, 1, 0), \left(\frac{1+\sqrt{-3}}{2}, 1, 0 \right), \left(\frac{1-\sqrt{-3}}{2}, 1, 0 \right) \right\} \subset \mathbb{P}^2.$$

If $X + Y = 0$ and $Z \neq 0$, then $(X, Y, Z) = (0, 0, 1) \in \mathbb{P}^2$.
(1) $P_1 = (-1, 1, 0)$: We dehomogenize F and G with respect to Y:

$$F_* = F(X, 1, Z), \qquad G_* = G(X, 1, Z).$$

Hence,

$$\begin{aligned} I(P_1, F \cap G) &= I((-1, 0), F_* \cap G_*) \\ &= I((-1, 0), F_* - G_* \cap G_*) \\ &= I_O((X^2 Z) \cap (X^3 - 3X^2 - 2XZ + 3X + 2Z)) \\ &= I_O((X^2) \cap (-2XZ + 3X + 2Z)) + I_O((Z) \cap (X^3 - 3X^2 + 3X)) \\ &= 3. \end{aligned}$$

(2) $P_2 = \left(\frac{1+\sqrt{-3}}{2}, 1, 0 \right)$ or $P_3 = \left(\frac{1-\sqrt{-3}}{2}, 1, 0 \right)$: Dehomogenize F and G with respect to Y.

Hence,

$$\begin{aligned} I(P_2, F \cap G) &= I(P_2, F_* \cap G_*) \\ &= I(P_2, F_* - G_* \cap G_*) \\ &= I(P_2, (X+1)^2 Z \cap X^3 + 1 - 2XZ) \\ &= I(P_2, Z \cap X^3 + 1 - 2XZ) \\ &= I(P_2, Z \cap X^3 + 1) \\ &= 1. \end{aligned}$$

Similarly, $I(P_3, F \cap G) = 1$.
(3) $P_4 = (0, 0, 1)$: Dehomogenize F and G with respect to Z. So (in what follows we make the change of variables $S = X + Y$)

$$\begin{aligned} I(P_4, F \cap G) &= I_O(F_* \cap G_*) \\ &= I_O((X+Y)^2 \cap X^3 + Y^3 - 2XY) \\ &= I_O(S^2 \cap (-2SY + 2Y^2 + 3SY^2)) \\ &= I_O(S^2 \cap Y(S - Y)) = 4 \end{aligned}$$

points	intersection numbers
$(-1, 1, 0)$	3
$\left(\frac{1+\sqrt{-3}}{2}, 1, 0\right)$	1
$\left(\frac{1-\sqrt{-3}}{2}, 1, 0\right)$	1
$(0, 0, 1)$	4

□

Exercise 5.6.4. Let P be a simple point on F. Show that the tangent line to F at P has the equation $F_X(P)X + F_Y(P)Y + F_Z(P)Z = 0$.

Solution. By symmetry, we may assume $P \in U_3$, say $P = (a, b, 1)$. Let L_* be a tangent line to F_* at $P_* = (a, b)$. Then L_* is of the form $\alpha(X - a) + \beta(Y - b) = 0$. It follows that $\alpha = (L_*)_X = F_X(P)$ and $\beta = (L_*)_Y = F_Y(P)$. Then

$$L = (L_*)^* = F_X(P)(X - aZ) + F_Y(P)(Y - bZ)\,.$$

By Euler's Theorem

$$\deg(F)F = XF_X + YF_Y + ZF_Z\,.$$

Evaluating both sides at $(a, b, 1)$ we get

$$0 = aF_X(P) + bF_Y(P) + F_Z(P)\,,$$

that is,

$$-aF_X(P) - bF_Y(P) = F_Z(P)\,.$$

Hence, $L = F_X(P)X + F_Y(P)Y + F_Z(P)Z$. □

Exercise 5.6.5. Let $P = [0 : 1 : 0]$, F a curve of degree n,

$$F = \sum F_i(X, Z)Y^{\,n-i}, \qquad F_i \text{ a form of degree } i.$$

Show that $m_P(F)$ is the smallest m such that $F_m \neq 0$, and the factors of F_m determine the tangents to F at P.

Solution. Dehomogenize F with respect to Y: $F_* = F(X, 1, Z) = \sum_{i=0}^{n} F_i(X, Z)$. So $m_P(F) = m_{(0,0)}(F_*) = m_{(0,0)}(\sum_{i=0}^{n} F_i(X, Z))$ is the smallest m such that $F_m \neq 0$. Also, if L is tangent to F, then $I(P, F \cap L) = \dim_k(\mathcal{O}_P(\mathbf{P}^2)/(F_*, L_*)) = \dim_k(\mathcal{O}_{(0,0)}(\mathbf{A}^2)/(F_*, L_*)) = I((0, 0), F_* \cap L_*)$. So $I(P, F \cap L) > m_P(F)$ iff $I((0, 0), F_* \cap L_*) > m_{(0,0)}(F_*)$ iff L_* is tangent to F_* iff L_* is a non-constant factor of F_m. Since F_m is a form, L_* is a non-constant form and thus $(L_*)^* = L$. Therefore, the factors of F_m determine the tangents to F at P. □

Exercise 5.6.6. For any F, $P \in F$, show that $m_P(F_X) \geq m_P(F) - 1$.

Solution. May assume $P = (0, 0, 1)$. Dehomogenize F with respect to Z: $f(X, Y) = F(X, Y, 1)$. So $f = f_m + \text{higher terms}$, where $m = m_P(F) = m_{(0,0)}(f)$ and $f_i \in k[X, Y]$ is a form of degree i. So $f_X = (f_m)_X + \text{higher terms}$. Note that $\deg(f_m)_X \geqslant m - 1$. Thus, $m_P(F_X) = m_{(0,0)}((F_X)_*) = m_{(0,0)}(f_X) \geqslant m - 1 = m_P(F) - 1$. □

Exercise 5.6.7. Let F be an irreducible curve.

(a) Show that one of F_X, F_Y, or F_Z is nonzero.

(b) Show that F has only a finite number of multiple points.

Solution. (a) By $XF_X + YF_Y + ZF_Z = mF$ where F is a form of degree m, F_X, F_Y, F_Z cannot be all zero. (b) WLOG, we may assume $F_X \neq 0$. If F and F_X has a common component G, then $G \mid F$, and thus F is not irreducible. (Since $\deg(F_X) = \deg(F) - 1$, G cannot be F and thus G is not trivial.) Hence, F and F_X have no common components, and thus they intersect in a finite number of points, i.e., $V(F, F_X)$ is a finite set. Note that the subset of the multiple points of F, $V(F, F_X, F_Y, F_Z)$, is contained in $V(F, F_X)$. So F has only a finite number of multiple points. □

Exercise 5.6.8. (a) Let F be an irreducible conic, $P = [0 : 1 : 0]$ a simple point on F, and $Z = 0$ the tangent line to F at P. Show that $F = aYZ - bX^2 - cXZ - dZ^2$, $a, b \neq 0$. Find a projective change of coordinates T so that $F^T = YZ - X^2 - c'XZ - d'Z^2$.Find T' so that $(F^T)^{T'} = YZ - X^2$. (*Hint:* $T' = (X, Y + c'X + d'Z, Z)$.)

(b) Show that, up to projective equivalence, there is only one irreducible conic: $YZ = X^2$. Any irreducible conic is non-singular.

Solution. (a) Let $F = aYZ - bX^2 - cXZ - dZ^2 + \alpha Y^2 + \beta XY$. $0 = F(0, 1, 0) = \alpha$. Hence, $F = (-bX^2 - cXZ - dZ^2) + (aZ + \beta X)Y$. Since $Z = 0$ is the tangent line to F at P, by 5.6.4 we have $a \neq 0$ and $\beta = 0$. Hence, $F = aYZ - bX^2 - cXZ - dZ^2, a \neq 0$. If $b = 0$, then $F = Z(aY - cX - dZ)$ is reducible, and thus $b \neq 0$. So $F = aYZ - bX^2 - cXZ - dZ^2, a, b \neq 0$.

Next we define $T = (\frac{1}{\sqrt{b}}X, \frac{1}{\sqrt{a}}Y, \frac{1}{\sqrt{a}}Z)$ (note that $a, b \neq 0$). T is a projective change of coordinates, and $F^T = YZ - X^2 - c'XZ - d'Z^2$ where $c' = \frac{c}{\sqrt{a}\sqrt{b}}, d' = \frac{d}{a}$. We define $T' = (X, Y + c'X + d'Z, Z)$. Clearly, T' is a projective change of coordinates too, and

$$(F^T)^{T'} = (Y + c'X + d'Z)Z - X^2 - c'XZ - d'Z^2 = YZ - X^2.$$

(b) Let F be an irreducible conic. Note that by Exercise 5.6.6, it has a simple point. After doing a projective change of coordinates, we may assume the tangent line at the simple point P is $Z = 0$. Now by the previous part, up to projective equivalence, this is conic $YZ - X^2$ up to projective equivalence. Note that $YZ - X^2$ is non-singular. □

Exercise 5.6.9. Let F be an irreducible cubic, $P = [0 : 0 : 1]$ a cusp on F, $Y = 0$ the tangent line to F at P. Show that $F = aY^2Z - bX^3 - cX^2Y - dXY^2 - eY^3$. Find projective changes of coordinates
(i) to make $a = b = 1$;
(ii) to make $c = 0$ (change X to $X - \frac{c}{3}Y$);
(iii) to make $d = e = 0$ (change Z to $Z + dX + eY$).
Up to projective equivalence, there is only one irreducible cubic with a cusp: $Y^2Z = X^3$. It has no other singularities.

Solution. Let

$$F = aY^2Z - bX^3 - cX^2Y - dXY^2 - eY^3 + \alpha Z^3 + \beta X^2Z + \gamma XYZ + \delta XZ^2 + \epsilon YZ^2.$$

$0 = F(0, 0, 1) = \alpha$. So

$$F = (-bX^3 - cX^2Y - dXY^2 - eY^3) + (aY^2 + \beta X^2 + \gamma XY)Z + (\delta X + \epsilon Y)Z^2$$

Since F is singular at $(0:0:1)$ we get $\delta = \epsilon = 0$. Thus,

$$F = (-bX^3 - cX^2Y - dXY^2 - eY^3) + (aY^2 + \beta X^2 + \gamma XY)Z\,.$$

Since $Y = 0$ is the unique tangent line, it follows $\beta = \gamma = 0$. Hence,

$$F = aY^2Z - bX^3 - cX^2Y - dXY^2 - eY^3$$

with $a \neq 0$. Since F is irreducible, $b \neq 0$. (If $b = 0$, then Y is a factor of F, which is absurd).
(i) To make $a = b = 1$, we define $T^{(i)} = (b^{-\frac{1}{3}}X, a^{-\frac{1}{3}}Y, a^{-\frac{1}{3}}Z)$ (note that $a, b \neq 0$). Clearly, $T^{(i)}$ is a projective changes of coordinate. So

$$F^{T^{(i)}} = Y^2Z - X^3 - c'X^2Y - d'XY^2 - e'Y^3$$

where $c' = cb^{-\frac{2}{3}}a^{-\frac{1}{3}}$, $d' = db^{-\frac{1}{3}}a^{-\frac{2}{3}}$, $e' = ea^{-1}$.
(ii) To make $c' = 0$, we define a projective change of coordinates $T^{(ii)} = (X - \frac{c'}{3}Y, Y, Z)$. So

$$(F^{T^{(i)}})^{T^{(ii)}} = Y^2Z - X^3 - d''XY^2 - e''Y^3$$

where $d'' = d' - \frac{c'^2}{3}$ and $e'' = e' - \frac{c'd'}{3} + \frac{2c'^3}{27}$. (iii) To make $d'' = e'' = 0$, we define a projective change of coordinates $T^{(iii)} = (X, Y, Z + d''X + e''Y)$. So

$$((F^{T^{(i)}})^{T^{(ii)}})^{T^{(iii)}} = Y^2Z - X^3.$$

Let F be an irreducible cubic which has a cusp P. There is a projective change of coordinates T' such that $P^{T'} = (0, 0, 1) \in F^{T'}$ is a cusp on F, and $Y = 0$ is the tangent line to $F^{T'}$ at $P^{T'}$. Hence, $F^T = Y^2Z - X^3$ where $T = T^{(iii)} \circ T^{(ii)} \circ T^{(i)} \circ T'$ is a projective change of coordinates.

□

Exercise 5.6.10. Up to projective equivalence, there is only one irreducible cubic with a node: $XYZ = X^3 + Y^3$. It has no other singularities.

Solution. The given cubic is irreducible with only one singular point, which is a node. Let F be an irreducible cubic, $P = (0, 0, 1)$ a node on F, $X = 0$ and $Y = 0$ the tangent lines to F at P. Reasoning as in Problem 5.6.9, we get

$$F = aXYZ - bX^3 - cY^3 - dX^2Y - eXY^2$$

where $a \neq 0, b \neq 0, c \neq 0$ (the irreducibility of F implies that $b \neq 0$ and $c \neq 0$). We take a projective change of coordinates to make $a = b = c = 1$: $T^{(i)} = (b^{-\frac{1}{3}}X, c^{-\frac{1}{3}}Y, a^{-1}b^{\frac{1}{3}}c^{\frac{1}{3}}Z)$. So

$$F^{T^{(i)}} = XYZ - X^3 - Y^3 - d'X^2Y - e'XY^2$$

where $d' = db^{-\frac{2}{3}}c^{-\frac{1}{3}}$ and $e' = eb^{-\frac{1}{3}}c^{-\frac{2}{3}}$. We take a projective change of coordinates to make $d' = e' = 0$: $T^{(ii)} = (X, Y, d'X + e'Y + Z)$. So

$$(F^{T^{(i)}})^{T^{(ii)}} = XYZ - X^3 - Y^3.$$

Clearly, $XYZ = X^3 + Y^3$ has only one singularities $(0, 0, 1)$. Therefore, for any $F, P \in F$, there is a projective change of coordinates T' such that $P^{T'} = (0, 0, 1) \in F^{T'}$ is a node on F, and that $X = 0, Y = 0$ are the tangent lines to F at P. So $F^T = XYZ - X^3 - Y^3$ is our desired where $T = T^{(ii)} \circ T^{(i)} \circ T'$ is a projective change of coordinates. □

Exercise 5.6.11. Prove that an irreducible cubic is either nonsingular or has at most one double point (a node or a cusp).

Solution. Let F be an irreducible cubic and suppose that it is not smooth. After a projective change of coordinates, we may assume that the singular point is $P = (0 : 0 : 1)$. Reasoning as in Exercise 5.6.9 we get that

$$F = (-bX^3 - cX^2Y - dXY^2 - eY^3) + (aY^2 + \beta X^2 + \gamma XY)Z\,.$$

If $\alpha = \beta = \gamma = 0$, then F will not be irreducible. Thus, the singularity of F at P is either a node or a cusp. There are no other singular points by Exercise 5.6.9 and 5.6.10. □

Exercise 5.6.12. Let C be an irreducible projective plane curve, $P_1, \ldots, P_n$ simple points on C, $m_1, \ldots, m_n$ integers. Show that there is a $z \in k(C)$ with

$$\mathrm{ord}_{P_i}(z) = m_i \quad \text{for } i = 1, \ldots, n.$$

Solution. Take lines L_i to be a line which passes through P_i and does not contain any other P_j. Let L_0 be a line which does not contain and P_i. Let

$$z = \prod L_i^{m_i} L_0^{-\sum m_i} \in k(C)\,.$$

The rational function L_i/L_0 (this is defined on $C \setminus V(L_0)$) vanishes to order exactly 1 at P_i and does not vanish at any other P_j. Thus, the order of vanishing of z at P_i is exactly m_i. □

Exercise 5.6.13. Let F be an irreducible curve in $\mathbf{P}^2$. Suppose $I(P, F \cap Z) = 1$, and $P \neq [1 : 0 : 0]$. Show that $F_X(P) \neq 0$. (Hint: If not, use Euler's Theorem to show that $F_Y(P) = 0$; but Z is not tangent to F at P.)

