Commutative Algebra and Algebraic Geometry

Gary Hu

This is still a work in progress.

This is a set of notes I typed while trying to learn commutative algebra and algebraic geometry through course material found on Brooke Ullery's website. These are notes based on the following 3 courses:

- Harvard Math 137: Undergraduate Algebraic Geometry
- Harvard Math 221: Commutative Algebra
- Emory Math 524: Scheme Theory (this will appear soon...)

This is an unofficial set of notes scribed by Gary Hu, who is responsible for all mistakes. None of these notes have been endorsed by the original lecturer. All of the course content is owned by their respective institutions and their professors, while mistakes should be attributed solely to me. If you do find any errors, please report them to: gh7@williams.edu

Contents

1 The Basics

1.1 The Language of Algebraic Geometry

1.1.1 What is Algebraic Geometry?

Algebraic geometry originates from the study of geometric objects described by polynomial equations. To begin, we introduce the central object of the first part of these notes, the **variety**, which is, speaking informally, a set defined locally by the simultaneous vanishing of such equations over a field k. More precisely, we have the following.

Definition 1.1. *Given a field k and a set of polynomials $S \subseteq k[x_1, \ldots, x_n]$, the corresponding **affine variety** is the set of common roots of all polynomials in S:*

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

Familiar curves from analytic geometry provide elementary examples of this definition.

Example 1.2. *Conics in $\mathbb{R}^2$ provide familiar examples:*

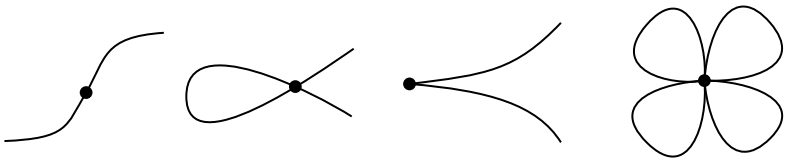
- ***Ellipse:*** $V_1 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + 4y^2 - 1 = 0\}$
- ***Hyperbola:*** $V_2 = \{(x, y) \in \mathbb{R}^2 \mid x^2 - y^2 - 1 = 0\}$

We can also construct varieties from the intersection of simpler ones.

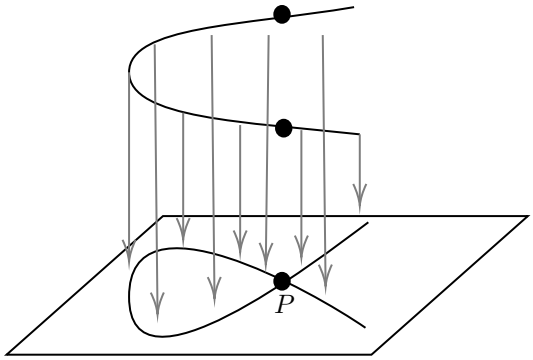
Example 1.3. *Consider the variety in $\mathbb{R}^2$ defined by the two polynomials $y - x^2$ and $y - 4$. Substituting $y = 4$ into the first equation yields $x^2 = 4$, so $x = \pm 2$. Thus, the variety V_3 consists of just two points: $(-2, 4)$ and $(2, 4)$.*

While varieties embedded in an affine space k^n are perhaps the easiest to start working with, the power of algebraic geometry stems from its "dictionary," which translates geometric properties into the language of commutative algebra and vice versa. This correspondence, wherein many geometric questions can be reduced to algebraic ones by analyzing a variety locally, an approach analogous to the study of manifolds via local charts. With this in mind, what are the fundamental questions we can ask about a variety V?

1. **Singularity Theory:** What is the local geometry of V at a given point? A point on a variety may be "smooth," or it may be "singular," exhibiting features like cusps or self-intersections.

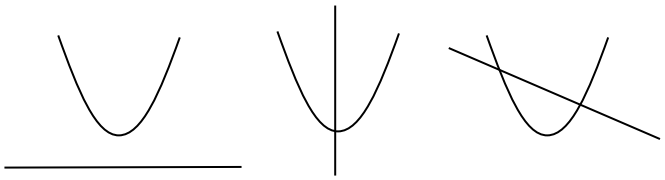


How are these geometric differences reflected in the corresponding algebra? This leads to the celebrated problem of *resolution of singularities*: if a variety has singular points, can we find a related "smooth model" that is isomorphic to the original variety everywhere except at the singularities?



Suppose the bottom variety is not smooth. How do we find a "smooth model" (the top variety) such that they are isomorphic away from P?

2. **Intersection Theory:** How do two or more varieties intersect? In the plane, a line and a conic can intersect in zero, one, or two points.

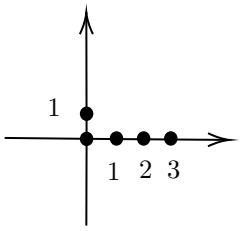


We will see that in "nice" settings (e.g., in projective space over an algebraically closed field), a line and a conic always intersect at exactly two points, provided we count these points with appropriate multiplicity. This is a simple case of a powerful classical result called Bézout's Theorem.

3. **Number Theory:** Questions from number theory often translate into more approachable questions in geometry. For instance, finding integer or rational solutions to Diophantine equations (such as the famous Fermat equation $x^n + y^n = 1$) is equivalent to studying the rational points on the corresponding variety defined over $\mathbb{Q}$.

4. **Embedding Questions:** Given an abstract variety V, can it be embedded into an affine space k^n or into a projective space $\mathbb{P}^n$? If so, what is the smallest dimension n for which such an embedding exists?

5. **Interpolation and Constraints:** Given a set of points, what varieties pass through them? For example, a classical result states that a unique conic passes through any set of five points in the plane, provided they are in general position. For special configurations of points, however, the solution may not be unique.



For instance, consider the five collinear points $(0,0), (1,0), (2,0), (3,0)$, and $(0,1)$ in $\mathbb{R}^2$. The degenerate conic $V(y)$, the x-axis, does not contain $(0,1)$. However, infinitely many conics pass through these five points. For any $a \in \mathbb{R}$, the conic defined by the equation $y(y - ax - 1) = 0$ passes through all five points.

1.1.2 Algebraic Sets, Ideals, and the Zariski Topology

Let k be a field. Throughout this first section in the notes, we will assume that k is algebraically closed, which helps ensure that polynomials behave predictably.

Definition 1.4. *A field k is **algebraically closed** if every non-constant polynomial in one variable with coefficients in k has a root in k. That is, for any $f \in k[x]$ with $\deg(f) \geq 1$, there exists some $\alpha \in k$ such that $f(\alpha) = 0$.*

Remark 1.5. *An inductive argument shows this is equivalent to the statement that every non-constant polynomial in $k[x]$ splits completely into linear factors: $f(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$ for some $c, \alpha_1, \ldots, \alpha_n \in k$.*

Example 1.6. *The Fundamental Theorem of Algebra states that $\mathbb{C}$ is algebraically closed. In contrast, $\mathbb{R}$ is not since the polynomial $x^2 + 1 \in \mathbb{R}[x]$ has no root in $\mathbb{R}$.*

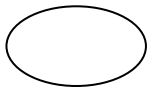
Definition 1.7. *The **affine n-space** over a field k, denoted $\mathbb{A}^n_k$ or simply $\mathbb{A}^n$, is the set of n-tuples of elements of k. We adopt this notation to emphasize that we are considering $\mathbb{A}^n$ as a set of points, rather than as a vector space with a distinguished origin. For a polynomial $f \in k[x_1, \ldots, x_n]$, a point $P = (a_1, \ldots, a_n) \in \mathbb{A}^n$ is a **zero** of f if $f(P) = f(a_1, \ldots, a_n) = 0$.*

Example 1.8 (Conics in $\mathbb{A}^2_{\mathbb{C}}$)**.** *A **conic** in $\mathbb{A}^2_k$ is the zero set of a single degree-two polynomial:*

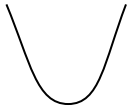
$$g(x, y) = ax^2 + bxy + cy^2 + dx + ey + f.$$

When $k = \mathbb{R}$, we can visualize the real points (the real locus) of these curves, which gives the familiar conic sections:

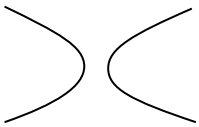
- *Ellipse*



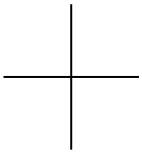
- *Parabola*



- *Hyperbola*



- *Degenerate cases, such as two intersecting lines (e.g., from $xy = 0$) or a single point (from $x^2+y^2 = 0$).*



However, considering only the real locus can be misleading. In $\mathbb{A}^2_{\mathbb{R}}$, the polynomial x^2+y^2 defines just a single point, $(0, 0)$, while x^2+y^2+1 defines the empty set. Over the complex numbers, both of these equations define curves with infinitely many points. The assumption that k is algebraically closed eliminates such pathologies.

More generally, a loci may be defined by the simultaneous vanishing of several polynomials.

Definition 1.9. *Let $S \subseteq k[x_1, \ldots, x_n]$ be any set of polynomials. The **vanishing set** of S is*

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

*A subset $X \subseteq \mathbb{A}^n$ is an **algebraic set** if $X = V(S)$ for some set of polynomials S.*

The use of an arbitrary set of polynomials S is notationally cumbersome. It is more elegant and powerful to work with the ideal generated by S, as the following proposition justifies.

Proposition 1.10. *For any set of polynomials $S \subseteq k[x_1, \ldots, x_n]$, if $I = \langle S \rangle$ is the ideal generated by S, then $V(S) = V(I)$.*

Proof. ($\supseteq$) Since $S \subseteq I$, any point that is a zero of every polynomial in I must, in particular, be a zero of every polynomial in S. Thus, $V(I) \subseteq V(S)$.

($\subseteq$) Let $P \in V(S)$, so that $f(P) = 0$ for all $f \in S$. An arbitrary polynomial $g \in I$ can be expressed as a finite linear combination $g = \sum_{i=1}^{m} h_i f_i$, where each $h_i \in k[x_1, \ldots, x_n]$ and each $f_i \in S$. Evaluating at P yields

$$g(P) = \sum_{i=1}^{m} h_i(P) f_i(P) = \sum_{i=1}^{m} h_i(P) \cdot 0 = 0.$$

Thus, P is a zero of g. As g was an arbitrary element of I, we conclude that $P \in V(I)$. □

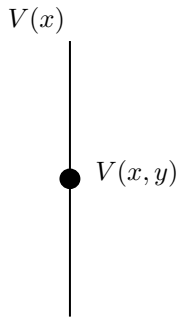
Corollary 1.11. *Every algebraic set is of the form $V(I)$ for some ideal $I \subseteq k[x_1, \ldots, x_n]$.*

Example 1.12. *If $I = (f)$ is a principal ideal generated by a single non-constant polynomial f, its vanishing set $V(I) = V(f)$ is called a **hypersurface**. For example, in $k[x, y]$, the ideal $I = (y)$ corresponds to the algebraic set $V(y)$, which is the x-axis.*

The operator V, which maps ideals in the polynomial ring to subsets of affine space, possesses several fundamental properties that form the basis for a new topology.

Proposition 1.13. *Let I, J, and $\{I_\alpha\}_{\alpha \in A}$ be a collection of ideals in $k[x_1, \ldots, x_n]$.*

1. ***Inclusion-reversing:** If $I \subseteq J$, then $V(J) \subseteq V(I)$. Intuitively, imposing more polynomial constraints can only shrink the resulting zero set. For example, in $k[x, y]$, we have the inclusion of ideals $(x) \subseteq (x, y)$, which corresponds to the reverse inclusion of algebraic sets $V(x, y) \subseteq V(x)$ (a point contained in a line).*



2. ***Arbitrary Intersections:** The intersection of any collection of algebraic sets is an algebraic set. Specifically, $\bigcap_{\alpha \in A} V(I_\alpha) = V(\sum_{\alpha \in A} I_\alpha)$, where $\sum I_\alpha$ is the ideal generated by the union $\bigcup_\alpha I_\alpha$.*
3. ***Finite Unions:** The union of two algebraic sets is an algebraic set. Specifically, $V(I) \cup V(J) = V(I \cdot J)$, where $I \cdot J$ is the product ideal. By induction, any finite union of algebraic sets is also an algebraic set.*

Remark 1.14. *The union of an infinite collection of algebraic sets is not necessarily algebraic. For example, in $\mathbb{A}^1_{\mathbb{C}}$, the set of integers $\mathbb{Z} = \bigcup_{n \in \mathbb{Z}} V(x - n)$ is an infinite union of points (which are themselves algebraic sets). However, $\mathbb{Z}$ is not an algebraic set, as any non-zero polynomial in $\mathbb{C}[x]$ has only a finite number of roots.*

Example 1.15. *The entire space $\mathbb{A}^n$ and the empty set $\emptyset$ are algebraic sets, corresponding to the zero ideal and the unit ideal, respectively: $V((0)) = \mathbb{A}^n$ and $V((1)) = \emptyset$. A single point $P = (a_1, \ldots, a_n)$ is an algebraic set, as it is the vanishing set $V(x_1 - a_1, \ldots, x_n - a_n)$.*

The properties from the proposition, together with the preceding example, are precisely the axioms for the closed sets of a topology.

Definition 1.16. *The **Zariski topology** on $\mathbb{A}^n$ is the topology whose **closed sets** are precisely the algebraic sets. A set $Y \subseteq \mathbb{A}^n$ is **Zariski open** if its complement, $\mathbb{A}^n \setminus Y$, is Zariski closed.*

Example 1.17. *In the Zariski topology on $\mathbb{A}^1_k$ (where k is algebraically closed), the algebraic sets are the zero sets of ideals in $k[x]$. Since $k[x]$ is a principal ideal domain, any ideal is of the form (f). If $f = 0$, $V(f) = \mathbb{A}^1$. If f is a non-zero polynomial, it has a finite number of roots. Thus, the closed sets are $\mathbb{A}^1$ itself and all finite subsets of points. Consequently, the non-empty open sets are the cofinite sets (complements of finite sets).*

Remark 1.18. *The Zariski topology on $\mathbb{A}^n_{\mathbb{C}}$ (or $\mathbb{A}^n_{\mathbb{R}}$) is significantly coarser than the standard Euclidean (metric) topology. Every Zariski closed set is also closed in the Euclidean topology, because polynomials are continuous functions and $V(S) = \bigcap_{f \in S} f^{-1}(\{0\})$ is an intersection of closed sets. The converse, however, is false; for instance, the closed unit disk in $\mathbb{R}^2$ is closed in the Euclidean topology but is not a Zariski-closed set.*

1.1.3 From Varieties to Ideals

Having established the map $V : \{\text{Ideals in } k[\vec{x}]\} \to \{\text{Algebraic Sets in } \mathbb{A}^n\}$, which translates algebraic data into geometric objects, we now construct its counterpart. That is, we need a map from subsets of affine space back to the world of ideals. Throughout, let k be an algebraically closed field and let $R = k[x_1, \ldots, x_n]$.

Definition 1.19. *For any subset $X \subseteq \mathbb{A}^n$, the **ideal of** X, denoted $I(X)$, is the set of all polynomials in R that vanish at every point in X:*

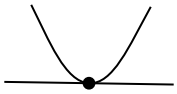
$$I(X) := \{f \in R \mid f(P) = 0 \text{ for all } P \in X\}.$$

Remark 1.20. *As its name suggests, $I(X)$ is indeed an ideal in R. The verification is a straightforward exercise. If $f, g \in I(X)$, then for any $P \in X$, $(f - g)(P) = f(P) - g(P) = 0 - 0 = 0$. If $h \in R$, then $(hf)(P) = h(P)f(P) = h(P) \cdot 0 = 0$. Thus $f - g \in I(X)$ and $hf \in I(X)$.*

One might hope that the operators I and V are perfect inverses. The following examples demonstrate that the relationship is more subtle.

Example 1.21. *The composition $V \circ I$ can enlarge a set. Consider the subset $X = \mathbb{Z} \subseteq \mathbb{A}^1_{\mathbb{C}}$. A polynomial that is zero at every integer must be the zero polynomial itself, since a non-zero polynomial in one variable has only finitely many roots. Thus, $I(\mathbb{Z}) = (0)$. Applying V gives $V(I(\mathbb{Z})) = V(0) = \mathbb{A}^1_{\mathbb{C}}$, which is the Zariski closure of $\mathbb{Z}$ but is strictly larger than the original set. In general, $V(I(X)) \neq X$. Instead, $V(I(X)) = \overline{X}$, the Zariski closure of X.*

Example 1.22. *The composition $I \circ V$ can enlarge an ideal. Let $J = (y, x^2) \subseteq \mathbb{C}[x, y]$. The variety $V(J)$ is the intersection of the line $V(y)$ (the x-axis) and the "double line" $V(x^2) = V(x)$ (the y-axis). Their intersection is the origin, so $V(J) = \{(0, 0)\}$.*



Now, let us apply I: $I(V(J)) = I(\{(0, 0)\})$. This is the ideal of all polynomials that vanish at the origin, which is precisely the maximal ideal (x, y). Observe that $(x, y) \supsetneq (y, x^2)$. So, in general, $I(V(J)) \neq J$.

The previous example showed that $J \subsetneq I(V(J))$. This inclusion always holds: if $f \in J$, then by definition f vanishes on every point of $V(J)$, so $f \in I(V(J))$. The discrepancy is not arbitrary; it is controlled by a purely algebraic construction. Notice that the polynomial x is in $I(V(J)) = (x, y)$, but not in $J = (y, x^2)$. However, a power of it, x^2, is in J. This suggests that we should take roots.

Definition 1.23. *Let R be a commutative ring and $I \subseteq R$ be an ideal. The* ***radical*** *of I, denoted $\sqrt{I}$, is the set of elements in R some power of which lies in I:*

$$\sqrt{I} := \{a \in R \mid a^n \in I \text{ for some integer } n > 0\}.$$

An ideal I is called a ***radical ideal*** *if $I = \sqrt{I}$.*

Lemma 1.24. *For any ideal I in a commutative ring R, the set $\sqrt{I}$ is itself a radical ideal of R.*

Proof. We first prove that $\sqrt{I}$ is an ideal. Let $a, b \in \sqrt{I}$. By definition, there exist positive integers n, m such that $a^n \in I$ and $b^m \in I$. Consider the binomial expansion of $(a-b)^{n+m-1}$. Each term in the expansion is of the form $c \cdot a^i b^j$ where $c \in R$ is an integer coefficient and $i + j = n + m - 1$. It is easy to see that for any such term, either $i \geq n$ or $j \geq m$. If $i \geq n$, then $a^i = a^{i-n}a^n \in I$, which implies the entire term is in I since I is an ideal. Similarly, if $j \geq m$, the term is in I. Thus, every term in the expansion is an element of I, and their sum, $(a-b)^{n+m-1}$, must also be in I. This implies that $a - b \in \sqrt{I}$. For closure under multiplication by elements of the ring, let $c \in R$. Since $a \in \sqrt{I}$, there is a positive integer n such that $a^n \in I$. Then $(ca)^n = c^n a^n \in I$, which means $ca \in \sqrt{I}$. Therefore, $\sqrt{I}$ is an ideal.

To show that $\sqrt{I}$ is a radical ideal, we must prove that $\sqrt{\sqrt{I}} = \sqrt{I}$. The inclusion $\sqrt{I} \subseteq \sqrt{\sqrt{I}}$ is immediate from the definition. For the reverse inclusion, let $a \in \sqrt{\sqrt{I}}$. This means that there exists a positive integer n such that $a^n \in \sqrt{I}$. By the definition of the radical, this implies that there exists a positive integer m such that $(a^n)^m \in I$. Simplifying gives $a^{nm} \in I$, which by definition means $a \in \sqrt{I}$. Thus, $\sqrt{\sqrt{I}} \subseteq \sqrt{I}$. We have therefore shown that $\sqrt{\sqrt{I}} = \sqrt{I}$, which confirms that $\sqrt{I}$ is a radical ideal. □

Lemma 1.25. *Let $R = k[x_1, \ldots, x_n]$.*

1. *For any ideal $J \subseteq R$, we have $\sqrt{J} \subseteq I(V(J))$.*
2. *For any subset $X \subseteq \mathbb{A}^n$, we have $X \subseteq V(I(X))$.*

Proof.

1. Let $f \in \sqrt{J}$. Then $f^m \in J$ for some $m > 0$. For any point $P \in V(J)$, we have $g(P) = 0$ for all $g \in J$. In particular, $f^m(P) = 0$. Since $f(P) \in k$, this means $(f(P))^m = 0$, which implies $f(P) = 0$. As this holds for all $P \in V(J)$, we conclude that $f \in I(V(J))$.
2. Let $P \in X$. By the definition of $I(X)$, every function $f \in I(X)$ satisfies $f(P) = 0$. This is precisely the condition for P to be an element of the set $V(I(X))$.

□

The operators I and V have the following basic properties:

Corollary 1.26. *Let $X, Y \subseteq \mathbb{A}^n$.*

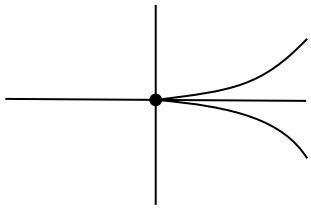
1. *If $X \subseteq Y$, then $I(Y) \subseteq I(X)$.*
2. *$I(\emptyset) = k[x_1, \ldots, x_n]$ and, for an infinite field k, $I(\mathbb{A}^n) = (0)$.*
3. *For a point $P = (a_1, \ldots, a_n)$, its ideal is the maximal ideal $I(\{P\}) = (x_1 - a_1, \ldots, x_n - a_n)$.*
4. *For any $X \subseteq \mathbb{A}^n$, the ideal $I(X)$ is a radical ideal.*
5. *For any ideal $J \subseteq k[x_1, \ldots, x_n]$, we have $V(J) = V(\sqrt{J})$.*

Let's apply these ideas on some concrete geometric objects.

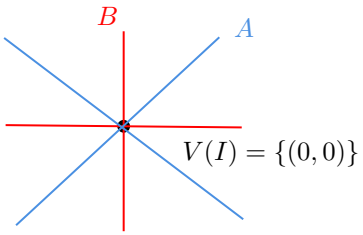
Example 1.27.

1. ***Cuspidal Plane Curve.*** *Consider the set* $X = \{(t^2, t^3) \mid t \in \mathbb{C}\} \subseteq \mathbb{A}^2_{\mathbb{C}}$. *Is this an algebraic set? For any point* $(x, y) \in X$, *we have* $x = t^2$ *and* $y = t^3$ *for some* t. *Then* $x^3 = (t^2)^3 = t^6$ *and* $y^2 = (t^3)^2 = t^6$, *so every point on the curve satisfies* $x^3 - y^2 = 0$. *This shows that* $X \subseteq V(x^3 - y^2)$.

   For the reverse inclusion, let $(a, b) \in V(x^3 - y^2)$, *so* $a^3 = b^2$. *Since* $k = \mathbb{C}$ *is algebraically closed, we can find* $t \in \mathbb{C}$ *such that* $t^2 = a$. *Then* $a^3 = (t^2)^3 = t^6$. *The equation becomes* $t^6 = b^2$, *which implies* $b = \pm t^3$. *If* $b = t^3$, *then* $(a, b) = (t^2, t^3) \in X$. *If* $b = -t^3$, *we may choose* $t' = -t$, *so* $(a, b) = ((-t')^2, (-t')^3) \in X$. *Thus, every point of* $V(x^3 - y^2)$ *lies on the parameterized curve* X. *We conclude that* $X = V(x^3 - y^2)$ *and is an algebraic set.*



2. *Let* $I = (x^2 + y^2, x^2 - y^2) \subseteq \mathbb{C}[x, y]$. *What is* $V(I)$? *We can simplify the ideal algebraically. Since* I *contains the generators, it must also contain their sum and difference:* $(x^2 + y^2) + (x^2 - y^2) = 2x^2$ *and* $(x^2 + y^2) - (x^2 - y^2) = 2y^2$. *Thus* $(x^2, y^2) \subseteq I$. *Conversely, we can recover the original generators from* x^2 *and* y^2, *so* $I = (x^2, y^2)$. *The radical is* $\sqrt{I} = (x, y)$. *Therefore,* $V(I) = V(\sqrt{I}) = V(x, y) = \{(0, 0)\}$.



1.2 Decomposition and Dimension

1.2.1 Irreducible Varieties and Decomposition

A central theme in algebra is the decomposition of objects into simpler, indecomposable parts, such as factoring integers into primes. We now develop the geometric analogue for algebraic sets.

Definition 1.28. *An algebraic set* X *is* ***reducible*** *if it can be written as a union of two proper algebraic subsets,* $X = X_1 \cup X_2$, *where* X_1, X_2 *are algebraic sets with* $X_1 \subsetneq X$ *and* $X_2 \subsetneq X$. *If* X *is not reducible, it is* ***irreducible****. An irreducible algebraic set is often called a* ***variety****. A decomposition of an algebraic set* X *as* $X = X_1 \cup \cdots \cup X_m$, *where each* X_i *is an irreducible algebraic set and no* X_i *is contained in any* X_j *for* $i \neq j$, *is called a decomposition into* ***irreducible components****.*

Example 1.29. *Any line* $L \subseteq \mathbb{A}^2$ *is an irreducible algebraic set. The proper algebraic subsets of a line are precisely the finite sets of points. Since a line is an infinite set of points, it cannot be expressed as the union of two of its proper algebraic subsets. Thus, a line is irreducible.*

Example 1.30. *The algebraic set* $V(xy) \subseteq \mathbb{A}^2$ *is reducible since it is the union of the y-axis* $(V(x))$ *and the x-axis* $(V(y))$, *both of which are proper algebraic subsets. In contrast, any single line* $L \subseteq \mathbb{A}^2$ *is irreducible, as its only proper algebraic subsets are finite sets of points.*

The geometric notion of irreducibility has a perfect algebraic counterpart.

Proposition 1.31. *An algebraic set* X *is irreducible if and only if its ideal* $I(X)$ *is a prime ideal.*

Proof. ($\Rightarrow$) Suppose X is reducible, so $X = X_1 \cup X_2$ with $X_1, X_2 \subsetneq X$. Since $X_1 \neq X$, $I(X_1) \supsetneq I(X)$. Let $f_1 \in I(X_1) \setminus I(X)$. Similarly, let $f_2 \in I(X_2) \setminus I(X)$. The product $f_1 f_2$ vanishes on all of X_1 (since f_1 does)

and on all of X_2 (since f_2 does). Therefore, $f_1 f_2$ vanishes on their union X, which means $f_1 f_2 \in I(X)$. Since neither factor is in $I(X)$, we conclude that $I(X)$ is not a prime ideal.

($\Leftarrow$) Suppose $I(X)$ is not prime. Then there exist polynomials $f, g \notin I(X)$ such that their product $fg \in I(X)$. As fg vanishes on all of X, we have $X \subseteq V(fg) = V(f) \cup V(g)$. This implies $X = (X \cap V(f)) \cup (X \cap V(g))$. Let $X_1 = X \cap V(f)$ and $X_2 = X \cap V(g)$. These are algebraic sets. Since $f \notin I(X)$, the set X is not contained in $V(f)$, so X_1 is a proper subset of X. Similarly, $X_2 \subsetneq X$. We have thus found a decomposition of X into two proper algebraic subsets, which means X is reducible. □

A major goal is to show the converse: if J is a prime ideal, then $V(J)$ is irreducible. For this to be true, it is essential that the field k is algebraically closed.

Example 1.32. *Consider the polynomial $f = y^2 + x^2(x-1)^2$ in $\mathbb{R}[x, y]$. It can be shown that f is an irreducible polynomial, so the ideal (f) is prime. However, the set of real zeros is $V(f) = \{(0, 0), (1, 0)\}$, since a sum of squares is zero in $\mathbb{R}$ only if each term is zero. This set is reducible, as it is the union of two distinct points. This demonstrates a failure of the correspondence over non-algebraically closed fields.*

1.2.2 The Noetherian Property

We now show that any algebraic set can be decomposed into a finite union of irreducible components, and that this decomposition is unique. The proof relies on a fundamental algebraic property of polynomial rings.

Definition 1.33. *A commutative ring R is **Noetherian** if every ideal $I \subseteq R$ is finitely generated.*

This condition has several powerful equivalent formulations. We leave the proof as an exercise.

Lemma 1.34. *The following are equivalent for a commutative ring R:*

1. *R is Noetherian (every ideal is finitely generated).*
2. *R satisfies the **ascending chain condition (ACC)** on ideals: every chain of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ must stabilize, i.e., there exists an N such that $I_n = I_N$ for all $n \geq N$.*
3. *Every non-empty collection of ideals of R has a maximal element with respect to inclusion.*

The fact that $k[x_1, \dots, x_n]$ is Noetherian has an important geometric consequence: every algebraic set can be defined by a finite number of polynomial equations. That is, for any algebraic set X, there exist $f_1, \dots, f_m$ such that

$$X = V(I(X)) = V((f_1, \dots, f_m)) = V(f_1) \cap V(f_2) \cap \dots \cap V(f_m).$$

This follows from one of the most important theorems in commutative algebra.

Theorem 1.35 (Hilbert Basis Theorem)**.** *If R is a Noetherian ring, then the polynomial ring $R[x]$ is also Noetherian.*

Proof Sketch. Let $I \subseteq R[x]$ be an ideal. Assume for contradiction that I is not finitely generated. We construct an infinite sequence of polynomials $\{f_k\}_{k=1}^{\infty} \subseteq I$. Let $f_1 \in I$ be a non-zero polynomial of minimal degree. Inductively, choose f_{k+1} to be a polynomial of minimal degree in the ideal $I \setminus (f_1, \dots, f_k)$. Let $a_k \in R$ be the leading coefficient of f_k. By construction, $\deg(f_1) \leq \deg(f_2) \leq \dots$.

Consider the ideal of leading coefficients, $J = (a_1, a_2, \dots) \subseteq R$. Since R is Noetherian, this chain of ideals $(a_1) \subseteq (a_1, a_2) \subseteq \dots$ must stabilize. Thus J is finitely generated, and there exists some m such that $J = (a_1, \dots, a_m)$. In particular, $a_{m+1} \in (a_1, \dots, a_m)$, so we can write $a_{m+1} = \sum_{j=1}^{m} u_j a_j$ for some $u_j \in R$.

Now, define the polynomial $g = \sum_{j=1}^{m} u_j x^{\deg(f_{m+1}) - \deg(f_j)} f_j$. By construction, $g \in (f_1, \dots, f_m)$ and its leading term is precisely $a_{m+1} x^{\deg(f_{m+1})}$. The polynomial $h = f_{m+1} - g$ has three key properties:

- $h \in I$ because f_{m+1} and g are in I.
- $h \notin (f_1, \dots, f_m)$, otherwise $f_{m+1} = h + g$ would be.
- $\deg(h) < \deg(f_{m+1})$ because we designed g to cancel the leading term of f_{m+1}.

The existence of h contradicts the choice of f_{m+1} as a polynomial of minimal degree in $I \setminus (f_1, \ldots, f_m)$. Thus, our initial assumption must be false, and I is finitely generated. □

We briefly mention two corollaries:

Corollary 1.36.

1. *A field k is trivially Noetherian. By induction, the Hilbert Basis Theorem implies that the polynomial ring $k[x_1, \ldots, x_n]$ is Noetherian.*
2. *The ACC on ideals in $k[x_1, \ldots, x_n]$ implies the **descending chain condition (DCC)** for algebraic sets in $\mathbb{A}^n$. That is, any sequence of algebraic sets $X_1 \supseteq X_2 \supseteq X_3 \supseteq \ldots$ must stabilize. This follows because such a chain gives rise to an ascending chain of ideals $I(X_1) \subseteq I(X_2) \subseteq I(X_3) \subseteq \ldots$, which must stabilize.*

We now have the tools to prove the main decomposition theorem.

Theorem 1.37. *Every algebraic set X can be written as a finite union $X = X_1 \cup \cdots \cup X_m$ of irreducible algebraic sets, such that $X_i \not\subseteq X_j$ for $i \neq j$. This decomposition is unique up to the reordering of the components X_i.*

Proof. **Existence.** Assume for contradiction that there exists an algebraic set X that cannot be written as a finite union of irreducibles. Such an X must be reducible, so $X = Y_1 \cup Z_1$ for proper algebraic subsets Y_1, Z_1. At least one of them, say Y_1, must also be non-decomposable into a finite union of irreducibles. Continuing this process, we write $Y_1 = Y_2 \cup Z_2$, where Y_2 is again non-decomposable. This yields an infinite, strictly descending chain of algebraic sets: $X \supsetneq Y_1 \supsetneq Y_2 \supsetneq Y_3 \supsetneq \ldots$, which contradicts the DCC. Therefore, every algebraic set admits such a decomposition.

Uniqueness. Suppose $X = \bigcup_{i=1}^{r} X_i$ and $X = \bigcup_{j=1}^{s} Y_j$ are two such decompositions. Consider a component X_i. We have $X_i \subseteq X = \bigcup_j Y_j$, which implies $X_i = X_i \cap (\bigcup_j Y_j) = \bigcup_j (X_i \cap Y_j)$. Since each $X_i \cap Y_j$ is an algebraic set and X_i is irreducible, it must be that $X_i = X_i \cap Y_j$ for some j. This means $X_i \subseteq Y_j$. By a symmetric argument, for this Y_j, we must have $Y_j \subseteq X_k$ for some k. This gives $X_i \subseteq Y_j \subseteq X_k$. By the minimality condition of the decomposition ($X_i \not\subseteq X_k$ for $i \neq k$), we must have $i = k$, which implies $X_i = Y_j$. This establishes a bijection between the sets of components, proving uniqueness. □

1.2.3 Dimension

We conclude by introducing the geometric notion of dimension. Intuitively, this should capture the number of independent parameters needed to describe a point on the set. We formalize this by considering chains of irreducible subsets.

Definition 1.38. *The **dimension** of an algebraic set X, denoted $\dim X$, is the supremum of all integers d for which there exists a strict chain of irreducible algebraic sets of length d:*

$$X_d \supsetneq X_{d-1} \supsetneq \cdots \supsetneq X_0,$$

where each $X_i \subseteq X$.

Example 1.39. *The chain $\mathbb{A}^2 \supsetneq V(y) \supsetneq V(x, y)$ consists of a plane, a line, and a point. This shows $\dim \mathbb{A}^2 \geq 2$. In fact, $\dim \mathbb{A}^n = n$. Proving this equality, however, requires significant commutative algebra. The algebraic counterpart to geometric dimension is the **Krull dimension** of the coordinate ring, defined as the maximum length of a chain of prime ideals. The correspondence ensures that $\dim X =$ Krull dim$(k[x_1, \ldots, x_n]/I(X))$.*

1.3 Hilbert's Nullstellensatz

The fundamental theorem of algebra establishes a correspondence between the roots of a polynomial in one variable and the linear factors of that polynomial. Hilbert's Nullstellensatz (German for "theorem of zeros") is a vast generalization of this idea to multiple variables, and is the most powerful tool for our dictionary.

Our primary goal is to prove this theorem. The journey will require a background on finiteness conditions on ring extensions, culminating in Zariski's Lemma.

1.3.1 Statement of the Theorems

The Nullstellensatz has two primary forms, commonly known as the "Weak" and "Strong" versions. Let k be a field and $S = k[x_1, \ldots, x_n]$ be the polynomial ring in n variables.

Theorem 1.40 (Weak Nullstellensatz)**.** *Let k be an algebraically closed field. If $J \subsetneq S$ is a proper ideal, then its vanishing locus $V(J)$ is non-empty.*

This theorem asserts that a system of polynomial equations over an algebraically closed field has a common solution, provided the equations do not generate a trivial contradiction (i.e., the ideal they generate is not the entire ring).

The Strong Nullstellensatz provides a precise dictionary between ideals and varieties.

Theorem 1.41 (Hilbert's Nullstellensatz)**.** *Let k be an algebraically closed field and let $J \subseteq S$ be an ideal. Then the ideal of functions vanishing on $V(J)$ is the radical of J. That is,*

$$I(V(J)) = \sqrt{J}.$$

This result is remarkable: it states that if a polynomial g vanishes at every common zero of a set of polynomials $\{f_i\}$, then some power of g must lie in the ideal generated by the $\{f_i\}$. The proof of the Weak Nullstellensatz hinges on a deep algebraic property of field extensions, to which we now turn.

1.3.2 Integral Extensions and Finiteness Conditions

To prove the Nullstellensatz, we must first establish a crucial result concerning the structure of maximal ideals in a polynomial ring over an algebraically closed field. The proof of this result, in turn, rests upon a careful distinction between several notions of "finiteness" for ring extensions.

Let R be a ring and S be a ring containing R as a subring. The ring S naturally possesses the structure of an R-module.

Definition 1.42. *Let S be a ring and $R \subseteq S$ a subring.*

1. *S is a **finitely generated R-module** (or **module-finite** over R) if there exist elements $s_1, \ldots, s_n \in S$ such that $S = \sum_{i=1}^{n} Rs_i$.*
2. *S is a **finitely generated R-algebra** (or **ring-finite** over R) if there exist elements $s_1, \ldots, s_n \in S$ such that $S = R[s_1, \ldots, s_n]$.*

Remark 1.43. *Module-finiteness is a substantially stronger condition than ring-finiteness. For example, the polynomial ring $R[x]$ is a ring-finite extension of R (generated as an algebra by the single element x), but it is not module-finite. No finite set of polynomials can span all of $R[x]$ as an R-module, as the degrees of polynomials are unbounded.*

A third, related concept is that of integrality, which generalizes the notion of an algebraic number over a field.

Definition 1.44. *An element $s \in S$ is **integral** over R if it is a root of a **monic** polynomial with coefficients in R. That is, there exists a polynomial $f(t) = t^m + r_{m-1}t^{m-1} + \cdots + r_0 \in R[t]$ such that $f(s) = 0$. The ring S is an **integral extension** of R if every element of S is integral over R.*

Example 1.45.

1. *The polynomial ring $R[x]$ is ring-finite over R but is neither module-finite nor integral.*
2. *The quotient ring $R[x]/(x^2)$ is spanned by $\{1, \overline{x}\}$ as an R-module. It is therefore module-finite. Every element $a + b\overline{x}$ is integral over R.*

3. *The field extension* $\mathbb{Q}[\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \dots] \subseteq \mathbb{C}$ *is an integral extension of* $\mathbb{Q}$*, but it is neither ring-finite nor module-finite.*

The relationship between these three conditions is fundamental. The following proposition establishes that for a single element, integrality is equivalent to the module-finiteness of the algebra it generates.

Proposition 1.46. *Let* $R \subseteq S$ *be rings and let* $v \in S$*. The following are equivalent:*

1. *The element* v *is integral over* R*.*
2. *The* R*-algebra* $R[v]$ *is a module-finite extension of* R*.*
3. *There exists a subring* $S' \subseteq S$ *containing* $R[v]$ *that is module-finite over* R*.*

Proof. (1) $\implies$ (2): Suppose v is integral over R. Then it satisfies a monic relation $v^m + a_{m-1}v^{m-1} + \cdots + a_0 = 0$ for some $a_i \in R$. This equation allows us to express v^m as an R-linear combination of $\{1, v, \dots, v^{m-1}\}$. By induction, any power v^k for $k \geq m$ can also be expressed as a linear combination of this set. Thus, the set $\{1, v, \dots, v^{m-1}\}$ generates $R[v]$ as an R-module.

(2) $\implies$ (3): This is trivial. Let $S' = R[v]$.

(3) $\implies$ (1): This is a classic application of the determinant trick, reminiscent of the Cayley-Hamilton theorem. Suppose S' is a module-finite extension of R containing $R[v]$, generated as an R-module by $\{w_1, \dots, w_m\}$. Since $v \in S'$, multiplication by v is an R-linear map from S' to itself. We can express the image of each generator under this map as a linear combination of the generators:

$$vw_i = \sum_{j=1}^{m} a_{ij} w_j \quad \text{for some } a_{ij} \in R.$$

This system of linear equations can be written in matrix form as:

$$\sum_{j=1}^{m} (v\delta_{ij} - a_{ij}) w_j = 0 \quad \text{for each } i = 1, \dots, m.$$

Let M be the $m \times m$ matrix whose (i, j)-entry is $v\delta_{ij} - a_{ij}$. Let $\mathbf{w}$ be the column vector of the generators. The system is $M\mathbf{w} = \mathbf{0}$. By Cramer's rule (or multiplying by the adjugate matrix), we have $\det(M)\mathbf{w} = \mathbf{0}$. Since $1 \in S'$ is a linear combination of the w_j, we must have $\det(M) \cdot 1 = 0$, so $\det(M) = 0$. Expanding $\det(vI - A)$, where A is the matrix of coefficients (a_{ij}), yields a monic polynomial in v of degree m with coefficients in R. Thus, v is integral over R. □

This proposition has powerful corollaries that illuminate the structure of integral extensions.

Corollary 1.47. *Let* $R \subseteq S$ *be rings. The set of elements in* S *that are integral over* R *forms a subring of* S*, called the* ***integral closure*** *of* R *in* S*.*

Proof. Let $a, b \in S$ be integral over R. By Proposition 1.46, $R[a]$ is a module-finite extension of R. Since b is integral over R, it is necessarily integral over the larger ring $R[a]$. Thus, the ring $(R[a])[b] = R[a, b]$ is module-finite over $R[a]$. By the tower property of modules, if $R[a, b]$ is module-finite over $R[a]$ and $R[a]$ is module-finite over R, then $R[a, b]$ is module-finite over R. The elements $a + b$ and ab both belong to $R[a, b]$. By the equivalence (3) $\implies$ (1) of Proposition 1.46, they must be integral over R. The elements of R are trivially integral over R. Thus, the set of integral elements is a subring. □

Corollary 1.48. *Let* S *be a ring-finite extension of a ring* R*. Then* S *is module-finite over* R *if and only if* S *is integral over* R*.*

Proof. ($\implies$) If S is module-finite over R, then for any $v \in S$, the subring $R[v] \subseteq S$ satisfies condition (3) of Proposition 1.46. Thus, every $v \in S$ is integral over R.

($\impliedby$) Suppose S is integral over R and ring-finite, say $S = R[v_1, \dots, v_n]$. We proceed by induction on n.

- **Base Case ($n = 1$):** $S = R[v_1]$. Since v_1 is integral over R, S is module-finite over R by Proposition 1.46.
- **Inductive Step:** Assume that $R_k = R[v_1, \ldots, v_k]$ is module-finite over R for $k < n$. Consider $R_{k+1} = R[v_1, \ldots, v_{k+1}] = R_k[v_{k+1}]$. By hypothesis, v_{k+1} is integral over R, and hence also over the larger ring R_k. By the base case, $R_k[v_{k+1}]$ is module-finite over R_k. By the inductive hypothesis, R_k is module-finite over R. The tower property implies R_{k+1} is module-finite over R.

By the principle of induction, $S = R[v_1, \ldots, v_n]$ is module-finite over R. □

To state Zariski's Lemma, we also need some language from the theory of field extensions, which we recall here. Let $K \subseteq L$ be a field extension. For any elements $v_1, \ldots, v_n \in L$, we denote by $K(v_1, \ldots, v_n)$ the smallest subfield of L containing both K and the set $\{v_1, \ldots, v_n\}$. This field is the field of fractions of the ring $K[v_1, \ldots, v_n]$.

Definition 1.49. *A field extension L of a field K is an **algebraic extension** if every element of L is algebraic over K.*

Example 1.50. *The field $\mathbb{Q}(\sqrt{5})$ is an algebraic extension of $\mathbb{Q}$. Note that because $\sqrt{5}$ is algebraic, the ring $\mathbb{Q}[\sqrt{5}]$ is already a field, so $\mathbb{Q}[\sqrt{5}] = \mathbb{Q}(\sqrt{5})$. Its elements are of the form $\alpha + \beta\sqrt{5}$ for $\alpha, \beta \in \mathbb{Q}$. Every such element is a root of the quadratic polynomial $x^2 - 2\alpha x + (\alpha^2 - 5\beta^2) = 0$, which has rational coefficients. This extension is also module-finite over $\mathbb{Q}$. In contrast, the extension $\mathbb{Q}(\pi)$ is not algebraic over $\mathbb{Q}$, as π is a transcendental element.*

For a field extension $K \subseteq L$, the set of all elements in L that are algebraic over K constitutes a subfield of L.

Proposition 1.51. *The field of rational functions $k(x)$ is a finitely generated field extension of k, but it is not a finitely generated k-algebra (i.e., it is not ring-finite over k).*

Proof. Assume for the sake of contradiction that $k(x)$ is ring-finite, so $k(x) = k[v_1, \ldots, v_n]$ for some $v_i \in k(x)$. Each v_i is a rational function $f_i(x)/g_i(x)$ for polynomials $f_i, g_i \in k[x]$. Let $b \in k[x]$ be the product of all denominators, $b = \prod_{i=1}^{n} g_i(x)$. Then $b \cdot v_i \in k[x]$ for all i.

Let $c \in k[x]$ be an irreducible polynomial that does not divide b. Such a polynomial exists because $k[x]$ contains infinitely many non-associate irreducibles. The element $1/c$ is in $k(x)$, so it must be expressible as a polynomial in the generators v_i:

$$\frac{1}{c} = P(v_1, \ldots, v_n)$$

for some polynomial P with coefficients in k. Let N be the total degree of P. If we multiply the equation by b^N, we get:

$$\frac{b^N}{c} = b^N P(v_1, \ldots, v_n) = P(bv_1, \ldots, bv_n)$$

Since each bv_i is in $k[x]$, the right-hand side is a polynomial expression in elements of $k[x]$, and thus is itself an element of $k[x]$. This implies that c must divide b^N in $k[x]$. As c is irreducible, it must divide b. This contradicts our choice of c. Therefore, the initial assumption that $k(x)$ is ring-finite over k must be false. □

Proposition 1.52. *The polynomial ring $k[x]$ is integrally closed in its field of fractions $k(x)$. That is, its integral closure in $k(x)$ is $k[x]$ itself.*

Proof. Let $z \in k(x)$ be an element that is integral over $k[x]$. By definition, z is a root of a monic polynomial with coefficients in $k[x]$:

$$z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0 = 0, \quad \text{where } a_i \in k[x].$$

We can write z as a fraction f/g, where $f, g \in k[x]$ are relatively prime polynomials and $g \neq 0$. Substituting this into the equation and multiplying through by g^n, we obtain:

$$f^n + a_{n-1}f^{n-1}g + \cdots + a_1 f g^{n-1} + a_0 g^n = 0.$$

Rearranging the terms gives:

$$f^n = -g(a_{n-1}f^{n-1} + \cdots + a_1 f g^{n-2} + a_0 g^{n-1}).$$

This equality shows that g divides f^n. Since $k[x]$ is a unique factorization domain and f and g are coprime, this is only possible if g is a unit in $k[x]$. The units of $k[x]$ are the non-zero constant polynomials, so $g \in k \setminus \{0\}$. Therefore, $z = f/g$ is an element of $k[x]$. This shows that any element of $k(x)$ that is integral over $k[x]$ must already be in $k[x]$. □

1.3.3 Zariski's Lemma

The machinery of integral extensions culminates in a celebrated result of Zariski, which forms the algebraic core of the Nullstellensatz proof. It clarifies the structure of field extensions that are also finitely generated as algebras. For a field extension $K \subseteq L$, being finitely generated as a K-algebra ($L = K[v_1, \ldots, v_n]$) is a much stronger condition than being a finitely generated field extension ($L = K(v_1, \ldots, v_n)$).

Proposition 1.53. *The field of rational functions $k(x)$ is a finitely generated field extension of k, but it is not a finitely generated k-algebra.*

Proof. Assume for contradiction that $k(x) = k[v_1, \ldots, v_m]$, where each $v_i = p_i(x)/q_i(x)$ for polynomials $p_i, q_i \in k[x]$. Let $d(x) \in k[x]$ be the product of all denominators, $d(x) = \prod_{i=1}^{m} q_i(x)$. Then any polynomial in the generators v_i can be written as a fraction whose denominator is a power of $d(x)$. Specifically, any element $z \in k[v_1, \ldots, v_m]$ can be written as $P(x)/d(x)^N$ for some $P(x) \in k[x]$ and integer $N \geq 0$. Now, let $f(x) \in k[x]$ be an irreducible polynomial that does not divide $d(x)$. Such a polynomial exists because $k[x]$ contains infinitely many non-associate irreducibles. The element $1/f(x)$ belongs to $k(x)$, so it must be expressible in the form described above:

$$\frac{1}{f(x)} = \frac{P(x)}{d(x)^N} \implies d(x)^N = f(x)P(x).$$

This implies that $f(x)$ divides $d(x)^N$. Since $f(x)$ is irreducible and $k[x]$ is a UFD, $f(x)$ must divide $d(x)$. This contradicts our choice of $f(x)$. The initial assumption must be false. □

Zariski's Lemma asserts that this phenomenon is general: a field that is ring-finite over a subfield must in fact be a finite-degree (and thus algebraic) extension.

Theorem 1.54 (Zariski's Lemma)**.** *Let $K \subseteq L$ be a field extension. If L is finitely generated as a K-algebra, then L is a finite algebraic extension of K.*

Proof. We use induction on the number of algebra generators, n, for $L = K[v_1, \ldots, v_n]$.

Base Case ($n = 1$): $L = K[v]$. Since L is a field, for any non-zero element $p(v) \in L$, its inverse exists in L. If v were transcendental over K, then $K[v]$ would be isomorphic to the polynomial ring $K[t]$, which is not a field. Thus, v must be algebraic over K. In this case, $L = K[v] = K(v)$ is a finite algebraic extension of K.

Inductive Step: Assume the lemma holds for extensions generated by fewer than n elements. Let $L = K[v_1, \ldots, v_n]$ and consider the tower of extensions $K \subseteq K(v_1) \subseteq L$. The field L can be viewed as an algebra over the intermediate field $K_1 = K(v_1)$, generated by $n-1$ elements: $L = K_1[v_2, \ldots, v_n]$. By the inductive hypothesis, L must be a finite algebraic extension of K_1.

We now have two cases for the nature of v_1 over K.

Case 1: v_1 is algebraic over K. In this case, $K_1 = K(v_1)$ is a finite algebraic extension of K. We have a tower $K \subseteq K_1 \subseteq L$ where L/K_1 is algebraic and K_1/K is algebraic. By the transitivity of algebraic extensions, L/K is algebraic. An extension that is both ring-finite and algebraic is module-finite by Corollary 1.48, so L is a finite algebraic extension of K.

Case 2: v_1 is transcendental over K. Let us denote v_1 by x. Then $K_1 = K(x)$ is the field of rational functions in x. Since L is algebraic over $K(x)$, each generator v_i for $i \in \{2, \ldots, n\}$ satisfies a polynomial

equation with coefficients in $K(x)$. By clearing denominators (multiplying by a suitable polynomial in $K[x]$), we find that each v_i is integral over some ring $K[x][1/d_i]$ for a polynomial $d_i \in K[x]$. Let $d = \prod d_i$. Then each v_i is integral over the localization $K[x][1/d]$. This implies that $L = K[x][1/d][v_2, \ldots, v_n]$ is an integral extension of $K[x][1/d]$. Now, consider any element $z \in L$. The element z is integral over $K[x][1/d]$.

This leads to a contradiction. Let $f \in K[x]$ be an irreducible polynomial that does not divide d. The element $1/f$ is in $K(x) \subseteq L$. As an element of L, $1/f$ must be integral over $K[x][1/d]$. This means it satisfies a monic equation:

$$(1/f)^m + c_{m-1}(1/f)^{m-1} + \cdots + c_0 = 0,$$

where $c_j \in K[x][1/d]$. Multiplying by f^m yields $1 = -f(c_{m-1} + c_{m-2}f + \cdots + c_0 f^{m-1})$. The right side is an element of $K[x][1/d]$, and the equation shows that f is invertible in this ring. But the units of $K[x][1/d]$ are of the form $c \cdot d^k$ for $c \in K^\times$. An irreducible polynomial f not dividing d cannot be a unit. This is a contradiction.

Therefore, Case 2 is impossible. By symmetry, every generator v_i must be algebraic over K, and the conclusion follows as in Case 1. □

1.3.4 The Proofs of the Nullstellensätze

With Zariski's Lemma secured, we can now prove the result that motivates this entire line of inquiry.

Theorem 1.55. *Let k be an algebraically closed field. Every maximal ideal $\mathfrak{m}$ of the polynomial ring $S = k[x_1, \ldots, x_n]$ is of the form*

$$\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$$

for some point $(a_1, \ldots, a_n) \in \mathbb{A}^n_k$.

Proof. Let $\mathfrak{m}$ be a maximal ideal in S. The quotient ring $L = S/\mathfrak{m}$ is a field. The canonical projection map $\pi : S \to L$ gives an embedding of k into L (if the kernel of $k \to L$ were non-zero, it would be all of k, making L the zero ring, which is not a field). The field L is generated as a k-algebra by the images of the variables, $\overline{x_1}, \ldots, \overline{x_n}$. Thus, $L = k[\overline{x_1}, \ldots, \overline{x_n}]$ is a ring-finite extension of k.

By Zariski's Lemma, L must be a finite algebraic extension of k. Since k is algebraically closed, the only algebraic extension of k is k itself. Therefore, the inclusion $k \hookrightarrow L$ must be an isomorphism, and $L \cong k$.

This isomorphism means that for each generator $\overline{x_i} \in L$, there is a corresponding unique scalar $a_i \in k$. This implies that $\overline{x_i} = a_i$ in the quotient ring, which is equivalent to the statement that $x_i - a_i \in \mathfrak{m}$ for each $i = 1, \ldots, n$. This containment implies that the ideal $J = (x_1 - a_1, \ldots, x_n - a_n)$ is contained in $\mathfrak{m}$. However, the ideal J is itself maximal (the quotient $S/J \cong k$ is a field). Since $J \subseteq \mathfrak{m}$ and J is maximal, we must have $J = \mathfrak{m}$. □

Proof of the Weak Nullstellensatz (Theorem 1.40). Let $J \subsetneq S$ be a proper ideal. By Zorn's Lemma, J is contained in some maximal ideal $\mathfrak{m} \subseteq S$. The inclusion $J \subseteq \mathfrak{m}$ implies a reverse inclusion of their vanishing loci: $V(\mathfrak{m}) \subseteq V(J)$. By Theorem 1.55, since k is algebraically closed, $\mathfrak{m}$ must be of the form $(x_1 - a_1, \ldots, x_n - a_n)$ for some point $P = (a_1, \ldots, a_n) \in \mathbb{A}^n_k$. The vanishing locus of this ideal is precisely the single point P: $V(\mathfrak{m}) = \{P\}$. Since $\{P\} \subseteq V(J)$, the variety $V(J)$ is non-empty. □

The proof of the Strong Nullstellensatz is a famous and ingenious argument known as the Rabinowitsch Trick.

Proof of Hilbert's Nullstellensatz (Theorem 1.41). The inclusion $\sqrt{J} \subseteq I(V(J))$ is straightforward from the definitions. If $g \in \sqrt{J}$, then $g^N \in J$ for some $N > 0$. For any point $P \in V(J)$, we have $f(P) = 0$ for all $f \in J$. In particular, $g(P)^N = 0$, which implies $g(P) = 0$. Thus, g vanishes on $V(J)$, so $g \in I(V(J))$.

For the reverse inclusion, $I(V(J)) \subseteq \sqrt{J}$, let $g \in I(V(J))$. We must show $g \in \sqrt{J}$. Let $J = (f_1, \ldots, f_r)$. We introduce a new variable, y, and consider the polynomial ring $S[y] = k[x_1, \ldots, x_n, y]$. In this larger ring, define the ideal

$$J' = (f_1, \ldots, f_r, yg - 1).$$

Let $P' = (a_1, \ldots, a_n, b) \in \mathbb{A}_k^{n+1}$ be a point in the vanishing locus $V(J')$. The conditions $f_i(P') = 0$ mean that the point $P = (a_1, \ldots, a_n)$ is in $V(J)$. By our assumption, $g \in I(V(J))$, so $g(P) = 0$. The final generator of J' imposes the condition $b \cdot g(P) - 1 = 0$, which becomes $b \cdot 0 - 1 = 0$, or $-1 = 0$. This is a contradiction. Thus, no such point P' can exist, which means $V(J') = \emptyset$.

By the Weak Nullstellensatz, an empty variety implies that the ideal must be the entire ring. So, $J' = S[y]$. This means $1 \in J'$, so we can write an identity

$$1 = \sum_{i=1}^{r} A_i(x_1, \ldots, y) f_i + B(x_1, \ldots, y)(yg - 1)$$

for some polynomials $A_i, B \in S[y]$. This is a polynomial identity. We can substitute $y = 1/g$ into this identity, which is a valid operation in the field of fractions $k(x_1, \ldots, x_n)$. The equation becomes:

$$1 = \sum_{i=1}^{r} A_i(x_1, \ldots, 1/g) f_i.$$

Let N be the highest power of y appearing in any of the polynomials A_i. Multiplying the equation by g^N clears all denominators, yielding an equation in $S = k[x_1, \ldots, x_n]$:

$$g^N = \sum_{i=1}^{r} \left(g^N A_i(x_1, \ldots, 1/g) \right) f_i.$$

Each term $g^N A_i(\ldots, 1/g)$ is a polynomial in $x_1, \ldots, x_n$. The right-hand side is therefore an element of the ideal $(f_1, \ldots, f_r) = J$. Thus, $g^N \in J$, which by definition means $g \in \sqrt{J}$. □

1.4 Consequences and Applications of the Nullstellensatz

The proof of the Nullstellensatz is a landmark achievement, but its true power lies in its consequences. The theorem unlocks a deep and beautiful correspondence between the geometric world of algebraic sets and the algebraic world of ideals. In this section, we explore this "algebra-geometry dictionary," apply it to classify the fundamental building blocks of plane geometry, and investigate how the algebraic structure of coordinate rings encodes geometric properties of varieties.

1.4.1 The Algebra-Geometry Dictionary

The Weak and Strong Nullstellensatz, taken together, establish a remarkable, order-reversing correspondence between the algebraic subsets of affine space $\mathbb{A}_k^n$ and the radical ideals of the polynomial ring $S = k[x_1, \ldots, x_n]$. This dictionary allows us to translate geometric problems into the language of commutative algebra, where powerful tools are available, and to interpret algebraic results geometrically, providing important intuition.

The fundamental maps are $V(\cdot)$, which takes an ideal to its vanishing locus, and $I(\cdot)$, which takes a set of points to its vanishing ideal. The Nullstellensatz ensures this correspondence is nearly a bijection. Specifically, over an algebraically closed field k:

1. There is a one-to-one, inclusion-reversing correspondence between **algebraic sets** in $\mathbb{A}_k^n$ and **radical ideals** in S.
2. Under this correspondence, the **irreducible algebraic sets** correspond precisely to the **prime ideals** of S.
3. The simplest non-trivial irreducible sets, the **points** of $\mathbb{A}_k^n$, correspond to the **maximal ideals** of S.

This dictionary is summarized in the table below.

Remark 1.56. *The inclusion-reversing nature of the correspondence is intuitive: adding more functions to an ideal (making the ideal larger) imposes more constraints, resulting in a smaller vanishing set. Conversely, requiring a function to vanish on a larger set of points is a stronger condition, so the ideal of such functions will be smaller.*

Table 1: The Algebra-Geometry Dictionary

Geometry (in $\mathbb{A}_k^n$)	**Algebra (in $S = k[x_1, \ldots, x_n]$)**
Algebraic set	Radical ideal
Irreducible algebraic set	Prime ideal
Point $(a_1, \ldots, a_n)$	Maximal ideal $(x_1 - a_1, \ldots, x_n - a_n)$
The empty set $\emptyset$	The unit ideal $(1) = S$
The whole space $\mathbb{A}_k^n$	The zero ideal (0)
Inclusion of sets $X \subseteq Y$	Reverse inclusion of ideals $I(Y) \subseteq I(X)$
Union of sets $X \cup Y$	Intersection of ideals $I(X) \cap I(Y)$
Intersection of sets $X \cap Y$	Radical of the sum of ideals $\sqrt{I(X) + I(Y)}$
Irreducible hypersurface	Principal prime ideal (f), f irreducible
Algebraic subsets of a variety $V(J)$	Radical ideals in the quotient ring S/J

1.4.2 The Structure of Irreducible Sets in the Plane

As a first concrete application of the dictionary, we can classify the irreducible algebraic subsets of the affine plane, $\mathbb{A}_k^2$. An irreducible set is one that cannot be written as the union of two proper algebraic subsets. In the language of ideals, this corresponds to a prime ideal. We seek, therefore, to classify the prime ideals of $k[x, y]$.

The candidates for irreducible algebraic sets in $\mathbb{A}_k^2$ are:

1. **The entire plane**, $\mathbb{A}^2 = V(0)$, corresponding to the prime ideal (0).
2. **Points**, $\{(a, b)\} = V(x - a, y - b)$, corresponding to maximal (and thus prime) ideals.
3. **Irreducible plane curves**, $V(f)$, where $f \in k[x, y]$ is an irreducible polynomial. This corresponds to a principal prime ideal (f).

The empty set, $V(1)$, is irreducible by convention but corresponds to the entire ring, which is not prime. What remains is to show that there are no other possibilities. A prime ideal in $k[x, y]$ must have height 0, 1, or 2. These correspond to the cases above. The only other possibility for an algebraic set would be the vanishing locus of an ideal that is not principal but is also not maximal, such as $V(f, g)$ for two polynomials f, g with no common factors. The following proposition shows that such a set is a finite collection of points, and therefore not irreducible (unless it is a single point, which is already classified).

To prove this, we require some standard results from algebra.

Definition 1.57. *Let R be an integral domain. The **field of fractions** of R, denoted $Frac(R)$, is the smallest field containing R. Its elements are formal fractions*

$$\left\{ \frac{a}{b} \mid a, b \in R, b \neq 0 \right\},$$

with the familiar rules for equality ($\frac{a}{b} = \frac{c}{d} \iff ad = bc$) and arithmetic.

Theorem 1.58 (Gauss's Lemma)**.** *If R is a Unique Factorization Domain (UFD), then so is the polynomial ring $R[t]$. A key consequence is that a polynomial in $R[t]$ is irreducible if and only if it is irreducible when viewed as a polynomial over the field of fractions, $Frac(R)[t]$.*

Proposition 1.59. *Let $f, g \in k[x, y]$ be polynomials with no common factors. Then their common vanishing set $V(f, g)$ is finite.*

Proof. We view the ring $k[x, y]$ as $(k[x])[y]$, a ring of polynomials in y whose coefficients are polynomials in x. Since $k[x]$ is a UFD, Gauss's Lemma applies. The condition that f and g have no common factors in $k[x, y]$ implies they remain coprime as elements of $k(x)[y]$, where $k(x) = \text{Frac}(k[x])$.

The ring $k(x)[y]$ is a polynomial ring in one variable over a field, which makes it a Principal Ideal Domain (PID). In a PID, the ideal generated by two coprime elements is the entire ring. Thus, there exist polynomials

$A(y), B(y) \in k(x)[y]$ such that $A(y)f + B(y)g = 1$. The coefficients of A and B are rational functions in x. We can find a common denominator $d(x) \in k[x]$ for all these coefficients. Multiplying the equation by $d(x)$ clears denominators, yielding an equation

$$\tilde{A}(x,y)f + \tilde{B}(x,y)g = d(x)$$

for some polynomials $\tilde{A}, \tilde{B} \in k[x,y]$ and a non-zero $d(x) \in k[x]$.

Now, consider any point $(x_0, y_0) \in V(f,g)$. By definition, $f(x_0,y_0) = 0$ and $g(x_0,y_0) = 0$. Substituting this point into our equation gives $\tilde{A}(x_0,y_0) \cdot 0 + \tilde{B}(x_0,y_0) \cdot 0 = d(x_0)$, so $d(x_0) = 0$. Since $d(x)$ is a non-zero polynomial in a single variable, it has only a finite number of roots. This shows that any point in $V(f,g)$ must have an x-coordinate from a finite set. By a symmetric argument (viewing $k[x,y]$ as $(k[y])[x]$), the y-coordinates must also belong to a finite set. Therefore, $V(f,g)$ must be a finite set. □

Corollary 1.60. *If $f \in k[x,y]$ is an irreducible polynomial over an algebraically closed field k, then $I(V(f)) = (f)$. Consequently, $V(f)$ is an irreducible algebraic set.*

Proof. Clearly, $(f) \subseteq I(V(f))$. For the reverse inclusion, let $g \in I(V(f))$. This means g vanishes everywhere f does, so $V(f) \subseteq V(g)$, which implies $V(f,g) = V(f)$. Since k is algebraically closed and f is not a constant, the variety $V(f)$ is an infinite set. (To see this, view f as a polynomial in x with coefficients in $k[y]$. For the infinitely many values of $y_0 \in k$ for which the leading coefficient of $f(x,y_0)$ does not vanish, the polynomial $f(x,y_0)$ is a non-zero polynomial in one variable and must have a root x_0.) Since $V(f,g)$ is infinite, our proposition implies that f and g must share a common factor. Because f is irreducible, that common factor must be f itself (up to a unit). Therefore, f divides g, which means $g \in (f)$. Thus, $I(V(f)) = (f)$. Since f is an irreducible element in a UFD, the principal ideal (f) is prime, and the dictionary tells us that $V(f)$ is an irreducible algebraic set. □

1.4.3 Coordinate Rings and Geometric Finiteness

The Nullstellensatz connects a variety $V(J)$ to its radical ideal $\sqrt{J}$. The quotient ring $A(V(J)) = S/\sqrt{J}$ is called the **coordinate ring** of the variety. Its elements are equivalence classes of polynomials, representing the distinct polynomial functions on $V(J)$. A finer algebraic object is the ring S/J itself, sometimes called the ring of functions on the *scheme* defined by J. The structure of this ring, particularly its dimension as a k-vector space, reveals deep geometric information.

Example 1.61 (Dimensions of Coordinate Rings)**.**

1. ***A "fat point":*** *Let $I = (x^2, y) \subseteq k[x,y]$. The variety is $V(I) = \{(0,0)\}$. The ring $S/I = k[x,y]/(x^2,y)$ has relations $\overline{y} = 0$ and $\overline{x}^2 = 0$. Any polynomial reduces to the form $a + b\overline{x}$. Thus, S/I is a 2-dimensional k-vector space with basis $\{1, \overline{x}\}$. The nilpotent element $\overline{x}$ encodes infinitesimal information—a "tangent vector"—at the origin.*
2. ***Two distinct points:*** *Let $I = (y, x(x-1))$. The variety is $V(I) = \{(0,0),(1,0)\}$. The ring is $S/I = k[x,y]/(y, x(x-1)) \cong k[x]/(x^2 - x)$. Since the polynomials x and $x-1$ are coprime, the Chinese Remainder Theorem applies:*

   $$k[x]/(x(x-1)) \cong k[x]/(x) \times k[x]/(x-1) \cong k \times k.$$

   This ring is also 2-dimensional. An element $(c_1, c_2) \in k \times k$ corresponds to a function that takes the value c_1 at the point $(0,0)$ and c_2 at $(1,0)$.
3. ***A finite set on a line:*** *If $f \in k[x]$ is a polynomial of degree $d > 0$ with distinct roots, then $I = (f) \subseteq k[x]$ defines d distinct points. The coordinate ring $k[x]/(f)$ is a d-dimensional vector space with basis $\{1, \overline{x}, \ldots, \overline{x}^{d-1}\}$.*

Remark 1.62 (Toward Schemes)**.** *The ideals $J_1 = (x,y)$ and $J_2 = (x^2,y)$ have the same variety, $V(J_1) = V(J_2) = \{(0,0)\}$, and the same radical, $\sqrt{J_2} = J_1$. However, the quotient rings $S/J_1 \cong k$ and S/J_2 have different dimensions. The vector space dimension $\dim_k(S/J)$ is a finer invariant than the variety itself. It*

is often called the "length" or "multiplicity" of the algebraic set defined by J. This extra algebraic structure, which is lost when passing to the radical, is the central object of study in the modern theory of ***schemes****. Schemes retain the nilpotent elements of S/J, interpreting them as encoding infinitesimal geometric data like tangent directions.*

The general principle illustrated by these examples is captured in the following corollary.

