Computational Commutative Algebra

Yash Sharma

CONTENTS

Contents

CHAPTER 1

FUNDAMENTALS OF COMMUTATIVE RINGS

Course Overview

This course focuses on **Computational Commutative Algebra**. The primary goal is to study commutative rings, ideals, and modules over them, with a specific emphasis on computational aspects and algorithms (e.g., using software like `Macaulay2`).

> **Remark 1.0.1: References**
> **Cox, Little, and O'Shea**: *Ideals, Varieties, and Algorithms.*[1]
> **Eisenbud**: *Commutative Algebra with a View Toward Algebraic Geometry.*[2]

1.1 Rings and Ideals

Definition of a Ring

Definition 1.1.1: Ring

A **ring** R is a set equipped with two binary operations: addition $(+)$ and multiplication $(\cdot)$, such that:

1. $(R, +)$ is an **abelian group**:
   - **Closure**: $a + b \in R$ for all $a, b \in R$.
   - **Associativity**: $(a + b) + c = a + (b + c)$ for all $a, b, c \in R$.
   - **Additive Identity**: There exists an element $0 \in R$ such that $a + 0 = a$ for all $a \in R$.
   - **Additive Inverse**: For every $a \in R$, there exists $-a \in R$ such that $a + (-a) = 0$.
   - **Commutativity**: $a + b = b + a$ for all $a, b \in R$.
2. Multiplication is **associative**: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$.

3. Multiplication **distributes** over addition:

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{and} \quad (b + c) \cdot a = b \cdot a + c \cdot a \quad \forall a, b, c \in R.$$

4. **Multiplicative Identity**: There exists an element $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in R$.

Definition 1.1.2: Commutative Ring

A ring R is said to be **commutative** if the multiplication operation is commutative, i.e.,

$$a \cdot b = b \cdot a \quad \forall a, b \in R.$$

Unless otherwise stated, all rings in this course are assumed to be commutative with identity 1.

Examples of Rings

Example 1.1.1: Standard Number Systems The following are commutative rings:

- $\mathbb{Z}$: The ring of integers.
- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$: The fields of rational, real, and complex numbers (every non-zero element has an inverse).

Example 1.1.2: Matrix Rings Let R be a commutative ring and $n \geq 1$ be an integer. Let $M_n(R)$ denote the set of $n \times n$ matrices with entries in R.

- Under usual matrix addition and multiplication, $M_n(R)$ is a ring.
- The additive identity is the zero matrix; the multiplicative identity is the identity matrix I_n.
- **Warning**: If $n \geq 2$, $M_n(R)$ is **not** commutative (since $AB \neq BA$ generally).

Example 1.1.3: Polynomial Rings Let R be a commutative ring. The polynomial ring in n variables, denoted $R[x_1, \ldots, x_n]$, consists of polynomials with coefficients in R:

$$p(x_1, \ldots, x_n) = \sum_{k_1, \ldots, k_n} c_{k_1, \ldots, k_n} x_1^{k_1} \cdots x_n^{k_n}$$

where only finitely many coefficients $c_{k_1, \ldots, k_n}$ are non-zero. This is a commutative ring.

—

1.2 Homomorphisms and Ideals

Ring Homomorphisms

Definition 1.2.1: Ring Homomorphism

Let R and S be rings. A function $\phi : R \to S$ is a **ring homomorphism** if for all $r, r' \in R$:

1. $\phi(r + r') = \phi(r) + \phi(r')$ (Preserves addition)
2. $\phi(r \cdot r') = \phi(r) \cdot \phi(r')$ (Preserves multiplication)
3. $\phi(1_R) = 1_S$ (Maps identity to identity)

Definition 1.2.2: Isomorphism

A homomorphism $\phi : R \to S$ is a **ring isomorphism** if it is bijective (one-to-one and onto). Alternatively, there exists $\psi : S \to R$ such that $\psi \circ \phi = \mathrm{id}_R$ and $\phi \circ \psi = \mathrm{id}_S$.

Example 1.2.1: Evaluation Map Let $\phi : R \to S$ be a ring map. Given $s_1, \dots, s_n \in S$, there exists a unique homomorphism $\tilde{\phi} : R[x_1, \dots, x_n] \to S$ defined by:

- $\tilde{\phi}(r) = \phi(r)$ for $r \in R$.
- $\tilde{\phi}(x_i) = s_i$ for each i.