Solution. $I(P, F \cap Z) = 1$ implies three things: (i) $P \in F \cap Z$; (ii) Z is not tangent to F at P; (iii) $m_P(F) = 1$ (P is a simple point of F). As $P \neq [1 : 0 : 0]$, we may write $P = (a, 1, 0) \in \mathbf{P}^2$ for some $a \in k$. Suppose $F_X(P) = 0$, then by Euler's Theorem ($XF_X + YF_Y + ZF_Z = mF$ with $m = \deg F$) we have $F_Y(P) = 0$. By Problem 5.6.4, $Z = 0$ is the tangent line to F at P, which is absurd. Therefore, $F_X(P) \neq 0$. □

Exercise 5.6.14. Let $P_1, P_2, P_3, P_4 \in \mathbf{P}^2$. Let V be the linear system of conics passing through these points. Show that $\dim(V) = 2$ if $P_1, \ldots, P_4$ lie on a line, and $\dim(V) = 1$ otherwise.

Solution. To solve this, we consider the vector space of all homogeneous quadratic polynomials in three variables X, Y, Z, which has dimension 6. A general conic is given by:

$$aX^2 + bXY + cY^2 + dXZ + eYZ + fZ^2 = 0.$$

Each point P_i that the conic must pass through imposes one linear constraint on the coefficients a, b, c, d, e, f.

Case 1: Points lie on a line

Suppose $P_1, \ldots, P_4$ all lie on a single line L. Let the equation of this line be $L = 0$. Any conic F passing through these points must contain the entire line L (since a conic and a line can intersect in at most 2 points unless the line is a component of the conic). Therefore, the conic must be reducible and of the form $F = L \cdot M$, where $M = 0$ is another linear form (a line). The space of linear forms M in X, Y, Z has dimension 3. Since $\mathcal{V}$ consists of all such conics $L \cdot M$, the dimension of the system $\mathcal{V}$ is the dimension of the space of linear forms, which is 3. Therefore, $\dim(\mathcal{V}) = 2$ when the points are collinear.

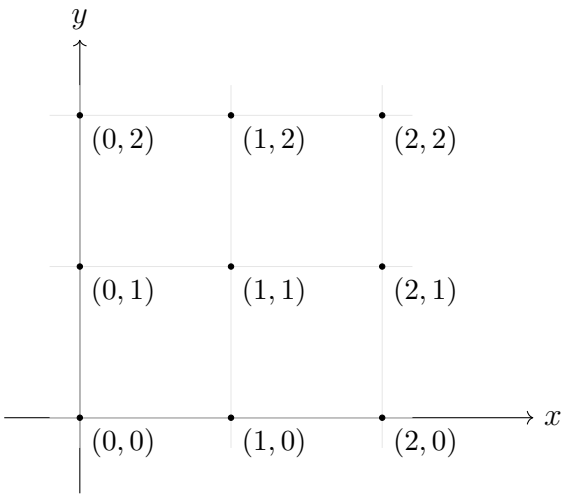
Case 2: Points are not collinear. We may assume that P_4 is not on the line joining P_1 and P_2. Assume that P_3 is on the line joining P_1 and P_2. Then, as in the previous case, we get that the conic equals LM. Thus, the space of such conics is two dimensional. Moreover, we need the conic to pass through P_4, which is not on L. Thus, we also need P_4 should be on M. This proves that the space of such conics is 1 dimensional. Next assume that no three points are collinear. Suppose the points do not impose linearly independent conditions and $\dim(V) \geqslant 2$. Let P_5 be a point which is on the line joining P_1 and P_2, say L. Also assume P_5 is not on the line joining P_3 and P_4. Consider the space V_1 of conics which pass through the points $P_1, \ldots, P_5$. It follows that $\dim(V_1) \geqslant 1$. If $C \in V_1$, then C meets L in at least 3 points, and so it follows $C = LM$, where M is a line passing through P_3 and P_4. It follows that the space of lines through P_3 and P_4 is one dimensional, which is a contradiction. This proves that the points impose independent conditions, and that $\dim(V) = 1$. □

Exercise 5.6.15. Show that there is only one conic passing through the five points $[0 : 0 : 1]$, $[0 : 1 : 0]$, $[1 : 0 : 0]$, $[1 : 1 : 1]$, $[1 : 2 : 3]$, and show that it is nonsingular.

Solution. Let $F = aX^2 + bY^2 + cZ^2 + dXY + eYZ + fZX$ be a conic passing these five points. Hence, $a = b = c = 0$ and $d + e + f = 0$ and $2d + 6e + 3f = 0$. Therefore, $F = 3XY + YZ - 4ZX$ is our desired unique conic. Besides, $F_X = 3Y - 4Z$, $F_Y = 3X + Z$, $F_Z = Y - 4X$. By letting $F = F_X = F_Y = F_Z = 0$, we have $(X, Y, Z) = (0, 0, 0) \notin \mathbf{P}^2$. By Exercise 5.6.1, F is non-singular. □

Exercise 5.6.16. Consider the nine points $[0 : 0 : 1]$, $[0 : 1 : 1]$, $[1 : 0 : 1]$, $[1 : 1 : 1]$, $[0 : 2 : 1]$, $[2 : 0 : 1]$, $[1 : 2 : 1]$, $[2 : 1 : 1]$, $[2 : 2 : 1] \in \mathbf{P}^2$ (sketch). Show that there are an infinite number of cubics passing through these points.

Solution.



Let L_i be the horizontal lines and let M_i be the vertical lines. Then $C_1 = L_1L_2L_3$ and $C_2 = M_1M_2M_3$ are distinct cubics through these nine points. Thus, any other cubic of the form $C_1 + tC_2$ also passes through these points. □

Exercise 5.6.17. Show that every nonsingular projective plane curve is irreducible. Is this true for affine curves?

Solution. Suppose by contradiction: If FG is a non-singular projective plane curve, then we can pick a point $P \in F \cap G$ by Bezout's Theorem. We claim that P is not a simple point. Assume it is simple. Let L be a line which is not tangent to FG at P. Then $I(P, FG \cap L) = 1$. Thus,

$$1 = I(P, FG \cap L) = I(P, F \cap L) + I(P, G \cap L) \geqslant 1 + 1 = 2\,,$$

which is a contradiction.

Let $F(X,Y) = X(X-1)$ be a hypersurface in $\mathbf{A}^2(k)$. F is reducible and non-singular as it consists of two parallel lines. □

Exercise 5.6.18. Let F be a projective plane curve of degree n with no multiple components, and c simple components. Show that

$$\sum \frac{m_P(m_P-1)}{2} \leq \frac{(n-1)(n-2)}{2} + c - 1 \leq \frac{n(n-1)}{2}.$$

(Hint: Let $F = F_1F_2$; consider separately the points on one F_i or on both.)

Solution. There are c components, each of degree $\geqslant 1$. Thus, $c \leqslant n$, which implies $\frac{(n-1)(n-2)}{2} + c - 1 \leqslant \frac{n(n-1)}{2}$. We use induction on c. Theorem 2 gives the case $c = 1$. Suppose this conclusion holds for $1 \leqslant c < c_0$. When $c = c_0$, we can write $F = F_1F_2$ such that each F_i has c_i simple components with $c_i < c_0$. ($c_1 + c_2 = c_0$.) Note that $m_P = m_P(F_1) + m_P(F_2)$. For brevity, we write $m_1 = m_P(F_1)$ and $m_2 = m_P(F_2)$. Consider separately the points on one F_i or on both: (i) If $P \in F_1 \setminus F_2$, then $m_2 = 0$ and thus $m_1 = m_P$. (ii) If $P \in F_2 \setminus F_1$, then $m_1 = 0$ and thus $m_2 = m_P$. (iii) If $P \in F_1 \cap F_2$, then $m_1, m_2 \geqslant 1$. In case (i),

$$\sum_{P \in F_1 \setminus F_2} \frac{m_P(m_P-1)}{2} = \sum_{P \in F_1 \setminus F_2} \frac{m_1(m_1-1)}{2}.$$

In case (ii),

$$\sum_{P \in F_2 \setminus F_1} \frac{m_P(m_P-1)}{2} = \sum_{P \in F_2 \setminus F_1} \frac{m_2(m_2-1)}{2}.$$

In case (iii), since

$$\frac{m_P(m_P-1)}{2} = \frac{m_1(m_1-1)}{2} + \frac{m_2(m_2-1)}{2} + m_1m_2\,.$$

we get

$$\sum_{P \in F_1 \cap F_2} \frac{m_P(m_P-1)}{2} = \sum_{P \in F_1 \cap F_2} \frac{m_1(m_1-1)}{2} + \sum_{P \in F_1 \cap F_2} \frac{m_2(m_2-1)}{2} + \sum_{P \in F_1 \cap F_2} m_1m_2.$$

Combine them:

$$\begin{aligned}
\sum_P \frac{m_P(m_P-1)}{2} &= \sum_{P\in F_1\setminus F_2} + \sum_{P\in F_2\setminus F_1} + \sum_{P\in F_1\cap F_2} \\
&= \sum_{P\in F_1\setminus F_2} \frac{m_1(m_1-1)}{2} + \sum_{P\in F_2\setminus F_1} \frac{m_2(m_2-1)}{2} \\
&\quad + \sum_{P\in F_1\cap F_2} \frac{m_1(m_1-1)}{2} + \sum_{P\in F_2\cap F_1} \frac{m_2(m_2-1)}{2} + \sum_{P\in F_1\cap F_2} m_1m_2 \\
&= \sum_{P\in F_1} \frac{m_1(m_1-1)}{2} + \sum_{P\in F_2} \frac{m_2(m_2-1)}{2} + \sum_{P\in F_1\cap F_2} m_1m_2 \\
&\leqslant \frac{(n_1-1)(n_1-2)}{2} + c_1 - 1 + \\
&\qquad \frac{(n_2-1)(n_2-2)}{2} + c_2 - 1 + \sum_{P\in F_1\cap F_2} m_1m_2 \\
&= \frac{(n-1)(n-2)}{2} + c_0 - 1 + \sum_{P\in F_1\cap F_2} m_1m_2 - n_1n_2.
\end{aligned}$$

where $n_i = \deg(F_i)$ $(n_1+n_2=n)$. Since F has no multiple components, that is, F_1 and F_2 have no common component, we can apply Bezout's Theorem to get

$$n_1n_2 = \sum_{P\in F_1\cap F_2} I(P, F_1\cap F_2) \geqslant \sum_{P\in F_1\cap F_2} m_1m_2.$$

Hence, $\sum_P \frac{m_P(m_P-1)}{2} \leqslant \frac{(n-1)(n-2)}{2} + c_0 - 1$. This completes the proof. □

Exercise 5.6.19. Assume $\mathrm{char}(k) = 0$. Let F be an irreducible curve of degree n in $\mathbf{P}^2$. Suppose $P \in \mathbf{P}^2$ with $m_P(F) = r \geq 0$. Then for all but a finite number of lines L through P, L intersects F in $n-r$ distinct points other than P. We outline a proof:

(a) We may assume $P = [0:1:0]$. If

$$L_\lambda = \{[\lambda : t : 1] \mid t \in k\} \cup \{P\},$$

we need only consider the L_λ. Then

$$F = A_r(X,Z)Y^{n-r} + \cdots + A_n(X,Z), \qquad A_r \neq 0$$

(see Exercise 4.4.21 and Exercise 5.6.5).

(b) Let $G_\lambda(t) = F(\lambda, t, 1)$. It is enough to show that for all but a finite number of λ, G_λ has $n - r$ distinct points.

(c) Show that G_λ has $n - r$ distinct roots if $A_r(\lambda, 1) \neq 0$, and $F \cap F_Y \cap L_\lambda = \{P\}$ (see Exercise 1.11.50).

Solution. (a) First note that the set $L_\lambda = \{(\lambda, t, 1) \mid t \in k\} \cup \{P\}$ is a line. In affine coordinates, it is the line $X - \lambda = 0$. Also note that as $t \to \infty$, we get the point P. Since there is an infinite number of $\lambda \in k$, it suffices to pick our desired lines from $\{L_\lambda \mid \lambda \in k\}$. By Problem 5.6.5, $F = A_r(X, Z)Y^{n-r} + \cdots + A_n(X, Z)$ with $A_r \neq 0$.
(b) A point on L_λ is of the form $(\lambda : t : 1)$. This is on F iff $F(\lambda : t : 1) = 0$, that is, iff $G_\lambda(t) = 0$. $G_\lambda(t) = A_r(\lambda, 1)t^{n-r} + \cdots + A_n(\lambda, 1)$. Write $A_r(X, Z) = \prod L_i^{r_i}$, where $\sum_i r_i = r$ and $L_i = \alpha_i X + \beta_i Z$ are distinct. Then $A_r(\lambda, 1) = \prod(\alpha_i\lambda + \beta_i)^{r_i}$. Note $\alpha_i\lambda + \beta_i \neq 0$. There are only a finite number of λ such that $A_r(\lambda, 1) = 0$. Hence, for all but a finite number of such above λ, it suffices to show that all roots of $G_\lambda(t)$ are distinct. (It is clear that $G_\lambda(t)$ has $n - r$ roots.)
(c) Suppose $A_r(\lambda, 1) \neq 0$. To show G_λ has $n-r$ distinct roots, it suffices to show $G_\lambda(t)$ and $G'_\lambda(t)$ have no common roots. Notice that $G'_\lambda(t) = F_Y(\lambda, t, 1)$. Since $F \cap F_Y$ consists of only finitely many points, it consists of only finitely many points of the type $(\lambda, t, 1)$. It follows that for infinitely many values of λ, there is no t such that $F(\lambda, t, 1) = F_Y(\lambda, t, 1) = 0$. Thus, for infinitely many values of λ, $G_\lambda(t)$ and $G'_\lambda(t)$ have no common roots. □

Exercise 5.6.20. Show that Exercise 5.6.19 remains true if F is reducible, provided it has no multiple components.

Solution. The only place where we used irreducibility of F was to say that F and F_Y have only finitely many common zeros. It is easy to check that if F has only simple factors then F and F_Y ave no common factors. □

Exercise 5.6.21. Let F be an irreducible projective plane curve. Suppose $z \in k(F)$ is defined at every $P \in F$. Show that $z \in k$. (*Hint:* Write $z = H/G$, and use Noether's Theorem.)

Solution. Since z is regular at each point $P \in F$, it follows that for every point $P \in \mathbb{P}^2$, $z \in \mathcal{O}_P(\mathbb{P}^2)$. Let us write $z = \bar{H}/\bar{G} \in k(F)$. Here $H, G \in k[X, Y, Z]$ are of the same degree. Then it follows that for any point $P \in F \cap G$, we have $H_* = zG_*$ in $\mathcal{O}_P(F)$. In other words, for each $P \in F \cap G$, we have $H_* \in (F_*, G_*)$. By Theorem 5.4.2, we get $H = AF + BG$. Going modulo F, and using the fact that H and G have the same degree, it follows that B has degree 0, that is, B is a constant. It follows that $z \in k$. □

Exercise 5.6.22. Suppose the intersections of the opposite sides of a hexagon lie on a straight line. Show that the vertices lie on a conic.

Solution. Let $P_1, P_2, P_3, P_4, P_5, P_6$ be the vertices of a hexagon such that the intersections of the opposite sides $P_1P_2 \cap P_4P_5$, $P_2P_3 \cap P_5P_6$, $P_3P_4 \cap P_6P_1$ are collinear. Let ℓ_i denote the line through P_i and P_{i+1}, where P_7 is to be taken as P_1. Denote these intersection points by

$$A = \ell_1 \cap \ell_4, \quad B = \ell_2 \cap \ell_5, \quad C = \ell_3 \cap \ell_6,$$

and suppose that A, B, C lie on a line ℓ. We prove that the six vertices lie on a conic.

Let $D = \ell_1\ell_3\ell_5$ and let $D' = \ell_2\ell_4\ell_6$. Then

$$D \cdot D' = P_1 + \ldots + P_6 + A + B + C\,.$$

Note that $\ell \cdot D = A + B + C$. The singular points of D are the points of intersections $\ell_1 \cap \ell_3$, $\ell_3 \cap \ell_5$ and $\ell_1 \cap \ell_5$. It is easily checked that A, B, C are simple points of D. Thus, applying Corollary 5.4.4, it follows that there is a conic through $P_1, \ldots, P_6$.