Corollary 1.63. *Let k be an algebraically closed field and $J \subseteq S = k[x_1, \ldots, x_n]$ be an ideal. The variety $V(J)$ is a finite set of points if and only if the quotient ring S/J is a finite-dimensional k-vector space.*

Proof. ($\Longleftarrow$) Assume $\dim_k(S/J)$ is finite. Let $V(J) = \{P_1, \ldots, P_m\}$. We must show m is finite. For any two distinct points P_i, P_j, there exists a linear polynomial L such that $L(P_i) = 0$ and $L(P_j) \neq 0$. By taking products of such linear forms, we can construct, for each $i \in \{1, \ldots, m\}$, a polynomial g_i such that $g_i(P_j) = \delta_{ij}$ (this is a multivariate generalization of Lagrange interpolation).

Consider the images of these polynomials, $\{\overline{g_1}, \ldots, \overline{g_m}\}$, in the vector space S/J. Suppose they are linearly dependent, so $\sum_{i=1}^{m} \lambda_i \overline{g_i} = 0$ for scalars $\lambda_i \in k$. This means the polynomial $G = \sum \lambda_i g_i$ is in the ideal J. As an element of J, G must vanish at every point in $V(J)$. Let's evaluate G at an arbitrary point $P_j \in V(J)$:

$$0 = G(P_j) = \left(\sum_{i=1}^{m} \lambda_i g_i \right)(P_j) = \sum_{i=1}^{m} \lambda_i g_i(P_j) = \lambda_j \cdot 1 = \lambda_j.$$

This holds for all $j = 1, \ldots, m$, so all λ_j must be zero. The set $\{\overline{g_1}, \ldots, \overline{g_m}\}$ is therefore linearly independent in S/J. The size of a linearly independent set cannot exceed the dimension of the space, so we must have $m \leq \dim_k(S/J)$. Since the dimension is finite, m must be finite.

($\Rightarrow$) Assume $V(J) = \{P_1, \ldots, P_m\}$ is a finite set. Let $P_i = (a_{i1}, \ldots, a_{in})$. We want to show that S/J is a finite-dimensional vector space. For each coordinate direction $j \in \{1, \ldots, n\}$, construct a polynomial in one variable, $g_j(x_j)$, whose roots are precisely the j-th coordinates of the points in our set:

$$g_j(x_j) := \prod_{i=1}^{m} (x_j - a_{ij}).$$

By construction, for any point $P_k \in V(J)$, its j-th coordinate a_{kj} is a root of $g_j(x_j)$, so $g_j(P_k) = 0$. This means the polynomial g_j vanishes on all of $V(J)$. By Hilbert's Nullstellensatz, $g_j \in I(V(J)) = \sqrt{J}$. This implies that for some integer $N_j > 0$, we have $g_j^{N_j} \in J$. In the quotient ring S/J, this becomes the relation $\overline{g_j(x_j)}^{N_j} = 0$. This is a monic polynomial equation satisfied by the element $\overline{x_j}$. This relation allows any sufficiently high power of $\overline{x_j}$ to be expressed as a k-linear combination of lower powers. Consequently, any monomial $\overline{x_1}^{e_1} \ldots \overline{x_n}^{e_n}$ in S/J can be reduced to an equivalent expression where each exponent e_j is bounded. The set of monomials with bounded exponents is finite. Since these monomials span the entire space S/J, it must be finite-dimensional. □

1.4.4 The Effective Nullstellensatz

The Strong Nullstellensatz is an existence theorem: it tells us that if a polynomial g vanishes on $V(J)$, then some power of g must lie in J. It does not, however, tell us which power. This leads to a natural computational question: given generators for an ideal J and a polynomial $g \in \sqrt{J}$, can we find an explicit upper bound on the exponent N such that $g^N \in J$?

This question is the subject of the **Effective Nullstellensatz**. Answering it is crucial for creating algorithms in computational algebra, as it turns an existence statement into a constructive one with a known search space. Early bounds were doubly exponential in the number of variables. A major breakthrough provided much sharper, and more practical, bounds.

Theorem 1.64 (Kollár, 1988)**.** *Let k be an algebraically closed field, and let $J = (f_1, \ldots, f_r) \subseteq k[x_1, \ldots, x_n]$ be an ideal where each polynomial f_i has degree at most $d \geq 3$. If a polynomial g vanishes on $V(J)$, then $g^q \in J$ where $q \leq d^n$.*

Remark 1.65. *This result is important because the bound depends only on the number of variables and the maximum degree of the generators, not on the number of generators. It provides a concrete stopping condition for algorithms that need to test for ideal membership in the radical.*

2 Affine Varieties

2.1 Affine Varieties and Regular Maps

We continue our story of making a dictionary between algebraic geometry and commutative algebra.

2.1.1 Affine Varieties and Coordinate Rings

Definition 2.1. *An **affine variety** is an irreducible algebraic set in some affine space $\mathbb{A}^n$.*

By the Nullstellensatz, there is a one-to-one, order-reversing correspondence between algebraic sets in $\mathbb{A}^n$ and radical ideals in the polynomial ring $k[x_1, \ldots, x_n]$. Consequently,

Theorem 2.2. *The correspondence $V(\cdot)$ and $I(\cdot)$ induces a bijection:*

$$\{\text{affine varieties in } \mathbb{A}^n\} \longleftrightarrow \{\text{prime ideals in } k[x_1, \ldots, x_n]\}$$

Having defined our geometric objects, we now turn to the natural class of functions upon them. Just as continuous functions are central to topology, a special class of functions is fundamental to algebraic geometry. We seek functions that respect the inherent polynomial structure of a variety.

Definition 2.3. *Let $V \subseteq \mathbb{A}^n$ be an algebraic set. A function $f : V \to k$ is a **polynomial function** or **regular function** on V if there exists a polynomial $F \in k[x_1, \ldots, x_n]$ such that f is the restriction of F to V. That is, $f(p) = F(p)$ for all $p \in V$.*

The set of all functions from V to k, denoted $\mathcal{F}(V, k)$, forms a ring under pointwise addition and multiplication. It is a straightforward exercise to verify that the subset of regular functions is a subring of $\mathcal{F}(V, k)$.

Definition 2.4. *The ring of regular functions on an algebraic set V is called the **coordinate ring** of V. It is denoted by $\Gamma(V)$.*

Example 2.5. ,

1. *For the entire affine space $\mathbb{A}^n$, any polynomial function is simply a polynomial. Thus, $\Gamma(\mathbb{A}^n) = k[x_1, \ldots, x_n]$.*
2. *Let $V = V(y - x^2) \subseteq \mathbb{A}^2$, the parabola. On V, the polynomial y and the polynomial x^2 define the exact same function, since for any point $(a, b) \in V$, we have $b = a^2$. Thus, in $\Gamma(V)$, the functions represented by y and x^2 are identical.*
3. *Consider the hyperbola $V = V(xy - 1) \subseteq \mathbb{A}^2$. Is the function $f(x, y) = 1/y$ a regular function on V? At first glance, it appears to be a rational function, not a polynomial. However, on V, the defining equation $xy - 1 = 0$ implies that $x = 1/y$. Since x is a polynomial in $k[x, y]$, its restriction to V is a regular function. Therefore, $1/y$ is indeed a regular function on V, as it coincides with the regular function defined by the polynomial x.*

The examples suggest that two different polynomials in $k[x_1, \ldots, x_n]$ can give rise to the same regular function on V. This occurs precisely when their difference vanishes on V. This observation leads to the fundamental structure theorem for coordinate rings. The natural restriction map from polynomials on $\mathbb{A}^n$ to regular functions on V is a surjective ring homomorphism:

$$k[x_1, \ldots, x_n] \twoheadrightarrow \Gamma(V) \quad \text{given by} \quad F \mapsto F|_V$$

The kernel of this map consists of all polynomials F such that $F|_V = 0$, which is by definition the ideal $I(V)$. The First Isomorphism Theorem for rings then yields the following canonical description.

Proposition 2.6. *Let V be an algebraic set in $\mathbb{A}^n$. The coordinate ring of V is isomorphic to the quotient of the polynomial ring by the ideal of V:*

$$\Gamma(V) \cong k[x_1, \ldots, x_n]/I(V)$$

Remark 2.7. *From this proposition, we deduce several crucial properties of* $\Gamma(V)$*.*

- $\Gamma(V)$ *is a finitely-generated* k*-algebra (often called an affine* k*-algebra).*
- *Since* $I(V)$ *is a radical ideal,* $\Gamma(V)$ *is a reduced ring (i.e., its nilradical is trivial).*
- *If* V *is an affine variety, then* $I(V)$ *is a prime ideal. Consequently,* $\Gamma(V)$ *is an integral domain.*

The dictionary extends further. Geometric substructures of a variety V correspond to algebraic substructures in its coordinate ring $\Gamma(V)$.

Definition 2.8. *A* ***subvariety*** *of a variety* V *is a variety* $W \subseteq \mathbb{A}^n$ *that is contained in* V*.*

The correspondences provided by the Nullstellensatz can now be relativized to V and its coordinate ring $\Gamma(V)$.

Theorem 2.9. *Let* V *be an affine variety. There are canonical bijections:*

$$\{\textit{subvarieties of } V\} \longleftrightarrow \{\textit{prime ideals in } \Gamma(V)\}$$
$$\{\textit{points of } V\} \longleftrightarrow \{\textit{maximal ideals in } \Gamma(V)\}$$

If $W \subseteq V$ is a subvariety, there is a natural restriction map $\Gamma(V) \to \Gamma(W)$ given by $f \mapsto f|_W$. The kernel of this map consists of regular functions on V that vanish on W. This set forms an ideal in $\Gamma(V)$, which we denote $I_V(W)$. It corresponds to the prime ideal $I(W)/I(V) \subseteq k[x_1, \ldots, x_n]/I(V)$. We thus have $\Gamma(W) \cong \Gamma(V)/I_V(W)$.

Example 2.10. *Revisiting* $V = V(xy - 1) \subseteq \mathbb{A}^2$*: we saw that on* V*, the relation* $y = 1/x$ *holds. The coordinate ring is therefore*

$$\Gamma(V) = k[x, y]/(xy - 1) \cong k[x, 1/x]$$

the ring of Laurent polynomials in one variable. This is an integral domain, as expected, since V *is a variety.*

2.1.2 Regular Maps Between Varieties

The next step is to define the structure-preserving maps between varieties, analogous to linear transformations between vector spaces or continuous maps between topological spaces. These are the morphisms of our category.

Definition 2.11. *Let* $V \subseteq \mathbb{A}^n$ *and* $W \subseteq \mathbb{A}^m$ *be algebraic sets. A function* $\varphi : V \to W$ *is a* ***regular map*** *(or* ***polynomial map****, or* ***morphism****) if there exist* m *polynomials* $T_1, \ldots, T_m \in k[x_1, \ldots, x_n]$ *such that for every point* $p \in V$*,*

$$\varphi(p) = (T_1(p), T_2(p), \ldots, T_m(p)).$$

Each component function $T_i|_V$ *is an element of* $\Gamma(V)$*.*

Example 2.12. *Consider the morphism* $\varphi : \mathbb{A}^1 \to \mathbb{A}^2$ *defined by the map* $t \mapsto (t, t^2)$*. The image of this morphism is the affine variety* $V = V(y - x^2)$*, which is the parabola in the affine plane.*

We can also consider a map in the opposite direction, $\psi : V \to \mathbb{A}^1$*. Since any point* (x, y) *on the variety* V *satisfies the relation* $y = x^2$*, we can define* ψ *in a couple of ways. For example, we could define it as* $\psi_1(x, y) = y$ *or as* $\psi_2(x, y) = x^2$*. On the variety* V*, these two definitions are equivalent.*

However, if we consider these maps as morphisms from the entire affine plane $\mathbb{A}^2$ *to* $\mathbb{A}^1$*, they are no longer the same. For instance, consider the point* $(2, 3) \in \mathbb{A}^2$*, which is not on the variety* V*. We have* $\psi_1(2, 3) = 3$ *and* $\psi_2(2, 3) = 2^2 = 4$*. This shows that while the two definitions of* ψ *agree on* V*, they are different functions on* $\mathbb{A}^2$*.*

Remark 2.13. *A regular function* $f \in \Gamma(V)$ *is, by this definition, precisely a regular map from* V *to* $\mathbb{A}^1$*.*

Every regular map $\varphi : V \to W$ induces a map on the corresponding coordinate rings, but in the reverse direction. Given a regular function $g \in \Gamma(W)$, we can pre-compose it with φ to obtain a regular function on V:

$$V \xrightarrow{\varphi} W \xrightarrow{g} k$$

The composition $g \circ \varphi$ is a regular function on V. This defines a k-algebra homomorphism $\varphi^* : \Gamma(W) \to \Gamma(V)$, called the **pullback** map, by the rule $\varphi^*(g) = g \circ \varphi$.

Remark 2.14. *This construction is functorial. Let $id_V : V \to V$ be the identity morphism. Then $id_V^*(f) = f \circ id_V = f$, so id_V^* is the identity on $\Gamma(V)$. Furthermore, if $\varphi : V \to W$ and $\psi : W \to X$ are regular maps, one can check that $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$. This means that the assignment $V \mapsto \Gamma(V)$ and $\varphi \mapsto \varphi^*$ defines a **contravariant functor** from the category of algebraic sets to the category of reduced, finitely-generated k-algebras.*

Example 2.15.

- *Consider the morphism $\varphi : \mathbb{A}^3 \to \mathbb{A}^2$ given by $(x, y, z) \mapsto (x^2 y, x - z)$. This induces a pullback homomorphism $\varphi^* : k[u, v] \to k[x, y, z]$ defined on the generators of the coordinate ring $k[u, v]$ as:*

$$\varphi^*(u) = x^2 y$$
$$\varphi^*(v) = x - z$$

- *Let $X \subseteq \mathbb{A}^m$ be a closed subvariety with the inclusion map $i : X \hookrightarrow \mathbb{A}^m$. The pullback $i^* : k[x_1, \ldots, x_m] \to \Gamma(X)$ is defined by its action on the generators:*

$$i^*(x_j) = \overline{x_j}$$

  for each coordinate function x_j. This map is the natural quotient map $k[x_1, \ldots, x_m] \to k[x_1, \ldots, x_m]/I(X)$, where $I(X)$ is the ideal of X.

Now, we present the central claim for this subsection:

Proposition 2.16. *Let $V \subseteq \mathbb{A}^n$ and $W \subseteq \mathbb{A}^m$ be algebraic sets. The map that sends a regular map $\varphi : V \to W$ to its pullback $\varphi^* : \Gamma(W) \to \Gamma(V)$ is a bijection:*

$$Hom_{AffVar}(V, W) \cong Hom_{k-alg}(\Gamma(W), \Gamma(V))$$

Proof. We have already constructed the map $\varphi \mapsto \varphi^*$. We must show it is both surjective and injective.

(Surjectivity) Let $\alpha : \Gamma(W) \to \Gamma(V)$ be an arbitrary k-algebra homomorphism. We must construct a regular map $\psi : V \to W$ such that $\psi^* = \alpha$. Let $\Gamma(W) = k[y_1, \ldots, y_m]/I(W)$. The coordinate functions on W are the images $\bar{y}_j \in \Gamma(W)$ of the variables y_j. Their images under α, namely $\alpha(\bar{y}_j)$, are regular functions on V. For each $j = 1, \ldots, m$, let us choose a representative polynomial $T_j \in k[x_1, \ldots, x_n]$ for the function $\alpha(\bar{y}_j)$.

Define a map $\psi : V \to \mathbb{A}^m$ by setting $\psi(p) = (T_1(p), \ldots, T_m(p))$ for any $p \in V$. By construction, ψ is a map whose components are polynomial functions, so it is a candidate for a regular map. First, we must verify that its image lies in W. A point $q \in \mathbb{A}^m$ is in $W = V(I(W))$ if and only if $g(q) = 0$ for all polynomials $g \in I(W)$. Let $p \in V$ be arbitrary. For any $g(y_1, \ldots, y_m) \in I(W)$, its image $\bar{g}$ in $\Gamma(W)$ is zero. Then we evaluate g at the image point $\psi(p)$:

$$g(\psi(p)) = g(T_1(p), \ldots, T_m(p)).$$

Since α is a k-algebra homomorphism and $\alpha(\bar{y}_j)$ is the function represented by T_j, the value of the polynomial $g(T_1, \ldots, T_m)$ at p is the same as the value of the function $\alpha(\bar{g})$ at p. But $\bar{g} = 0$ in $\Gamma(W)$, so $\alpha(\bar{g}) = \alpha(0) = 0$. The function $\alpha(\bar{g})$ is the zero function on V. Thus, $g(\psi(p)) = 0$. This holds for all $p \in V$ and all $g \in I(W)$, which shows $\psi(V) \subseteq W$. So ψ is a regular map from V to W.

Finally, we check that $\psi^* = \alpha$. It suffices to check this on the generators $\bar{y}_j$ of $\Gamma(W)$. For any j,

$$\psi^*(\bar{y}_j) = \bar{y}_j \circ \psi.$$

By definition of ψ, this is the function on V given by the polynomial T_j, which is precisely how we defined T_j: as a representative for $\alpha(\bar{y}_j)$. Thus $\psi^*(\bar{y}_j) = \alpha(\bar{y}_j)$, and since they agree on generators, $\psi^* = \alpha$.

(Injectivity) Suppose $\psi, \varphi : V \to W$ are regular maps such that $\psi^* = \varphi^*$. Let the component functions of ψ be $\{T_j|_V\}_{j=1}^m$ and those of φ be $\{S_j|_V\}_{j=1}^m$. The equality $\psi^* = \varphi^*$ means that for any $g \in \Gamma(W)$, $g \circ \psi = g \circ \varphi$ as functions on V. In particular, we may choose g to be the j-th coordinate function on W, $g = \bar{y}_j$. Then

$$\psi^*(\bar{y}_j) = \bar{y}_j \circ \psi = T_j|_V \quad \text{and} \quad \varphi^*(\bar{y}_j) = \bar{y}_j \circ \varphi = S_j|_V.$$

The condition $\psi^* = \varphi^*$ implies $T_j|_V = S_j|_V$ for all $j = 1, \ldots, m$. This means the component functions of the maps ψ and φ are identical. Therefore, $\psi(p) = \varphi(p)$ for all $p \in V$, so $\psi = \varphi$. □

Example 2.17. *Let $n \geq r$. Consider the projection $\varphi : \mathbb{A}^n \to \mathbb{A}^r$ defined by $(x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_r)$. This is a regular map. Its pullback $\varphi^* : \Gamma(\mathbb{A}^r) \to \Gamma(\mathbb{A}^n)$ is the homomorphism $k[y_1, \ldots, y_r] \to k[x_1, \ldots, x_n]$ that sends a polynomial $g(y_1, \ldots, y_r)$ to $g(x_1, \ldots, x_r)$. This is the natural inclusion map of polynomial rings.*

Example 2.18 (Constructing a Map from a Homomorphism)**.** *Let's construct the geometric map corresponding to the k-algebra homomorphism*

$$\alpha : k[x, y, z] \to k[u, v]/(u - v^3)$$

defined by $x \mapsto \bar{u}$, $y \mapsto 2\bar{u}$, and $z \mapsto 3\bar{u}$. Here, the domain is $\Gamma(\mathbb{A}^3)$ and the codomain is $\Gamma(V)$ for the variety $V = V(u - v^3) \subseteq \mathbb{A}^2$. The map α corresponds to a regular map $\varphi : V \to \mathbb{A}^3$. Following the proof of Proposition 2.16, the components of φ are given by the images of the coordinate functions of the target space $\mathbb{A}^3$.

$$\varphi = (\alpha(\bar{x}), \alpha(\bar{y}), \alpha(\bar{z})).$$

Given a point $(a, b) \in V$, so that $a = b^3$, the map is

$$\varphi(a, b) = (a, 2a, 3a) = (b^3, 2b^3, 3b^3).$$

2.1.3 Isomorphisms and Geometric Properties

The notion of equivalence in the category of affine varieties is that of isomorphism.

Definition 2.19. *A regular map $\varphi : V \to W$ is an **isomorphism** if there exists a regular map $\psi : W \to V$ such that $\psi \circ \varphi = id_V$ and $\varphi \circ \psi = id_W$.*

Remark 2.20. *A bijective regular map is not necessarily an isomorphism. The inverse map, which is guaranteed to exist as a set map, must also be regular. A classic counterexample is the map $\varphi : \mathbb{A}^1 \to C = V(y^2 - x^3)$ given by $t \mapsto (t^2, t^3)$. This map is a bijection, but its inverse is not regular at the origin $(0, 0) \in C$.*

The correspondence between maps and homomorphisms immediately gives a criterion for isomorphism.

Corollary 2.21. *A regular map $\varphi : V \to W$ is an isomorphism if and only if its pullback $\varphi^* : \Gamma(W) \to \Gamma(V)$ is a k-algebra isomorphism.*

Proof. This is a direct consequence of the functoriality of the pullback construction. If φ is an isomorphism with inverse ψ, then $\varphi \circ \psi = \mathrm{id}_W$ and $\psi \circ \varphi = \mathrm{id}_V$. Applying the contravariant functor Γ yields $(\varphi \circ \psi)^* = \psi^* \circ \varphi^* = \mathrm{id}_{\Gamma(W)}$ and similarly $\varphi^* \circ \psi^* = \mathrm{id}_{\Gamma(V)}$. This shows φ^* is an isomorphism with inverse ψ^*. The converse follows by applying the correspondence from Proposition 2.16 to the inverse homomorphism. □

Example 2.22. *The map $\varphi : \mathbb{A}^1 \to V = V(y - x^2)$ given by $t \mapsto (t, t^2)$ is an isomorphism. Its inverse is $\psi : V \to \mathbb{A}^1$ given by $(x, y) \mapsto x$, which is clearly regular. Algebraically, the pullback $\varphi^* : \Gamma(V) \to \Gamma(\mathbb{A}^1)$ is the map*

$$\varphi^* : k[x, y]/(y - x^2) \to k[t] \quad \text{sending} \quad \bar{x} \mapsto t, \quad \bar{y} \mapsto t^2.$$

This is an isomorphism, as $k[x, y]/(y - x^2) \cong k[x]$, and the map becomes the isomorphism $k[x] \to k[t]$ sending $x \mapsto t$.

Example 2.23. *Let $T : \mathbb{A}^n \to \mathbb{A}^n$ be a regular map where each component T_i is a polynomial of degree 1, and assume T is a bijection. Such a map is called an **affine change of coordinates**. Any such map can be decomposed as $T = \tau \circ L$, where $L : \mathbb{A}^n \to \mathbb{A}^n$ is an invertible linear transformation and $\tau : \mathbb{A}^n \to \mathbb{A}^n$ is a translation. Both L and τ are regular maps, and their inverses (L^{-1} and translation by the opposite vector) are also regular. The composition of isomorphisms is an isomorphism, so any affine change of coordinates is an isomorphism of $\mathbb{A}^n$ with itself.*

Regular maps behave well with respect to topological properties (in the Zariski topology).

Lemma 2.24. *Let $\varphi : V \to W$ be a regular map and let $X \subseteq W$ be an algebraic set.*

1. *The preimage $\varphi^{-1}(X)$ is an algebraic set in V.*
2. *If $X \subseteq \varphi(V)$ and $\varphi^{-1}(X)$ is irreducible, then X is irreducible.*

Proof. 1. Since regular maps are continuous in the Zariski topology, this is immediate. More constructively, let $X = V(f_1, \ldots, f_r)$ for some polynomials f_i whose restrictions define functions in $\Gamma(W)$. A point $p \in V$ is in $\varphi^{-1}(X)$ if and only if $\varphi(p) \in X$, which means $f_i(\varphi(p)) = 0$ for all i. This is equivalent to $(\varphi^*(f_i))(p) = 0$ for all i. Thus,

$$\varphi^{-1}(X) = \{p \in V \mid (\varphi^*(f_i))(p) = 0 \text{ for all } i\} = V(\varphi^*(f_1), \ldots, \varphi^*(f_r)),$$

which is an algebraic set in V.

2. Suppose $X = A \cup B$ for closed subsets $A, B \subseteq X$. Then $\varphi^{-1}(X) = \varphi^{-1}(A) \cup \varphi^{-1}(B)$. Since $\varphi^{-1}(X)$ is irreducible, we must have $\varphi^{-1}(A) = \varphi^{-1}(X)$ or $\varphi^{-1}(B) = \varphi^{-1}(X)$. Suppose the former holds. Since we assumed $X \subseteq \varphi(V)$ (i.e., the map is surjective onto X), we can apply φ to both sides to get $\varphi(\varphi^{-1}(A)) = \varphi(\varphi^{-1}(X))$. This implies $A = X$. Hence X is irreducible.

□

Remark 2.25. *The converse of part 2 is false; the image of an irreducible variety need not be irreducible. However, this is only possible if the image is not a variety. It is a more advanced result (Chevalley's Theorem) that the image of a variety contains a dense open subset of its closure.*

2.1.4 Injectivity and Surjectivity

A surjective map of sets $f : A \to B$ implies that any function on B that becomes zero when pulled back to A must have been zero to begin with. The same holds for regular maps.

Proposition 2.26. *If a regular map $\varphi : V \to W$ is surjective, then its pullback $\varphi^* : \Gamma(W) \to \Gamma(V)$ is injective.*

Proof. Let $f \in \Gamma(W)$ be an element in the kernel of φ^*, so $\varphi^*(f) = 0$. By definition, this means the composite function $f \circ \varphi : V \to k$ is the zero function. Since φ is surjective, for any point $q \in W$, there exists some $p \in V$ such that $\varphi(p) = q$. We may then evaluate f at this point:

$$f(q) = f(\varphi(p)) = (f \circ \varphi)(p) = 0.$$

As this holds for all $q \in W$, the function f must be the zero function in $\Gamma(W)$. Thus, $\ker(\varphi^*) = \{0\}$, and φ^* is injective. □

Remark 2.27. *The converse to this proposition is false. An injective pullback does not imply a surjective morphism.*

Example 2.28. *Consider the hyperbola $V = V(xy - 1) \subseteq \mathbb{A}^2$. Define a morphism $\varphi : V \to \mathbb{A}^1$ by the projection onto the first coordinate: $\varphi(x, y) = x$. The pullback map on coordinate rings is*

$$\varphi^* : \Gamma(\mathbb{A}^1) \to \Gamma(V) \quad \textit{which is} \quad k[t] \to k[x, y]/(xy - 1) \quad \textit{sending} \quad t \mapsto x.$$

Since $\Gamma(V) \cong k[x, 1/x]$, the map φ^* is the natural inclusion of the polynomial ring $k[x]$ into the larger ring of Laurent polynomials $k[x, 1/x]$. This is clearly an injection.

However, the map φ is not surjective. The point $0 \in \mathbb{A}^1$ is not in the image, because if $\varphi(x, y) = x = 0$, the defining equation $xy - 1 = 0$ would imply $-1 = 0$, a contradiction. The image is $\varphi(V) = \mathbb{A}^1 \setminus \{0\}$. This set is not a closed algebraic set in $\mathbb{A}^1$. (This phenomenon, where the image of a variety is not necessarily closed, is specific to the affine setting. As we will see, morphisms between projective varieties always have closed images.)

The example shows that the correct geometric notion corresponding to an injective pullback is not surjectivity, but rather that the image is topologically dense.

Definition 2.29. *A regular map $\varphi : V \to W$ is **dominant** if its image is dense in the Zariski topology of W, i.e., $\overline{\varphi(V)} = W$.*

Proposition 2.30. *A regular map $\varphi : V \to W$ between affine varieties is dominant if and only if its pullback $\varphi^* : \Gamma(W) \to \Gamma(V)$ is injective.*

Proof. The pullback φ^* is injective if and only if its kernel is trivial. Let's identify the kernel. An element $\bar{f} \in \Gamma(W)$ (represented by a polynomial f) is in $\ker(\varphi^*)$ if and only if $\varphi^*(\bar{f}) = \bar{f} \circ \varphi = 0$. This means the function f vanishes on the image set $\varphi(V)$. This is precisely the condition that $f \in I(\varphi(V))$. Therefore, $\ker(\varphi^*) = I(\varphi(V))/I(W)$.

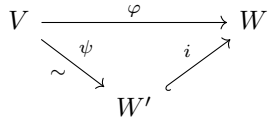
($\Rightarrow$) Assume φ^* is injective. Then $\ker(\varphi^*) = \{0\}$, which implies $I(\varphi(V)) = I(W)$. By the Nullstellensatz, taking the vanishing locus of both sides gives $V(I(\varphi(V))) = V(I(W))$. This translates to $\overline{\varphi(V)} = W$, so φ is dominant.

($\Leftarrow$) Assume φ is dominant. This means $\overline{\varphi(V)} = W$, which by the Nullstellensatz implies $I(\overline{\varphi(V)}) = I(W)$. Since $I(\overline{S}) = I(S)$ for any set S, we have $I(\varphi(V)) = I(W)$. Now, suppose $\bar{f} \in \Gamma(W)$ is in the kernel of φ^*. This means $f \in I(\varphi(V))$. But since this ideal is equal to $I(W)$, we have $f \in I(W)$, which means $\bar{f} = 0$ in $\Gamma(W) = k[\mathbf{y}]/I(W)$. Thus, the kernel is trivial and φ^* is injective. □

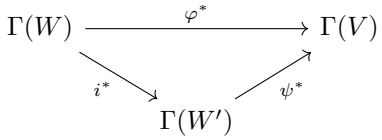
We now analyze the dual situation: what is the geometric meaning of a surjective pullback? It corresponds to the map being an isomorphism onto a closed subvariety of the target.

Proposition 2.31. *A regular map $\varphi : V \to W$ induces a surjective pullback $\varphi^* : \Gamma(W) \to \Gamma(V)$ if and only if φ is an isomorphism from V onto a closed subvariety of W. Such a map is often called a **closed embedding**.*

Proof. ($\Leftarrow$) First, assume that φ is an isomorphism from V onto a closed subvariety $W' \subseteq W$. This means the map φ can be factored as the composition of an isomorphism $\psi : V \xrightarrow{\sim} W'$ followed by the inclusion map $i : W' \hookrightarrow W$.



By the contravariant nature of the coordinate ring functor, the pullback $\varphi^* : \Gamma(W) \to \Gamma(V)$ factors as the composition of the pullbacks of i and ψ:



We analyze the two maps in this composition:

1. The map $i : W' \hookrightarrow W$ is a closed embedding of an algebraic set. Its pullback $i^* : \Gamma(W) \to \Gamma(W')$ is the natural restriction homomorphism, which sends a function on W to its restriction on W'. This map is always surjective.
2. The map $\psi : V \to W'$ is an isomorphism of varieties. Its pullback $\psi^* : \Gamma(W') \to \Gamma(V)$ must therefore be a k-algebra isomorphism.

The map $\varphi^* = \psi^* \circ i^*$ is the composition of a surjective homomorphism followed by an isomorphism. Such a composition is always surjective. This completes the first direction.

($\Rightarrow$) Conversely, assume the pullback $\varphi^* : \Gamma(W) \to \Gamma(V)$ is surjective. Let $W' = \overline{\varphi(V)}$. As the closure of the image of an irreducible set, W' is a closed subvariety of W. We can view φ as a map from V to W', which we will call $\psi : V \to W'$.

$$V \xrightarrow{\psi} W' \xhookrightarrow{i} W, \quad V \xrightarrow{\varphi} W$$

By its very construction, the image of ψ is dense in its codomain W', meaning ψ is a dominant map. A key result states that a morphism is dominant if and only if its pullback is injective. Therefore, the pullback $\psi^* : \Gamma(W') \to \Gamma(V)$ is an **injective** k-algebra homomorphism.

Now consider the corresponding diagram of pullbacks:

$$\begin{array}{ccc} \Gamma(W) & \xrightarrow{\varphi^*} & \Gamma(V) \\ & {\scriptstyle i^*} \searrow \quad \nearrow {\scriptstyle \psi^*} & \\ & \Gamma(W') & \end{array}$$

This diagram commutes, meaning $\varphi^* = \psi^* \circ i^*$. We know the following:

1. φ^* is surjective by our initial assumption.
2. i^* is the surjective restriction map from $\Gamma(W)$ to $\Gamma(W')$.

Since the total map φ^* is surjective, and it factors through ψ^*, the map ψ^* must also be surjective. To see this, let $g \in \Gamma(V)$. Since φ^* is surjective, there exists an $f \in \Gamma(W)$ such that $\varphi^*(f) = g$. Then $g = \psi^*(i^*(f))$. The element $i^*(f) \in \Gamma(W')$ is a preimage of g under ψ^*, proving its surjectivity.

We have now shown that $\psi^* : \Gamma(W') \to \Gamma(V)$ is both injective (from dominance) and surjective. It is therefore a k-algebra isomorphism. This implies that the corresponding geometric map $\psi : V \to W'$ is an isomorphism of varieties. Since $W' = \overline{\varphi(V)}$ is a closed subvariety of W, we have shown that φ is an isomorphism onto a closed subvariety, as required. □

2.2 Rational Functions and Local Rings

Having established the global algebraic object associated with a variety (its coordinate ring $\Gamma(V)$), we now turn our attention to functions that may not be defined everywhere. This move from "polynomial" to "rational" functions allows for a more local analysis of a variety's geometry, analogous to the transition from polynomials to rational functions in single-variable calculus.

2.2.1 Basic Definitions

Let $V \subseteq \mathbb{A}^n$ be an affine variety. Since V is irreducible, its ideal $I(V)$ is prime, and consequently, the coordinate ring $\Gamma(V) = k[x_1, \ldots, x_n]/I(V)$ is an integral domain. This algebraic fact allows us to construct its field of fractions, which we interpret geometrically as the field of rational functions on V.

Definition 2.32. *The **field of rational functions** on a variety V, denoted $k(V)$, is the field of fractions of its coordinate ring $\Gamma(V)$. An element $f \in k(V)$ is called a **rational function** on V.*

An element $f \in k(V)$ is an equivalence class of fractions $\frac{g}{h}$, where $g, h \in \Gamma(V)$ and $h \neq 0$. The equivalence relation is the usual one for fractions: $\frac{g}{h} = \frac{g'}{h'}$ if and only if $gh' = g'h$ in $\Gamma(V)$.

Example 2.33. *Consider the quadric cone $V = V(xy - z^2) \subseteq \mathbb{A}^3$. In its coordinate ring $\Gamma(V)$, we have the relation $\bar{x}\bar{y} = \bar{z}^2$. Consider the rational function $f = \frac{\bar{x}}{\bar{z}} \in k(V)$. Multiplying the numerator and denominator by $\bar{y}$ is not helpful, but we can use the ring relation:*

$$\frac{\bar{x}}{\bar{z}} = \frac{\bar{x}\bar{z}}{\bar{z}^2} = \frac{\bar{x}\bar{z}}{\bar{x}\bar{y}} = \frac{\bar{z}}{\bar{y}}.$$

Thus, $\frac{\bar{x}}{\bar{z}}$ and $\frac{\bar{z}}{\bar{y}}$ represent the same rational function on V.

Unlike a regular function, a rational function may not be defined at every point of the variety. The ability to choose different representatives for the same function is important for determining its domain.

Definition 2.34. *A rational function $f \in k(V)$ is said to be **defined** or **regular** at a point $P \in V$ if there exists a representation $f = \frac{g}{h}$ with $g, h \in \Gamma(V)$ such that the denominator does not vanish at P, i.e., $h(P) \neq 0$.*

Example 2.35. *Let $f = \frac{\bar{x}}{\bar{z}} = \frac{\bar{z}}{\bar{y}}$ on $V = V(xy - z^2)$. The representation $\frac{\bar{x}}{\bar{z}}$ shows that f is defined at any point where $\bar{z} \neq 0$. The representation $\frac{\bar{z}}{\bar{y}}$ shows it is also defined where $\bar{y} \neq 0$. Therefore, f is regular at any point $(a, b, c) \in V$ as long as $b \neq 0$ or $c \neq 0$.*

2.2.2 The Pole Set of a Rational Function

The set of points where a rational function is not defined is of fundamental importance.

Definition 2.36. *A point $P \in V$ is a **pole** of a rational function $f \in k(V)$ if f is not regular at P. The set of all poles of f is called the **pole set** of f.*

This means that for a pole P, every possible representation $f = \frac{g}{h}$ has a denominator that vanishes at P, i.e., $h(P) = 0$.

Remark 2.37. *If the coordinate ring $\Gamma(V)$ happens to be a Unique Factorization Domain (UFD), the situation is simpler. Any $f \in k(V)$ has a unique representation $f = \frac{a}{b}$ where $a, b \in \Gamma(V)$ are coprime. In this case, the pole set of f is precisely the zero locus of the denominator, $V(b) \subseteq V$. However, $\Gamma(V)$ is not a UFD in general. For $V = V(xy - z^2)$, the coordinate ring $\Gamma(V)$ is not a UFD, which is why we needed to consider multiple representations of $f = \frac{\bar{x}}{\bar{z}}$.*

Despite this, the pole set always has a nice geometric structure.

Proposition 2.38. *The set of poles of a rational function $f \in k(V)$ is a proper algebraic subset of V.*

Proof. Let $f \in k(V)$. To identify the pole set, we consider all possible denominators for f. Let $J_f \subseteq \Gamma(V)$ be the set of all possible denominators, more formally defined as:

$$J_f = \{h \in \Gamma(V) \mid hf \in \Gamma(V)\}.$$

It is a straightforward exercise to verify that J_f is a non-zero ideal of $\Gamma(V)$. Now we relate this ideal to the pole set.

Let $P \in V$. The function f is regular at P if and only if there exists a representation $f = \frac{g}{h}$ with $h(P) \neq 0$. The condition $f = \frac{g}{h}$ is equivalent to $hf = g \in \Gamma(V)$, which means $h \in J_f$. Therefore:

$$\begin{aligned} P \text{ is not a pole of } f &\iff f \text{ is regular at } P \\ &\iff \exists h \in \Gamma(V) \text{ s.t. } f = g/h \text{ and } h(P) \neq 0 \\ &\iff \exists h \in J_f \text{ s.t. } h(P) \neq 0 \\ &\iff P \notin V(J_f). \end{aligned}$$

Thus, the pole set of f is precisely the algebraic set $V(J_f)$. Since J_f is a non-zero ideal (as f must have at least one denominator), $V(J_f)$ is a proper subset of V. □

2.2.3 Local Rings of a Variety

The set of all functions regular at a point forms a ring, which allows us to study the "local" geometry of a variety near that point.

Definition 2.39. *Let V be an affine variety and let $P \in V$ be a point. The* ***local ring of*** *V* ***at*** *P, denoted $\mathcal{O}_P(V)$, is the set of all rational functions on V that are regular at P:*

$$\mathcal{O}_P(V) = \{f \in k(V) \mid f \text{ is regular at } P\} = \left\{ \frac{g}{h} \mid g, h \in \Gamma(V), h(P) \neq 0 \right\}.$$

It is a straightforward verification that $\mathcal{O}_P(V)$ forms a subring of the function field $k(V)$. The inclusions $k \subseteq \Gamma(V) \subseteq \mathcal{O}_P(V) \subseteq k(V)$ are clear, with a regular function g being identified with the fraction $g/1$.

Example 2.40. *It is important to distinguish the local ring $\mathcal{O}_P(V)$ from the coordinate ring of the point itself, $\Gamma(P)$. Let P be the origin in $\mathbb{A}^1$, so that $P = V(x)$. The point P is itself a variety, and its coordinate ring is $\Gamma(P) = k[x]/(x) \cong k$. Its function field is thus also $k(P) \cong k$.*

However, the local ring of the ambient space $\mathbb{A}^1$ at P is $\mathcal{O}_P(\mathbb{A}^1)$. This ring is not a field. For instance, the function x (represented by $x/1$) is in $\mathcal{O}_P(\mathbb{A}^1)$ since its denominator does not vanish at P. But its inverse, $1/x$, is not in $\mathcal{O}_P(\mathbb{A}^1)$ because any representation of $1/x$ must have a denominator divisible by x, which necessarily vanishes at P. This example gives us two key facts:

- *A function can be a non-zero element in $\mathcal{O}_P(V)$ even if its evaluation at P is zero. The function $x \in \mathcal{O}_P(\mathbb{A}^1)$ is not the zero element, though its value $x(P)$ is 0.*
- *The ring $\mathcal{O}_P(V)$ contains information about the ambient variety V in a neighborhood of P, not just about the point P in isolation.*

Proposition 2.41. *The set $\mathcal{O}_P(V)$ is a subring of the function field $k(V)$ that contains the coordinate ring $\Gamma(V)$.*

Proof. Let $f_1 = a/b$ and $f_2 = c/d$ be two elements of $\mathcal{O}_P(V)$, where $a, b, c, d \in \Gamma(V)$ and $b(P) \neq 0$, $d(P) \neq 0$. Since $\Gamma(V)$ is an integral domain, the product $b(P)d(P)$ is also non-zero. The difference and product of these functions are

$$f_1 - f_2 = \frac{ad - bc}{bd} \quad \text{and} \quad f_1 f_2 = \frac{ac}{bd}.$$

In both cases, the denominator bd does not vanish at P, so both $f_1 - f_2$ and $f_1 f_2$ belong to $\mathcal{O}_P(V)$. Thus, $\mathcal{O}_P(V)$ is a subring of $k(V)$. The inclusion $\Gamma(V) \subseteq \mathcal{O}_P(V)$ is given by identifying any $g \in \Gamma(V)$ with the fraction $g/1$. □

While local rings describe local data, they can be aggregated to recover global information. A function that is regular everywhere must be a global polynomial function.

Proposition 2.42. *For any affine variety V, the coordinate ring is the intersection of all its local rings:*

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

Proof. The inclusion $\Gamma(V) \subseteq \bigcap_{P \in V} \mathcal{O}_P(V)$ is clear. For the reverse inclusion, let $f \in \bigcap_{P \in V} \mathcal{O}_P(V)$. This means f is regular at every point of V, so its pole set is empty. The pole set is $V(J_f)$, where $J_f = \{h \in \Gamma(V) \mid hf \in \Gamma(V)\}$. An empty pole set means $V(J_f) = \emptyset$. By the weak Nullstellensatz, this implies that the ideal J_f cannot be proper, so $J_f = \Gamma(V)$. In particular, the unit element $1 \in J_f$. By definition of J_f, this means $1 \cdot f = f \in \Gamma(V)$. □

For any $f \in \mathcal{O}_P(V)$, we can define its value at P. If $f = g/h$ with $h(P) \neq 0$, we define $f(P) = g(P)/h(P)$. This value is well-defined, for if $f = g'/h'$ is another representation with $h'(P) \neq 0$, then $gh' = g'h$ in $\Gamma(V)$. Evaluating at P gives $g(P)h'(P) = g'(P)h(P)$, which implies $g(P)/h(P) = g'(P)/h'(P)$ in k. This evaluation process defines a surjective ring homomorphism $\mathrm{ev}_P : \mathcal{O}_P(V) \to k$. The kernel of this map,

$\ker(\text{ev}_P) = \{f \in \mathcal{O}_P(V) \mid f(P) = 0\}$, is therefore a maximal ideal, which we denote by $\mathfrak{m}_P(V)$. This ideal consists of precisely the non-units of $\mathcal{O}_P(V)$, which justifies the name "local ring."

Definition 2.43. *A commutative ring R with unity is a **local ring** if it satisfies one of the following equivalent conditions:*

1. *The set of all non-units in R forms an ideal.*
2. *R has a unique maximal ideal.*

Proof. (1) $\Rightarrow$ (2): Let $\mathfrak{m}$ be the ideal of non-units. Any other proper ideal $I \subsetneq R$ must consist entirely of non-units (as it cannot contain a unit), so $I \subseteq \mathfrak{m}$. This makes $\mathfrak{m}$ the unique maximal ideal.

(2) $\Rightarrow$ (1): Let $\mathfrak{m}$ be the unique maximal ideal. Every non-unit $a \in R$ generates a proper principal ideal $(a) \subsetneq R$. By Zorn's Lemma, (a) must be contained in some maximal ideal, which must be $\mathfrak{m}$. Thus, $\mathfrak{m}$ contains all non-units. Since $\mathfrak{m}$ is a proper ideal, it contains no units, so it is precisely the set of non-units. □

Example 2.44.

1. *The ring $R = \{a/b \in \mathbb{Q} \mid a, b \in \mathbb{Z}, b \text{ is odd}\}$ is the localization of $\mathbb{Z}$ at the prime ideal (2). It is a local ring whose unique maximal ideal is $(2/1)$, the set of fractions whose numerator is even.*
2. *The polynomial ring $\mathbb{C}[x]$ is not a local ring. The elements x and $x - 1$ are non-units, but their sum, 1, is a unit. Thus the non-units do not form an ideal.*
3. *The ring $\mathcal{O}_0(\mathbb{A}^1) = \{g/h \in k(x) \mid h(0) \neq 0\}$ is a local ring. Its maximal ideal is $(x/1)$, the set of all rational functions that vanish at the origin.*

Proposition 2.45. *The local ring $\mathcal{O}_P(V)$ is a Noetherian ring.*

Proof. Let $I \subseteq \mathcal{O}_P(V)$ be an ideal. We aim to show I is finitely generated. Consider the contraction of I to the coordinate ring, $J = I \cap \Gamma(V)$. This is an ideal of $\Gamma(V)$. Since $\Gamma(V)$ is a quotient of a polynomial ring, it is Noetherian, so J must be finitely generated. Let $J = (g_1, \ldots, g_r)_{\Gamma(V)}$ for some $g_i \in \Gamma(V)$.

We claim these same elements also generate I as an ideal in $\mathcal{O}_P(V)$. The inclusion $(g_1, \ldots, g_r)_{\mathcal{O}_P(V)} \subseteq I$ is clear. For the other direction, take any $f \in I$. Since $f \in \mathcal{O}_P(V)$, we can write $f = a/b$ for some $a, b \in \Gamma(V)$ with $b(P) \neq 0$. Then $a = b \cdot f$. Since $f \in I$ and $b \in \Gamma(V) \subseteq \mathcal{O}_P(V)$, their product a lies in the ideal I. As a is also in $\Gamma(V)$, we have $a \in I \cap \Gamma(V) = J$. Since $a \in J$, we can write it as a $\Gamma(V)$-linear combination $a = \sum_{i=1}^{r} c_i g_i$ for some $c_i \in \Gamma(V)$. Dividing by b, we find an expression for f:

$$f = \frac{a}{b} = \sum_{i=1}^{r} \frac{c_i}{b} g_i.$$

Since $b(P) \neq 0$, each coefficient $\frac{c_i}{b}$ is an element of $\mathcal{O}_P(V)$. This shows that f is in the ideal generated by the g_i in $\mathcal{O}_P(V)$. Thus $I = (g_1, \ldots, g_r)_{\mathcal{O}_P(V)}$, proving that I is finitely generated. □

Finally, we observe that regular maps between varieties induce homomorphisms on their local rings in a natural way. Let $\varphi : V \to W$ be a regular map of affine varieties. This induces a pullback $\varphi^* : \Gamma(W) \to \Gamma(V)$. While this map does not generally extend to a map of function fields $k(W) \to k(V)$ (unless φ is dominant), it always induces a map on local rings.

Let $P \in V$, and set $Q = \varphi(P) \in W$. If a rational function $f = g/h$ is regular at Q, then $h(Q) \neq 0$. The pullback function $\varphi^*(h)$ therefore has the property that $(\varphi^*(h))(P) = h(\varphi(P)) = h(Q) \neq 0$. This means that the rational function $\frac{\varphi^*(g)}{\varphi^*(h)}$ is regular at P. This correspondence defines a ring homomorphism $\varphi_P^* : \mathcal{O}_Q(W) \to \mathcal{O}_P(V)$.

This induced map is a local homomorphism, meaning it maps the maximal ideal of the domain into the maximal ideal of the codomain. Indeed, if $f = g/h \in \mathfrak{m}_Q(W)$, then $g(Q) = 0$. The image $\varphi_P^*(f)$ evaluates

to $g(Q)/h(Q) = 0$ at P, so $\varphi_P^*(f) \in \mathfrak{m}_P(V)$. Thus, $\varphi_P^*(\mathfrak{m}_Q(W)) \subseteq \mathfrak{m}_P(V)$. This algebraic mapping of local rings is the consequence of the geometric map φ near the point P.

2.2.4 Affine Plane Curves

We have thus far associated geometry with radical ideals. An irreducible affine plane curve, for instance, corresponds to a principal ideal $(f) \subseteq k[x, y]$ where f is an irreducible polynomial. This geometric perspective, however, is insufficient for studying things like intersection theory, where we must account for multiplicities and reducible objects. To this end, we shift our perspective slightly, defining a curve not by its locus of points, but by its defining polynomial itself.

This change is motivated by the fact that different polynomials can define the same set of points. The ideals (f) and (g) define the same algebraic set if and only if $\sqrt{(f)} = \sqrt{(g)}$. For principal ideals in $k[x, y]$, this is equivalent to f and g having the same irreducible factors, possibly with different powers. For example, $V(x) = V(x^2)$ both describe the y-axis in $\mathbb{A}^2$. Yet, the curve defined by $x^2 = 0$ should be thought of as a "double line," a geometric object carrying more information than the simple line $x = 0$. To capture this, we must modify our definition. We note that the ideals (f) and (g) are identical if and only if f and g are scalar multiples of each other. This leads to the following formulation.

Definition 2.46. *An **affine plane curve** is an equivalence class of non-constant polynomials in $k[x, y]$ under the equivalence relation $f \sim g$ if and only if $f = \lambda g$ for some non-zero scalar $\lambda \in k$.*

Two polynomials f and g satisfying this relation are said to be **equivalent**. The **degree** of the curve is the total degree of its defining polynomial f. A curve of degree one is called a **line**.

Remark 2.47 (Curves vs. Varieties)**.** *We are now distinguishing between the curve defined by f and the curve defined by f^n for $n > 1$. While they correspond to the same variety (since $V(f) = V(f^n)$), they are now distinct objects using our new terminology. This distinction is caused algebraically in the quotient ring. The ring $k[x, y]/(f)$ is reduced (if f is square-free), while the ring $k[x, y]/(f^n)$ contains non-zero nilpotent elements. These nilpotents carry the "infinitesimal" information that corresponds geometrically to multiplicity.*

This framework accommodates reducible curves. Let the prime factorization of a polynomial f in $k[x, y]$ be $f = \prod_{i=1}^{k} f_i^{e_i}$, where the f_i are distinct irreducible polynomials.

- The curves defined by the individual polynomials f_i are called the **irreducible components** of the curve f.
- The integer $e_i \geq 1$ is the **multiplicity** of the component f_i.
- If $e_i = 1$, the component f_i is called a **simple** component.

For example:

Example 2.48. *The curve $f = (x - y)^3(x^2 + y^2 - 1)$ of degree 5 has two components: the line $x - y = 0$ with multiplicity 3, and the unit circle $x^2 + y^2 - 1 = 0$, which is a simple component.*

2.3 Tangent Lines and Homogeneous Polynomials

2.3.1 Tangent Lines via Calculus

Our study of the local geometry of a curve begins with the classical question: how does one define the tangent line to a plane curve at a point? An approach using differential calculus is to consider the gradient of the defining polynomial. Given a plane curve defined by the vanishing of a polynomial $f(x, y)$, the gradient of f provides the normal vector to the level set, from which the tangent line can be determined.

For example, let the curve be the unit circle, defined by $f(x, y) = y^2 + x^2 - 1 = 0$. Consider the point $P = (-\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2})$ on the curve. The partial derivatives are $f_x := \frac{\partial f}{\partial x} = 2x$ and $f_y := \frac{\partial f}{\partial y} = 2y$. Evaluating at P, we have $f_x(P) = -\sqrt{2}$ and $f_y(P) = \sqrt{2}$. The equation of the tangent line at a point (a, b) is given by the

linear approximation of the curve:

$$f_x(P)(x-a) + f_y(P)(y-b) = 0.$$

Substituting our values gives $-\sqrt{2}(x + \frac{\sqrt{2}}{2}) + \sqrt{2}(y - \frac{\sqrt{2}}{2}) = 0$, which simplifies to $y = x + \sqrt{2}$.

This method works precisely when the gradient vector is non-zero. This provides the motivation for the following classification of points on a curve.

Definition 2.49. *Let f be an affine plane curve and let P be a point on the curve. P is a **simple point** (or **smooth**, or **nonsingular** point) of f if the gradient is non-zero at P; that is, if $\frac{\partial f}{\partial x}(P) \neq 0$ or $\frac{\partial f}{\partial y}(P) \neq 0$. In this case, the **tangent line** to f at $P = (a, b)$ is the line defined by the equation:*

$$\frac{\partial f}{\partial x}(P)(x-a) + \frac{\partial f}{\partial y}(P)(y-b) = 0.$$

*A point that is not simple is called a **multiple** or **singular** point. A curve is **nonsingular** or **smooth** if all of its points are simple.*

Example 2.50. *Consider the point $(0, 0)$ for several curves.*

1. ***The Elliptic Curve*** $y^2 - x^3 + x = 0$*: Let $f = y^2 - x^3 + x$. Then $f_x = -3x^2 + 1$ and $f_y = 2y$. A singular point must satisfy $f_x = 0$ and $f_y = 0$, which implies $x = \pm 1/\sqrt{3}$ and $y = 0$. However, these points do not lie on the curve $V(f)$. Thus, the curve is nonsingular. At the origin $(0, 0)$, the lowest degree term of f is x. The line $x = 0$ is the tangent to the curve at the origin.*
2. ***The Cusp*** $y^2 - x^3 = 0$*: Let $g = y^2 - x^3$. We have $g_x = -3x^2$ and $g_y = 2y$. Both vanish only at $(0, 0)$, which is a point on the curve. Thus, $(0, 0)$ is a singular point. Here, the lowest degree term is y^2. The line $y = 0$ is the unique tangent at the origin.*
3. ***The Trefoil Knot*** $(x^2+y^2)^2+3x^2y-y^3 = 0$*: Let $h = (x^2+y^2)^2+3x^2y-y^3$. The partial derivatives are $h_x = 2(x^2+y^2)(2x)+6xy$ and $h_y = 2(x^2+y^2)(2y)+3x^2-3y^2$. One can verify that both partials vanish simultaneously only at $(0, 0)$. The lowest degree part of the polynomial is the cubic form $3x^2y - y^3$. This form factors as $y(3x^2 - y^2) = y(\sqrt{3}x - y)(\sqrt{3}x + y)$. As we will see, these three lines are the tangent lines at the origin.*

The examples suggest a relationship between the tangent geometry at the origin and the lowest degree terms of the defining polynomial. To formalize this, we need a purely algebraic framework that does not rely on calculus.

2.3.2 Homogenous Polynomials

An important algebraic tool is the decomposition of a polynomial into its homogeneous components.

Definition 2.51. *A polynomial $F \in k[x_1, \ldots, x_n]$ is **homogeneous** of degree d, or a **form** of degree d, if all of its monomials have total degree d.*

Any polynomial $f \in k[x_1, \ldots, x_n]$ of degree d can be uniquely written as a sum of forms, $f = f_0 + f_1 + \cdots + f_d$, where f_i is a form of degree i. One can convert between homogeneous and non-homogeneous polynomials.

Definition 2.52. *Let $F \in k[x_1, \ldots, x_n]$ be a form. The **dehomogenization** of F with respect to a variable, say x_n, is the polynomial $f = F(x_1, \ldots, x_{n-1}, 1) \in k[x_1, \ldots, x_{n-1}]$.*

*Conversely, let $f \in k[x_1, \ldots, x_n]$ be a polynomial of degree d, written as $f = \sum_{i=0}^{d} f_i$ where f_i are forms. The **homogenization** of f with respect to a new variable x_{n+1} is the form*

$$F(x_1, \ldots, x_{n+1}) = \sum_{i=0}^{d} x_{n+1}^{d-i} f_i(x_1, \ldots, x_n) = x_{n+1}^d f_0 + x_{n+1}^{d-1} f_1 + \cdots + f_d.$$

By construction, F is a homogeneous polynomial of degree d.

Example 2.53. *The operations of homogenization and dehomogenization are not, in general, inverses of each other. Let $F = x^2z+y^2z+xz^2+z^3$. Dehomogenizing with respect to z yields $f = x^2+y^2+x+1$, a polynomial of degree 2. If we now homogenize f with respect to z, we obtain the form $F' = z^2(x^2+y^2)+z(x)+(1) = x^2+y^2+xz+z^2$. Clearly $F' \neq F$. Information is lost because the original form $F = z \cdot F'$ was divisible by the dehomogenizing variable.*

Remark 2.54. *Homogenization respects multiplication but not addition. That is, for polynomials f, g, the homogenization of their product fg is the product of their homogenizations F_hG_h. However, the homogenization of the sum $f+g$ is not generally the sum of the homogenizations $F_h + G_h$.*

An important property of homogeneous polynomials in two variables is their complete factorizability over an algebraically closed field.

Proposition 2.55. *If $F \in k[x,y]$ is a homogeneous polynomial and k is algebraically closed, then F factors into a product of linear forms.*

Proof. Let $d = \deg(F)$. We may write $F = y^rG(x,y)$ for some $r \geq 0$, where y does not divide the form G. Dehomogenizing G with respect to y gives a polynomial $g(x) = G(x,1)$ in $k[x]$. Since k is algebraically closed, $g(x)$ factors completely: $g(x) = \alpha\prod_{i=1}^{d-r}(x-\lambda_i)$ for some $\alpha, \lambda_i \in k$. Homogenizing this expression gives back G:

$$G(x,y) = \alpha\prod_{i=1}^{d-r}(x-\lambda_i y).$$

Therefore, the original form F factors completely into linear forms: $F(x,y) = \alpha y^r\prod_{i=1}^{d-r}(x-\lambda_i y)$. □

2.3.3 Multiplicities

We now formalize the connection between the lowest degree terms of a polynomial and the tangent geometry at the origin.

Let f be a plane curve passing through the origin $P = (0,0)$. We can write f as a sum of its homogeneous parts, $f = f_m + f_{m+1} + \cdots + f_d$, where f_i is a form of degree i and $f_m \neq 0$ is the non-zero form of lowest degree.

Definition 2.56. *Let f be a curve passing through $P = (0,0)$.*

- *The form f_m is the **initial form** of f at the origin, denoted $in_P(f)$.*
- *The integer $m \geq 1$ is the **multiplicity** of f at $P = (0,0)$, denoted $m_P(f)$.*

Remark 2.57. *The condition that the origin $(0,0)$ is a point on the curve $V(f)$ is equivalent to the constant term of f being zero, which is equivalent to $m_{(0,0)}(f) \geq 1$.*

This algebraic definition of multiplicity is consistent with the calculus-based definition of simple points.

Proposition 2.58. *A point $P = (0,0)$ is a simple point of a curve f if and only if its multiplicity at P is one.*

Proof. Let $f = \sum f_i$ be the decomposition of f into forms. The partial derivative of a form f_i is either zero or a form of degree $i-1$. Thus, when we evaluate the partial derivatives of f at $P = (0,0)$, only the derivatives of the degree-1 form f_1 can contribute a non-zero constant. Let $f_1 = ax+by$. Then $\frac{\partial f}{\partial x}(P) = a$ and $\frac{\partial f}{\partial y}(P) = b$. The point P is simple if and only if not both partial derivatives are zero, which is equivalent to $(a,b) \neq (0,0)$. This, in turn, is equivalent to the linear form f_1 being non-zero. By definition, this means the multiplicity $m_P(f)$ is 1. □

In the case of a simple point, the initial form $f_1 = ax+by$ defines the tangent line. This concept generalizes to singular points. Since the initial form f_m is a homogeneous polynomial in x and y, it factors into m linear forms L_i, counted with multiplicity: $f_m = \prod L_i^{r_i}$.

Definition 2.59. *Let f be a curve with multiplicity $m = m_P(f)$ at the origin $P = (0,0)$, and let the initial form be $f_m = \prod_{i=1}^{k} L_i^{r_i}$.*

- *The lines defined by $L_i = 0$ are the **tangent lines** to f at P.*
- *The integer r_i is the **multiplicity** of the tangent line L_i.*
- *The initial form f_m is also called the **tangent cone** to f at the origin.*
- *If f has m distinct tangent lines at P (i.e., all $r_i = 1$), then P is an **ordinary** singular point. An ordinary multiple point of multiplicity 2 is called a **node**.*

Example 2.60. *Revisiting our singular examples at $P = (0,0)$:*

1. *For $h = (x^2+y^2)^2 + 3x^2y - y^3$, the initial form is $in_P(h) = 3x^2y - y^3 = y(\sqrt{3}x - y)(\sqrt{3}x + y)$. The multiplicity is 3, and there are three distinct tangent lines. The origin is an ordinary triple point.*
2. *For the curve $f = y^2 - x^2 - x^3 = 0$, the initial form is $in_P(f) = y^2 - x^2 = (y-x)(y+x)$. The multiplicity is 2, and the tangents are two distinct lines. The origin is a node.*
3. *For the cusp $g = y^2 - x^3 = 0$, the initial form is $in_P(g) = y^2$. The multiplicity is 2, but there is only one tangent line, $y = 0$, with multiplicity 2. The origin is a singular point but is not ordinary.*

One can verify that these lines are tangent in the standard sense by parameterizing the branches of the curve near the origin and computing the limiting secant lines.

Remark 2.61. *The initial form respects multiplication: $in_P(fg) = in_P(f)in_P(g)$. It follows that multiplicity is additive over products. If a curve f factors into components $f = \prod h_i^{e_i}$, then the multiplicity of f at P is the sum of the multiplicities of its components: $m_P(f) = \sum e_i m_P(h_i)$.*

To analyze the multiplicity and tangents at an arbitrary point $P = (a,b)$, we perform an affine change of coordinates that moves P to the origin. Let $T : \mathbb{A}^2 \to \mathbb{A}^2$ be the translation $T(x,y) = (x+a, y+b)$. The pullback map on polynomials is $T^* : k[x,y] \to k[x,y]$ given by $T^*(f)(x,y) = f(x+a, y+b)$. The local geometry of the curve f at $P = (a,b)$ is identical to the geometry of the translated curve $T^*(f)$ at the origin $(0,0)$.

We define $m_P(f) := m_{(0,0)}(T^*(f))$. If $L = \alpha x + \beta y$ is a tangent line to $T^*(f)$ at the origin, then the corresponding tangent line to f at P is given by applying the inverse translation to the coordinates, resulting in the line $\alpha(x-a) + \beta(y-b) = 0$.

Example 2.62. *Let $f = x^3 + y^2 - 3x^2 - 4y + 3x + 3$. The partial derivatives are $f_x = 3x^2 - 6x + 3 = 3(x-1)^2$ and $f_y = 2y - 4$. Both vanish at $P = (1,2)$. Since $f(1,2) = 1 + 4 - 3 - 8 + 3 + 3 = 0$, the point P is a singular point on the curve. To analyze it, we translate P to the origin. Let $g(x,y) = f(x+1, y+2)$:*

$$g(x,y) = (x+1)^3 + (y+2)^2 - 3(x+1)^2 - 4(y+2) + 3(x+1) + 3 = y^2 + x^3.$$

The translated curve is the cusp $y^2 + x^3 = 0$, which is singular at the origin. We have $m_{(1,2)}(f) = m_{(0,0)}(g) = 2$. The initial form of g is y^2, corresponding to the tangent line $y = 0$ with multiplicity 2. Translating this back, the tangent line to f at $(1,2)$ is $y - 2 = 0$ with multiplicity 2.

2.3.4 Points On Curves Away From The Origin

So far, our algebraic definitions of multiplicity and the tangent cone were formulated specifically for a curve at the origin, $P = (0,0)$. To analyze a curve at an arbitrary point $P = (a,b)$, we use the principle that local geometric properties are invariant under affine transformations. The simplest such transformation is a translation of coordinates that moves the point of interest to the origin.

Let $P = (a,b)$ be a point in $\mathbb{A}^2$. Consider the translation map $T : \mathbb{A}^2 \to \mathbb{A}^2$ defined by

$$T(x', y') = (x' + a, y' + b) = (x, y).$$

This map sends the origin $(0,0)$ in the (x',y') coordinate system to the point $P=(a,b)$ in the (x,y) system. To study a curve $f(x,y)=0$ at P, we can study the transformed curve at the origin. The equation of the transformed curve is given by the pullback $T^*(f)$:

$$g(x',y') := (T^*f)(x',y') = f(x'+a, y'+b).$$

The local behavior of f at $P=(a,b)$ is identical to the local behavior of g at $(0,0)$. This allows us to extend our origin-based definitions to any point on the plane.

Definition 2.63. *Let f be a plane curve and let $P=(a,b)$ be a point. Let $g(x,y)=f(x+a,y+b)$ be the translated polynomial.*

- *The **multiplicity** of f at P is defined as the multiplicity of g at the origin: $m_P(f) := m_{(0,0)}(g)$.*
- *If $L=\alpha x+\beta y$ is a tangent line to g at $(0,0)$ with multiplicity r, then the line defined by $\alpha(x-a)+\beta(y-b)=0$ is a **tangent line** to f at P with multiplicity r.*

In other words, we can perform an affine change of coordinates so that the point we are interested in is at the origin, perform our analysis there, and then translate the results back.

Example 2.64. *Consider the curve defined by $f(x,y)=x^3+y^2-3x^2-4y+3x+3=0$. First, we find its singular points. The partial derivatives are:*

$$\frac{\partial f}{\partial x} = 3x^2-6x+3 = 3(x-1)^2 \quad \textit{and} \quad \frac{\partial f}{\partial y} = 2y-4 = 2(y-2).$$

These both vanish simultaneously only at the point $P=(1,2)$. We check if this point lies on the curve:

$$f(1,2) = (1)^3+(2)^2-3(1)^2-4(2)+3(1)+3 = 1+4-3-8+3+3 = 0.$$

Since $P=(1,2)$ is on the curve, it is a singular point. To analyze its structure, we translate P to the origin. Let $g(x',y')=f(x'+1,y'+2)$:

$$\begin{aligned} g(x',y') &= (x'+1)^3+(y'+2)^2-3(x'+1)^2-4(y'+2)+3(x'+1)+3 \\ &= (x'^3+3x'^2+3x'+1)+(y'^2+4y'+4)-3(x'^2+2x'+1)-(4y'+8)+(3x'+3)+3 \\ &= y'^2+x'^3. \end{aligned}$$

The translated curve is the cusp $g(x',y')=y'^2+x'^3$, which we have previously analyzed. The multiplicity of g at the origin is $m_{(0,0)}(g)=2$, since the initial form is y'^2. The tangent cone is given by $y'^2=0$, which corresponds to the single tangent line $y'=0$ with multiplicity 2.

Translating this information back to the original curve f at the point $P=(1,2)$:

- *The multiplicity is $m_{(1,2)}(f)=m_{(0,0)}(g)=2$.*
- *The tangent line is given by replacing y' with $(y-2)$, so the tangent line is $y-2=0$ with multiplicity 2.*

2.3.5 Tangent Spaces and Local Rings

We now introduce the modern algebraic definition of the tangent space. This formulation is immensely powerful as it is intrinsic to the variety and does not depend on a particular embedding in affine space or the language of calculus. The key insight is that the "linear" part of the geometry at a point P is encoded in the structure of the local ring $\mathcal{O}_P(V)$, specifically in the quotient of its maximal ideal $\mathfrak{m}_P$ by the ideal of functions that vanish to second order, $\mathfrak{m}_P^2$.

Let $f \in k[x,y]$ define a plane curve, let P be a point on the curve, and let $(\mathcal{O}_P(f), \mathfrak{m}_P)$ be the local ring of the curve at P with its unique maximal ideal.

Definition 2.65. *The **cotangent space** of the curve f at the point P is the vector space $\mathfrak{m}_P/\mathfrak{m}_P^2$. This is a vector space over the residue field $\mathcal{O}_P(f)/\mathfrak{m}_P \cong k$.*

The dimension of this vector space distinguishes between simple and singular points. A simple point will have a one-dimensional cotangent space, while a singular point will have a cotangent space of dimension greater than one.