This maps a polynomial $p(x_1, \dots, x_n)$ to its evaluation $p(s_1, \dots, s_n)$ inside S.

Ideals

Definition 1.2.3: Kernel

The **kernel** of a homomorphism $\phi : R \to S$ is the set:

$$\ker(\phi) = \{r \in R \mid \phi(r) = 0_S\}.$$

Definition 1.2.4: Ideal

A subset $I \subseteq R$ is an **ideal** if:

1. I is a subgroup of $(R, +)$ (i.e., $0 \in I$, and if $a, b \in I$, then $a - b \in I$).
2. **Absorption**: For every $r \in R$ and $a \in I$, the product $ra \in I$.

Proposition 1.2.1: Kernel is an Ideal

For any ring homomorphism $\phi : R \to S$, $\ker(\phi)$ is an ideal of R.

Definition 1.2.5: Generated Ideal

Let $G = \{g_1, \ldots, g_m\} \subseteq R$. The ideal generated by G, denoted $\langle g_1, \ldots, g_m \rangle$ or $(g_1, \ldots, g_m)$, is the set of all linear combinations:

$$(g_1, \ldots, g_m) = \left\{ \sum_{i=1}^{m} r_i g_i \mid r_i \in R \right\}.$$

If an ideal I admits a finite generating set, it is called **finitely generated**.

Example 1.2.2: Computing the Kernel Consider the homomorphism $\phi : \mathbb{Q}[x, y] \to \mathbb{Q}[t]$ defined by $\phi(x) = t^2$ and $\phi(y) = t^3$. We claim that $\ker(\phi) = \langle y^2 - x^3 \rangle$. **Proof**: Clearly, $y^2 - x^3 \in \ker(\phi)$ because $\phi(y^2 - x^3) = (t^3)^2 - (t^2)^3 = t^6 - t^6 = 0$. Thus $\langle y^2 - x^3 \rangle \subseteq \ker(\phi)$.

Conversely, let $p(x, y) \in \ker(\phi)$. We treat $p(x, y)$ as a polynomial in y with coefficients in $\mathbb{Q}[x]$. By the division algorithm (in one variable y), we can divide p by $y^2 - x^3$:

$$p(x, y) = q(x, y)(y^2 - x^3) + r(x, y)$$

where the remainder r has degree in y less than 2. Thus, $r(x, y) = r_0(x) + r_1(x)y$. Applying ϕ:

$$0 = \phi(p) = \phi(q) \cdot 0 + \phi(r_0(x)) + \phi(r_1(x))\phi(y) = r_0(t^2) + r_1(t^2)t^3.$$

Since $r_0(t^2)$ contains only even powers of t, and $r_1(t^2)t^3$ contains only odd powers of t, there can be no cancellation between them. For the sum to be the zero polynomial, both $r_0(x)$ and $r_1(x)$ must be zero. Thus, $r(x, y) = 0$, implying $p \in \langle y^2 - x^3 \rangle$.

—

1.3 Prime and Maximal Ideals

Prime and Maximal Ideals

Definition 1.3.1: Prime Ideal

An ideal $I \subsetneq R$ is a **prime ideal** if for any $r, s \in R$, $rs \in I$ implies $r \in I$ or $s \in I$.

Definition 1.3.2: Integral Domain

A ring R is an **integral domain** (or simply a domain) if it has no zero divisors, i.e., $rs = 0$ implies $r = 0$ or $s = 0$ (for $r, s \neq 0$).

Proposition 1.3.1: Domain Criterion

R/I is an integral domain if and only if I is a prime ideal.

Definition 1.3.3: Maximal Ideal

An ideal $I \subsetneq R$ is a **maximal ideal** if there is no proper ideal J such that $I \subsetneq J \subsetneq R$.

Proposition 1.3.2: Field Criterion

R/I is a field if and only if I is a maximal ideal.

Corollary 1.3.1: Maximal implies Prime Every maximal ideal is a prime ideal (since every field is an integral domain).