Through any five points in the plane, there passes a conic. If the conic is reducible, then it is the union of two lines. It follows that one of these will contain 3 points. Since our points are the vertices of a hexagon, no three are collinear, and so any conic containing these must be irreducible and hence smooth. □

Exercise 5.6.23. Let C be an irreducible cubic, L a line such that $L \cdot C = P_1 + P_2 + P_3$, P_i distinct. Let L_i be the tangent line to C at P_i: $L_i \cdot C = 2P_i + Q_i$ for some Q_i. Show that Q_1, Q_2, Q_3 lie on a line. (L^2 is a conic!)

Solution. Let C be an irreducible cubic and let L be a line such that

$$L \cdot C = P_1 + P_2 + P_3,$$

where P_1, P_2, P_3 are distinct points. Let L_i be the tangent line to C at P_i. Then

$$L_i \cdot C = 2P_i + Q_i$$

for some point $Q_i \in C$.

Consider the reducible conic $F = L^2$, that is, the conic consisting of the line L taken with multiplicity two. We apply Noether's theorem by taking $F = C$, $G = L^2$ and

$$H = L_1L_2L_3\,.$$

First observe the intersections of F and C. Since

$$L \cdot C = P_1 + P_2 + P_3,$$

we have

$$F \cdot C = L^2 \cdot C = 2P_1 + 2P_2 + 2P_3.$$

Next compute the intersection of H with C:

$$H \cdot C = (L_1 L_2 L_3) \cdot C = (2P_1 + Q_1) + (2P_2 + Q_2) + (2P_3 + Q_3).$$

Since P_i are distinct, they are simple points of F. We apply Corollary 5.4.4. We easily see that there is a line B such that Q_1, Q_2 and Q_3 are on B. □

Exercise 5.6.24. Show that a line through two flexes on a cubic passes through a third flex.

Solution. Let C be a nonsingular cubic and let P_1, P_2 be flexes of C. Let L be the line through P_1 and P_2. Since P_1 and P_2 are flexes, the tangent line at each of these points meets C with multiplicity three. Thus if T_i denotes the tangent at P_i,then

$$T_i \cdot C = 3P_i \qquad (i = 1, 2).$$

Let P_3 be the third intersection point of L with C. Since L passes through P_1 and P_2, Bézout's theorem gives $L \cdot C = P_1 + P_2 + P_3$. If $P_1 = P_2$ then since this point is a flex, it follows $P_3 = P_1$. Thus, in the case there is nothing to prove. So we may assume that $P_1 \neq P_2$. If $P_3 = P_1$ then again we see that $P_1 = P_2$, which is a contradiction. Thus, it follows that $P_1 \neq P_3$ and similarly $P_2 \neq P_3$. Thus, these are distinct points and so P_3 is simple.

Let T_3 be the tangent line to C at P_3. Then

$$T_3 \cdot C = 2P_3 + Q$$

for some point Q on C. If $Q = P_3$ then we are done. If not, then it is forced to be a simple point of C. Consider the cubic

$$H' = T_1 T_2 T_3.$$

Its intersection with C is

$$H \cdot C = 3P_1 + 3P_2 + (2P_3 + Q) \geqslant 2(P_1 + P_2 + P_3) = L^2 \cdot C\,.$$

Apply Corollary 5.4.4 with $F = C$, $G = L^2$. We see that P_1, P_2 and Q are collinear. It follows that $P_3 = Q$, a contradiction. □

Exercise 5.6.25. In subsection 5.5.5, suppose O is a flex on C.

(a) Show that the flexes are exactly the elements of order three in the group (that is, exactly those elements P such that $P \oplus P \oplus P = O$).

(b) Show that a point P is of order two in the group if and only if the tangent to C at P passes through O.

(c) Let $C = Y^2Z - X(X - Z)(X - \lambda Z)$, $\lambda \neq 0, 1$, $O = [0 : 1 : 0]$. Find the points of order two.

(d) Show that the points of order two on a nonsingular cubic form a group isomorphic to $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$.

(e) Show that the flexes form a subgroup of C; as an abelian group, this subgroup is isomorphic to $\mathbb{Z}/(3) \times \mathbb{Z}/(3)$.

(f) Let C be a nonsingular cubic, $P \in C$. How many lines through P are tangent to C at some point $Q \neq P$? (The answer depends on whether P is a flex.)

Solution. Let C be a nonsingular projective cubic curve and O a flex on C serving as the identity for the group law $\oplus$. Since O is a flex, it follows that for any point R, we have $\varphi(O, R) = -R$. Recall that multiplication was defined as $m(P, Q) = \varphi(O, \varphi(P, Q))$. Thus, if O is a flex, then we have $m(P, Q) = -\varphi(P, Q)$. In other words, three points $P, Q, R \in C$ satisfy $P \oplus Q \oplus R = O$ if and only if they are the intersection points of a line L with C, counted with multiplicity.

(a) A point P is a flex if and only if the tangent line L at P has intersection multiplicity $I(P, L \cap C) = 3$. In the group law, this corresponds to $P \oplus P \oplus P = O$, or $3P = O$. The flexes are therefore the kernel of the "multiplication by 3" map.

(b) An element P is of order two if $P \neq O$ and $2P = O$. In the group law, $P \oplus P = O$ implies $P \oplus P \oplus O = O$. This means that the tangent line at P passes through O. Conversely, if $P \neq O$ and the tangent line passes through O, it follows that $P \oplus P \oplus O = O$, that is, $P \oplus P = O$, that is, P is an element of order 2.

(c) Note that the intersection of C with the line $Z = 0$ is exactly the point $[0 : 1 : 0]$. Consider the curve in the affine chart $Z = 1$:

$$f(x, y) = y^2 - x(x - 1)(x - \lambda)\,.$$

The tangent line at a point $P = (a, b)$ is

$$f_x(P)(X - aZ) + f_y(P)(Y - bZ)\,.$$

For this point to pass through $[0:1:0]$ we need $f_y(P) = 0$, that is, $b = 0$. Putting $b = 0$, we get $x = 0, 1, \lambda$. Thus, the points of order two are:

$$(0:0:1), (1:0:1), (\lambda:0:1)\,.$$

(d) The set of points $\{P \in C \mid 2P = O\}$ consists of the three points found in part (d) plus the identity O. This is a subgroup of order 4. Since every non-identity element has order 2, the subgroup is not cyclic and must be isomorphic to the Klein Four-group $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$.

(e) We use the same notation as above. We want to find how many 3-torsion points there are. Let $P = (a, b)$ be a point on C in affine coordinates $Z = 1$. Then it is clear that the point $P' = (a : -b : 1)$ is on C. Moroever, the line joining $(a : b : 1)$ and $(0 : 1 : 0)$ contains

$$(a : -b : 1) = (a : b : 1) - 2b(0 : 1 : 0)\,.$$

It follows that P, P' and O are on a line and so $P' = -P$. Thus, if $P = (a, b)$ then $-P = (a, -b)$.

Let $P = (a, b)$ be a point in affine coordinates $Z = 1$ such that $b \neq 0$. Let $h(x) = x(x-1)(x-\lambda)$. The tangent line L through P is

$$-h'(a)(x-a) + 2b(y-b)\,.$$

Since $b \neq 0$, the closure of this tangent line (given by the equation $-h'(a)(X - aZ) + 2b(Y - bZ)$) does not contain $(0 : 1 : 0)$. Thus, the line $-h'(a)(x-a) + 2b(y-b)$ meets the curve in the affine plane in precisely 3 points. Let $\mu = h'(a)/2b$. Then this line may be written as

$$y = b + \mu(x-a)\,.$$

The points of intersection $L \cap C$ have x coordinate which are roots of the equation

$$g_{(a,b)}(x) = g(x) = (b + \mu(x-a))^2 - x(x-1)(x-\lambda)\,.$$

It is easy to check (by explicit computation) that $g'(a) = 0$, in fact, since the line is tangent to the curve at P, clearly, a has to be a root of mutliplicity at least 2. Then $g_{(a,b)}(x)$ has $x = a$ as a root with mutliplicity 3 iff $g''(a) = 0$.

$$g''(a) = 2\mu^2 - 2(3a - \lambda - 1) = \frac{h'(a)^2}{2b^2} - 2(3a - \lambda - 1) = 0\,.$$

This gives

$$h'(a)^2 - 4a(a-1)(a-\lambda)(3a - \lambda - 1) = 0\,.$$

Let

$$H(a) = h'(a)^2 - 4h(a)(3a - \lambda - 1)\,.$$

We conclude that

$$\text{The polynomial } g_{(a,b)}(x) \text{ has a unique root } \Leftrightarrow \ a \text{ is a root of } H\,.$$

Thus, a necessary condition for the point (a, b) to be 3 torsion is that a has to be a root of the polynomial H, which depends only on λ.

We will show next that corresponding to each root of H, we get two 3 torsion points on C. Let a_0 be a root of H. Note that since h has distinct roots, $a = 0, 1, \lambda$ are not roots of H. Thus, $h(a_0) \neq 0$. Let b_0 be such that $b_0^2 = h(a_0)$. We claim that $P = (a_0, b_0)$ is a 3 torsion point. Since a_0 is a root of H, it follows that $g_{(a_0,b_0)}(x)$ has exactly one root, which is $x = a_0$. Thus, if L is the tangent line through P, then the x coordinate of every point in $L \cap C$ equals a_0. Thus, it follows that every point of $L \cap C$ is either (a_0, b_0) or $(a_0, -b_0)$. The equation of L is $y = b_0 + \mu(x - a_0)$. It is clear that $(a_0, -b_0)$ is not on this line. Thus, $L \cap C = 3P$, and so P is a 3 torsion point. Thus, it follows that for every root of H, we get a pair of 3 torsion points.

One can easily check that H is a degree 4 equation in a, and after some calcuations, that the discriminant of H is a constant multiple of $\lambda^4(1-\lambda)^4$. Since $\lambda \notin \{0, 1\}$, it follows that this equation has four distinct roots. This shows that we get eight 3 torsion points. Moreover, the point O also satisfies $3O = O$. Thus, there are 9 points in total which satisft $3P = O$. The kernel of the multiplication by 3 map is an abelian group of order 9, such that every element is killed by 3. This group is forced to be $\mathbb{Z}/3 \times \mathbb{Z}/3$.

(f) Let L be a line through P which is tangent to C at Q. In the group law, this is equivalent to $Q \oplus Q \oplus P = O$, that is, $2Q = -P$.

Consider the map $[2] : C \to C$ given by $Q \mapsto 2Q$. We claim that this map is surjective. To prove this, we need to show that for any point $P \in C$, there is a point Q such that $2Q = P$. This is clearly true when $P = O = [0 : 1 : 0]$. Since $P \mapsto -P$ is an isomorphism, it suffices to show that for each $P \neq O$, we can find a point Q such that $2Q = -P$, that is, we can find a point Q such that the tangent line through Q meets the curve at the given point P.

Given a point Q, let us compute the intersection point of the tangent line through Q and the curve. Let $Q = (a, b)$ in the affine open set $Z = 1$. Let us further assume that $b \neq 0$. The tangent line through Q is the line

$$y = b + \frac{h'(a)}{2b}(x - a)\,,$$

and suppose it meets the curve at Q'. Substituting the expression for y into $f(x,y)=0$ and using the fact that $x-a$ is a repeated root, we get the third root of $f(x, b+\frac{h'(a)}{2b}(x-a))=0$ is

$$x_{Q'} = \frac{h'(a)^2 + (-8a+4\lambda+4)h(a)}{4h(a)}\,.$$

Note that since we assumed $b \neq 0$, we have $h(a) \neq 0$. It follows that

$$y_{Q'} = b + \frac{h'(a)}{2b}(x_{Q'} - a)\,.$$

Now suppose $P=(s,t)$ is given. We want to find a point Q such that the tangent line through Q meets the curve at P. The above computation shows that we need to find $Q=(a,b)\in C$ such that the following two equations are satisfied:

$$s = \frac{h'(a)^2 + (-8a+4\lambda+4)h(a)}{4h(a)}\,, \tag{5.6.26}$$

$$t = b + \frac{h'(a)}{2b}(x_{Q'} - a)\,. \tag{5.6.27}$$

Thus, we consider the polynomial equation (in the variable a)

$$h'(a)^2 + (-8a+4\lambda+4-4s)h(a) = 0\,.$$

This is a polynomial of degree 4 and so has a solution a_0. Note that $a_0 \notin \{0,1,\lambda\}$. Let b_0 be such that $(a_0,b_0)\in C$. Since $h(a_0)\neq 0$, there are exactly two choices for b_0, namely, $\pm\sqrt{h(a_0)}$. Let $Q_1=(a_0,b_0)$ and $Q_2=(a_0,-b_0)$. Let L_i be the tangent line through Q_i and let the third point of intersection of L_i and C be Q_i'. Then it follows that

$$\begin{aligned}
x_{Q_1'} &= \frac{h'(a_0)^2 + (-8a_0+4\lambda+4)h(a_0)}{4h(a_0)} = s\,,\\
y_{Q_1'} &= b_0 + \frac{h'(a_0)}{2b_0}(x_{Q_1'} - a_0) = b_0 + \frac{h'(a_0)}{2b_0}(s-a_0)\,,\\
x_{Q_2'} &= \frac{h'(a_0)^2 + (-8a_0+4\lambda+4)h(a_0)}{4h(a_0)} = s\,,\\
y_{Q_2'} &= -b_0 + \frac{h'(a_0)}{-2b_0}(x_{Q_2'} - a_0) = -b_0 + \frac{h'(a_0)}{-2b_0}(s-a_0) = -y_{Q_1'}\,.
\end{aligned}$$

Moreover,

$$y_{Q_i'}^2 = h(x_{Q_i'}) = h(s) = t^2\,.$$

Thus, either $y_{Q_1'} = t$ or $y_{Q_2'} = t$. It follows that one of Q_1 or Q_2 satisfies both equations (5.6.26) and (5.6.27). Thus, we have found a point Q such that $2Q = -P$. This proves that the map $[2] : C \to C$ is surjective. We also know that the kernel of this map is $\mathbb{Z}/2 \times \mathbb{Z}/2$.

Now let P be a point in C and let L be a line through P which is tangent to C at a point $Q \neq P$. It follows that $2Q = -P$. Conversely, if $2Q = -P$, then there is a line through P which is tangent to C at Q. We know that there are precisely 4 distinct points Q which satisfy this condition, as this is the fiber of the map $[2]$ over the point $[-P]$. Suppose P is a flex, then one of these points is P itself. Thus, if P is a flex then there are 3 such lines. If P is not a flex then there are 4 such lines. □

Exercise 5.6.28. Let C be a non-singular cubic given by the equation

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3\,,$$

$O = [0 : 1 : 0]$. Let $P_i = [x_i : y_i : 1]$, $i = 1, 2, 3$, and suppose $P_1 \oplus P_2 = P_3$. If $x_1 = x_2$ but $P_1 \neq P_2$ then $P_3 = O$. So consider the cases $x_1 \neq x_2$ or $P_1 = P_2$. Let

$$\lambda = \begin{cases} (y_1 - y_2)/(x_1 - x_2) & \text{if } x_1 \neq x_2 \\ (3x_1^2 + 2ax_1 + b)/(2y_1) & \text{if } P_1 = P_2 \end{cases}$$

Let

$$\mu = y_1 - \lambda x_1\,.$$

Show that $x_3 = \lambda^2 - a - x_1 - x_2$ and $y_3 = -\lambda x_3 - \mu$. This gives an explicit method for calculating in the group.

Solution. Consider the non-singular cubic C in the affine chart $Z = 1$, given by the equation:

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

The point $O = [0 : 1 : 0]$ is the identity of the group. According to the definition of the group law on a cubic, three points P_1, P_2, P_4 sum to O if and only if they are collinear. If $P_1 \oplus P_2 = P_3$, then by definition $P_1 \oplus P_2 \oplus (-P_3) = O$. Thus, P_1, P_2, and $P_4 = -P_3$ lie on a line L.