Example 2.66. *Let $f = x - y^3$ and $P = (0,0)$. This is a smooth curve. The coordinate ring is $\Gamma(V(f)) = k[x,y]/(x-y^3) \cong k[y]$. The maximal ideal corresponding to the origin is $\mathfrak{m}_P = (\bar{x}, \bar{y})$ in $\Gamma(V(f))$. Using the relation $\bar{x} = \bar{y}^3$, this simplifies to $\mathfrak{m}_P = (\bar{y}^3, \bar{y}) = (\bar{y})$. The square of the maximal ideal is $\mathfrak{m}_P^2 = (\bar{y}^2)$. The cotangent space is $\mathfrak{m}_P/\mathfrak{m}_P^2 = (\bar{y})/(\bar{y}^2)$. As a vector space over k, this quotient is spanned by the single vector corresponding to the class of $\bar{y}$. Thus, $\dim_k(\mathfrak{m}_P/\mathfrak{m}_P^2) = 1$.*

Example 2.67. *Let $f = x^2 - y^3$ (a cusp) and $P = (0,0)$. This is a singular point. The maximal ideal corresponding to the origin in $\Gamma(V(f))$ is $\mathfrak{m}_P = (\bar{x}, \bar{y})$. The square of this ideal is $\mathfrak{m}_P^2 = (\bar{x}^2, \bar{y}^2, \bar{x}\bar{y})$. In the quotient space $\mathfrak{m}_P/\mathfrak{m}_P^2$, the generators are the classes of $\bar{x}$ and $\bar{y}$. The relation $x^2 - y^3 = 0$ implies $\bar{x}^2 = \bar{y}^3$. Since $\bar{y}^3 = \bar{y} \cdot \bar{y}^2 \in \mathfrak{m}_P^3 \subset \mathfrak{m}_P^2$, the class of $\bar{x}^2$ is zero in $\mathfrak{m}_P/\mathfrak{m}_P^2$. However, there are no non-trivial linear relations between $\bar{x}$ and $\bar{y}$ in this quotient. They form a basis for the vector space. Therefore, $\dim_k(\mathfrak{m}_P/\mathfrak{m}_P^2) = 2$. The dimension of the cotangent space detected the singularity.*

The geometric tangent space is recovered by taking the vector space dual of the cotangent space.

Definition 2.68. *The **Zariski tangent space** of f at P, denoted $T_P(f)$, is the dual of the cotangent space as a k-vector space:*

$$T_P(f) = (\mathfrak{m}_P/\mathfrak{m}_P^2)^* = \mathrm{Hom}_k(\mathfrak{m}_P/\mathfrak{m}_P^2, k).$$

How does this abstract definition give us a geometric tangent space, i.e., a set of vectors? An element of the tangent space is a linear map $\lambda : \mathfrak{m}_P/\mathfrak{m}_P^2 \to k$. Such a map is determined by the values it assigns to the basis vectors of the cotangent space. These values can be interpreted as coordinates.

Example 2.69. *Let $f = y - 3x + x^3$ and $P = (0,0)$. In the local ring $\mathcal{O}_P(f)$, the maximal ideal is $\mathfrak{m}_P = (\bar{x}, \bar{y})$. The defining equation gives the relation $\bar{y} - 3\bar{x} + \bar{x}^3 = 0$. In the cotangent space $\mathfrak{m}_P/\mathfrak{m}_P^2$, the term $\bar{x}^3$ is zero, since it belongs to $\mathfrak{m}_P^3 \subset \mathfrak{m}_P^2$. Thus, the relation becomes $\bar{y} = 3\bar{x}$. This means the cotangent space is one-dimensional, spanned by the class of $\bar{x}$.*

Now consider the dual space, the Zariski tangent space. A linear map $\lambda : \mathfrak{m}_P/\mathfrak{m}_P^2 \to k$ is completely determined by the value it assigns to the basis vector $\bar{x}$, say $\lambda(\bar{x}) = c$ for some $c \in k$. Because the map must be linear and respect the relation $\bar{y} = 3\bar{x}$, we must have $\lambda(\bar{y}) = \lambda(3\bar{x}) = 3\lambda(\bar{x}) = 3c$. We can identify the tangent space with the set of all possible coordinate vectors $(\lambda(\bar{x}), \lambda(\bar{y}))$:

$$T_P(f) = \{(c, 3c) \in \mathbb{A}^2 \mid c \in k\}.$$

This is precisely the line $y = 3x$, which is the tangent line we would compute using calculus. This method therefore recovers the geometric tangent line as an embedded subspace of $\mathbb{A}^2$.

2.4 Discrete Valuation Rings and Order Functions

2.4.1 Basic Definitions

Before we can go into more depth about the geometry of a curve near a point, we need to introduce a key algebraic structure. The local ring $\mathcal{O}_P(C)$ of a curve C at a point P is a Discrete Valuation Ring if and only if P is a smooth point on C. This makes the study of these rings essential for understanding local geometric properties algebraically.

Definition 2.70. *Let R be an integral domain that is not a field. Then R is a **Discrete Valuation Ring (DVR)** if it satisfies either of the two following equivalent properties:*

1. *R is a Noetherian local ring and its maximal ideal is principal.*
2. *There exists an irreducible element $t \in R$ (called a uniformizing parameter) such that every non-zero element $z \in R$ can be written uniquely in the form $z = ut^n$ for some unit $u \in R$ and a unique integer $n \geq 0$.*

Proof. **(1) $\implies$ (2):** Let R be a Noetherian local ring whose maximal ideal $\mathfrak{m}$ is principal, say $\mathfrak{m} = (t)$ for some $t \in R$. First, we prove uniqueness. Suppose $ut^n = vt^m$ where u, v are units and, without loss of generality, $n \geq m$. Since R is an integral domain, we can cancel to get $ut^{n-m} = v$. If $n > m$, then t divides the unit v, which would imply t is also a unit. But t generates the maximal ideal $\mathfrak{m} \neq R$, so t cannot be a unit. Therefore, we must have $n = m$, which in turn implies $u = v$.

Next, we prove existence. Let $z \in R$ be a non-zero element. If z is a unit, we are done by taking $n = 0$. If z is not a unit, then $z \in \mathfrak{m} = (t)$, so $z = z_1 t$ for some $z_1 \in R$. If z_1 is a unit, we have found our representation $z = z_1 t^1$. If not, $z_1 \in \mathfrak{m}$, so $z_1 = z_2 t$, which gives $z = z_2 t^2$. We can continue this process, generating a sequence $z, z_1, z_2, \ldots$ such that $z_n = z_{n+1} t$. This gives rise to a chain of principal ideals $(z) \subseteq (z_1) \subseteq (z_2) \subseteq \ldots$. Since R is Noetherian, this chain must stabilize. So, for some n, we have $(z_n) = (z_{n+1})$. This means $z_{n+1} = v z_n$ for some unit $v \in R$. Substituting into $z_n = z_{n+1} t$ gives $z_n = (v z_n) t$. Since $z_n \neq 0$, we can cancel it to get $1 = vt$. This implies t is a unit, which contradicts that $\mathfrak{m} = (t)$ is a proper ideal. The only way to avoid this contradiction is if the process terminates, which means some z_n must be a unit. Thus, every non-unit z can be written as $z = ut^n$ for some unit u and $n \geq 1$.

(2) $\implies$ (1): Assume every non-zero $z \in R$ has the form ut^n. An element is a non-unit if and only if $n \geq 1$, which is equivalent to saying the element is a multiple of t. The set of non-units is therefore the principal ideal (t). Since the set of non-units forms an ideal, R is a local ring with maximal ideal $\mathfrak{m} = (t)$. The maximal ideal is principal by construction. We only need to show R is Noetherian. Let $I \subseteq R$ be a non-zero ideal. Let n be the minimum non-negative integer such that there exists an element of the form $ut^n \in I$. Then every other element $vt^m \in I$ must have $m \geq n$. If $m < n$, it would contradict the minimality of n. Therefore, any element $vt^m \in I$ can be written as $(vt^{m-n})t^n$, showing that $vt^m \in (t^n)$. This implies $I \subseteq (t^n)$. Since we know some $ut^n \in I$, we also have $(t^n) = (u^{-1}ut^n) \subseteq I$. Thus, $I = (t^n)$. Since every ideal is principal, R is a Principal Ideal Domain, and therefore is Noetherian. □

Definition 2.71. *The element t in property (2) of the definition is called a **uniformizing parameter** for the DVR. It is uniquely determined up to multiplication by a unit.*

Remark 2.72. *The proof of (2) $\implies$ (1) shows that if R is a DVR with uniformizing parameter t, then its ideals are precisely the principal ideals generated by powers of t. This gives a complete picture of the ideal structure as a simple descending chain:*

$$R = (t^0) \supset (t^1) \supset (t^2) \supset (t^3) \supset \cdots \supset (0).$$

Example 2.73. *Let $a \in \mathbb{A}^1$. The local ring of $\mathbb{A}^1$ at a is $\mathcal{O}_a(\mathbb{A}^1) = \{\frac{f}{g} \mid f, g \in k[x], g(a) \neq 0\}$. An element of this ring is a non-unit if and only if, when written in lowest terms, its numerator vanishes at a. This is equivalent to the numerator being divisible by $(x - a)$. The maximal ideal is therefore the principal ideal generated by the function $(x - a)$. Since $\mathcal{O}_a(\mathbb{A}^1)$ is a local ring with a principal maximal ideal (and it can be shown to be Noetherian), it is a **DVR** with uniformizing parameter $(x - a)$.*

Example 2.74. *In contrast, consider the local ring of the affine plane $\mathbb{A}^2$ at the origin, $\mathcal{O}_{(0,0)}(\mathbb{A}^2)$. Its maximal ideal consists of rational functions f/g where $f(0, 0) = 0$. This ideal is generated by the functions x and y, so $\mathfrak{m}_{(0,0)}(\mathbb{A}^2) = (x, y)$. This ideal is not principal. Therefore, $\mathcal{O}_{(0,0)}(\mathbb{A}^2)$ is a local ring but it is **not a DVR**.*

The unique factorization property of a DVR allows us to define a valuation on its field of fractions. Let R be a DVR with uniformizing parameter t, and let K be its field of fractions. Any non-zero element $z \in K$ can be written as a fraction f/g, where $f = ut^n$ and $g = vt^m$. Thus, $z = (u/v)t^{n-m}$. Since u, v are units in R, so is u/v. It is a straightforward exercise to show that every non-zero element $z \in K$ has a unique expression $z = ut^k$ where u is a unit in R and $k \in \mathbb{Z}$.

Definition 2.75. *For a non-zero element $z = ut^k \in K$, the integer k is called the **order** of z, denoted $ord(z)$. By convention, we define $ord(0) = \infty$.*

The order function provides a concise description of the ring and its maximal ideal.

$$R = \{z \in K \mid \text{ord}(z) \geq 0\}$$

$$\mathfrak{m} = \{z \in K \mid \text{ord}(z) \geq 1\} = \{z \in R \mid \text{ord}(z) > 0\}$$

The order function has the following key properties, characteristic of a valuation:

- $\text{ord}(ab) = \text{ord}(a) + \text{ord}(b)$
- $\text{ord}(a+b) \geq \min(\text{ord}(a), \text{ord}(b))$

It can also be shown that the definition of order is independent of the choice of uniformizing parameter.

Now let's discuss quotients of DVRs.

Example 2.76. *Let $R = \mathcal{O}_0(\mathbb{A}^1)$. Maximal ideal $= m = (x)$. Let $M = (x^n)/(x^{n+1}) \subseteq R/(x^{n+1})$. This is a k-vector space since $k \subseteq R$. Then every $z \in M$ can be written as $\frac{x^n}{f(x)}, f(0) \neq 0$. Note that $f(x)x^n = f(0)x^n$, since higher powers of x vanish $\implies z = \frac{x^n}{f(x)} = \left(\frac{1}{f(0)}\right)x^n$ so M is 1-dimensional!*

More generally: let R be a DVR containing a field k such that the composition $k \to R \to R/m$ with $k \xrightarrow{\alpha} R/m$ is an isomorphism.

Let $t \in R$ be a uniformizing parameter. Consider $z \in m^n$. Then $z = ut^n, u$ a unit. Then the image of u in R/m is nonzero, so $\exists \lambda \in k$ such that $\alpha(\lambda) = \alpha(u)$. Thus $u = \lambda + at \in R$, some $\alpha \in R \implies z = \lambda t^n + at^{n+1}$.

But then if we look at $\overline{z} \in m^n/m^{n+1}$, we get $\overline{z} = \lambda \overline{t}^r$. Thus, $\dim\left(m^n/m^{n+1}\right) = 1$. Since $\dim(R/m) = 1$, by induction, we get the following short exact sequence of k-vector spaces:

$$0 \to m^n/m^{n+1} \to R/m^{n+1} \to R/m^n \to 0$$

with dimensions $1, n+1, n$, respectively.

Note: $\text{ord}(z) = n \iff (z) = m^n$, so $\text{ord}(z) = \dim_k(R/(z))$.

2.4.2 Multiplicities, Revisited

We are now prepared to connect the algebraic structure of the local ring of a curve at a point with the geometric notion of smoothness. Let f be an irreducible plane curve. For brevity, we will denote the coordinate ring $\Gamma(V(f))$ by $\Gamma(f)$, the local ring $\mathcal{O}_P(V(f))$ by $\mathcal{O}_P(f)$, and the function field $k(V(f))$ by $k(f)$.

The central question is: under what geometric conditions is the local ring $\mathcal{O}_P(f)$ a Discrete Valuation Ring (DVR)?

Example 2.77. *Let $f = y - x^2$ be the standard parabola and let $P = (0,0)$ be the origin. The coordinate ring is $\Gamma(f) = k[x,y]/(y-x^2) \cong k[x]$. The maximal ideal of $\mathcal{O}_P(f)$ is generated by the images of x and y in this ring.*

$$\mathfrak{m}_P = (\bar{x}, \bar{y}) = (\bar{x}, \bar{x}^2) = (\bar{x}).$$

*Since the maximal ideal is principal, and $\mathcal{O}_P(f)$ is a Noetherian local ring, it is a **DVR**. Note that P is a smooth point of the parabola.*

Example 2.78. *Let $f = y^2 - x^3$ be the cusp and let $P = (0,0)$. The maximal ideal of the local ring $\mathcal{O}_P(f)$ is $\mathfrak{m}_P = (\bar{x}, \bar{y})$. In the ring $\Gamma(f) = k[x,y]/(y^2 - x^3)$, the ideal $(\bar{x}, \bar{y})$ is not principal. (This is a non-trivial fact, related to $\Gamma(f)$ not being integrally closed). Therefore, $\mathcal{O}_P(f)$ is **not a DVR**. Note that P is a singular point of the cusp.*

These examples suggest that the DVR property is characteristic of smooth points. To prove this, we state a result connecting the geometric multiplicity, $m_P(f)$, with the algebraic structure of the local ring.

Theorem 2.79. *Let P be a point on an irreducible curve f, and let $\mathfrak{m}_P$ be the maximal ideal of the local ring $\mathcal{O}_P(f)$. For all sufficiently large integers n, the dimension of the k-vector space $\mathfrak{m}_P^n/\mathfrak{m}_P^{n+1}$ is constant and equal to the multiplicity of the curve at P.*

$$m_P(f) = \dim_k(\mathfrak{m}_P^n/\mathfrak{m}_P^{n+1}) \quad \text{for } n \gg 0.$$

Proof Sketch. This result follows from the theory of the Hilbert-Samuel function of the local ring $(\mathcal{O}_P, \mathfrak{m}_P)$. One considers the short exact sequence of finite-dimensional vector spaces:

$$0 \to \mathfrak{m}_P^n/\mathfrak{m}_P^{n+1} \to \mathcal{O}_P/\mathfrak{m}_P^{n+1} \to \mathcal{O}_P/\mathfrak{m}_P^n \to 0.$$

This implies $\dim_k(\mathfrak{m}_P^n/\mathfrak{m}_P^{n+1}) = \dim_k(\mathcal{O}_P/\mathfrak{m}_P^{n+1}) - \dim_k(\mathcal{O}_P/\mathfrak{m}_P^n)$. A theorem of dimension theory (cf. Fulton, "Algebraic Curves," §3.2, Theorem 2) states that for n greater than or equal to the multiplicity $m_P(f)$, the dimension $\dim_k(\mathcal{O}_P/\mathfrak{m}_P^n)$ is a linear function of n, specifically $n \cdot m_P(f) + s$ for some constant s. For $n \gg 0$, the difference is then

$$((n+1)m_P(f) + s) - (nm_P(f) + s) = m_P(f).$$

□

If $\mathcal{O}_P(f)$ is a DVR, its maximal ideal $\mathfrak{m}_P$ is principal, say $\mathfrak{m}_P = (t)$. Then $\mathfrak{m}_P^n = (t^n)$ and $\mathfrak{m}_P^{n+1} = (t^{n+1})$. The quotient $\mathfrak{m}_P^n/\mathfrak{m}_P^{n+1}$ is a one-dimensional vector space over $k = \mathcal{O}_P/\mathfrak{m}_P$ for all $n \geq 0$. By the theorem above, this implies $m_P(f) = 1$. Since a point has multiplicity 1 if and only if it is a simple point, we have one direction of the main theorem. The converse also holds.

Theorem 2.80. *Let f be an irreducible plane curve and $P \in V(f)$. The point P is a simple point of f if and only if the local ring $\mathcal{O}_P(f)$ is a DVR.*

Proof. ($\Leftarrow$) As argued above, if $\mathcal{O}_P(f)$ is a DVR, then $\dim_k(\mathfrak{m}_P^n/\mathfrak{m}_P^{n+1}) = 1$ for all n. By the previous theorem, this implies $m_P(f) = 1$. A point of multiplicity one is a simple point.

($\Rightarrow$) Assume P is a simple point. By an affine change of coordinates, we can assume $P = (0,0)$ and that the tangent line to f at the origin is the line $y = 0$. This means the initial form of f is cy for some $c \in k^*$. The polynomial f can therefore be written as

$$f = cy + (\text{terms of degree } \geq 2).$$

Because the tangent line is not the line $x = 0$, we can further write f in the form $f = yg(x,y) - x^2h(x)$ for some polynomials g and h, where $g(0,0) \neq 0$. In the coordinate ring $\Gamma(f)$, this gives the relation $\bar{y}\bar{g} = \bar{x}^2\bar{h}$. Since $g(0,0) \neq 0$, the function $\bar{g}$ is a unit in the local ring $\mathcal{O}_P(f)$. We can therefore write

$$\bar{y} = \left(\frac{\bar{h}}{\bar{g}}\right)\bar{x}^2.$$

This shows that $\bar{y}$ is in the ideal generated by $\bar{x}$ inside the local ring $\mathcal{O}_P(f)$. The maximal ideal $\mathfrak{m}_P = (\bar{x}, \bar{y})$ thus simplifies to $\mathfrak{m}_P = (\bar{x}, (\frac{\bar{h}}{\bar{g}})\bar{x}^2) = (\bar{x})$. Since the maximal ideal is principal, $\mathcal{O}_P(f)$ is a DVR. □

A consequence of this proof is that if P is a simple point on a curve f, then the image of any line L passing through P but not tangent to f at P serves as a uniformizing parameter for the DVR $\mathcal{O}_P(f)$.

Since the local ring $\mathcal{O}_P(f)$ at a simple point P is a DVR, we can use the order function ord_P^f defined on its field of fractions, which is the function field $k(f)$. This function measures the order of vanishing (or the order of a pole) of any rational function on the curve at the point P. We can apply this to measure the intersection of the curve with a line.

Let P be a simple point on an irreducible curve f. Let L be the defining polynomial of a line in $\mathbb{A}^2$. The function $\bar{L} \in \Gamma(f)$ is an element of the local ring $\mathcal{O}_P(f)$. We can analyze its order. If L is a line through P that is not tangent to f at P, then as noted above, $\bar{L}$ is a uniformizing parameter for $\mathcal{O}_P(f)$. Thus, $\text{ord}_P^f(L) = 1$. If L is the tangent line to f at P, we may assume after a change of coordinates that $P = (0,0)$ and $L = y$. From the proof of the previous theorem, we have the relation $\bar{y} = (\bar{h}/\bar{g})\bar{x}^2$ in $\mathcal{O}_P(f)$. Here, $\bar{x}$ is a uniformizing parameter. Since $g(P) \neq 0$, the order of $\bar{g}$ is 0. Thus, $\text{ord}_P^f(y) = \text{ord}_P^f(x^2) + \text{ord}_P^f(h) - \text{ord}_P^f(g) = 2 + \text{ord}_P^f(h) \geq 2$.

This leads to a complete geometric characterization of the order of a line at a simple point.

Theorem 2.81. *Let P be a simple point on an irreducible curve f. Let L be a line in the plane, viewed as a function in $\mathcal{O}_P(f)$.*

1. *$ord_P^f(L) = 0$ if and only if L does not pass through P.*
2. *$ord_P^f(L) = 1$ if and only if L passes through P and is not tangent to f at P.*
3. *$ord_P^f(L) \geq 2$ if and only if L is the tangent line to f at P.*

2.4.3 Intersection Numbers

Let f and g be two plane curves and let $P \in \mathbb{A}^2$ be a point. We wish to define an **intersection number**, denoted $I_P(f, g)$, that quantifies "how many times" f and g intersect at P. This number should capture the geometric intuition of tangency and multiplicity. We will take an axiomatic approach: first, we will list seven properties that this intersection number must satisfy. Then, we will show that these properties uniquely determine such a number and provide a concrete algebraic definition for it.

Proposition 2.82 (Axioms for the Intersection Number)**.** *There exists a unique intersection number $I_P(f, g)$ defined for any two plane curves f, g and any point $P \in \mathbb{A}^2$, satisfying the following properties:*

1. *$I_P(f, g)$ is a non-negative integer if f and g share no common component passing through P, and $I_P(f, g) = \infty$ otherwise.*
2. *$I_P(f, g) = 0$ if and only if P is not a common point of the two curves, i.e., $P \notin V(f) \cap V(g)$. This implies that $I_P(f, g)$ depends only on the components of f and g that pass through P.*
3. *The intersection number is invariant under affine changes of coordinates. If T is an affine change of coordinates on $\mathbb{A}^2$ and $T(Q) = P$, then $I_P(f, g) = I_Q(T^*f, T^*g)$.*
4. *The intersection number is symmetric: $I_P(f, g) = I_P(g, f)$.*
5. *$I_P(f, g) \geq m_P(f)m_P(g)$, where m_P denotes the multiplicity at P. Equality holds if and only if f and g have no tangent lines in common at P.*
6. *The intersection number is additive over products. If $f = \prod f_i^{r_i}$ and $g = \prod g_j^{s_j}$ are factorizations into irreducible components, then $I_P(f, g) = \sum_{i,j} r_i s_j I_P(f_i, g_j)$.*
7. *$I_P(f, g) = I_P(f, g + af)$ for any polynomial $a \in k[x, y]$. This means the intersection number depends only on the ideal (f, g) in the local ring at P.*

Definition 2.83. *Two curves f and g **intersect transversally** at P if P is a simple point on both f and g, and their tangent lines at P are distinct. In this case, Axiom 5 implies $I_P(f, g) = m_P(f)m_P(g) = 1 \cdot 1 = 1$.*

Lemma 2.84. *Any function $I_P(f, g)$ satisfying properties (1) through (7) is uniquely determined.*

Proof. We provide an algorithm that calculates $I_P(f, g)$ based only on these properties. By Axiom 3, we may assume $P = (0, 0)$. By Axiom 1, we assume $I_P(f, g)$ is finite. The algorithm proceeds by induction on the value of the intersection number. Axiom 2 provides the base case: $I_P(f, g) = 0$. Assume we can calculate $I_P(a, b)$ for any pair with intersection number less than n, and we wish to calculate $I_P(f, g) = n > 0$.

Let $f(x, 0)$ and $g(x, 0)$ be the polynomials obtained by restricting to the x-axis, with degrees r and s respectively. By Axiom 4, we can assume $r \leq s$.

Case 1: $r = 0$**.** This means $f(x, 0) = 0$, so y must be a factor of f. Let $f = yh$. By Axiom 6, $I_P(f, g) = I_P(y, g) + I_P(h, g)$. Let's compute the first term. Let $g(x, 0) = x^m(c_0 + c_1x + \dots)$ with $c_0 \neq 0$. Then $g = g(x, y)$ can be written as $g = g(x, 0) + yG(x, y)$ for some polynomial G. By Axiom 7, $I_P(y, g) = I_P(y, g(x, 0))$. By Axiom 6, $I_P(y, g(x, 0)) = I_P(y, x^m) + I_P(y, c_0 + \dots)$. The second term is 0 by Axiom 2 since $c_0 \neq 0$. The first term is $m \cdot I_P(y, x)$. By Axiom 5, $I_P(y, x) = 1$ since they are distinct lines. Thus, $I_P(y, g) = m = \deg_x(g(x, 0))$. The term $I_P(h, g)$ has a smaller intersection number and can be computed by the induction hypothesis.

Case 2: $r > 0$**.** Let $f(x,0)$ and $g(x,0)$ be made monic by scaling (which does not change the intersection number). Let $h = g - x^{s-r}f$. By Axiom 7, $I_P(f,g) = I_P(f,h)$. The degree of $h(x,0)$ is $\deg(g(x,0) - x^{s-r}f(x,0)) < s$. We can repeat this process, which is analogous to the Euclidean algorithm, reducing the degree of one of the polynomials' restrictions to the x-axis at each step. This process must terminate, eventually leading to Case 1.

Since this procedure gives a determined value, the intersection number is unique. □

Theorem 2.85. *There is a unique intersection number satisfying properties (1) through (7), given by the formula:*

$$I_P(f,g) = \dim_k \left(\mathcal{O}_P(\mathbb{A}^2)/(f,g)\right)$$

where $\mathcal{O}_P(\mathbb{A}^2)$ is the local ring of the plane at P, and (f,g) is the ideal generated by f and g in that ring.

Proof Sketch. Uniqueness has been established. We need only verify that this formula satisfies the axioms.

- **Axiom 2a:** $I_P(f,g) = 0 \iff \dim_k(\mathcal{O}_P/(f,g)) = 0 \iff \mathcal{O}_P/(f,g) = 0 \iff (f,g) = \mathcal{O}_P$. This is equivalent to the ideal (f,g) containing a unit. An element $h \in \mathcal{O}_P$ is a unit if and only if $h(P) \neq 0$. Thus, $I_P(f,g) = 0$ iff there exists some $h \in (f,g)$ such that $h(P) \neq 0$, which is equivalent to $P \notin V(f) \cap V(g)$.
- **Axiom 2b:** If $f = f_1 f_2$ and $f_2(P) \neq 0$, then f_2 is a unit in $\mathcal{O}_P(\mathbb{A}^2)$. Thus the ideal $(f,g) = (f_1 f_2, g)$ is the same as (f_1, g) in $\mathcal{O}_P(\mathbb{A}^2)$, so their dimensions are equal.
- **Axiom 3:** An affine change of coordinates T with $T(Q) = P$ induces a k-algebra isomorphism $\mathcal{O}_P(\mathbb{A}^2) \cong \mathcal{O}_Q(\mathbb{A}^2)$ which maps the ideal (f,g) to (T^*f, T^*g). Isomorphic structures yield the same dimension.
- **Axioms 4 and 7:** These are immediate from the definition, as $(f,g) = (g,f)$ and $(f,g) = (f, g+af)$ as ideals.
- **Axioms 1, 5, 6:** These proofs are more involved and can be found in standard texts, e.g., Fulton's "Algebraic Curves."

□

Example 2.86. *Let $P = (0,0)$, $f = (x^2+y^2)^3 - 4x^2y^2$, and $g = (x^2+y^2)^2 + 3x^2y - y^3$. Let's compute $I_P(f,g)$. By Axiom 7, we can replace f with $f - (x^2+y^2)g$. $f - (x^2+y^2)g = -4x^2y^2 - (x^2+y^2)(3x^2y - y^3) = -4x^2y^2 - y(x^2+y^2)(3x^2 - y^2) =: yh$. So $I_P(f,g) = I_P(yh,g) = I_P(y,g) + I_P(h,g)$ by Axiom 6. $I_P(y,g) = I_P(y,(x^2+y^2)^2 + 3x^2y - y^3) = I_P(y,x^4) = 4I_P(y,x) = 4$. The new intersection number to compute is $I_P(h,g)$. The initial forms are $in(g) = 3x^2y - y^3$ (multiplicity 3) and $in(h) = y^4$ (multiplicity 4). This calculation is still complicated. The algorithmic proof of uniqueness provides a more direct path, though often tedious. (A full calculation shows the final answer is 14).*

Finally, we connect the general intersection number to the order function defined on smooth curves.

Proposition 2.87. *If P is a simple point of an irreducible curve f, then $I_P(f,g) = ord_P^f(\bar{g})$, where $\bar{g}$ is the image of g in the coordinate ring of f, and ord_P^f is the order function associated with the DVR $\mathcal{O}_P(f)$.*

Proof. Since P is a simple point on f, $\mathcal{O}_P(f)$ is a DVR. The order of an element $\bar{g}$ in this ring is given by $\text{ord}_P^f(\bar{g}) = \dim_k(\mathcal{O}_P(f)/(\bar{g}))$. We have a chain of isomorphisms:

$$\mathcal{O}_P(f)/(\bar{g}) \cong (\mathcal{O}_P(\mathbb{A}^2)/(f))/((f,g)/(f)) \cong \mathcal{O}_P(\mathbb{A}^2)/(f,g).$$

Taking dimensions gives $\dim_k(\mathcal{O}_P(f)/(\bar{g})) = \dim_k(\mathcal{O}_P(\mathbb{A}^2)/(f,g))$. By the theorem, the right hand side is $I_P(f,g)$. □

3 Projective Varieties

3.1 Projective Space

3.1.1 Introduction

Why projective space?

In affine space, many theorems (such as Bézout's theorem) are complicated by edge cases. For instance, in the affine plane $\mathbb{A}^2$, two distinct lines intersect at a single point, unless they are parallel. Similarly, a line may intersect a conic section at two points, one point (if tangent), or not at all. This lack of uniformity suggests that affine space is, in some sense, incomplete.

Projective geometry fixes this by adding "points at infinity" where parallel lines can meet. The construction of projective space elegantly formalizes this intuition by "compactifying" affine space.

Consider the relationship between points in the affine line $\mathbb{A}^1$ and lines through the origin in the affine plane $\mathbb{A}^2$. We may identify each point $x \in \mathbb{A}^1$ with the point $(x, 1) \in \mathbb{A}^2$. Each such point uniquely determines a line in $\mathbb{A}^2$ passing through the origin $(0, 0)$. This correspondence captures every line through the origin except for the horizontal axis, the line defined by the equation $y = 0$. This exceptional line, which has no corresponding point in our affine chart, can be naturally interpreted as the "point at infinity." The set of all lines through the origin in $\mathbb{A}^2$ is our first example of a projective space, the projective line $\mathbb{P}^1$. This motivates the general construction.

Definition 3.1. *Let k be a field. **Projective n-space** over k, denoted $\mathbb{P}^n_k$ or simply $\mathbb{P}^n$, is the set of all one-dimensional vector subspaces (lines through the origin) in the affine space $\mathbb{A}^{n+1}$.*

Any non-zero point $(a_0, \ldots, a_n) \in \mathbb{A}^{n+1} \setminus \{(0, \ldots, 0)\}$ determines a unique line through the origin, namely the set of all scalar multiples $\{(\lambda a_0, \ldots, \lambda a_n) \mid \lambda \in k\}$. Two distinct points, $a = (a_0, \ldots, a_n)$ and $b = (b_0, \ldots, b_n)$, determine the same line if and only if they are scalar multiples of each other, i.e., $b = \lambda a$ for some non-zero $\lambda \in k$. This naturally defines an equivalence relation.

This leads to an alternative, but equivalent, formulation of projective space.

Definition 3.2. *Projective n-space, $\mathbb{P}^n$, is the set of equivalence classes of points in $\mathbb{A}^{n+1} \setminus \{(0, \ldots, 0)\}$ under the equivalence relation $\sim$, where $a \sim b$ if and only if $a = \lambda b$ for some $\lambda \in k^*$.*

We denote the equivalence class of a point $(a_0, \ldots, a_n)$ by $[a_0 : \cdots : a_n]$. These are known as the **homogeneous coordinates** of the point in $\mathbb{P}^n$.

Remark 3.3. *The individual components a_i of a homogeneous coordinate vector are not well-defined for a point $P \in \mathbb{P}^n$. However, whether a given coordinate is zero or non-zero is a well-defined property of the point P. Consequently, for any two non-zero coordinates $a_i, a_j \neq 0$, the ratio a_i/a_j is also well-defined, since $(\lambda a_i)/(\lambda a_j) = a_i/a_j$ for any $\lambda \in k^*$.*

Example 3.4. *In $\mathbb{P}^2$, the points $[1 : 0 : 2]$ and $[2 : 0 : 4]$ are identical, because $(2, 0, 4) = 2 \cdot (1, 0, 2)$.*

3.1.2 Covering $\mathbb{P}^n$ in $\mathbb{A}^n$'s

An important feature of projective space is that it can be viewed as a union of overlapping copies of affine space. This structure, known as an affine cover, is the key to transfer concepts from affine to projective geometry.

For each $i \in \{0, \ldots, n\}$, let us define the subset $U_i \subset \mathbb{P}^n$ as:

$$U_i = \{[x_0 : \cdots : x_n] \in \mathbb{P}^n \mid x_i \neq 0\}.$$

Each point $P \in U_i$ has a unique representative in $\mathbb{A}^{n+1}$ whose i-th coordinate is 1. By scaling the homogeneous coordinates by $1/x_i$, we can write P uniquely in the form:

$$P = \left[\frac{x_0}{x_i} : \cdots : \frac{x_{i-1}}{x_i} : 1 : \frac{x_{i+1}}{x_i} : \cdots : \frac{x_n}{x_i}\right].$$

This establishes a canonical bijection between the points of U_i and the points of the affine space $\mathbb{A}^n$, via the map $\phi_i : U_i \to \mathbb{A}^n$:

$$\phi_i([x_0 : \cdots : x_n]) = \left(\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right).$$

The coordinates in $\mathbb{A}^n$ are often called the **non-homogeneous coordinates** for P with respect to the affine chart U_i.

Since any point $P = [x_0 : \cdots : x_n] \in \mathbb{P}^n$ must have at least one non-zero coordinate, it must belong to at least one U_i. Thus, we have a covering of $\mathbb{P}^n$ by $n+1$ sets, each identifiable with $\mathbb{A}^n$:

$$\mathbb{P}^n = \bigcup_{i=0}^{n} U_i.$$

The complement of any such affine chart U_i is also a geometric object of interest. Let us consider the complement of U_n. This set, denoted H_n, consists of all points whose last coordinate is zero:

$$H_n = \mathbb{P}^n \setminus U_n = \{[x_0 : \cdots : x_{n-1} : 0] \in \mathbb{P}^n\}.$$

This set is called the **hyperplane at infinity** (with respect to the chart U_n). There is a natural one-to-one correspondence between points in H_n and points in $\mathbb{P}^{n-1}$, given by the map:

$$[x_0 : \cdots : x_{n-1} : 0] \mapsto [x_0 : \cdots : x_{n-1}].$$

This reveals a fundamental recursive structure of projective space. We can decompose $\mathbb{P}^n$ into a disjoint union:

$$\mathbb{P}^n = U_n \cup H_n \cong \mathbb{A}^n \cup \mathbb{P}^{n-1}.$$

Geometrically, U_n corresponds to the lines through the origin in $\mathbb{A}^{n+1}$ that are not contained in the hyperplane defined by $x_n = 0$, while H_n corresponds to the lines that are contained within that hyperplane.

Example 3.5.

1. ***Dimension 0:*** *$\mathbb{P}^0$ is the set of lines through the origin in $\mathbb{A}^1$. There is only one such line, so $\mathbb{P}^0$ is a single point.*
2. ***Dimension 1:*** *Following the decomposition, $\mathbb{P}^1 \cong \mathbb{A}^1 \cup \mathbb{P}^0$. This is the affine line plus a single point "at infinity". This is the projective line.*
3. ***Lines in $\mathbb{P}^2$:*** *Consider a line L in $\mathbb{A}^2$ defined by $y = mx + b$. We identify $\mathbb{A}^2$ with the affine chart $U_2 \subset \mathbb{P}^2$ via the map $(x, y) \mapsto [x : y : 1]$. A point on L corresponds to a point $[x : y : 1]$ where $y = mx + b$. A naive translation of the equation $y = mx + b$ is not well-defined in homogeneous coordinates, since for a scalar λ, we have $\lambda y = m(\lambda x) + b$, which simplifies to $\lambda y = \lambda(mx) + b$, an inconsistency if $\lambda \neq 1$. The correct procedure is to homogenize the polynomial. We introduce a new variable z (corresponding to x_2) and ensure all terms have the same degree. The equation $y = mx + b$ becomes $y/z = m(x/z) + b$, which clears to $y = mx + bz$. Let $L' = \{[x : y : z] \in \mathbb{P}^2 \mid y = mx + bz\}$. This is a well-defined projective set. Its intersection with the affine chart U_2 (where $z = 1$) is precisely our original line L. Its intersection with the hyperplane at infinity H_2 (where $z = 0$) is given by the equation $y = mx$. This yields a single point $[x : mx : 0] = [1 : m : 0]$. This demonstrates that all lines of a given slope m in the affine plane meet at the same point at infinity.*
4. ***Conics in $\mathbb{P}^2$:*** *Consider the hyperbola in $\mathbb{A}^2$ defined by $y^2 = x^2 + 1$. To find its closure in $\mathbb{P}^2$, we homogenize the equation to $y^2 z = x^2 z + z^3$. If we homogenize to preserve the degree, we get $y^2 = x^2 + z^2$. The intersection of this projective curve with the hyperplane at infinity ($z = 0$) is given by $y^2 = x^2$, which implies $y = \pm x$. This yields two points at infinity: $[1 : 1 : 0]$ and $[1 : -1 : 0]$. These correspond to the two asymptotes of the hyperbola.*

3.1.3 Projective Algebraic Sets

Having established the geometry of $\mathbb{P}^n$, we now define algebraic subsets within it. The key challenge is that a polynomial $f(x_0, \ldots, x_n)$ does not have a well-defined value at a point $P \in \mathbb{P}^n$, as its value depends on the choice of homogeneous coordinates.

Definition 3.6. *A point $P \in \mathbb{P}^n$ is a **zero** of a polynomial $f \in k[x_0, \ldots, x_n]$ if $f(a_0, \ldots, a_n) = 0$ for every choice of homogeneous coordinates $[a_0 : \cdots : a_n]$ for P.*

Example 3.7. *Let $f(x, y) = x - y + 1$ in $k[x, y]$ and consider the point $P = [2 : 1] \in \mathbb{P}^1$. For the representative $(2, 1)$, we have $f(2, 1) = 2 - 1 + 1 = 2 \neq 0$. For the representative $(4, 2)$, we have $f(4, 2) = 4 - 2 + 1 = 3 \neq 0$. It is clear this is poorly behaved. (Even if one representative gave zero, another might not.)*

For the notion of a zero to be meaningful, we must restrict our attention to a special class of polynomials.

Proposition 3.8. *Let $F \in k[x_0, \ldots, x_n]$ be a homogeneous polynomial of degree d. If F vanishes at one representative coordinate vector for a point $P \in \mathbb{P}^n$, then it vanishes at all representative vectors for P.*

Proof. Let $P = [a_0 : \cdots : a_n]$ and suppose $F(a_0, \ldots, a_n) = 0$. Any other set of homogeneous coordinates for P is of the form $(\lambda a_0, \ldots, \lambda a_n)$ for some $\lambda \in k^*$. Since F is homogeneous of degree d, we have:

$$F(\lambda a_0, \ldots, \lambda a_n) = \lambda^d F(a_0, \ldots, a_n) = \lambda^d \cdot 0 = 0.$$

The proposition follows. □

This proposition shows that homogeneous polynomials, also known as *forms*, are the correct building blocks for projective algebraic geometry.

If a general polynomial f is written as a sum of its homogeneous components, $f = \sum_{i=0}^{d} f_i$ where f_i is a form of degree i, then a point $P \in \mathbb{P}^n$ is a zero of f if and only if P is a zero of each homogeneous component f_i. The proof of this is an exercise based on the Vandermonde determinant.

Definition 3.9. *Let S be a set of polynomials in $k[x_0, \ldots, x_n]$. The **projective algebraic set** defined by S, denoted $V(S)$, is the set of all points in $\mathbb{P}^n$ that are simultaneous zeros of every polynomial in S.*

$$V(S) = \{P \in \mathbb{P}^n \mid P \text{ is a zero of each } f \in S\}.$$

Remark 3.10.

1. *Let $I = \langle S \rangle$ be the ideal generated by the set S. Then it is immediate that $V(S) = V(I)$.*
2. *If $I = \langle f_1, \ldots, f_r \rangle$ and we decompose each generator into its homogeneous parts, $f_i = \sum_j F_{ij}$, then $V(I) = V(\{F_{ij}\}_{i,j})$. This implies that any projective algebraic set is the zero set of a finite collection of homogeneous polynomials.*

With the notion of algebraic sets established, we define the corresponding algebraic object.

Definition 3.11. *Let $X \subseteq \mathbb{P}^n$ be any subset. The **homogeneous ideal** of X, denoted $I(X)$, is the set of all polynomials in $k[x_0, \ldots, x_n]$ that vanish at every point in X.*

$$I(X) = \{f \in k[x_0, \ldots, x_n] \mid \text{every } P \in X \text{ is a zero of } f\}.$$

*An ideal $I \subseteq k[x_0, \ldots, x_n]$ is said to be **homogeneous** if for every polynomial $f \in I$, its homogeneous components f_i are also in I.*

Remark 3.12. *An important and easily verifiable fact is that for any subset $X \subseteq \mathbb{P}^n$, the ideal $I(X)$ is always a homogeneous ideal.*

Proposition 3.13. *An ideal $I \subseteq k[x_0, \ldots, x_n]$ is homogeneous if and only if it can be generated by a finite set of homogeneous polynomials (forms).*

Proof. ($\Leftarrow$) Suppose $I = \langle F_1, \ldots, F_r \rangle$, where each F_i is a form of degree d_i. Let $g = \sum_{j=m}^{s} g_j \in I$, where g_j is a form of degree j. We must show that each $g_j \in I$. We can write $g = \sum_{i=1}^{r} A_i F_i$ for some polynomials $A_i \in k[x_0, \ldots, x_n]$. Decomposing each A_i into its homogeneous parts, $A_i = \sum_k A_{ik}$, we have

$$g = \sum_{j=m}^{s} g_j = \sum_{i=1}^{r} \left(\sum_k A_{ik} \right) F_i = \sum_{i,k} A_{ik} F_i.$$

The term $A_{ik}F_i$ is a form of degree $k + d_i$. Equating terms of the same degree, the lowest degree component of g, which is g_m, must be a sum of those $A_{ik}F_i$ for which $k + d_i = m$. Specifically, $g_m = \sum_{i=1}^{r} A_{i,m-d_i} F_i$, which implies $g_m \in I$. Now consider $g - g_m = \sum_{j=m+1}^{s} g_j \in I$. By induction on the number of non-zero homogeneous components, we conclude that all g_j must be in I.

($\Rightarrow$) Suppose I is a homogeneous ideal. By Hilbert's Basis Theorem, I is finitely generated, say $I = \langle f_1, \ldots, f_r \rangle$. Since I is homogeneous, for each f_i, its homogeneous components F_{ij} must also belong to I. The set of all such components $\{F_{ij}\}$ is a finite set of forms that also generates I, since each original f_i is a sum of these forms. □

This establishes the fundamental correspondence in projective algebraic geometry. We have a relationship between geometric objects and algebraic objects:

$$\{ \quad \text{projective algebraic sets in } \mathbb{P}^n \quad \} \quad \longleftrightarrow \quad \{ \, \text{homogeneous ideals in } k[x_0, \ldots, x_n] \, \}$$

The map from right to left is given by V, and the map from left to right is given by I. As in the affine case, this correspondence is inclusion-reversing and will be made more precise by the Projective Nullstellensatz.

Example 3.14. ***Ideal of a Point in*** $\mathbb{P}^2$. *Let $P = [a : b : c] \in \mathbb{P}^2$. Assume without loss of generality that $c \neq 0$, so we can scale the coordinates to have $P = [a : b : 1]$. Consider the ideal $I = \langle x - az, y - bz \rangle$. This is a homogeneous ideal generated by two forms of degree 1. Any point in $V(I)$ must satisfy $x = az$ and $y = bz$, so it must be of the form $[az : bz : z]$. If $z \neq 0$, this is just $[a : b : 1] = P$. If $z = 0$, we get $[0 : 0 : 0]$, which is not a point in $\mathbb{P}^2$. Thus $V(I) = \{P\}$.*

Finally, we introduce the projective analogue of a variety.

Definition 3.15. *A projective algebraic set $V \subseteq \mathbb{P}^n$ is* ***irreducible*** *if it cannot be expressed as the union of two proper projective algebraic subsets. An irreducible projective algebraic set is called a* ***projective variety****.*

Proposition 3.16. *A projective algebraic set $V \subseteq \mathbb{P}^n$ is irreducible if and only if its homogeneous ideal $I(V)$ is a prime ideal.*

Proof. The proof is identical to the affine case, relying only on the properties $V(I \cup J) = V(I) \cup V(J)$ and $I(V \cup W) = I(V) \cap I(W)$. One must simply verify that these properties hold for projective sets and homogeneous ideals. □

3.2 Homogeneous Structures

Now, we introduce some projective algebraic objects. To deepen our understanding of projective algebraic sets, we introduce algebraic structures that are intrinsically linked to their projective nature. A key technique is to relate a projective set $V \subseteq \mathbb{P}^n$ to a corresponding cone in the ambient affine space $\mathbb{A}^{n+1}$, which allows us to leverage the powerful tools of affine geometry, including the classical Nullstellensatz.

3.2.1 Affine Cones

Definition 3.17. *Let $V \subseteq \mathbb{P}^n$ be a projective algebraic set. The* ***affine cone*** *over V, denoted $C(V)$, is the subset of $\mathbb{A}^{n+1}$ formed by the union of all lines passing through the origin that correspond to points in V. Formally,*

$$C(V) = \{(a_0, \ldots, a_n) \in \mathbb{A}^{n+1} \mid [a_0 : \cdots : a_n] \in V\} \cup \{(0, \ldots, 0)\}.$$

Example 3.18.

1. *Let $V = \{[1:0],[0:1]\} \subseteq \mathbb{P}^1$. The corresponding lines through the origin in $\mathbb{A}^2$ are the x-axis (spanned by $(1,0)$) and the y-axis (spanned by $(0,1)$). Thus, $C(V) = \{(x,0) \mid x \in k\} \cup \{(0,y) \mid y \in k\}$, which is the affine variety $V_a(xy)$.*
2. *Let $I = \langle x^2+y^2-z^2\rangle \subseteq \mathbb{C}[x,y,z]$, and let $V = V_P(I) \subseteq \mathbb{P}^2$. In the affine chart $U_2 \cong \mathbb{A}^2$ (where $z=1$), this curve is the circle $x^2+y^2=1$. The affine cone $C(V)$ is the affine variety $V_a(I) \subseteq \mathbb{A}^3$, which is a standard circular cone. The intersection of V with the hyperplane at infinity ($z=0$) is determined by the equation $x^2+y^2=0$. Over $\mathbb{C}$, this factors as $(x-iy)(x+iy)=0$, yielding the two points $[1:i:0]$ and $[1:-i:0]$ at infinity.*

The connection between projective sets and affine cones is captured by the following relations between their ideals.

Remark 3.19. *Let k be an algebraically closed field.*

1. *If $V \subseteq \mathbb{P}^n$ is a non-empty projective algebraic set, then the affine ideal of its cone is precisely the homogeneous ideal of the set: $I_a(C(V)) = I_P(V)$.*
2. *Conversely, if $I \subseteq k[x_0,\dots,x_n]$ is a homogeneous ideal such that its projective zero locus $V_P(I)$ is non-empty, then the affine cone over this locus is the affine zero locus of the ideal: $C(V_P(I)) = V_a(I)$.*

This correspondence is the key to proving the projective analogue of Hilbert's Nullstellensatz.

Theorem 3.20 (Projective Nullstellensatz)**.** *Let k be an algebraically closed field and let I be a homogeneous ideal in $S = k[x_0,\dots,x_n]$.*

1. *$V_P(I) = \emptyset$ if and only if I contains the ideal $\langle x_0,\dots,x_n\rangle^N$ for some integer $N \geq 1$. This ideal is the set of all forms of degree at least N.*
2. *If $V_P(I) \neq \emptyset$, then $I_P(V_P(I)) = \sqrt{I}$.*

Proof. The proof proceeds by reduction to the affine case. Let $\mathfrak{m} = \langle x_0,\dots,x_n\rangle$ be the maximal ideal corresponding to the origin in $\mathbb{A}^{n+1}$.

1. The condition $V_P(I) = \emptyset$ is equivalent to the statement that the only point in the affine variety $V_a(I)$ is the origin, i.e., $V_a(I) \subseteq \{(0,\dots,0)\}$. By the affine Nullstellensatz, this is equivalent to $\sqrt{I} \supseteq I_a(\{(0,\dots,0)\}) = \mathfrak{m}$. Thus, $V_P(I) = \emptyset \iff \mathfrak{m} \subseteq \sqrt{I}$. This means that for each $i \in \{0,\dots,n\}$, there exists an integer r_i such that $x_i^{r_i} \in I$. Let $r = \max\{r_i\}$. Then for any sufficiently large N, any monomial of degree N will be divisible by some x_i^r, implying that $\mathfrak{m}^N \subseteq I$.
2. If $V_P(I) \neq \emptyset$, then its cone $C(V_P(I))$ is a non-trivial affine variety equal to $V_a(I)$. We can then apply the previous remarks and the affine Nullstellensatz:
$$I_P(V_P(I)) = I_a(C(V_P(I))) = I_a(V_a(I)) = \sqrt{I}.$$

□

The Nullstellensatz provides the sought-after dictionary between geometry and algebra. The only special consideration is the ideal $\mathfrak{m} = \langle x_0,\dots,x_n\rangle$ because its projective zero locus is empty.

Corollary 3.21. *Let $S = k[x_0,\dots,x_n]$. There are the following inclusion-reversing bijections:*

$$\left\{\begin{array}{c}\textit{Projective algebraic sets}\\ \textit{in } \mathbb{P}^n\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\textit{Homogeneous radical ideals in } S \textit{ not}\\ \textit{equal to } \mathfrak{m}\end{array}\right\}$$

$$\left\{\begin{array}{c}\textit{Projective varieties in}\\ \mathbb{P}^n\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\textit{Homogeneous prime ideals in } S \textit{ not equal}\\ \textit{to } \mathfrak{m}\end{array}\right\}$$

$$\left\{\begin{array}{c}\textit{Irreducible hypersurfaces}\\ \textit{in } \mathbb{P}^n\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\textit{Principal ideals } \langle F\rangle\textit{, where } F \textit{ is an}\\ \textit{irreducible non-constant form, up to}\\ \textit{scaling}\end{array}\right\}$$

Proof. The proof follows directly from the Projective Nullstellensatz and the definitions of radical and prime ideals. It is a foundational exercise for the reader. □

The simplest non-trivial projective algebraic sets are the linear ones. The sets $V(x_i)$ for $i = 0, \ldots, n$ are the **coordinate hyperplanes**. Each $V(x_i)$ is the hyperplane at infinity with respect to the standard affine chart U_i.

Example 3.22. *In $\mathbb{P}^2$, the coordinate hyperplanes are the lines $V(x_0)$, $V(x_1)$, and $V(x_2)$. These can be visualized as the three "axes" of the projective plane. Any pair of these lines intersects at a single point: $V(x_0) \cap V(x_1) = \{[0:0:1]\}$, for instance.*

With a characterization of the closed sets, we can define a topology on projective space.

Definition 3.23. *The **Zariski topology** on $\mathbb{P}^n$ is the topology whose closed sets are the projective algebraic sets. A set $U \subseteq \mathbb{P}^n$ is **Zariski open** if its complement $\mathbb{P}^n \setminus U$ is a projective algebraic set.*

Exercise 3.24. *The reader should verify that this definition is consistent with the Zariski topology on affine space. Show that for any standard affine chart $U_i \cong \mathbb{A}^n$, the subspace topology induced on U_i from $\mathbb{P}^n$ is identical to the Zariski topology on $\mathbb{A}^n$.*

3.2.2 Homogeneous Coordinate Rings

Just as an affine variety has a coordinate ring, a projective variety has an analogous (but more subtle) algebraic counterpart.

Definition 3.25. *Let $V \subseteq \mathbb{P}^n$ be a non-empty projective variety. The **homogeneous coordinate ring** of V is the quotient ring*

$$S(V) = k[x_0, \ldots, x_n]/I_P(V).$$

Remark 3.26. *Unlike the affine case, the elements of $S(V)$ cannot be interpreted as functions on V. A polynomial F is not well-defined on $\mathbb{P}^n$, and even if $F \in I_P(V)$, the value of a representative polynomial G for a class $\bar{G} \in S(V)$ is not well-defined at a point $P \in V$. The ring $S(V)$ is a fundamental algebraic invariant, but not a ring of functions.*

Because $I_P(V)$ is a homogeneous ideal, the ring $S(V)$ inherits a natural grading from $k[x_0, \ldots, x_n]$.

Definition 3.27. *Let $\Gamma = k[x_0, \ldots, x_n]/I$ where I is a homogeneous ideal. An element $f \in \Gamma$ is a **form of degree** d if it is the image of a homogeneous polynomial $F \in k[x_0, \ldots, x_n]$ of degree d.*

Remark 3.28. *The degree of a non-zero form in Γ is well-defined. Suppose $f = \bar{F} = \bar{G}$ where F and G are forms. Then $F - G \in I$. If $\deg(F) \neq \deg(G)$, since I is a homogeneous ideal, this implies $F \in I$ and $G \in I$. Thus $f = \bar{0}$, contradicting that f is a non-zero form.*

Proposition 3.29. *Let $\Gamma = k[x_0, \ldots, x_n]/I$ for a homogeneous ideal I. Every element $f \in \Gamma$ can be written uniquely as a sum $f = f_0 + f_1 + \cdots + f_d$, where each f_i is a form of degree i.*

Proof. For existence, let $g \in k[x_0, \ldots, x_n]$ be a representative of f. We can write $g = \sum g_i$ as a sum of its homogeneous components. Then $f = \bar{g} = \sum \bar{g_i}$.

For uniqueness, suppose $\sum f_i = \sum h_i$, where f_i, h_i are forms of degree i. Then $\sum(f_i - h_i) = 0$. Let F_i, H_i be homogeneous preimages. Then $\sum(\overline{F_i - H_i}) = 0$, which implies $\sum(F_i - H_i) \in I$. Since I is a homogeneous ideal, we must have $F_i - H_i \in I$ for each i. Therefore, $f_i = \bar{F_i} = \bar{H_i} = h_i$. □

This structure means $S(V)$ is a **graded ring**, $S(V) = \bigoplus_{d=0}^{\infty} S(V)_d$, where $S(V)_d$ is the vector space of forms of degree d.

3.2.3 Rational Functions on Projective Varieties

While elements of $S(V)$ are not functions, we can construct functions on V by taking ratios of its homogeneous elements.

Definition 3.30. *Let V be a projective variety. The **homogeneous function field** of V, denoted $k_h(V)$, is the field of fractions of the integral domain $S(V)$.*

The elements of $k_h(V)$ are fractions F/G where $F, G \in S(V)$ with $G \neq 0$. In general, these are not functions on V. However, a special subclass of these elements is well-defined. Let F and G be forms of the same degree d in $k[x_0, \ldots, x_n]$, and consider a point $P = [a_0 : \cdots : a_n] \in V$ where $G(P) \neq 0$. For any $\lambda \in k^*$, we have:

$$\frac{F(\lambda a_0, \ldots, \lambda a_n)}{G(\lambda a_0, \ldots, \lambda a_n)} = \frac{\lambda^d F(a_0, \ldots, a_n)}{\lambda^d G(a_0, \ldots, a_n)} = \frac{F(a_0, \ldots, a_n)}{G(a_0, \ldots, a_n)}.$$

The value of the ratio is independent of the chosen homogeneous coordinates. This motivates the following definition

Definition 3.31. *The **field of rational functions** on a projective variety V, denoted $k(V)$, is the subfield of $k_h(V)$ consisting of elements of degree zero:*

$$k(V) = \left\{ \frac{F}{G} \mid F, G \in S(V) \text{ are forms of the same degree, } G \neq 0 \right\}.$$

*An element of $k(V)$ is called a **rational function** on V.*

Remark 3.32. *The constant polynomials provide an embedding $k \subseteq k(V)$. The field $k(V)$ is a subfield of the homogeneous function field $k_h(V)$.*

Example 3.33. *Consider $\mathbb{P}^1$ with homogeneous coordinate ring $k[x, y]$. Its function field $k(\mathbb{P}^1)$ consists of ratios $F(x, y)/G(x, y)$ where F, G are homogeneous of the same degree. Let's restrict to the affine chart $U_0 \cong \mathbb{A}^1$ by setting $x = 1$. A rational function becomes $F(1, y)/G(1, y)$, which is a rational function in the single variable y. This gives an isomorphism $k(\mathbb{P}^1) \cong k(y) \cong k(\mathbb{A}^1)$. In general, for any variety V, $k(V)$ is isomorphic to the function field of any of its open affine subvarieties.*

Definition 3.34. *Let V be a projective variety, $P \in V$, and $\phi \in k(V)$. We say ϕ is defined (or **regular**) at P if it can be written as a fraction $\phi = F/G$ where F, G are forms of the same degree in $S(V)$ and $G(P) \neq 0$. The set of all rational functions on V defined at P forms a ring. This is the **local ring of** V **at** P, denoted $\mathcal{O}_{V,P}$.*

Remark 3.35. *For any $P \in V$, the ring $\mathcal{O}_{V,P}$ is a subring of the function field $k(V)$. It is a local ring, and its unique maximal ideal, denoted $\mathfrak{m}_{V,P}$, consists of all functions that vanish at P:*

$$\mathfrak{m}_{V,P} = \{\phi \in \mathcal{O}_{V,P} \mid \phi = F/G \text{ with } F(P) = 0 \text{ and } G(P) \neq 0\}.$$

Example 3.36. *There is a natural isomorphism between the local ring of a projective variety at a point P and the local ring of an affine chart containing P at that same point. Let $P = [0 : 0 : 1] \in \mathbb{P}^2$. This point lies in the affine chart $U_2 \cong \mathbb{A}^2$, where it corresponds to the origin $(0, 0)$. The local ring $\mathcal{O}_{\mathbb{P}^2,P}$ consists of fractions $F(x, y, z)/G(x, y, z)$ where F, G are forms of the same degree and $G(0, 0, 1) \neq 0$. The map $\psi : \mathcal{O}_{\mathbb{P}^2,P} \to \mathcal{O}_{\mathbb{A}^2,(0,0)}$ given by dehomogenization (setting $z = 1$),*

$$\psi\left(\frac{F(x, y, z)}{G(x, y, z)}\right) = \frac{F(x, y, 1)}{G(x, y, 1)},$$

is an isomorphism of rings. This demonstrates that the local geometry of a projective variety is affine.

3.3 Projective Transformations

We have established that projective space $\mathbb{P}^n$ is covered by affine charts $U_i \cong \mathbb{A}^n$. A central theme in algebraic geometry is the interplay between local affine properties and global projective structure. We now formalize the precise relationship between algebraic sets in an affine chart and their closures within the ambient projective space.

3.3.1 Converting Between Affine and Projective Varieties

Let $V \subseteq \mathbb{A}^n$ be an affine algebraic set, where we identify $\mathbb{A}^n$ with the standard chart $U_n \subset \mathbb{P}^n$. Let $I = I(V) \subseteq k[x_1, \ldots, x_n]$ be its vanishing ideal. To embed V into $\mathbb{P}^n$, we must work with homogeneous ideals in $k[x_1, \ldots, x_{n+1}]$.

For any polynomial $f \in k[x_1, \ldots, x_n]$, its **homogenization** $F \in k[x_1, \ldots, x_{n+1}]$ is given by $F = x_{n+1}^{\deg(f)} f(x_1/x_{n+1}, \ldots, x_n/x_{n+}$ We define the homogeneous ideal associated to I as

$$I^h = \langle \{F \mid F \text{ is the homogenization of some } f \in I\} \rangle \subseteq k[x_1, \ldots, x_{n+1}].$$

Definition 3.37. *The **projective closure** of an affine algebraic set $V \subseteq \mathbb{A}^n$, denoted $\overline{V}$, is the projective algebraic set $V_P(I^h) \subseteq \mathbb{P}^n$.*

Topologically, the projective closure $\overline{V}$ is precisely the Zariski closure of V within $\mathbb{P}^n$. By construction, the part of $\overline{V}$ in the original affine chart is V itself, i.e., $\overline{V} \cap U_n = V$.

Remark 3.38. *It is important to note that if $I = \langle f_1, \ldots, f_r \rangle$, it is not generally true that $I^h = \langle F_1, \ldots, F_r \rangle$, where F_i is the homogenization of f_i. Homogenizing the generators of an ideal may not produce a set of generators for the homogenized ideal.*

Example 3.39. *Let $I = \langle x^2 + y, x \rangle \subseteq k[x, y]$. Since $x \in I$, we have $y = (x^2 + y) - x^2 \in I$, so $I = \langle x, y \rangle$. The corresponding affine variety is the origin, $V = \{(0, 0)\} \subset \mathbb{A}^2$. The correct homogenized ideal is $I^h = \langle x, y \rangle \subseteq k[x, y, z]$, and its zero locus is $\overline{V} = V_P(x, y) = \{[0 : 0 : 1]\}$. However, if we naively homogenize the original generators, we get the ideal $J' = \langle x^2 + yz, x \rangle$. The zero locus of J' is given by $x = 0$ and $yz = 0$. This yields two points: $[0 : 0 : 1]$ and $[0 : 1 : 0]$. The extra point at infinity, $[0 : 1 : 0]$, is the result of an incorrect procedure.*

The reverse process is more straightforward. Let $V \subseteq \mathbb{P}^n$ be a projective algebraic set with homogeneous ideal $I = I_P(V) \subseteq k[x_1, \ldots, x_{n+1}]$. To find the affine part $V \cap U_{n+1}$, we simply set the last coordinate to 1. Algebraically, this corresponds to dehomogenization. The ideal of $V \cap U_{n+1}$ in $k[x_1, \ldots, x_n]$ is the image of I under the map that sets $x_{n+1} = 1$. This is equivalent to taking the quotient $\overline{I} = I/\langle x_{n+1} - 1 \rangle$, which lives in $k[x_1, \ldots, x_{n+1}]/\langle x_{n+1} - 1 \rangle \cong k[x_1, \ldots, x_n]$.

Remark 3.40. *This process has a nice geometric interpretation via the affine cone $C(V)$. The ideal I is the ideal of $C(V) \subseteq \mathbb{A}^{n+1}$. The quotient map $k[x_1, \ldots, x_{n+1}] \to k[x_1, \ldots, x_{n+1}]/\langle x_{n+1} - 1 \rangle$ corresponds algebraically to the geometric intersection with the hyperplane $V_a(x_{n+1} - 1)$. Thus, the ideal $\overline{I}$ defines the affine variety $C(V) \cap V_a(x_{n+1} - 1) = V \cap U_{n+1}$.*

3.3.2 Fields of Rational Functions

The geometric correspondence between an affine variety and its projective closure is mirrored by an algebraic isomorphism of their function fields.

Let $V \subseteq \mathbb{A}^n$ be an affine variety (identified with $V \subseteq U_{n+1}$) and let $W = \overline{V} \subseteq \mathbb{P}^n$ be its projective closure. We can define a map $\alpha : k(W) \to k(V)$ by dehomogenizing:

$$\alpha\left(\frac{F}{G}\right) = \frac{F(x_1, \ldots, x_n, 1)}{G(x_1, \ldots, x_n, 1)},$$

where F, G are forms of the same degree in the homogeneous coordinate ring $S(W)$. This map is a well-defined field homomorphism.

Proposition 3.41. *The map $\alpha : k(W) \to k(V)$ is an isomorphism of fields.*

Proof. Since α is a homomorphism of fields, it is injective. To show surjectivity, take any element $\frac{a}{b} \in k(V)$, where $a, b \in k[x_1, \ldots, x_n]$. Let A, B be their respective homogenizations in $k[x_1, \ldots, x_{n+1}]$. To make them have the same degree, we can multiply by a suitable power of x_{n+1}. Let $d_a = \deg(a)$ and $d_b = \deg(b)$.

Consider the element $\phi = \frac{A \cdot x_{n+1}^{\max(0, d_b - d_a)}}{B \cdot x_{n+1}^{\max(0, d_a - d_b)}} \in k(W)$. Its image under α is precisely $\frac{a}{b}$. Thus α is surjective, hence an isomorphism. □

Corollary 3.42. *For any point $P \in V$, the map α induces an isomorphism of local rings $\mathcal{O}_{W,P} \cong \mathcal{O}_{V,P}$.*

Proof. A rational function $F/G \in k(W)$ is regular at $P \in V \subseteq U_{n+1}$ if $G(P) \neq 0$. After dehomogenizing, the denominator becomes $G(x_1, \ldots, x_n, 1)$, which is non-zero at P. This shows $\alpha(\mathcal{O}_{W,P}) \subseteq \mathcal{O}_{V,P}$. Injectivity follows from that of α. Surjectivity follows from reversing the homogenization process in the proof of the proposition, noting that if $b(P) \neq 0$, its homogenization $B(P)$ will also be non-zero. □

Remark 3.43. *The isomorphism of local rings holds at any point $P \in W$. If $P \notin U_{n+1}$, one simply chooses a different affine chart U_i containing P and dehomogenizes with respect to the variable x_i. This confirms that the local geometry of a projective variety is everywhere affine.*

3.3.3 Morphisms of Projective Varieties

Defining morphisms between projective varieties requires care, as polynomial functions are not well-defined. The solution is to define morphisms locally using homogeneous polynomials of the same degree.

Let's motivate this with a key example. Consider the map $\varphi : \mathbb{P}^1 \to \mathbb{P}^2$ given by

$$[s : t] \mapsto [s^2 : st : t^2].$$

This map is well-defined because if we rescale the input, $[\lambda s : \lambda t]$, the output becomes $[\lambda^2 s^2 : \lambda^2 st : \lambda^2 t^2] = [s^2 : st : t^2]$. The coordinates are homogeneous polynomials of the same degree (degree 2). The image of this map lies in the conic $C = V(xz - y^2) \subseteq \mathbb{P}^2$, since $(s^2)(t^2) - (st)^2 = 0$. Locally, this map is a morphism of affine varieties. For instance, on the chart $U_0 \subset \mathbb{P}^1$ (where $s = 1$), the map is $t \mapsto [1 : t : t^2]$, which is the familiar parabola map $\mathbb{A}^1 \to \mathbb{A}^2$ given by $\alpha \mapsto (\alpha, \alpha^2)$.

Definition 3.44. *Let $V \subseteq \mathbb{P}^n$ and $W \subseteq \mathbb{P}^m$ be projective algebraic sets. A function $\varphi : V \to W$ is a **morphism** if for every point $P \in V$, there exists a Zariski open neighborhood U of P in V and $m + 1$ homogeneous polynomials $F_0, \ldots, F_m \in k[x_0, \ldots, x_n]$ of the same degree, such that:*

1. *For every $Q \in U$, at least one $F_i(Q)$ is non-zero.*
2. *The map φ on U is given by $Q \mapsto [F_0(Q) : \cdots : F_m(Q)]$.*

Remark 3.45. *The choice of representing polynomials F_i may be different on different open sets, although sometimes a single set of polynomials works globally, as in the example above.*

Example 3.46. *Let $C = V(xz - y^2) \subseteq \mathbb{P}^2$. Consider the map $\varphi : C \to \mathbb{P}^1$ defined piecewise:*

$$[x : y : z] \mapsto \begin{cases} [x : y] & \text{on } C \setminus \{[0 : 0 : 1]\} \\ [y : z] & \text{on } C \setminus \{[1 : 0 : 0]\} \end{cases}$$

On the overlap, where $x \neq 0$ and $z \neq 0$, we have $y^2 = xz \neq 0$. The two definitions agree:

$$[x : y] = [xz : yz] = [y^2 : yz] = [y : z].$$

This defines a global morphism. In fact, it is the inverse of the map $[s : t] \mapsto [s^2 : st : t^2]$.