Quotient Rings and Correspondence

Definition 1.3.4: Quotient Ring

Let $I \subseteq R$ be an ideal. The quotient ring R/I is the set of cosets $\{r + I \mid r \in R\}$ with operations:

$$(r + I) + (s + I) = (r + s) + I$$

$$(r + I)(s + I) = rs + I$$

The zero element is $0 + I$ and the identity is $1 + I$.

Theorem 1.3.1: Correspondence Theorem

There is a bijective correspondence between the ideals of R containing I and the ideals of R/I.

$$\{J \text{ ideal of } R \mid I \subseteq J\} \longleftrightarrow \{\text{Ideals of } R/I\}$$

Under this map:

- Prime ideals correspond to prime ideals.
- Maximal ideals correspond to maximal ideals.

Operations on Ideals

Definition 1.3.5: Radical of an Ideal

The **radical** of an ideal I, denoted $\sqrt{I}$, is defined as:

$$\sqrt{I} = \{r \in R \mid r^n \in I \text{ for some } n \geq 1\}.$$

$\sqrt{I}$ is always an ideal containing I. If $\sqrt{I} = I$, the ideal is called a **radical ideal**.

Definition 1.3.6: Nilradical

The **nilradical** of R is $\sqrt{\langle 0 \rangle}$, the set of all nilpotent elements. It equals the intersection of all prime ideals of R.

—

1.4 Noetherian Rings and Algebras

Operations Continued

Definition 1.4.1: Product of Ideals

Let I, J be ideals. The product ideal IJ is generated by products of elements:

$$IJ = \langle \{ \sum a_i b_i \mid a_i \in I, b_i \in J \} \rangle.$$

Noetherian Rings

Definition 1.4.2: Noetherian Ring

A ring R is **Noetherian** if every ideal of R is finitely generated.

Theorem 1.4.1: Equivalent Conditions for Noetherian Rings

The following are equivalent for a ring R:

1. R is Noetherian (ideals are finitely generated).
2. **Ascending Chain Condition (ACC)**: Every ascending chain of ideals $I_1 \subseteq I_2 \subseteq \dots$ stabilizes (i.e., there exists N such that $I_n = I_N$ for all $n \geq N$).
3. Every non-empty set of ideals has a maximal element (with respect to inclusion).

Example 1.4.1: Examples

- Fields and Principal Ideal Domains (PIDs) like $\mathbb{Z}$ and $k[x]$ are Noetherian.
- If R is Noetherian, then R/I is Noetherian.

Algebras and Finite Generation

Definition 1.4.3: R-Algebra

Let R be a ring. An **R-algebra** is a ring S equipped with a ring homomorphism $\phi : R \to S$.

Definition 1.4.4: Finite Type

An R-algebra S is **finitely generated** (of finite type) if there exist elements $s_1, \dots, s_n \in S$ such that the evaluation map $\phi : R[x_1, \dots, x_n] \to S$ (sending $x_i \mapsto s_i$) is surjective. Equivalently, $S \cong R[x_1, \dots, x_n]/I$.

Theorem 1.4.2: Hilbert Basis Theorem

If R is a Noetherian ring, then the polynomial ring $R[x_1, \dots, x_n]$ is Noetherian.

—

1.5 Monomial Ideals and Dickson's Lemma

We focus on the proof of the Hilbert Basis Theorem for the case $R = k[x_1, \dots, x_n]$ where k is a field.

Monomial Ideals

Definition 1.5.1: Monomial Ideal

An ideal $I \subseteq k[x_1, \dots, x_n]$ is a **monomial ideal** if it is generated by monomials. That is, $I = \langle x^\alpha \mid \alpha \in A \rangle$ for some set $A \subseteq \mathbb{N}^n$.

Lemma 1.5.1: Property of Monomial Ideals

A polynomial $f = \sum c_\alpha x^\alpha$ belongs to a monomial ideal I if and only if each term x^α (where $c_\alpha \neq 0$) lies in I.

Dickson's Lemma

Lemma 1.5.2: Dickson's Lemma

Every monomial ideal $I \subseteq k[x_1, \dots, x_n]$ is finitely generated.