In this coordinate system, for any point $P = (x, y)$, its inverse is $-P = (x, -y)$. Since $P_3 = (x_3, y_3)$, we have $P_4 = (x_3, -y_3)$. Let the line L passing through P_1, P_2, and P_4 be given by $y = \lambda x + \mu$.

The slope λ is determined as follows:

- If $x_1 \neq x_2$, L is the secant line through P_1 and P_2, so $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$.

- If $P_1 = P_2$, L is the tangent line at P_1. Differentiating $y^2 = f(x)$ implicitly gives $2yy' = f'(x) = 3x^2 + 2ax + b$. Thus, $\lambda = \frac{3x_1^2+2ax_1+b}{2y_1}$.

The y-intercept is $\mu = y_i - \lambda x_i$ for $i = 1, 2$.

The intersection of the line L and the cubic C is found by substituting $y = \lambda x + \mu$ into the curve equation:

$$(\lambda x + \mu)^2 = x^3 + ax^2 + bx + c$$
$$\lambda^2 x^2 + 2\lambda\mu x + \mu^2 = x^3 + ax^2 + bx + c$$

Rearranging into a monic cubic polynomial in x:

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\mu)x + (c - \mu^2) = 0$$

By the fundamental theorem of algebra (or Vieta's formulas), the sum of the roots x_1, x_2, x_4 of this cubic is equal to the negative of the coefficient of the x^2 term:

$$x_1 + x_2 + x_4 = -(a - \lambda^2) = \lambda^2 - a$$

Since $P_4 = (x_3, -y_3)$, we have $x_4 = x_3$. Substituting this into the sum of roots:

$$x_1 + x_2 + x_3 = \lambda^2 - a \implies x_3 = \lambda^2 - a - x_1 - x_2$$

To find y_3, we use the fact that $(x_3, -y_3)$ lies on the line L:

$$-y_3 = \lambda x_3 + \mu \implies y_3 = -\lambda x_3 - \mu$$

This completes the justification for the explicit coordinates of P_3. □

Exercise 5.6.29. (a) Let $C = Y^2Z - X^3 - 4XZ^2$, $O = [0 : 1 : 0]$, $A = [0 : 0 : 1]$, $B = [2 : 4 : 1]$, and $C = [2 : -4 : 1]$. Show that $\{0, A, B, C\}$ form a subgroup of C that is cyclic of order 4.

(b) Let $C = Y^2Z - X^3 - 43XZ^2 - 166Z^3$. Let $O = [0 : 1 : 0]$, $P = [3 : 8 : 1]$. Show that P is an element of order 7 in C.

Solution. We use the explicit group law formulas derived in Exercise 5.6.28. The identity is $O = [0 : 1 : 0]$. For any point $P = (x, y)$, its inverse is $-P = (x, -y)$.
(a) The curve is $y^2 = x^3 + 4x$. Here $a = c = 0$, $b = 4$. The given points in affine coordinates are $A = (0, 0)$, $B = (2, 4)$, and $C = (2, -4)$. Note that $C = -B$.

- **Order of A:** Since $y_A = 0$, the tangent at A is vertical, passing through O. Thus, $2A = O$, so A has order 2.

- **Addition $B \oplus B$:** We calculate $2B$. The slope λ of the tangent at $B(2,4)$ is:

$$\lambda = \frac{3x_B^2 + b}{2y_B} = \frac{3(2^2)+4}{2(4)} = \frac{16}{8} = 2\,.$$

$$\mu = y_B - \lambda x_B = 4 - 2(2) = 0\,.$$

$$x_{2B} = \lambda^2 - a - 2x_B = 2^2 - 2(2) = 0$$
$$y_{2B} = -\lambda x_{2B} - \mu = 0$$

  It follows that $2B = A$. Since A has order 2, it follows that $4B = O$.

- **Compute $3B$:** We will compute $3B = B + A$.

$$\lambda = 2$$
$$\mu = y_A - \lambda x_A = 0\,.$$

  Then

$$x_{3B} = \lambda^2 - 0 - x_A - x_B = 2$$
$$y_{3B} = -\lambda x_{3B} - \mu = -4\,.$$

  Thus, $3B = C$. This proves that the subgroup generated by B is cyclic of order 4.

(b) The curve is $y^2 = x^3 - 43x + 166$. Then $a = 0$ and $b = -43$. Let $P = (3,8)$. To show P has order 7, we show $4P = -3P$.

1. **Calculate $2P$:**

$$\lambda = \frac{3(x_P^2) + b}{2(8y_P)} = \frac{3(3^2) - 43}{2(8)} = -1$$
$$\mu = y_P - \lambda x_P = 11$$
$$x_{2P} = 1 - 0 - 2(3) = -5$$
$$y_{2P} = -\lambda x_{2P} - \mu = -16$$

2. **Calculate $3P$:**

$$\lambda = \frac{y_{2P} - y_P}{x_{2P} - x_P} = 3$$
$$\mu = y_P - \lambda x_P = -1$$
$$x_{3P} = 9 - 0 + 5 - 3 = 11$$
$$y_{3P} = -33 + 1 = -32$$

3. **Calculate** $4P$**:**

$$\begin{aligned}\lambda &= \frac{3(x_{2P}^2)+b}{2(8y_{2P})} = \frac{3(25)-43}{2(-16)} = -1\\ \mu &= y_{2P} - \lambda x_{2P} = -21\\ x_{4P} &= 1 - 0 - 2(-5) = 11\\ y_{4P} &= -\lambda x_{4P} - \mu = 32\end{aligned}$$

□

Exercise 5.6.30. Let C be a nonsingular cubic, O a flex on C. Let $P_1, \ldots, P_{3m} \in C$. Show that $P_1 \oplus \cdots \oplus P_{3m} = O$ if and only if there is a curve F of degree m such that

$$F \cdot C = \sum_{i=1}^{3m} P_i.$$

(*Hint:* Use induction on m. Let $L \cdot C = P_1 + P_2 + Q$, $L' \cdot C = P_3 + P_4 + R$, $L'' \cdot C = Q + R + S$, and apply induction to $S, P_5, \ldots, P_{3m}$; use Noether's Theorem.)

Solution. We prove the statement by induction on m.
Base Case ($m = 1$): For $m = 1$, we have $3m = 3$ points P_1, P_2, P_3. By the definition of the group law on a cubic, $P_1 \oplus P_2 \oplus P_3 = O$ if and only if the points are collinear. Thus, the statement holds for $m = 1$.
Inductive Step: Suppose the statement holds for $m - 1$. Let $P_1, \ldots, P_{3m}$ be points on C. Suppose $P_1 \oplus \cdots \oplus P_{3m} = O$. Let L, L', L'' be lines such that:

$$L \cdot C = P_1 + P_2 + Q, \quad L' \cdot C = P_3 + P_4 + R, \quad L'' \cdot C = Q + R + S$$

In the group law, these imply $P_1 \oplus P_2 \oplus Q = O$, $P_3 \oplus P_4 \oplus R = O$, and $Q \oplus R \oplus S = O$. By substitution, $P_1 \oplus P_2 = -Q$ and $P_3 \oplus P_4 = -R$. Then

$$(P_1 \oplus P_2) \oplus (P_3 \oplus P_4) = -(Q \oplus R) = S\,.$$

Thus $P_1 \oplus P_2 \oplus P_3 \oplus P_4 = S$. The original sum $P_1 \oplus \cdots \oplus P_{3m} = O$ becomes $S \oplus P_5 \oplus \cdots \oplus P_{3m} = O$. This is a sum of $3m - 4 + 1 = 3(m-1)$ points. By the inductive hypothesis, there exists a curve G of degree $m - 1$ such that $G \cdot C = S + \sum_{i=5}^{3m} P_i$. Now consider the curve $F' = G \cdot L \cdot L'$ of degree $(m-1) + 1 + 1 = m + 1$. Its intersection with C is:

$$F' \cdot C = (S + P_5 + \cdots + P_{3m}) + (P_1 + P_2 + Q) + (P_3 + P_4 + R)$$

Rearranging:

$$F' \cdot C = \sum_{i=1}^{3m} P_i + (Q + R + S)\,.$$

Since $Q+R+S$ is the intersection $L'' \cdot C$, we have $F' \cdot C = \sum_{i=1}^{3m} P_i + L'' \cdot C$. By Noether's Fundamental Theorem, since L'' is a line and its intersection with C is contained in the intersection of F' with C, there exists a curve F of degree $(m+1)-1 = m$ such that $F \cdot C = F' \cdot C - L'' \cdot C = \sum_{i=1}^{3m} P_i$.

Conversely, suppose there exists a curve F of degree m such that $F \cdot C = \sum_{i=1}^{3m} P_i$. We use the same construction for L, L', L'' to find S such that $P_1 \oplus P_2 \oplus P_3 \oplus P_4 = S$. As before,

$$F \cdot L'' \cdot C = \sum_{i=1}^{3m} P_i + Q + R + S = (P_1 + P_2 + Q) + (P_3 + P_4 + R) + (S + \sum_{i=5}^{3m} P_i)\,.$$

This simplifies to $F \cdot L'' \cdot C = L \cdot L' \cdot C + (S + \sum_{i=5}^{3m} P_i)$. Applying Noether's Theorem we get there exists a curve G of degree $m-1$ such that $G \cdot C = S + \sum_{i=5}^{3m} P_i$. By the inductive hypothesis, $S \oplus P_5 \oplus \cdots \oplus P_{3m} = O$. Replacing S with $P_1 \oplus P_2 \oplus P_3 \oplus P_4$, we obtain $\sum_{i=1}^{3m} P_i = O$. □

Exercise 5.6.31. Let C be a nonsingular cubic, F, F' curves of degree m such that $F \cdot C = \sum_{i=1}^{3m} P_i, \quad F' \cdot C = \sum_{i=1}^{3m-1} P_i + Q$. Show that $P_{3m} = Q$.

Solution. This problem follows directly from Exercise 5.6.30. Applying Exercise 5.6.30, we have:

$$P_1 \oplus P_2 \oplus \cdots \oplus P_{3m-1} \oplus P_{3m} = O\,,$$
$$P_1 \oplus P_2 \oplus \cdots \oplus P_{3m-1} \oplus Q = O\,.$$

We may cancel the common sum $(P_1 \oplus \cdots \oplus P_{3m-1})$ from both sides, which yields $P_{3m} = Q$. □

Exercise 5.6.32. For which points P on a nonsingular cubic C does there exist a nonsingular conic that intersects C only at P?

Solution. Let C be a nonsingular projective cubic curve and let O be a flex on C serving as the identity of the group $(C, \oplus)$. We seek the condition on a point $P \in C$ such that there exists a nonsingular conic Q with $Q \cap C = \{P\}$.

By Bézout's Theorem, the intersection of a conic ($d = 2$) and a cubic ($d = 3$) consists of $2 \cdot 3 = 6$ points, counted with multiplicity. If the conic intersects the cubic only at P, then the intersection cycle must be:

$$Q \cdot C = 6P\,.$$

We apply Exercise 5.6.30 to see that the above happens iff:

$$P \oplus P \oplus P \oplus P \oplus P \oplus P = O$$

Therefore, such a conic exists if and only if P is a 6-torsion point in the group C.

To satisfy the requirement that the conic Q is **nonsingular**, we must ensure that it is not the union of two lines. Suppose $Q = L_1 L_2$. It follows that $L_1 \cdot C = L_2 \cdot C = 3P$. It follows that L_1 and L_2 equal the tangent line at P and $L_1 \cdot C = 3P$. This shows that P is forced to be a 3-torsion point. Thus, if P is such that $6P = O$ and $3P \neq O$, then there is a nonsingular conic Q which meets C only at P.

Finally, we prove that if P is a 3 torsion point, then there is no nonsingular cubic Q which meets C only at P. Since P is a 3 torsion point, there is a line L such that $L \cap C = 3P$. By Noether's Theorem, there is a line L' such that $Q \cdot C = L \cdot C + L' \cdot C$. This forces that $L = L'$. It follows that the rational function Q/LL' has valuation 0 in every local ring of C. Thus, this is a regular function on all of C, and so is constant by Exercise 5.6.21. □

Chapter 6

Varieties, morphisms and rational maps

Fulton writes the following:

"This chapter begins the study of intrinsic properties of a variety - properties that do not depend on its embedding in affine or projective spaces (or products of these). Making this transition from extrinsic to intrinsic geometry has not been easy historically; the abstract language required demands some fortitude from the reader."

For ordinary mortals like me, it seems reasonable to change the last phrase to:

"the abstract language required demands an immense amount of fortitude from the reader."

6.1 Zariski Topology

Recall that we have had the following notions of an algebraic set:

1. We started by considering closed algebraic subsets of $\mathbb{A}^n$.

2. Then we considered closed algebraic subsets of $\mathbb{P}^n$.

3. Since $\mathbb{A}^n \subset \mathbb{P}^n$ as an open subset, from Remark 4.3.2, it follows that we can recover the objects in (1) as open subsets of objects in (2).

6.2 Quasi-projective varieties

Recall that a projective algebraic variety is a closed algebraic subset of $\mathbb{P}^n$ which is irreducible. Let V be a projective algebraic variety. Then we have the Zariski topology on V.

Proposition 6.2.1. *Let V be a projective algebraic variety. Let U_1 and U_2 be non-empty open subsets in V. Then $U_1 \cap U_2 \neq \emptyset$.*

Proof. If $U_1 \cap U_2 = \emptyset$, then

$$V = (V \setminus U_1) \cup (V \setminus U_2),$$

which contradicts irreducibility of V. □

Corollary 6.2.2. *Let $U \neq \emptyset$ be an open subset of V. Then U is dense in V.*

Let $T \subset \mathbb{P}^n$ be a subset. Then we may give T the subspace topology from the Zariski topology on $\mathbb{P}^n$. We will say that T is irreducible if it cannot be written as the union of two proper closed subsets.

Lemma 6.2.3. *Let V be a projective algebraic variety. Let $U \subset V$ be a non-empty open subset. Then U is irreducible.*

Proof. Let us assume that U is reducible. Then there are proper closed subsets $Y_1 \subset U$ and $Y_2 \subset U$ such that

$$U = Y_1 \cup Y_2.$$

Let $x \in U \setminus Y_1$. Since Y_1 is closed in U, it follows that $U \setminus Y_1$ is open in U and hence also open in V. Thus, there is an open subset of x which does not meet Y_1, and so $x \notin \overline{Y_1}$ (the closure of Y_1 in V). It follows that $\overline{Y_1} \subset V$ is a proper closed subset. Similarly, it follows that $\overline{Y_2} \subset V$ is a proper closed subset. Since U is dense in V, it follows that

$$V = \overline{U} = \overline{Y_1} \cup \overline{Y_2},$$

which contradicts the irreducibility of V. □

Definition 6.2.4. *In view of the above lemma, it makes sense to define a quasi-projective variety (or simply a variety) as an open subset of a projective variety.*

Let V be a projective variety and let $U \subset V$ be an open subset. Recall that we had defined the homogeneous coordinate ring of V as

$$\Gamma_h(V) = k[X_1, \ldots, X_{n+1}]/I(V),$$

where $V \subset \mathbb{P}^n$ and $I(V)$ is the homogeneous ideal of V. Recall that

$$k(V) = \left\{ \frac{F}{G} \;\middle|\; F, G \in \Gamma_h(V) \text{ homogeneous of the same degree, } G \neq 0 \right\}.$$

This defines a genuine function on the open subset $V \setminus V(G)$ given by

$$P \mapsto \frac{F(P)}{G(P)}.$$

Given an open subset $U \subset V$, define $k(U) = k(V)$. Given a point $P \in U$, define $\mathcal{O}_P(U) = \mathcal{O}_P(V)$. We define the regular functions on U to be

$$\bigcap_{P \in U} \mathcal{O}_P(U) \subset k(V).$$

This space, of regular functions on U, is denoted $\Gamma(U)$.