Definition 3.47. *A morphism $\varphi : V \to W$ is an **isomorphism** if there exists an inverse morphism $\psi : W \to V$ such that $\psi \circ \varphi = id_V$ and $\varphi \circ \psi = id_W$.*

The previous example shows that the conic $C = V(xz - y^2)$ is isomorphic to the projective line $\mathbb{P}^1$.

3.3.4 Projective Change of Coordinates

The most fundamental morphisms of a projective space onto itself are those induced by linear transformations of the underlying vector space.

Let $T : k^{n+1} \to k^{n+1}$ be an invertible linear transformation. Since T maps lines through the origin to lines through the origin, it induces a well-defined map on $\mathbb{P}^n$, called a **projective change of coordinates** or **projectivity**. If we represent points in k^{n+1} as column vectors, T can be represented by an $(n+1)\times(n+1)$ invertible matrix $M \in \mathrm{GL}(n+1,k)$.

Remark 3.48. *The matrix M and any non-zero scalar multiple λM represent the same projectivity, since they define the same map on equivalence classes. The group of all such transformations is the **Projective General Linear Group**, $PGL(n+1,k) = GL(n+1,k)/k^*$. These are, in fact, all the automorphisms of $\mathbb{P}^n$.*

Definition 3.49. *Two projective algebraic sets $V, W \subseteq \mathbb{P}^n$ are **projectively equivalent** if there exists a projective change of coordinates $T : \mathbb{P}^n \to \mathbb{P}^n$ that restricts to an isomorphism from V to W.*

Example 3.50. *Any two hyperplanes in $\mathbb{P}^n$ are projectively equivalent. For example, in $\mathbb{P}^2$, the lines $V = V(x)$ and $W = V(y-x)$ are projectively equivalent. The change of coordinates $T : \mathbb{P}^2 \to \mathbb{P}^2$ defined by $[x : y : z] \mapsto [x : y + x : z]$ is an isomorphism that maps V to W. Its inverse map T^{-1} sends a point $[x' : y' : z'] \in W$ (so $y' - x' = 0$) to $[x' : y' - x' : z'] = [x' : 0 : z']$, which is a point in $V = V(y)$. Thus $T^{-1}(W) = V$.*

Proposition 3.51. *Let $T : \mathbb{P}^n \to \mathbb{P}^n$ be a projective change of coordinates.*

1. *If $V = V(F_1, \ldots, F_r)$, then $T^{-1}(V) = V(F_1 \circ T, \ldots, F_r \circ T)$.*
2. *T induces isomorphisms $S(V) \cong S(T^{-1}(V))$, $k(V) \cong k(T^{-1}(V))$, and $\mathcal{O}_{T(P)}(V) \cong \mathcal{O}_P(T^{-1}(V))$.*
3. *Any linear subvariety $W \subseteq \mathbb{P}^n$ of dimension d is projectively equivalent to the standard subvariety $V(x_{d+1}, \ldots, x_n)$.*

Remark 3.52. *In the affine setting, two varieties are isomorphic if and only if their coordinate rings are isomorphic. This is false in the projective case. We saw that $\mathbb{P}^1$ is isomorphic to the conic $C = V(xz - y^2) \subseteq \mathbb{P}^2$. However, their homogeneous coordinate rings, $k[s,t]$ and $k[x,y,z]/\langle xz - y^2\rangle$, are not isomorphic (the latter is not a UFD, while the former is). The geometric isomorphism of varieties does not imply an algebraic isomorphism of their homogeneous coordinate rings, because the rings describe the extrinsic geometry of the embedding (i.e., the affine cones), which can differ.*

3.3.5 Projective Plane Curves

We conclude by applying these concepts to the important case of curves in the projective plane, $\mathbb{P}^2$.

Definition 3.53. *A **projective plane curve** is an equivalence class of non-constant homogeneous polynomials $F \in k[x,y,z]$ under the relation $F \sim \lambda F$ for $\lambda \in k^*$. The degree of the curve is the degree of the defining polynomial.*

Local properties of curves, such as multiplicity and tangents, are defined by dehomogenizing in an appropriate affine chart.

Remark 3.54. *If $C = V(F)$ is a projective curve and $P = [a : b : 1] \in C \cap U_2$, then the local ring of C at P is isomorphic to the local ring of the affine curve $c = V(f)$ at the point (a,b), where $f = F(x,y,1)$. That is, $\mathcal{O}_{C,P} \cong \mathcal{O}_{c,(a,b)}$.*

Remark 3.55. *The multiplicity of an affine curve $V(f)$ at the origin $P = (0,0)$ is the degree of the lowest-degree homogeneous component of f. If $f = f_m + f_{m+1} + \cdots + f_d$, then the multiplicity $m_P(f)$ is m. The multiplicity of a projective curve $V(F)$ at a point P is defined to be the multiplicity of its dehomogenization at the corresponding affine point.*

Proposition 3.56. *A point P is a singular (multiple) point of the curve $V(F)$ if and only if it is a simultaneous zero of all partial derivatives:*

$$F(P) = \frac{\partial F}{\partial x}(P) = \frac{\partial F}{\partial y}(P) = \frac{\partial F}{\partial z}(P) = 0.$$

Proof Sketch. By Euler's homogeneous function theorem, if F is a form of degree d, then $d \cdot F = xF_x + yF_y + zF_z$. Thus, if all partials vanish at P, so does F. We can assume $P \in U_2$, so $P = [a : b : 1]$. Singularity in the affine chart means $f(a, b) = f_x(a, b) = f_y(a, b) = 0$. Since $f_x(a, b) = F_x(a, b, 1)$ and $f_y(a, b) = F_y(a, b, 1)$, this implies $F_x(P) = F_y(P) = 0$. The condition $F_z(P) = 0$ then follows from Euler's theorem. □

Definition 3.57. *Let F be a projective plane curve and let P be a point on F. Let L be a line through P. We say that L is **tangent** to F at P if, upon dehomogenizing in a chart U_i containing P, the corresponding affine line l is tangent to the affine curve f at the point corresponding to P.*

Example 3.58. *Let $F = xy^4 + yz^4 + xz^4$. The singular points are found by solving:*

$$\begin{aligned} F_x &= y^4 + z^4 = 0 \\ F_y &= 4xy^3 + z^4 = 0 \\ F_z &= 4yz^3 + 4xz^3 = 4z^3(y + x) = 0 \end{aligned}$$

From $F_z = 0$, either $z = 0$ or $y = -x$. Case 1: $z = 0$. The equations become $y^4 = 0$ and $4xy^3 = 0$, which implies $y = 0$. The point must be $[1 : 0 : 0]$ (since not all coordinates can be zero). We check $F(1, 0, 0) = 0$, so $[1 : 0 : 0]$ is a singular point. Case 2: $y = -x$. The first equation becomes $x^4 + z^4 = 0$. The second becomes $-4x^4 + z^4 = 0$. Together these imply $x = z = 0$, which implies $y = 0$, a contradiction. So $[1 : 0 : 0]$ is the only singular point. To analyze its multiplicity, we dehomogenize with respect to x (by setting $x = 1$) to get $f(y, z) = y^4 + yz^4 + z^4$. The lowest degree term is $y^4 + z^4$, so the multiplicity at the origin $(0, 0)$ is 4. The tangent lines are given by the factors of this term.

Definition 3.59. *Let F, G be projective plane curves and $P \in \mathbb{P}^2$. Choose an affine chart U_i containing P. The **intersection number** of F and G at P, denoted $I_P(F, G)$, is defined as the intersection number of their dehomogenizations in that chart: $I_P(F, G) := I_P(f, g)$. This definition can be shown to be independent of the choice of chart.*

Remark 3.60. *The intersection number in the projective plane satisfies the same axioms as in the affine case, with two modifications:*

- *The translation invariance axiom is replaced by invariance under projective transformations.*
- *The axiom $I_P(F, G) = I_P(F, G + AF)$ requires A to be a homogeneous polynomial such that $\deg(G) = \deg(F) + \deg(A)$, to ensure $G + AF$ is homogeneous.*

4 More on Varieties and Blow-Ups

4.1 The Building Blocks

4.1.1 Linear Systems of Curves

The set of all plane curves of a fixed degree possesses a natural and powerful geometric structure of its own. By parameterizing the coefficients of the defining polynomials, we can identify this set with a projective space, allowing us to study families of curves using the techniques of linear algebra and projective geometry.

Let $d \geq 1$ be an integer. The space of homogeneous polynomials of degree d in three variables, $k[x, y, z]_d$, is a vector space over k. The number of monomials of degree d, which form a basis for this space, can be calculated using a stars-and-bars argument to be $N = \binom{d+2}{2} = \frac{(d+2)(d+1)}{2}$.

Any curve of degree d is defined by a non-zero polynomial $F = \sum_{i=1}^{N} a_i M_i$, where the M_i are the basis monomials and $a_i \in k$. Since two polynomials F and G define the same curve if and only if $G = \lambda F$ for some $\lambda \in k^*$, the curve is uniquely determined by the coefficient vector up to scale. This means the point $[a_1 : \cdots : a_N]$ in projective space $\mathbb{P}^{N-1}$ determines a unique plane curve. This establishes an important bijection:

$$\{\text{Projective plane curves of degree } d\} \longleftrightarrow \mathbb{P}^{N-1} = \mathbb{P}^{\frac{d(d+3)}{2}}.$$

Example 4.1.

1. *For $d = 1$ (lines), $N = \binom{3}{2} = 3$. A line $ax + by + cz = 0$ corresponds to a unique point $[a : b : c]$ in the projective plane $\mathbb{P}^2$. This $\mathbb{P}^2$ is often called the **dual projective space**, as its points correspond to lines in the original $\mathbb{P}^2$.*
2. *For $d = 2$ (conics), $N = \binom{4}{2} = 6$. A conic section given by $a_1x^2 + a_2xy + a_3xz + a_4y^2 + a_5yz + a_6z^2 = 0$ corresponds to a unique point $[a_1 : \cdots : a_6]$ in $\mathbb{P}^5$. The set of all conics in the plane is thus parameterized by a $\mathbb{P}^5$.*

Imposing geometric constraints on curves often translates to linear conditions on their coefficients.

Definition 4.2. *A **linear system** of plane curves of degree d is a family of curves corresponding to the points of a linear subvariety (a sub-projective space) of $\mathbb{P}^{N-1}$.*

Example 4.3. *Consider the set of all lines in $\mathbb{P}^2$ that pass through the point $P = [0 : 0 : 1]$. A line $ax + by + cz = 0$ contains P if and only if $c = 0$. The corresponding points in the dual $\mathbb{P}^2$ are of the form $[a : b : 0]$. This set is a line in $\mathbb{P}^2$, demonstrating that the family of lines through a point is a linear system of dimension 1.*

This observation generalizes.

Lemma 4.4.

1. *Fix a point $P \in \mathbb{P}^2$. The set of all curves of degree d that pass through P forms a hyperplane in the parameter space $\mathbb{P}^{N-1}$.*
2. *A projective change of coordinates on $\mathbb{P}^2$ induces a projective change of coordinates on the parameter space $\mathbb{P}^{N-1}$.*

Proof.

1. Let the curve be represented by the coefficient vector $[\alpha_1 : \cdots : \alpha_N]$ corresponding to the polynomial $F = \sum \alpha_i M_i$. The curve passes through P if and only if $F(P) = 0$, which means $\sum_{i=1}^{N} \alpha_i M_i(P) = 0$. Since not all monomials vanish at any given point, this is a non-trivial linear equation in the coefficients α_i, defining a hyperplane in $\mathbb{P}^{N-1}$.
2. This follows from the fact that a projective transformation acts linearly on the coefficients of the polynomial.

□

Requiring a curve to pass through a set of m distinct points corresponds to intersecting m hyperplanes in $\mathbb{P}^{N-1}$. The dimension of the resulting linear system depends on whether these linear conditions are independent.

Example 4.5. *Let's consider the linear system V of conics ($d = 2, N = 6, \mathbb{P}^5$) passing through four points P_1, P_2, P_3, P_4. We expect the four linear conditions to be independent, which would imply* $\dim(V) = 5-4 = 1$. *However, consider the case where the four points are collinear, all lying on a line L. If a conic F passes through these four points, then by Bézout's Theorem, the intersection number $I(F, L)$ would be at least 4. Since* $\deg(F)\deg(L) = 2$, *this implies that L must be a component of F. Thus, $F = L \cdot L'$ for some other line L'. The system V is therefore in one-to-one correspondence with the set of all possible lines L', which is a $\mathbb{P}^2$. In this degenerate case,* $\dim(V) = 2$.

Remark 4.6. *A fundamental fact of linear algebra is that the intersection of k hyperplanes in $\mathbb{P}^M$ is always non-empty if $k \leq M$. In our context, $M = N - 1$. This implies that there exists at least one curve of degree d passing through any given set of $N - 1 = \frac{d(d+3)}{2}$ points.*

What if we impose conditions on the multiplicity of a curve at a point?

Example 4.7. *Let $P = [0 : 0 : 1]$. For the multiplicity $m_P(F)$ of a conic F to be at least 2, we must analyze the dehomogenized polynomial $f(x, y) = F(x, y, 1)$. For $m_P(f) \geq 2$, the constant and linear terms must vanish. This means the coefficients of z^2, xz, and yz in F must all be zero. This imposes three independent linear conditions on the $\mathbb{P}^5$ of conics. The resulting linear system has dimension $5 - 3 = 2$. Such a conic has the form $F = ax^2 + bxy + cy^2 = (\alpha x + \beta y)(\gamma x + \delta y)$, which represents a pair of lines passing through P.*

In general, requiring a curve of degree d to have multiplicity at least r at a point P imposes $\binom{r+1}{2}$ linear conditions. Let $P = [0 : 0 : 1]$. For $m_P(F) \geq r$, all terms $x^a y^b z^c$ in F where $a + b < r$ must have a zero coefficient. There are $\binom{r+1}{2} = \frac{r(r+1)}{2}$ such terms. This reduces the dimension of the parameter space accordingly.

We adopt the following notation for such linear systems. Let $P_1, \ldots, P_n \in \mathbb{P}^2$ be distinct points and $r_1, \ldots, r_n \in \mathbb{Z}_{\geq 0}$.

$$V_d(r_1P_1, \ldots, r_nP_n) := \{\text{Curves } F \text{ of degree } d \mid m_{P_i}(F) \geq r_i \text{ for all } i\}.$$

Corollary 4.8.

1. *The set $V = V_d(r_1P_1, \ldots, r_nP_n)$ is a linear subvariety of $\mathbb{P}^{N-1}$ of dimension*

$$\dim(V) \geq N - 1 - \sum_{i=1}^{n} \frac{r_i(r_i + 1)}{2}.$$

   (Here we use projective dimension, so $\dim \mathbb{P}^k = k$).

2. *If $d \geq (\sum r_i) - 1$, then the equality holds.*

Proof. The first part of the theorem is a direct consequence of counting linear constraints. The condition of having a multiplicity of at least r_i at a point P_i imposes $\binom{r_i+1}{2} = \frac{r_i(r_i+1)}{2}$ linear conditions on the coefficients of the curve's defining polynomial. Summing these constraints gives the stated lower bound for the dimension.

The second part, proving that these conditions are independent for sufficiently large d, requires a more intricate argument. We proceed by induction on $m = \sum_{i=1}^{n} r_i$.

Base Case: If $m = 1$, the system is $V_d(1P_1)$. This imposes a single linear condition (passing through P_1), which defines a hyperplane. The dimension is $(N - 1) - 1$, so the formula holds.

Inductive Hypothesis: Assume the equality holds for any system defined by points and multiplicities where the sum of multiplicities is less than m.

Now, let $V = V_d(r_1P_1, \ldots, r_nP_n)$ with $\sum r_i = m > 1$ and $d \geq m - 1$. We divide the proof into two cases.

Case 1: All multiplicities are one ($r_i = 1$ for all i). In this case, $m = n$. We must show that $\dim_{\text{proj}}(V_d(P_1, \ldots, P_n)) = (N-1) - n$, given $d \geq n - 1$. Consider the chain of nested linear systems:

$$V_d(P_1) \supset V_d(P_1, P_2) \supset \cdots \supset V_d(P_1, \ldots, P_n).$$

Let $V_i = V_d(P_1, \ldots, P_i)$. By the inductive hypothesis, since $\sum_{j=1}^{n-1} r_j = n - 1$, the dimension of V_{n-1} is $\dim_{\text{proj}}(V_{n-1}) = (N-1) - (n-1)$. The system V_n is obtained from V_{n-1} by imposing one additional linear condition (passing through P_n). Therefore, its dimension is either $\dim_{\text{proj}}(V_{n-1})$ or $\dim_{\text{proj}}(V_{n-1}) - 1$. To prove the equality, we must show that the condition is independent, which means demonstrating that V_n is a proper subvariety of V_{n-1}. To do this, we construct a curve $F \in V_{n-1} \setminus V_n$. Since the points P_i are distinct, for each $i \in \{1, \ldots, n-1\}$, we can choose a line L_i that passes through P_i but not through P_n. Furthermore, let L_0 be a line that does not pass through any of the points $P_1, \ldots, P_n$. Since $d \geq n - 1$, the integer $k = d - (n-1)$ is non-negative. Consider the curve of degree d given by the product:

$$F = L_1 \cdot L_2 \cdots L_{n-1} \cdot L_0^k.$$

By construction, $F(P_i) = 0$ for all $i \in \{1, \ldots, n-1\}$, so $F \in V_{n-1}$. However, $F(P_n) \neq 0$ because none of the lines $L_0, L_1, \ldots, L_{n-1}$ pass through P_n. Thus, $F \notin V_n$. This shows $V_n \subsetneq V_{n-1}$, so the dimension must drop by exactly one. The formula holds.

Case 2: At least one multiplicity is greater than one. Without loss of generality, assume $r_1 > 1$ and, by a projective transformation, that $P_1 = [0 : 0 : 1]$. Let $V = V_d(r_1P_1, r_2P_2, \ldots, r_nP_n)$. We compare it with the system $V_0 = V_d((r_1 - 1)P_1, r_2P_2, \ldots, r_nP_n)$. The sum of multiplicities for V_0 is $m - 1$, and the degree condition $d \geq m - 1 > (m-1) - 1$ is satisfied. Thus, by the inductive hypothesis, we know the exact dimension of V_0. A curve $F \in V_0$ has multiplicity at least $r_1 - 1$ at P_1. Let its dehomogenization with respect to z be $f(x, y)$. The terms of total degree less than $r_1 - 1$ in f are already zero. The terms of degree $r_1 - 1$ are of the form

$$f_{r_1-1} = \sum_{j=0}^{r_1-1} a_j x^j y^{r_1-1-j}.$$

For F to be in V, its multiplicity at P_1 must be at least r_1. This requires that all these coefficients $a_0, \ldots, a_{r_1-1}$ must be zero. This imposes r_1 additional linear conditions. Our goal is to show these r_1 conditions are independent.

To do this, we construct curves that satisfy some of these conditions but not others. Consider the auxiliary system of curves of degree $d - 1$:

$$W = V_{d-1}((r_1 - 2)P_1, r_2P_2, \ldots, r_nP_n).$$

The sum of multiplicities for W is $m - r_1 + (r_1 - 2) = m - 2$. The degree is $d - 1$. The condition $d \geq m - 1$ implies $d - 1 \geq m - 2$, so the inductive hypothesis applies to W. For $j = 0, \ldots, r_1 - 2$, we can impose j additional zero-coefficient conditions on W to get a descending chain of non-empty subspaces. By the inductive hypothesis on W, for each $k \in \{0, \ldots, r_1 - 2\}$, we can find a curve $G_k \in W$ such that its dehomogenization g_k has a non-zero $x^k y^{r_1-2-k}$ term, while all terms of degree $r_1 - 2$ with fewer powers of x are zero.

Now, construct curves of degree d by multiplying by linear forms:

1. For $k \in \{0, \ldots, r_1 - 2\}$, consider the curve $F_k = y \cdot G_k$. This curve has degree d. Its dehomogenization is $f_k = yg_k$. The lowest-degree terms of f_k are of degree $r_1 - 1$, and the term with the fewest powers of x is a non-zero multiple of $x^k y^{r_1-1-k}$. This curve F_k satisfies the conditions $a_0 = \cdots = a_{k-1} = 0$, but fails the condition $a_k = 0$.

2. To handle the last condition ($a_{r_1-1} = 0$), we need a curve whose lowest-degree term in its dehomogenization is x^{r_1-1}. Let G_{r_1-1} be a curve in $V_{d-1}((r_1-1)P_1, \dots)$ which does not have multiplicity r_1 at P_1. By induction, such a curve exists. Consider $F_{r_1-1} = x \cdot G_{r_1-1}$. Its dehomogenization has a non-zero x^{r_1-1} term while satisfying $a_0 = \cdots = a_{r_1-2} = 0$.

This sequence of constructed curves $F_0, \dots, F_{r_1-1}$ shows that the r_1 linear conditions are linearly independent. Therefore, $\dim_{\text{proj}}(V) = \dim_{\text{proj}}(V_0) - r_1$. The dimension of V_0 is given by the inductive hypothesis:

$$\dim_{\text{proj}}(V_0) = (N-1) - \left(\frac{(r_1-1)r_1}{2} + \sum_{i=2}^{n} \frac{r_i(r_i+1)}{2} \right).$$

Subtracting r_1 gives:

$$\begin{aligned}
\dim_{\text{proj}}(V) &= \dim_{\text{proj}}(V_0) - r_1 \\
&= (N-1) - \left(\frac{r_1^2 - r_1}{2} + r_1 + \sum_{i=2}^{n} \frac{r_i(r_i+1)}{2} \right) \\
&= (N-1) - \left(\frac{r_1^2 + r_1}{2} + \sum_{i=2}^{n} \frac{r_i(r_i+1)}{2} \right) \\
&= (N-1) - \sum_{i=1}^{n} \frac{r_i(r_i+1)}{2}.
\end{aligned}$$

This is the required formula, and the induction is complete. □

Example 4.9. *Let $V = V_3(3P)$ where $P = [0:0:1]$. This is the linear system of cubics with a triple point at P. Since the degree condition $d = 3 \geq (\sum r_i) - 1 = 3 - 1 = 2$ is met, the dimension is exactly*

$$\dim(V) = \left(\frac{3(3+3)}{2} - 1 \right) - \frac{3(3+1)}{2} = 8 - 6 = 2.$$

(The dimension of the projective space is 2). Geometrically, if a cubic curve F has a triple point at P, any line L through P must intersect F with multiplicity at least 3. By Bézout's Theorem, this means L must be a component of F. Therefore, any curve in $V_3(3P)$ must be a union of three lines (not necessarily distinct) passing through P. The set of lines through P is a $\mathbb{P}^1$. The set of unordered triples of such lines (e.g. products $L_1L_2L_3$) is parameterized by a $\mathbb{P}^2$.

4.1.2 Bézout's Theorem

We begin with the central result of this section. The theorem asserts that the number of intersection points between two projective plane curves, when counted correctly, is precisely the product of their degrees.

Theorem 4.10 (Bézout's Theorem)**.** *Let F and G be projective plane curves over an algebraically closed field k, having degrees m and n, respectively. If F and G share no common component, then they intersect in exactly mn points, counted with multiplicity. In symbols,*

$$\sum_{P \in F \cap G} I_P(F, G) = mn,$$

where $I_P(F, G)$ denotes the intersection multiplicity of F and G at the point P.

Proof. The proof presented here is a sketch of the algebraic argument, which relies on the dimension of certain quotient rings.

First, since the curves have no common component, their intersection $F \cap G$ is a finite set of points. We may therefore perform a projective change of coordinates such that none of these intersection points lie on the line at infinity $Z = 0$. This allows us to dehomogenize the defining polynomials $F(X, Y, Z)$ and $G(X, Y, Z)$

to obtain affine curves defined by $f(x,y) = F(x,y,1)$ and $g(x,y) = G(x,y,1)$. The intersection points in $\mathbb{P}^2$ now correspond bijectively to the intersection points of the affine curves $V(f)$ and $V(g)$ in $\mathbb{A}^2$.

The intersection multiplicity at a point $P \in \mathbb{A}^2$ is defined via the local ring at P, denoted $\mathcal{O}_P(\mathbb{A}^2)$. Specifically, $I_P(F,G) = \dim_k(\mathcal{O}_P(\mathbb{A}^2)/(f,g)\mathcal{O}_P(\mathbb{A}^2))$. The sum over all intersection points is therefore

$$\sum_{P \in F \cap G} I_P(F,G) = \sum_{P \in V(f,g)} \dim_k(\mathcal{O}_P(\mathbb{A}^2)/(f,g)).$$

A standard result from commutative algebra, which follows from the Nullstellensatz and the structure theory of Artinian rings, asserts that if the variety $V(I)$ of an ideal $I \subset k[x,y]$ is a finite set $\{P_1, \ldots, P_N\}$, then there is a natural isomorphism of k-algebras:

$$k[x,y]/I \cong \prod_{i=1}^{N} \mathcal{O}_{P_i}(\mathbb{A}^2)/I\mathcal{O}_{P_i}(\mathbb{A}^2).$$

Applying this to the ideal $I = (f,g)$, we find that the sum of the local dimensions is the dimension of the global coordinate ring of the intersection:

$$\sum_{P \in F \cap G} I_P(F,G) = \dim_k(k[x,y]/(f,g)).$$

Let us denote $\gamma := k[x,y]/(f,g)$. Let $R = k[X,Y,Z]$ be the homogeneous coordinate ring of $\mathbb{P}^2$, and let $\Gamma = R/(F,G)$. The ring Γ is a graded ring, and we denote its degree-d homogeneous component by Γ_d. The core of the proof lies in relating the dimension of the affine ring γ to the dimensions of the graded pieces Γ_d. One can show that for sufficiently large d, $\dim_k(\Gamma_d) = \dim_k(\gamma)$. We shall demonstrate that for $d \geq m+n$, $\dim_k(\Gamma_d) = mn$.

To compute $\dim_k(\Gamma_d)$, we consider a free resolution of Γ as a graded R-module. Since F and G share no common component, they form a regular sequence in R. This yields the following short exact sequence of graded R-modules, known as the Koszul complex for (F,G):

$$0 \to R(-m-n) \xrightarrow{\psi} R(-m) \oplus R(-n) \xrightarrow{\varphi} R \xrightarrow{\pi} \Gamma \to 0,$$

where the maps are given by $\psi(C) = (GC, -FC)$ and $\varphi(A,B) = AF + BG$. The notation $R(k)$ denotes the twisted module whose degree-d part is R_{d+k}.

Restricting this sequence to the degree-d components gives an exact sequence of finite-dimensional k-vector spaces:

$$0 \to R_{d-m-n} \to R_{d-m} \oplus R_{d-n} \to R_d \to \Gamma_d \to 0.$$

The dimension of the space of homogeneous polynomials of degree k in three variables is $\dim_k(R_k) = \binom{k+2}{2} = \frac{(k+1)(k+2)}{2}$. From the exactness of the sequence of vector spaces, the alternating sum of dimensions is zero (the Euler-Poincaré principle). For any $d \geq m+n$ (so that all indices are non-negative), we have:

$$\dim_k(\Gamma_d) - \dim_k(R_d) + (\dim_k(R_{d-m}) + \dim_k(R_{d-n})) - \dim_k(R_{d-m-n}) = 0.$$

Therefore,

$$\begin{aligned}\dim_k(\Gamma_d) &= \dim_k(R_d) - \dim_k(R_{d-m}) - \dim_k(R_{d-n}) + \dim_k(R_{d-m-n}) \\ &= \frac{(d+1)(d+2)}{2} - \frac{(d-m+1)(d-m+2)}{2} - \frac{(d-n+1)(d-n+2)}{2} \\ &\quad + \frac{(d-m-n+1)(d-m-n+2)}{2}.\end{aligned}$$

A direct algebraic simplification of this expression reveals that the terms involving d^2 and d cancel, leaving a constant:

$$\begin{aligned}\dim_k(\Gamma_d) &= \frac{1}{2}\big[(d^2+3d+2) - (d^2-2dm+m^2+3d-3m+2) \\ &\quad -(d^2-2dn+n^2+3d-3n+2) \\ &\quad +(d^2-2d(m+n)+(m+n)^2+3d-3(m+n)+2)\big] \\ &= \frac{1}{2}[2dm-m^2+3m+2dn-n^2+3n \\ &\quad -2d(m+n)+(m^2+2mn+n^2)-3(m+n)] \\ &= \frac{1}{2}[2mn] = mn.\end{aligned}$$

This concludes the sketch of the proof. □

Bézout's theorem is a powerful tool with many profound corollaries that shape our understanding of plane curves.

Corollary 4.11. *For any two plane curves F and G without common components,*

$$\sum_{P \in F \cap G} m_P(F) m_P(G) \leq \deg(F) \cdot \deg(G),$$

where $m_P(C)$ is the multiplicity of the curve C at point P.

Proof. This follows immediately from Bézout's theorem and the well-known inequality $I_P(F,G) \geq m_P(F)m_P(G)$, which holds for any point P. □

Corollary 4.12. *If two curves F and G of degrees m and n meet in exactly mn distinct points, then each intersection point is a simple point (i.e., nonsingular) on both F and G, and the intersections are transverse.*

Proof. If there are mn distinct intersection points, the sum $\sum I_P(F,G) = mn$ implies that $I_P(F,G) = 1$ for each intersection point P. An intersection multiplicity of 1 occurs if and only if P is a simple point on both curves and their tangent lines at P are distinct. □

Corollary 4.13. *If two curves of degrees m and n intersect at more than mn points, they must share a common component.*

Corollary 4.14. *A nonsingular projective plane curve is irreducible.*

Proof. Suppose, for the sake of contradiction, that a nonsingular curve F is reducible. Then F can be factored as a product of two polynomials, $F = GH$, where G and H define curves of smaller degree. By Bézout's theorem, G and H must intersect (since $\deg(G)\deg(H) \geq 1$). Let $P \in G \cap H$. At such a point, the local equation of F is the product of the local equations of G and H. If we choose coordinates such that $P = (0,0)$ in an affine chart, the dehomogenized polynomials g and h both vanish at the origin, implying they have no constant term. Thus, the polynomial $f = gh$ has no terms of degree 0 or 1. This means the multiplicity of F at P is $m_P(F) \geq 2$, so P is a singular point. This contradicts the assumption that F is nonsingular. □

Remark 4.15. *The preceding corollary is specific to the projective setting. An affine curve can be nonsingular yet reducible. For instance, the affine curve in $\mathbb{A}^2$ defined by $x(x-1) = 0$ is the disjoint union of two lines ($x = 0$ and $x = 1$) and is nonsingular, yet clearly reducible.*

Bézout's theorem can be masterfully applied to constrain the number and type of singularities an irreducible curve can possess. Let us explore this application.

Let F be an irreducible curve of degree d.

- If $d = 1$ (a line) or $d = 2$ (a conic), it is a classical result that F must be nonsingular. (An irreducible conic cannot be a pair of lines, which is the only way a degree 2 curve can be singular).
- If $d = 3$ (a cubic), suppose P is a singular point. Then its multiplicity $m_P(F)$ must be 2, as a multiplicity of 3 would imply F is a union of 3 lines through P, contradicting irreducibility. Let L be any line passing through P and another point Q on the curve. By Bézout's theorem, $\sum_{R \in F \cap L} I_R(F, L) = 3 \cdot 1 = 3$. We know $I_P(F, L) \geq m_P(F) = 2$ and $I_Q(F, L) \geq m_Q(F) \geq 1$. Thus, we must have $I_P(F, L) = 2$ and $I_Q(F, L) = 1$, and there can be no other intersection points. If there were a second singular point P', the line through P and P' would yield an intersection sum of at least $m_P(F) + m_{P'}(F) = 2 + 2 = 4$, which is impossible. Therefore, an irreducible cubic can have at most one singular point, which must be a double point (a node or a cusp).
- If $d = 4$ (a quartic), how many singular points can F have? We can use an auxiliary curve. Let $P_1, \ldots, P_5$ be any five points on F. The space of conics (curves of degree 2) in $\mathbb{P}^2$ has dimension $\binom{2+2}{2} - 1 = 5$. Imposing the condition that a conic passes through a point is one linear condition. Thus, there exists at least one conic C passing through these five points. By Bézout's theorem, F and C intersect in $4 \cdot 2 = 8$ points, counted with multiplicity. If F and C share no common component, then $8 \geq \sum_{i=1}^{5} m_{P_i}(F) m_{P_i}(C) \geq \sum_{i=1}^{5} m_{P_i}(F)$. If we choose the five points to be singular points, this inequality limits their multiplicities. For instance, a quartic cannot have three singular points of multiplicity 3, as this would give a sum $\geq 3 + 3 + 3 = 9 > 8$. More carefully, using the inequality $\sum I_P(F, C) \geq \sum m_P(F)$, we see that a quartic cannot have four double points, since $2+2+2+2 = 8$, and the conic would have to pass through these points, which is generally not possible. An irreducible quartic can have at most 3 singular points.

This line of reasoning can be generalized to derive a powerful bound for a curve of any degree d. The method involves constructing an auxiliary curve, often called an "adjoint" of F, that is tailored to its singularities.

Theorem 4.16. *Let F be an irreducible plane curve of degree d with singular points $P_1, \ldots, P_n$ of respective multiplicities $m_1, \ldots, m_n$. Then*

$$\sum_{i=1}^{n} m_i(m_i - 1) \leq (d - 1)(d - 2).$$

Proof. Consider the linear system of curves of degree $d - 1$. The vector space of homogeneous polynomials of degree $d - 1$ in three variables, R_{d-1}, has dimension $\dim_k(R_{d-1}) = \binom{d-1+2}{2} = \frac{d(d+1)}{2}$.

We impose conditions on these curves. For each singular point P_i of F, we require our auxiliary curves to pass through P_i with multiplicity at least $m_i - 1$. The condition of passing through a point P with multiplicity k imposes $\binom{k+1}{2}$ linear conditions on the coefficients of the curve's polynomial. Thus, for each P_i, we impose $\binom{(m_i-1)+1}{2} = \binom{m_i}{2} = \frac{m_i(m_i-1)}{2}$ conditions.

The dimension of the projective linear system $\mathcal{L}$ of curves of degree $d - 1$ satisfying these conditions is at least

$$\dim \mathcal{L} \geq \left(\frac{d(d+1)}{2} - 1 \right) - \sum_{i=1}^{n} \frac{m_i(m_i - 1)}{2}.$$

Let us pick $r = \dim \mathcal{L}$ additional simple points $Q_1, \ldots, Q_r$ on F, distinct from the P_i. The condition of passing through these r additional points ensures that there is at least one curve $G \in \mathcal{L}$ that passes through all P_i with multiplicity $m_i - 1$ and also passes through all Q_j.

Since F is irreducible and $\deg(G) = d - 1 < \deg(F)$, F and G cannot share a component. We may therefore apply Bézout's theorem to find their total intersection number:

$$\sum_{P \in F \cap G} I_P(F, G) = \deg(F) \deg(G) = d(d - 1).$$

The sum on the left can be bounded from below by considering the known points of intersection:

- At each singular point P_i, $I_{P_i}(F, G) \geq m_{P_i}(F) m_{P_i}(G) \geq m_i(m_i - 1)$.

- At each simple point Q_j, $I_{Q_j}(F,G) \geq m_{Q_j}(F)m_{Q_j}(G) \geq 1 \cdot 1 = 1$.

Combining these gives:

$$d(d-1) \geq \sum_{i=1}^{n} m_i(m_i-1) + \sum_{j=1}^{r} 1 = \sum_{i=1}^{n} m_i(m_i-1) + r.$$

Substituting the lower bound for $r = \dim \mathcal{L}$:

$$d(d-1) \geq \sum m_i(m_i-1) + \left(\frac{d(d+1)}{2} - 1 - \sum \frac{m_i(m_i-1)}{2} \right).$$

Rearranging the terms to isolate the sum involving multiplicities:

$$d(d-1) - \frac{d(d+1)}{2} + 1 \geq \sum m_i(m_i-1) - \sum \frac{m_i(m_i-1)}{2}.$$

$$\frac{2d(d-1) - d(d+1) + 2}{2} \geq \frac{1}{2} \sum m_i(m_i-1).$$

$$2d^2 - 2d - d^2 - d + 2 \geq \sum m_i(m_i-1).$$

$$d^2 - 3d + 2 \geq \sum m_i(m_i-1).$$

Factoring the quadratic on the left gives the desired inequality:

$$(d-1)(d-2) \geq \sum_{i=1}^{n} m_i(m_i-1).$$

□

Remark 4.17. *This inequality is deeply connected to the genus of a curve. For a plane curve, the arithmetic genus is given by $p_a = \frac{(d-1)(d-2)}{2}$, and the geometric genus g of its normalization is given by $g = p_a - \sum \frac{m_i(m_i-1)}{2}$. The fact that the geometric genus must be non-negative ($g \geq 0$) is precisely the statement of the theorem.*

Finally, we show that this bound is sharp, meaning there exist curves for which equality holds.

Example 4.18. *Consider the irreducible curve F defined by the homogeneous polynomial $F(X,Y,Z) = X^d + Y^{d-1}Z$. This curve has degree d. Let us find its singularities. The only potential singular point is where all partial derivatives vanish. In the affine chart $Z = 1$, we have $f(x,y) = x^d + y^{d-1}$. The partial derivatives are $\frac{\partial f}{\partial x} = dx^{d-1}$ and $\frac{\partial f}{\partial y} = (d-1)y^{d-2}$. Both vanish only at $(0,0)$. The lowest degree term of f is y^{d-1}, so the origin is a singular point of multiplicity $m = d-1$. Checking other charts confirms that the point $[0:0:1]$ is the only singularity.*

For this curve, the sum of singularities is

$$\sum m_i(m_i-1) = (d-1)((d-1)-1) = (d-1)(d-2).$$

This matches the upper bound derived in the theorem, demonstrating that the bound is indeed sharp.

4.1.3 Multiprojective Space

Our study of algebraic geometry has so far defined varieties as subsets of a single ambient space, either affine $\mathbb{A}^n$ or projective $\mathbb{P}^n$. This approach, where a variety's definition depends on its embedding, makes it difficult to work with constructions that are independent of any specific ambient space, such as the product of two varieties.

The need for a more general approach is clear when we consider products. The product of two affine spaces, $\mathbb{A}^n \times \mathbb{A}^m$, is isomorphic to $\mathbb{A}^{n+m}$. An algebraic set in this product is therefore an affine variety in $\mathbb{A}^{n+m}$, and its structure is described by the polynomial ring in $n+m$ variables.

However, the product of projective spaces presents a new challenge. In general, $\mathbb{P}^n \times \mathbb{P}^m$ is not isomorphic to $\mathbb{P}^{n+m}$. This means we need a new method for defining algebraic sets within these product spaces, as we cannot simply appeal to the definition of a projective variety in a single ambient space.

The solution is to use polynomials that are homogeneous in each set of projective coordinates separately. Let us consider the polynomial ring $k[X,Y] = k[X_0, \ldots, X_n, Y_0, \ldots, Y_m]$.

Definition 4.19. *A polynomial $F \in k[X,Y]$ is a **biform of bidegree** (p,q) if it is a homogeneous polynomial of degree p in the variables $\{X_0, \ldots, X_n\}$ and simultaneously a homogeneous polynomial of degree q in the variables $\{Y_0, \ldots, Y_m\}$.*

Example 4.20. *The polynomial $F = X_1Y_1Y_2^3 + X_2Y_3^4$ is a biform of bidegree $(1,4)$ in the ring $k[X_1, X_2, Y_1, Y_2, Y_3]$.*

Every polynomial $F \in k[X,Y]$ can be written uniquely as a sum $F = \sum_{p,q} F_{p,q}$, where each $F_{p,q}$ is a biform of bidegree (p,q).

The key property of a biform is that its vanishing is well-defined on $\mathbb{P}^n \times \mathbb{P}^m$. If F is a biform, the condition $F(X,Y) = 0$ does not depend on the choice of scalar representatives for the homogeneous coordinate vectors of points in $\mathbb{P}^n$ and $\mathbb{P}^m$. This allows us to define algebraic sets.

Definition 4.21. *An **algebraic set** in $\mathbb{P}^n \times \mathbb{P}^m$ is the set of common zeroes of a set of biforms S. This is denoted*

$$V(S) = \{([X],[Y]) \in \mathbb{P}^n \times \mathbb{P}^m \mid F(X,Y) = 0 \text{ for all } F \in S\}.$$

We can now define the associated ideals and coordinate rings in a manner analogous to the standard projective case.

Definition 4.22. *Let $V \subseteq \mathbb{P}^n \times \mathbb{P}^m$ be a subset.*

1. *The **ideal** of V, denoted $I(V)$, is the ideal in $k[X,Y]$ generated by all the biforms that are zero for all points $([X],[Y]) \in V$.*
2. *The **bihomogeneous coordinate ring** of V is the quotient ring $\Gamma_b(V) = k[X,Y]/I(V)$.*
3. *The **field of rational functions** of an irreducible algebraic set V is*

$$k(V) = \left\{ \frac{F}{G} \mid F, G \text{ are biforms of the same bidegree in } \Gamma_b(V) \text{ and } G \notin I(V) \right\}.$$

Remark 4.23. *These definitions can be extended to finite products of projective spaces, such as $\mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_r}$, by considering polynomials that are homogeneous in each of the r sets of variables. One can also include an affine factor, $\mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_r} \times \mathbb{A}^m$. In this case, a polynomial is required to be homogeneous in each set of variables corresponding to the projective factors, but there is no restriction on the variables corresponding to the affine factor.*

Fortunately, there is a result that connects this theory of algebraic sets in product spaces back to the familiar theory of projective varieties. This is achieved by an explicit embedding of the product space into a single, larger projective space.

Definition 4.24. *The map $\sigma : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^{(n+1)(m+1)-1}$ given by*

$$([X_0 : \cdots : X_n], [Y_0 : \cdots : Y_m]) \mapsto [\cdots : X_iY_j : \ldots]_{0 \le i \le n, 0 \le j \le m}$$

*is called the **Segre embedding**.*

The Segre map is a morphism that is an isomorphism onto its image. Furthermore, its image is a closed algebraic set in the target projective space. This means that any algebraic set in $\mathbb{P}^n \times \mathbb{P}^m$ corresponds to a projective variety under this embedding. The important consequence is that the product space $\mathbb{P}^n \times \mathbb{P}^m$ is itself a projective variety.

4.2 Morphisms and Properties of Varieties

4.2.1 Varieties: The General Case

Let $X = \mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_r} \times \mathbb{A}^m$. As with affine and projective space, we can define a topology on X using algebraic sets. A subset is defined to be closed if it is the common zero locus of a set of appropriate multihomogeneous polynomials.

Definition 4.25. *The **Zariski topology** is defined on X by declaring its closed sets to be the algebraic sets. A set $U \subseteq X$ is open if and only if its complement $X \setminus U$ is an algebraic set.*

Any subset $Y \subseteq X$ inherits a topology from X (the subspace topology), where the open sets of Y are of the form $Y \cap U$ for some open set $U \subseteq X$.

We can now give a more general definition of a variety. This definition will include not only the affine and projective varieties we have already studied, but also open subsets of them.

Definition 4.26. *Let V be a nonempty, irreducible algebraic set in a product space $\mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_r} \times \mathbb{A}^m$. Any non-empty open subset $X \subseteq V$ is called a **variety**.*

1. *The **field of rational functions** on X, denoted $k(X)$, is defined to be the function field of its closure, $k(V)$.*
2. *The **local ring** of X at a point $P \in X$, denoted $\mathcal{O}_P(X)$, is defined to be the local ring of V at P, $\mathcal{O}_P(V)$.*

The central concept for studying these varieties is the notion of a regular function. A rational function is regular on an open set if it is well-defined at every point of that set.

Definition 4.27. *Let X be a variety and let $U \subseteq X$ be an open subset. A rational function $f \in k(X)$ is said to be **regular** on U if it is defined at each point $P \in U$. The **ring of regular functions** on U is the set of all such functions:*

$$\Gamma(U, \mathcal{O}_X) := \{f \in k(X) \mid f \text{ is regular on } U\}.$$

This ring can also be described as the intersection of the local rings of all points in U:

$$\Gamma(U, \mathcal{O}_X) = \bigcap_{P \in U} \mathcal{O}_P(X).$$

Remark 4.28. *If X is an affine variety, then the ring of regular functions on X is precisely its coordinate ring: $\Gamma(X, \mathcal{O}_X) = \Gamma(X)$. This is a foundational result from the theory of affine varieties.*

Example 4.29. *The situation is very different for projective varieties. Let $X = \mathbb{P}^n$. The ring of regular functions on all of $\mathbb{P}^n$ consists only of the constant functions:*

$$\begin{aligned}\Gamma(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}) &= \{F/G \mid F, G \text{ homogeneous of the same degree}, G(P) \neq 0 \text{ for all } P \in \mathbb{P}^n\} \\ &= k.\end{aligned}$$

This is because a homogeneous polynomial G that never vanishes on $\mathbb{P}^n$ must be a constant (by the Projective Nullstellensatz). For F/G to be a well-defined rational function, F must then also be a constant. This result holds for any projective variety X; we have $\Gamma(X, \mathcal{O}_X) = k$.

Each element $f \in \Gamma(U, \mathcal{O}_X)$ determines a function from U to the field k. The following proposition states that this correspondence is faithful; distinct elements in the ring of regular functions define distinct functions.

Proposition 4.30. *The natural ring map from the ring of regular functions to the ring of all k-valued functions on U,*

$$\Gamma(U, \mathcal{O}_X) \to \mathcal{F}(U, k) := \{\text{functions } U \to k\},$$

is injective.

Proof. Let $\gamma \in \Gamma(U, \mathcal{O}_X)$ be an element that maps to the zero function, meaning $\gamma(P) = 0$ for all $P \in U$. We need to show that γ is the zero element in the function field $k(X)$.

By definition, $k(X) = k(\overline{X})$, where $\overline{X}$ is the closure of X. So we may assume X is a closed, irreducible algebraic set in some product space $\mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_r} \times \mathbb{A}^m$. Since U is a non-empty open set, we can find an affine chart that intersects it. That is, we can find a standard affine open set $A \cong \mathbb{A}^N$ of the ambient space such that $U' = U \cap A$ is non-empty.

Let $X' = X \cap A$. Then X' is a non-empty open subset of X, so $k(X') = k(X)$. Since X' is a closed subset of an affine space A, X' is an affine variety. The set $U' \subseteq X'$ is a non-empty open subset of an affine variety.

The element γ is in $k(X) = k(X')$, so we can write it as a fraction $\gamma = f/g$, where f, g are in the coordinate ring $\Gamma(X')$ and $g(P) \neq 0$ for all P in some open subset of X'. Since $\gamma \in \Gamma(U, \mathcal{O}_X)$, for any point $P \in U'$, we can find a representation $\gamma = f_P/g_P$ with $g_P(P) \neq 0$.

The condition $\gamma(P) = 0$ for all $P \in U$ implies $f_P(P) = 0$ for all $P \in U'$. This means the numerator of our rational function vanishes on the non-empty open set U'. Since X' is an irreducible affine variety, its coordinate ring $\Gamma(X')$ is an integral domain. In such a ring, a function that is zero on a non-empty open set must be the zero element. Thus, $f = 0$ in $\Gamma(X')$, which implies that $\gamma = 0$ in the function field $k(X')$, and therefore $\gamma = 0$ in $k(X)$. □

Definition 4.31. *Let X be a variety. A closed subset $Y \subseteq X$ is **irreducible** if it cannot be written as the union of two proper closed subsets.*

Remark 4.32. *In many applications, we will be concerned with projective varieties or open subsets of them. However, the general theory outlined here is the proper context for discussing concepts like dimension, birationality, and the resolution of singularities.*

4.2.2 Morphisms of Varieties

With a general definition of a variety, we must now define the maps between them. A morphism is a function that is continuous and respects the structure of regular functions.

Definition 4.33. *Let X and Y be varieties. A **morphism** from X to Y is a function $\varphi : X \to Y$ such that:*

1. *φ is continuous with respect to the Zariski topologies. That is, for every open set $U \subseteq Y$, the preimage $\varphi^{-1}(U)$ is an open set in X.*
2. *φ preserves regular functions. That is, for every open set $U \subseteq Y$ and for every regular function $f \in \Gamma(U, \mathcal{O}_Y)$, the pullback function $\varphi^*(f) := f \circ \varphi$ is a regular function on the open set $\varphi^{-1}(U)$. So, $\varphi^*(f) \in \Gamma(\varphi^{-1}(U), \mathcal{O}_X)$.*

*An **isomorphism** of X with Y is a morphism $\varphi : X \to Y$ for which there exists an inverse morphism $\psi : Y \to X$.*

Remark 4.34. *This definition agrees with the more concrete definitions of morphisms between affine or projective varieties that are given in terms of polynomial or rational maps.*

Remark 4.35. *If $U \subseteq X$ is an open subset of a variety and $\varphi : X \to Y$ is a morphism, then the restriction of φ to U, denoted $\varphi|_U : U \to Y$, is also a morphism.*

Example 4.36 (Affine Charts of Projective Space)**.** *The standard open sets of projective space are isomorphic to affine space. Consider the standard affine chart $U_n = \{[X_0 : \cdots : X_n] \in \mathbb{P}^n \mid X_n \neq 0\}$ and the map $\varphi : \mathbb{A}^n \to U_n$ given by*

$$(x_1, \ldots, x_n) \mapsto [x_1 : \cdots : x_n : 1].$$

This map is a morphism. Its inverse, $\varphi^{-1} : U_n \to \mathbb{A}^n$, which is given by dehomogenization $[X_0 : \cdots : X_n] \mapsto (X_0/X_n, \ldots, X_{n-1}/X_n)$, is also a morphism. Therefore, φ is an isomorphism, and we can identify the open set $U_n \subset \mathbb{P}^n$ with the affine space $\mathbb{A}^n$.

Example 4.37 (An Open Set Isomorphic to an Affine Variety)**.** *Consider the hyperbola $V = V(xy-1) \subseteq \mathbb{A}^2$. This is an irreducible closed set in $\mathbb{A}^2$, so it is an affine variety. Its coordinate ring is $\Gamma(V) = k[x,y]/(xy-1)$.*

Now consider the open subset $W = \mathbb{A}^1 \setminus \{0\}$. Let us show that V is isomorphic to W. Define a morphism $\varphi : V \to W$ by $\varphi(x,y) = x$. This is a morphism because it is given by a polynomial. The image is clearly W, since for any $x \neq 0$, the point $(x, 1/x)$ is in V. Define a map $\psi : W \to V$ by $\psi(t) = (t, 1/t)$. The coordinate functions of ψ are t and $1/t$. While $1/t$ is not a polynomial in $k[t]$, it is a regular function on the open set $W = \mathbb{A}^1 \setminus \{0\}$. Therefore, ψ is a morphism.

The maps φ and ψ are inverse to each other. Thus, V and W are isomorphic. This is a significant example: the open subset $W = \mathbb{A}^1 \setminus \{0\}$ is an affine variety, even though it is not a closed subset of $\mathbb{A}^1$.

The previous example can be generalized. Certain open subsets of affine varieties, known as principal open sets, are always affine.

Proposition 4.38. *Let V be an affine variety and let $f \in \Gamma(V)$ be a non-zero regular function. Let V_f be the open set where f does not vanish:*

$$V_f = \{P \in V \mid f(P) \neq 0\} = V \setminus V(f).$$

This set is called a principal open set.

1. *The ring of regular functions on V_f is the localization of the coordinate ring $\Gamma(V)$ at f:*

$$\Gamma(V_f) = \Gamma(V)[\frac{1}{f}] = \left\{ \frac{a}{f^n} \in k(V) \mid a \in \Gamma(V), n \in \mathbb{Z}_{\geq 0} \right\}.$$

2. *The variety V_f is an affine variety. That is, V_f is isomorphic to a closed algebraic set in some affine space.*

Proof. 1. This is a standard result from commutative algebra relating localization to the topology of the spectrum of a ring. (Proof omitted).

2. We can construct the isomorphism explicitly. Suppose $V \subseteq \mathbb{A}^n$ and let $I = I(V) \subseteq k[x_1, \ldots, x_n]$. Consider a new ideal $I' \subseteq k[x_1, \ldots, x_n, x_{n+1}]$ defined as:

$$I' = (I, x_{n+1}f - 1).$$

Let $V' = V(I')$. This is a closed algebraic set in $\mathbb{A}^{n+1}$, so it is an affine variety. The claim is that $V_f \cong V'$. The isomorphism $\phi : V_f \to V'$ is given by

$$\phi(P) = (P, 1/f(P)).$$

Its inverse $\psi : V' \to V_f$ is the projection onto the first n coordinates. One can verify that these are mutually inverse morphisms.

□

This result has a far-reaching consequence. It implies that any variety, as we have defined it, can be covered by open sets that are themselves affine varieties.

Theorem 4.39. *Any variety X has an open cover by subvarieties that are affine varieties.*

Sketch. For any point $P \in X$, we can find an open set U containing P that is an open subset of some affine variety V. We can then find a function $f \in \Gamma(V)$ such that $P \in V_f \subseteq U$. By the proposition, V_f is an affine variety. Repeating this for all points in X gives the desired cover. □

4.2.3 Dimension

Our geometric intuition provides a clear, albeit informal, understanding of dimension: a curve is one-dimensional, a surface is two-dimensional, and the spaces $\mathbb{A}^n$ and $\mathbb{P}^n$ are naturally n-dimensional. We have previously established an algebraic definition for the dimension of an affine variety. We now introduce an equivalent, and in many ways more intrinsic, definition rooted in the structure of the field of rational functions on a variety. This perspective conceives of dimension as a measure of the "number of independent variables" required to define the function field.

A key feature of this approach is its invariance under birational equivalence. Since the field of rational functions $k(X)$ of a variety X is identical to that of any of its non-empty open subsets U, i.e., $k(U) = k(X)$, our definition will immediately imply that dimension is a local property. Consequently, an open subset and its ambient variety share the same dimension. This aligns with our geometric intuition, as exemplified by the birational equivalence of affine space $\mathbb{A}^n$ and projective space $\mathbb{P}^n$ via the standard open charts $U_i \subset \mathbb{P}^n$.

To formalize this, we must first recall some fundamental concepts from field theory. Recall that for a field extension $L \subseteq K$, the field $L(v_1, \ldots, v_n)$ denotes the smallest field containing L and the elements $v_1, \ldots, v_n \in K$; it is precisely the field of fractions of the polynomial ring $L[v_1, \ldots, v_n]$.

Definition 4.40. *A field K is said to be a **finitely generated field extension** of a subfield L if there exist elements $v_1, \ldots, v_n \in K$ such that $K = L(v_1, \ldots, v_n)$.*

The notion of dimension is captured by the extent to which such an extension is "algebraic."

Definition 4.41. *Let K be a finitely generated field extension of a field k. The **transcendence degree** of K over k, denoted $tr.deg_k K$, is the minimal integer $n \geq 0$ for which there exist elements $x_1, \ldots, x_n \in K$ such that K is an algebraic extension of the field $k(x_1, \ldots, x_n)$. The set $\{x_1, \ldots, x_n\}$ is called a **transcendence basis**. A field K with $tr.deg_k K = n$ is called an **algebraic function field** in n variables over k.*

Example 4.42. *Consider the field $K = \mathbb{Q}(\sqrt{5}, \pi, x)$, where x is an indeterminate. The elements $\sqrt{5}$ and π are transcendental over $\mathbb{Q}$, while $\sqrt{5}$ is algebraic over $\mathbb{Q}(\pi, x)$. The field K is an algebraic extension of $\mathbb{Q}(\pi, x)$, as it is generated by adjoining $\sqrt{5}$, which is a root of the polynomial $t^2 - 5 \in \mathbb{Q}(\pi, x)[t]$. Thus, $tr.deg_{\mathbb{Q}} K = 2$.*

Example 4.43. *Let $V = V(x^2 - y) \subset \mathbb{A}^2_{\mathbb{C}}$ be the standard parabola. The coordinate ring is $\Gamma(V) = \mathbb{C}[x, y]/(x^2 - y) \cong \mathbb{C}[x]$. The field of rational functions is $k(V) = Frac(\mathbb{C}[x]) = \mathbb{C}(x)$. This field is a purely transcendental extension of $\mathbb{C}$ of degree one. Alternatively, viewing the function field as a subfield of $\mathbb{C}(x, y)$, we note that $y = x^2$, so the field is generated by x over $\mathbb{C}$. The field $k(V)$ is algebraic over $\mathbb{C}(y)$, since x satisfies the polynomial $T^2 - y = 0$ with coefficients in $\mathbb{C}(y)$. Hence, $tr.deg_{\mathbb{C}} k(V) = 1$.*

We are now prepared to state our main definition.

Definition 4.44. *Let X be an algebraic variety over a field k. The **dimension** of X, denoted $\dim(X)$, is the transcendence degree of its function field over the base field k:*

$$\dim(X) := tr.deg_k k(X).$$

This definition immediately applies to varieties of dimension one, commonly known as curves. The following proposition establishes several foundational properties of such fields. Let us assume for simplicity that the base field k is algebraically closed.

Proposition 4.45. *Let K be an algebraic function field in one variable over an algebraically closed field k. Let $x \in K$ be an element that is not in k.*

1. *The field K is a finite algebraic extension of the purely transcendental extension $k(x)$.*
2. *If $char(k) = 0$, the Primitive Element Theorem holds: there exists an element $y \in K$ such that $K = k(x, y)$.*
3. *Let R be an integral domain with $k \subseteq R \subset K$ and $Frac(R) = K$. If $P \subset R$ is a non-zero prime ideal, then the residue field R/P is isomorphic to k.*

Proof. 1. By definition of K being a function field of one variable, there exists some $t \in K$ such that K is algebraic over $k(t)$. Since $x \in K$, x must be algebraic over $k(t)$. This implies the existence of a non-zero polynomial relationship $f(t, x) = 0$ with coefficients in k. As x is transcendental over k (since $x \notin k$ and k is algebraically closed), the variable t must appear in this polynomial. We may thus view $f(t, x) = 0$ as a polynomial equation for t with coefficients in $k[x]$. This shows that t is algebraic over $k(x)$. Consequently, the extension $k(x, t)$ is algebraic over $k(x)$. Since K is algebraic over $k(t)$, and $k(t)$ is algebraic over $k(x)$, it follows by transitivity of algebraic extensions that K is algebraic over $k(x)$.

2. This is a standard result from field theory and its proof is omitted.

3. Suppose, for the sake of contradiction, that there exists an element $\bar{x} \in R/P$ that is not in the image of k. Let $x \in R$ be a representative of this class. Since $\bar{x} \notin k$, x must be transcendental over k. Let $y \in P$ be any non-zero element. Since $x, y \in K$ and $\mathrm{tr.deg}_k K = 1$, x and y must be algebraically dependent over k. Thus, there exists a polynomial $f(X, Y) \in k[X, Y]$ such that $f(x, y) = 0$. We may write this as $f(x, y) = \sum_{i=0}^{m} a_i(x) y^i = 0$. By factoring out the highest possible power of y, we may assume without loss of generality that the constant term $a_0(x)$ is non-zero. From the relation, we have $a_0(x) = -y \sum_{i=1}^{m} a_i(x) y^{i-1}$. Since $y \in P$, the right-hand side is in P, which implies $a_0(x) \in P$. Passing to the quotient R/P, we find $a_0(\bar{x}) = 0$. This constitutes a non-trivial polynomial equation for $\bar{x}$ over k. However, since k is algebraically closed, any element algebraic over k must lie in k itself. This implies $\bar{x} \in k$, contradicting our initial assumption. Therefore, the map $k \to R/P$ must be surjective, and since it is clearly injective, it is an isomorphism.

□

With this framework, we can now deduce several fundamental geometric properties concerning the dimension of varieties.

Proposition 4.46. *Let X be a variety over an algebraically closed field k.*

1. *If $U \subseteq X$ is a non-empty open subset, then $\dim U = \dim X$. In particular, if X is an affine variety, its dimension is equal to the dimension of its projective closure $\overline{X}$.*
2. *$\dim X = 0$ if and only if X is a point.*
3. *Every proper closed subvariety of an irreducible curve C consists of a finite set of points.*
4. *A closed subvariety of $\mathbb{A}^2$ (respectively, $\mathbb{P}^2$) has dimension one if and only if it is an affine (respectively, projective) plane curve.*

Proof. 1. This is an immediate consequence of the definition, as $k(U) = k(X)$ for any non-empty open subset U of an irreducible variety X. The statement about projective closure follows from the fact that an affine variety is a dense open subset of its closure.

2. If $\dim X = 0$, then its function field $k(X)$ is an algebraic extension of k. Since k is algebraically closed, this implies $k(X) = k$. Let $U = X \cap \mathbb{A}^n$ be a non-empty affine open subset of X. Then the coordinate ring $\Gamma(U)$ is a subring of $k(U) = k(X) = k$. As an integral domain that is a finitely generated k-algebra, $\Gamma(U)$ must be k itself. By the Nullstellensatz, U must be a single point. Since U is dense in X, X must also be a single point. The converse is clear.

3. Let C be a curve, so $\dim C = 1$. Let $V \subsetneq C$ be a proper closed subvariety. We may assume without loss of generality that C is affine. Let $R = \Gamma(C)$ be its coordinate ring and let $P = I(V) \subset R$ be the prime ideal corresponding to V. Since V is a proper subvariety, P is a non-zero ideal. The coordinate ring of V is $\Gamma(V) = R/P$. By the result on residue fields of function fields of one variable established in the previous section, the residue field R/P is isomorphic to k. The function field $k(V)$ is the fraction field of $\Gamma(V) \cong k$, so $k(V) = k$. Thus, $\dim V = \mathrm{tr.deg}_k k = 0$. By part (2), V must be a point. If V is reducible, it is a finite union of points.

4. This is left as an exercise for the reader. It follows from the fact that the function field of a plane curve defined by an irreducible polynomial $F(x, y)$ is the fraction field of $k[x, y]/(F)$, which has transcendence degree one.

□

4.2.4 Rational Maps and Birational Equivalence

While morphisms are the natural analogues of continuous functions for varieties, they are often too rigid for certain geometric investigations. A more flexible notion is that of a *rational map*, which is a morphism defined only on a dense open subset of a variety. This concept is central to the classification of varieties up to birational equivalence, a coarser but profoundly important equivalence relation.

Definition 4.47. *Let X and Y be varieties. A **rational map** $f : X \dashrightarrow Y$ is an equivalence class of pairs (U, ϕ_U), where $U \subseteq X$ is a non-empty open set and $\phi_U : U \to Y$ is a morphism. Two pairs (U, ϕ_U) and (V, ϕ_V) are considered equivalent if ϕ_U and ϕ_V agree on the intersection $U \cap V$. The **domain** of f is the union of all open sets U for which such a representative (U, ϕ_U) exists. A rational map is defined as having a maximal domain of definition; that is, it cannot be extended to a morphism on any strictly larger open set.*

Example 4.48. *The map $f : \mathbb{A}^1 \dashrightarrow \mathbb{A}^1$ given by the rational function $x \mapsto 1/x$ is a rational map. It defines a morphism on the open set $U = \mathbb{A}^1 \setminus \{0\}$. This morphism cannot be extended to the point $x = 0$, so U is the maximal domain of definition.*

The uniqueness of a rational map is guaranteed by a fundamental property of morphisms.

Proposition 4.49. *Let $f, g : X \to Y$ be two morphisms of varieties. If f and g agree on a dense subset of X, then $f = g$.*

Sketch. Consider the product variety $Y \times Y$. The diagonal $\Delta_Y = \{(y, y) \mid y \in Y\}$ is a closed subvariety. This can be seen locally, where if Y is affine with coordinate ring A, then $Y \times Y$ is affine with coordinate ring $A \otimes_k A$, and the ideal of the diagonal is generated by elements of the form $a \otimes 1 - 1 \otimes a$. Now, consider the morphism $(f, g) : X \to Y \times Y$ defined by $x \mapsto (f(x), g(x))$. The set where f and g agree is precisely the preimage of the diagonal, $(f, g)^{-1}(\Delta_Y)$. Since Δ_Y is closed, this preimage is a closed subset of X. By hypothesis, this closed set contains a dense subset of X, and therefore must be all of X. Thus, $f(x) = g(x)$ for all $x \in X$. □

Since any non-empty open set in an irreducible variety is dense, this proposition ensures that a rational map is uniquely determined by its behavior on any open set where it is defined. This allows us to study the induced maps on function fields.

Definition 4.50. *A rational map $f : X \dashrightarrow Y$ is said to be **dominant** if for some (and hence any) representative morphism $\phi_U : U \to Y$, the image $\phi_U(U)$ is a dense subset of Y.*

A dominant map is precisely one for which we can define a pullback homomorphism on function fields.

Proposition 4.51. *Let $f : X \dashrightarrow Y$ be a dominant rational map. Then f induces an injective field homomorphism $f^* : k(Y) \to k(X)$.*

Proof. Let (U, ϕ_U) be a representative for f. Since f is dominant, $\phi_U(U)$ is dense in Y. Let $V \subseteq Y$ be an affine open set. Its preimage $\phi_U^{-1}(V)$ is an open subset of U, and hence of X. We may replace U with this smaller set and assume we have a morphism $\phi : U \to V$ where U and V are affine and $\phi(U)$ is dense in V. This morphism induces a ring homomorphism $\phi^* : \Gamma(V) \to \Gamma(U)$. This homomorphism is injective because $\phi(U)$ is dense in V. This injection of integral domains extends to an injection of their fields of fractions, $f^* : k(V) \to k(U)$. Since $k(V) = k(Y)$ and $k(U) = k(X)$, we obtain the desired injective homomorphism $f^* : k(Y) \to k(X)$. □

This leads to a central question: what is the geometric significance of an isomorphism of function fields?

Definition 4.52. *A rational map $f : X \dashrightarrow Y$ is **birational** if it is dominant and there exists a dominant rational map $g : Y \dashrightarrow X$ such that $g \circ f = id_X$ and $f \circ g = id_Y$ as rational maps. This is equivalent to the existence of non-empty open sets $U \subseteq X$ and $V \subseteq Y$ such that f restricts to an isomorphism $f|_U : U \xrightarrow{\cong} V$. Two varieties X and Y are **birationally equivalent** if such a map exists.*

Example 4.53. *The standard inclusion of affine space into projective space, $f : \mathbb{A}^n \to \mathbb{P}^n$ given by $(x_1, \ldots, x_n) \mapsto [x_1 : \cdots : x_n : 1]$, is a birational map. Its image is the open set $U_0 = \{[z_0 : \cdots : z_n] \mid z_n \neq 0\}$, and it is an isomorphism onto this set.*

Example 4.54. *Consider the map $f : \mathbb{P}^1 \to C \subset \mathbb{P}^2$, where $C = V(Y^3 - XZ^2)$, given by $[a : b] \mapsto [a^3 : ab^2 : b^3]$. The image lies on the cubic curve C, since $(ab^2)^3 - (a^3)(b^3)^2 = a^3b^6 - a^3b^6 = 0$. The curve C has a singularity (a cusp) at $[1 : 0 : 0]$. The map f is a morphism, but it is not an isomorphism because the curve C is singular while $\mathbb{P}^1$ is smooth. However, it is birational. An inverse rational map $g : C \dashrightarrow \mathbb{P}^1$ is given by $[X : Y : Z] \mapsto [Y : Z]$. This map is well-defined away from the point where $Y = Z = 0$, which is the point $[1 : 0 : 0]$.*

Remark 4.55. *A deep result in the theory of algebraic curves states that a smooth projective cubic curve (an elliptic curve) is never birational to $\mathbb{P}^1$. In general, a projective curve is birational to $\mathbb{P}^1$ if and only if it is a rational curve, which for cubics, corresponds to having a singular point.*

The connection between birational maps and function fields is made precise by the following results. To establish them, we require the algebraic notion of dominance for local rings.