Proof (Induction on n):

- **Base Case ($n = 1$)**: $I \subseteq k[x]$. Let $J = \{\deg(f) \mid f \in I, f \text{ monomial}\} \subseteq \mathbb{N}$. Since $\mathbb{N}$ is well-ordered, there is a least degree d. Then $I = \langle x^d \rangle$.

- **Inductive Step**: Assume the lemma holds for $n-1$ variables. Let $I \subseteq k[x_1, \dots, x_n]$ be a monomial ideal. We view monomials in R as $m = m' x_n^k$, where m' is a monomial in $x_1, \dots, x_{n-1}$.

  For each $j \geq 0$, let I_j be the ideal in $k[x_1, \dots, x_{n-1}]$ generated by monomials m' such that $m' x_n^j \in I$. Note that $I_0 \subseteq I_1 \subseteq \dots$ is an ascending chain of ideals in $k[x_1, \dots, x_{n-1}]$.

By the inductive hypothesis, $k[x_1, \dots, x_{n-1}]$ is Noetherian, so this chain stabilizes at some N. That is, $I_N = I_{N+1} = \dots$. Also, each I_j is finitely generated (say by a set G_j) by the inductive hypothesis.

We claim that the set $G = \bigcup_{j=0}^{N} \{g \cdot x_n^j \mid g \in G_j\}$ generates I. Since this is a finite union of finite sets, I is finitely generated.

—

1.6 Monomial Orders and Initial Ideals

Monomial Orders

To perform division in multiple variables, we need to order monomials.

Definition 1.6.1: Monomial Ordering

A **monomial ordering** $>$ on $k[x_1, \dots, x_n]$ is a relation on the set of monomials such that:

1. $>$ is a total (linear) ordering.
2. $>$ is a **well-ordering** (every non-empty set of monomials has a smallest element).
3. If $x^\alpha > x^\beta$, then $x^\alpha x^\gamma > x^\beta x^\gamma$ for any γ.

Example 1.6.1: Examples of Orders

- **Lexicographic (Lex)**: $x^\alpha >_{lex} x^\beta$ if the first non-zero entry of $\alpha - \beta$ is positive. (Dictionary order).
- **Graded Lex (Glex)**: Compare total degree first ($|\alpha| > |\beta|$). If degrees are equal, use Lex.

Initial Ideals and Hilbert Basis Theorem

Definition 1.6.2: Initial Term

Fix a monomial order $>$. For any non-zero polynomial f, the **initial term** (or leading term), denoted $in_>(f)$ or $LT(f)$, is the largest monomial appearing in f.

Definition 1.6.3: Initial Ideal

For an ideal I, the **initial ideal** is the ideal generated by the leading terms of all elements in I:

$$in_>(I) = \langle in_>(f) \mid f \in I \rangle.$$

Theorem 1.6.1: Hilbert Basis Theorem (Proof Strategy)

Theorem: $R = k[x_1, \dots, x_n]$ is Noetherian.

Proof: Let $I \subseteq R$ be an ideal. Pick a monomial order $>$. Consider the monomial ideal $J = in_>(I)$. By Dickson's Lemma, J is finitely generated, say $J = \langle m_1, \dots, m_k \rangle$. Since $m_i \in in_>(I)$, there exist polynomials $g_1, \dots, g_k \in I$ such that $in_>(g_i) = m_i$.

Claim: $I = \langle g_1, \dots, g_k \rangle$. Let $f \in I$. We can use the multivariate division algorithm (generalized) to divide f by $\{g_1, \dots, g_k\}$.

$$f = \sum q_i g_i + r$$

where no term of r is divisible by any $in_>(g_1), \dots, in_>(g_k)$. However, $f \in I$ and $\sum q_i g_i \in I$, so $r \in I$. If $r \neq 0$, then $in_>(r) \in in_>(I)$. But $in_>(I) = \langle in_>(g_1), \dots, in_>(g_k) \rangle$, meaning $in_>(r)$ must be divisible by some $in_>(g_i)$. This contradicts the property of the remainder r (that no term is divisible by $LT(g_i)$). Therefore, r must be 0. Thus $f = \sum q_i g_i$, so I is finitely generated.