Proposition 6.2.5. *Let $f \in \bigcap_{P \in U} \mathcal{O}_P(U)$ be such that $f(P) = 0$ for all $P \in U$. Then $f = 0$.*

Proof. Recall that U is an open subset of a projective variety $V \subset \mathbb{P}^n$. Let $P \in U$ and let $f \in \mathcal{O}_P(V)$. Then there are homogeneous polynomials $F, G \in k[x_0, \ldots, x_n]$ such that $\deg(F) = \deg(G)$, $G(P) \neq 0$ and $f = \frac{F}{G}\big|_V$. Consider the open subset $V \setminus V(G)$. Then $\frac{F}{G}$ defines a function on $V \setminus V(G)$, and by our hypothesis, this function vanishes on $U \setminus V(G)$. It follows that $V(F)$ contains $U \setminus V(G)$. Since $U \setminus V(G)$ is dense in V, and $V(F)$ is a closed subset of $\mathbb{P}^n$, it follows that $V(F)$ contains V. Thus, it follows that $F \in I(V(F)) \subset I(V)$. Thus, $F = 0$ in $\Gamma_h(V)$, which means that $f = 0$. □

Let $\mathcal{F}(U, k)$ denote the space of maps of sets $U \to k$. Then the above proposition shows that the natural map $\Gamma(U) \to \mathcal{F}(U, k)$ is an inclusion.

6.3 Morphisms of Varieties

Definition 6.3.1. *Let X and Y be varieties. Given a map of sets $\phi : X \to Y$, we get a natural map $\tilde{\phi} : \mathcal{F}(Y, k) \to \mathcal{F}(X, k)$ given by $f \mapsto f \circ \phi$. We say that ϕ is a morphism of varieties if:*

(i) If $U \subset Y$ is open, then $\phi^{-1}(U)$ is open in X.

(ii) Given $U \subset Y$ open, $\tilde{\phi}(\Gamma(U)) \subset \Gamma(\phi^{-1}(U))$.

Given a morphism of varieties $\phi : X \to Y$, we say it is an isomorphism if ϕ is bijective and ϕ^{-1} is also a morphism.

A variety X is said to be affine if there is an affine variety $Y \subset \mathbb{A}^m$ and an isomorphism $\phi : X \to Y$.

Recall that we had already defined a notion of "maps" between affine varieties, namely, polynomial maps. Next we will show that morphisms between affine varieties are the same as polynomial maps.

Proposition 6.3.2. *Let X and Y be affine varieties. There is a natural bijective correspondence between morphisms $\phi : X \to Y$ and polynomial maps $\theta : X \to Y$.*

Proof. Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$. Let us check that a morphism $\phi : X \to Y$ is the same as a polynomial map. Let $\Gamma(Y) = k[Y_1, \ldots, Y_m]/I(Y)$ and let $\Gamma(X) = k[X_1, \ldots, X_n]/I(X)$. First let us show that a polynomial map $\theta : X \to Y$ gives rise to a morphism $\phi : X \to Y$. Since θ is a polynomial map, we have a diagram:

$$\begin{array}{ccc} \mathbb{A}^n & \xrightarrow{\theta'} & \mathbb{A}^m \\ \uparrow & & \uparrow \\ X & \xrightarrow{\theta} & Y \end{array}$$

where

$$\theta'(a_1, \ldots, a_n) = (F_1(a_1, \ldots, a_n), \ldots, F_m(a_1, \ldots, a_n)),$$

for polynomials $F_1, \ldots, F_m \in k[X_1, \ldots, X_n]$. Since X and Y are closed subspaces, to show that θ is continuous, it suffices to show that θ' is continuous. Let $Z \subseteq \mathbb{A}^m$ be a closed subset. We need to show that $(\theta')^{-1}(Z) \subseteq \mathbb{A}^n$ is closed. Let $(G_1, \ldots, G_r) = I(Z) \subset k[Y_1, \ldots, Y_m]$. Then $P \in (\theta')^{-1}(Z)$ iff $\theta'(P) \in Z$ iff $G_i(\theta'(P)) = 0$ iff $(G_i \circ \theta')(P) = 0$. Note that $G_i \circ \theta' = G_i(F_1, \ldots, F_m) \in k[X_1, \ldots, X_n]$. Thus, $(\theta')^{-1}(Z) = V(G_1 \circ \theta', \ldots, G_r \circ \theta')$ and so it is closed. This proves that θ' is continuous and so θ is continuous.

Recall the correspondence between polynomial maps $\theta : X \to Y$ and k-algebra homomorphism $\tilde{\theta} : \Gamma(Y) \to \Gamma(X)$. Here $\tilde{\theta}(f) = f \circ \theta$. We need to show that

$$\tilde{\theta}\left(\bigcap_{Q \in U} \mathcal{O}_Q(Y)\right) \subset \bigcap_{P \in \theta^{-1}(U)} \mathcal{O}_P(X).$$

Let $f \in \bigcap_{Q \in U} \mathcal{O}_Q(Y)$ and let $P \in \theta^{-1}(U)$. Let $Q = \theta(P)$. Since $Q \in U$ and $f \in \mathcal{O}_Q(Y)$, it follows that we may write $f = \frac{a}{b}$, where $a, b \in \Gamma(Y)$ and $b(Q) \neq 0$. Then $\tilde{\theta}(f) = f \circ \theta = \frac{a \circ \theta}{b \circ \theta}$. Clearly, $b \circ \theta(P) \neq 0$ and so $\tilde{\theta}(f) \in \mathcal{O}_P(X)$. Thus, given $f \in \bigcap_{Q \in U} \mathcal{O}_Q(Y)$, it follows

that $\tilde{\theta}(f) \in \bigcap_{P \in \theta^{-1}(U)} \mathcal{O}_P(X)$. This completes the proof that a polynomial map gives a morphism.

On the other hand, let us start with a morphism $\phi : X \to Y$ and show that it arises from a polynomial map. Consider the coordinate functions $\bar{Y}_1, \ldots, \bar{Y}_m \in \Gamma(Y)$. Let $G_i := \bar{Y}_i \circ \phi$. Since ϕ is a morphism, this means that $G_i \in \Gamma(X)$. If we choose lifts of G_i, say $\tilde{G}_i$, in $k[X_1, \ldots, X_n]$, then it is clear that we have the following commutative diagram:

$$\begin{array}{ccc} \mathbb{A}^n & \xrightarrow{(\tilde{G}_1,\ldots,\tilde{G}_m)} & \mathbb{A}^m \\ \uparrow & & \uparrow \\ X & \xrightarrow{\phi} & Y \end{array}$$

Thus, it follows that ϕ equals a polynomial map. It is easy to see that this establishes a bijection between the set of polynomial maps and the set of morphisms from $X \to Y$. □

Covering by affine varieties. Let $Y_1, \ldots, Y_{n+1}$ denote the homogeneous coordinates on $\mathbb{P}^n$. Let $y_1, \ldots, y_n$ denote coordinates on $\mathbb{A}^n$. Consider the open subset $\mathcal{U}_{n+1} := \{P \in \mathbb{P}^n \,|\, Y_{n+1}(P) \neq 0\}$. Recall the bijective map $\mathbb{A}^n \xrightarrow{\varphi} \mathcal{U}_{n+1}$ given by

$$(a_1, \ldots, a_n) \mapsto (a_1 : \ldots : a_n : 1)\,.$$

Proposition 6.3.3. *The above map is an isomorphism of varieties.*

Proof. We already saw in Remark 4.3.2 that this map is a homeomorphism. Let $V \subset \mathcal{U}_{n+1}$ be an open subset. Recall that the space of maps $V \to k$ was denoted by $\mathcal{F}(V, k)$. We have the map $\tilde{\varphi} : \mathcal{F}(V, k) \to \mathcal{F}(\varphi^{-1}(V), k)$ given by $\tilde{\varphi}(f) = f \circ \varphi$. Recall that the field of rational functions on $\mathbb{P}^n$ was defined to be the set F/G, where $F, G \in k[Y_1, \ldots, Y_{n+1}]$ are homogeneous of the same degree. Given such a rational function, it defines a map of sets $\mathbb{P}^n \setminus V(G) \to k$, and thus it may be viewed as an element of $\mathcal{F}(\mathbb{P}^n \setminus V(G), k)$. The effect of $\tilde{\varphi}$ on these rational functions is easily seen to be the following:

$$\frac{F(Y_1, \ldots, Y_{n+1})}{G(Y_1, \ldots, Y_{n+1})} \mapsto \frac{F}{G} \circ \varphi = \frac{F(y_1, \ldots, y_n, 1)}{G(y_1, \ldots, y_n, 1)} = \frac{F_*}{G_*}\,.$$

Note that for any homogeneous polynomial G, the polynomial $G(y_1, \ldots, y_n, 1) \neq 0$ and so the above makes sense. It is easily checked that this gives an isomorphism of fields

$$k(\mathcal{U}_{n+1}) \xrightarrow{\tilde{\varphi}} k(\mathbb{A}^n)\,.$$

It is also easily checked that, given a point $P \in \mathbb{A}^n$, the above map induces an isomorphism

$$\mathcal{O}_{\varphi(P)}(\mathcal{U}_{n+1}) \xrightarrow{\sim} \mathcal{O}_P(\mathbb{A}^n)\,.$$

If $V \subset \mathcal{U}_{n+1}$ is an open subset, it easily follows that $\tilde{\varphi}$ induces an isomorphism $\Gamma(V) \xrightarrow{\sim} \Gamma(\varphi^{-1}(V))$. □

Corollary 6.3.4. $\Gamma(\mathcal{U}_{n+1}) = k[\frac{Y_1}{Y_{n+1}}, \ldots, \frac{Y_n}{Y_{n+1}}]$.

Proof. The regular functions on $\mathcal{U}_{n+1}$ are precisely the pullbacks of regular functions from $\mathbb{A}^n$. The regular functions on $\mathbb{A}^n$ are $k[y_1, \ldots, y_n]$. □

Let $V \subset \mathbb{P}^n$ be a projective variety. Then $V_i = V \cap \mathcal{U}_i$ is a closed subset of $\mathcal{U}_i \cong \mathbb{A}^n$ and so is an affine variety. Also V_i is open in V. Since $\mathcal{U}_i$ cover $\mathbb{P}^n$, it follows that V_i cover V. Thus, every projective variety can be covered by affine open sets. In what follows, we will show that every variety can be covered by open sets which are affine.

Proposition 6.3.5. *Let V be an affine variety and let $f \in \Gamma(V)$, with $f \neq 0$. Consider the open subset $V_f = \{P \in V \mid f(P) \neq 0\}$. Then*

(1) $\Gamma(V_f) = \Gamma(V)[1/f] = \{a/f^n \mid a \in \Gamma(V), n \geq 0\}$.

(2) V_f is an affine variety.

Proof. Recall that $\Gamma(V_f)$ is defined as $\bigcap_{P \in V_f} \mathcal{O}_P(V)$. Clearly, $\{a/f^n \mid a \in \Gamma(V), n \geq 0\}$ is contained in $\bigcap_{P \in V_f} \mathcal{O}_P(V)$. Conversely, let $z \in \bigcap_{P \in V_f} \mathcal{O}_P(V)$. Consider the ideal $I = \{c \in \Gamma(V) \mid cz \in \Gamma(V)\}$. If $P \in V_f$, then $z \in \mathcal{O}_P(V)$ and so there exist $a, b \in \Gamma(V)$, $b(P) \neq 0$ and $z = a/b$. Thus, $b \in I$ and so $P \notin V(I)$. This shows $V(f)^c \subset V(I)^c$, that is, $V(I) \subset V(f)$. By Nullstellensatz, it follows that $\mathrm{Rad}(I) = I(V(I)) \supset I(V(f)) \ni f$. Thus, $\exists n$ such that $f^n \in I$. It follows that $f^n z \in \Gamma(V)$. Thus, $z = \frac{a}{f^n}$. This proves (1).

Let $V \subset \mathbb{A}^n$ and let $I \subset k[X_1, \ldots, X_n]$ denote the ideal of V. Consider the ideal $J \subset k[X_1, \ldots, X_n, X_{n+1}]$ given by $I + (1 - FX_{n+1})$, where F is a lift of f. Let $W = V(J) \subset \mathbb{A}^{n+1}$. Consider the projection map $\pi : \mathbb{A}^{n+1} \to \mathbb{A}^n$, $\pi(a_1, \ldots, a_{n+1}) = (a_1, \ldots, a_n)$. It is easy to check that π maps W bijectively onto V_f. Let us denote the restriction by $\pi' : W \to V_f$. It is also clear that π' is continuous, as it is the restriction of a continuous map. Let us show that π' is a closed map, which will prove it is a homeomorphism. Let $W \cap V(G_1, \ldots, G_r)$ be a closed subset of W. Here $G_i \in k[x_1, \ldots, x_{n+1}]$. Choose $N \gg 0$ so that $H_i := F^N G_i(X_1, \ldots, X_n, \frac{1}{F}) \in k[X_1, \ldots, X_n]$. We claim that $\pi'(W \cap V(G_1, \ldots, G_r)) = V_f \cap V(H_1, \ldots, H_r)$. Let $(a_1, \ldots, a_n)$ be in $\pi'(W \cap V(G_1, \ldots, G_r))$. Then $F(a_1, \ldots, a_n) \neq 0$ and $G_i(a_1, \ldots, a_n, \frac{1}{F(a_1, \ldots, a_n)}) = 0$, which shows that $(a_1, \ldots, a_n) \in V(H_1, \ldots, H_r)$. Conversely, suppose $(a_1, \ldots, a_n) \in V_f$ and $H_i(a_1, \ldots, a_n) = 0$. Then $F(a_1, \ldots, a_n) \neq 0$ and so $G_i(a_1, \ldots, a_n, \frac{1}{F(a_1, \ldots, a_n)}) = 0$, which shows that $(a_1, \ldots, a_n, \frac{1}{F(a_1, \ldots, a_n)}) \in W \cap V(G_1, \ldots, G_r)$. Clearly, this shows that $(a_1, \ldots, a_n) \in \pi'(W \cap V(G_1, \ldots, G_r))$. This proves π' is closed and so a homeomorphism.

Next we will try to understand $\tilde{\pi}' : \Gamma(V_f) \to \Gamma(W)$. Let π_1 denote the morphism $\pi_1 : W \to V$. Then we have a commutative diagram

$$\begin{array}{ccc} W & \xrightarrow{\pi_1} & V \\ {\scriptstyle \pi'}\downarrow & \nearrow & \\ V_f & & \end{array}$$

Since π_1 is a map between affine schemes, it corresponds to the ring homomorphism $\tilde{\pi}_1 : \Gamma(V) \to \Gamma(W)$. It is easy to see that

$$\begin{aligned} \Gamma(W) &\cong \Gamma(V)[X_{n+1}]/(1 - X_{n+1}f) \\ &\cong \Gamma(V)[1/f]. \end{aligned}$$

Under this isomorphism, $\tilde{\pi}_1$ corresponds to the canonical inclusion $\Gamma(V) \to \Gamma(V)[1/f]$. We also have the following commutative diagram

$$\begin{array}{ccccc} \Gamma(V)[1/f] & \xleftarrow{\cong} & \Gamma(W) & \xleftarrow{\tilde{\pi}_1} & \Gamma(V) \\ \| & & & \nwarrow^{\tilde{\pi}'} & \downarrow \\ \Gamma(V)[1/f] & & \xleftarrow{\cong} & & \Gamma(V_f) \end{array} \tag{6.3.6}$$

For each point $Q \in V_f$, we have the natural ring homomorphism

$$\Gamma(V_f) \to \mathcal{O}_Q(V) \to \mathbb{C}$$

given by evaluation at Q. Let $\mathfrak{m}_Q$ denote the kernel. Let $P \in W$ be the unique point such that $\pi'(P) = Q$, let $\mathfrak{m}_P \subset \Gamma(W)$ denote the kernel of the evaluation at P map. Then since $\pi'(P) = Q$, it is clear that $\tilde{\pi}'(\mathfrak{m}_Q) \subset \mathfrak{m}_P$. Since $\tilde{\pi}'$ is an isomorphism, it follows that $\tilde{\pi}'(\mathfrak{m}_Q) = \mathfrak{m}_P$. It follows that $\tilde{\pi}'$ induces an isomorphism of local rings

$$\left\{ \frac{a}{b} \mid a, b \in \Gamma(V_f), b \notin \mathfrak{m}_Q \right\} \xrightarrow{\sim} \left\{ \frac{\alpha}{\beta} \mid \alpha, \beta \in \Gamma(W), \beta \notin \mathfrak{m}_P \right\} = \mathcal{O}_P(W)\,.$$

We will show that $\left\{ \frac{a}{b} \mid a, b \in \Gamma(V_f), b \notin \mathfrak{m}_Q \right\} \cong \mathcal{O}_Q(V)$.