Definition 4.56. *Let (A, m_A) and (B, m_B) be local rings with $A \subseteq B$. We say that B **dominates** A if $m_A \subseteq m_B$.*

Lemma 4.57. *Let $f : X \dashrightarrow Y$ be a dominant rational map, inducing $f^* : k(Y) \to k(X)$. Let $P \in X$ and $Q \in Y$ be points.*

1. *If P is in the domain of f and $f(P) = Q$, then the local ring $\mathcal{O}_{P,X}$ dominates the subring $f^*(\mathcal{O}_{Q,Y})$.*
2. *Conversely, if $\mathcal{O}_{P,X}$ dominates $f^*(\mathcal{O}_{Q,Y})$, then P is in the domain of f and $f(P) = Q$.*

Proof. 1. Let $\phi \in \mathcal{O}_{Q,Y}$. By definition, $\phi = a/b$ for regular functions a, b in a neighborhood of Q with $b(Q) \neq 0$. Then $f^*(\phi) = (a \circ f)/(b \circ f)$. Since $f(P) = Q$, $(b \circ f)(P) = b(Q) \neq 0$, so $f^*(\phi)$ is regular at P. Thus, $f^*(\mathcal{O}_{Q,Y}) \subseteq \mathcal{O}_{P,X}$. If ϕ is in the maximal ideal $m_Q \subset \mathcal{O}_{Q,Y}$, then $a(Q) = 0$. This implies $(a \circ f)(P) = a(Q) = 0$, so $f^*(\phi) \in m_P$. Hence, $f^*(m_Q) \subseteq m_P$.

2. Let W be an affine neighborhood of Q with coordinate ring $\Gamma(W) = k[y_1, \ldots, y_n]/I(W)$. The functions y_i are in $\mathcal{O}_{Q,Y}$. By hypothesis, their images $f^*(y_i)$ are in $\mathcal{O}_{P,X}$. Thus, for each i, we can write $f^*(y_i) = a_i/b_i$ where a_i, b_i are regular in an affine neighborhood V of P and $b_i(P) \neq 0$. Let $b = \prod b_i$. Then $b(P) \neq 0$, and all $f^*(y_i)$ are regular on the distinguished open affine set $V_b \subseteq V$. This implies that $f^*(\Gamma(W)) \subseteq \Gamma(V_b)$. This inclusion of coordinate rings induces a morphism $g : V_b \to W$ which represents the rational map f. To see that $g(P) = Q$, let $\alpha \in I(Q) \subset \Gamma(W)$. Then $\alpha \in m_Q \subset \mathcal{O}_{Q,Y}$. By the dominance hypothesis, $f^*(\alpha) \in m_P$. This means the regular function representing $f^*(\alpha)$ on V_b vanishes at P. This holds for all generators of $I(Q)$, so $g(P) = Q$.

□

This lemma is the key to showing that the correspondence between dominant rational maps and field homomorphisms is a bijection.

Theorem 4.58. *Let X and Y be varieties. Any non-zero k-algebra homomorphism $\varphi : k(Y) \to k(X)$ is induced by a unique dominant rational map $f : X \dashrightarrow Y$.*

Sketch. Uniqueness follows from the preceding proposition regarding the uniqueness of morphisms. For existence, we may replace X and Y with affine open subsets. Let $\Gamma(Y)$ be the coordinate ring of Y. Since $\Gamma(Y)$ is a finitely generated k-algebra, its image $\varphi(\Gamma(Y))$ is a finitely generated subalgebra of $k(X)$. For a finite set of generators of $\varphi(\Gamma(Y))$, we can find a common denominator $b \in \Gamma(X)$ such that all generators

lie in the localized ring $\Gamma(X)_b = \Gamma(X_b)$. Thus, we have an inclusion $\varphi(\Gamma(Y)) \subseteq \Gamma(X_b)$, which induces a morphism $f : X_b \to Y$. This morphism represents a rational map $X \dashrightarrow Y$, which is dominant because φ is injective. □

We now arrive at the main theorem of this section, which establishes that the study of varieties up to birational equivalence is entirely equivalent to the study of their function fields up to k-algebra isomorphism.

Theorem 4.59. *Two varieties X and Y are birationally equivalent if and only if their function fields $k(X)$ and $k(Y)$ are isomorphic as k-algebras.*

Proof. ($\implies$) If X and Y are birationally equivalent, there exist open sets $U \subseteq X$ and $V \subseteq Y$ and an isomorphism $f : U \to V$. An isomorphism induces an isomorphism of coordinate rings $\Gamma(U) \cong \Gamma(V)$, which in turn gives an isomorphism of their fraction fields. Thus, $k(X) = k(U) \cong k(V) = k(Y)$.

($\impliedby$) Suppose $\varphi : k(Y) \xrightarrow{\cong} k(X)$ is a k-algebra isomorphism. By the preceding theorem, φ is induced by a dominant rational map $f : X \dashrightarrow Y$, and its inverse $\varphi^{-1} : k(X) \xrightarrow{\cong} k(Y)$ is induced by a dominant rational map $g : Y \dashrightarrow X$. The composition $g \circ f$ induces the homomorphism $(\varphi)^{-1} \circ \varphi = \mathrm{id}_{k(Y)}$, which is the identity. The identity map on $k(Y)$ is induced by the identity rational map on Y. By uniqueness, $g \circ f = \mathrm{id}_Y$. Similarly, $f \circ g = \mathrm{id}_X$. Therefore, f is a birational equivalence. □

This powerful theorem motivates a central classification problem in algebraic geometry.

Definition 4.60. *A variety X of dimension n is said to be **rational** if it is birationally equivalent to projective space $\mathbb{P}^n$. This is equivalent to its function field $k(X)$ being a purely transcendental extension of k, i.e., $k(X) \cong k(t_1, \ldots, t_n)$.*

Remark 4.61. *Determining whether a given variety is rational is a notoriously difficult problem. For example, it is a long-standing open question whether all smooth cubic hypersurfaces in $\mathbb{P}^5$ (known as cubic fourfolds) are rational.*

As a final application, we show that from a birational perspective, all curves are planar.

Corollary 4.62. *Every irreducible algebraic curve is birationally equivalent to a plane curve.*

Proof. Let C be an irreducible curve. Its function field $k(C)$ has transcendence degree one over k. Assuming $\mathrm{char}(k) = 0$, by the Primitive Element Theorem established in the previous section, there exist $a, b \in k(C)$ such that $k(C) = k(a, b)$. Consider the k-algebra homomorphism $\psi : k[x, y] \to k[a, b] \subseteq k(C)$ defined by $x \mapsto a, y \mapsto b$. The kernel $I = \ker(\psi)$ is a prime ideal in $k[x, y]$ because its image $k[a, b]$ is an integral domain. Therefore, $V' = V(I) \subset \mathbb{A}^2$ is an irreducible affine plane curve. The coordinate ring of V' is $\Gamma(V') = k[x, y]/I \cong k[a, b]$. Taking fields of fractions, we get $k(V') \cong \mathrm{Frac}(k[a, b]) = k(a, b) = k(C)$. By the main theorem of this section, it follows that C and V' are birationally equivalent. □

4.3 Blowing Up and Birational Geometry

4.3.1 Blowing Up A Point in $\mathbb{A}^2$

A central theme in the study of algebraic varieties is the management and elimination of singularities. While singular points are geometrically interesting, they are often the source of technical difficulties, as many fundamental theorems and constructions require the hypothesis of smoothness. The process of **resolving singularities** for a variety C aims to construct a non-singular variety X along with a birational morphism $f : X \to C$. This process provides a smooth model that is birationally equivalent to the original, allowing us to study its geometry in a more controlled setting. From an algebraic perspective, for a curve C, the points on the resolution X correspond to the DVRs of the function field $k(C)$.

The fundamental tool for resolving singularities is the **blow-up**, a surgical procedure that modifies a variety locally around a singular point. The geometric intuition is as follows: given a singular point P on a curve $C \subset \mathbb{P}^2$, we excise the point P and replace it with a copy of $\mathbb{P}^1$. Each point on this new $\mathbb{P}^1$ corresponds to a distinct tangent direction through P in the ambient space. The new curve, living in this modified space,

will have singularities that are, in a precise sense, "less severe" than the original. By iterating this process, one can eventually resolve all singularities of the curve.

We begin by constructing the blow-up of a point in the affine plane, $\mathbb{A}^2$. The construction relies on the concept of the graph of a map.

Definition 4.63 (Graph of a Morphism)**.** *If $f : X \to Y$ is a morphism of varieties, the **graph** of f, denoted $G(f)$, is the subset*

$$G(f) := \{(x, y) \in X \times Y \mid y = f(x)\}.$$

It is a standard result that the graph $G(f)$ is a closed subvariety of the product variety $X \times Y$. Furthermore, the projection map $\pi_X : G(f) \to X$ is an isomorphism.

Remark 4.64 (Topology on Product Varieties)**.** *It is crucial to note that the Zariski topology on a product of varieties, such as $X \times Y$, is not the product topology of the respective Zariski topologies. Instead, the topology is defined by considering an embedding of the product into a single large ambient space. For instance, the product $\mathbb{P}^n \times \mathbb{P}^m$ is endowed with the topology it inherits as a closed subvariety of $\mathbb{P}^{(n+1)(m+1)-1}$ via the Segre embedding.*

By an appropriate choice of coordinates, any point in $\mathbb{A}^2$ can be moved to the origin. Therefore, to understand the local structure of a blow-up, it suffices to construct the blow-up of $\mathbb{A}^2$ at the point $(0, 0)$. This construction will serve as the local model for all subsequent blowing-up procedures.

4.3.2 Directions For Blowing Up $\mathbb{A}^2$ at $(0, 0)$

The blow-up is constructed by taking the closure of the graph of a rational map that assigns to each point its direction from the origin.

1. Let $P = (0, 0) \in \mathbb{A}^2$. Consider the open set $U = \mathbb{A}^2 \setminus \{P\}$. We can define a rational map from $\mathbb{A}^2$ to $\mathbb{P}^1$ by $(x, y) \mapsto [x : y]$. This map is a well-defined morphism from U to $\mathbb{P}^1$. The blow-up of $\mathbb{A}^2$ at P, denoted $B_P(\mathbb{A}^2)$, is defined as the closure of the graph of this morphism in $\mathbb{A}^2 \times \mathbb{P}^1$.
2. Let the coordinates on $\mathbb{A}^2$ be (x, y) and the homogeneous coordinates on $\mathbb{P}^1$ be $[u : v]$. Then the graph is the set $\{((x, y), [u : v]) \in U \times \mathbb{P}^1 \mid xv = yu\}$. The blow-up $B_P(\mathbb{A}^2)$ is the closed subvariety of $\mathbb{A}^2 \times \mathbb{P}^1$ defined by the single homogeneous equation $xv - yu = 0$.
3. The blow-up comes with a natural projection morphism $\pi : B_P(\mathbb{A}^2) \to \mathbb{A}^2$. The fiber over any point $(x, y) \in U$ is a single point. However, the fiber over the origin $P = (0, 0)$ is the set $\{((0, 0), [u : v]) \mid 0 \cdot v - 0 \cdot u = 0\}$, which is $\{P\} \times \mathbb{P}^1$. This fiber $E = \pi^{-1}(P)$ is called the **exceptional divisor**.
4. The map π is an isomorphism from $B_P(\mathbb{A}^2) \setminus E$ to $\mathbb{A}^2 \setminus \{P\}$. Thus, the blow-up is a birational morphism.

For computational purposes, it is often more convenient to work with affine charts. The space $B_P(\mathbb{A}^2)$ is covered by two affine charts, corresponding to $u \neq 0$ and $v \neq 0$ on $\mathbb{P}^1$.

Let's analyze the chart where $v \neq 0$. We can dehomogenize by setting $v = 1$, so the coordinate on this chart of $\mathbb{P}^1$ is $z = u/v$. The equation becomes $x - yz = 0$, or $x = yz$. This chart is an affine plane $\mathbb{A}^2$ with coordinates (y, z). The projection map π in these coordinates is given by $\pi(y, z) = (yz, y)$.

Similarly, in the chart where $u \neq 0$, we set $u = 1$ and let the coordinate be $w = v/u$. The equation is $xw - y = 0$, or $y = xw$. This chart is an affine plane with coordinates (x, w), and the projection is $\pi(x, w) = (x, xw)$.

Let us focus on the second chart, with the map $\psi : \mathbb{A}^2 \to \mathbb{A}^2$ given by $\psi(x, w) = (x, xw)$. This map is birational and represents one of the two affine pieces of the blow-up. The exceptional divisor in this chart is given by the equation $x = 0$.

Example 4.65. *Let $C = V(y^2 - x^2(x + 1))$, a nodal cubic. We analyze its behavior under the blow-up. The preimage $\psi^{-1}(C)$ is the set of points (x, w) such that $\psi(x, w) \in C$. Substituting the defining equations:*

$$(xw)^2 - x^2(x + 1) = 0$$

$$x^2w^2 - x^3 - x^2 = 0$$
$$x^2(w^2 - x - 1) = 0$$

The total preimage $\psi^{-1}(C)$ is the union of two components: $V(x^2)$ and $V(w^2 - x - 1)$.

- *The component $V(x)$ is the exceptional divisor E.*
- *The component $V(w^2 - x - 1)$ is the closure of $\pi^{-1}(C \setminus \{P\})$, and is called the **strict transform** of C, denoted C'.*

The curve C is birationally equivalent to the smooth parabola $C' = V(w^2 - x - 1)$. The points of C' lying over the origin P are the points in the intersection $C' \cap E$. This is given by setting $x = 0$ in the equation for C', which yields $w^2 - 1 = 0$, so $w = \pm 1$. The two points are $(0, 1)$ and $(0, -1)$ in the (x, w)-plane. These two points correspond to the two distinct tangent directions of the node at the origin.

More generally, let $C \subset \mathbb{A}^2$ be an irreducible curve defined by $g(x, y) = 0$. Let $g = g_r + g_{r+1} + \cdots + g_n$ be the decomposition of g into homogeneous forms, where g_i has degree i and $g_r \neq 0$. The integer r is the multiplicity of C at the origin, $m_P(C)$. The equation of the strict transform C' is given by the following proposition.

Proposition 4.66. *The strict transform C' is the variety $V(g')$, where*

$$g'(x, w) = g_r(1, w) + xg_{r+1}(1, w) + \cdots + x^{n-r}g_n(1, w).$$

Proof. The total preimage is given by $g(x, xw) = 0$. Using the homogeneity of the forms g_i:

$$g(x, xw) = g_r(x, xw) + \cdots + g_n(x, xw) = x^r g_r(1, w) + \cdots + x^n g_n(1, w) = x^r g'(x, w).$$

Since g_r is the lowest degree form, $g_r(1, w)$ is not identically zero, so x does not divide g'. The irreducibility of g' follows from the irreducibility of g. Thus, $V(g')$ is the correct component corresponding to the strict transform. □

The points on the exceptional divisor that lie on the strict transform correspond to the tangent directions of the original curve at the singular point.

Proposition 4.67. *Let the tangent lines to C at $P = (0, 0)$ be given by the factors of the lowest degree form, $g_r = \prod_{i=1}^{s}(y - \alpha_i x)^{r_i}$. Then the points of the strict transform C' lying over P are precisely the points $P_i = (0, \alpha_i)$ in the (x, w)-plane. Furthermore, the multiplicity of C' at such a point is bounded by the multiplicity of the corresponding tangent line:*

$$m_{P_i}(C') \leq I_{P_i}(C', E) = r_i.$$

In particular, if P is an ordinary multiple point on C (meaning all $r_i = 1$), then each P_i is a simple (non-singular) point on C'.

Proof. The points in $C' \cap E$ are found by setting $x = 0$ in the equation for g'. This yields $g_r(1, w) = 0$. Since $g_r(x, y) = \prod(y - \alpha_i x)^{r_i}$, we have $g_r(1, w) = \prod(w - \alpha_i)^{r_i}$, whose roots are precisely the α_i. The intersection multiplicity $I_{P_i}(C', E)$ is computed by the length of the ring $\mathcal{O}_{\mathbb{A}^2, P_i}/(g', x)$. This is

$$I_{P_i}(g', x) = I_{P_i}(g_r(1, w), x) = I_{P_i}(\prod_{j=1}^{s}(w - \alpha_j)^{r_j}, x) = I_{P_i}((w - \alpha_i)^{r_i}, x) = r_i.$$

The multiplicity $m_{P_i}(C')$ is always less than or equal to the intersection multiplicity with any curve, in particular with the line E. □

Example 4.68. *Let $C = V(y^2 - x^3)$. Here the lowest degree form is $g_2 = y^2$, so the origin is a singular point with a single tangent line $y = 0$ of multiplicity 2. This is a cusp. The strict transform is given by the equation $(xw)^2 - x^3 = x^2(w^2 - x) = 0$, so $C' = V(w^2 - x)$. The point lying over the origin is $(0, 0)$ in the*

(x, w)-plane. The new curve C' is a smooth parabola, but it is tangent to the exceptional divisor $E = V(x)$ at this point. To resolve this tangency and separate the curve from the exceptional divisor, a further blow-up may be required.

Example 4.69. *Consider the curve C defined by $g(x, y) = 2x^4 - 3x^2y + y^2 - 2y^3 + y^4 = 0$. This curve has a singularity at the origin $P = (0, 0)$. The lowest degree homogeneous part of g is $g_2 = y^2$. This indicates a singularity of multiplicity 2 with a single tangent line $y = 0$ of multiplicity 2. This type of singularity, where two branches of a curve are tangent, is known as a* ***tacnode****.*

We perform a blow-up at the origin using the standard chart given by the birational map $\psi : \mathbb{A}^2 \to \mathbb{A}^2$, where $\psi(x, w) = (x, xw)$. The total transform $\psi^{-1}(C)$ is defined by the equation $g(x, xw) = 0$:

$$2x^4 - 3x^2(xw) + (xw)^2 - 2(xw)^3 + (xw)^4 = 0$$

$$2x^4 - 3x^3w + x^2w^2 - 2x^3w^3 + x^4w^4 = 0$$

Factoring out the highest possible power of x, which corresponds to the exceptional divisor, we get:

$$x^2(2x^2 - 3xw + w^2 - 2xw^3 + x^4w^4) = 0$$

The strict transform C' is the curve defined by $g'(x, w) = 2x^2 - 3xw + w^2 - 2xw^3 + x^4w^4 = 0$.

To analyze the result of the blow-up, we find the points of C' that lie over the origin P. These are the points in the intersection of C' with the exceptional divisor $E = V(x)$. Setting $x = 0$ in the equation for g' gives $w^2 = 0$, so $w = 0$. The only such point is $P' = (0, 0)$ in the (x, w)-plane.

Now we examine the nature of the singularity of C' at P'. We find the lowest degree homogeneous part of $g'(x, w)$ at $(0, 0)$. This is the polynomial $w^2 - 3xw + 2x^2$. This quadratic form is not zero and factors into distinct linear terms:

$$w^2 - 3xw + 2x^2 = (w - x)(w - 2x)$$

This indicates that the new point P' is an ordinary double point (a node) on C', with two distinct tangent lines $w = x$ and $w = 2x$. Thus, the single blow-up has simplified the singularity, transforming the tacnode on C into a simpler node on C'. A further blow-up at P' would separate these two branches completely.

4.3.3 Blowing Up $\mathbb{P}^2$ At A Point

Our previous construction of the blow-up of $\mathbb{A}^2$ at a point provides a crucial local model for resolving singularities. However, to work with projective varieties, such as curves in $\mathbb{P}^2$, we require a global construction that respects the projective structure. We now define the blow-up of the projective plane $\mathbb{P}^2$ at a point. This construction will be seen to agree with the affine blow-up on local charts.

Let us choose coordinates on $\mathbb{P}^2$ such that the point to be blown up is $P = [0 : 0 : 1]$. The core idea is to define a rational map from $\mathbb{P}^2$ to $\mathbb{P}^1$ that is undefined precisely at P, and then to define the blow-up as the closure of the graph of this map. This process effectively replaces the point P with the $\mathbb{P}^1$ of all lines passing through it.

Let $U = \mathbb{P}^2 \setminus \{P\}$. We define a morphism $f : U \to \mathbb{P}^1$ by the rule

$$f([x_1 : x_2 : x_3]) = [x_1 : x_2].$$

This map is well-defined because for any point in U, at least one of x_1 or x_2 must be non-zero. Let $G \subseteq U \times \mathbb{P}^1$ be the graph of this morphism. The blow-up of $\mathbb{P}^2$ at P is the closure of this graph in the product space $\mathbb{P}^2 \times \mathbb{P}^1$.

Let $([x_1 : x_2 : x_3], [y_1 : y_2])$ be coordinates for a point in $\mathbb{P}^2 \times \mathbb{P}^1$. A point lies on the graph G if and only if $[x_1 : x_2] = [y_1 : y_2]$, which is equivalent to the condition $x_1y_2 - x_2y_1 = 0$.

Definition 4.70. *The* ***blow-up*** *of $\mathbb{P}^2$ at the point $P = [0 : 0 : 1]$, denoted $B_P(\mathbb{P}^2)$, is the closed subvariety of $\mathbb{P}^2 \times \mathbb{P}^1$ defined by the bi-homogeneous equation:*

$$V(x_1y_2 - x_2y_1) \subseteq \mathbb{P}^2 \times \mathbb{P}^1.$$

Let $B = B_P(\mathbb{P}^2)$. The set-theoretic difference $B \setminus G$ consists of points where the map f was not originally defined, namely points over P. If we substitute $x_1 = 0, x_2 = 0$ into the defining equation, we get $0 \cdot y_2 - 0 \cdot y_1 = 0$, which is always satisfied. Thus, the fiber over P is the set $\{([0:0:1], [y_1 : y_2]) \mid [y_1 : y_2] \in \mathbb{P}^1\}$. This fiber is isomorphic to $\mathbb{P}^1$ and is the **exceptional divisor** E. The blow-up B is therefore the disjoint union of the graph G and the exceptional divisor E.

The projection onto the first factor, $\pi : B \to \mathbb{P}^2$, is a birational morphism. By construction, it restricts to an isomorphism from $B \setminus E$ to $U = \mathbb{P}^2 \setminus \{P\}$.

We now demonstrate that this global, projective construction is locally identical to the affine blow-up constructed previously. To study the blow-up near a point on the exceptional divisor, we may restrict to an affine neighborhood.

Let $Q = ([0:0:1], [1:\lambda])$ be a point on the exceptional divisor E. We can study the geometry of B near Q by working in an affine chart of $\mathbb{P}^2 \times \mathbb{P}^1$ that contains Q. A natural choice is the chart where $x_3 \neq 0$ and $y_1 \neq 0$.

Let $\varphi_3 : \mathbb{A}^2 \to U_3 \subset \mathbb{P}^2$ be the standard affine chart map, given by $(x, y) \mapsto [x : y : 1]$. In these coordinates, the point P corresponds to the origin $(0, 0) \in \mathbb{A}^2$. Let the affine coordinate on the chart $y_1 \neq 0$ of $\mathbb{P}^1$ be $z = y_2/y_1$.

The defining equation for the blow-up is $x_1 y_2 - x_2 y_1 = 0$. In our chosen affine chart, we can dehomogenize by dividing by $x_3 y_1$:

$$\frac{x_1}{x_3}\frac{y_2}{y_1} - \frac{x_2}{x_3}\frac{y_1}{y_1} = 0$$
$$xz - y = 0.$$

This is precisely the equation $y = xz$ that defined one of the affine charts of the blow-up of $\mathbb{A}^2$ at the origin. The projection map π, when restricted to this chart, sends a point with coordinates (x, z) to the point $[x : xz : 1]$ in $\mathbb{P}^2$. Composing with the inverse of φ_3, this corresponds to the map $(x, z) \mapsto (x, xz)$ from $\mathbb{A}^2$ to $\mathbb{A}^2$.

This shows that the global projective blow-up, when viewed locally in an appropriate affine coordinate system, is identical to the affine blow-up. Therefore, our previous local computations for analyzing singularities of affine curves are fully justified and can be understood as taking place within a chart of the proper global construction.

5 Rings and Modules I

5.1 Foundations

5.1.1 Introduction

This text is an advanced introduction to commutative algebra for first year graduate students. While the material is presented with a view toward applications in algebraic geometry, it also serves as a comprehensive, self-contained treatment of the subject for those interested in the field in its own right.

Background needed: A strong background in abstract algebra is assumed, equivalent to a year-long undergraduate sequence: familiarity with the theory of rings, modules, and fields is assumed.

Material covered: The primary goal is to cover the core material corresponding to the first thirteen chapters of David Eisenbud's *Commutative Algebra with a View Toward Algebraic Geometry*. Key topics will include: Localization and Primary Decomposition, Hilbert's Nullstellensatz, The Artin-Rees Lemma, Flat Families and the Tor Functor, Completions of Rings, Noether Normalization, Systems of Parameters, Discrete Valuation Rings and Dedekind Domains, Dimension Theory, Hilbert-Samuel Polynomials, and more!

Throughout this text, all rings are assumed to be commutative and possess a multiplicative identity element, denoted by 1, unless explicitly stated otherwise.

Definition 5.1. *A **ring homomorphism** between rings R and S is a map $\phi : R \to S$ that preserves the underlying abelian group structure, respects multiplication (i.e., $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R$), and maps the identity of R to the identity of S (i.e., $\phi(1_R) = 1_S$).*

Definition 5.2. *Let R be a ring. An ideal $I \subsetneq R$ is said to be **prime** if for any $f, g \in R$, the condition $fg \in I$ implies that $f \in I$ or $g \in I$. An ideal $I \subsetneq R$ is **maximal** if it is not properly contained in any other proper ideal of R.*

Definition 5.3. *A ring R is a **local ring** if it contains exactly one maximal ideal.*

Commutative algebra is deeply connected with algebraic geometry. The central theme of this connection is that the algebraic properties of a ring R are reflected in the geometric properties of an associated object, such as an algebraic variety or a scheme, and vice versa.

The most classical and intuitive examples arise from polynomial rings. Let k be an algebraically closed field, and consider the ring $R = k[x_1, \ldots, x_n]$. The zero locus of a set of polynomials in R defines a geometric subset of affine n-space, $\mathbb{A}^n_k$. These subsets are the fundamental objects of study in classical algebraic geometry. In this setting, there is a beautiful correspondence: the prime ideals of $k[x_1, \ldots, x_n]$ correspond bijectively to the irreducible affine subvarieties of $\mathbb{A}^n_k$.

More generally, for any commutative ring R, one can associate a geometric space, denoted $\mathrm{Spec}(R)$, whose points are the prime ideals of R. This space, called an affine scheme, is the modern generalization of an affine variety. Since all varieties and schemes can be constructed by gluing together affine pieces, the study of commutative rings and their ideals can be viewed as the study of local algebraic geometry.

The concept of a local ring has a direct geometric interpretation. It allows us to study the geometry of a scheme in the immediate neighborhood of a point. For instance, the geometric distinctions between a smooth point, a cusp, and a node on a curve are captured algebraically by the distinct structures of their corresponding local rings. We will develop the tools to make these notions precise in the chapters to come.

5.1.2 Noetherian Rings and Modules

One property of rings that is central to both commutative algebra and algebraic geometry is the finite generation of ideals. For a polynomial ring over a field, $k[x_1, \ldots, x_n]$, the fact that every ideal is finitely generated has a profound geometric consequence: every algebraic variety in $\mathbb{A}^n$ can be realized as the intersection of a finite number of hypersurfaces. That is, the zero locus of any ideal is the zero locus of a finite subset of its elements. This finiteness condition, which is far from obvious, is captured by the concept of a Noetherian ring.

Definition 5.4. *A commutative ring R is said to be **Noetherian** if every ideal of R is finitely generated.*

An equivalent and often more practical characterization of Noetherian rings is in terms of chains of ideals.

Proposition 5.5. *A ring R is Noetherian if and only if it satisfies the **ascending chain condition** (ACC) for ideals; that is, every ascending chain of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ eventually stabilizes, meaning there exists an integer N such that $I_n = I_N$ for all $n \geq N$.*

Proof. ($\implies$) Assume R is Noetherian. Let $I_1 \subseteq I_2 \subseteq \ldots$ be an ascending chain of ideals. Consider the set $I = \bigcup_{i=1}^{\infty} I_i$. It is straightforward to verify that I is an ideal of R. Since R is Noetherian, I must be finitely generated. Let $I = (f_1, \ldots, f_m)$. Each generator f_j must belong to some ideal in the chain, say $f_j \in I_{n_j}$. Let $N = \max\{n_1, \ldots, n_m\}$. Then all generators $f_1, \ldots, f_m$ are contained in I_N. Consequently, $I = (f_1, \ldots, f_m) \subseteq I_N$. But $I_N \subseteq I$ by definition. Thus, $I_N = I$, and for any $n \geq N$, we have $I_N \subseteq I_n \subseteq I = I_N$, which implies $I_n = I_N$. The chain stabilizes.

($\impliedby$) Assume R satisfies the ACC. Let I be an ideal of R. Suppose, for the sake of contradiction, that I is not finitely generated. We can then construct an infinite, strictly ascending chain of ideals. Choose $f_1 \in I$. Since $(f_1) \neq I$, we can choose $f_2 \in I \setminus (f_1)$. Continuing this process, having chosen $f_1, \ldots, f_{n-1}$, we choose $f_n \in I \setminus (f_1, \ldots, f_{n-1})$. This gives rise to a strictly ascending chain of ideals $(f_1) \subsetneq (f_1, f_2) \subsetneq \ldots$, which contradicts the ACC. Therefore, I must be finitely generated.

□

Example 5.6. *Familiar examples of Noetherian rings include any field (which has only the ideals* (0) *and* (1)*), the ring of integers* $\mathbb{Z}$ *(as it is a principal ideal domain), and, as we shall see, polynomial rings over these.*

The property of being Noetherian is preserved under the construction of polynomial rings. This cornerstone result is due to Hilbert.

Theorem 5.7 (Hilbert Basis Theorem)**.** *If* R *is a Noetherian ring, then the polynomial ring* $R[x]$ *is also Noetherian.*

Remark 5.8. *By a straightforward induction, this theorem implies that if* R *is Noetherian, then the polynomial ring in any finite number of variables,* $R[x_1, \ldots, x_n]$*, is also Noetherian. In particular,* $k[x_1, \ldots, x_n]$ *is Noetherian for any field* k*.*

Proof. Let $I \subseteq R[x]$ be an ideal. We must show that I is finitely generated. If $I = (0)$, we are done. Otherwise, let $J \subseteq R$ be the set of leading coefficients of all polynomials in I, together with 0. It is an exercise to show that J is an ideal of R. Since R is Noetherian, J is finitely generated; let $J = (a_1, \ldots, a_m)$ where each a_i is the leading coefficient of some polynomial $f_i \in I$.

Let $d = \max\{\deg(f_1), \ldots, \deg(f_m)\}$. For each $k \in \{0, 1, \ldots, d-1\}$, let $J_k \subseteq R$ be the set of leading coefficients of all polynomials in I of degree k. Each J_k is an ideal and is thus finitely generated; let $J_k = (b_{k1}, \ldots, b_{k,m_k})$, where b_{kj} is the leading coefficient of some $g_{kj} \in I$ of degree k.

We claim that I is generated by the set $\{f_1, \ldots, f_m\} \cup \{g_{kj}\}$. Let $f \in I$ be an arbitrary polynomial of degree D. We proceed by induction on D. Let a be the leading coefficient of f. If $D \geq d$, then $a \in J$, so $a = \sum_{i=1}^{m} r_i a_i$ for some $r_i \in R$. Consider the polynomial

$$h = \sum_{i=1}^{m} r_i f_i x^{D - \deg(f_i)}.$$

This polynomial h is in the ideal generated by $\{f_1, \ldots, f_m\}$, has degree D, and its leading coefficient is $\sum r_i a_i = a$. Thus, $f - h$ is a polynomial in I of degree strictly less than D. By the inductive hypothesis, $f - h$ is in the ideal generated by our proposed set of generators, and therefore so is f. If $D < d$, a similar argument applies using the generators g_{Dj}. The leading coefficient a is in J_D, so it can be written as a combination of the b_{Dj}. We can form a polynomial h' of degree D with leading coefficient a using the g_{Dj}, and again $f - h'$ has smaller degree.

The base cases for the induction are trivial. Thus, any polynomial in I is generated by our finite set, and $R[x]$ is Noetherian. □

Corollary 5.9. *If* R *is a Noetherian ring and* S *is a finitely generated* R*-algebra, then* S *is also a Noetherian ring.*

Proof. Since S is a finitely generated R-algebra, there exists a surjective R-algebra homomorphism $\phi : R[x_1, \ldots, x_n] \to S$ for some n. By the Hilbert Basis Theorem, the ring $R[x_1, \ldots, x_n]$ is Noetherian. Let I be an ideal in S. Its preimage $\phi^{-1}(I)$ is an ideal in $R[x_1, \ldots, x_n]$ and is therefore finitely generated. The images of these generators under ϕ will then generate I. Thus, every ideal in S is finitely generated. □

The concept of the ascending chain condition can be extended from rings to modules.

Definition 5.10. *An* R*-module* M *is* ***Noetherian*** *if every submodule of* M *is finitely generated. Equivalently,* M *is Noetherian if it satisfies the ascending chain condition on submodules.*

Proposition 5.11. *If* R *is a Noetherian ring and* M *is a finitely generated* R*-module, then* M *is a Noetherian module.*

Proof. We proceed by induction on the number of generators of M. Let $\{m_1, \ldots, m_n\}$ be a set of generators for M. Base Case: $n = 1$. Then M is generated by a single element m_1. There is a surjective R-module homomorphism $\phi : R \to M$ given by $r \mapsto rm_1$. Let N be a submodule of M. Its preimage $\phi^{-1}(N)$ is a submodule of R, i.e., an ideal. Since R is a Noetherian ring, this ideal is finitely generated. The images of its generators under ϕ form a finite set of generators for N. Thus M is Noetherian.

Inductive Step: Assume the proposition holds for all modules generated by $n-1$ elements. Let M be generated by $\{m_1, \ldots, m_n\}$. Consider the submodule $M' = (m_1, \ldots, m_{n-1})$. By the inductive hypothesis, M' is a Noetherian module. Now consider the quotient module M/M'. This module is generated by the single element $\overline{m_n} = m_n + M'$, so by the base case, M/M' is Noetherian.

Let N be any submodule of M. Consider the submodule $N \cap M'$. As a submodule of the Noetherian module M', $N \cap M'$ is finitely generated. Let $\{a_1, \ldots, a_k\}$ be its generators. Consider the image of N in the quotient, $\overline{N} = (N + M')/M' \subseteq M/M'$. As a submodule of the Noetherian module M/M', $\overline{N}$ is finitely generated. Let its generators be $\{\overline{b_1}, \ldots, \overline{b_l}\}$, where $b_j \in N$.

We claim that N is generated by the set $\{a_1, \ldots, a_k, b_1, \ldots, b_l\}$. Let $x \in N$. Its image $\overline{x} \in \overline{N}$ can be written as $\overline{x} = \sum r_j \overline{b_j}$ for some $r_j \in R$. This means $x - \sum r_j b_j$ is in the kernel of the projection map, which is M'. So, $x - \sum r_j b_j \in N \cap M'$. Therefore, $x - \sum r_j b_j = \sum s_i a_i$ for some $s_i \in R$. This gives $x = \sum s_i a_i + \sum r_j b_j$, showing that x is in the submodule generated by our finite set. Thus N is finitely generated, and M is Noetherian. □

5.1.3 Graded Modules and Hilbert Functions

We now introduce algebraic structures that are fundamental to the study of projective geometry. The concept of a graded ring allows us to speak of "homogeneous" elements, which is the algebraic analogue of homogeneous polynomials that define varieties in projective space.

Definition 5.12. *A **graded ring** is a ring R that admits a direct sum decomposition into additive subgroups $R = \bigoplus_{i=0}^{\infty} R_i$ such that $R_i R_j \subseteq R_{i+j}$ for all $i, j \geq 0$. An element $f \in R$ is said to be **homogeneous** of degree i if $f \in R_i$. An ideal $I \subseteq R$ is a **homogeneous ideal** if it is generated by homogeneous elements.*

Example 5.13. *The archetypal example of a graded ring is the polynomial ring $R = k[x_0, \ldots, x_n]$. It has a **standard grading** $R = \bigoplus_{d=0}^{\infty} R_d$, where R_d is the k-vector space of homogeneous polynomials of total degree d. Here $R_0 = k$, R_1 is the space spanned by the variables $x_0, \ldots, x_n$, and so on.*

This notion extends naturally to modules.

Definition 5.14. *Let $R = \bigoplus R_i$ be a graded ring. A **graded R-module** is an R-module M with a direct sum decomposition $M = \bigoplus_{i \in \mathbb{Z}} M_i$ such that $R_i M_j \subseteq M_{i+j}$ for all i, j.*

Example 5.15. *Let $R = k[x_0, \ldots, x_n]$ with the standard grading.*

1. *If $I \subseteq R$ is a homogeneous ideal, then the quotient ring $S = R/I$ is a graded R-module. Its grading is given by $S_d = R_d/(I \cap R_d)$.*
2. *For any integer d, we can form the **twisted** module $M(d)$. As an R-module, $M(d)$ is isomorphic to M, but its grading is shifted: $M(d)_e = M_{d+e}$. This seemingly simple device is extremely powerful, as it allows multiplication by a homogeneous element of degree d to be viewed as a degree-preserving map from $M(-d)$ to M.*

The graded pieces M_s of a finitely generated graded module over a polynomial ring are finite-dimensional k-vector spaces. Their dimensions encode geometric information.

Definition 5.16. *Let M be a finitely generated graded module over the polynomial ring $R = k[x_0, \ldots, x_r]$ with its standard grading. The **Hilbert function** of M is the map $H_M : \mathbb{Z} \to \mathbb{Z}$ defined by*

$$H_M(s) := \dim_k(M_s).$$

Example 5.17. *Let $M = R = k[x_0, \dots, x_r]$ with the standard grading. The dimension of the space of homogeneous polynomials of degree s in $r+1$ variables is a classical combinatorial result:*

$$H_R(s) = \binom{s+r}{r} \quad \text{for } s \geq 0, \text{ and } H_R(s) = 0 \text{ for } s < 0.$$

Example 5.18. *Consider the module $M = k[x,y]/(x^2, y^2)$. The graded pieces are:*

- $M_0 = \text{span}_k\{1\}$, *so* $H_M(0) = 1$.
- $M_1 = \text{span}_k\{x, y\}$, *so* $H_M(1) = 2$.
- $M_2 = \text{span}_k\{xy\}$ *(since $x^2 = 0, y^2 = 0$), so* $H_M(2) = 1$.
- *For $s \geq 3$, any monomial of degree s must contain x^2 or y^2 as a factor, so $M_s = \{0\}$. Thus $H_M(s) = 0$ for $s \geq 3$.*

Remarkably, for large values of s, the Hilbert function always behaves like a polynomial.

Theorem 5.19 (Hilbert)**.** *If M is a finitely generated graded module over $k[x_0, \dots, x_r]$, then there exists a polynomial $P_M(s) \in \mathbb{Q}[s]$ of degree at most r such that $H_M(s) = P_M(s)$ for all sufficiently large integers s. This polynomial $P_M(s)$ is called the* ***Hilbert polynomial*** *of M.*

The proof relies on the following elementary lemma about functions whose differences are polynomial.

Lemma 5.20. *Let $H : \mathbb{Z}_{\geq 0} \to \mathbb{Z}$ be a function. If the difference function $\Delta H(s) = H(s) - H(s-1)$ agrees with a polynomial of degree $d-1$ for all $s \gg 0$, then $H(s)$ agrees with a polynomial of degree d for all $s \gg 0$.*

Proof of Theorem. We proceed by induction on the number of variables, $r+1$. Base case: $r = -1$. The ring is $k[x_0, \dots, x_{-1}] = k$. A finitely generated graded k-module is a finite-dimensional graded vector space $M = \bigoplus M_s$. Thus, $M_s = 0$ for $s \gg 0$, so $H_M(s) = 0$ for large s. The zero polynomial has degree $-1 \leq -1$.

Inductive step: Assume the theorem holds for polynomial rings in r variables. Let M be a finitely generated graded module over $R = k[x_0, \dots, x_r]$. Consider the homomorphism $\phi : M \to M$ given by multiplication by x_r. This is not a degree-preserving map. To remedy this, we use a twist, defining $\phi : M(-1) \to M$. This is a degree-preserving homomorphism of graded modules. Let $K = \ker(\phi)$ and $C = \text{coker}(\phi) = M/x_r M$. We have a short exact sequence of graded modules:

$$0 \to K \to M(-1) \xrightarrow{\cdot x_r} M \to C \to 0.$$

Because the dimension function is additive on exact sequences, for each degree s we have:

$$H_K(s) - H_{M(-1)}(s) + H_M(s) - H_C(s) = 0.$$

Using the definition of the twisted module, $H_{M(-1)}(s) = H_M(s-1)$, this becomes:

$$H_M(s) - H_M(s-1) = H_C(s) - H_K(s).$$

The modules K and C are both annihilated by x_r, so they are finitely generated modules over the ring $R/(x_r) \cong k[x_0, \dots, x_{r-1}]$. By the inductive hypothesis, their Hilbert functions $H_C(s)$ and $H_K(s)$ agree with polynomials of degree at most $r-1$ for large s. Therefore, their difference, $\Delta H_M(s) = H_M(s) - H_M(s-1)$, also agrees with a polynomial of degree at most $r-1$ for large s. By the lemma, $H_M(s)$ must agree with a polynomial of degree at most r for large s. □

Remark 5.21 (Geometric Interpretation)**.** *The Hilbert polynomial of the homogeneous coordinate ring $S(X) = k[x_0, \dots, x_r]/I(X)$ of a projective variety $X \subseteq \mathbb{P}^r$ contains a wealth of geometric information.*

- *The* ***degree*** *of the Hilbert polynomial $P_X(s)$ is equal to the* ***dimension*** *of the variety X.*
- *If $\dim(X) = d$, the leading term of $P_X(s)$ is $\frac{\deg(X)}{d!} s^d$. The integer $\deg(X)$ is the* ***degree*** *of the variety, which geometrically corresponds to the number of intersection points with a generic linear subspace of complementary dimension.*

- *The celebrated **Riemann-Roch theorem** for curves and its generalizations to higher dimensions provide powerful tools for computing the Hilbert polynomial, connecting it to intrinsic geometric invariants of the variety.*
- *In modern algebraic geometry, the coefficients of the Hilbert polynomial are related to the **Chern classes** of the coherent sheaf associated with the module, providing a bridge to algebraic topology.*

5.1.4 Localization

Many questions in commutative algebra and algebraic geometry are "local" in nature, meaning they can be understood by studying the structure of a ring or module in an infinitesimal neighborhood of a point (or more accurately, a prime ideal). The algebraic tool for this is **localization**, a process that simplifies a ring by focusing on a single prime ideal. The resulting ring, a "local ring," has a unique maximal ideal, making its ideal structure much more transparent.

The fundamental idea of localization is to formally adjoin multiplicative inverses for a chosen subset of elements of a ring, in much the same way that the rational numbers $\mathbb{Q}$ are constructed from the integers $\mathbb{Z}$ by adjoining inverses for all non-zero elements.

The first question to address is which elements we can sensibly adjoin inverses for. If we adjoin f^{-1} and g^{-1}, to maintain a ring structure we must also include their product, $(fg)^{-1}$. This leads to the requirement that the set of elements whose inverses we introduce must be closed under multiplication.

Definition 5.22. *A subset $U \subseteq R$ of a ring R is said to be **multiplicatively closed** if $1 \in U$ and for any $s, t \in U$, their product st is also in U.*

Example 5.23.

1. *For any non-zero element $t \in R$, the set $\{1, t, t^2, \dots\}$ is multiplicatively closed.*
2. *If $P \subseteq R$ is an ideal, the complement $R \setminus P$ is multiplicatively closed if and only if P is a prime ideal.*
3. *The set of all non-zero elements, $R \setminus \{0\}$, is multiplicatively closed if and only if R is an integral domain.*

We can now formally define the ring of fractions.

Definition 5.24. *Let R be a ring, $U \subseteq R$ a multiplicatively closed subset, and M an R-module. The **localization of M with respect to U**, denoted $U^{-1}M$ or $M[U^{-1}]$, is the set of equivalence classes of pairs (m, u) with $m \in M$ and $u \in U$. We write such a class as $\frac{m}{u}$. The equivalence relation is defined by:*

$$\frac{m}{u} \sim \frac{m'}{u'} \iff \exists v \in U \text{ such that } v(u'm - um') = 0 \text{ in } M.$$

The set $U^{-1}M$ forms an R-module with addition $\frac{m}{u} + \frac{m'}{u'} = \frac{u'm+um'}{uu'}$ and scalar multiplication $r \cdot \frac{m}{u} = \frac{rm}{u}$. When $M = R$, the set $U^{-1}R$ is a ring with multiplication $\frac{r}{u}\frac{r'}{u'} = \frac{rr'}{uu'}$, and $U^{-1}M$ is naturally a $U^{-1}R$-module.

Remark 5.25. *The element v in the equivalence relation is crucial for handling torsion. If $um = 0$ for some $u \in U$, then $\frac{m}{1} = \frac{um}{u} = \frac{0}{u}$, so $\frac{m}{1}$ is equivalent to the zero element in $U^{-1}M$.*

Example 5.26.

1. *If R is an integral domain, localizing at the set $U = R \setminus \{0\}$ yields the **field of fractions** of R, denoted $K(R)$.*
2. *If $P \subseteq R$ is a prime ideal, we localize at the multiplicatively closed set $U = R \setminus P$. The resulting ring is denoted R_P, and for an R-module M, the localization is M_P. The ring R_P is a **local ring**; its unique maximal ideal consists of the fractions $\frac{a}{b}$ where $a \in P$ and $b \notin P$.*

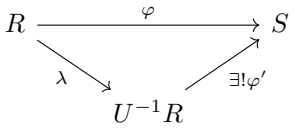
Localization is not merely a construction; it is a well-behaved operation that respects the structure of module homomorphisms.

Proposition 5.27. *Localization is an exact functor from the category of R-modules to the category of $U^{-1}R$-modules.*

Proof Sketch. Given an R-module homomorphism $\varphi : M \to N$, there is an induced $U^{-1}R$-module homomorphism $\varphi[U^{-1}] : U^{-1}M \to U^{-1}N$ defined by $\frac{m}{u} \mapsto \frac{\varphi(m)}{u}$. One can verify that this respects composition, making localization a functor. The key property is that this functor is exact: it transforms short exact sequences of R-modules into short exact sequences of $U^{-1}R$-modules. □

Localization is also characterized by a universal property, which states that it is the "most efficient" way to make the elements of U into units.

Proposition 5.28 (Universal Property of Localization)**.** *Let $U \subseteq R$ be a multiplicatively closed set and let $\lambda : R \to U^{-1}R$ be the natural ring homomorphism $r \mapsto \frac{r}{1}$. For any ring homomorphism $\varphi : R \to S$ such that $\varphi(u)$ is a unit in S for all $u \in U$, there exists a unique ring homomorphism $\varphi' : U^{-1}R \to S$ such that $\varphi = \varphi' \circ \lambda$.*



There is a close relationship between the ideals of a ring R and its localization $U^{-1}R$.

Proposition 5.29. *There is a one-to-one, inclusion-preserving correspondence between the prime ideals of $U^{-1}R$ and the prime ideals of R that do not intersect U. The correspondence is given by $I \mapsto \lambda^{-1}(I)$ for a prime ideal $I \subseteq U^{-1}R$, and $P \mapsto U^{-1}P$ for a prime ideal $P \subseteq R$ with $P \cap U = \emptyset$.*

Example 5.30. *If $P \subseteq R$ is a prime ideal, the prime ideals of the local ring R_P are in one-to-one correspondence with the prime ideals of R that are contained in P. This is a key reason why localization simplifies the ideal structure so effectively.*

Remark 5.31. *This correspondence should be compared with the ideal structure of a quotient ring: the prime ideals of R/I correspond to the prime ideals of R that contain I. Localization and quotienting are thus dual operations in their effect on the spectrum of prime ideals.*

Corollary 5.32. *If R is a Noetherian ring, then any localization $U^{-1}R$ is also Noetherian.*

Proof. Let I be an ideal in $U^{-1}R$. Let $J = \lambda^{-1}(I)$ be its contraction in R. Since R is Noetherian, J is finitely generated, say $J = (r_1, \ldots, r_n)$. We claim that I is generated by $\{\frac{r_1}{1}, \ldots, \frac{r_n}{1}\}$. Indeed, any element of I is of the form $\frac{r}{u}$ where $r \in J$. Then $r = \sum c_i r_i$ for $c_i \in R$, so $\frac{r}{u} = \sum \frac{c_i}{u}\frac{r_i}{1}$, which shows that the image of the generators of J generate I. □

5.1.5 Hom and Tensor

Definition 5.33. *Let M and N be modules over a ring R. The set of all R-module homomorphisms from M to N is denoted by $Hom_R(M, N)$. This set forms an R-module under pointwise addition and scalar multiplication of functions.*

Example 5.34. *For any R-module N, we have an isomorphism $Hom_R(R, N) \cong N$. More generally, for a free module, we have $Hom_R\left(\bigoplus_{i=1}^n R, N\right) \cong \bigoplus_{i=1}^n Hom_R(R, N) \cong N^n$.*

The Hom construction is functorial in each of its arguments.

- For a fixed R-module M, $\mathrm{Hom}_R(M, -)$ is a **covariant functor**. A homomorphism $\psi : A \to B$ induces a homomorphism $\psi_* : \mathrm{Hom}_R(M, A) \to \mathrm{Hom}_R(M, B)$ by post-composition: $f \mapsto \psi \circ f$. This functor is **left-exact**: an exact sequence $0 \to A \to B \to C$ induces an exact sequence $0 \to \mathrm{Hom}_R(M, A) \to \mathrm{Hom}_R(M, B) \to \mathrm{Hom}_R(M, C)$.

- For a fixed R-module M, $\mathrm{Hom}_R(-, M)$ is a **contravariant functor**. A homomorphism $\psi : A \to B$ induces a homomorphism $\psi^* : \mathrm{Hom}_R(B, M) \to \mathrm{Hom}_R(A, M)$ by pre-composition: $f \mapsto f \circ \psi$. This functor is also left-exact, which for a contravariant functor means that an exact sequence $A \to B \to C \to 0$ induces an exact sequence $0 \to \mathrm{Hom}_R(C, M) \to \mathrm{Hom}_R(B, M) \to \mathrm{Hom}_R(A, M)$.

Definition 5.35. *Let M and N be modules over a ring R. The **tensor product** of M and N over R, denoted $M \otimes_R N$, is the R-module generated by symbols of the form $m \otimes n$ (for $m \in M, n \in N$), subject to the following relations for all $m, m' \in M$, $n, n' \in N$, and $r \in R$:*

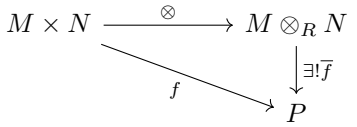
- $(m + m') \otimes n = m \otimes n + m' \otimes n$
- $m \otimes (n + n') = m \otimes n + m \otimes n'$
- $(rm) \otimes n = r(m \otimes n) = m \otimes (rn)$

Remark 5.36. *An arbitrary element of $M \otimes_R N$ is a finite sum of "simple tensors," $\sum_i m_i \otimes n_i$. It is a notoriously difficult problem in general to determine if a given element is zero or to find the minimal number of simple tensors needed to write it. This latter question is related to the notion of tensor rank.*

Example 5.37.
1. *For any R-module M, we have $R \otimes_R M \cong M$.*
2. *$R[x_1, \ldots, x_m] \otimes_R R[y_1, \ldots, y_n] \cong R[x_1, \ldots, x_m, y_1, \ldots, y_n]$.*
3. *$\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}[x] \cong \mathbb{Q}[x]$.*
4. *For ideals $I, J \subseteq R$, we have $R/I \otimes_R R/J \cong R/(I + J)$.*
5. *If S is an R-algebra and M is an R-module, then $S \otimes_R M$ becomes an S-module via scalar extension: $s(t \otimes m) = (st) \otimes m$.*

The tensor product is also characterized by a universal property, which formalizes the idea that it is the most general construction preserving bilinearity.

Proposition 5.38 (Universal Property of the Tensor Product)**.** *The canonical map $\otimes : M \times N \to M \otimes_R N$ is R-bilinear. Furthermore, for any R-module P and any R-bilinear map $f : M \times N \to P$, there exists a unique R-module homomorphism $\overline{f} : M \otimes_R N \to P$ such that $f = \overline{f} \circ \otimes$.*



The tensor product is a covariant functor in both arguments and is **right-exact**. An exact sequence $A \to B \to C \to 0$ induces an exact sequence $A \otimes_R M \to B \otimes_R M \to C \otimes_R M \to 0$.

Remark 5.39 (Geometric Context)**.** *If R and S are coordinate rings of affine varieties X and Y over an algebraically closed field, then $R \otimes_k S$ is the coordinate ring of the product variety $X \times Y$.*

The process of localization can be elegantly reformulated using the tensor product.

Lemma 5.40. *Let $U \subseteq R$ be a multiplicatively closed set. For any R-module M, there is a canonical isomorphism of $U^{-1}R$-modules:*

$$U^{-1}R \otimes_R M \xrightarrow{\cong} U^{-1}M$$

given by the map $\frac{r}{u} \otimes m \mapsto \frac{rm}{u}$.

Proof. We construct the inverse map $\varphi : U^{-1}M \to U^{-1}R \otimes_R M$ by defining $\varphi(\frac{m}{u}) = \frac{1}{u} \otimes m$. To see this is well-defined, suppose $\frac{m}{u} = \frac{m'}{u'}$. Then there exists $v \in U$ such that $v(u'm - um') = 0$. In the tensor product, this implies $v(u'm - um') \otimes 1 = 0$. Using the tensor relations, we have $1 \otimes v(u'm - um') = 0$, so $\frac{1}{uu'v} \otimes v(u'm - um') = 0$. This leads to $\frac{u'v}{uu'v} \otimes m - \frac{uv}{uu'v} \otimes m' = 0$, which simplifies to $\frac{1}{u} \otimes m = \frac{1}{u'} \otimes m'$. The map is thus well-defined. It is routine to check that it is the inverse of the given map. □

This formulation immediately tells us that localization is right-exact. In fact, it is exact, a property known as flatness.

Definition 5.41. *An R-module F is **flat** if the functor $- \otimes_R F$ is exact. This is equivalent to requiring that for every injective R-module map $M \to N$, the induced map $M \otimes_R F \to N \otimes_R F$ is also injective.*

Proposition 5.42. *For any multiplicatively closed set $U \subseteq R$, the localized ring $U^{-1}R$ is a flat R-module.*

Proof. Let $\varphi : M' \to M$ be an injective map of R-modules. We must show that the induced map $\varphi[U^{-1}] : M'[U^{-1}] \to M[U^{-1}]$ is injective. Suppose an element $\frac{m'}{u} \in M'[U^{-1}]$ is in the kernel. Then $\frac{\varphi(m')}{u} = 0$ in $M[U^{-1}]$. By definition of localization, this means there exists some $v \in U$ such that $v\varphi(m') = 0$ in M. Since φ is a homomorphism, this is $\varphi(vm') = 0$. As φ is injective, we must have $vm' = 0$. But this implies that $\frac{m'}{u} = \frac{vm'}{vu} = \frac{0}{vu} = 0$ in $M'[U^{-1}]$. Thus, the kernel is trivial and the map is injective. □

The power of localization lies in its ability to translate properties of a module into properties of its localizations at prime (or maximal) ideals. A property that holds for a module if and only if it holds for all its localizations is called a "local property."

Lemma 5.43. *Let M be an R-module. The following are equivalent:*

1. *$M = 0$.*
2. *$M_P = 0$ for all prime ideals $P \subseteq R$.*
3. *$M_m = 0$ for all maximal ideals $m \subseteq R$.*

Proof. The implications (1) $\implies$ (2) $\implies$ (3) are clear. For (3) $\implies$ (1), suppose $M \neq 0$ and let $a \in M$ be a non-zero element. The annihilator of a, $\mathrm{Ann}(a) = \{r \in R \mid ra = 0\}$, is a proper ideal of R. Therefore, it is contained in some maximal ideal m. We claim that $\frac{a}{1} \neq 0$ in M_m. If $\frac{a}{1} = 0$, then there would exist some $u \in R \setminus m$ such that $ua = 0$. But this means $u \in \mathrm{Ann}(a) \subseteq m$, which is a contradiction. Thus $M_m \neq 0$. □

Corollary 5.44. *A homomorphism of R-modules $\varphi : M \to N$ is injective (resp. surjective, an isomorphism) if and only if the induced map on localizations $\varphi_m : M_m \to N_m$ is injective (resp. surjective, an isomorphism) for all maximal ideals $m \subseteq R$.*

Proof. Consider the kernel, $K = \ker(\varphi)$. The sequence $0 \to K \to M \to N$ is exact. Since localization is an exact functor, the sequence $0 \to K_m \to M_m \to N_m$ is also exact for any maximal ideal m. Thus, $K_m = \ker(\varphi_m)$. Now, φ is injective if and only if $K = 0$. By the preceding lemma, this is true if and only if $K_m = 0$ for all m, which is true if and only if φ_m is injective for all m. A similar argument applied to the cokernel proves the statement for surjectivity. □

5.2 Ideals and Spectrum

5.2.1 Radical Ideals

The relationship between prime ideals and localization leads to a fundamental characterization of the set of elements in an ideal that have a power lying in the ideal.

Definition 5.45. *Let I be an ideal in a ring R. The **radical** of I, denoted $\sqrt{I}$ or $\mathrm{rad}(I)$, is the set $\{f \in R \mid f^n \in I \text{ for some integer } n > 0\}$. The radical of the zero ideal, $\sqrt{(0)}$, is the set of all nilpotent elements of R and is called the **nilradical**. An ideal I is a **radical ideal** if $I = \sqrt{I}$.*

It is not immediately obvious that $\sqrt{I}$ is an ideal. The following result provides a beautiful characterization that makes this clear.

Theorem 5.46. *For any ideal $I \subseteq R$, its radical is the intersection of all prime ideals containing it:*

$$\sqrt{I} = \bigcap_{P \supseteq I, P \text{ prime}} P.$$

Proof. ($\subseteq$) Let $f \in \sqrt{I}$. Then $f^n \in I$ for some n. If P is any prime ideal containing I, then $f^n \in P$. Since P is prime, this implies $f \in P$. As this holds for all such primes, f is in their intersection.

($\supseteq$) Suppose f is in the intersection of all primes containing I. Assume, for contradiction, that $f \notin \sqrt{I}$. This means that no power of f lies in I. The set $U = \{1, f, f^2, \dots\}$ is a multiplicatively closed set that does not intersect I (i.e., $I \cap U = \emptyset$). By a standard result using Zorn's Lemma, there exists an ideal P that is maximal with respect to the property of containing I and being disjoint from U. Such an ideal must be prime. But this prime ideal P contains I and does not contain f, which contradicts our assumption that f was in the intersection of all such primes. □

Corollary 5.47. *The nilradical of a ring R is the intersection of all prime ideals of R.*

Definition 5.48. *A ring R is **reduced** if it has no non-zero nilpotent elements, i.e., if its nilradical is the zero ideal.*

Example 5.49. *The ring $k[x]/(x^2)$ is not reduced, as the class of x is a non-zero nilpotent element. Its nilradical is the ideal generated by x.*

Remark 5.50. *The nilradical itself is not always a prime ideal. For example, in the ring $\mathbb{Z}/12\mathbb{Z}$, the nilpotent elements are $\overline{0}$ and $\overline{6}$. The nilradical is $(\overline{6})$, which is not a prime ideal since $2 \cdot 3 \in (\overline{6})$ but neither 2 nor 3 are in $(\overline{6})$.*

5.2.2 The Spectrum of a Ring

A central idea in modern algebraic geometry, pioneered by Grothendieck, is that a commutative ring can be viewed as a geometric object. This is achieved by associating to each ring a topological space whose points are the prime ideals of the ring. This construction, known as the spectrum, provides a rich geometric language for studying commutative algebra.

Definition 5.51. *Let R be a commutative ring. The **spectrum** of R, denoted $Spec(R)$, is the set of all prime ideals of R.*

To endow this set with a geometric structure, we define a topology.

Definition 5.52. *The **Zariski topology** on $Spec(R)$ is defined by specifying its closed sets. For any subset of elements $I \subseteq R$, we define the set*

$$V(I) := \{P \in Spec(R) \mid I \subseteq P\}.$$

The sets $V(I)$ are the closed sets of the Zariski topology.

Remark 5.53. *Note that $V(I) = V(\langle I \rangle)$, where $\langle I \rangle$ is the ideal generated by I. Thus, we may restrict our attention to ideals when defining closed sets. Furthermore, since an ideal is contained in a prime ideal if and only if its radical is, we have $V(I) = V(\sqrt{I})$.*

We must verify that this definition indeed satisfies the axioms for a topology.

Proposition 5.54. *The sets $V(I)$ form the closed sets of a topology on $Spec(R)$.*

1. *For any collection of ideals $\{I_\lambda\}_{\lambda \in \Lambda}$, we have $\bigcap_\lambda V(I_\lambda) = V\left(\sum_\lambda I_\lambda\right)$.*
2. *For any two ideals I, J, we have $V(I) \cup V(J) = V(I \cap J) = V(IJ)$.*

Proof. The empty set and the whole space are closed, as $V(R) = \emptyset$ and $V((0)) = \mathrm{Spec}(R)$.

1. A prime ideal P is in $\bigcap_\lambda V(I_\lambda)$ if and only if $I_\lambda \subseteq P$ for all λ. This is equivalent to the condition that the ideal generated by the union, $\sum_\lambda I_\lambda$, is contained in P. This, in turn, is equivalent to $P \in V(\sum_\lambda I_\lambda)$.
2. We have the inclusions $IJ \subseteq I \cap J \subseteq I$ and $I \cap J \subseteq J$. These imply the inclusions of closed sets $V(I) \subseteq V(I \cap J) \subseteq V(IJ)$ and $V(J) \subseteq V(I \cap J)$. Thus, $V(I) \cup V(J) \subseteq V(I \cap J) \subseteq V(IJ)$. For the reverse inclusion, suppose $P \in V(IJ)$, so $IJ \subseteq P$. Since P is prime, this implies $I \subseteq P$ or $J \subseteq P$. Therefore, $P \in V(I)$ or $P \in V(J)$, which means $P \in V(I) \cup V(J)$. Thus, $V(IJ) \subseteq V(I) \cup V(J)$.

□

In this topology, a point $\{P\}$ is closed if and only if P is a maximal ideal. The subset of maximal ideals, denoted $\mathrm{mSpec}(R)$, often corresponds to the classical geometric points of a variety.

Example 5.55. *1. Let $R = k[x]$ where k is an algebraically closed field. The prime ideals are of two types: the zero ideal (0), and maximal ideals of the form $(x - a)$ for $a \in k$. Thus, $Spec(k[x]) = \{(x-a) \mid a \in k\} \cup \{(0)\}$. The set of maximal ideals, $mSpec(k[x])$, is in one-to-one correspondence with the points of the affine line $\mathbb{A}^1_k$. The point (0) is not closed; its closure is the entire space.*

2. Let $R = k[x, y]$ where k is algebraically closed. By Hilbert's Nullstellensatz, the maximal ideals are of the form $(x - a, y - b)$ for $(a, b) \in k^2$. These closed points of $Spec(k[x, y])$ are in bijection with the points of the affine plane $\mathbb{A}^2_k$. The non-maximal prime ideals correspond to irreducible subvarieties of dimension one (i.e., irreducible curves), such as $(f(x, y))$ for an irreducible polynomial f, and the zero ideal (0).

Remark 5.56. *More generally, for an algebraically closed field k, we define affine n-space as $\mathbb{A}^n_k = Spec(k[x_1, \ldots, x_n])$.*

The construction of the spectrum is functorial.

Definition 5.57. *The operation Spec is a **contravariant functor** from the category of commutative rings to the category of topological spaces. A ring homomorphism $\varphi : R \to S$ induces a continuous map $Spec(\varphi) : Spec(S) \to Spec(R)$ defined by $P \mapsto \varphi^{-1}(P)$ for any prime ideal $P \in Spec(S)$.*

Proposition 5.58. *The induced map $Spec(\varphi)$ is continuous.*

Proof. To show continuity, we must show that the preimage of any closed set in $\mathrm{Spec}(R)$ is a closed set in $\mathrm{Spec}(S)$. Let $V(I)$ be a closed set in $\mathrm{Spec}(R)$ for some ideal $I \subseteq R$. We compute its preimage:

$$\begin{aligned}(\mathrm{Spec}(\varphi))^{-1}(V(I)) &= \{P \in \mathrm{Spec}(S) \mid \mathrm{Spec}(\varphi)(P) \in V(I)\} \\ &= \{P \in \mathrm{Spec}(S) \mid \varphi^{-1}(P) \supseteq I\} \\ &= \{P \in \mathrm{Spec}(S) \mid P \supseteq \varphi(I)\} \\ &= V(\varphi(I)S)\end{aligned}$$

where $\varphi(I)S$ is the ideal in S generated by the image of I. This is a closed set in $\mathrm{Spec}(S)$, so the map is continuous. □

5.2.3 Connection to Quotients and Localizations

The functorial nature of Spec provides a geometric interpretation for the algebraic operations of quotienting and localizing a ring.

Proposition 5.59. *1. The natural projection $R \to R/I$ induces a map $Spec(R/I) \to Spec(R)$ which is a homeomorphism onto the closed subset $V(I) \subseteq Spec(R)$.*

2. The natural map $R \to U^{-1}R$ induces a map $Spec(U^{-1}R) \to Spec(R)$ which is a homeomorphism onto the subset $Y = \{P \in Spec(R) \mid P \cap U = \emptyset\}$. This subset Y is an open set in $Spec(R)$ if U is finitely generated.

Proof. The proofs of these statements follow directly from the correspondence between prime ideals established in the study of quotient rings and localizations. The induced maps are bijections onto their respective images. One must then verify that they are homeomorphisms, which is a standard exercise. □

6 Rings and Modules II

6.1 Associated Primes and Primary Decomposition

6.1.1 Module Length

In the study of modules over a ring R, finiteness conditions provide crucial structural insights. The ascending chain condition (ACC), which defines Noetherian modules, is central to the theory of finitely generated modules. We now turn our attention to its dual notion, the descending chain condition (DCC), which leads to the definition of Artinian modules and the powerful concept of module length.

Definition 6.1. *Let M be an R-module. We say that M is **Artinian** if every strictly decreasing chain of submodules of M terminates. That is, for any sequence of submodules $M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \dots$, there exists an integer $n \geq 0$ such that $M_n = M_{n+1} = \dots$. A ring R is Artinian if it is Artinian as a module over itself.*

While the definitions of Artinian and Noetherian modules are dual, their consequences are not. A surprising result, which we will prove, is that any Artinian ring is necessarily Noetherian. To establish this and other structural properties, we first introduce a way to measure the "size" of a module.

Definition 6.2. *A **chain of submodules** of an R-module M is a sequence $M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n = \{0\}$. If all inclusions are strict, i.e., $M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n$, the chain is said to have **length** n.*

The most important chains are those that cannot be refined.

Definition 6.3. *A chain $M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = \{0\}$ is a **composition series** if each quotient module M_j/M_{j+1} for $j = 0, \dots, n-1$ is a nonzero **simple module**. A module S is simple if its only submodules are $\{0\}$ and S.*

Equivalently, a composition series is a maximal chain of submodules; it is impossible to insert a new submodule strictly between M_j and M_{j+1} for any j.