Consider the natural inclusion $\Gamma(V) \to \Gamma(V_f)$ given by $b \mapsto b|_{V_f}$. Let $b \in \Gamma(V)$ be such that $b(Q) \neq 0$. Then clearly, $b|_{V_f}(Q) \neq 0$ and so $b|_{V_f} \notin \mathfrak{m}_Q$. Thus, there is a natural inclusion

$$\mathcal{O}_Q(V) = \left\{ \frac{a}{b} \mid a, b \in \Gamma(V), b(Q) \neq 0 \right\} \hookrightarrow \left\{ \frac{a}{b} \mid a, b \in \Gamma(V_f), b(Q) \neq 0 \right\}\,.$$

Note that since $\Gamma(V_f) \cong \Gamma(V)[1/f]$, and $1/f \in \mathcal{O}_Q(V)$, it follows that all elements of the form $\frac{a}{1}$ in the RHS are in the image. If $b \in \Gamma(V_f)$ and $b(Q) \neq 0$, then we may write $b = \frac{c}{f^n}$, where $c \in \Gamma(V)$ and $c(Q) \neq 0$. Then $\frac{1}{b} \in \mathcal{O}_Q(V)$. Thus, $\frac{1}{b}$ is in the image. This shows that the above inclusion is a surjection. Let $P \in W$ and let $\pi_1(P) = Q \in V_f \subset V$. We conclude that the diagram (6.3.6) induces isomorphisms of local rings

$$\begin{array}{ccc} \mathcal{O}_P(W) & \xleftarrow{\tilde{\pi}_1} & \mathcal{O}_Q(V) \\ & \overset{\cong}{\nwarrow}^{\tilde{\pi}'} & \downarrow \cong \\ & & \{\frac{a}{b} \mid a, b \in \Gamma(V_f), b(Q) \neq 0\} \end{array}$$

Recall that $\mathcal{O}_Q(V_f)$ was defined to be $\mathcal{O}_Q(V)$. This in turn completes the proof that $\tilde{\pi}'$ induces an isomorphism of local rings $\mathcal{O}_Q(V_f) \to \mathcal{O}_P(W)$.

Using this we will show that π' is an isomorphism. We have already seen that $\tilde{\pi}'$ induces an isomorphism of domains $\Gamma(V_f) \to \Gamma(W)$, and so also of the corresponding fields of fractions. Viewing the local rings as sitting inside the fields of fractions, we get

$$\tilde{\pi}'(\bigcap_{Q \in V'} \mathcal{O}_Q(V)) = \bigcap_{Q \in V'} \tilde{\pi}'(\mathcal{O}_Q(V)) = \bigcap_{P \in \pi'^{-1}(V')} \mathcal{O}_P(W)\,.$$

Let $\phi : V_f \to W$ denote the inverse. We need to show that ϕ is a morphism. It suffices to show that for an open subset $U \subset W$, we have $\tilde{\phi}(\Gamma(U)) \subset \Gamma(\phi^{-1}(U))$, that is,

$$\tilde{\phi}(\bigcap_{P \in U} \mathcal{O}_P(W)) \subset \bigcap_{Q \in \pi'(U)} \mathcal{O}_Q(V)\,.$$

But $\tilde{\phi}(g) = g \circ \phi = g \circ \pi'^{-1}$. We have already seen that $\tilde{\pi}' : \mathcal{O}_Q(V) \xrightarrow{\cong} \mathcal{O}_P(W)$ is an isomorphism. It follows easily that $\tilde{\phi} = \tilde{\pi}'^{-1}$, which shows it is an isomorphism. This shows that $\tilde{\phi}(\bigcap_{P \in U} \mathcal{O}_P(W)) \subset \bigcap_{Q \in \pi'(U)} \mathcal{O}_Q(V)$.

This completes the proof of the Proposition. □

Corollary 6.3.7. *Let X be a variety and let $U \subset X$ be an open subset. Let $P \in U$. Then there is an affine open V containing P such that $V \subset U$.*

Proof. Since X is a variety, it is an open subset of X', where $X' \subset \mathbb{P}^n$ is a projective variety. Let $U_i \subset \mathbb{P}^n$ denote one of the coordinate open subsets such that $P \in U_i$. Then it suffices to find V containing P such that V is contained inside $U \cap U_i$. As $U \cap U_i$ is contained in $X' \cap U_i$, which is affine, we may replace X by $X' \cap U_i$, and assume it is affine,

and replace U by $U \cap U_i$. Thus, we reduce to the case where X is affine and $U \subset X$ is open. Let $X \setminus U = V(f_1, \ldots, f_r)$. Then $f_i(P) \neq 0$ for some i. Clearly $X \setminus U \subset V(f_i)$. Thus, $X \setminus V(f_i) \subset U$ and this is an open subset containing P. The previous proposition shows that $X \setminus V(f_i)$ is affine. This completes the proof of the Corollary. □

6.4 Products and Graphs

The first result we want to prove in this section is that if X and Y are varieties, then the set $X \times Y$ can be made into a variety. By this we mean the following: If $X \subset \mathbb{P}^n$ and $Y \subset \mathbb{P}^m$, then there is N such that:

(i) $X \times Y \subset \mathbb{P}^N$

(ii) The closure of $X \times Y$ in $\mathbb{P}^N$, say Z, is a variety (that is, the closure is irreducible)

(iii) $X \times Y$ is an open subset of Z.

Remark 6.4.1. It is important to emphasize that the product topology on $X \times Y$ will typically be very different from the subspace topology on $X \times Y$ induced by the Zariski topology on $\mathbb{P}^N$. □

To begin with, let $N = n + m + nm$ and consider the following map of sets

$$\mathbb{P}^n \times \mathbb{P}^m \xrightarrow{\varphi} \mathbb{P}^N ,$$

given by

$$((a_1 : \ldots : a_{n+1}), (b_1 : \ldots : b_{m+1})) \mapsto (a_i b_j)_{i,j} . \tag{6.4.2}$$

Proposition 6.4.3 (Segre embedding)**.** *The morphism φ is an inclusion whose image is a closed subset of $\mathbb{P}^N$. The morphism φ is called the Segre embedding.*

Proof. Let us denote the homogeneous coordinates on $\mathbb{P}^N$ by T_{ij}, where $1 \leqslant i \leqslant n+1$ and $1 \leqslant j \leqslant m+1$. First, this map is well-defined as a map of sets, as if $a_i \neq 0$ and $b_j \neq 0$, then $a_i b_j \neq 0$. It is clear that scaling (a_i) or (b_j) does not affect the image. Next, let us show that this map is an inclusion. Suppose $((a_i), (b_j))$ and $((a'_i), (b'_j))$ map to the same point. Then it follows that $a_i b_j \neq 0$ for some (i, j) and so $a'_i b'_j \neq 0$, as they are nonzero

scalar multiples of each other. Then

$$\begin{aligned}(a_0,\dots,a_n) &= \left(\frac{a_0}{a_i},\dots,\frac{a_i}{a_i},\dots,\frac{a_n}{a_i}\right)\\ (b_0,\dots,b_m) &= \left(\frac{b_0}{b_j},\dots,\frac{b_j}{b_j},\dots,\frac{b_m}{b_j}\right)\\ (a'_0,\dots,a'_n) &= \left(\frac{a'_0}{a'_i},\dots,\frac{a'_i}{a'_i},\dots,\frac{a'_n}{a'_i}\right)\\ (b'_0,\dots,b'_m) &= \left(\frac{b'_0}{b'_j},\dots,\frac{b'_j}{b'_j},\dots,\frac{b'_m}{b'_j}\right).\end{aligned}$$

We compute $\varphi((a_i),(b_j))$ and $\varphi((a'_i),(b'_j))$ using these coordinates. Since the (i,j) coordinate is 1 for both of them, it follows that the other coordinates have to be the same. Thus, it follows that the $(i\ell)$ coordinates are equal for all ℓ, that is,

$$\frac{a_i}{a_i}\frac{b_\ell}{b_j} = \frac{a'_i}{a'_i}\frac{b'_\ell}{b'_j} \implies \frac{b_\ell}{b_j} = \frac{b'_\ell}{b'_j} \quad \forall \ell.$$

Similarly, looking at the (ℓj) coordinate we get

$$\frac{a_\ell}{a_i} = \frac{a'_\ell}{a'_i}\ \forall \ell\,.$$

This shows that $(a_i) = (a'_i)$ and $(b_j) = (b'_j)$. This proves injectivity.

Finally we want to prove that the image of φ equals $V(T_{ij}T_{rs} - T_{is}T_{rj})_{i,j,r,s}$. Since $(a_ib_j)(a_rb_s) - (a_ib_s)(a_rb_j) = 0$ it is clear that $\mathrm{Im}(\varphi) \subset V(T_{ij}T_{rs} - T_{is}T_{rj})_{i,j,r,s}$. Conversely, suppose $(a_{ij}) \in V(T_{ij}T_{rs} - T_{is}T_{rj})_{i,j,r,s}$. One of the $a_{ij} \neq 0$. Define $c_\ell = \frac{a_{\ell j}}{a_{ij}}$ and $d_s = \frac{a_{is}}{a_{ij}}$. Clearly, $(c_\ell) \in \mathbb{P}^n$ and $(d_s) \in \mathbb{P}^m$.

$$\varphi((c_\ell),(d_s)) = (c_\ell d_s)_{\ell,s} = \left(\frac{a_{\ell j}}{a_{ij}} \cdot \frac{a_{is}}{a_{ij}}\right) = \left(\frac{a_{\ell s}\cdot a_{ij}}{a_{ij}\cdot a_{ij}}\right) = \left(\frac{a_{\ell s}}{a_{ij}}\right) = (a_{\ell s})\,.$$

This proves that $\mathrm{Im}(\varphi) = V(T_{ij}T_{rs} - T_{is}T_{rj})_{i,j,r,s}$. This completes the proof of the Proposition. □

Remark 6.4.4. Let F be a homogeneous polynomial of degree d in the variables T_{ij}. We want to describe the intersection of $V(F) \subset \mathbb{P}^N$ with $\mathbb{P}^n \times \mathbb{P}^m$. It is clear that this intersection is the set of points (a,b) such that $F(a_ib_j) = 0$. When we substitute $T_{ij} = X_iY_j$, we get that $F(X_iY_j)$ is a polynomial in X_i and Y_j of the type

$$\sum_i F_iG_i\,,$$

where each F_i is a homogeneous polynomial of degree d in $X_1, \ldots, X_{n+1}$ and each G_i is a homogeneous polynomial of degree d in $Y_1, \ldots, Y_{n+1}$. Thus,

$$V(F) \cap \mathbb{P}^n \times \mathbb{P}^m$$

is the vanishing loci of a bihomogeneous polynomial. Conversely, suppose we are given a polynomial $H \in k[X_1, \ldots, X_{n+1}, Y_1, \ldots, Y_{n+1}]$, such that

$$H = \sum_i F_i G_i \,,$$

where each F_i is a homogeneous polynomial of degree d in $X_1, \ldots, X_{n+1}$ and each G_i is a homogeneous polynomial of degree d in $Y_1, \ldots, Y_{n+1}$. Then it is easy to see that there is a homogeneous $F \in k[T_{ij}]_{i,j}$ of degree d such that $F(X_i Y_j) = H$. Thus, it follows that the closed subsets of $\mathbb{P}^n \times \mathbb{P}^m$ are precisely the vanishing loci of such bihomogeneous polynomials. □

Lemma 6.4.5. *Let $A \subset \mathbb{P}^n$ and $B \subset \mathbb{P}^m$ be closed subsets. Then $A \times B$ is a closed subset of $\mathbb{P}^N$ under the Segre embedding. Moreover, if A and B are also irreducible, then so is $A \times B$.*

Proof. Note that $A \times B = (A \times \mathbb{P}^m) \cap (\mathbb{P}^n \times B)$. Since the intersection of closed sets is closed, it suffices to show that $A \times \mathbb{P}^m$ and $\mathbb{P}^n \times B$ are closed subsets. Since A is an intersection of hypersurfaces, it suffices to show that $V(F) \times \mathbb{P}^m$ is a closed subset. Let the homogeneous coordinates on $\mathbb{P}^n$ be $X_1, \ldots, X_{n+1}$ and let the homogeneous coordinates on $\mathbb{P}^m$ be $Y_1, \ldots, Y_{m+1}$. Let F be a homogeneous polynomial in the variables X_i of $\deg(F) = d$. For any j, consider the polynomial $F \cdot Y_j^d$. This is bihomogeneous of bidegree (d, d). We claim that the vanishing locus of the polynomials $FY_1^d, \ldots, FY_{m+1}^d$ inside $\mathbb{P}^n \times \mathbb{P}^m$ is precisely the set $V(F) \times \mathbb{P}^m$. A point in this vanishing locus is of the type $R = (P, Q) \in \mathbb{P}^n \times \mathbb{P}^m$ such that $F(P)Y_j(Q)^d = 0$ for all j. Since there is j such that $Y_j(Q) \neq 0$, it follows that $F(P) = 0$. Thus, $P \in V(F)$. Conversely, it is clear that $V(F) \times \mathbb{P}^m$ is in the vanishing locus of the above polynomials. From Remark 6.4.4, it follows that $V(F) \times \mathbb{P}^m$ is closed in the topology coming from the Segre embedding. The case of $\mathbb{P}^n \times B$ is similar. This proves that $A \times B$ is a closed subset.

Next we will show that $A \times B$ is irreducible. For this we will need a few preliminary results.

Fix a point $a \in A$. On the set $a \times B$, which is naturally identified with B, we have two topologies. The first one, which we denote $\mathcal{Z}_1$, is the subspace topology on B coming from the inclusion $B \subset \mathbb{P}^m$. The second one, which we denote $\mathcal{Z}_2$, is the subspace topology on B coming from the inclusion $a \times B \subset \mathbb{P}^N$. We claim that both these topologies are the

same. We will use Remark 6.4.4. The closed subsets in $\mathcal{Z}_2$ are precisely the vanishing loci of bihomogeneous polynomials of bidegree (d, d) restricted to $a \times B$. But it is clear that the restriction is a homogeneous polynomial of degree d in the variables Y_j. It follows that $\mathcal{Z}_2 \subset \mathcal{Z}_1$. Conversely, given a closed subset $C \subset B$ in $\mathcal{Z}_1$, from what we have just seen, the subset $a \times C$ is closed in the topology $\mathcal{Z}_2$. This shows that $\mathcal{Z}_1 \subset \mathcal{Z}_2$. Thus, both topologies are the same. Since $B \subset \mathbb{P}^m$ is irreducible, it follows that $a \times B \subset \mathbb{P}^N$ is irreducible.

Next let $A_1 \subset A$. Let F be a homogeneous polynomial in the variables T_{ij}. Assume that F vanishes on the set $A_1 \times B$. We claim that it also vanishes on the set $\overline{A_1} \times B$. Fix a point $b \in B$. As we saw before, the restriction of F to $\mathbb{P}^n \times b$ is a homogeneous polynomial in X_i, let us call it G. Since G vanishes on A_1, it is clear that G also vanishes on $\overline{A_1} \times b$. Thus, it follows that F vanishes on $\overline{A_1} \times b$. Since this happens for all $b \in B$, it follows that F vansihes on $\overline{A_1} \times B$. This proves the claim. This also shows that if $Z \subset \mathbb{P}^N$ is a closed subset which contains $A_1 \times B$, then it also contains $\overline{A_1} \times B$.

Now we return to proving that $A \times B$ is irreducible. Let us assume that there are closed subsets Z_1 and Z_2 such that $A \times B \subset Z_1 \cup Z_2$. Fix $a \in A$. It follows that $a \times B \subset Z_1 \cup Z_2$. Since $a \times B$ is irreducible, it follows that it is either contained in Z_1 or in Z_2. Let A_i be the set of points such that $a \times B$ is contained in Z_i. We have proved that $A = A_1 \cup A_2$. Since $A_i \times B \subset Z_i$, the discussion in the preceding paragraph shows that $\bar{A}_i \times B \subset Z_i$. Thus, it follows that A_1 and A_2 are closed subsets of A. Since A is irreducible, it follows that one of these is equal to A, and so we get that one of the Z_i equals $A \times B$. This proves that $A \times B$ is a variety. □

Proposition 6.4.6. *Let $A \subset \mathbb{P}^n$ and $B \subset \mathbb{P}^m$ be varieties. Then $A \times B$ is a variety.*

Proof. As mentioned in the beginning of this section, we need to show the following: There is N such that:

(i) $X \times Y \subset \mathbb{P}^N$

(ii) The closure of $X \times Y$ in $\mathbb{P}^N$, say Z, is a variety (that is, the closure is irreducible)

(iii) $X \times Y$ is an open subset of Z.

Let $A \subset \bar{A} \subset \mathbb{P}^n$ denote the closure of A and let $B \subset \bar{B} \subset \mathbb{P}^m$ denote the closure of B. Then $\bar{A} \times \bar{B} \subset \mathbb{P}^N$ is a closed subvariety. Let $A_1 := \bar{A} \setminus A$ and let $B_1 := \bar{B} \setminus B$. Then A_1 is a closed subset of $\mathbb{P}^n$ and B_1 is a closed subset of $\mathbb{P}^m$. The previous Lemma shows that $\bar{A} \times \bar{B}$ is a closed irreducible subset of $\mathbb{P}^N$. Moreover, $A_1 \times \bar{B}$ and $\bar{A} \times B_1$ are closed subsets of $\mathbb{P}^N$. Thus, it follows that

$$A \times B = (\bar{A} \times \bar{B}) \setminus ((A_1 \times \bar{B}) \cup (\bar{A} \times B_1))$$

is an open subset of $\bar{A} \times \bar{B}$ and so is irreducible by Lemma 6.2.3. This completes the proof of the Proposition. □

Exactly the way we do in topology, there are some very natural maps, and we want to prove that these are morphisms in our category. To begin with, we will need the following preliminary results.

Lemma 6.4.7. *Let X and Y be varieties. Let $f : X \to Y$ be a maps of sets. Suppose we can find open coverings $X = \cup_i U_i$ and $Y = \cup_i V_i$ such that for each i, we have $f(U_i) \subset V_i$. Then f is a morphism iff for each i the restriction $f : U_i \to V_i$ is a morphism.*

Proof. It is clear that if f is a morphism then for each i, the restriction of f to U_i is a morphism. Next, assume that the restriction of f to each U_i is a morphism. If V is an open subset of Y, then to check that $f^{-1}(V)$ is open, it suffices to check that $f^{-1}(V) \cap U_i$ is open in U_i for each i. This is true as $f^{-1}(V) \cap U_i = f^{-1}(V \cap V_i) \cap U_i$. Thus, the first condition for f being a morphism is satisfied. Let us consider the second condition. For each open subset $V \subset Y$ we need to show that $\tilde{f}(\Gamma(V)) \subset \Gamma(f^{-1}(V))$. Recall the definition

$$\Gamma(V) = \bigcap_{P \in V} \mathcal{O}_P(Y)\,, \qquad \Gamma(f^{-1}(V)) = \bigcap_{Q \in f^{-1}(V)} \mathcal{O}_Q(X)\,.$$

Let $\theta \in \Gamma(V)$. Let $Q \in f^{-1}(V)$ and let $P = f(Q)$. Assume that $Q \in U_i$ for some i. Then $P = f(Q) \in f(U_i) \subset V_i$. Since $f : U_i \to V_i$ is a morphism, it follows that

$$\tilde{f}(\Gamma(V_i \cap V)) \subset \Gamma(U_i \cap f^{-1}(V)) \subset \mathcal{O}_Q(X)\,.$$

Clearly, $\theta \in \Gamma(V_i \cap V)$ and so $\tilde{f}(\theta) \in \Gamma(U_i \cap f^{-1}(V))$. It follows that $\tilde{f}(\theta) \in \mathcal{O}_Q(X)$ for all $Q \in f^{-1}(V)$. This proves that $\tilde{f}(\Gamma(V)) \subset \Gamma(f^{-1}(V))$. This completes the proof of the Lemma. □

The following basic facts are easily checked, and these are left to the reader as exercises.

Lemma 6.4.8.

(1) If $U \hookrightarrow X$ is the inclusion of an open subset then it is a morphism.

(2) If $X \hookrightarrow Y$ is the inclusion of a closed subset, then it is a morphism.

(3) Let $X \xrightarrow{\varphi} Y$ be a morphism. If $U \subset Y$ is open and $\varphi(X) \subset U$, then φ factors as

$$\begin{array}{ccc} X & \xrightarrow{\varphi} & Y \\ {\scriptstyle \varphi_1}\downarrow & \nearrow_{i} & \\ U & & \end{array}$$

where φ_1 is a morphism.

(4) Let $X \xrightarrow{\varphi} Y$ be a morphism. If $Z \subset Y$ is closed and $\varphi(X) \subset Z$, then φ factors as

$$\begin{array}{ccc} X & \xrightarrow{\varphi} & Y \\ {\scriptstyle\varphi_1}\downarrow & \nearrow_{i} & \\ Z & & \end{array}$$

where φ_1 is a morphism.

(5) Composite of morphisms is a morphism.

Next we will show that $\mathbb{A}^n \times \mathbb{A}^m$ is isomorphic to $\mathbb{A}^{n+m}$. Note that the variety structure on $\mathbb{A}^n \times \mathbb{A}^m$ *a priori* comes from a seemingly complicated embedding $\mathbb{A}^n \times \mathbb{A}^m \hookrightarrow \mathbb{P}^N$.

Lemma 6.4.9. *$\mathbb{A}^n \times \mathbb{A}^m$ is isomorphic to $\mathbb{A}^{n+m}$.*

Proof. Recall the embedding $\mathbb{A}^n \times \mathbb{A}^m \xrightarrow{\varphi} \mathbb{P}^N$ is given by

$$(a_1, a_2, \ldots, a_n) \times (b_1, \ldots, b_m) \mapsto (a_1 : a_2 : \cdots : a_n : 1) \times (b_1 : b_2 : \cdots : b_m : 1) \mapsto (a_i b_j)$$

It is clear that the image lands inside the affine open $\{T_{n+1,m+1} \neq 0\} \cong \mathbb{A}^N$ (see Proposition 6.3.3). Thus, by Lemma 6.4.8, this morphism factors as

$$\mathbb{A}^n \times \mathbb{A}^m \xrightarrow{\varphi_1} \mathbb{A}^N \hookrightarrow \mathbb{P}^N .$$

Recall from Corollary 6.3.4 that the affine coordinates on $\mathbb{A}^N$ are $T_{ij}/T_{n+1,m+1}$. From $T_{i,m+1}/T_{n+1,m+1}$ we may recover the a_i's and from the coordinates $T_{n+1,j}/T_{n+1,m+1}$ we may recover the b_j's. It follows easily that the image $\varphi_1(\mathbb{A}^n \times \mathbb{A}^m)$ is the closed subset Y given by the vanishing of the equations

$$\left\{ \frac{T_{ij}}{T_{n+1,m+1}} - \frac{T_{i,m+1}T_{n+1,j}}{T_{n+1,m+1}^2} \right\}_{i,j} .$$

The variety $\mathbb{A}^n \times \mathbb{A}^m$ is, by definition, the variety Y. We need to show that Y is isomorphic to $\mathbb{A}^{n+m}$. Thus, we have the following morphisms:

$$\begin{array}{ccc} Y & \xrightarrow{\psi} & \mathbb{A}^{n+m} \\ \downarrow{\scriptstyle i} & & \| \\ \mathbb{A}^N & \xrightarrow{\pi} & \mathbb{A}^{n+m} \end{array}$$

The map π is the projection onto the coordinates which give the a_i and the b_j. Since π is a polynomial map, it is a morphism. Since i is the inclusion of a closed subset, it follows

that it is a morphism. Thus, using Lemma 6.4.8, it follows that ψ is a morphism. We can give a map $\tilde{f} : \mathbb{A}^{n+m} \to \mathbb{A}^N$ using the same definition of φ. Clearly, this is a polynomial map and so a morphism. It is also clear that the image lands in Y, and so, again using Lemma 6.4.8, we get a morphism $f : \mathbb{A}^{n+m} \to Y$. It is easily checked that f and ψ are inverses of each other and so isomorphisms. At the level of points, this isomorphism $\mathbb{A}^n \times \mathbb{A}^m \to \mathbb{A}^{n+m}$ is given by

$$((a_1, \ldots, a_n), (b_1, \ldots, b_m)) \mapsto (a_1, \ldots, a_n, b_1, \ldots, b_m) .$$

This completes the proof of the Lemma. □

Recall the Segre embedding $\varphi : \mathbb{P}^n \times \mathbb{P}^m \hookrightarrow \mathbb{P}^N$ from (6.4.2). The intersection of the hyperplane $\{T_{n+1,m+1} = 0\}$ with the image equals

$$\varphi(\mathbb{P}^n \times \mathbb{P}^m) \cap \{T_{n+1,m+1} = 0\} = \varphi\left(\{X_{n+1} = 0\} \times \mathbb{P}^m \bigcup \mathbb{P}^n \times \{Y_{m+1} = 0\}\right) .$$

Thus,

$$\begin{aligned} \varphi(\mathbb{P}^n \times \mathbb{P}^m) \cap \{T_{n+1,m+1} \neq 0\} &= \varphi\left(\{X_{n+1} \neq 0\} \times \mathbb{P}^m \bigcap \mathbb{P}^n \times \{Y_{m+1} \neq 0\}\right) \\ &= \varphi(\mathbb{A}^n \times \mathbb{A}^m) \end{aligned}$$

Lemma 6.4.10. *Let $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ be affine varieties. Then $X \times Y$ is an affine variety. The coordinate ring of $X \times Y$ is isomorphic to $k[X_1, \ldots, X_n, Y_1, \ldots, Y_m]/(I(X), I(Y))$.*

Proof. Let $\bar{X} \subset \mathbb{P}^n$ and $\bar{Y} \subset \mathbb{P}^m$ denote the closures of X and Y. Then using Proposition 4.3.1,

$$X = \bar{X} \cap \mathbb{A}^n , \qquad \text{and} \qquad Y = \bar{Y} \cap \mathbb{A}^m .$$

It follows that

$$X \times Y = (\bar{X} \cap \mathbb{A}^n) \times (\bar{Y} \cap \mathbb{A}^m) = (\bar{X} \times \bar{Y}) \cap (\mathbb{A}^n \times \mathbb{A}^m) .$$

Thus,

$$\varphi(X \times Y) = \varphi(\bar{X} \times \bar{Y}) \cap \varphi(\mathbb{A}^n \times \mathbb{A}^m) \subset \mathbb{P}^N .$$

Recall that the variety structure on $X \times Y$ is, by definition, the one it inherits from $\varphi(X \times Y)$. Similarly, for $\bar{X} \times \bar{Y}$ and $\mathbb{A}^n \times \mathbb{A}^m$. We saw in the previous Lemma that $\mathbb{A}^n \times \mathbb{A}^m$ is an affine variety. We have already seen that $\bar{X} \times \bar{Y}$ is a closed subset of $\mathbb{P}^N$. Thus, it follows that $X \times Y$, being a closed subset of an affine variety, is again an affine variety.

It is trivial to check that under the isomorphism $\mathbb{A}^n \times \mathbb{A}^m \to \mathbb{A}^{n+m}$, the image of $X \times Y$ is equal to $V(I(X), I(Y))$. Here $k[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$ is the coordinate ring of $\mathbb{A}^{n+m}$. Thus, by Nullstellensatz, $I(X \times Y) = \mathrm{Rad}(I(X), I(Y))$. Thus, to complete the proof of the Lemma, it suffices to show that $(I(X), I(Y))$ is a prime ideal. Let A denote the ring $k[X_1, \ldots, X_n]/I(X)$ and let B denote the ring $k[Y_1, \ldots, Y_m]/I(Y)$. Let R denote the ring

$$k[X_1, \ldots, X_n, Y_1, \ldots, Y_m]/(I(X), I(Y))\,.$$

A nonzero element of R may be written as

$$\sum_i a_i b_i$$

where a_i are polynomials involving only the variables X_i and b_i are polynomials involving only the variables Y_j. We may assume that the b_i are linearly independent over k in B, and that at least one of the a_i is nonzero in A. Similarly, let another nonzero element be

$$\sum_i c_i d_i\,.$$

Again, c_i are polynomials involving only the variables X_i and d_i are polynomials involving only the variables Y_j. We may assume that the d_i are linearly independent over k in B, and that at least one of the c_i is nonzero in A. Now suppose their product is 0 in R. Let P be a point in X. We may restrict the function $(\sum a_i b_i)(\sum c_i d_i)$ to $\{P\} \times Y$. Let $\mathfrak{m}_P \subset k[X_1, \ldots, X_n]$ denote the ideal of P. Then $I(X) \subset \mathfrak{m}_P$. Moreover, $\mathfrak{m}_P = (X_1 - \lambda_1, \ldots, X_n - \lambda_n)$. Consider the ring homomorphism

$$k[X_1, \ldots, X_n, Y_1, \ldots, Y_m] \to B\,,$$

which sends $X_i \mapsto \lambda_i$ and $Y_i \mapsto Y_i$. Clearly, the kernel contains $\mathfrak{m}_P$ and $I(Y)$. It follows that this induces the "restriction to $\{P\} \times Y$" map $R \to B$. Then looking at the image of $(\sum a_i b_i)(\sum c_i d_i)$, we get

$$(\sum_i a_i(P) b_i)(\sum_i c_i(P) d_i) = 0\,.$$

Since B is a domain, it follows that one of these is zero, say the first one. But since the b_i were linearly independent over k, it follows that all the $a_i(P)$ are 0. Thus, it follows that for each point $P \in X$, either $P \in V(a_1, a_2, \ldots)$ or $P \in V(c_1, c_2, \ldots)$. We may assume that $a_1 \neq 0$ and that $c_1 \neq 0$. It follows that $X = V(a_1) \cup V(c_1)$. Both these are proper closed subsets and this contradicts the irreducibility of X. This completes the proof of the Lemma. $\square$

Lemma 6.4.11. *Let X and Y be affine varieties. Then the projection maps $X \times Y \to X$ and $X \times Y \to Y$ are morphisms.*

Proof. It is clear that the projections are restrictions of the projections $\mathbb{A}^{n+m} \to \mathbb{A}^n$ and $\mathbb{A}^{n+m} \to \mathbb{A}^m$. Thus, it follows that these are polynomial maps and so morphisms. At the level of coordinate rings, this corresponds to the map

$$k[X_1, \ldots, X_n]/I(X) \to k[X_1, \ldots, X_n, Y_1, \ldots, Y_m]/(I(X), I(Y)) .$$

□

Proposition 6.4.12.

(1) The projections $pr_1 : X \times Y \to X$ and $pr_2 : X \times Y \to Y$ are morphisms.

(2) If $f : Z \to X$, $g : Z \to Y$ are morphisms, then $(f, g) : Z \to X \times Y$ defined by $(f, g)(z) = (f(z), g(z))$ is a morphism.

(3) If $f : X_0 \to X$, $g : Y_0 \to Y$ are morphisms, then $f \times g : X_0 \times Y_0 \to X \times Y$ defined by $(f \times g)(x_0, y_0) = (f(x_0), g(y_0))$ is a morphism.

(4) The diagonal $\Delta_X = \{(x, y) \in X \times X \mid y = x\}$ is a closed subvariety of $X \times X$, and the diagonal map $\delta_X : X \to \Delta_X$ defined by $\delta_X(x) = (x, x)$ is an isomorphism.

Proof. Recall that we may cover X and Y by affine open subsets using Corollary 6.3.7. Now the first assertion follows from Lemma 6.4.7 and Lemma 6.4.11.