Remark 6.4 (Structure of Simple Modules)**.** *Let S be a simple R-module. For any nonzero element $a \in S$, the submodule Ra must be equal to S. This induces a surjective R-module homomorphism $\phi : R \to S$ given by $r \mapsto ra$. The kernel of this map is the annihilator of S, $ann(S) := \{r \in R \mid rS = \{0\}\}$. By the First Isomorphism Theorem for modules, $S \cong R/ann(S)$. Since S is simple, the ideal $ann(S)$ must be a maximal ideal of R. Consequently, each factor M_j/M_{j+1} in a composition series is isomorphic to R/P_j for some maximal ideal P_j of R.*

Definition 6.5. *The **length** of an R-module M, denoted $\ell(M)$, is the length of a composition series for M. If M does not possess a finite composition series, its length is defined to be ∞.*

This definition presumes that if a module has a finite composition series, then all such series have the same length. This is a non-trivial fact, established by the Jordan-Hölder theorem. The following theorem and its proof will substantiate this claim.

Theorem 6.6. *An R-module M has a finite composition series if and only if M is both Artinian and Noetherian.*

Proof. ($\Leftarrow$) Suppose M is both Artinian and Noetherian. We construct a composition series as follows. If $M = \{0\}$, the series is trivial. If $M \neq \{0\}$, the set of proper submodules of M is non-empty. Since M is Noetherian, this set contains a maximal element, say M_1. By construction, M/M_1 is a simple module. If $M_1 \neq \{0\}$, we repeat the argument. Since M_1 is a submodule of a Noetherian module, it is also Noetherian. Thus, we can find a maximal proper submodule $M_2 \subsetneq M_1$. This process generates a strictly decreasing chain of submodules:

$$M \supsetneq M_1 \supsetneq M_2 \supsetneq \dots$$

Since M is Artinian, this chain must terminate after a finite number of steps, say at $M_n = \{0\}$. The resulting chain $M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = \{0\}$ is a finite composition series, as each factor M_j/M_{j+1} is simple by construction.

($\Rightarrow$) Suppose M has a finite composition series. We will prove the stronger statement that all composition series for M have the same length, and that any chain of submodules can be refined to a composition series of that length. This will imply that any strictly increasing or decreasing chain must be finite, hence M is Noetherian and Artinian.

Lemma 6.7 (Jordan-Hölder Theorem for Modules)**.** *Let M be an R-module with a finite composition series of length n. Then:*

1. *Any other composition series for M also has length n.*
2. *Any strictly decreasing chain of submodules of M has length at most n.*

Proof of Lemma. We prove both statements by induction on $n = \ell(M)$.

Base Case: If $n = 0$, then $M = \{0\}$, and the only chain has length 0. If $n = 1$, then M is a simple module. The only composition series is $M \supsetneq \{0\}$, of length 1. Any other strictly decreasing chain must be a sub-chain of this, so it has length at most 1. The claims hold.

Inductive Step: Assume the lemma holds for all modules of length less than n. Let M have a composition series $\mathcal{M} : M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = \{0\}$. Let $\mathcal{N} : M = N_0 \supsetneq N_1 \supsetneq \cdots \supsetneq N_k = \{0\}$ be another composition series for M. We want to show $k = n$.

If $M_1 = N_1$, then $M_1 \supsetneq M_2 \supsetneq \dots$ and $N_1 \supsetneq N_2 \supsetneq \dots$ are both composition series for the module M_1. Since $\ell(M_1) = n - 1 < n$, the inductive hypothesis applies to M_1. Thus, $k - 1 = n - 1$, which implies $k = n$.

If $M_1 \neq N_1$, consider the submodule $M_1 + N_1$. Since M_1 and N_1 are distinct maximal submodules of M, their sum must be M itself. Let $K = M_1 \cap N_1$. By the Second Isomorphism Theorem for modules:

$$M/M_1 = (M_1 + N_1)/M_1 \cong N_1/(M_1 \cap N_1) = N_1/K$$

$$M/N_1 = (M_1 + N_1)/N_1 \cong M_1/(M_1 \cap N_1) = M_1/K$$

Since M/M_1 and M/N_1 are simple, so are M_1/K and N_1/K. This means that K is a maximal submodule of both M_1 and N_1.

Let $\mathcal{K} : K = K_0 \supsetneq K_1 \supsetneq \cdots \supsetneq K_p = \{0\}$ be a composition series for K. Then we can form two new composition series for M:

1. $\mathcal{M}' : M \supsetneq M_1 \supsetneq K \supsetneq K_1 \supsetneq \cdots \supsetneq \{0\}$
2. $\mathcal{N}' : M \supsetneq N_1 \supsetneq K \supsetneq K_1 \supsetneq \cdots \supsetneq \{0\}$

The length of $\mathcal{M}'$ is $2 + p$, and the length of $\mathcal{N}'$ is $2 + p$. Now compare the original series $\mathcal{M}$ with $\mathcal{N}'$. Both are composition series for M starting with a different second term. But we can view them as composition series for M_1 and N_1 respectively:

- $M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_n = \{0\}$ is a series for M_1 of length $n - 1$.
- $M_1 \supsetneq K \supsetneq K_1 \supsetneq \cdots \supsetneq \{0\}$ is another series for M_1 of length $1 + p$.

Since $\ell(M_1) = n - 1 < n$, the inductive hypothesis applies to M_1, so any two composition series for M_1 have the same length. Thus, $n - 1 = 1 + p$. Similarly, by applying the inductive hypothesis to N_1 (which has length $k - 1$), we find that $k - 1 = 1 + p$. Therefore, $n - 1 = k - 1$, which implies $n = k$. This proves statement (1).

For statement (2), let $L : M = L_0 \supsetneq L_1 \supsetneq \cdots \supsetneq L_k = \{0\}$ be any strict chain. If this chain is not a composition series, it is because at least one quotient L_i/L_{i+1} is not simple. This means there exists a submodule N such that $L_i \supsetneq N \supsetneq L_{i+1}$. We can insert N into the chain to make it longer. We can continue this refinement process. Since $\ell(M) = n$ is finite, this refinement process must terminate. It terminates precisely when all successive quotients are simple, at which point we have a composition series. The length of this refined series must be n. Since the original chain had length k and was strictly shorter than its

refinement, we must have $k < n$. If the original chain was already a composition series, then $k = n$. In all cases, $k \leq n$.

This concludes the proof of the lemma. □

The lemma directly implies that if M has a finite composition series, any strictly increasing or decreasing chain of submodules must be finite. Therefore, M is both Noetherian and Artinian. This completes the proof of Theorem 6.6. □

We now specialize to the case of rings. When a ring R is viewed as an R-module, its submodules are precisely its ideals. The results of the previous section thus apply directly. For rings, however, the Artinian condition has remarkably strong consequences, leading to a complete and elegant structural characterization.

Theorem 6.8. *Let R be a commutative ring with unity. The following conditions are equivalent:*

1. *R is Noetherian and every prime ideal of R is maximal.*
2. *R has finite length as an R-module.*
3. *R is an Artinian ring.*

Moreover, if these conditions hold, then R has only a finite number of maximal ideals.

Proof. We prove the cycle of implications (1) $\implies$ (2) $\implies$ (3) $\implies$ (1).

(1) $\implies$ (2)**:** Assume R is Noetherian and every prime ideal is maximal. Suppose for contradiction that R does not have finite length. Since R is Noetherian, the set Σ of ideals $I \subset R$ for which the module R/I does not have finite length is non-empty (as $(0) \in \Sigma$). By the ACC, Σ has a maximal element, say I_0. We claim I_0 is prime.

Let $a, b \in R$ with $ab \in I_0$. Assume $a \notin I_0$ and $b \notin I_0$. Consider the ideal $I_0 + (a)$. Since $a \notin I_0$, we have $I_0 \subsetneq I_0 + (a)$. By the maximality of I_0 in Σ, the quotient module $R/(I_0 + (a))$ must have finite length. Consider the short exact sequence of R-modules:

$$0 \to \frac{I_0 + (a)}{I_0} \to \frac{R}{I_0} \to \frac{R}{I_0 + (a)} \to 0$$

The length of a module is additive over short exact sequences. If both $\frac{I_0+(a)}{I_0}$ and $\frac{R}{I_0+(a)}$ have finite length, then so does $\frac{R}{I_0}$. We know $\ell(R/(I_0 + (a))) < \infty$. Now consider the first term. There is an isomorphism of R-modules:

$$\frac{I_0 + (a)}{I_0} \cong \frac{R}{(I_0 : a)}$$

given by the map $\bar{x} \mapsto \overline{xa}$. This map is well-defined and injective because $x \in (I_0 : a) \iff xa \in I_0$. It is surjective by definition. Since $b \notin I_0$ and $ab \in I_0$, we have $b \in (I_0 : a)$. This shows that $I_0 \subsetneq (I_0 : a)$. By the maximality of I_0 in Σ, the module $R/(I_0 : a)$ must have finite length. Consequently, $\frac{I_0+(a)}{I_0}$ has finite length. From the exact sequence, it follows that R/I_0 must have finite length, which contradicts the definition of I_0. Thus, our assumption must be false: either $a \in I_0$ or $b \in I_0$. This proves I_0 is a prime ideal.

By our hypothesis (1), every prime ideal is maximal. So I_0 is a maximal ideal. But if I_0 is maximal, then R/I_0 is a field. A field is a simple R-module, so it has a composition series $R/I_0 \supsetneq \{0\}$ of length 1. This contradicts that R/I_0 does not have finite length. Therefore, the set Σ must be empty, which means $R = R/(0)$ has finite length.

(2) $\implies$ (3)**:** If R has finite length as an R-module, then by Theorem 6.6, R is both Artinian and Noetherian as a module over itself. In particular, R is an Artinian ring.

(3) $\implies$ (1)**:** Assume R is an Artinian ring. First, we show that (0) is a product of maximal ideals. Let $\mathcal{S}$ be the set of all ideals that can be written as a finite product of maximal ideals. Since R has maximal ideals (by Zorn's lemma), $\mathcal{S}$ is non-empty. Since R is Artinian, the set $\mathcal{S}$ must have a minimal element under

inclusion, say $J = \mathfrak{m}_1 \dots \mathfrak{m}_k$. We claim $J = \{0\}$. For any maximal ideal $\mathfrak{m}$ of R, the ideal $\mathfrak{m}J$ is also a product of maximal ideals. Since $\mathfrak{m}J \subseteq J$, by the minimality of J, we must have $\mathfrak{m}J = J$. This implies that J is contained in every maximal ideal $\mathfrak{m}$ of R. Thus J is contained in the Jacobson radical $J(R)$ of R. Since $J = \mathfrak{m}J$ for any maximal ideal, we have $J = J(R)J$. Now we show $J = \{0\}$. Suppose $J \neq \{0\}$. Consider the set of ideals $\{I \subseteq R \mid IJ \neq \{0\}\}$. This set is non-empty (it contains R) and thus has a minimal element I_0 because R is Artinian. Since $I_0 J \neq \{0\}$, there must be an element $f \in I_0$ such that $fJ \neq \{0\}$. The ideal (f) is contained in I_0, so $(f)J \neq \{0\}$. By minimality of I_0, we must have $(f) = I_0$. Now, since $I_0 J = I_0$, we have $(f)J = (f)$. This means there exists an element $g \in J$ such that $f = fg$. This can be rewritten as $f(1-g) = 0$. Since $g \in J \subseteq J(R)$, the element $1-g$ is a unit in R. (If u is not a unit, it is contained in some maximal ideal $\mathfrak{m}$. But if $g \in J(R) \subseteq \mathfrak{m}$, then $1 = u+g$ would be in $\mathfrak{m}$, a contradiction). Because $f(1-g) = 0$ and $1-g$ is a unit, we must have $f = 0$. This implies $I_0 = (f) = \{0\}$, which contradicts $I_0 J \neq \{0\}$. This final contradiction forces our assumption $J \neq \{0\}$ to be false. Thus $J = \{0\}$, and we have shown that (0) is a product of maximal ideals, say $(0) = \mathfrak{m}_1 \dots \mathfrak{m}_t$.

Now we build a composition series for R. Consider the chain:

$$R \supset \mathfrak{m}_1 \supset \mathfrak{m}_1\mathfrak{m}_2 \supset \cdots \supset \mathfrak{m}_1 \dots \mathfrak{m}_t = \{0\}$$

Each quotient module $M_s = (\mathfrak{m}_1 \dots \mathfrak{m}_s)/(\mathfrak{m}_1 \dots \mathfrak{m}_{s+1})$ is annihilated by $\mathfrak{m}_{s+1}$, so it is a module over the field $R/\mathfrak{m}_{s+1}$, i.e., a vector space. Any chain of submodules in M_s corresponds to a chain of ideals in R. Since R is Artinian, M_s must satisfy the DCC on subspaces, which means it must be a finite-dimensional vector space. A finite-dimensional vector space has a finite composition series (given by a basis). By refining the chain above with composition series for each vector space factor, we obtain a finite composition series for R. By Theorem 6.6, if R has a finite composition series, it is both Artinian and Noetherian.

Finally, we show every prime ideal is maximal. Let P be a prime ideal. Then $P \supseteq (0) = \mathfrak{m}_1 \dots \mathfrak{m}_t$. Since P is prime, it must contain one of the factors, so $P \supseteq \mathfrak{m}_i$ for some i. Since $\mathfrak{m}_i$ is a maximal ideal, we must have $P = \mathfrak{m}_i$. Thus every prime ideal is maximal. In particular, this shows that the only prime ideals are the maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_t$ appearing in the product for (0). Therefore, R has only finitely many maximal ideals. □

The powerful algebraic characterization of Artinian rings has a direct and intuitive geometric interpretation through the language of algebraic geometry, specifically via the prime spectrum of a ring, $\mathrm{Spec}(R)$.

Corollary 6.9. *Let R be a commutative ring. If R is Artinian, then its prime spectrum $\mathrm{Spec}(R)$ is a finite set of closed points.*

Proof. By Theorem 6.8, an Artinian ring R has only finitely many maximal ideals, and every prime ideal of R is maximal. The points of $\mathrm{Spec}(R)$ are the prime ideals of R. Thus, $\mathrm{Spec}(R)$ is a finite set. In the Zariski topology on $\mathrm{Spec}(R)$, points corresponding to maximal ideals are always closed points. □

The converse is also true: a Noetherian ring R with a finite spectrum is Artinian. The Artinian condition thus forces the geometry to be zero-dimensional and finite. A particularly rich source of examples comes from finite-dimensional algebras over a field.

Remark 6.10 (Artinian k-algebras)**.** *Let R be a finitely generated algebra over an algebraically closed field k, e.g., $R = k[x_1, \dots, x_n]/I$. If R is Artinian, then by Theorem 6.8, it is a finite-dimensional vector space over k. Its length as an R-module is equal to its dimension as a k-vector space: $\ell(R) = \dim_k(R)$. In this setting, $\mathrm{Spec}(R)$ corresponds to a finite set of points, and the length $\ell(R)$ is the total number of these points, counted with multiplicity. This "multiplicity" captures non-reduced structure, such as tangent directions or infinitesimal neighborhoods, at the geometric points.*

Example 6.11. *Let k be an algebraically closed field.*

1. *Let $R = k[x,y]/(x,y)$. Here $\mathrm{Spec}(R)$ consists of a single point, the maximal ideal (x,y). We have an isomorphism $R \cong k$, so $\dim_k(R) = 1$. The composition series is $R \supsetneq \{0\}$, so $\ell(R) = 1$. This corresponds to a simple point in the plane.*

2. *Let $R = k[x]/(x(x-1))$. The prime ideals are (x) and $(x-1)$, so Spec(R) consists of two distinct points. By the Chinese Remainder Theorem, $R \cong k[x]/(x) \times k[x]/(x-1) \cong k \times k$. Thus $\dim_k(R) = 2$. A composition series is $R \supsetneq (x) \supsetneq \{0\}$, showing $\ell(R) = 2$. The length equals the number of geometric points.*

3. *Let $R = k[x,y]/(x,y^2)$. The only prime ideal is (x,y), so Spec(R) is a single point. However, as a k-vector space, R is generated by $\{1, y\}$ (since $x = 0$ and $y^2 = 0$), so $\dim_k(R) = 2$. A composition series is $R \supsetneq (y) \supsetneq \{0\}$, so $\ell(R) = 2$.*

   Here, the length (2) is greater than the number of geometric points (1). The ring R is not a field; it contains the nilpotent element y. Geometrically, this represents a "thickened" point, or a point equipped with a tangent direction (in this case, along the y-axis). This is a fundamental example in scheme theory of a non-reduced structure, which can be visualized as the limit of two distinct points on a line colliding and merging into one.

6.1.2 Associated Primes

We begin with motivation via an analogy from number theory: The Fundamental Theorem of Arithmetic provides a canonical decomposition of any integer $n \in \mathbb{Z}$. This decomposition can be recast in the language of ideals. For an integer $n = \pm p_1^{d_1} \cdots p_t^{d_t}$ with distinct primes p_i, the corresponding principal ideal (n) has a decomposition as an intersection of ideals:

$$(n) = (p_1^{d_1}) \cap \cdots \cap (p_t^{d_t})$$

This is a primary decomposition of the ideal (n). The set of prime ideals $\{(p_1), \ldots, (p_t)\}$ associated with this decomposition is uniquely determined by (n). The ideals $(p_i^{d_i})$ are called the **primary components**. The theory of associated primes and primary decomposition aims to generalize this structural result from the ring of integers to modules over general commutative rings.

Additionally, a powerful motivation for this theory comes from algebraic geometry. Let $R = k[x_1, \ldots, x_n]$ be the polynomial ring over a field k, and let $I \subseteq R$ be an ideal. The vanishing set of I, denoted $V(I)$, is the set of points in affine space k^n where all polynomials in I evaluate to zero. A central goal is to decompose the geometric object $V(I)$ into its fundamental, indivisible pieces.

Definition 6.12. *A closed algebraic set $V(I)$ is **reducible** if it can be written as a union of two proper closed subsets, i.e., $V(I) = V(I') \cup V(I'')$ where $V(I) \neq V(I')$ and $V(I) \neq V(I'')$. Otherwise, $V(I)$ is called **irreducible**.*

The algebraic counterpart to the geometric notion of irreducibility is the primality of an ideal. Specifically, it relates to the radical of the ideal.

Proposition 6.13. *Let I be an ideal in $R = k[x_1, \ldots, x_n]$. The algebraic set $V(I)$ is irreducible if and only if its corresponding radical ideal rad$I$ is a prime ideal.*

Proof. Recall that for any ideals I' and I'', we have $V(I') \cup V(I'') = V(I' \cap I'')$. Also, $V(I) = V(\text{rad}I)$.

($\Leftarrow$) Assume rad$I$ is a prime ideal. Suppose for contradiction that $V(I)$ is reducible, so $V(I) = V(I') \cup V(I'')$ for some ideals I', I'' such that $V(I') \subsetneq V(I)$ and $V(I'') \subsetneq V(I)$. This implies $V(\text{rad}I) = V(I' \cap I'')$, and by Hilbert's Nullstellensatz, $\text{rad}I = \text{rad}I' \cap I'' = \text{rad}I'\text{rad}I''$. The inclusions $V(I') \subsetneq V(I)$ and $V(I'') \subsetneq V(I)$ imply $\text{rad}I \subsetneq \text{rad}I'$ and $\text{rad}I \subsetneq \text{rad}I''$. Let $f \in \text{rad}I'$ such that $f \notin \text{rad}I$, and let $g \in \text{rad}I''$ such that $g \notin \text{rad}I$. The product fg is in $\text{rad}I'\text{rad}I''$, so $fg \in \text{rad}I$. Since rad$I$ is prime, this implies either $f \in \text{rad}I$ or $g \in \text{rad}I$, which is a contradiction. Therefore, $V(I)$ must be irreducible.

($\Rightarrow$) Assume $V(I)$ is irreducible. Suppose for contradiction that rad$I$ is not prime. Then there exist polynomials $f, g \in R$ such that $fg \in \text{rad}I$ but $f \notin \text{rad}I$ and $g \notin \text{rad}I$. Let $I' = I + (f)$ and $I'' = I + (g)$. Then $fg \in \text{rad}I$ implies that $V(I) \subseteq V(fg) = V(f) \cup V(g)$. Thus, $V(I) = (V(I) \cap V(f)) \cup (V(I) \cap V(g)) = V(I + (f)) \cup V(I + (g)) = V(I') \cup V(I'')$. Since $f \notin \text{rad}I$, there exists a point $P \in V(I)$ such that $f(P) \neq 0$. This means $P \notin V(I')$, so $V(I') \subsetneq V(I)$. Similarly, since $g \notin \text{rad}I$, $V(I'') \subsetneq V(I)$. We have written $V(I)$ as

a union of two proper closed subsets, which contradicts its irreducibility. Therefore, rad$I$ must be a prime ideal. □

This proposition suggests that the irreducible components of $V(I)$ correspond to a special set of prime ideals related to I. For a general Noetherian ring, any radical ideal can be written uniquely as a finite, irredundant intersection of prime ideals, rad$I = P_1 \cap \cdots \cap P_t$. This corresponds to a unique decomposition of $V(I)$ into irreducible components: $V(I) = V(P_1) \cup \cdots \cup V(P_t)$. These primes $P_1, \ldots, P_t$ are precisely the primes minimal over I.

However, the ideal I itself contains more information than its radical rad$I$ (e.g., multiplicities, embedded structures). The theory of associated primes aims to identify the correct set of primes to describe the structure of the module R/I, not just the geometry of $V(I)$.

Example 6.14. *Let $I = (x^2, xy) \subseteq k[x, y]$. The radical is rad$I = (x)$, which is prime. Thus $V(I) = V(x)$ is the y-axis, which is irreducible. Algebraically, however, I has a more intricate structure. We can write I as an intersection of ideals:*

$$I = (x) \cap (x^2, y) \quad or \quad I = (x) \cap (x, y)^2$$

Notice that the radicals of the ideals in the intersection are (x) and (x, y). The prime (x, y) corresponds to the origin, a geometric point embedded within the y-axis. As we will see, the "correct" set of primes associated to I is $\{(x), (x, y)\}$, which captures both the main component (the line) and the embedded structure (the point). The description of I as an intersection of ideals whose radicals are these associated primes is not unique, which motivates the more refined theory of primary decomposition.

We now formalize the algebraic notion of primes "belonging" to a module.

Definition 6.15. *Let R be a commutative ring and M be an R-module. A prime ideal $P \subset R$ is **associated** to M if there exists an element $x \in M$ such that P is the annihilator of x. That is,*

$$P = ann(x) := \{r \in R \mid rx = 0\}$$

The set of all associated primes of M is denoted $Ass_R(M)$, or simply $Ass(M)$ when the ring is clear. For an ideal $I \subseteq R$, the associated primes of I are defined as $Ass(R/I)$.

Remark 6.16. *An immediate and powerful consequence of the definition is the following equivalence:*

$$P \in Ass(M) \iff R/P \text{ is isomorphic to a submodule of } M.$$

Indeed, if $P = ann(x)$, the submodule $Rx \subseteq M$ is isomorphic to R/P via the map $r \mapsto rx$. Conversely, if there is an embedding $\phi : R/P \hookrightarrow M$, then the image of $\bar{1} \in R/P$, say $x = \phi(\bar{1})$, has annihilator precisely P. This viewpoint reveals that the associated primes of M are precisely the prime ideals that arise as annihilators of cyclic submodules of M.

For finitely generated modules over a Noetherian ring, the set of associated primes is well-behaved and captures essential information about the module.

Theorem 6.17. *Let R be a Noetherian ring and let M be a non-zero, finitely generated R-module. Then:*

1. *The set $Ass(M)$ is finite and non-empty.*
2. *Every prime ideal minimal among those containing $ann(M)$ is in $Ass(M)$.*
3. *The set of zero-divisors on M is precisely the union of the associated primes:*

$$\{r \in R \mid \exists m \neq 0 \in M, rm = 0\} = \bigcup_{P \in Ass(M)} P$$

4. *For any multiplicatively closed subset $U \subseteq R$, the associated primes of the localized module $M_U = M[U^{-1}]$ are the localized associated primes of M that do not meet U:*

$$Ass_{R_U}(M_U) = \{P_U \mid P \in Ass(M) \text{ and } P \cap U = \emptyset\}$$

Proof. The proof of this theorem requires several preliminary lemmas and is deferred. A key first step is to show that in a Noetherian ring, any ideal maximal among annihilators of non-zero elements is prime, which guarantees that $\mathrm{Ass}(M)$ is non-empty. □

Remark 6.18. *The existence of prime ideals minimal over any given ideal I is guaranteed by Zorn's Lemma and does not require the ring to be Noetherian. Let Σ be the set of prime ideals containing I. Consider a chain of primes $\{Q_j\}$ in Σ. Their intersection $Q = \cap Q_j$ is an ideal containing I. If $ab \in Q$, then $ab \in Q_j$ for all j. Since each Q_j is prime, for each j, either $a \in Q_j$ or $b \in Q_j$. Since $\{Q_j\}$ is a chain, this implies that either a is in all Q_j or b is in all Q_j. Thus, either $a \in Q$ or $b \in Q$, proving that Q is prime. Every chain in Σ has a lower bound in Σ, so by Zorn's Lemma, Σ has minimal elements.*

The set of associated primes often contains inclusion relations, which have important geometric meaning. This leads to a crucial distinction.

Definition 6.19. *Let M be an R-module. An associated prime $P \in Ass(M)$ is said to be a **minimal** (or **isolated**) prime of M if it is minimal with respect to inclusion in the set $Ass(M)$. An associated prime that is not minimal is called an **embedded** prime of M.*

If $M = R/I$, the minimal primes of R/I are precisely the minimal prime ideals containing I. Geometrically, if P is a minimal prime, $V(P)$ is an irreducible component of the support of the module. If Q is an embedded prime, then it properly contains some minimal prime P, so geometrically $V(Q)$ is a subvariety contained within the component $V(P)$.

Example 6.20. *Let us revisit the ideal $I = (x^2, xy) \subseteq R = k[x, y]$. We compute the associated primes of the module $M = R/I$. The elements of M are residue classes of polynomials, which we denote by $\bar{f}$.*

- *Consider the element $\bar{y} \in M$. What is its annihilator? We need $f \in R$ such that $f\bar{y} = \overline{0}$, which means $fy \in I = (x^2, xy) = x(x, y)$. This requires f to be a multiple of x. Thus, $ann(\bar{y}) = (x)$. Since (x) is a prime ideal, we have $(x) \in Ass(R/I)$.*
- *Consider the element $\bar{x} \in M$. What is its annihilator? We need $f \in R$ such that $f\bar{x} = \overline{0}$, which means $fx \in I = (x^2, xy)$. We can write $fx = g(x)x^2 + h(x, y)xy = x(gx + hy)$. This is satisfied if $f \in (x, y)$. Thus, $ann(\bar{x}) = (x, y)$. Since (x, y) is a maximal (and hence prime) ideal, we have $(x, y) \in Ass(R/I)$.*

It can be shown that these are the only associated primes. So, $Ass(R/I) = \{(x), (x, y)\}$. Since $(x) \subsetneq (x, y)$, we have:

- *(x) is a **minimal associated prime**. It corresponds to the **isolated component** $V(x)$ (the y-axis), which is the geometric support of the module.*
- *(x, y) is an **embedded associated prime**. It corresponds to the **embedded component** $V(x, y)$ (the origin). This component is "embedded" in the sense that it lies on the isolated component. The existence of this embedded prime reveals the special "thicker" structure of our scheme at the origin, which is lost when we only consider the radical $radI = (x)$.*

6.1.3 Prime Avoidance

A recurring theme in commutative algebra is the ability to find an element in an ideal that simultaneously avoids a finite collection of other ideals, particularly prime ideals. This notion is formalized by the Prime Avoidance Theorem.

Theorem 6.21 (Prime Avoidance)**.** *Let R be a commutative ring, and let $J, I_1, \ldots, I_n$ be ideals in R. Suppose that $J \subseteq \bigcup_{j=1}^{n} I_j$.*

1. *If R contains an infinite field k and J is a k-subspace, then $J \subseteq I_j$ for some j.*
2. *If at most two of the ideals I_j are not prime, then $J \subseteq I_j$ for some j.*

Remark 6.22. *The name of the theorem comes from its contrapositive statement: if an ideal J is not contained in any of the prime ideals $P_1, \ldots, P_n$, then there exists an element $x \in J$ that is not in any of the P_j. In short, x "avoids" all the primes.*

Proof. (1) This is a standard result from linear algebra. A vector space over an infinite field cannot be the union of a finite number of proper subspaces. Suppose $J \not\subseteq I_j$ for all j. Then $J \cap I_j$ is a proper subspace of J for each j. Since $J \subseteq \bigcup I_j$, we have $J = \bigcup (J \cap I_j)$, which is a contradiction.

(2) We proceed by induction on n. The base case $n = 1$ is trivial: if $J \subseteq I_1$, the conclusion holds. For the inductive step, assume $n > 1$ and the theorem holds for unions of fewer than n ideals. We may assume without loss of generality that the union is irredundant, i.e., $J \not\subseteq \bigcup_{j \neq k} I_j$ for any $k \in \{1, \ldots, n\}$. This assumption allows us to choose, for each k, an element $x_k \in J$ such that $x_k \notin \bigcup_{j \neq k} I_j$. Since $x_k \in J \subseteq \bigcup_{j=1}^{n} I_j$, it must be that $x_k \in I_k$.

Case $n = 2$: We have $J \subseteq I_1 \cup I_2$. We have chosen $x_1 \in J$ with $x_1 \in I_1, x_1 \notin I_2$, and $x_2 \in J$ with $x_2 \in I_2, x_2 \notin I_1$. Consider the element $y = x_1 + x_2$. Since $x_1, x_2 \in J$, we have $y \in J$. Suppose $y \in I_1$. Since $x_1 \in I_1$, it follows that $x_2 = y - x_1 \in I_1$, which contradicts our choice of x_2. Suppose $y \in I_2$. Since $x_2 \in I_2$, it follows that $x_1 = y - x_2 \in I_2$, which contradicts our choice of x_1. Thus, y is not in $I_1 \cup I_2$. But $y \in J$, so this contradicts $J \subseteq I_1 \cup I_2$. Therefore, our initial assumption must be false, and J must be contained in either I_1 or I_2. Note that this case requires no primality assumption.

Case $n > 2$: By hypothesis, at most two of the ideals I_j are not prime. By relabeling, we may assume that I_n is a prime ideal. As before, we have elements $x_j \in J \cap I_j$ such that $x_j \notin I_k$ for $j \neq k$. Consider the element $y = x_n + (x_1 x_2 \cdots x_{n-1})$. Since $x_j \in J$ for all j, we have $y \in J$. Let's check for its membership in the ideals I_j.

- Suppose $y \in I_n$. Since $x_n \in I_n$, this implies $x_1 x_2 \cdots x_{n-1} \in I_n$. As I_n is prime, this means $x_j \in I_n$ for some $j \in \{1, \ldots, n-1\}$. This contradicts the choice of x_j. Thus, $y \notin I_n$.
- Now consider I_k for some $k \in \{1, \ldots, n-1\}$. By construction, $x_k \in I_k$, so the product $x_1 x_2 \cdots x_{n-1}$ is in I_k. If $y \in I_k$, then $x_n = y - (x_1 \cdots x_{n-1})$ must be in I_k. This contradicts the choice of x_n. Thus, $y \notin I_k$.

We have constructed an element $y \in J$ such that $y \notin \bigcup_{j=1}^{n} I_j$, which is a contradiction. Therefore, our assumption that the union was irredundant is false, and J must be contained in some I_j. □

Remark 6.23. *If R is a graded ring, J is an ideal generated by homogeneous elements of positive degree, and all the I_j are prime ideals, then it is sufficient to assume that the set of homogeneous elements of J is contained in $\bigcup I_j$. The proof is modified by ensuring the constructed element is homogeneous. For example, one can replace x_k with suitable powers to make the degrees match in the element $y = x_n^d + (x_1 \cdots x_{n-1})$. The primality of all I_j ensures that if $x_k \notin I_j$, then $x_k^d \notin I_j$ for $j \neq k$.*

A crucial application of Prime Avoidance relates an ideal to the zero-divisors of a module.

Corollary 6.24. *Let R be a Noetherian ring, $M \neq 0$ a finitely generated R-module, and $I \subseteq R$ an ideal. Then either I contains a non-zero-divisor on M, or I is contained in the annihilator of some non-zero element of M.*

Proof. The set of zero-divisors on M is the union of its associated primes, $Z(M) = \bigcup_{P \in \mathrm{Ass}(M)} P$. Since M is a finitely generated module over a Noetherian ring, the set $\mathrm{Ass}(M)$ is finite. If $I \subseteq Z(M)$, then $I \subseteq \bigcup_{P \in \mathrm{Ass}(M)} P$. By the Prime Avoidance Theorem, I must be contained in some associated prime $P \in \mathrm{Ass}(M)$. By definition of an associated prime, $P = \mathrm{ann}(x)$ for some non-zero $x \in M$. Thus, $I \subseteq \mathrm{ann}(x)$. Conversely, if I is not contained in any associated prime, then by Prime Avoidance, $I \not\subseteq \bigcup_{P \in \mathrm{Ass}(M)} P = Z(M)$. This means there exists an element in I which is not a zero-divisor on M. □

We now provide the proofs for the fundamental properties of associated primes stated in the previous section. We begin by establishing their existence.

Proposition 6.25. *Let R be a ring and $M \neq 0$ be an R-module. If $I \subseteq R$ is an ideal that is maximal among all annihilators of non-zero elements of M, then I is a prime ideal. In particular, if R is Noetherian, $Ass(M)$ is non-empty.*

Proof. Let $I = \text{ann}(x)$ for some $x \neq 0 \in M$. To show I is prime, let $a, b \in R$ with $ab \in I$ and suppose $b \notin I$. We must show $a \in I$. Since $ab \in I = \text{ann}(x)$, we have $(ab)x = a(bx) = 0$. Since $b \notin I$, the element $bx \in M$ is non-zero. The annihilator of bx is $\text{ann}(bx) = \{r \in R \mid r(bx) = 0\}$. We see that $I \subseteq \text{ann}(bx)$ (since for $r \in I$, $r(bx) = b(rx) = b \cdot 0 = 0$), and also $a \in \text{ann}(bx)$. Thus, the ideal $I + (a)$ is contained in $\text{ann}(bx)$. Since I is maximal in the set of annihilators and $I \subseteq \text{ann}(bx)$, we must have either $I = \text{ann}(bx)$ or $\text{ann}(bx) = R$. The latter is impossible since $bx \neq 0$. Thus $I = \text{ann}(bx)$. Since $I + (a) \subseteq \text{ann}(bx) = I$, we must have $a \in I$. This proves that I is prime.

If R is Noetherian, the set of ideals $\Sigma = \{\text{ann}(x) \mid x \in M, x \neq 0\}$ is non-empty (as $M \neq 0$). By the ACC, this set has a maximal element. By the first part of the proposition, this maximal element is a prime ideal and is in $\text{Ass}(M)$. Thus $\text{Ass}(M) \neq \emptyset$. □

This proposition, combined with the definition of a zero-divisor, immediately proves part of the main theorem.

Proof of Theorem 6.17 (3). The set of zero-divisors on M is $Z(M) = \{r \in R \mid \exists x \neq 0, rx = 0\} = \bigcup_{x \neq 0} \text{ann}(x)$. If $P \in \text{Ass}(M)$, then $P = \text{ann}(x)$ for some $x \neq 0$, so every element of P is a zero-divisor. This shows $\bigcup_{P \in \text{Ass}(M)} P \subseteq Z(M)$. Conversely, let $r \in Z(M)$. Then $r \in \text{ann}(x)$ for some $x \neq 0$. In a Noetherian ring, the ideal $\text{ann}(x)$ is contained in a maximal annihilator ideal, which by Proposition 6.25 is an associated prime P. Thus $r \in P \subseteq \bigcup_{Q \in \text{Ass}(M)} Q$. This shows $Z(M) \subseteq \bigcup_{P \in \text{Ass}(M)} P$. □

We can refine the classical result that an element is zero if and only if it is zero in all localizations at maximal ideals.

Corollary 6.26. *Let R be a Noetherian ring and M be an R-module. An element $x \in M$ is zero if and only if its image $x/1$ is zero in the localization M_P for every maximal associated prime P of M.*

Proof. ($\Rightarrow$) This direction is clear. ($\Leftarrow$) Suppose $x \neq 0$. Let $I = \text{ann}(x)$, which is a proper ideal of R. The submodule $Rx \subseteq M$ is non-zero, so $\text{Ass}(Rx)$ is non-empty. Let $P \in \text{Ass}(Rx)$. Then $P = \text{ann}(sx)$ for some $s \in R$. By definition, $P \supseteq \text{ann}(Rx) = \text{ann}(x) = I$. Since $\text{Ass}(Rx) \subseteq \text{Ass}(M)$, P is an associated prime of M. There exists a maximal element P_{max} in the set $\text{Ass}(M)$ such that $P \subseteq P_{max}$. We claim the image of x in $M_{P_{max}}$ is non-zero. If $x/1 = 0$ in $M_{P_{max}}$, then there exists some $u \in R \setminus P_{max}$ such that $ux = 0$. This means $u \in \text{ann}(x) = I \subseteq P \subseteq P_{max}$. This is a contradiction, as $u \notin P_{max}$. Therefore, $x/1 \neq 0$ in $M_{P_{max}}$. □

The following lemma describes the behavior of associated primes in short exact sequences and is key to proving their finiteness.

Lemma 6.27. *Let R be a Noetherian ring. For any short exact sequence of R-modules $0 \to M' \to M \to M'' \to 0$, we have*

$$Ass(M') \subseteq Ass(M) \subseteq Ass(M') \cup Ass(M'').$$

Proof. The inclusion $\text{Ass}(M') \subseteq \text{Ass}(M)$ is immediate, since any submodule of M' isomorphic to R/P is also a submodule of M. For the second inclusion, let $P \in \text{Ass}(M)$. Then there is a submodule $N \subseteq M$ with $N \cong R/P$. If $N \cap M' \neq \{0\}$, then since every non-zero element of $N \cong R/P$ has annihilator P, any non-zero element in $N \cap M'$ has annihilator P. This implies $P \in \text{Ass}(M')$. If $N \cap M' = \{0\}$, then the composition $N \hookrightarrow M \to M''$ is injective. So N is isomorphic to a submodule of M''. This implies $P \in \text{Ass}(M'')$. In either case, $P \in \text{Ass}(M') \cup \text{Ass}(M'')$. □

The final piece needed is the existence of a prime filtration for any finitely generated module.

Proposition 6.28. *If R is a Noetherian ring and M is a finitely generated R-module, then M has a filtration $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$ such that each quotient M_{i+1}/M_i is isomorphic to R/P_i for some prime ideal $P_i \subseteq R$.*

Proof. If $M = 0$, the filtration is trivial. If $M \neq 0$, since R is Noetherian, $\text{Ass}(M)$ is non-empty. Let $P_1 \in \text{Ass}(M)$. Then there exists a submodule $M_1 \subseteq M$ with $M_1 \cong R/P_1$. Now consider the quotient module M/M_1. If it is non-zero, it also has an associated prime $P_2 \in \text{Ass}(M/M_1)$, giving a submodule $M_2/M_1 \subseteq M/M_1$ with $M_2/M_1 \cong R/P_2$. We build a chain $0 \subseteq M_1 \subseteq M_2 \subseteq \dots$. Since M is a finitely generated module over a Noetherian ring, it is a Noetherian module. This ascending chain of submodules must terminate, i.e., $M_n = M$ for some n. This gives the desired filtration. □

We are now equipped to prove the remaining parts of the main theorem.

Proof of Theorem 6.17 (1): Finiteness and Minimal Primes. Let M have a prime filtration as in Proposition 6.28. We prove that $\text{Ass}(M)$ is finite by induction on the length n of the filtration. If $n = 1$, then $M \cong R/P_1$. Any non-zero element $x \in M$ generates the entire module as a submodule, and $\text{ann}(x) = P_1$. Thus $\text{Ass}(M) = \{P_1\}$, which is finite. For $n > 1$, consider the short exact sequence $0 \to M_{n-1} \to M \to R/P_n \to 0$. By Lemma 6.27, $\text{Ass}(M) \subseteq \text{Ass}(M_{n-1}) \cup \text{Ass}(R/P_n)$. By the inductive hypothesis, $\text{Ass}(M_{n-1})$ is finite. As we just saw, $\text{Ass}(R/P_n) = \{P_n\}$. Therefore, $\text{Ass}(M)$ is a subset of a finite set, and is itself finite.

Now, let P be a prime ideal minimal over $\text{ann}(M)$. We must show $P \in \text{Ass}(M)$. Localize at P. The module M_P over the local ring R_P is non-zero, otherwise there would be an $s \in R \setminus P$ with $sM = 0$, implying $\text{ann}(M) \not\subseteq P$. Since R_P is Noetherian and $M_P \neq 0$, $\text{Ass}_{R_P}(M_P)$ is non-empty. Let $Q' \in \text{Ass}_{R_P}(M_P)$. Any such prime must contain the annihilator $\text{ann}_{R_P}(M_P) = (\text{ann}(M))_P$. The prime ideals of R_P containing $(\text{ann}(M))_P$ correspond to prime ideals of R containing $\text{ann}(M)$ and contained in P. Since P is minimal over $\text{ann}(M)$, the only such prime is P itself. Thus, the only prime in R_P containing $(\text{ann}(M))_P$ is P_P. So we must have $Q' = P_P$. This shows $\text{Ass}_{R_P}(M_P) = \{P_P\}$. By the localization property (part 4), $\text{Ass}_{R_P}(M_P)$ consists of primes Q_P where $Q \in \text{Ass}(M)$ and $Q \subseteq P$. Since $\text{Ass}_{R_P}(M_P)$ is non-empty and equal to $\{P_P\}$, there must be some $Q \in \text{Ass}(M)$ with $Q \subseteq P$ such that $Q_P = P_P$. This implies $Q = P$. Therefore, $P \in \text{Ass}(M)$. □

Proof of Theorem 6.17 (4): Localization. ($\Rightarrow$) Suppose $P \in \text{Ass}(M)$ and $P \cap U = \emptyset$. Then there is an injective map $R/P \to M$. Localization is an exact functor, so applying $(\cdot)_U$ yields an injective map $(R/P)_U \to M_U$. Since $P \cap U = \emptyset$, $(R/P)_U \cong R_U/P_U$, and P_U is a prime ideal of R_U. Thus R_U/P_U embeds into M_U, which means $P_U \in \text{Ass}_{R_U}(M_U)$.

($\Leftarrow$) Suppose $Q \in \text{Ass}_{R_U}(M_U)$. Any prime in R_U is of the form P_U for some prime $P \subset R$ with $P \cap U = \emptyset$. So we have an embedding $\phi : R_U/P_U \hookrightarrow M_U$. This embedding is a map in $\text{Hom}_{R_U}(R_U/P_U, M_U)$. For finitely presented modules over a Noetherian ring, Hom commutes with localization. Specifically, there is a natural isomorphism:

$$\text{Hom}_{R_U}((R/P)_U, M_U) \cong (\text{Hom}_R(R/P, M))_U$$

So our map ϕ corresponds to an element f/u for some $f \in \text{Hom}_R(R/P, M)$ and $u \in U$. This means that after localizing, the map f becomes ϕ. Since ϕ is injective, for any $a/1 \in R_U/P_U$, if $\phi(a/1) = 0$ then $a/1 = 0$. We have $\phi(a/1) = (f/u)(a/1) = f(\bar{a})/u$. For this to be zero in M_U, there must be some $v \in U$ such that $vf(\bar{a}) = 0$. So $f(v\bar{a}) = 0$. Consider the kernel of f. Let $\bar{a} \in \ker f$. Then $f(\bar{a}) = 0$, so $\phi(a/1) = 0$, which implies $a/1 = 0$ in $(R/P)_U$. This means there is some $w \in U$ such that $wa \in P$. Since $P \cap U = \emptyset$ and P is prime, this implies $a \in P$, so $\bar{a} = 0$ in R/P. Therefore, $\ker f = \{0\}$ and $f : R/P \to M$ is injective. This implies $P \in \text{Ass}(M)$. □

6.1.4 Introduction to Primary Decomposition

The theory of associated primes provides the foundation for a powerful generalization of prime factorization known as primary decomposition. Throughout this section, we assume that R is a Noetherian ring and M is a non-zero, finitely generated R-module. While the theory is often first developed for ideals, we define it more generally for submodules.

Definition 6.29. *A proper submodule $N \subsetneq M$ is called **primary** if the set of associated primes of the quotient module M/N consists of a single element. If $Ass(M/N) = \{P\}$, we say that N is a P-**primary***

***submodule**. An R-module M is **coprimary** if the zero submodule $\{0\} \subseteq M$ is primary, i.e., if $Ass(M)$ consists of a single element. If $Ass(M) = \{P\}$, we say M is P-**coprimary**.*

An important property is that the intersection of submodules that are primary to the same prime is again primary to that prime.

Proposition 6.30. *If $N_1, \ldots, N_t \subseteq M$ are P-primary submodules for a given prime ideal P, then their intersection $N = \bigcap_{i=1}^{t} N_i$ is also a P-primary submodule.*

Proof. By induction, it suffices to prove the case $t = 2$. Let $N = N_1 \cap N_2$. There is a canonical injection of M/N into the direct sum $M/N_1 \oplus M/N_2$ given by the map $m+N \mapsto (m+N_1, m+N_2)$. Using the properties of associated primes for submodules and direct sums, we have:

$$\mathrm{Ass}(M/N) \subseteq \mathrm{Ass}(M/N_1 \oplus M/N_2) = \mathrm{Ass}(M/N_1) \cup \mathrm{Ass}(M/N_2)$$

By hypothesis, $\mathrm{Ass}(M/N_1) = \{P\}$ and $\mathrm{Ass}(M/N_2) = \{P\}$. Therefore, $\mathrm{Ass}(M/N) \subseteq \{P\}$. Since N is a proper submodule, $M/N \neq 0$, so its set of associated primes is non-empty. We conclude that $\mathrm{Ass}(M/N) = \{P\}$, and thus N is P-primary. □

The modern definition of a primary module can be connected to more classical characterizations involving zero-divisors and annihilators.

Proposition 6.31. *Let M be a finitely generated R-module and $P \subseteq R$ be a prime ideal. The following are equivalent:*

1. *M is P-coprimary (i.e., $Ass(M) = \{P\}$).*
2. *P is the unique minimal prime ideal over $ann(M)$, and every zero-divisor on M is in P.*
3. *There exists an integer $n > 0$ such that $P^n \subseteq ann(M)$, and every element of $R \setminus P$ is a non-zero-divisor on M.*

Proof. (1) $\implies$ (2): If $\mathrm{Ass}(M) = \{P\}$, then P is the only associated prime. Since the minimal primes over $\mathrm{ann}(M)$ are a subset of $\mathrm{Ass}(M)$, P must be the unique minimal prime. The set of zero-divisors on M is the union of the associated primes, which in this case is just P.

(2) $\implies$ (3): The second condition states that every element of $R \setminus P$ is a non-zero-divisor on M. We only need to show that $P^n \subseteq \mathrm{ann}(M)$ for some n. Let's localize at P. The ring is R_P and the module is M_P. The annihilator is $\mathrm{ann}_{R_P}(M_P) = (\mathrm{ann}(M))_P$. Since P is the unique minimal prime over $\mathrm{ann}(M)$, the ideal P_P is the unique minimal prime over $(\mathrm{ann}(M))_P$ in the local ring R_P. In a local ring, the unique minimal prime over an ideal is precisely its nilradical. Thus, $P_P = \mathrm{rad}(\mathrm{ann}_{R_P}(M_P))$. Since R_P is Noetherian, its maximal ideal P_P is finitely generated. The radical property implies that some power of P_P is contained in $\mathrm{ann}_{R_P}(M_P)$, say $(P_P)^n \subseteq \mathrm{ann}_{R_P}(M_P)$. This means $(P^n)_P \subseteq (\mathrm{ann}(M))_P$. This implies that for any $x \in P^n$ and any $m \in M$, we have $xm/1 = 0$ in M_P. By definition of localization, there exists $u \in R \setminus P$ such that $uxm = 0$. By hypothesis, every element of $R \setminus P$ is a non-zero-divisor on M, so we can conclude that $xm = 0$. Since this holds for all $m \in M$, we have $x \in \mathrm{ann}(M)$. Thus, $P^n \subseteq \mathrm{ann}(M)$.

(3) $\implies$ (1): Let $Q \in \mathrm{Ass}(M)$. Then $Q \supseteq \mathrm{ann}(M)$. Since $P^n \subseteq \mathrm{ann}(M)$, we have $Q \supseteq P^n$, which implies $Q \supseteq P$ because Q is prime. On the other hand, the set of zero-divisors on M is $\bigcup_{Q' \in \mathrm{Ass}(M)} Q'$. By hypothesis, every element of $R \setminus P$ is a non-zero-divisor, so the set of zero-divisors is contained in P. Thus, $\bigcup_{Q' \in \mathrm{Ass}(M)} Q' \subseteq P$. This implies that every associated prime Q must be contained in P. Combining $Q \supseteq P$ and $Q \subseteq P$, we get $Q = P$. Thus, any associated prime must be equal to P, which means $\mathrm{Ass}(M) = \{P\}$. □

Remark 6.32. *If we apply the proposition to a module $M = R/I$ for a proper ideal $I \subset R$, we find that I is a P-primary ideal if and only if $P^n \subseteq I$ for some n and for any $r, s \in R$, if $rs \in I$ and $r \notin P$, then $s \in I$. This is equivalent to the classical definition: an ideal I is P-primary if $rad(I) = P$ and for any $r, s \in R$ with $rs \in I$, if $r \notin I$ then $s \in P$. For example, in $R = k[x, y]$, the ideal $I = (x^2, y)$ has radical $rad(I) = (x, y)$. This is not (x, y)-primary since, for instance, (x)-primary since $rad(I) \neq (x)$.*

Remark 6.33. *An important consequence of the characterizations above is that if a submodule N is P-primary in M, then the radical of the annihilator of the quotient is P. That is, $rad(ann(M/N)) = P$. This follows because if $Ass(M/N) = \{P\}$, then P is the unique minimal prime over $ann(M/N)$, so $P = rad(ann(M/N))$.*

The previous remark shows that if I is P-primary, then $\text{rad}(I) = P$. However, the converse is false: an ideal whose radical is prime is not necessarily primary. For instance, $I = (x^2, xy) \subseteq k[x, y]$ has $\text{rad}(I) = (x)$, which is prime. But we have seen that $\text{Ass}(R/I) = \{(x), (x, y)\}$, so I is not primary. This motivates the need for a decomposition into an intersection of primary ideals.

Theorem 6.34 (Lasker-Noether)**.** *Let M be a finitely generated module over a Noetherian ring R. Any proper submodule $N \subsetneq M$ can be written as a finite intersection of primary submodules, $N = \bigcap_{i=1}^{n} N_i$.*

*Furthermore, if this decomposition is **minimal** (meaning the associated primes P_i are all distinct and the intersection is irredundant, i.e., $\bigcap_{j \neq i} N_j \not\subseteq N_i$ for all i), then:*

1. *The set of primes $\{P_1, \ldots, P_n\}$ is uniquely determined by N; it is precisely the set of associated primes $Ass(M/N)$.*
2. *The primary submodules N_i corresponding to the **minimal** primes in $Ass(M/N)$ are uniquely determined by N.*

Proof of Existence. A submodule $N \subsetneq M$ is called **irreducible** if it is not the intersection of two strictly larger submodules. Since M is a Noetherian module, any proper submodule N can be written as a finite intersection of irreducible submodules. So we can write $N = \bigcap_{i=1}^{n} N_i$ with each N_i irreducible. The existence of a primary decomposition then follows from the fact that in a finitely generated module over a Noetherian ring, every irreducible submodule is primary.

Let $N \subsetneq M$ be irreducible. Suppose for contradiction that $\text{Ass}(M/N)$ has at least two distinct primes, say P_1, P_2. Then there exist submodules L_1/N and L_2/N of M/N with $L_1/N \cong R/P_1$ and $L_2/N \cong R/P_2$. Since every non-zero element in L_1/N has annihilator P_1 and every non-zero element in L_2/N has annihilator P_2, their intersection must be trivial: $(L_1/N) \cap (L_2/N) = \{0\}$. In M, this means $L_1 \cap L_2 = N$. Since $L_1/N \neq 0$ and $L_2/N \neq 0$, we have $L_1 \supsetneq N$ and $L_2 \supsetneq N$. This expresses N as the intersection of two strictly larger submodules, contradicting its irreducibility. Thus $\text{Ass}(M/N)$ must contain only one element, so N is primary. □

Proof of Uniqueness Properties. Let $N = \bigcap_{i=1}^{n} N_i$ be a minimal primary decomposition. By factoring out N, we may assume $N = \{0\}$. The decomposition is $0 = \bigcap N_i$ where N_i is P_i-primary.

(1) **The set of primes is unique.** The canonical map $\phi : M \to \bigoplus_{i=1}^{n} M/N_i$ is injective, since $\text{Ker}(\phi) = \bigcap N_i = \{0\}$. This implies $\text{Ass}(M) \subseteq \text{Ass}(\bigoplus M/N_i) = \bigcup \text{Ass}(M/N_i) = \{P_1, \ldots, P_n\}$. For the reverse inclusion, let $L_j = \bigcap_{i \neq j} N_i$. Since the decomposition is irredundant, $L_j \neq \{0\}$. Also, $L_j \cap N_j = \{0\}$. Thus, $L_j \cong L_j/(L_j \cap N_j)$, which embeds into M/N_j. Since M/N_j is P_j-coprimary, its non-zero submodule L_j is also P_j-coprimary. Hence $\text{Ass}(L_j) = \{P_j\}$. As $L_j \subseteq M$, we have $\text{Ass}(L_j) \subseteq \text{Ass}(M)$, so $P_j \in \text{Ass}(M)$. This shows $\{P_1, \ldots, P_n\} \subseteq \text{Ass}(M)$, establishing equality.

(2) **The minimal components are unique.** Let P_i be a minimal prime in $\text{Ass}(M)$. We claim the corresponding primary component N_i is unique. We show it can be constructed directly from M and P_i as $N_i = \text{Ker}(M \to M_{P_i})$. Let's analyze the localization of the intersection $0 = \bigcap_{j=1}^{n} N_j$ at the minimal prime P_i.

$$\{0\} = \{0\}_{P_i} = \left(\bigcap_{j=1}^{n} N_j \right)_{P_i} = \bigcap_{j=1}^{n} (N_j)_{P_i}$$

For any $j \neq i$, since P_i is minimal, $P_j \not\subseteq P_i$. Thus we can choose an element $u \in P_j \setminus P_i$. Since M/N_j is P_j-coprimary, some power u^k annihilates M/N_j. Since $u \notin P_i$, u is a unit in R_{P_i}, so u^k is also a unit. This means $(M/N_j)_{P_i} = M_{P_i}/(N_j)_{P_i} = 0$, so $(N_j)_{P_i} = M_{P_i}$. The intersection thus collapses to $\{0\} = (N_i)_{P_i} \cap \bigcap_{j \neq i} M_{P_i} = (N_i)_{P_i}$. So, $(N_i)_{P_i} = \{0\}$. This means for any $m \in N_i$, its image $m/1$ is zero

in M_{P_i}, so $m \in \mathrm{Ker}(M \to M_{P_i})$. Conversely, let $m \in \mathrm{Ker}(M \to M_{P_i})$. This means there exists $u \in R \setminus P_i$ such that $um = 0$. Consider the image $\bar{m}$ of m in M/N_i. Then $u\bar{m} = 0$. Since M/N_i is P_i-coprimary and $u \notin P_i$, u is a non-zero-divisor on M/N_i. Thus we must have $\bar{m} = 0$, which means $m \in N_i$. This shows $N_i = \mathrm{Ker}(M \to M_{P_i})$, proving its uniqueness. □

Example 6.35.

1. *Let $I = (x^2y) \subseteq k[x, y]$. The minimal primes over I are (x) and (y). A minimal primary decomposition is $I = (x^2) \cap (y)$. Here, (x^2) is (x)-primary and (y) is (y)-primary. Since both associated primes are minimal, both components are unique. We can recover them as:*

$$(x^2) = Ker(R/I \to (R/I)_{(x)}), \quad (y) = Ker(R/I \to (R/I)_{(y)})$$

2. *Let $I = (x^2, xy) \subseteq k[x, y]$. The associated primes are (x) (minimal) and (x, y) (embedded). The (x)-primary component is unique: $N_{(x)} = Ker(R/I \to (R/I)_{(x)}) = (x)$. However, $(x) \neq I$. The primary decomposition $I = (x) \cap (x, y)^2$ shows how the embedded component is needed to recover the full ideal.*

Primary decomposition behaves predictably under localization; it filters the decomposition, keeping only the components corresponding to primes that survive the process.

Proposition 6.36. *Let $N = \bigcap_{i=1}^{n} N_i$ be a minimal primary decomposition of $N \subseteq M$. Let $U \subseteq R$ be a multiplicatively closed set. Let the indices be ordered such that $P_i \cap U = \emptyset$ for $i = 1, \ldots, t$ and $P_i \cap U \neq \emptyset$ for $i = t + 1, \ldots, n$. Then the localization of N in M_U has the minimal primary decomposition:*

$$N_U = \bigcap_{i=1}^{t} (N_i)_U$$

over the ring R_U.

Proof. By factoring out N, we can assume $N = \{0\}$. Localization commutes with finite intersections of submodules, so we have:

$$0 = \{0\}_U = \left(\bigcap_{i=1}^{n} N_i \right)_U = \bigcap_{i=1}^{n} (N_i)_U$$

If $P_i \cap U \neq \emptyset$ for $i > t$, there is an element $u \in P_i \cap U$. Since M/N_i is P_i-coprimary, some power u^k annihilates it. In R_U, $u/1$ is a unit, so $u^k/1$ is a unit. Since $u^k/1$ annihilates $(M/N_i)_U = M_U/(N_i)_U$, this module must be zero. This implies $(N_i)_U = M_U$. These terms are redundant in the intersection, which becomes $0 = \bigcap_{i=1}^{t} (N_i)_U$. For $i \leq t$, since $P_i \cap U = \emptyset$, $(N_i)_U$ is a $(P_i)_U$-primary submodule of M_U. The associated primes $\{(P_1)_U, \ldots, (P_t)_U\}$ are distinct, and it can be verified that the intersection remains irredundant. This gives the minimal primary decomposition of $\{0\}$ in M_U. □

6.1.5 Primary Decomposition and Localization

A key strength of primary decomposition is its compatibility with localization. This property provides a powerful tool for studying modules locally and then assembling the information to understand their global structure. It demonstrates that the decomposition of a module into its primary components behaves predictably when we restrict our attention to an open subset of $\mathrm{Spec}(R)$.

Throughout this section, we maintain the standing assumption that R **is a Noetherian ring** and M **is a finitely generated** R**-module**.

Proposition 6.37. *Let $N = \bigcap_{i=1}^{n} N_i$ be a minimal primary decomposition of a submodule $N \subseteq M$, with N_i being a P_i-primary submodule for each i. Let $U \subseteq R$ be a multiplicatively closed set. After reindexing, let $P_1, \ldots, P_t$ be the associated primes that do not intersect U (i.e., $P_i \cap U = \emptyset$), and let $P_{t+1}, \ldots, P_n$ be the primes that do intersect U (i.e., $P_i \cap U \neq \emptyset$).*

Then the localization of N in the R_U-module M_U, denoted N_U, has the minimal primary decomposition:

$$N_U = \bigcap_{i=1}^{t} (N_i)_U$$

Proof. To simplify the notation, we can factor out the submodule N. Consider the quotient module $\overline{M} = M/N$. The zero submodule $\{0\} \subseteq \overline{M}$ has the minimal primary decomposition $\{0\} = \bigcap_{i=1}^{n} (N_i/N)$. Proving the proposition for $N \subseteq M$ is equivalent to proving it for the zero submodule $\{0\} \subseteq \overline{M}$. Thus, without loss of generality, we assume $N = \{0\}$ and we have a minimal primary decomposition $0 = \bigcap_{i=1}^{n} N_i$ in the module M.

Localization is an exact functor, so it commutes with finite intersections of submodules. Applying the functor $(\cdot)_U$ to the decomposition gives:

$$\{0\} = \{0\}_U = \left(\bigcap_{i=1}^{n} N_i \right)_U = \bigcap_{i=1}^{n} (N_i)_U$$

This provides a decomposition of the zero submodule of M_U as an intersection of the localized submodules $(N_i)_U$. We must now analyze each of these components.

1. **Case 1:** Consider a prime P_i such that $P_i \cap U \neq \emptyset$, for $i \in \{t+1, \ldots, n\}$. By definition, N_i is a P_i-primary submodule of M, which means the quotient module M/N_i is P_i-coprimary. From our characterization of coprimary modules (Proposition 6.31), this implies that there exists an integer $k > 0$ such that $P_i^k \subseteq \operatorname{ann}(M/N_i)$. Since $P_i \cap U \neq \emptyset$, let u be an element in this intersection. Then $u \in P_i$, so $u^k \in P_i^k \subseteq \operatorname{ann}(M/N_i)$. This means u^k annihilates every element of M/N_i. When we localize, the element $u/1 \in R_U$ is a unit because $u \in U$. Since $u^k/1$ annihilates the localized module $(M/N_i)_U$, and $u^k/1$ is a unit, the module must be the zero module. Therefore, $(M/N_i)_U = M_U/(N_i)_U = \{0\}$, which implies that $(N_i)_U = M_U$.

2. **Case 2:** Consider a prime P_i such that $P_i \cap U = \emptyset$, for $i \in \{1, \ldots, t\}$. We know that N_i is P_i-primary in M. The associated primes of the localized module $(M/N_i)_U = M_U/(N_i)_U$ over the ring R_U are given by

   $$\operatorname{Ass}_{R_U}(M_U/(N_i)_U) = \{Q_U \mid Q \in \operatorname{Ass}_R(M/N_i) \text{ and } Q \cap U = \emptyset\}$$

   Since $\operatorname{Ass}_R(M/N_i) = \{P_i\}$ and we are in the case where $P_i \cap U = \emptyset$, it follows that

   $$\operatorname{Ass}_{R_U}(M_U/(N_i)_U) = \{(P_i)_U\}$$

   This shows that $(N_i)_U$ is a $(P_i)_U$-primary submodule of the R_U-module M_U.

Now, we substitute these findings back into our localized intersection:

$$\{0\} = \bigcap_{i=1}^{n} (N_i)_U = \left(\bigcap_{i=1}^{t} (N_i)_U \right) \cap \left(\bigcap_{i=t+1}^{n} (N_i)_U \right) = \left(\bigcap_{i=1}^{t} (N_i)_U \right) \cap \left(\bigcap_{i=t+1}^{n} M_U \right)$$

The intersection with M_U is redundant, so we are left with:

$$\{0\} = \bigcap_{i=1}^{t} (N_i)_U$$

This is a primary decomposition of the zero submodule in M_U. To show that it is *minimal*, we must verify that the primes $\{(P_1)_U, \ldots, (P_t)_U\}$ are distinct and that the intersection is irredundant. The map $P \mapsto P_U$ is a bijection between primes of R disjoint from U and primes of R_U. Since the original primes $P_1, \ldots, P_t$ were distinct, their localizations $(P_1)_U, \ldots, (P_t)_U$ are also distinct. The irredundancy of the localized decomposition can also be shown to be inherited from the irredundancy of the original. Thus, we have obtained the minimal primary decomposition of $\{0\}$ in M_U, as desired. □

6.2 Integrality and Other Important Lemmas

6.2.1 Cayley-Hamilton Theorem

The classical Cayley-Hamilton Theorem states that a square matrix over a field satisfies its own characteristic polynomial. This powerful result can be generalized from vector spaces to finitely generated modules over any commutative ring, where it becomes a foundational tool.

Theorem 6.38 (Cayley-Hamilton Theorem for Modules)**.** *Let R be a commutative ring, $I \subseteq R$ an ideal, and M an R-module generated by n elements. Let $\varphi : M \to M$ be an R-module homomorphism such that $\varphi(M) \subseteq IM$. Then φ satisfies a monic polynomial equation of the form:*

$$p(x) = x^n + p_1 x^{n-1} + \cdots + p_n$$

where each coefficient $p_j \in I^j$. As an endomorphism of M, $p(\varphi) = \varphi^n + p_1\varphi^{n-1} + \cdots + p_n \cdot id_M = 0$.

Proof. Let $m_1, \ldots, m_n$ be a set of generators for M. The condition $\varphi(M) \subseteq IM$ means that for each generator m_i, its image can be written as an I-linear combination of the generators. That is, for each $i \in \{1, \ldots, n\}$,

$$\varphi(m_i) = \sum_{j=1}^{n} a_{ij} m_j$$

for some coefficients $a_{ij} \in I$.

We can view M as an $R[x]$-module where the indeterminate x acts on M via the endomorphism φ; that is, for any $m \in M$, $x \cdot m := \varphi(m)$. The above equations can then be rewritten as:

$$\sum_{j=1}^{n} (\delta_{ij} x - a_{ij}) m_j = 0$$

where δ_{ij} is the Kronecker delta. Let $\mathbf{m}$ be the column vector of generators and let $\mathbf{A}$ be the $n \times n$ matrix (a_{ij}). The system of equations can be expressed in matrix form as $(x\mathbf{I} - \mathbf{A})\mathbf{m} = 0$.

Let $\mathbf{B}$ be the adjugate (classical adjoint) matrix of $(x\mathbf{I} - \mathbf{A})$. Standard linear algebra shows that $\mathbf{B}(x\mathbf{I} - \mathbf{A}) = \det(x\mathbf{I} - \mathbf{A})\mathbf{I}$. Multiplying the matrix equation on the left by $\mathbf{B}$, we get:

$$\det(x\mathbf{I} - \mathbf{A})\mathbf{I}\mathbf{m} = \mathbf{B}(x\mathbf{I} - \mathbf{A})\mathbf{m} = \mathbf{B} \cdot 0 = 0$$

This means that the endomorphism of M corresponding to multiplication by the polynomial $p(x) = \det(x\mathbf{I} - \mathbf{A})$ annihilates each generator m_i. Since the m_i generate M, the endomorphism $p(\varphi)$ must be the zero map on all of M.

Finally, we check the coefficients of $p(x)$. The determinant is a sum of products of entries of the matrix $(x\mathbf{I} - \mathbf{A})$. The coefficient p_j of x^{n-j} is, up to sign, the sum of the principal $j \times j$ minors of $\mathbf{A}$. Since every entry a_{ij} of $\mathbf{A}$ is in the ideal I, any product of j such entries must lie in I^j. Therefore, $p_j \in I^j$ for each j, as required. □

While stated for general modules, this theorem has particularly strong consequences for free modules, which are the closest analogues of vector spaces over fields.

Definition 6.39. *An R-module F is **free** if it has a **free basis**, which is a subset $B \subseteq F$ such that every element of F can be written uniquely as an R-linear combination of elements of B. This is equivalent to saying that for any distinct elements $b_1, \ldots, b_n \in B$, the relation $\sum a_i b_i = 0$ implies all coefficients a_i are zero. A free module with a finite basis of size n is isomorphic to R^n.*

Corollary 6.40. *Let R be a ring and M a finitely generated R-module.*

1. *A surjective R-module homomorphism $\alpha : M \to M$ is an isomorphism.*

2. *If $M \cong R^n$ is a free module of rank n, then any set of n elements that generate M is a free basis. In particular, the rank of a free module is well-defined.*

Proof. (1) We view M as an $R[t]$-module, where t acts as α. Since α is surjective, we have $\alpha(M) = M$. Let $I = (t) \subseteq R[t]$. Then $IM = M$. We apply the Cayley-Hamilton theorem to the identity map $\varphi = \mathrm{id}_M : M \to M$. Since $\mathrm{id}_M(M) = M = IM$, there exists a polynomial $p(x) = x^n + p_1 x^{n-1} + \cdots + p_n$ with $p_j \in I^j = (t^j)$ such that $p(\mathrm{id}_M) = 0$. So, $p_j = c_j t^j$ for some $c_j \in R[t]$. Evaluating the polynomial at id_M and remembering that t acts as α, we get:

$$(\mathrm{id}_M + c_1\alpha + c_2\alpha^2 + \cdots + c_n\alpha^n)(m) = 0 \quad \text{for all } m \in M.$$

Factoring out α, we can write this as $(\mathrm{id}_M + \alpha \circ q(\alpha)) = 0$, where $q(\alpha) = c_1\mathrm{id}_M + c_2\alpha + \cdots + c_n\alpha^{n-1}$. This gives $\alpha \circ (-q(\alpha)) = \mathrm{id}_M$, showing that α has a right inverse and is therefore an isomorphism.

(2) Let $m_1, \ldots, m_n$ be a set of generators for M. We can define a surjective homomorphism $\beta : R^n \to M$ by sending the i-th standard basis vector of R^n to m_i. Since M is free of rank n, there is also an isomorphism $\gamma : M \to R^n$. The composition $\gamma \circ \beta : R^n \to R^n$ is a surjective endomorphism of a finitely generated module, so by part (1), it is an isomorphism. This implies that its kernel is trivial. The kernel of $\gamma \circ \beta$ is precisely the kernel of β, since γ is an isomorphism. Therefore, β is an isomorphism, which means that the generators $m_1, \ldots, m_n$ must be linearly independent and thus form a free basis.

To see that the rank is well-defined, suppose $R^m \cong R^n$ and, without loss of generality, $m < n$. Let $\{e_1, \ldots, e_m\}$ be a free basis for R^m. Under the isomorphism, these map to m elements in R^n which generate R^n. We can form a set of n generators for R^n by taking these m elements and augmenting the set with $n - m$ copies of the zero vector. This gives a set of n generators for R^n which is manifestly not a free basis, contradicting what we just proved. Hence, we must have $m = n$. □

Remark 6.41. *The process of creating a new ring by imposing a polynomial relation on an element is fundamental. For a polynomial $p \in R[x]$, the quotient ring $R[x]/(p)$ can be thought of as adjoining an element to R that is a "root" of p. A related construction is localization: adjoining an inverse to an element $a \in R$ is equivalent to forming the quotient ring $R[x]/(ax - 1)$, where x represents the inverse of a.*

The Cayley-Hamilton theorem gives a precise characterization of when such quotient rings are finite over the base ring.

Proposition 6.42. *Let R be a ring, $J \subseteq R[x]$ an ideal, and let $S = R[x]/J$. Let s be the image of x in S.*

1. *S is generated by at most n elements as an R-module if and only if J contains a monic polynomial of degree n. In this case, S is generated by $\{1, s, \ldots, s^{n-1}\}$.*
2. *S is a finitely generated free R-module of rank n if and only if J can be generated by a single monic polynomial of degree n. In this case, $\{1, s, \ldots, s^{n-1}\}$ is a free basis.*

Proof. (1) ($\Leftarrow$) Suppose J contains a monic polynomial $p(x) = x^n + r_1 x^{n-1} + \cdots + r_n$. In S, this relation becomes $p(s) = 0$, so $s^n = -(r_1 s^{n-1} + \cdots + r_n)$. Any higher power s^d for $d \geq n$ can be inductively reduced to an R-linear combination of $\{1, s, \ldots, s^{n-1}\}$. Since $\{1, s, s^2, \ldots\}$ generates S as an R-module, this shows that $\{1, s, \ldots, s^{n-1}\}$ is a generating set.

($\Rightarrow$) Suppose S is generated by n elements as an R-module. Let $\varphi : S \to S$ be the R-module homomorphism given by multiplication by s. Since $\varphi(S) = sS \subseteq S$, we can apply the Cayley-Hamilton theorem with $I = R$. This guarantees the existence of a monic polynomial $p(x)$ of degree n with coefficients in R such that $p(\varphi) = 0$. Acting on $1 \in S$, we get $p(s) \cdot 1 = p(s) = 0$. This means $p(x) \in J$.

(2) ($\Leftarrow$) Suppose $J = (p)$ where p is monic of degree n. By (1), S is generated by $\{1, s, \ldots, s^{n-1}\}$. To show this is a free basis, suppose there is a relation $\sum_{i=0}^{n-1} a_i s^i = 0$ for $a_i \in R$. This means the polynomial $q(x) = \sum a_i x^i$ is in J. So $q(x)$ must be a multiple of $p(x)$. But $\deg(q) < n = \deg(p)$, so this is only possible if $q(x) = 0$, which means all $a_i = 0$.

($\Rightarrow$) Suppose S is a free R-module of rank n. By (1), there is a monic polynomial $p \in J$ of degree n. This implies that $\{1, s, \ldots, s^{n-1}\}$ generates S. Since S is free of rank n, this set must be a free basis. We claim $J = (p)$. Let $f \in J$ be any polynomial. By the division algorithm for monic polynomials, we can write $f = qp + r$ where $\deg(r) < n$. Since $f \in J$ and $p \in J$, the remainder r must also be in J. But if $r(x) = \sum c_i x^i$ is in J, then $r(s) = \sum c_i s^i = 0$ in S. As $\{1, s, \ldots, s^{n-1}\}$ is a basis, this implies all $c_i = 0$, so $r = 0$. Thus $f = qp$, which shows $J = (p)$. □

6.2.2 R-Algebras and Integrality

The appearance of monic polynomials in the Cayley-Hamilton theorem motivates the study of a special class of ring extensions defined by such polynomials. This leads to the fundamental concept of integrality.

Definition 6.43. *An R-**algebra** is a ring S equipped with a ring homomorphism $\phi : R \to S$. This structure makes S an R-module where the action is defined by $r \cdot s := \phi(r)s$.*

Definition 6.44. *An element $s \in S$ is **integral** over R if it is a root of a monic polynomial with coefficients in R. If every element of S is integral over R, then S is an **integral extension** of R. The set of elements in S integral over R is the **integral closure** of R in S. If R is an integral domain, its integral closure in its field of fractions is called the **normalization** of R.*

Geometrically, normalizing a ring corresponds to resolving singularities of the associated algebraic variety. For instance, the normalization of an algebraic curve is always a smooth curve.

Definition 6.45. *An R-algebra S is **finite** over R if it is finitely generated as an R-module.*

The following examples illustrate the distinctions between these concepts.

Example 6.46.
1. *The polynomial ring $R[x]$ is a finitely generated R-algebra, but it is not a finite R-module, and the element x is not integral over R. This is the canonical example of an algebra that is finitely generated but not finite.*
2. *The quotient ring $R[x]/(x^2)$ is finite over R (generated as a module by $\{1, \bar{x}\}$) and every element is integral over R.*
3. *The ring $\mathbb{Q}[\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots]$ is an integral extension of $\mathbb{Q}$ (as each generator is integral), but it is not a finite $\mathbb{Q}$-module.*

The relationship between finiteness and integrality is captured precisely in the following proposition.

Proposition 6.47. *An R-algebra S is finite over R if and only if S is generated as an R-algebra by a finite number of integral elements.*

Proof. ($\Rightarrow$) If S is finite over R, let $s \in S$. Multiplication by s is an R-linear map $\varphi_s : S \to S$. By the Cayley-Hamilton theorem, s is integral over R. Since this holds for all $s \in S$, S is generated by integral elements (namely, its finite set of module generators). ($\Leftarrow$) Let $S = R[s_1, \ldots, s_n]$ where each s_i is integral. We proceed by induction on n. The base case $n = 1$, $S = R[s_1]$, is finite over R because the monic relation for s_1 allows any power of s_1 to be reduced to a linear combination of lower powers. For the inductive step, let $R' = R[s_1, \ldots, s_{n-1}]$. By induction, R' is finite over R. Then $S = R'[s_n]$. Since s_n is integral over R, it is also integral over R'. By the base case, S is finite over R'. Since a finite extension of a finite extension is finite, S is finite over R. □

The next result gives another powerful criterion for checking integrality, which will be used to show that integral elements form a subring.

Proposition 6.48. *If S is an R-algebra and $s \in S$, then s is integral over R if and only if there exists a faithful S-module N and a finitely generated R-submodule $M \subseteq N$ such that $sM \subseteq M$. In particular, s is integral over R if and only if $R[s]$ is a finitely generated R-module.*

Proof. The final sentence follows from the main statement by taking $S = R[s]$ and $M = N = R[s]$. If s is integral, we have shown $R[s]$ is finite over R. If $R[s]$ is finite over R, we can take $M = R[s]$, which is faithful as an $R[s]$-module, and $sM \subseteq M$.

Now we prove the main statement. ($\Rightarrow$) Assume s is integral. Take $N = S$ and $M = R[s]$. Since s is integral, $R[s]$ is a finite R-module. Also $sM = sR[s] \subseteq R[s] = M$. As $1 \in M$, M is faithful as an S-module. ($\Leftarrow$) Let $\varphi : M \to M$ be multiplication by s. Since $sM \subseteq M$, this is a well-defined R-linear map. By Cayley-Hamilton with $I = R$, there is a monic polynomial $p(x)$ with coefficients in R such that $p(s)$ annihilates M. Since M is a faithful S-module, we must have $p(s) = 0$. Thus s is integral. □

This criterion makes the proof that integral elements form a subring almost immediate.

Theorem 6.49. *Let S be an R-algebra. The set of all elements of S integral over R is a subalgebra of S.*

Proof. Let $a, b \in S$ be integral over R. We want to show $a + b$ and ab are integral. The ring $R[a, b]$ is an R-algebra generated by two integral elements, so by Proposition 6.47 it is a finite R-module. Let $s = a+b$ or $s = ab$. In either case, $s \in R[a, b]$. Let $M = R[a, b]$ and $N = S$. Then M is a finitely generated R-submodule of N, it is faithful as an S-module (since $1 \in M$), and $sM \subseteq M$. By the previous proposition, s is integral over R. □

6.2.3 Nakayama's Lemma

We conclude with one of the most versatile and important results in commutative algebra. It is a direct and powerful consequence of the Cayley-Hamilton theorem. We first isolate the key ingredient.

Corollary 6.50 (of Cayley-Hamilton)**.** *Let M be a finitely generated R-module and I an ideal of R. If $IM = M$, then there exists an element $r \in I$ such that $(1 - r)M = 0$.*

Proof. Apply the Cayley-Hamilton theorem to $\varphi = \mathrm{id}_M : M \to M$. The hypothesis $IM = M$ allows this. The theorem yields $p_1, \ldots, p_n$ with $p_j \in I^j \subseteq I$ such that $(\mathrm{id}^n + p_1\mathrm{id}^{n-1} + \cdots + p_n\mathrm{id})M = 0$. This is equivalent to $(1 + p_1 + \cdots + p_n)M = 0$. Let $r' = p_1 + \cdots + p_n \in I$. Then $(1 + r')M = 0$. Setting $r = -r' \in I$ gives $(1 - r)M = 0$. □

This result is most powerful when the ideal I is contained in the Jacobson radical.

Definition 6.51. *The **Jacobson radical** of a ring R, denoted $J(R)$, is the intersection of all maximal ideals of R.*

Remark 6.52. *The Jacobson radical contains the nilradical (the intersection of all prime ideals), but they need not coincide. For example, in the local ring $R = k[x, y]_{(x,y)}$, the Jacobson radical is the maximal ideal $(x, y)R$, but the nilradical is $\{0\}$.*

Lemma 6.53 (Nakayama's Lemma)**.** *Let I be an ideal contained in the Jacobson radical of R, and let M be a finitely generated R-module.*

1. *If $IM = M$, then $M = 0$.*
2. *If $m_1, \ldots, m_n \in M$ have images in M/IM that generate it as an R-module, then $m_1, \ldots, m_n$ generate M as an R-module.*

Proof. (1) If $IM = M$, Corollary 6.50 gives an element $r \in I$ such that $(1 - r)M = 0$. Since $r \in I \subseteq J(R)$, r belongs to every maximal ideal of R. Therefore, $1 - r$ cannot belong to any maximal ideal, so $1 - r$ must be a unit. Multiplying $(1 - r)M = 0$ by $(1 - r)^{-1}$ yields $M = 0$.

(2) Let N be the submodule of M generated by $\{m_1, \ldots, m_n\}$. The hypothesis means $M = N + IM$. Consider the quotient module $\overline{M} = M/N$. Then $\overline{M} = (N + IM)/N = I(M/N) = I\overline{M}$. Since M is finitely generated, so is $\overline{M}$. By part (1), since $I\overline{M} = \overline{M}$, we must have $\overline{M} = 0$. This means $M/N = 0$, so $M = N$. □

Remark 6.54. *The hypothesis that M is finitely generated is essential. Part (2) cannot be used to prove that a module is finitely generated. It only allows one to lift a generating set from the quotient M/IM to M itself.*

Corollary 6.55. *Let R be a ring, and let M, N be finitely generated R-modules. If $M \otimes_R N = 0$, then $ann(M) + ann(N) = R$. If R is a local ring, this implies that either $M = 0$ or $N = 0$.*

Proof. First, assume R is a local ring with maximal ideal $\mathfrak{m} = J(R)$. Suppose $M \neq 0$ and $N \neq 0$. Since M is finitely generated, Nakayama's Lemma implies $M/\mathfrak{m}M \neq 0$. This quotient is a non-zero vector space over the field $R/\mathfrak{m}$. Similarly, $N/\mathfrak{m}N \neq 0$. We have a surjection of $R/\mathfrak{m}$-vector spaces:

$$(M \otimes_R N) \otimes_R (R/\mathfrak{m}) \cong (M/\mathfrak{m}M) \otimes_{R/\mathfrak{m}} (N/\mathfrak{m}N) \twoheadrightarrow 0.$$

Since the tensor product of two non-zero vector spaces over a field is non-zero, this contradicts the hypothesis that $M \otimes_R N = 0$. Thus, either $M = 0$ or $N = 0$.

Now, let R be any ring. Suppose for contradiction that $\text{ann}(M) + \text{ann}(N) \neq R$. Then this sum is contained in some maximal ideal P. Let's localize at P. The localized modules M_P and N_P are modules over the local ring R_P. We have $(M \otimes_R N)_P \cong M_P \otimes_{R_P} N_P = 0$. If we can show that $M_P \neq 0$ and $N_P \neq 0$, the local case will give a contradiction. Suppose $M_P = 0$. Since M is finitely generated, this implies there exists an element $s \in R \setminus P$ such that $sM = 0$. This means $s \in \text{ann}(M)$. But we assumed $\text{ann}(M) \subseteq P$, which is a contradiction to $s \notin P$. Thus $M_P \neq 0$. Similarly, $N_P \neq 0$. This completes the proof. □

6.3 Normality and its Consequences

6.3.1 Normal Rings and Normalization

We now focus on an important class of rings that arise naturally in both number theory and geometry. The concept of normality provides an algebraic abstraction of the desirable property of a space having no "unnecessary" singularities. Recall the following definition:

Definition 6.56. *An integral domain R is said to be **normal** if it is integrally closed in its field of fractions. That is, any element of the fraction field of R that is a root of a monic polynomial with coefficients in R must itself be an element of R.*

A large and important class of normal rings comes from rings with unique factorization.

Proposition 6.57. *Every Unique Factorization Domain (UFD) is a normal ring.*

Proof. Let R be a UFD and let K be its field of fractions. Consider an element $\alpha = r/s \in K$, with $r, s \in R$ and $s \neq 0$. Since R is a UFD, we can cancel common factors and assume that r and s are relatively prime. Suppose that α is integral over R. Then it satisfies a monic polynomial equation:

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

for some $a_1, \ldots, a_n \in R$. Multiplying by s^n to clear the denominators, we obtain:

$$r^n + a_1 r^{n-1} s + \cdots + a_{n-1} r s^{n-1} + a_n s^n = 0$$

We can rearrange this equation to solve for r^n:

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

The right-hand side is a multiple of s, so we conclude that s divides r^n. However, we assumed that r and s were relatively prime. In a UFD, if s divides a product and shares no common factors with one term (r), it must divide the other. By induction, if s divides r^n and is relatively prime to r, s must be a unit in R. If s is a unit, then its inverse s^{-1} is in R, which means the element $\alpha = rs^{-1}$ is an element of R. This shows that any element of K integral over R is already in R, so R is normal. □

Since the ring of integers $\mathbb{Z}$ is a UFD, we immediately have a classical result from number theory.

Corollary 6.58 (Rational Root Theorem)**.** *The ring of integers $\mathbb{Z}$ is normal. Consequently, the only rational numbers that are roots of a monic polynomial with integer coefficients are the integers themselves.*

Normality is also well-behaved with respect to forming polynomial rings, a much deeper result.

Corollary 6.59. *If R is a normal domain, then the polynomial ring $R[x_1, \ldots, x_n]$ is also a normal domain.*

Sketch. The proof is non-trivial. One typically proves by induction that if R is normal, then $R[x]$ is normal. The key step involves showing that if an element $f/g \in \mathrm{Frac}(R[x])$ is integral over $R[x]$, it must also be integral over R, which then implies it must be in $R[x]$ since R is normal. This step often relies on a version of Gauss's Lemma for monic polynomials. □

6.3.2 Normality and Polynomial Rings

The connection between integrality and polynomial factorization is deep. Suppose we have rings $R \subseteq S$. If a monic polynomial $f \in R[x]$ has a root $\alpha \in S$, we know that $(x - \alpha)$ divides f in $S[x]$. A more general statement holds for factors of any degree.

Proposition 6.60 (Gauss's Lemma for Monic Polynomials)**.** *Let $R \subseteq S$ be an extension of rings and let $f \in R[x]$ be a monic polynomial. If f factors in $S[x]$ as a product of monic polynomials, $f = gh$, then the coefficients of the factors g and h are integral over R.*

Remark 6.61. *This proposition is a powerful generalization of the classical Gauss's Lemma. If we take $R = \mathbb{Z}$ and $S = \mathbb{Q}$, the proposition states that if a monic polynomial in $\mathbb{Z}[x]$ factors into monic polynomials in $\mathbb{Q}[x]$, then the coefficients of the factors must be integral over $\mathbb{Z}$. But since $\mathbb{Z}$ is normal, these coefficients must be integers. This recovers the result that if a monic integer polynomial is reducible in $\mathbb{Q}[x]$, it is reducible in $\mathbb{Z}[x]$.*

Proof. Let $f = gh$, where $f \in R[x]$ and $g, h \in S[x]$ are all monic. There exists a larger ring extension T of S in which g and h split into linear factors:

$$g(x) = \prod(x - \alpha_i) \quad \text{and} \quad h(x) = \prod(x - \beta_j) \quad \text{in } T[x].$$

The roots $\{\alpha_i\}$ and $\{\beta_j\}$ are also the roots of $f(x)$. Since f is a monic polynomial with coefficients in R, all of its roots are integral over R by definition. The coefficients of g and h are the elementary symmetric polynomials in their respective roots (up to sign). For instance, the coefficient of x^k in $g(x)$ is a polynomial with integer coefficients in the α_i. The set of elements integral over R forms a subring. Since each α_i and β_j is integral over R, any polynomial expression in them is also integral over R. Therefore, the coefficients of g and h are integral over R. □

This has an important consequence for the ideal structure of polynomial rings over normal domains.

Corollary 6.62. *If R is a normal domain, then any monic irreducible polynomial $f \in R[x]$ generates a prime ideal.*

Proof. Let R be a normal domain with field of fractions Q. Let $f \in R[x]$ be a monic irreducible polynomial. First, we claim that f is also irreducible in $Q[x]$. Suppose for contradiction that $f = gh$ for some $g, h \in Q[x]$ of smaller degree. Since f is monic, we can scale g and h to be monic as well. By the previous proposition (with $S = Q$), the coefficients of g and h must be integral over R. But R is normal, so these coefficients must lie in R. This means $f = gh$ is a factorization in $R[x]$, which contradicts the irreducibility of f in $R[x]$. Thus, f is irreducible in $Q[x]$.

Since Q is a field, the polynomial ring $Q[x]$ is a UFD. In a UFD, irreducible elements generate prime ideals. Therefore, the ideal (f) is prime in $Q[x]$, which means the quotient ring $Q[x]/(f)$ is an integral domain.

Now consider the quotient ring $R[x]/(f)$. Because f is monic of degree n, this is a free R-module with basis $\{1, \bar{x}, \ldots, \bar{x}^{n-1}\}$. Consider the natural map:

$$\phi : R[x]/(f) \to Q \otimes_R (R[x]/(f)) \cong Q[x]/(f)$$

This is a map from an R-module to a Q-vector space. Since $R[x]/(f)$ is a free R-module, it is torsion-free. The kernel of the map $M \to Q \otimes_R M$ consists of the R-torsion submodule of M. As $R[x]/(f)$ is torsion-free, the map ϕ is injective. We have shown that $R[x]/(f)$ is a subring of the integral domain $Q[x]/(f)$. Therefore, $R[x]/(f)$ must itself be an integral domain. This means that the ideal (f) is a prime ideal in $R[x]$. □

6.3.3 Normalization and Geometry

An essential property of normalization is that it is a "local" property: a ring is normal if and only if all of its localizations at prime ideals are normal. More generally, the process of taking the integral closure commutes with localization.

This is geometrically significant. In algebraic geometry, localizing a ring at a multiplicative set corresponds to restricting attention to an open subset of the associated scheme. The following proposition says that we can normalize a scheme by normalizing the affine patches that cover it and then gluing them back together, and the gluing maps will remain compatible.

Proposition 6.63. *Let $R \subseteq S$ be an extension of rings, and let $U \subseteq R$ be a multiplicatively closed subset. Let S' be the integral closure of R in S. Then $S'_U = S'[U^{-1}]$ is the integral closure of $R_U = R[U^{-1}]$ in $S_U = S[U^{-1}]$.*

Proof. First, we show that S'_U is integral over R_U. Let $s'/u \in S'_U$, where $s' \in S'$ and $u \in U$. By definition, s' satisfies a monic polynomial equation with coefficients in R:

$$(s')^n + r_1(s')^{n-1} + \cdots + r_n = 0$$

Dividing by u^n, we get:

$$(s'/u)^n + (r_1/u)(s'/u)^{n-1} + \cdots + (r_n/u^n) = 0$$

This is a monic polynomial equation for s'/u with coefficients in R_U. Thus every element of S'_U is integral over R_U.

Conversely, we must show that any element of S_U that is integral over R_U is contained in S'_U. Let $s/u \in S_U$ (with $s \in S, u \in U$) be integral over R_U. It satisfies an equation:

$$(s/u)^n + (r_1/u_1)(s/u)^{n-1} + \cdots + (r_n/u_n) = 0$$

where $r_i \in R, u_i \in U$. Let $v = u_1 u_2 \cdots u_n \in U$. We can multiply the entire equation by $(uv)^n$ to clear all denominators:

$$(sv)^n + (r_1 uv/u_1)(sv)^{n-1} + \cdots + (r_n u^n v^n/u_n) = 0$$

Each coefficient $(r_i u^i v^i/u_i)$ is an element of R. This equation shows that the element $sv \in S$ is a root of a monic polynomial with coefficients in R. Therefore, sv is integral over R, so $sv \in S'$. Then the original element s/u can be written as:

$$s/u = (sv)/(uv)$$

Since $sv \in S'$ and $uv \in U$, this shows that $s/u \in S'_U$. This completes the proof. □

The geometric meaning of normalization is best understood through an example.

Example 6.64. *Consider the nodal cubic curve defined by the polynomial $f = y^2 - x^2(x+1)$ in $\mathbb{C}[x, y]$. The coordinate ring of this curve is $R = \mathbb{C}[x, y]/(f)$. This ring consists of polynomial functions restricted to the curve. Geometrically, the curve $\mathcal{V}(f)$ has a self-intersection (a "node") at the origin.*

This ring R is not normal. To see this, consider the element $t = y/x$ in the field of fractions of R. On the curve, we have $y^2 = x^2(x+1)$, so $(y/x)^2 = x+1$. Rearranging this gives:

$$t^2 - (x+1) = 0$$

This is a monic polynomial equation for t with coefficients in R. Thus, $t = y/x$ is integral over R. However, t is not an element of R itself (it's not a polynomial function), so R is not integrally closed and hence not normal.

What is the geometric meaning of the element y/x? Away from the origin $(x, y) = (0, 0)$, it is a well-defined rational function. Near the origin, the curve has two distinct branches. The tangent lines at the origin are given by $y^2 - x^2 = 0$, or $y = \pm x$. If we approach the origin along the branch where $y \approx x$, the limit of the function y/x is 1. If we approach the origin along the branch where $y \approx -x$, the limit of y/x is -1. The function y/x does not have a single well-defined value at the singular point.

The normalization of R is the ring $R' = R[y/x] \cong \mathbb{C}[x, y, t]/(y^2 - x^2(x+1), t - y/x)$. One can show this is isomorphic to $\mathbb{C}[t^2-1, t(t^2-1)] \cong \mathbb{C}[t]$. The ring $\mathbb{C}[t]$ is the coordinate ring of a simple line, which is smooth. The normalization process has "separated" the two branches of the curve at the node. Geometrically, the normalization creates a new smooth curve that maps to the original singular curve. This map is a bijection everywhere except at the singular point, where two points on the smooth curve map to the single node on the original curve. The integral element y/x becomes a coordinate function on this new smooth curve, and its two different limiting values correspond to its values at the two distinct points lying over the singularity.

6.3.4 The Lying Over and Going Up Theorems

Given an integral ring extension $R \subseteq S$, we wish to understand the relationship between their respective prime ideal spectra, Spec$S$ and Spec$R$. This relationship is described by a series of fundamental results, beginning with the Lying Over and Going Up theorems.

Theorem 6.65 (Lying Over Theorem)**.** *Suppose $R \subseteq S$ is an integral extension of rings. For any prime ideal $\mathfrak{p} \subseteq R$, there exists a prime ideal $\mathfrak{q} \subseteq S$ such that $\mathfrak{q} \cap R = \mathfrak{p}$.*

A more general version of this theorem, often called the Going Up theorem, allows us to lift chains of prime ideals.

Theorem 6.66 (Going Up Theorem)**.** *Suppose $R \subseteq S$ is an integral extension. Let $\mathfrak{p} \subseteq R$ be a prime ideal. Then for any ideal $I \subseteq S$ satisfying $I \cap R \subseteq \mathfrak{p}$, there exists a prime ideal $\mathfrak{q} \subseteq S$ such that $\mathfrak{q} \supseteq I$ and $\mathfrak{q} \cap R = \mathfrak{p}$.*

Proof. By passing to the quotient rings $R/(I \cap R)$ and S/I, we can reduce to the case where $I = \{0\}$ and $I \cap R = \{0\}$. Our goal is then to prove the Lying Over theorem: for a prime $\mathfrak{p} \subseteq R$, there exists a prime $\mathfrak{q} \subseteq S$ with $\mathfrak{q} \cap R = \mathfrak{p}$.

Let $U = R \setminus \mathfrak{p}$ be the multiplicative set. We consider the localized rings $R_\mathfrak{p}$ and $S_U = S[U^{-1}]$. The extension $R_\mathfrak{p} \subseteq S_U$ is still integral. Now, $R_\mathfrak{p}$ is a local ring with maximal ideal $\mathfrak{p}R_\mathfrak{p}$. We need to show that there exists a prime ideal in S_U that lies over $\mathfrak{p}R_\mathfrak{p}$. Let $\mathfrak{m}$ be any maximal ideal of S_U. Then $\mathfrak{m} \cap R_\mathfrak{p}$ is a prime ideal of $R_\mathfrak{p}$, which must be $\mathfrak{p}R_\mathfrak{p}$ since it is the unique maximal ideal.

It suffices to show that S_U is not the zero ring, which is equivalent to showing that $\mathfrak{p}S \neq S$. Suppose for contradiction that $\mathfrak{p}S = S$. Then we can write $1 = \sum_{i=1}^n p_i s_i$ for some $p_i \in \mathfrak{p}$ and $s_i \in S$. Let $S' \subseteq S$ be the R-subalgebra generated by $\{s_1, \ldots, s_n\}$. Since S' is generated by elements integral over R, S' is a finitely generated R-module. We have $1 \in \mathfrak{p}S'$, which implies $\mathfrak{p}S' = S'$. By Nakayama's Lemma, since S' is a finitely generated R-module, this implies $S' = \{0\}$, a contradiction. Thus $\mathfrak{p}S \neq S$, and the theorem holds. □

The Lying Over theorem implies that the induced map on spectra, Spec$S \to$ Spec$R$, is surjective. However, we do require integrality for this:

Example 6.67. *Consider the ring homomorphism $\varphi : k[t] \to k[x, y]/(xy - 1)$ defined by $t \mapsto x$. This makes $k[t]$ a subring of $S = k[x, y]/(xy - 1) \cong k[x, x^{-1}]$. This extension is not integral. The corresponding map*

SpecS → Speck[t] is not surjective. For example, the maximal ideal $(t) \subseteq k[t]$ is not in the image. Any prime in the image is of the form $(x-a) \cap k[t] = (t-a)$ for $a \in k^\times$, so (t) is missed.

A direct application of the Going Up theorem allows us to lift chains of prime ideals.

Corollary 6.68 (Classical "Going Up")**.** *Let $R \subseteq S$ be an integral extension. If $\mathfrak{p}_0 \subseteq \mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_d$ is a chain of prime ideals in R, then there exists a chain of prime ideals $\mathfrak{q}_0 \subseteq \mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_d$ in S such that $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ for all i.*

Proof. We construct the chain inductively. By the Lying Over Theorem (6.65), there exists a prime $\mathfrak{q}_0$ in S with $\mathfrak{q}_0 \cap R = \mathfrak{p}_0$. Now, assume we have constructed a chain $\mathfrak{q}_0 \subseteq \cdots \subseteq \mathfrak{q}_{i-1}$ lying over $\mathfrak{p}_0 \subseteq \cdots \subseteq \mathfrak{p}_{i-1}$. Consider the integral extension $R/\mathfrak{p}_{i-1} \subseteq S/\mathfrak{q}_{i-1}$. Applying the Lying Over theorem to the prime ideal $\mathfrak{p}_i/\mathfrak{p}_{i-1} \subseteq R/\mathfrak{p}_{i-1}$, we find a prime ideal in $S/\mathfrak{q}_{i-1}$ lying over it. Its preimage in S is a prime ideal $\mathfrak{q}_i \supseteq \mathfrak{q}_{i-1}$ such that $\mathfrak{q}_i \cap R = \mathfrak{p}_i$. □

Remark 6.69. *A corresponding "Going Down" theorem, which allows for the downward lifting of prime ideal chains, holds under stronger hypotheses (e.g., if R is a normal domain and S is a domain).*

We can now deduce several important structural consequences of integral extensions.

Lemma 6.70. *Let $R \subseteq S$ be an extension of integral domains. If S is integral over R, then any nonzero ideal of S has a nonzero intersection with R.*

Proof. Let $b \in S$, $b \neq 0$. Since S is integral over R, b satisfies a monic polynomial equation with coefficients in R:

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0, \quad a_i \in R.$$

We can choose this polynomial to be of minimal degree, which ensures $a_0 \neq 0$ (otherwise, we could factor out b and get a smaller degree polynomial, since S is a domain). Rearranging, we have $a_0 = -b(b^{n-1} + \cdots + a_1)$. This shows that $0 \neq a_0 \in (b) \cap R$. Thus, the principal ideal (b) has a nontrivial intersection with R, which suffices to prove the lemma. □

Corollary 6.71. *Let $R \subseteq S$ be an integral extension of domains. Then S is a field if and only if R is a field.*

Proof. ($\Rightarrow$) Suppose R is a field. Let $b \in S$, $b \neq 0$. Since S is integral over $R = k$, $k[b]$ is a finite-dimensional k-vector space. As $k[b]$ is a domain, it must be a field. Thus b has an inverse in $k[b] \subseteq S$. So, S is a field.

($\Leftarrow$) Suppose S is a field. Let $\mathfrak{m} \subseteq R$ be a maximal ideal. By the Lying Over theorem, there exists a prime ideal $\mathfrak{q} \subseteq S$ such that $\mathfrak{q} \cap R = \mathfrak{m}$. Since S is a field, its only prime ideal is $\{0\}$. Thus $\mathfrak{q} = \{0\}$, which implies $\mathfrak{m} = \{0\}$. A ring whose only maximal ideal is the zero ideal must be a field. Thus R is a field. □

Remark 6.72. *If $\mathfrak{p} \subseteq S$ is a prime ideal in an integral extension $R \subseteq S$, then $R/(\mathfrak{p} \cap R) \subseteq S/\mathfrak{p}$ is also an integral extension. By Corollary 6.71, $S/\mathfrak{p}$ is a field if and only if $R/(\mathfrak{p} \cap R)$ is a field. This means a prime ideal $\mathfrak{p} \subseteq S$ is maximal if and only if its contraction $\mathfrak{p} \cap R$ is maximal in R.*

Finally, we show that distinct prime ideals in an integral extension cannot lie over the same prime ideal.

Corollary 6.73 (Incomparability)**.** *Let $R \subseteq S$ be an integral extension. If $\mathfrak{q} \subseteq \mathfrak{q}'$ are prime ideals of S such that $\mathfrak{q} \cap R = \mathfrak{q}' \cap R$, then $\mathfrak{q} = \mathfrak{q}'$.*

Proof. Let $\mathfrak{p} = \mathfrak{q} \cap R = \mathfrak{q}' \cap R$. We pass to the quotient rings $R' = R/\mathfrak{p}$ and $S' = S/\mathfrak{q}$. The extension $R' \subseteq S'$ is an integral extension of domains. The ideal $\mathfrak{q}'/\mathfrak{q}$ is a prime ideal in S' and its intersection with R' is $(\mathfrak{q}' \cap R)/\mathfrak{p} = \mathfrak{p}/\mathfrak{p} = \{0\}$. By Lemma 6.70, any nonzero ideal in S' must have a nonzero intersection with R'. Since the intersection is zero, we must have $\mathfrak{q}'/\mathfrak{q} = \{0\}$, which implies $\mathfrak{q}' = \mathfrak{q}$. □

6.4 The Nullstellensatz

The classical Nullstellensatz establishes a correspondence between geometric objects (algebraic sets in affine space) and algebraic objects (radical ideals in a polynomial ring). We will prove a more general version of this theorem, from which the classical form follows as a corollary.

Definition 6.74. *A ring R is a **Jacobson ring** if every prime ideal of R is an intersection of maximal ideals.*

Example 6.75.

1. *A local ring $(R, \mathfrak{m})$ is Jacobson if and only if $\mathfrak{m}$ is its only prime ideal.*
2. *A Principal Ideal Domain (PID) is Jacobson. Its nonzero prime ideals are all maximal. The zero ideal is the intersection of all maximal ideals, provided the ring has infinitely many primes (e.g., $\mathbb{Z}$ or $k[x]$).*

Theorem 6.76 (General Nullstellensatz)**.** *Let R be a Jacobson ring. If S is a finitely generated R-algebra, then:*

1. *S is also a Jacobson ring.*
2. *If $\mathfrak{n} \subseteq S$ is a maximal ideal, then $\mathfrak{m} := \mathfrak{n} \cap R$ is a maximal ideal of R, and the residue field extension $S/\mathfrak{n}$ over $R/\mathfrak{m}$ is finite.*

This theorem can fail if R is not Jacobson.

Example 6.77. *Let $R = k[t]_{(t)}$ be the localization of a polynomial ring at the origin. R is not Jacobson. Let $S = R[x]$. The ideal $\mathfrak{n} = (xt - 1) \subseteq S$ is maximal, since $S/\mathfrak{n} \cong k(t)$, which is a field. However, $\mathfrak{n} \cap R = \{0\}$, which is not a maximal ideal of R.*

The proof of the theorem relies on the following characterization of Jacobson rings.

Lemma 6.78. *A ring R is Jacobson if and only if for every prime ideal $\mathfrak{p} \subseteq R$, if the domain $S = R/\mathfrak{p}$ contains an element $b \neq 0$ such that $S[b^{-1}]$ is a field, then S is itself a field.*

Proof of Theorem 6.76. We proceed by induction on the number of generators of S as an R-algebra.

Base Case: $S = R[t]$. First, we prove statement (1), that S is Jacobson. Using Lemma 6.78, let $\mathfrak{p} \subseteq S$ be a prime ideal and set $S' = S/\mathfrak{p}$. Assume there is some $b \in S', b \neq 0$ such that $S'[b^{-1}]$ is a field. We must show S' is a field. Let $R' = R/(R \cap \mathfrak{p})$, so $R' \subseteq S'$. Since $S'[b^{-1}]$ is a field and integral over $R'[b^{-1}]$, Corollary 6.71 implies that $R'[b^{-1}]$ is a field. But R' is an image of the Jacobson ring R, so it is Jacobson. By Lemma 6.78, R' must be a field. Now S' is a domain that is generated by one element over a field R', and $S'[b^{-1}]$ is a field. If S' is not a field, it must be isomorphic to $R'[t]$, but $R'[t][b^{-1}]$ is a field only if b is a constant, which means S' was already a field. So S' is a field.

Next, we prove statement (2). Let $\mathfrak{n} \subseteq S = R[t]$ be a maximal ideal. Set $\mathfrak{m} = \mathfrak{n} \cap R$. The extension $R/\mathfrak{m} \subseteq S/\mathfrak{n}$ is a field extension where $S/\mathfrak{n}$ is generated by one element (the image of t) over $R/\mathfrak{m}$. Let $S' = S/\mathfrak{n}$ and $R' = R/\mathfrak{m}$. We just showed that if $S'[b^{-1}]$ is a field, then R' must be a field. Here S' is already a field, so we can take $b = 1$. It follows that R' must be a field, so $\mathfrak{m}$ is maximal. Since $S/\mathfrak{n}$ is an algebraic extension of $R/\mathfrak{m}$ generated by one element, it is a finite extension.

Inductive Step. Assume the theorem holds for all algebras generated by $r - 1$ elements. Let S be an R-algebra generated by r elements, say $t_1, \ldots, t_r$. Let $S' = R[t_1, \ldots, t_{r-1}]$. By the inductive hypothesis, S' is a Jacobson ring. Now, $S = S'[t_r]$ is generated by one element over the Jacobson ring S'. By our base case:

1. S is a Jacobson ring.
2. If $\mathfrak{n} \subseteq S$ is a maximal ideal, then $\mathfrak{n} \cap S'$ is a maximal ideal of S'. By the inductive hypothesis applied to S' over R, $\mathfrak{m} = (\mathfrak{n} \cap S') \cap R = \mathfrak{n} \cap R$ is a maximal ideal of R. Furthermore, the extensions $S/\mathfrak{n}$ over $S'/(\mathfrak{n} \cap S')$ and $S'/(\mathfrak{n} \cap S')$ over $R/\mathfrak{m}$ are both finite. By the tower law, the extension $S/\mathfrak{n}$ over $R/\mathfrak{m}$ is finite.

This completes the induction. □

Now, we move onto discuss the classical Nullstellensatz. Let k be a field and let $\mathbb{A}_k^n$ denote the affine n-space over k.

Definition 6.79. *For a set of polynomials $F \subseteq k[x_1, \ldots, x_n]$, the **algebraic set** (or variety) defined by F is*

$$Z(F) := \{(a_1, \ldots, a_n) \in \mathbb{A}_k^n \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in F\}.$$

If I is the ideal generated by F, then $Z(F) = Z(I)$.

Definition 6.80. *For a subset $X \subseteq \mathbb{A}_k^n$, the **ideal of** X is*

$$I(X) := \{f \in k[x_1, \ldots, x_n] \mid f(p) = 0 \text{ for all } p \in X\}.$$

The ideal $I(X)$ is always a radical ideal.

These two operations form a Galois connection between subsets of $\mathbb{A}_k^n$ and ideals of $k[x_1, \ldots, x_n]$. A point $p = (a_1, \ldots, a_n) \in \mathbb{A}_k^n$ corresponds to the maximal ideal $\mathfrak{m}_p = (x_1 - a_1, \ldots, x_n - a_n)$. The Nullstellensatz provides a precise description of this correspondence when the field k is algebraically closed.

Corollary 6.81 (Weak Nullstellensatz)**.** *Let k be an algebraically closed field and $S = k[x_1, \ldots, x_n]$. Every maximal ideal of S is of the form $\mathfrak{m}_p = (x_1 - a_1, \ldots, x_n - a_n)$ for some point $p = (a_1, \ldots, a_n) \in \mathbb{A}_k^n$.*

Proof. Let $\mathfrak{n} \subseteq S$ be a maximal ideal. We apply the General Nullstellensatz (Theorem 6.76) with $R = k$. Since a field is Jacobson, S is Jacobson. The theorem states that $\mathfrak{n} \cap k = \{0\}$ is maximal in k, and $S/\mathfrak{n}$ is a finite field extension of $k/\{0\} \cong k$. Since k is algebraically closed, the only finite extension is k itself. So, $S/\mathfrak{n} \cong k$. Let $\pi : S \to S/\mathfrak{n} \cong k$ be the quotient map. Let $a_i = \pi(x_i) \in k$. Then for each i, $\pi(x_i - a_i) = 0$, so $(x_i - a_i) \in \ker(\pi) = \mathfrak{n}$. This implies that $\mathfrak{m}_p = (x_1 - a_1, \ldots, x_n - a_n) \subseteq \mathfrak{n}$. Since $\mathfrak{m}_p$ is a maximal ideal, we must have $\mathfrak{n} = \mathfrak{m}_p$. □

Theorem 6.82 (Hilbert's Nullstellensatz)**.** *Let k be an algebraically closed field. If $I \subseteq k[x_1, \ldots, x_n]$ is an ideal, then*

$$I(Z(I)) = \mathit{rad}(I).$$

This establishes a one-to-one, order-reversing correspondence between algebraic sets in $\mathbb{A}_k^n$ and radical ideals in $k[x_1, \ldots, x_n]$.

Proof. The inclusion $\mathrm{rad}(I) \subseteq I(Z(I))$ is straightforward: if $f^m \in I$, then for any point $p \in Z(I)$, $f(p)^m = 0$, so $f(p) = 0$. Thus $f \in I(Z(I))$.

For the reverse inclusion, $I(Z(I)) \subseteq \mathrm{rad}(I)$, we use the famous "Rabinowitsch trick". Let $f \in I(Z(I))$. Consider the polynomial ring $S[y] = k[x_1, \ldots, x_n, y]$ and the ideal $J = IS[y] + (1 - yf) \subseteq S[y]$. Any point in $Z(J) \subseteq \mathbb{A}_k^{n+1}$ must satisfy all equations in I and also $1 - yf = 0$. If $(a_1, \ldots, a_n, b)$ is such a point, then $(a_1, \ldots, a_n) \in Z(I)$. Since $f \in I(Z(I))$, we have $f(a_1, \ldots, a_n) = 0$. But then the equation $1 - yf = 0$ becomes $1 - b \cdot 0 = 1 = 0$, a contradiction. Therefore, $Z(J)$ is empty. By the Weak Nullstellensatz, if an ideal has an empty zero set, it must be the entire ring. So $J = S[y]$. This means $1 \in J$, so we can write:

$$1 = \sum_i g_i(x, y) p_i(x) + h(x, y)(1 - yf(x))$$

where $p_i \in I$. In the field of fractions $k(x_1, \ldots, x_n)(y)$, we can substitute $y = 1/f(x)$. This yields:

$$1 = \sum_i g_i(x, 1/f) p_i(x).$$

Clearing denominators by multiplying by a sufficiently high power of f, say f^N, we get:

$$f^N = \sum_i (f^N g_i(x, 1/f)) p_i(x).$$

The term $f^N g_i(x, 1/f)$ is a polynomial in $S = k[x_1, \ldots, x_n]$. Since each $p_i \in I$, the right-hand side is in I. Thus $f^N \in I$, which means $f \in \mathrm{rad}(I)$. □

7 Homological Methods

7.1 Filtrations and Graded Constructions

7.1.1 Filtrations and Associated Graded Rings and Modules

This section introduces several fundamental definitions from commutative algebra that are instrumental in constructing important geometric objects such as the blowup algebra and the tangent cone. These constructions often begin with a **multiplicative filtration** of a ring R. This is a sequence of ideals $R = I_0 \supset I_1 \supset I_2 \supset \cdots$ such that $I_i I_j \subset I_{i+j}$ for all $i, j \geq 0$.

A particularly important case is the **I-adic filtration**, where $I \subseteq R$ is an ideal and the filtration is given by the powers of I: $R \supset I \supset I^2 \supset I^3 \supset \cdots$. This concept can be extended to modules: for an R-module M, the sequence $M \supset IM \supset I^2M \supset \cdots$ is the I-adic filtration of M.

Definition 7.1. *Let $I \subseteq R$ be an ideal and M be an R-module. A filtration of M is a sequence of submodules $M = M_0 \supset M_1 \supset M_2 \supset \cdots$.*

- *The filtration is called an **I-filtration** if $IM_n \subset M_{n+1}$ for all $n \geq 0$.*
- *An I-filtration is **stable** if $IM_n = M_{n+1}$ for all sufficiently large n (i.e., for $n \gg 0$).*

Later, we will prove the Artin-Rees Lemma, which states that for a finitely generated module over a Noetherian ring, the I-adic filtration induces a stable filtration on any submodule.

Definition 7.2. *Let $I \subseteq R$ be an ideal. The **associated graded ring of R with respect to I** is the direct sum*

$$gr_I(R) := \bigoplus_{n=0}^{\infty} I^n/I^{n+1} = R/I \oplus I/I^2 \oplus I^3/I^4 \oplus \cdots$$

The multiplication is defined as follows: for homogeneous elements $\bar{a} \in I^m/I^{m+1}$ and $\bar{b} \in I^n/I^{n+1}$, represented by $a \in I^m$ and $b \in I^n$, their product $\bar{a}\bar{b} \in I^{m+n}/I^{m+n+1}$ is the image of ab.

To see this is well-defined, let $a' = a + x$ and $b' = b + y$ be other representatives, where $x \in I^{m+1}$ and $y \in I^{n+1}$. Then $a'b' = ab + ay + bx + xy$. Since $ay \in I^m I^{n+1} \subset I^{m+n+1}$, $bx \in I^n I^{m+1} \subset I^{m+n+1}$, and $xy \in I^{m+1}I^{n+1} \subset I^{m+n+2}$, the term $ay + bx + xy$ is in I^{m+n+1}. Thus, $a'b'$ and ab have the same image modulo I^{m+n+1}.

Definition 7.3. *More generally, if $\mathcal{M} : M = M_0 \supset M_1 \supset M_2 \supset \cdots$ is an I-filtration of an R-module M, the **associated graded module** is*

$$gr_{\mathcal{M}}(M) := \bigoplus_{n=0}^{\infty} M_n/M_{n+1} = M/M_1 \oplus M_1/M_2 \oplus \cdots$$

This is a graded module over $gr_I(R)$. The action of $\bar{a} \in I^m/I^{m+1}$ on $\bar{b} \in M_n/M_{n+1}$ (with lifts $a \in I^m$, $b \in M_n$) is given by the image of ab in M_{n+m}/M_{n+m+1}. The condition $I^m M_n \subseteq M_{n+m}$ ensures this is well-defined.

The stability of a filtration has a important consequence.

Proposition 7.4. *Let $I \subseteq R$ be an ideal and M a finitely generated R-module. If $\mathcal{M} : M = M_0 \supset M_1 \supset \cdots$ is a stable I-filtration where each M_i is a finitely generated R-module, then $gr_{\mathcal{M}}(M)$ is a finitely generated $gr_I(R)$-module.*

Proof. Since the filtration is stable, there exists an integer N such that $IM_n = M_{n+1}$ for all $n \geq N$. The module action implies that for $n \geq N$, the graded piece $(I/I^2) \cdot (M_n/M_{n+1})$ generates M_{n+1}/M_{n+2}. This means that the higher graded components of $gr_{\mathcal{M}}(M)$ are generated by the lower ones. Specifically, the entire module $gr_{\mathcal{M}}(M)$ is generated as a $gr_I(R)$-module by the first $N+1$ components:

$$M_0/M_1 \oplus M_1/M_2 \oplus \cdots \oplus M_N/M_{N+1}$$

Since each M_i is a finitely generated R-module, each quotient M_i/M_{i+1} is also a finitely generated R-module, and thus a finitely generated R/I-module. The union of the finite sets of generators for these first $N+1$ components forms a finite generating set for $gr_{\mathcal{M}}(M)$ over $gr_I(R)$. □

While there is no natural homomorphism $M \to gr_{\mathcal{M}}(M)$, we can define a map on elements. Let $\mathcal{M} : M = M_0 \supset M_1 \supset \cdots$ be a filtration. For an element $f \in M$, if there exists an integer m such that $f \in M_m$ but $f \notin M_{m+1}$, we define the **initial form** of f to be $in(f) := \bar{f} \in M_m/M_{m+1} \subset gr_{\mathcal{M}}(M)$. If $f \in \bigcap_{m=0}^{\infty} M_m$, we define $in(f) = 0$.

Example 7.5. *Let $R = k[x, y]$, $I = (x, y)$, and consider the I-adic filtration of R. Let $J = (xy+y^3, x^2) \subseteq R$. Define $in(J)$ to be the ideal in $gr_I(R)$ generated by the initial forms of all elements in J. We have $in(x^2) = x^2 \in I^2/I^3$ and $in(xy+y^3) = xy \in I^2/I^3$. However, the ideal $in(J)$ is not necessarily generated by just these two initial forms. Consider the element $y^5 \in J$, which can be seen from the combination $y^2(xy+y^3)-x(y^3) = y^5$. Oops, this does not show $y^5 \in J$. Let's check the original argument: $x(xy + y^3) - y(x^2) = xy^3 \in J$. Then $y^2(xy + y^3) - x(xy^3) = y^5 \in J$. Since $y^5 \in I^5 \setminus I^6$, we have $in(y^5) = y^5 \in in(J)$. The ideal in $gr_I(R) \cong k[x, y]$ generated by $in(x^2) = x^2$ and $in(xy + y^3) = xy$ is (x^2, xy). The element y^5 is not in this ideal. This illustrates that to find a generating set for $in(J)$, one cannot simply take the initial forms of a generating set for J.*

The construction of the associated graded ring allows us to apply techniques from the theory of graded rings to arbitrary local rings. If $(R, \mathfrak{m})$ is a Noetherian local ring, then $gr_{\mathfrak{m}}(R)$ is a graded ring generated over the field $R/\mathfrak{m}$ by the finite-dimensional vector space $\mathfrak{m}/\mathfrak{m}^2$. It is therefore a finitely generated algebra over a field.

Definition 7.6. *If $(R, \mathfrak{m})$ is a local ring, the **Hilbert function** of R is*

$$H_R(n) = \dim_{R/\mathfrak{m}}(\mathfrak{m}^n/\mathfrak{m}^{n+1})$$

If M is a finitely generated R-module, its Hilbert function is

$$H_M(n) = \dim_{R/\mathfrak{m}}(\mathfrak{m}^n M/\mathfrak{m}^{n+1}M)$$

These are the Hilbert functions of the graded ring $gr_{\mathfrak{m}}(R)$ and the graded module $gr_{\mathfrak{m}}(M)$, respectively. From the theory of graded rings, we know that for large n, these functions agree with polynomials $P_R(n)$ and $P_M(n)$.

To ensure that no information is lost when passing from R to $gr_I(R)$, we need to know that distinct elements of R have distinct initial forms in some sense. This is guaranteed if $\bigcap_{j=0}^{\infty} I^j = \{0\}$. The Krull Intersection Theorem, which we will prove later, states that this condition holds in most reasonable cases (e.g., for Noetherian local rings).

7.1.2 The Blowup Algebra and The Tangent Cone

Definition 7.7. *Let R be a ring and $I \subseteq R$ be an ideal. The **Rees algebra** (or **blowup algebra**) of I in R is the graded ring*

$$B_I(R) := R \oplus I \oplus I^2 \oplus \cdots = \bigoplus_{n=0}^{\infty} I^n$$

Remark 7.8. *The Rees algebra can be realized as a subring of the polynomial ring $R[t]$ by identifying the n-th graded component I^n with $I^n t^n$. Thus,*

$$B_I(R) \cong \bigoplus_{n=0}^{\infty} I^n t^n \subseteq R[t]$$

An element is a polynomial $a_0 + a_1 t + a_2 t^2 + \cdots$ where $a_k \in I^k$ for each k.

The associated graded ring can be recovered from the Rees algebra. The ideal $IB_I(R)$ is $I \oplus I^2 \oplus I^3 \oplus \cdots$. Taking the quotient, we find:

$$B_I(R)/IB_I(R) = (R \oplus I \oplus I^2 \oplus \cdots)/(I \oplus I^2 \oplus I^3 \oplus \cdots) \cong R/I \oplus I/I^2 \oplus \cdots = gr_I(R)$$

Example 7.9. *Let $R = k[x_1, x_2]$ and $I = (x_1, x_2)$. The Rees algebra $B_I(R)$ is the subring of $k[x_1, x_2, t]$ generated by x_1, x_2, x_1t, x_2t. Consider the surjective homomorphism*

$$\phi : k[x_1, x_2, y_1, y_2] \to B_I(R) \subset k[x_1, x_2, t]$$

given by $x_i \mapsto x_i$ and $y_i \mapsto x_it$. The kernel of this map is generated by relations among the generators. For instance, $x_1(x_2t) - x_2(x_1t) = 0$, which corresponds to the element $x_1y_2 - x_2y_1 \in ker(\phi)$. In fact, $ker(\phi) = (x_1y_2 - x_2y_1)$. Geometrically, this corresponds to the blowup of the affine plane $\mathbb{A}^2$ at the origin. The map of rings corresponds to a morphism of varieties $Z \to \mathbb{A}^2$, where $Z = V(x_1y_2 - x_2y_1) \subset \mathbb{A}^2 \times \mathbb{P}^1$. The fiber over a point $(a_1, a_2) \in \mathbb{A}^2$ other than the origin is the single point in $\mathbb{P}^1$ defined by $a_2y_1 - a_1y_2 = 0$. The fiber over the origin $(0, 0)$ consists of all points satisfying $0 = 0$, which is the entire $\mathbb{P}^1$. Thus, the blowup replaces the origin with a projective line, where each point on the line corresponds to a direction through the origin.

Definition 7.10. *The **exceptional set** of the blowup is the fiber over the point corresponding to the ideal I. Algebraically, this corresponds to the ring $B_I(R)/IB_I(R)$, which is isomorphic to $gr_I(R)$.*

If $X = V(J) \subseteq \mathbb{A}^n$ is an affine variety defined by an ideal $J \subseteq k[x_1, \ldots, x_n]$, and $p \in X$ is a point, we can blow up X at p. If p is the origin, corresponding to the maximal ideal $I = (x_1, \ldots, x_n)$, we are interested in the geometry of X near p. This local geometry is captured by the tangent cone.

Definition 7.11. *Let $R = k[x_1, \ldots, x_n]/J$ and let $I \subseteq R$ be the ideal corresponding to the origin. The **tangent cone** of $V(J)$ at the origin is the affine scheme defined by the ideal of initial forms $in_I(J) \subseteq gr_I(k[x_1, \ldots, x_n])$. It is the spectrum of the ring*

$$gr_I(k[x_1, \ldots, x_n])/in_I(J) \cong gr_I(R)$$

Geometrically, it consists of the limits of secant lines to the variety through the origin.

Example 7.12.

- *Let $J = (y^2 - x^2(x + 1)) = (y^2 - x^3 - x^2)$. With respect to $I = (x, y)$, the initial form is the lowest degree part, $in(y^2 - x^3 - x^2) = y^2 - x^2 = (y - x)(y + x)$. The tangent cone is Spec$(k[x, y]/(y - x)(y + x))$, which is the union of two lines through the origin.*
- *Let $J = (y^2 - x^3)$. The initial form is $in(y^2 - x^3) = y^2$. The tangent cone is Spec$(k[x, y]/(y^2))$, which is the x-axis counted with multiplicity two (a "double line").*

When blowing up a curve in the plane at the origin, each line in its tangent cone corresponds to a distinct point in the fiber over the origin.

7.1.3 The Artin-Rees Lemma and the Krull Intersection Theorem

The blowup construction can be generalized for modules. Let M be an R-module and $\mathcal{M} : M = M_0 \supset M_1 \supset \cdots$ be an I-filtration. Then $B_{\mathcal{M}}(M) := M \oplus M_1 \oplus M_2 \oplus \cdots$ is a graded $B_I(R)$-module.

Proposition 7.13. *Assume R is a Noetherian ring, $I \subseteq R$ is an ideal, and M is a finitely generated R-module. Let $\mathcal{M} : M = M_0 \supset M_1 \supset \cdots$ be an I-filtration where each M_i is finitely generated. Then the filtration $\mathcal{M}$ is I-stable if and only if $B_{\mathcal{M}}(M)$ is a finitely generated $B_I(R)$-module.*

Proof. ($\Rightarrow$) If $\mathcal{M}$ is stable, there is an N such that $M_{n+1} = IM_n$ for all $n \geq N$. Then the module $B_{\mathcal{M}}(M)$ is generated over $B_I(R)$ by the elements in $M_0 \oplus \cdots \oplus M_N$. Since each M_i is finitely generated over R, this is a finite set of generators.

($\Leftarrow$) If $B_{\mathcal{M}}(M)$ is finitely generated over $B_I(R)$, let the generators be in $\bigoplus_{i=0}^{N} M_i$ for some N. Then for any $n \geq N$, an element in M_{n+1} can be written as a sum of products of generators of $B_I(R)$ (which are in I) and the chosen generators of $B_{\mathcal{M}}(M)$. This implies that $M_{n+1} \subseteq IM_n$. Since $IM_n \subseteq M_{n+1}$ by definition of an I-filtration, we have equality. Thus, the filtration is stable. □

This result provides a surprisingly simple proof of the Artin-Rees Lemma.

Lemma 7.14 (Artin-Rees Lemma)**.** *Let R be a Noetherian ring, $I \subseteq R$ an ideal, M a finitely generated R-module, and $M' \subseteq M$ a submodule. The I-adic filtration on M, given by $M_n = I^n M$, induces a filtration on M' defined by $M'_n = M' \cap I^n M$. This induced filtration is I-stable.*

Proof. Since R is Noetherian and I is an ideal, I is finitely generated. Thus the Rees algebra $B_I(R)$ is a finitely generated R-algebra, and by the Hilbert Basis Theorem, it is Noetherian. The filtration $M_n = I^n M$ is stable by construction ($IM_n = I^{n+1}M = M_{n+1}$). Since M is a finitely generated R-module, $B_I(M) := \bigoplus I^n M$ is a finitely generated $B_I(R)$-module. Because $B_I(R)$ is Noetherian, the submodule $B(M') := \bigoplus (M' \cap I^n M) \subseteq B_I(M)$ is also a finitely generated $B_I(R)$-module. By the previous proposition, this implies that the filtration $M'_n = M' \cap I^n M$ is I-stable. That is, there exists an integer k such that for all $n \geq k$, $I(M' \cap I^n M) = M' \cap I^{n+1} M$. □

Theorem 7.15 (Krull Intersection Theorem)**.** *Let R be a Noetherian ring, $I \subseteq R$ an ideal, and M a finitely generated R-module. Let $M' = \bigcap_{j=1}^{\infty} I^j M$. There exists an element $r \in I$ such that $(1-r)M' = 0$.*

Furthermore, if R is an integral domain and I is a proper ideal, or if R is a local ring and I is a proper ideal contained in its Jacobson radical, then $\bigcap_{j=1}^{\infty} I^j = \{0\}$.

Proof. Let $M' = \bigcap_{j=1}^{\infty} I^j M$. As R is Noetherian and M is finitely generated, M is a Noetherian module, so the submodule M' is finitely generated. Applying the Artin-Rees Lemma to the submodule $M' \subseteq M$ with the I-adic filtration, we know there exists a k such that for all $n \geq k$, $M' \cap I^{n+1} M = I(M' \cap I^n M)$. Since $M' \subseteq I^n M$ for all n, this simplifies to $M' = IM'$. Since M' is finitely generated, Nakayama's Lemma implies that there is an element $r \in I$ such that $(1-r)M' = 0$.

For the second statement, let $M = R$. Then we have $\bigcap I^j = M'$. If R is an integral domain and I is a proper ideal, then $I \neq R$, so $1 \notin I$, which means $1 - r \neq 0$. Since R is a domain, $1 - r$ is a non-zero-divisor, so $(1-r)M' = 0$ implies $M' = 0$. If R is a local ring and I is a proper ideal, then I is contained in the maximal ideal (the Jacobson radical). Any element of the form $1 - r$ for $r \in I$ is a unit. Thus $(1-r)M' = 0$ implies $M' = 0$. □

Example 7.16. *The conclusion of the theorem may fail if R is not an integral domain. Let $R = k[x]/(x^2 - x)$. Let $I = (x)$. Then $I^2 = (x^2) = (x) = I$. Thus, $I^j = I$ for all $j \geq 1$, and $\bigcap_j I^j = I \neq \{0\}$. Geometrically, R is the coordinate ring of two points, $\{0, 1\}$. The ideal I corresponds to the point $\{1\}$. The function x vanishes to arbitrarily high order at the point $\{0\}$ but is not the zero function.*

Corollary 7.17. *Let $(R, \mathfrak{m})$ be a Noetherian local ring. If $gr_{\mathfrak{m}}(R)$ is an integral domain, then so is R.*

Proof. Suppose $f, g \in R$ are non-zero elements such that $fg = 0$. By the Krull Intersection Theorem, $\bigcap \mathfrak{m}^n = \{0\}$. Thus, there exist integers $m, n \geq 0$ such that $f \in \mathfrak{m}^m \setminus \mathfrak{m}^{m+1}$ and $g \in \mathfrak{m}^n \setminus \mathfrak{m}^{n+1}$. This means their initial forms $in(f) \in \mathfrak{m}^m/\mathfrak{m}^{m+1}$ and $in(g) \in \mathfrak{m}^n/\mathfrak{m}^{n+1}$ are non-zero. Since $gr_{\mathfrak{m}}(R)$ is an integral domain, the product $in(f)in(g)$ is non-zero. The product $in(f)in(g)$ is the image of fg in $\mathfrak{m}^{m+n}/\mathfrak{m}^{m+n+1}$. For this image to be non-zero, we must have $fg \neq 0$, which is a contradiction. Therefore, R must be an integral domain. □

7.2 Flatness and Tor

7.2.1 Flat Families

Definition 7.18. *An R-module M is **flat** if for every injective map of R-modules $N' \hookrightarrow N$, the induced map $M \otimes_R N' \to M \otimes_R N$ is also injective. (The functor $M \otimes_R -$ is exact.)*

For example, localization is an exact functor, which means $S^{-1}R$ is a flat R-algebra for any multiplicative set S. The concept of flatness provides the correct algebraic framework for studying how geometric objects, such as varieties or schemes, vary in a continuous family.

Example 7.19. *The set of plane curves of degree d is parameterized by the coefficients of the defining polynomials $f = \sum_{i+j \leq d} a_{ij} x^i y^j$. Varying the coefficients (a_{ij}) varies the curve $V(f)$. Algebraically, we have a family of rings $\bar{k}[x,y]/(f)$. The coefficients live in a "parameter space," and for each point in this space, we have a corresponding curve, which is the fiber of a map.*

A naive definition of a family as simply the fibers of a morphism is too general. Consider the family of curves defined by $xy - a = 0$. As the parameter a approaches 0, the hyperbola degenerates into the union of the two coordinate axes. This is a well-behaved degeneration. However, if we consider the map $B \to \mathbb{A}^2$ which is the blowup of the plane at the origin, the fiber over any point is a single point, except for the fiber over the origin, which is an entire projective line. Such a "jump" in dimension is undesirable. Flatness is the condition that rules out such pathological behavior.

A morphism of varieties $\phi : X \to B$ is a flat family if, locally, the corresponding map of rings $R \to S$ makes S a flat R-module.

We consider some examples where $R = k[t]$ with k algebraically closed.

Example 7.20. *Let $S = R[x]/(x - t)$. Here $S \cong R$ as an R-module. Since R is a free R-module, it is flat. The corresponding geometric object is the line $x = t$ in the plane $\mathbb{A}^2 = Speck[x,t]$. The fiber over a point $(t - a) \in SpecR$ is $Speck[x]/(x - a)$, a single point.*

Example 7.21. *Let $S = R[x]/(x^2 - t)$. As an R-module, S is free with basis $\{1, x\}$, since $x^2 - t$ is monic. Free modules are flat. The fiber over $(t - a)$ is $Spec(k[x]/(x^2 - a))$. For $a \neq 0$, this consists of two distinct points. For $a = 0$, it is $Spec(k[x]/(x^2))$, a single point with multiplicity two. Note that the dimension of the fiber as a k-vector space, $\dim_k(k[x]/(x^2 - a))$, is 2 for all a.*

Example 7.22. *Let $S = R[x]/(t(x - 1))$. In S, we have the relation $tx = t$. The fiber over $(t - a)$ for $a \neq 0$ is $Spec(k[x]/(a(x - 1))) = Spec(k[x]/(x - 1))$, which is one point. The fiber over the ideal (t) is $Spec(R[x]/(t)) \cong Spec(k[x]) = \mathbb{A}^1$. The dimension of the fiber jumps from 0 to 1. This is not a flat family, and as we will see, S is not a flat R-module.*

7.2.2 Free Resolutions and Tor

To better understand flatness, we introduce some tools from homological algebra.

Definition 7.23. *Let M be an R-module. A **free resolution** of M is an exact sequence*

$$\cdots \to F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} M \to 0$$

where each F_i is a free R-module.

Any module has a free resolution. We can construct one by taking a set of generators for M, which gives a surjection $d_0 : F_0 \to M$ from a free module F_0. Then we take generators for $\ker(d_0)$ to get a surjection $d_1 : F_1 \to \ker(d_0)$, and so on.

Example 7.24. *Let $R = k[x,y]$ and $M = k \cong R/(x,y)$. A free resolution is given by the Koszul complex:*

$$0 \to R \xrightarrow{d_2} R^2 \xrightarrow{d_1} R \xrightarrow{d_0} M \to 0$$

where $d_0(1) = 1_k$, $d_1(a,b) = ax + by$, and $d_2(c) = (-cy, cx)$.

Definition 7.25. *Let M and N be R-modules. Let $\mathbf{F}_\bullet \to M \to 0$ be a free resolution of M. The complex obtained by tensoring with N is*

$$\cdots \to F_1 \otimes_R N \to F_0 \otimes_R N \to 0$$

*The i-th **Tor** module, denoted $Tor_i^R(M,N)$, is the i-th homology of this complex:*

$$Tor_i^R(M,N) = \frac{ker(d_i \otimes 1_N)}{im(d_{i+1} \otimes 1_N)}$$

7.2.3 Properties of Tor

The Tor modules have several fundamental properties.

1. They are well-defined, i.e., independent of the choice of free resolution.
2. $\mathrm{Tor}_i^R(M,N) \cong \mathrm{Tor}_i^R(N,M)$. We can compute them by resolving N instead of M.
3. $\mathrm{Tor}_0^R(M,N) \cong M \otimes_R N$. This follows from the right-exactness of the tensor product.
4. If M is a free (or more generally, flat) module, then $\mathrm{Tor}_i^R(M,N) = 0$ for all $i > 0$.
5. For any short exact sequence of R-modules $0 \to A \to B \to C \to 0$, there is a long exact sequence in homology:
$$\cdots \to \mathrm{Tor}_1^R(C,N) \to A \otimes N \to B \otimes N \to C \otimes N \to 0$$
6. If S is a flat R-algebra (base change), then $S \otimes_R \mathrm{Tor}_i^R(M,N) \cong \mathrm{Tor}_i^S(S \otimes_R M, S \otimes_R N)$.