For the second assertion, we may find affine open coverings $X = \cup_i X_i$, $Y = \cup_i Y_i$ and $Z = \cup_i Z_i$ such that $f(Z_i) \subset X_i$ and $g(Z_i) \subset Y_i$. By Lemma 6.4.7, it suffices to show that $Z_i \to X_i \times Y_i$ is a morphism. If $X_i \subset \mathbb{A}^n$ and $Y_i \subset \mathbb{A}^m$, then the map $f : Z_i \to X_i$ is given by polynomials $f = (f_1, \ldots, f_n)$. Similarly, $g = (g_1, \ldots, g_m)$. Putting these together, we get a $Z_i \to \mathbb{A}^{n+m}$ and the image is clearly $X_i \times Y_i$. Lemma 6.4.8 now says that this is a morphism $Z_i \to X_i \times Y_i$. We use Lemma 6.4.7 to conclude (2).

The third assertion follows similarly.

We prove the fourth assertion. If we can show that $\Delta_{\mathbb{P}^n}$ is a closed subspace of $\mathbb{P}^n \times \mathbb{P}^n$ then it follows that $\Delta_X = \Delta_{\mathbb{P}^n} \cap (X \times X)$ is a closed subspace of $X \times X$. One easily checks that $\Delta_{\mathbb{P}^n}$ equals

$$V(T_{ij} - T_{ji})_{i,j} \cap (\mathbb{P}^n \times \mathbb{P}^n) .$$

From (2) it follows that $X \to \Delta_X$ is a morphism. The inverse of this map is the restriction of the first projection, $pr_1 : \Delta_X \to X$, which is a morphism by (1) and Lemma 6.4.8. □

Corollary 6.4.13. *If $f, g : X \to Y$ are morphisms of varieties, then $\{x \in X \mid f(x) = g(x)\}$ is closed in X. If f and g agree on a dense set of X, then $f = g$.*

Proof. $\{x \mid f(x) = g(x)\} = (f,g)^{-1}(\Delta_Y)$. □

If $f : X \to Y$ is a morphism of varieties, the **graph of** f, $G(f)$, is defined to be

$$G(f) = \{(x,y) \in X \times Y \mid y = f(x)\}.$$

Proposition 6.4.14. *$G(f)$ is a closed subvariety of $X \times Y$. The projection of $X \times Y$ onto X restricts to an isomorphism of $G(f)$ with X.*

Proof. We have $G(f) = (f \times i)^{-1}(\Delta_Y)$, where i is the identity on Y. Now $(j,f) : X \to X \times Y$, where j is the identity on X, maps X onto $G(f)$, and this is inverse to the projection to X. □

6.5 Algebraic Function Fields and Dimension of Varieties

Let K be a finitely generated field extension of k. The **transcendence degree** of K over k, written **tr deg**$_k K$, is defined to be the smallest integer n such that for some $x_1, \ldots, x_n \in K$, K is algebraic over $k(x_1, \ldots, x_n)$. We say then that K is an **algebraic function field** in n variables over k.

Proposition 6.5.1. *Let K be an algebraic function field over k in one variable. Let $x \in K \setminus k$. Then*

(1) K is algebraic over $k(x)$.

(2) There is an element $y \in K$ such that $K = k(x,y)$.

(3) If $k \subset R \subset K$ is a domain with quotient field K, and $\mathfrak{p}$ is a prime ideal in R, $0 \neq \mathfrak{p} \neq R$, then the natural homomorphism from k to $R/\mathfrak{p}$ is an isomorphism.

Proof. (1) Take any $t \in K$ so that K is algebraic over $k(t)$. Since x is algebraic over $k(t)$, there is a polynomial $F \in k[T,X]$ such that $F(t,x) = 0$ (clear denominators if necessary). Since x is not algebraic over k (Exercise 1.11.45), T must appear in F, so t is algebraic over $k(x)$. Then $k(x,t)$ is algebraic over $k(x)$ (Exercise 1.11.47), so K is algebraic over $k(x)$ (Exercise 1.11.43).
(2) Since $\mathrm{char}(k(x)) = 0$, this is an immediate consequence of the "Theorem of the Primitive Element."
(3) Suppose there is an $x \in R$ whose residue $\bar{x}$ in $R/\mathfrak{p}$ is not in k. Let $y \in \mathfrak{p}$, $y \neq 0$. Since y is algebraic over $k(x)$, there is $F = \sum a_i(X)Y^i \in k[X,Y]$ so that $F(x,y) = 0$. If we

choose F of lowest possible degree, then $a_0(X) \neq 0$. But then $a_0(x) \in \mathfrak{p}$, so $a_0(\bar{x}) = 0$. In other words, $\bar{x}$ is a root of the polynomial $a_0(X) \in k[X]$. Since k is algebraically closed, it follows that $\bar{x} \in k$, which is a contradiction. □

If X is a variety, $k(X)$ is a finitely generated extension of k. Define the **dimension** of X, denoted $\dim(X)$, to be

$$\dim(X) := \text{tr. deg}_k k(X)\,.$$

A variety of dimension one is called a **curve**, of dimension two a **surface**, etc.

Proposition 6.5.2.

(1) If U is an open subvariety of X, then $\dim U = \dim X$.

(2) If V^* is the projective closure of an affine variety V, then $\dim V = \dim V^*$.

(3) A variety has dimension zero if and only if it is a point.

(4) Every proper closed subvariety of a curve is a point.

(5) A closed subvariety of $\mathbb{A}^2$ (resp. $\mathbb{P}^2$) has dimension one if and only if it is an affine (resp. projective) plane curve.

Proof. (1) and (2) follow from the fact that the varieties have the same function fields.
(3): Suppose $\dim V = 0$. By (1) we may assume that V is affine by (1). Then $k(V)$ is algebraic over k, so $k(V) = k$, so $\Gamma(V) = k$. Since the coordinate ring of a point and that of V are isomorphic as k-algebras, and both are affine, it follows that they are isomorphic.
(4): Again we may assume V is affine. If W is a closed subvariety of V, let $R = \Gamma(V)$ and let $\mathfrak{p}$ be the prime ideal of R corresponding to W. Then $\Gamma(W) = R/\mathfrak{p}$. Now apply Proposition 6.5.1 (3).
(5): Assume $V \subset \mathbb{A}^2$. By Proposition 6.5.1 (2), $k(V) = k(x, y)$. Thus, $\dim V$ must be 0, 1, or 2. Assume that V is a curve. Then $\Gamma(V) = k[X, Y]/(F(X, Y))$ for some irreducible polynomial F. Thus, $F(x, y) = 0$ in $k(x, y)$ and so $\dim(V) = \text{tr. deg}_k k(V) \leqslant 1$. Using (3), $\dim(V) \neq 0$. Thus, $\dim(V) = 1$. Conversely, suppose $\dim(V) = 1$, then V cannot be a point, by (3), or all of $\mathbb{A}^2$, since $\dim(\mathbb{A}^2) = 2$. By Corollary 1.6.3, V is a plane curve. For a closed subvariety of $\mathbb{P}^2$, we intersect with a coordinate affine open set and use (1) to reduce to this case. □

6.6 Rational Maps

Let X, Y be varieties. Two morphisms $f_i : U_i \to Y$ from open subvarieties U_i of X to Y are said to be **equivalent** if their restrictions to $U_1 \cap U_2$ are the same. Since $U_1 \cap U_2$ is dense in X (Corollary 6.2.2), each f_i is determined by its restriction to $U_1 \cap U_2$ (Corollary 6.4.13). An equivalence class of such morphisms is called a **rational map** from X to Y. Given such an equivalence class, there is an obvious way to construct a morphism on an open subset of X. Let $\{(U_\alpha, f_\alpha)\}_\alpha$ be an equivalence class. Take $U = \cup_\alpha U_\alpha$ and define $f : U \to Y$ by defining it to be f_α on U_α. The open subset U is called the **domain** of the rational map. Clearly, U is the largest open subset on which the rational map can be defined.

A rational map from X to Y is said to be **dominating** if $f(U)$ is dense in Y, where $f : U \to Y$ is any morphism representing the map (it is easy to see that this is independent of U).

If A and B are local rings, and A is a subring of B, we say that B **dominates** A if the maximal ideal of B contains the maximal ideal of A.

Proposition 6.6.1. *(1) Let F be a dominating rational map from X to Y. Let $U \subset X$, $V \subset Y$ be affine open sets, $f : U \to V$ a morphism that represents F. Then the induced map $\tilde{f} : \Gamma(V) \to \Gamma(U)$ is one-to-one, so $\tilde{f}$ extends to a one-to-one homomorphism from $k(Y) = k(V)$ into $k(X) = k(U)$. This homomorphism is independent of the choice of f, and is denoted by $\tilde{F}$.*

(2) If P belongs to the domain of F, and $F(P) = Q$, then $\mathcal{O}_P(X)$ dominates $\tilde{F}(\mathcal{O}_Q(Y))$. Conversely, if $P \in X$, $Q \in Y$, and $\mathcal{O}_P(X)$ dominates $\tilde{F}(\mathcal{O}_Q(Y))$, then P belongs to the domain of F, and $F(P) = Q$.

(3) Any homomorphism from $k(Y)$ into $k(X)$ is induced by a unique dominating rational map from X to Y.

Proof. (1) Let $g : V \to k$ be a morphism such that $\tilde{f}(g) = g \circ f = 0$. Since $f(U)$ is dense in V, it follows from Corollary 6.4.13, that $g = 0$. This proves injectivity. If $f_1 : U_1 \to V_1$ and $f_2 : U_2 \to V_2$ are representatives of F, then we can find affine open subsets $V_3 \subset V_1 \cap V_2$ and $U_3 \subset U_1 \cap U_2$ such that $f_1 = f_2 : U_3 \to V_3$. We have the following coommutative diagram

$$\begin{array}{ccccc} \Gamma(V_1) & \longrightarrow & \Gamma(V_3) & \longleftarrow & \Gamma(V_2) \\ {\scriptstyle \tilde{f}_1}\downarrow & & \downarrow & & \downarrow{\scriptstyle \tilde{f}_2} \\ \Gamma(U_1) & \longrightarrow & \Gamma(U_3) & \longleftarrow & \Gamma(U_2) \end{array}$$

From this the second assertion follows.

(2) Suppose P belongs to the domain of F, and $F(P) = Q$. Take affine neighborhoods V of P, W of Q and a representative $f : V \to W$. We get $\tilde{f} : \Gamma(W) \to \Gamma(V)$. Let $\mathfrak{m}_Q \subset \Gamma(W)$ denote the maximal ideal corresponding to the point Q, and let $\mathfrak{m}_P \subset \Gamma(V)$ denote the maximal ideal corresponding to the point P. Let $\theta \in \Gamma(W)$. Since $f(P) = Q$, it follows that

$$\tilde{f}(\theta) \in \mathfrak{m}_P \Leftrightarrow \tilde{f}(\theta)(P) = 0 \Leftrightarrow \theta(f(P)) = 0 \Leftrightarrow \theta(Q) = 0 \Leftrightarrow \theta \in \mathfrak{m}_Q\,.$$

Thus, $\tilde{f}^{-1}(\mathfrak{m}_P) = \mathfrak{m}_Q$. It follows that we get a ring homomorphism $\mathcal{O}_Q(W) \to \mathcal{O}_P(V)$. It is easily checked that this is an inclusion and that $\mathcal{O}_P(V)$ dominates $\mathcal{O}_Q(W)$.

Conversely, suppose $P \in X$ and $Q \in Y$ such that $\mathcal{O}_P(X)$ dominates $\mathcal{O}_Q(Y)$. Take affine neighborhoods V of P and W of Q. We have the map

$$\begin{array}{ccccccc} & & & & & & \mathcal{O}_P(V) \\ & & & & & \overset{\tilde{F}}{\nearrow} & \cap \\ \Gamma(W) & \subset & \mathcal{O}_Q(W) & \subset & k(W) & \xrightarrow{\tilde{F}} & k(V) \end{array}$$

Let $\Gamma(W) = k[y_1, \ldots, y_n]$. Then $\tilde{F}(y_i) = a_i/b_i$, $a_i, b_i \in \Gamma(V)$, and $b_i(P) \neq 0$. If we let $b = b_1 \cdots b_n$, then $\tilde{F}(\Gamma(W)) \subset \Gamma(V_b)$ (Proposition 6.3.5) so $\tilde{F} : \Gamma(W) \to \Gamma(V_b)$ is induced by a unique morphism $f : V_b \to W$ (Proposition 6.3.2). Note that $P \in V_b$. If $g \in \Gamma(W)$ vanishes at Q, then $\tilde{F}(g)$ vanishes at P, from which it follows easily $f(P) = Q$.
(3) We may assume X and Y are affine. Then, as in (2), if $\phi : k(Y) \to k(X)$, $\phi(\Gamma(Y)) \subset \Gamma(X_b)$ for some $b \in \Gamma(X)$, so ϕ is induced by a morphism $f : X_b \to Y$. Therefore $f(X_b)$ is dense in Y since f is one-to-one (Problem 6.26). □

A rational map F from X to Y is said to be **birational** if there are open sets $U \subset X$, $V \subset Y$, and an isomorphism $f : U \to V$ that represents F. We say that X and Y are **birationally equivalent** if there is a birational map from X to Y (This is easily seen to be an equivalence relation). A variety is birationally equivalent to any open subvariety of itself. The varieties $\mathbb{A}^n$ and $\mathbb{P}^n$ are birationally equivalent.

Proposition 6.6.2. *Two varieties are birationally equivalent if and only if their function fields are isomorphic.*

Proof. Since $k(U) = k(X)$ for any open subvariety U of X, birationally equivalent varieties have isomorphic function fields.

Conversely, suppose $\phi : k(X) \to k(Y)$ is an isomorphism. We may assume X and Y are affine. Then

$$\phi : \Gamma(X) \to \Gamma(Y_b) \tag{6.6.3}$$

for some $b \in \Gamma(Y)$, and

$$\phi^{-1} : \Gamma(Y) \to \Gamma(X_d) \tag{6.6.4}$$

for some $d \in \Gamma(X)$, as in the proof of Proposition 6.6.1. Since $d \in \Gamma(X)$, inverting d we get the following map from (6.6.3)

$$\phi : \Gamma(X_d) \to \Gamma((Y_b)_{\phi(d)}) . \tag{6.6.5}$$

Further, since $\phi^{-1}(b) \in \Gamma(X_d)$, we get the following map from (6.6.5)

$$\phi : \Gamma((X_d)_{\phi^{-1}(b)}) \to \Gamma(((Y_b)_{\phi(d)})_b) = \Gamma((Y_b)_{\phi(d)}) . \tag{6.6.6}$$

Similarly, since $b \in \Gamma(Y)$, we get

$$\phi^{-1} : \Gamma(Y_b) \to \Gamma((X_d)_{\phi^{-1}(b)}) .$$

Since $\phi(d) \in Y_b$, we get

$$\phi^{-1} : \Gamma((Y_b)_{\phi(d)}) \to \Gamma(((X_d)_{\phi^{-1}(b)})_d) = \Gamma((X_d)_{\phi^{-1}(b)}) .$$

Then ϕ restricts to an isomorphism of $\Gamma((X_d)_{\phi^{-1}(b)})$ onto $\Gamma((Y_b)_{\phi(d)})$, so $(X_d)_{\phi^{-1}(b)}$ is isomorphic to $(Y_b)_{\phi(d)}$, as desired. □

Corollary 6.6.7. *Every curve is birationally equivalent to a plane curve.*

Proof. If V is a curve, $k(V) = k(x, y)$ for some $x, y \in k(V)$ (Proposition 6.5.1 (2)). Let I be the kernel of the natural homomorphism from $k[X, Y]$ onto $k[x, y] \subset k(V)$. Then I is prime, so $V' = V(I) \subset \mathbb{A}^2$ is a variety. Since $\Gamma(V') = k[X, Y]/I$ is isomorphic to $k[x, y]$, it follows that $k(V')$ is isomorphic to $k(x, y) = k(V)$. So $\dim V' = 1$, and V' is a plane curve (Proposition 6.5.2). □

A variety is said to be **rational** if it is birationally equivalent to $\mathbb{A}^n$ (or $\mathbb{P}^n$) for some n.