Example 7.26. *Let R be a ring and $x \in R$ be a non-zero-divisor. Consider the module $R/(x)$. It has a simple free resolution: $0 \to R \xrightarrow{\cdot x} R \to R/(x) \to 0$. To compute $Tor_i^R(R/(x), M)$ for any R-module M, we tensor this resolution with M:*

$$0 \to R \otimes M \xrightarrow{\cdot x \otimes 1} R \otimes M \to 0 \quad \cong \quad 0 \to M \xrightarrow{\cdot x} M \to 0$$

The homology of this complex gives:

$$\begin{aligned} Tor_0^R(R/(x), M) &= coker(\cdot x) = M/xM \\ Tor_1^R(R/(x), M) &= ker(\cdot x) = \{m \in M \mid xm = 0\} \\ Tor_i^R(R/(x), M) &= 0 \quad \text{for } i \geq 2. \end{aligned}$$

7.2.4 Tor and Flatness

An R-module M is flat if and only if $\mathrm{Tor}_1^R(M,N) = 0$ for all R-modules N. In this case, all higher Tor modules also vanish. While checking this for all modules N is impractical, a stronger criterion simplifies the task.

Proposition 7.27 (Ideal Criterion for Flatness)**.** *An R-module M is flat if and only if $Tor_1^R(R/I, M) = 0$ for all ideals $I \subseteq R$. Equivalently, M is flat if and only if for every ideal $I \subseteq R$, the natural map $I \otimes_R M \to M$ (given by $i \otimes m \mapsto im$) is injective.*

Proof. The equivalence of the two conditions follows from the long exact sequence for Tor associated to the short exact sequence $0 \to I \to R \to R/I \to 0$:

$$\cdots \to \mathrm{Tor}_1^R(R,M) \to \mathrm{Tor}_1^R(R/I,M) \to I \otimes M \to R \otimes M \to \cdots$$

Since R is free, $\mathrm{Tor}_1^R(R,M) = 0$. Thus, the map $I \otimes M \to R \otimes M \cong M$ is injective if and only if $\mathrm{Tor}_1^R(R/I,M) = 0$. The fact that this condition for all ideals I is sufficient for flatness follows from a reduction argument, showing that injectivity for $N' \otimes M \to N \otimes M$ can be deduced from this ideal criterion. □

Definition 7.28. *An R-module M is **torsion-free** if for any non-zero-divisor $r \in R$, the map $M \xrightarrow{\cdot r} M$ is injective. That is, $rm = 0$ implies $m = 0$ for $m \in M$.*

Corollary 7.29.

1. *If an R-module M is flat, then it is torsion-free.*
2. *If R is a PID, then an R-module M is flat if and only if it is torsion-free.*

Proof.

1. Let $a \in R$ be a non-zero-divisor. The map $R \xrightarrow{\cdot a} R$ is injective. Since M is flat, tensoring with M preserves this injection, so $M \otimes R \xrightarrow{1\otimes(\cdot a)} M \otimes R$ is injective. This is the map $M \xrightarrow{\cdot a} M$, so a is a non-zero-divisor on M.
2. ($\Rightarrow$) Follows from part 1. ($\Leftarrow$) Assume R is a PID and M is torsion-free. By the ideal criterion, we must check that $\operatorname{Tor}_1^R(R/I, M) = 0$ for all ideals I. Since R is a PID, any ideal is principal, so $I = (a)$ for some $a \in R$. By the previous example, $\operatorname{Tor}_1^R(R/(a), M) = \{m \in M \mid am = 0\}$. If $a \neq 0$, it is a non-zero-divisor (since PIDs are integral domains), so this set is $\{0\}$ because M is torsion-free. If $a = 0$, $I = (0)$, then $R/I \cong R$ is flat, so Tor vanishes. Thus M is flat.

□

Example 7.30. *Let $R = k[t]$ and $S = R[x]/(t(x-1))$. Since R is a PID, we can check for flatness by checking if S is torsion-free. The element $t \in R$ is a non-zero-divisor. However, in S, $t \cdot (x-1) = 0$, but $x - 1 \neq 0$ in S. Therefore, S has t-torsion and is not a flat R-module.*

An important property of flatness is that it is a local property. Geometrically, this means flatness can be verified by examining the infinitesimal neighborhood of each point. Algebraically, this translates to the ability to check for flatness by localizing at each prime ideal of the base ring.

Proposition 7.31. *An R-module M is flat over R if and only if the localization M_P is a flat module over the local ring R_P for every prime ideal $P \subset R$.*

Proof. ($\Rightarrow$) Suppose M is a flat R-module. Let $0 \to N' \to N$ be an injective map of R_P-modules. Since M is flat over R, the sequence obtained by tensoring over R is also exact:

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

Localization is an exact functor, so applying the functor $(-)_P$ preserves exactness:

$$0 \to (M \otimes_R N')_P \to (M \otimes_R N)_P$$

There is a canonical isomorphism of R_P-modules $(M \otimes_R A)_P \cong M_P \otimes_{R_P} A_P$ for any R-module A. Since N' and N are already R_P-modules, we have $N'_P \cong N'$ and $N_P \cong N$. The sequence thus becomes:

$$0 \to M_P \otimes_{R_P} N' \to M_P \otimes_{R_P} N$$

This shows that the functor $M_P \otimes_{R_P} -$ is exact, so M_P is a flat R_P-module.

($\Leftarrow$) We prove the contrapositive. Assume M is not a flat R-module. Then there exists an injective map of R-modules $\phi : N' \to N$ such that the induced map $1 \otimes \phi : M \otimes_R N' \to M \otimes_R N$ is not injective. Let $K = \ker(1 \otimes \phi)$. Since the map is not injective, K is a non-zero R-module.

A fundamental result states that an R-module is zero if and only if its localization at every prime ideal is zero. Since $K \neq 0$, there must exist a prime ideal $P \subset R$ such that $K_P \neq 0$.

Because localization is an exact functor, it commutes with taking kernels. Therefore, K_P is the kernel of the localized map:

$$(1 \otimes \phi)_P : (M \otimes_R N')_P \to (M \otimes_R N)_P$$

Using the isomorphism mentioned earlier, this is the map:

$$M_P \otimes_{R_P} N'_P \to M_P \otimes_{R_P} N_P$$

Since $K_P \neq 0$, the kernel of this map is non-zero, which means the map is not injective. The existence of such a map shows that M_P is not a flat R_P-module. This contradicts the hypothesis that M_P is flat for all prime ideals P. □

Remark 7.32. *In the statement of the proposition, the condition "for every prime ideal P" can be replaced with the seemingly weaker condition "for every maximal ideal P."*

Example 7.33. *Recall the example of $S = k[t][x]/(t(x-1))$ as a module over the ring $R = k[t]$. We observed that this was not a flat family. We can see this now by checking the local conditions. The prime ideals of R are (0) and the maximal ideals $(t-a)$ for $a \in k$.*

Let's consider a maximal ideal $P = (t-a)$ where $a \neq 0$. Upon localizing at P, the element $t \in R$ becomes a unit in R_P. In the localized module S_P, the relation $t(x-1) = 0$ implies $x - 1 = 0$. Therefore,

$$S_P \cong R_P[x]/(x-1) \cong R_P$$

Since R_P is a free module over itself, S_P is a flat R_P-module for all $P = (t-a)$ with $a \neq 0$.

Now, consider the "problem point," the maximal ideal $P = (t)$. When we localize at P, the element t is not a unit. The relation $t(x-1) = 0$ persists in $S_{(t)}$, showing that $S_{(t)}$ has t-torsion over the ring $R_{(t)}$. Since t is a non-zero-divisor in the local ring $R_{(t)}$, a flat $R_{(t)}$-module must be torsion-free. As $S_{(t)}$ has torsion, it is not flat over $R_{(t)}$.

Since we have found a prime ideal $P = (t)$ for which S_P is not flat over R_P, we conclude that S is not a flat R-module.

7.3 Completions of Rings

7.3.1 Completions

In algebraic geometry, the localization of a ring R at a prime ideal $\mathfrak{m}$, denoted $R_{\mathfrak{m}}$, provides information about the Zariski open neighborhoods of the corresponding point in $\mathrm{Spec}(R)$. The concept of completion, which we introduce here, allows us to study infinitesimally smaller neighborhoods. For algebras over a field k, the completion can be thought of as providing information about Euclidean neighborhoods.

A key example to keep in mind is the polynomial ring $R = k[x_1, \ldots, x_n]$ and the maximal ideal $\mathfrak{m} = (x_1, \ldots, x_n)$. The completion of R with respect to $\mathfrak{m}$, denoted $\widehat{R}_{\mathfrak{m}}$, is isomorphic to the ring of formal power series $k[[x_1, \ldots, x_n]]$. Consequently, for an ideal $I \subset R$, the completion of the quotient ring is given by $(\widehat{R/I})_{\mathfrak{m}} \cong k[[x_1, \ldots, x_n]]/Ik[[x_1, \ldots, x_n]]$.

Example 7.34. *Consider the ring $R = k[x,y]/(y^2 - x - 1)$, which is the coordinate ring of the parabola $x = y^2 - 1$. The inclusion $k[x] \hookrightarrow R$ induces a projection morphism $\pi : Spec(R) \to \mathbb{A}^1_k = Spec(k[x])$. The point $(0,-1)$ on the curve is mapped to the origin $0 \in \mathbb{A}^1_k$. In the affine plane k^2, this corresponds to the projection onto the x-axis.*

In the standard Euclidean topology (if $k = \mathbb{R}$ or $\mathbb{C}$), the projection π has a non-zero derivative at $(0,-1)$. By the Inverse Function Theorem, there exists a neighborhood U of 0 on the x-axis and a neighborhood V of $(0,-1)$ on the curve such that π has an analytic inverse map $U \to V$, given by $x \mapsto (x, -\sqrt{x+1})$.

This inverse is not algebraic, as $-\sqrt{x+1}$ is not a polynomial. However, it can be expressed as a formal power series:

$$-\sqrt{x+1} = -1 - \frac{x}{2} + \frac{x^2}{8} - \ldots$$

This series converges for $|x| < 1$. Thus, while an algebraic inverse does not exist, an inverse exists at the level of formal power series. This illustrates the transition from the algebraic setting to the setting of completions.

To formally define the completion of a ring, we first need the concept of an inverse limit.

Definition 7.35. *An **inverse system** of groups (or rings) is a collection of groups $\{A_i\}_{i\in J}$ indexed by a partially ordered set J, together with a set of homomorphisms $\{\varphi_{ij} : A_j \to A_i\}_{i\le j}$ satisfying:*

1. *φ_{ii} is the identity map on A_i for all $i \in J$.*
2. *$\varphi_{ik} = \varphi_{ij} \circ \varphi_{jk}$ for all $i \le j \le k$. This is the commutativity condition illustrated by the diagram:*

$$\begin{array}{ccc} A_k & & \\ \downarrow{\scriptstyle \varphi_{jk}} & \searrow^{\varphi_{ik}} & \\ A_j & \xrightarrow{\varphi_{ij}} & A_i \end{array}$$

Definition 7.36. *The **inverse limit** (or projective limit) of an inverse system $\{A_i, \varphi_{ij}\}$ is the subgroup of the direct product $\prod_{i\in J} A_i$ defined as:*

$$\varprojlim_{i\in J} A_i := \left\{ (a_i)_{i\in J} \in \prod_{i\in J} A_i \mid a_i = \varphi_{ij}(a_j) \text{ for all } i \le j \text{ in } J \right\}.$$

We now apply this construction to a ring R and an ideal $\mathfrak{m} \subseteq R$. The set of quotient rings $\{R/\mathfrak{m}^i\}_{i\in\mathbb{Z}^+}$ forms an inverse system. For any $j > i$, the natural quotient map $\varphi_{ij} : R/\mathfrak{m}^j \to R/\mathfrak{m}^i$ serves as the homomorphism.

Definition 7.37. *The **$\mathfrak{m}$-adic completion** of a ring R with respect to an ideal $\mathfrak{m}$ is the inverse limit of the system of quotient rings $\{R/\mathfrak{m}^i\}$:*

$$\widehat{R}_{\mathfrak{m}} := \varprojlim_{i\in\mathbb{Z}^+} R/\mathfrak{m}^i.$$

An element of $\widehat{R}_{\mathfrak{m}}$ is a sequence $g = (g_1, g_2, \dots)$ where $g_i \in R/\mathfrak{m}^i$ and $g_j \equiv g_i \pmod{\mathfrak{m}^i}$ for all $j > i$.

The completion $\widehat{R}_{\mathfrak{m}}$ forms a ring under coordinate-wise addition and multiplication. For each $n \in \mathbb{Z}^+$, we can define an ideal

$$\widehat{\mathfrak{m}}_n := \ker(\widehat{R}_{\mathfrak{m}} \to R/\mathfrak{m}^n) = \left\{ g = (g_1, g_2, \dots) \in \widehat{R}_{\mathfrak{m}} \mid g_j = 0 \text{ for all } j \le n \right\}.$$

This gives a filtration $\widehat{\mathfrak{m}}_1 \supset \widehat{\mathfrak{m}}_2 \supset \dots$ on $\widehat{R}_{\mathfrak{m}}$. The quotient rings are $\widehat{R}_{\mathfrak{m}}/\widehat{\mathfrak{m}}_n \cong R/\mathfrak{m}^n$.

If $\mathfrak{m}$ is a maximal ideal, then $\widehat{R}_{\mathfrak{m}}$ is a local ring. The ideal $\widehat{\mathfrak{m}}_1$ is maximal because $\widehat{R}_{\mathfrak{m}}/\widehat{\mathfrak{m}}_1 \cong R/\mathfrak{m}$, which is a field. To see that it is the unique maximal ideal, consider an element $g = (g_1, g_2, \dots) \in \widehat{R}_{\mathfrak{m}} \setminus \widehat{\mathfrak{m}}_1$. Then $g_1 \not\equiv 0 \pmod{\mathfrak{m}}$, so g_1 is a unit in $R/\mathfrak{m}$. Since $g_i \equiv g_1 \pmod{\mathfrak{m}}$ for all $i > 1$, each g_i is a unit in $R/\mathfrak{m}^i$. The compatibility condition $g_j \equiv g_i \pmod{\mathfrak{m}^i}$ ensures that the sequence of inverses $(g_1^{-1}, g_2^{-1}, \dots)$ is a well-defined element of $\widehat{R}_{\mathfrak{m}}$ and is the inverse of g. Thus, every element not in $\widehat{\mathfrak{m}}_1$ is a unit, proving that $\widehat{R}_{\mathfrak{m}}$ is local with maximal ideal $\widehat{\mathfrak{m}}_1$.

Note that the completion of R at $\mathfrak{m}$ is the same as the completion of the localization $R_{\mathfrak{m}}$ at its maximal ideal $\mathfrak{m}R_{\mathfrak{m}}$, since $R/\mathfrak{m}^i \cong R_{\mathfrak{m}}/(\mathfrak{m}R_{\mathfrak{m}})^i$.

Example 7.38 (Formal Power Series Rings)**.** *Let $R = S[x_1, \dots, x_n]$ be a polynomial ring over a ring S, and let $\mathfrak{m} = (x_1, \dots, x_n)$. We claim that the completion $\widehat{R}_{\mathfrak{m}}$ is isomorphic to the formal power series ring $S[[x_1, \dots, x_n]]$.*

First, observe that $R/\mathfrak{m}^i \cong S[[x_1, \dots, x_n]]/\mathfrak{m}^i S[[x_1, \dots, x_n]]$. This provides a natural homomorphism

$$\Phi : S[[x_1, \dots, x_n]] \to \widehat{R}_{\mathfrak{m}}, \quad f \mapsto (f \pmod{\mathfrak{m}}, f \pmod{\mathfrak{m}^2}, \dots).$$

To construct an inverse map, consider an element $(f_1 + \mathfrak{m}, f_2 + \mathfrak{m}^2, \dots) \in \widehat{R}_{\mathfrak{m}}$. The condition $f_i \equiv f_j \pmod{\mathfrak{m}^j}$ for $i > j$ implies that $f_i - f_{i-1}$ consists of terms of degree at least $i - 1$. We can form the series

$$f_1 + (f_2 - f_1) + (f_3 - f_2) + \cdots \in S[[x_1, \dots, x_n]].$$

This map is well-defined (independent of the choice of representatives f_i) and serves as the inverse to Φ, establishing the isomorphism.

Example 7.39 (The Ring of p-adic Integers)**.** *A basic example from number theory is the completion of the integers $\mathbb{Z}$ with respect to a prime ideal (p). The resulting ring, denoted $\mathbb{Z}_p$, is the* ***ring of p-adic integers****.*

$$\mathbb{Z}_p = \widehat{\mathbb{Z}}_{(p)} = \varprojlim_{i \in \mathbb{Z}^+} \mathbb{Z}/(p^i).$$

An element of $\mathbb{Z}_p$ is a sequence $(a_1, a_2, \dots)$ where $a_i \in \mathbb{Z}/(p^i)$ and $a_j \equiv a_i \pmod{p^i}$ for $j > i$.

Any p-adic integer can be uniquely represented by a formal power series in p, known as its ***p-adic expansion****. Given $(a_1, a_2, \dots)$, we may choose representatives such that $0 \leq a_i < p^i$. The compatibility condition $a_{i+1} \equiv a_i \pmod{p^i}$ implies $a_{i+1} - a_i = b_i p^i$ for some integer b_i. We can uniquely choose b_i such that $0 \leq b_i < p$. Then we can write*

$$a_1 = b_0, \quad a_2 = b_0 + b_1 p, \quad a_3 = b_0 + b_1 p + b_2 p^2, \quad \dots$$

This gives rise to the expansion $\sum_{i=0}^{\infty} b_i p^i$. The partial sums of this series recover the sequence $(a_1, a_2, \dots)$.

Addition in $\mathbb{Z}_p$ is defined coordinate-wise, but this does not correspond to term-by-term addition of the power series coefficients. Instead, it involves a "carrying" operation, analogous to standard integer arithmetic. For example, in $\mathbb{Z}_2$, let $x = (1, 1, 1, 9, \dots)$ and $y = (1, 1, 1, 1, \dots)$. Then

$$x + y = (1 + 1 \pmod 2, 1 + 1 \pmod 4, 1 + 1 \pmod 8, 9 + 1 \pmod{16}, \dots) = (0, 2, 2, 10, \dots).$$

The corresponding power series for x is $1 + 0 \cdot 2 + 0 \cdot 2^2 + 1 \cdot 2^3 + \dots$ and for y is 1. The sum is not found by simply adding coefficients. Another example, in $\mathbb{Z}_3$:

$$(1 + 2 \cdot 3 + 2 \cdot 3^2) + (1 + 2 \cdot 3 + 1 \cdot 3^2) = 2 + 4 \cdot 3 + 3 \cdot 3^2 = 2 + (1 + 3) \cdot 3 + 3^3 = 2 + 1 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3.$$

There is a natural embedding $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$. For any non-zero integer r, if p^a is the highest power of p dividing r, then $r \not\equiv 0 \pmod{p^{a+1}}$, so the image of r in $\mathbb{Z}_p$ is non-zero. For example, in $\mathbb{Z}_2$, the integer 1 corresponds to the constant sequence $(1, 1, 1, \dots)$. The power series $1 + 2 + 2^2 + \dots$ corresponds to the element whose n-th term is $\sum_{i=0}^{n-1} 2^i = 2^n - 1 \equiv -1 \pmod{2^n}$. Thus, $(1, 3, 7, 15, \dots)$ represents -1. This leads to the famous identity in $\mathbb{Z}_2$:

$$1 + 2 + 4 + 8 + \cdots = -1.$$

The ring $\mathbb{Z}_p$ is much larger than $\mathbb{Z}$. The bijection between elements of $\mathbb{Z}_p$ and their p-adic expansions $\sum a_i p^i$ (where $0 \leq a_i < p$) shows that the cardinality of $\mathbb{Z}_p$ is that of the continuum. In particular, $\mathbb{Z}_p$ is uncountable.

7.3.2 Properties of Completion

Definition 7.40. *Let R be a ring and $\mathfrak{m} \subset R$ an ideal. The natural map $\phi : R \to \widehat{R}_{\mathfrak{m}}$ sends $r \mapsto (r \pmod{\mathfrak{m}}, r \pmod{\mathfrak{m}^2}, \dots)$. If ϕ is an isomorphism, we say R is* ***complete with respect to*** *$\mathfrak{m}$. If $\mathfrak{m}$ is a maximal ideal and R is complete with respect to $\mathfrak{m}$, we call R a* ***complete local ring****.*

Remark 7.41. *The kernel of the natural map $\phi : R \to \widehat{R}_{\mathfrak{m}}$ is $\bigcap_{j=1}^{\infty} \mathfrak{m}^j$. Therefore, if R is complete with respect to $\mathfrak{m}$, it must be the case that $\bigcap_{j=1}^{\infty} \mathfrak{m}^j = \{0\}$.*

Let $\widehat{R} = \widehat{R}_{\mathfrak{m}}$. Recall the ideals $\widehat{\mathfrak{m}}_n = \ker(\widehat{R} \to R/\mathfrak{m}^n)$. We can also consider the ideals $\mathfrak{m}^n \widehat{R}$ generated by the image of $\mathfrak{m}^n$ in $\widehat{R}$. An element of $\mathfrak{m}^n \widehat{R}$ is a finite sum of elements of the form $a \cdot \hat{r}$ where $a \in \mathfrak{m}^n$ and $\hat{r} \in \widehat{R}$. This implies that for any such element, its i-th coordinate (for $i \leq n$) is zero, so $a\hat{r} \in \widehat{\mathfrak{m}}_n$. Thus, we always have the inclusion $\mathfrak{m}^n \widehat{R} \subseteq \widehat{\mathfrak{m}}_n$. If R is Noetherian, this inclusion becomes an equality, but in general, the ideals may differ.

Proposition 7.42. *The ring $\widehat{R}$ is complete with respect to the filtration given by the ideals $\{\widehat{\mathfrak{m}}_n\}$.*

Proof. By definition, the completion of $\widehat{R}$ with respect to the filtration $\{\widehat{\mathfrak{m}}_n\}$ is the inverse limit $\varprojlim_n \widehat{R}/\widehat{\mathfrak{m}}_n$. As we have seen, $\widehat{R}/\widehat{\mathfrak{m}}_n \cong R/\mathfrak{m}^n$. Therefore,

$$\text{Completion of } \widehat{R} = \varprojlim_n (\widehat{R}/\widehat{\mathfrak{m}}_n) \cong \varprojlim_n (R/\mathfrak{m}^n) = \widehat{R}.$$

Thus, $\widehat{R}$ is complete with respect to this filtration. □

When the base ring R is Noetherian, the completion $\widehat{R}$ inherits several important properties.

Theorem 7.43. *Let R be a Noetherian ring and $\mathfrak{m} \subset R$ an ideal. Let $\widehat{R}$ be the $\mathfrak{m}$-adic completion of R. Then:*

1. *$\widehat{R}$ is a Noetherian ring.*
2. *$\widehat{R}$ is complete with respect to the ideal $\mathfrak{m}\widehat{R}$.*
3. *$\widehat{R}$ is a flat R-module.*

Proof. For a proof of these basic results, see, for example, Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry.* □

7.3.3 Limits and Topology

The structure of a completion can be understood topologically. The ideals $\mathfrak{m}^n$ (or $\widehat{\mathfrak{m}}_n$ in the completion) define a system of neighborhoods of 0, endowing the ring with a topology. In this context, elements of the completion can be viewed as limits of sequences from the original ring.

Example 7.44. *In the polynomial ring $R[x]$, the sequence of polynomials $a_0, a_0 + a_1x, a_0 + a_1x + a_2x^2, \ldots$ can be said to "converge" to the formal power series $\sum_{i=0}^{\infty} a_i x^i \in R[[x]]$.*

Example 7.45. *In $\mathbb{Z}_2$, the sequence of integers $1, 3, 7, 15, \ldots$ (i.e., $2^n - 1$) converges to the element -1. This corresponds to the series $1 + 2 + 2^2 + \ldots$.*

This notion of convergence can be made precise. Let $\widehat{R}$ be a completion with filtration $\{\widehat{\mathfrak{m}}_n\}$.

Definition 7.46. *A sequence $(a_j)_{j\in\mathbb{Z}^+}$ in $\widehat{R}$ **converges** to an element $a \in \widehat{R}$ if for every $n \in \mathbb{Z}^+$, there exists an integer $N(n)$ such that for all $j \geq N(n)$, we have $a - a_j \in \widehat{\mathfrak{m}}_n$.*

*A sequence (a_j) is a **Cauchy sequence** if for every $n \in \mathbb{Z}^+$, there exists an integer $N(n)$ such that for all $i, j \geq N(n)$, we have $a_i - a_j \in \widehat{\mathfrak{m}}_n$.*

The completeness of $\widehat{R}$ means that every Cauchy sequence converges to a unique limit in $\widehat{R}$.

Exercise 7.47. *Show that in a complete ring $\widehat{R}$, every Cauchy sequence converges to a unique limit.*

This topology is the same as the one generated by the basis of open sets $\{a + \widehat{\mathfrak{m}}_n \mid a \in \widehat{R}, n \in \mathbb{Z}^+\}$.

7.3.4 Hensel's Lemma

Complete rings possess a property for finding roots of polynomials, analogous to Newton's method in analysis. This property is encapsulated in Hensel's Lemma. The underlying idea is that an approximate solution to a polynomial congruence modulo an ideal can be "lifted" to an exact solution in the completion.

In the p-adic integers, a congruence $a \equiv b \pmod{p^n}$ signifies that a and b are "close," agreeing in their first n coefficients in the p-adic expansion. Hensel's Lemma specifies when a solution modulo p can be refined to a true solution in $\mathbb{Z}_p$.

For instance, consider $f(x) = x^2 - 5$ in $\mathbb{Z}_2$. We have $5 \equiv 1^2 \pmod 2$ and $5 \equiv 1^2 \pmod 4$. However, $5 \not\equiv a^2 \pmod 8$ for any integer a. This failure to lift the solution indicates that 5 is not a square in $\mathbb{Z}_2$.

Now consider $f(x) = x^2 - 7$ in $\mathbb{Z}_3$. We can find approximate solutions modulo powers of 3:

$$7 \equiv 1^2 \pmod 3 \quad (\text{since } 1 - 7 = -6)$$
$$7 \equiv 4^2 \pmod 9 \quad (\text{since } 16 - 7 = 9)$$
$$7 \equiv 13^2 \pmod{27} \quad (\text{since } 169 - 7 = 162 = 6 \cdot 27)$$

Here, $1 \equiv 1 \pmod 3$, $4 \equiv 1 \pmod 3$, and $13 \equiv 4 \pmod 9$. This suggests a sequence of approximations that converges to a root of $x^2 - 7$ in $\mathbb{Z}_3$. Hensel's Lemma provides the precise conditions for this lifting to be possible.

We first state the classical version for the p-adic integers.

Theorem 7.48 (Hensel's Lemma)**.** *Let $f(x) \in \mathbb{Z}_p[x]$ be a polynomial. If there exists an integer $a \in \mathbb{Z}_p$ that is an approximate root in the sense that*

$$f(a) \equiv 0 \pmod p \quad \textit{and} \quad f'(a) \not\equiv 0 \pmod p,$$

then there exists a unique root $b \in \mathbb{Z}_p$ such that $f(b) = 0$ and $b \equiv a \pmod p$.

Example 7.49. *For $f(x) = x^2 - 5$ in $\mathbb{Z}_2$, the derivative is $f'(x) = 2x$. For any integer a, $f'(a) = 2a \equiv 0 \pmod 2$. The condition $f'(a) \not\equiv 0 \pmod 2$ is never met, so this version of the lemma is inconclusive.*

Example 7.50. *For $f(x) = x^2 - 7$ in $\mathbb{Z}_3$, let's test $a = 1$. We have $f(1) = 1 - 7 = -6 \equiv 0 \pmod 3$. The derivative is $f'(x) = 2x$, so $f'(1) = 2 \not\equiv 0 \pmod 3$. By Hensel's Lemma, there is a unique root $b \in \mathbb{Z}_3$ such that $b \equiv 1 \pmod 3$. Similarly, testing $a = 2$, we have $f(2) = 4 - 7 = -3 \equiv 0 \pmod 3$, and $f'(2) = 4 \equiv 1 \not\equiv 0 \pmod 3$. Thus, there is also a unique root $c \in \mathbb{Z}_3$ such that $c \equiv 2 \pmod 3$.*

We can use this to characterize the square elements in $\mathbb{Z}_p$. Let $c \in \mathbb{Z}_p$ be non-zero. We can write $c = p^n b$ where $p \nmid b$. Then c is a square in $\mathbb{Z}_p$ if and only if n is even and b is a square. To determine if b is a square, we consider the polynomial $f(x) = x^2 - b$. Its derivative is $f'(x) = 2x$.

Case 1: $p \neq 2$. If b is a quadratic residue modulo p, there exists an integer a such that $a^2 \equiv b \pmod p$. Since $p \nmid b$, we have $a \not\equiv 0 \pmod p$. As $p \neq 2$, it follows that $f'(a) = 2a \not\equiv 0 \pmod p$. By Hensel's Lemma, there exists a root of $f(x)$ in $\mathbb{Z}_p$. Therefore, for $p \neq 2$, an element $c = p^n b$ is a square in $\mathbb{Z}_p$ if and only if n is even and b is a quadratic residue modulo p.

Case 2: $p = 2$. The condition $f'(a) \not\equiv 0 \pmod p$ is never satisfied. A more general version of the lemma is needed.

Theorem 7.51 (Generalized Hensel's Lemma)**.** *Let R be a ring that is complete with respect to an ideal $\mathfrak{m}$. Let $f(x) \in R[x]$ be a polynomial. If there exists $a \in R$ such that*

$$f(a) \in f'(a)^2 \mathfrak{m},$$

then there exists a root b of f such that $f(b) = 0$ and $b - a \in f'(a)\mathfrak{m}$. If $f'(a)$ is a non-zero-divisor in R, then this root b is unique.

Example 7.52. *We return to the question of which elements are squares in $\mathbb{Z}_2$. Let $c = 2^n b$ with b odd. For c to be a square, n must be even and b must be a square. Let us determine the condition for an odd integer b to be a square. A simple calculation shows that the square of any odd integer is congruent to $1 \pmod 8$.*

$$(1 + 2k)^2 = 1 + 4k + 4k^2 = 1 + 4k(k + 1) \equiv 1 \pmod 8.$$

Thus, a necessary condition for b to be a square in $\mathbb{Z}_2$ is $b \equiv 1 \pmod 8$. We now show this is sufficient.

Let $f(x) = x^2 - b$. The ring is $R = \mathbb{Z}_2$, which is complete with respect to $\mathfrak{m} = (2)$. The derivative is $f'(x) = 2x$. Let's choose the approximate root $a = 1$. Then $f(a) = 1 - b$ and $f'(a) = 2$. The condition from the Generalized Hensel's Lemma is

$$f(a) \in f'(a)^2 \mathfrak{m} \implies 1 - b \in (2)^2(2) = (8).$$

This is precisely the condition $b \equiv 1 \pmod 8$. If this holds, the lemma guarantees the existence of a root in $\mathbb{Z}_2$. Thus, an odd integer b is a square in $\mathbb{Z}_2$ if and only if $b \equiv 1 \pmod 8$.

8 Dimension Theory

8.1 Preliminaries

8.1.1 Introduction to Dimension Theory

Definition 8.1. *The **Krull dimension** of a ring R, denoted $\dim R$, is the supremum of lengths of chains of prime ideals in R. A chain of prime ideals $P_r \supsetneq P_{r-1} \supsetneq \cdots \supsetneq P_0$ is said to have length r.*

Example 8.2. *In the polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$, the chain of prime ideals*

$$(x_1, \ldots, x_n) \supsetneq (x_1, \ldots, x_{n-1}) \supsetneq \cdots \supsetneq (x_1) \supsetneq (0)$$

has length n. We will later see that this is a chain of maximal length, which implies that $\dim \mathbb{C}[x_1, \ldots, x_n] = n$.

Definition 8.3. *Let $I \subsetneq R$ be a proper ideal.*

1. *The **dimension** of I is defined as $\dim I := \dim(R/I)$.*
2. *If I is a prime ideal, its **codimension** (or height) is the supremum of lengths of chains of prime ideals descending from I. We denote this by $\operatorname{codim} I$. Note that this is equivalent to the dimension of the localization, i.e., $\operatorname{codim} I = \dim R_I$.*
3. *If I is not prime, its **codimension** is defined as the minimum of the codimensions of the prime ideals containing it:*
$$\operatorname{codim} I := \min\{\operatorname{codim} P \mid P \supseteq I \text{ is prime}\}.$$

The notion of dimension can also be extended to modules.

Definition 8.4. *Let M be an R-module. The **dimension of** M is defined in terms of its annihilator:*

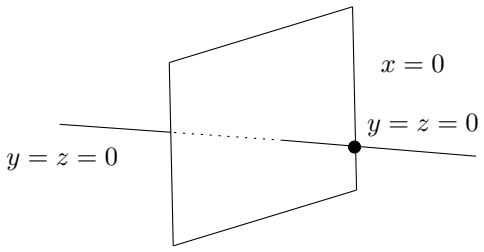
$$\dim M := \dim(ann M) = \dim(R/ann M).$$

Remark 8.5. *This definition can lead to ambiguity. For instance, if I is an ideal in an integral domain R, its dimension as an R-module is $\dim_R I = \dim(R/ann(I))$. Since R is a domain, $ann(I) = (0)$, so $\dim_R I = \dim R$. However, its dimension as an ideal is $\dim I = \dim(R/I)$. When we write $\dim I$, we will mean its dimension as an ideal unless specified otherwise. The context should make the intended meaning clear.*

Problem 8.6. *Let $I \subseteq R$ be an ideal. Why is it not always possible to define the codimension of I as $\operatorname{codim} I = \dim R - \dim I$?*

While this formula holds in many well-behaved cases (e.g., for ideals in a domain that is a finitely generated k-algebra), it fails in general.

Example 8.7. *Consider the variety in $\mathbb{A}^3$ defined by the ideal $(x)(y, z) = (xy, xz)$. This variety is the union of the plane $x = 0$ and the line $y = z = 0$.*



Let $R = k[x, y, z]/(xy, xz)$. The chain of prime ideals corresponding to $(x, y, z) \supset (x, y) \supset (x)$ shows that $\dim R \geq 2$. In fact, $\dim R = 2$.

Now consider the ideal $I = (x-1, y, z)R$. Geometrically, this corresponds to the point $(1,0,0)$, which lies only on the component defined by $y = z = 0$. The ideal I is maximal in R, so its dimension as an ideal is $\dim I = \dim(R/I) = 0$.

However, its codimension is codim $I = \dim R_I$.

$$R_I = \left(\frac{k[x,y,z]}{(xy, xz)}\right)_{(x-1,y,z)} = \frac{k[x,y,z]_{(x-1,y,z)}}{(y,z)k[x,y,z]_{(x-1,y,z)}} \cong k[x]_{(x-1)}.$$

The dimension is therefore $\dim k[x]_{(x-1)} = 1$. *So, we have codim* $I = 1$. *In this case,* $\dim I + \text{codim } I = 0 + 1 = 1 \neq 2 = \dim R$.

The intuition here is that $\dim R$ measures the dimension of the largest irreducible component of the corresponding variety, while codim I provides the "local" codimension of the subvariety $V(I)$ within the component on which it lies.

8.1.2 Connection to Artinian Rings

Recall that a ring R is **Artinian** if every strictly decreasing chain of ideals terminates. We have previously established the following key result.

Theorem 8.8. *A ring R is Artinian if and only if it is Noetherian and every prime ideal of R is maximal.*

This algebraic characterization has a geometric counterpart for the prime spectrum of the ring.

Corollary 8.9. *If R is a Noetherian ring, then R is Artinian if and only if Spec(R) is a finite set of points.*

The condition that every prime ideal is maximal is equivalent to the statement that there are no prime ideal chains of length 1 or greater. This allows us to rephrase the above results in the language of dimension theory.

Corollary 8.10. *If R is a Noetherian ring, the following are equivalent:*

1. $\dim R = 0$.
2. *R is Artinian.*
3. *Spec(R) is a finite, discrete space.*

8.1.3 Dimension and Morphisms

Recall the "going-up" and "incomparability" theorems for integral extensions. The going-up theorem allows us to lift an ascending chain of prime ideals from a ring R to a ring S that is integral over R. The incomparability theorem states that if two prime ideals in S, one contained in the other, contract to the same prime ideal in R, then they must be equal. These theorems allow us to relate the dimensions of rings and their integral extensions.

Proposition 8.11. *Let $\psi : R \to S$ be a ring homomorphism that makes S an integral extension of $\psi(R)$. Let $I \subseteq S$ be an ideal. Then*

$$\dim I = \dim \psi^{-1}(I).$$

Proof. First, observe that we can reduce to the case of an inclusion. The homomorphism ψ induces an isomorphism $R/\ker\psi \cong \psi(R)$. The ring S is integral over $\psi(R)$. The ideal $\psi^{-1}(I)$ in R corresponds to the ideal $\psi(R) \cap I$ in $\psi(R)$. The dimension formula is $\dim \psi^{-1}(I) = \dim(R/\psi^{-1}(I)) = \dim(\psi(R)/(\psi(R) \cap I))$. The dimension of I is $\dim(S/I)$. Since S/I is integral over $\psi(R)/(\psi(R) \cap I)$, we can replace R with $\psi(R)$, S with S/I, and assume $R \subseteq S$ is an integral extension of domains, and we wish to show $\dim S = \dim R$.

Let $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_r$ be a chain of prime ideals in R. By the going-up theorem, there exists a chain of prime ideals $Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_r$ in S such that $Q_i \cap R = P_i$. This implies $\dim S \geq \dim R$.

Conversely, let $Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_s$ be a chain of prime ideals in S. Let $P_i = Q_i \cap R$. By the incomparability theorem, the chain $P_0 \subseteq P_1 \subseteq \cdots \subseteq P_s$ must be a strictly increasing chain of prime ideals in R. Thus, $\dim R \geq \dim S$. Combining these inequalities, we conclude $\dim R = \dim S$. □

This proposition has a powerful geometric interpretation.

Corollary 8.12. *Let $\phi : S \to R$ be a ring homomorphism such that R is a finite S-algebra. Let $\phi^* :$ Spec $R \to$ Spec S be the corresponding morphism of spectra.*

1. *The fibers of ϕ^* are finite sets. (A finite morphism has finite fibers).*
2. *If $X = V(I) \subseteq$ Spec R is a closed subscheme, then its image $\phi^*(X) \subseteq$ Spec S is a closed subscheme of the same dimension as X.*

Proof. Let's prove them in reverse order:

(2) Let $X = V(I)$. The image $\phi^*(X)$ is the set of prime ideals in S that are preimages of primes in X. This is $V(\phi^{-1}(I))$. So the image is closed. By the previous proposition, $\dim X = \dim(R/I) = \dim(S/\phi^{-1}(I)) = \dim \phi^*(X)$.

(1) Let $P \in$ Spec S be a point. The fiber over P is Spec$(R \otimes_S k(P))$, where $k(P)$ is the residue field at P. The ring $R \otimes_S k(P)$ is a finite-dimensional algebra over the field $k(P)$. Such a ring is Artinian, and therefore has dimension 0. A Noetherian scheme of dimension 0 is a finite set of points. □

8.2 Main Theorems and Applications

8.2.1 Krull's Principal Ideal Theorem

Assume all rings are Noetherian.

Problem 8.13. *If an ideal I is generated by n elements, $I = (a_1, \ldots, a_n)$, how does its codimension relate to n? As a starting point, what is the codimension of a principal ideal (a)?*

We begin with a simple observation about primes contained within a principal ideal.

Lemma 8.14. *Let (x) be a proper principal ideal in a domain R. Any prime ideal P properly contained in (x) has codimension 0.*

Proof. Suppose for contradiction that there is a chain of prime ideals $Q \subsetneq P \subsetneq (x)$. By passing to the quotient ring R/Q, we may assume $Q = (0)$ and R is a domain. Let $y \in P$. Since $y \in (x)$, we can write $y = ax$ for some $a \in R$. Because P is prime and $x \notin P$ (as $P \subsetneq (x)$), it must be that $a \in P$. This holds for all $y \in P$, which implies $P \subseteq xP$. Since $xP \subseteq P$ is always true, we have $P = xP$. As R is Noetherian, P is finitely generated, so by Nakayama's Lemma, there exists an element $r \in (x)$ such that $(1 - r)P = 0$. Since R is a domain and $P \neq (0)$, we must have $1 - r = 0$, so $r = 1$. But this implies $1 \in (x)$, meaning $(x) = R$, which contradicts the assumption that (x) is a proper ideal. Therefore, no such prime Q can exist, and P must be a minimal prime, i.e., codim $P = 0$. □

Krull's Principal Ideal Theorem (PIT) generalizes this idea to primes that are minimal over a principal ideal.

Theorem 8.15 (Krull's Principal Ideal Theorem)**.** *If x is an element of a Noetherian ring R, and P is a prime ideal minimal over (x), then codim $P \leq 1$.*

To prove this, we first recall a useful characterization of minimal primes.

Corollary 8.16. *Let R be a Noetherian ring and $I \subseteq R$ an ideal. For a prime ideal $P \supseteq I$, the following are equivalent:*

1. *P is minimal among primes containing I.*
2. *The ring R_P/IR_P is Artinian.*

3. For some $n > 0$, $(PR_P)^n \subseteq IR_P$ in the ring R_P.

Proof. See Eisenbud, Corollary 2.19. The proof relies on properties of primary decomposition and localization. □

We also introduce the concept of symbolic powers of a prime ideal.

Definition 8.17. *Let $Q \subseteq R$ be a prime ideal. The n-**th symbolic power** of Q is*

$$Q^{(n)} := Q^n R_Q \cap R = \{r \in R \mid sr \in Q^n \text{ for some } s \in R \setminus Q\}.$$

It is clear that $Q^n \subseteq Q^{(n)}$. The containment can be strict.

Example 8.18. *Let $R = k[x, y, z]/(xy - z^2)$ and let $P = (x, z)$, which is a prime ideal in R. The relation $xy = z^2$ holds in R. Since $y \notin P$, y is a unit in R_P. In R, we have $xy = z^2 \in P^2$. This means $x \in P^{(2)}$. However, $x \notin P^2 = (x^2, xz, z^2)$, so $P^2 \subsetneq P^{(2)}$.*

Proof of the Principal Ideal Theorem. Let P be a prime ideal minimal over (x). We want to show codim $P \leq 1$. This is equivalent to showing that for any prime ideal $Q \subsetneq P$, there is no prime ideal strictly between Q and P.

By localizing at P, we may assume R is a local ring with unique maximal ideal P. Suppose there exists a prime ideal Q such that $Q \subsetneq P$. We must show that Q is a minimal prime of R (i.e., codim $Q = 0$).

Since P is minimal over (x), the ring $R/(x)$ is Artinian by the corollary above. Consider the descending chain of ideals in $R/(x)$:

$$\frac{Q + (x)}{(x)} \supseteq \frac{Q^{(2)} + (x)}{(x)} \supseteq \frac{Q^{(3)} + (x)}{(x)} \supseteq \dots$$

Since $R/(x)$ is Artinian, this chain must stabilize. So for some $n \gg 0$, we have $Q^{(n)} + (x) = Q^{(n+1)} + (x)$. This implies $Q^{(n)} \subseteq Q^{(n+1)} + (x)$. For any $f \in Q^{(n)}$, we can write $f = g + ax$ where $g \in Q^{(n+1)}$ and $a \in R$. Then $ax = f - g \in Q^{(n)}$. Since P is minimal over (x), we have $x \notin Q$. As Q is prime, this means $a \in Q^{(n)}$. Therefore, $Q^{(n)} \subseteq Q^{(n+1)} + (x)Q^{(n)}$. Since the reverse inclusion is trivial, we have equality.

Now consider the module $M = Q^{(n)}/Q^{(n+1)}$. We have $M = (x)M$. Since $x \in P = J(R)$ (the Jacobson radical), by Nakayama's Lemma, we must have $M = 0$, which means $Q^{(n)} = Q^{(n+1)}$.

Localizing at Q, this equality becomes $(QR_Q)^n = (QR_Q)^{n+1}$. Again, by Nakayama's Lemma (applied to the local ring R_Q), this implies $(QR_Q)^n = (0)$. By the corollary, this means the ring $R_Q/(0)$ is Artinian, so $\dim R_Q = 0$. This shows that Q is a minimal prime, and thus codim $P \leq 1$. □

This theorem generalizes to ideals generated by multiple elements.

Theorem 8.19 (Krull's Height Theorem)**.** *If an ideal I in a Noetherian ring R can be generated by c elements, and P is a prime ideal minimal over I, then codim $P \leq c$.*

Sketch of Proof. The proof proceeds by induction on c. The base case $c = 1$ is the Principal Ideal Theorem. For the inductive step, assume the theorem holds for ideals generated by $c - 1$ elements. Let P be minimal over $I = (x_1, \dots, x_c)$. We may assume R is local with maximal ideal P. Let P_1 be any prime ideal such that $P_1 \subsetneq P$. We need to show that codim $P_1 \leq c - 1$. By passing to R/P_1 and avoiding the minimal primes, we can find an element $y \in P$ such that P_1 is minimal over an ideal generated by $c - 1$ elements. The inductive hypothesis then gives the result. □

Krull's theorem provides a fundamental upper bound on the lengths of chains of prime ideals.

Corollary 8.20. *In a Noetherian ring, any strictly descending chain of prime ideals has finite length. Specifically, if P is a prime ideal generated by c elements, any chain of primes descending from P has length at most c.*

Corollary 8.21. *The ideal $(x_1, \ldots, x_c)$ in the polynomial ring $k[x_1, \ldots, x_n]$ has codimension c.*

Proof. The chain $(x_1, \ldots, x_c) \supsetneq (x_1, \ldots, x_{c-1}) \supsetneq \cdots \supsetneq (x_1) \supsetneq (0)$ shows $\operatorname{codim}(x_1, \ldots, x_c) \geq c$. Krull's Height Theorem provides the reverse inequality, $\operatorname{codim}(x_1, \ldots, x_c) \leq c$. □

There is a useful partial converse to Krull's Height Theorem.

Corollary 8.22. *If P is a prime ideal of codimension c in a Noetherian ring, then P is a minimal prime ideal over some ideal generated by c elements.*

Proof. We construct the generators inductively. Let $r = 0$. A prime of codimension 0 is minimal over the ideal (0), which is generated by 0 elements. Now, assume we have found $x_1, \ldots, x_r \in P$ with $r < c$ such that any prime minimal over $(x_1, \ldots, x_r)$ has codimension r. Let $\{Q_i\}$ be the set of minimal primes over $(x_1, \ldots, x_r)$. Since $\operatorname{codim} P = c > r = \operatorname{codim} Q_i$, P cannot be equal to any Q_i. By prime avoidance, $P \not\subseteq \bigcup Q_i$. So we can choose $x_{r+1} \in P \setminus \bigcup Q_i$. Any prime minimal over $(x_1, \ldots, x_{r+1})$ must properly contain some Q_i, and thus has codimension at least $r+1$. By Krull's theorem, it has codimension exactly $r+1$. We continue this process until $r = c$, at which point P must be a minimal prime over $(x_1, \ldots, x_c)$. □

Finally, we connect these results to unique factorization domains.

Corollary 8.23. *Let R be a Noetherian domain. Then R is a UFD if and only if every prime ideal of codimension 1 is principal.*

Proof. A standard result states that a Noetherian domain is a UFD if and only if every minimal prime over a non-zero principal ideal is itself principal. Let P be a prime minimal over (x) for some $x \neq 0$. By the Principal Ideal Theorem, $\operatorname{codim} P \leq 1$. Since $x \neq 0$, $P \neq (0)$, so $\operatorname{codim} P = 1$. By hypothesis, P is principal. Thus, R is a UFD. The converse is a standard property of UFDs. □

8.2.2 Systems of Parameters

Assume all rings are Noetherian.

Using the Principal Ideal Theorem along with the corollary about primes minimal over an ideal in a local ring, we get the following characterization of the dimension of a local ring:

Corollary 8.24. *If (R, m) is a local ring, then $\dim R$ is the smallest number d such that there exist d elements $x_1, \ldots, x_d \in m$ with $m^n \subseteq (x_1, \ldots, x_d)$ for $n \gg 0$.*

Proof. If $m^n \subseteq (x_1, \ldots, x_d) \subseteq m$, then m is a minimal prime over $(x_1, \ldots, x_d)$, so $\dim R \leq d$ by the Principal Ideal Theorem.

For the other inequality, let $e = \dim R$. By the converse of the Principal Ideal Theorem, we can find $x_1, \ldots, x_e \in m$ such that m is a minimal prime over $(x_1, \ldots, x_e)$. Then the ring $R/(x_1, \ldots, x_e)$ has only one prime ideal (the image of m). Thus, its maximal ideal must be nilpotent. This implies $m^n \subseteq (x_1, \ldots, x_e)$ for some $n \gg 0$. Since d is the minimum such number of elements, we must have $d \leq e = \dim R$. □

Definition 8.25. *If (R, m) is a local ring with $d = \dim R$, a sequence of elements $x_1, \ldots, x_d$ as in the corollary is called a* ***system of parameters*** *for R.*

If (R, m) is a local ring of dimension d, the following are equivalent for elements $x_1, \ldots, x_d \in m$:

1. The set $\{x_1, \ldots, x_d\}$ is a system of parameters.
2. $\operatorname{rad}(x_1, \ldots, x_d) = m$.
3. m is a minimal prime ideal over $(x_1, \ldots, x_d)$.

Recall that for a local ring (R, m), the following are equivalent: it has finite length, it is Artinian, m is the only prime ideal, and $m^n = 0$ for some $n \gg 0$.

Thus, for an ideal q in a local ring R, $m^n \subseteq q$ for $n \gg 0$ if and only if R/q has finite length. Such an ideal q is said to have **finite colength**.

More generally, if M is a finitely generated module over a local ring (R, m), then an ideal $q \subseteq m$ has **finite colength** on M if the module M/qM has finite length. This is true if and only if a power of m annihilates M/qM, i.e., $m^n \subseteq \operatorname{ann}(M/qM)$ for some $n \gg 0$. This implies $m \subseteq \operatorname{rad}(\operatorname{ann}(M/qM))$. Since m is maximal, we must have $m = \operatorname{rad}(\operatorname{ann}(M/qM))$.

Proposition 8.26. *If R is any ring, M a finitely generated R-module, and $q \subseteq R$ an ideal, then $\operatorname{rad}(\operatorname{ann}(M/qM)) = \operatorname{rad}(q + \operatorname{ann}M)$.*

Proof. It suffices to show that a prime ideal P of R contains $\operatorname{ann}(M/qM)$ if and only if P contains $q + \operatorname{ann}M$.

A prime $P \supseteq \operatorname{ann}(M/qM)$ if and only if $(M/qM)_P \neq 0$. Note that $(M/qM)_P \cong M_P/q_P M_P$. By Nakayama's Lemma, $M_P/q_P M_P \neq 0$ if and only if $M_P \neq 0$ and $q_P \subseteq P_P$ (the maximal ideal of R_P). These conditions are equivalent to P not containing $\operatorname{ann}M$ (so $M_P \neq 0$) and $P \supseteq q$. Thus, P must contain both q and $\operatorname{ann}M$, which means $P \supseteq q + \operatorname{ann}M$. □

Proposition 8.27. *Let (R, m) be a local ring and M a finitely generated R-module. Let $q \subseteq m$ be an ideal. Then:*

1. *q has finite colength on M if and only if $m = \operatorname{rad}(q + \operatorname{ann}M)$, which is equivalent to q having finite colength on the ring $R/\operatorname{ann}M$.*
2. *If $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of R-modules, then q has finite colength on M if and only if q has finite colength on both M' and M''.*
3. *$\dim M$ is the least number d such that there exists an ideal of finite colength on M generated by d elements.*

Proof.

1. An ideal q has finite colength on $M \iff \operatorname{rad}(\operatorname{ann}(M/qM)) = m$. By the previous proposition, this is equivalent to $\operatorname{rad}(q + \operatorname{ann}M) = m$. The annihilator of the $R/\operatorname{ann}M$-module $(R/\operatorname{ann}M)/(q(R/\operatorname{ann}M))$ is precisely $q + \operatorname{ann}M$. Thus, q has finite colength on $R/\operatorname{ann}M \iff \operatorname{rad}(q + \operatorname{ann}M) = m$.
2. Suppose q has finite colength on M. Then $\operatorname{rad}(q + \operatorname{ann}M) = m$. Since $\operatorname{ann}M \subseteq \operatorname{ann}M' \cap \operatorname{ann}M''$, we have $q + \operatorname{ann}M \subseteq q + \operatorname{ann}M'$ and $q + \operatorname{ann}M \subseteq q + \operatorname{ann}M''$. Taking radicals, $m = \operatorname{rad}(q + \operatorname{ann}M) \subseteq \operatorname{rad}(q + \operatorname{ann}M')$ and $m \subseteq \operatorname{rad}(q + \operatorname{ann}M'')$. Since these radicals must be proper ideals, they must equal m. Thus q has finite colength on M' and M''.

   For the converse, tensoring the short exact sequence with R/q yields the exact sequence

   $$M'/qM' \to M/qM \to M''/qM'' \to 0.$$

   If M'/qM' and M''/qM'' have finite length, then any submodule and quotient module of M/qM have finite length, implying M/qM itself has finite length.
3. By definition, $\dim M = \dim(R/\operatorname{ann}M)$. By the first corollary, this is the smallest number d such that there exists an ideal $q = (x_1, \ldots, x_d)$ having finite colength on $R/\operatorname{ann}M$. By part (1), this is equivalent to q having finite colength on M.

□

Corollary 8.28. *If (R, m) is a local ring and M is a finitely generated R-module, then for any $x \in m$, we have*

$$\dim M - 1 \leq \dim(M/xM) \leq \dim M.$$

Proof. The second inequality is clear since $\operatorname{ann} M \subseteq \operatorname{ann}(M/xM)$. For the first, set $d = \dim(M/xM)$. Then there exists an ideal $q = (x_1, \ldots, x_d)$ of finite colength on M/xM. Thus, $M/(x,q)M = (M/xM)/q(M/xM)$ has finite length. This means the ideal $(x, x_1, \ldots, x_d)$ has finite colength on M. Therefore, $\dim M \leq d+1$, which implies $\dim M - 1 \leq d = \dim(M/xM)$. □

8.2.3 The Going-Down Theorem

Assume all rings are Noetherian.

Proposition 8.29. *Let (R, m) be a local ring and S be an R-algebra such that $mS \neq S$. Then codim$(mS) \leq \dim R$.*

Proof. Let $x_1, \ldots, x_d$ be a system of parameters in R, where $d = \dim R$. Then $\operatorname{rad}(x_1, \ldots, x_d) = m$. Any prime minimal over mS is also minimal over the ideal $I = (x_1, \ldots, x_d)S$. To see this, let P be a prime minimal over mS. Suppose $I \subseteq Q \subseteq P$ for some prime Q. Let $\varphi : R \to S$ be the algebra map. Then $(x_1, \ldots, x_d) \subseteq \varphi^{-1}(I) \subseteq \varphi^{-1}(Q) \subseteq \varphi^{-1}(P) = m$. Since $\operatorname{rad}(x_1, \ldots, x_d) = m$, we must have $\varphi^{-1}(Q) = m$. This implies $mS \subseteq Q$, so by minimality $P = Q$. The inequality follows from the Principal Ideal Theorem, as mS is contained in the radical of an ideal generated by d elements. □

Theorem 8.30. *Let $\varphi : (R, m) \to (S, n)$ be a homomorphism of local rings such that $\varphi(m) \subseteq n$. Then*

$$\dim S \leq \dim R + \dim(S/mS).$$

Proof. Set $d = \dim R$ and $e = \dim(S/mS)$. Let $x_1, \ldots, x_d \in m$ be a system of parameters for R, and let $y_1, \ldots, y_e \in n$ be elements whose images in S/mS form a system of parameters for S/mS. For $\alpha \gg 0$, we have $n^\alpha \subseteq (y_1, \ldots, y_e)S + mS$. For $\beta \gg 0$, we have $m^\beta \subseteq (x_1, \ldots, x_d)R$. Then, considering the images in S, we have $(mS)^\beta \subseteq (\varphi(x_1), \ldots, \varphi(x_d))S$. Combining these,

$$\begin{aligned} n^{\alpha\beta} &\subseteq ((y_1, \ldots, y_e)S + mS)^\beta \\ &\subseteq (y_1, \ldots, y_e)S + (mS)^\beta \\ &\subseteq (y_1, \ldots, y_e)S + (\varphi(x_1), \ldots, \varphi(x_d))S. \end{aligned}$$

Thus, n is in the radical of an ideal generated by $d+e$ elements. By the Principal Ideal Theorem, $\dim S \leq d+e$. □

Geometrically, this theorem suggests that if $f : X \to Y$ is a map of varieties (or schemes), the dimension of X is at most the sum of the dimension of Y and the dimension of a typical fiber of f.

Example 8.31. *Define $\varphi : \mathbb{C}[x] \to \mathbb{C}[x,y]/(x(y-1))$ and consider the induced map on local rings at the relevant maximal ideals.*

$$\mathbb{C}[x]_{(x)} \to (\mathbb{C}[x,y]/(x(y-1)))_{(x,y)}.$$

Let $R = \mathbb{C}[x]_{(x)}$ and $S = (\mathbb{C}[x,y]/(x(y-1)))_{(x,y)}$. Then $\dim R = 1$. The target ring is $S \cong (\mathbb{C}[x,y]_{(x,y)})/(x(y-1)) \cong (\mathbb{C}[x,y]_{(x,y)})/(x) \cong \mathbb{C}[y]_{(y)}$. So $\dim S = 1$. The fiber ring is $S/mS = S/(x)S \cong S$. Thus $\dim(S/mS) = 1$. Here, $\dim S = 1$ and $\dim R + \dim(S/mS) = 1 + 1 = 2$, so the inequality $\dim S \leq \dim R + \dim(S/mS)$ is strict.

For flat R-algebras, equality holds. To prove this, we need the following theorem.

Theorem 8.32 (Going-Down Theorem for Flat Extensions)**.** *Let $\varphi : R \to S$ be a ring homomorphism such that S is a flat R-module. If $P' \subset P$ are prime ideals of R and Q is a prime of S with $\varphi^{-1}(Q) = P$, then there exists a prime Q' of S contained in Q such that $\varphi^{-1}(Q') = P'$. In fact, Q' may be taken to be any prime of S contained in Q and minimal over $P'S$.*

Proof. Since $P'S \subseteq \varphi(P)S \subseteq Q$, we can find a prime $Q' \subseteq Q$ minimal over $P'S$. We may replace R with R/P' and S with $S/P'S$. The module $S/P'S \cong S \otimes_R R/P'$ is flat over R/P', so the hypotheses are preserved. This reduces the problem to the case where R is an integral domain and $P' = (0)$.

We need to show that $\varphi^{-1}(Q') = (0)$. Since S is flat over R, every non-zero-divisor in R maps to a non-zero-divisor in S. As R is a domain, every non-zero element of R is a non-zero-divisor. Now, Q' is a minimal prime of S (since $P' = (0)$), so it is an associated prime of S. Thus, every element of Q' is a zero-divisor in S. Therefore, no non-zero element of R can map into Q', which means $\varphi^{-1}(Q') = (0)$, as desired. □

Corollary 8.33. *Let $\varphi : (R, m) \to (S, n)$ be a homomorphism of local rings such that S is a flat R-module. Then*

$$\dim S = \dim R + \dim(S/mS).$$

Proof. We have already shown $\dim S \leq \dim R + \dim(S/mS)$. We need to prove the reverse inequality. Let $Q \subseteq S$ be a prime ideal minimal over mS such that $\dim(S/Q) = \dim(S/mS)$. The dimension formula for domains gives

$$\dim S \geq \dim(S/Q) + \operatorname{ht}(Q) = \dim(S/mS) + \operatorname{ht}(Q).$$

Thus, it suffices to show that $\operatorname{ht}(Q) \geq \dim R$.

Since Q contains mS, we have $\varphi^{-1}(Q) \supseteq m$. As n is the unique maximal ideal of S containing Q, we must have $\varphi^{-1}(n) = m$, and thus $\varphi^{-1}(Q) = m$. Let $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_d = m$ be a chain of prime ideals in R of length $d = \dim R$. Since $\varphi^{-1}(Q) = P_d$, by the Going-Down Theorem for flat extensions, there exists a prime $Q_{d-1} \subsetneq Q$ such that $\varphi^{-1}(Q_{d-1}) = P_{d-1}$. Applying the theorem repeatedly, we can construct a chain of primes $Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_d = Q$ such that $\varphi^{-1}(Q_i) = P_i$. Thus, $\operatorname{ht}(Q) \geq d = \dim R$. □

Corollary 8.34. *If R is a ring, then $\dim R[x] = 1 + \dim R$. In particular, if k is a field, $\dim k[x_1, \ldots, x_r] = r$.*

Proof. The second statement follows from the first by induction. For the first statement, if $P_0 \subsetneq \cdots \subsetneq P_d$ is a chain of primes in R, then $P_0R[x] \subsetneq \cdots \subsetneq P_dR[x] \subsetneq P_dR[x] + (x)$ is a chain of primes in $R[x]$ of length $d + 1$. Thus, $\dim R[x] \geq \dim R + 1$.

For the other inequality, it suffices to show that for any maximal ideal $Q \subset R[x]$, $\operatorname{ht}(Q) \leq \dim R_P + 1$, where $P = Q \cap R$. Let $Q \subset R[x]$ be a maximal ideal and let $P = Q \cap R$. The ring $R[x]_Q$ is a localization of $R_P[x]$. The map of local rings $R_P \to R[x]_Q$ is flat. The fiber ring is $R[x]_Q/PR[x]_Q \cong (R_P/PR_P)[x]_Q \cong k(P)[x]_Q$, where $k(P)$ is the residue field of R_P. This is a localization of a polynomial ring in one variable over a field, so its dimension is 1. Applying the previous corollary,

$$\dim R[x]_Q = \dim R_P + \dim(k(P)[x]_Q) = \dim R_P + 1.$$

Since $\operatorname{ht}(Q) = \dim R[x]_Q$, we have $\operatorname{ht}(Q) \leq \dim R + 1$. As this holds for any maximal ideal Q, we conclude $\dim R[x] \leq \dim R + 1$. □

8.2.4 Regular Local Rings

All rings are Noetherian. Let (R, m) be a local ring of dimension d. By the Principal Ideal Theorem, the minimal number of generators for m, denoted $\mu(m)$, is at least d.

Definition 8.35. *A local ring (R, m) is called **regular** if $\mu(m) = \dim R$. A system of parameters that generates m is called a **regular system of parameters**.*

Example 8.36. *Let $R = (\mathbb{C}[x, y]/(y^2 - x^3))_{(x,y)}$. The maximal ideal $m = (\bar{x}, \bar{y})$ is not principal. However, $m^2 = (\bar{x}^2, \bar{x}\bar{y}, \bar{y}^2) = (\bar{x}^2, \bar{x}\bar{y}, \bar{x}^3) \subseteq (\bar{x})$. Thus, $rad(\bar{x}) = m$, so $\dim R = 1$. Since $\mu(m) = 2 > \dim R = 1$, the ring R is not regular. This corresponds to the singularity (a cusp) at the origin of the curve $y^2 = x^3$.*

In algebraic geometry, a point on a scheme (or variety) is smooth if and only if its corresponding local ring is regular.

Proposition 8.37. *A regular local ring is an integral domain.*

Proof. Let (R, m) be a regular local ring. We proceed by induction on $d = \dim R$. If $d = 0$, then $m = (0)$, so R is a field and thus an integral domain. Assume $d > 0$. By Nakayama's Lemma, $m \neq m^2$. By prime avoidance, we can find an element $x \in m \setminus m^2$ that is not in any minimal prime of R. Let $S = R/(x)$ with maximal ideal $n = m/(x)$. Since x is not in any minimal prime, $\dim S = \dim R - 1 = d - 1$. The number of generators for n is $\mu(n)$. We have the map $m/m^2 \twoheadrightarrow n/n^2$. Since $x \in m \setminus m^2$, its image in m/m^2 is non-zero. The kernel of this map contains the image of x. Thus, $\dim_{R/m}(n/n^2) = \dim_{R/m}(m/m^2) - 1 = d - 1$. By Nakayama's Lemma, $\mu(n) = d - 1 = \dim S$. So S is a regular local ring. By the induction hypothesis, $S = R/(x)$ is an integral domain. This means (x) is a prime ideal in R. Since x was chosen not to be in any minimal prime of R, the prime ideal (x) must properly contain some minimal prime Q of R. Let $y \in Q$. Then $y \in (x)$, so $y = ax$ for some $a \in R$. Since $y \in Q$ and $x \notin Q$ (as (x) is not a minimal prime), we must have $a \in Q$. Thus $Q = mQ$. By Nakayama's Lemma, $Q = (0)$. Therefore, (0) is the unique minimal prime ideal, and R is an integral domain. □

Definition 8.38. *A sequence of elements $x_1, \ldots, x_d$ in a ring R is an **R-sequence** or **regular sequence** if $(x_1, \ldots, x_d)$ is a proper ideal and for each $i = 1, \ldots, d-1$, x_{i+1} is a non-zero-divisor in $R/(x_1, \ldots, x_i)$.*

In general, whether a sequence is regular can depend on the order of the elements.

Example 8.39. *In $\mathbb{C}[x, y, z]$, the sequence $x, y(1-x), z(1-x)$ is a regular sequence. However, the sequence $y(1-x), z(1-x), x$ is not, because $z(1-x)$ is a zero-divisor on $\mathbb{C}[x, y, z]/(y(1-x))$ (since $z(1-x) \cdot y = 0$ in the quotient).*

However, for a regular system of parameters in a local ring, the order does not matter.

Corollary 8.40. *Any regular system of parameters in a regular local ring is a regular sequence.*

Proof. Let $x_1, \ldots, x_d$ be a regular system of parameters for a regular local ring R. For each i, the ring $R_i = R/(x_1, \ldots, x_i)$ is a local ring of dimension $d - i$, and its maximal ideal is generated by the images of $x_{i+1}, \ldots, x_d$. Thus, R_i is a regular local ring for each i. By the previous proposition, each R_i is an integral domain. The image of x_{i+1} in R_i is non-zero (by minimality of generators), and since R_i is a domain, x_{i+1} is a non-zero-divisor. This holds for all i, so the sequence is regular. □

8.2.5 Discrete Valuation Rings

Regular local rings of dimension one correspond to smooth points on curves. These rings have a special name.

Definition 8.41. *A **discrete valuation ring** (DVR) is a regular local ring of dimension one.*

If R is a DVR, its maximal ideal is principal, $m = (\pi)$ for some $\pi \in R$. The element π is called a **uniformizing parameter**.

Proposition 8.42. *Let R be a DVR with uniformizing parameter π and field of fractions K. Then every non-zero element $t \in K$ can be uniquely written as $t = u\pi^n$ where $u \in R$ is a unit and $n \in \mathbb{Z}$. (The map $v : K^\times \to \mathbb{Z}$ defined by $t \mapsto n$ is the corresponding valuation). In particular, every non-zero ideal of R is of the form (π^n) for some $n \geq 0$, and R is a PID.*

Proof. By the Krull Intersection Theorem, $\bigcap_{i=1}^{\infty}(\pi^i) = (0)$. For any non-zero $s \in R$, we can choose the largest integer $n \geq 0$ such that $s \in (\pi^n)$. So, $s = u\pi^n$ for some $u \in R$. By maximality of n, $u \notin (\pi)$, which means u is a unit.

If $t \in K^\times$, we can write $t = s_1/s_2$ for $s_1, s_2 \in R \setminus \{0\}$. Write $s_1 = u_1\pi^{n_1}$ and $s_2 = u_2\pi^{n_2}$. Then $t = (u_1/u_2)\pi^{n_1 - n_2}$. The element u_1/u_2 is a unit in R. For uniqueness, if $u\pi^n = v\pi^m$ with u, v units, then $u/v = \pi^{m-n}$. Since u/v is a unit, we must have $m - n = 0$, so $m = n$ and thus $u = v$. □