—

1.7 Division Algorithm

Theorem 1.7.1: Division Algorithm in $k[x_1, \dots, x_n]$

Fix a monomial order $>$ on $R = k[x_1, \dots, x_n]$. Let $F = (g_1, \dots, g_s)$ be an ordered s-tuple of polynomials in R. Then every $f \in R$ can be written as:

$$f = a_1 g_1 + \cdots + a_s g_s + r$$

where $a_i, r \in R$, and either $r = 0$ or no monomial appearing in r is divisible by any of $in_>(g_1), \dots, in_>(g_s)$. The polynomial r is called the **remainder** of f on division by F.

Remark 1.7.1: Note on Uniqueness Unlike the one-variable case, the remainder r in multivariate division is **not** necessarily unique; it depends on the ordering of the divisors $(g_1, \dots, g_s)$.

CHAPTER 2

GRÖBNER BASES AND ALGEBRAIC GEOMETRY

2.1 Gröbner Bases and the Division Algorithm

Uniqueness of Remainder

We begin by recalling the division algorithm in $R = \mathbb{K}[x_1, \ldots, x_n]$. While the quotient in the division algorithm depends on the order of the divisors, the remainder is unique *if* we divide by a Gröbner basis.

Lemma 2.1.1: Uniqueness of Remainder

Let $I \subseteq R$ be an ideal and $G = \{g_1, \ldots, g_m\}$ be a Gröbner basis for I. Let $f \in R$. Suppose there are two expressions for f resulting from the division algorithm:

$$f = \sum_{i=1}^{m} a_i g_i + r \quad \text{and} \quad f = \sum_{i=1}^{m} a'_i g_i + r'$$

where r and r' are remainders (i.e., no term of r or r' is divisible by any leading term in $\mathrm{LT}(G)$). Then $r = r'$.

Proof. Consider the difference between the two expressions:

$$0 = \sum_{i=1}^{m} (a_i - a'_i) g_i + (r - r').$$

Rearranging terms, we get:

$$r' - r = \sum_{i=1}^{m} (a_i - a'_i) g_i.$$

The right-hand side is clearly an element of the ideal I generated by G. Thus, $r' - r \in I$.

Suppose $r \neq r'$. Then $r' - r \neq 0$. Since G is a Gröbner basis for I, by definition, the leading term of any non-zero element in I must be divisible by the leading term of some generator in G. Therefore:

$$\mathrm{LT}(r' - r) \in \langle \mathrm{LT}(g) \mid g \in G \rangle.$$

However, $r' - r$ is a difference of remainders. Both r and r' contain only terms that are *not* divisible by any $\mathrm{LT}(g_i)$. Consequently, any term in their difference (including the leading term) cannot be divisible by any $\mathrm{LT}(g_i)$.

This is a contradiction. Therefore, we must have $r - r' = 0$, which implies $r = r'$. □

Ideal Membership Test

The uniqueness of the remainder modulo a Gröbner basis provides a distinct algorithmic method for checking ideal membership.

Definition 2.1.1: Normal Form / Remainder

Let G be a Gröbner basis for an ideal I. For any $f \in R$, the element r obtained from the division algorithm is called the **remainder** or **normal form** of f with respect to G, denoted as $\overline{f}^G$ or $\mathrm{rem}_G(f)$.

Proposition 2.1.1: Ideal Membership Test

Let I be an ideal and $G = \{g_1, \ldots, g_m\}$ be a Gröbner basis for I. Let $f \in R$. Then:

$$f \in I \iff \mathrm{rem}_G(f) = 0.$$

Proof. ($\Leftarrow$) If $\mathrm{rem}_G(f) = 0$, then the division algorithm yields $f = \sum a_i g_i + 0$. Since $g_i \in I$, clearly $f \in I$.

($\Rightarrow$) Let $f \in I$. Let $r = \mathrm{rem}_G(f)$. We can write $r = f - \sum a_i g_i$. Since $f \in I$ and $\sum a_i g_i \in I$, it follows that $r \in I$. If $r \neq 0$, then $\mathrm{LT}(r) \in \langle \mathrm{LT}(G) \rangle$ because G is a Gröbner basis. This means $\mathrm{LT}(r)$ is divisible by some $\mathrm{LT}(g_i)$. But this contradicts the definition of the remainder (no term of r is divisible by $\mathrm{LT}(G)$). Thus, we must have $r = 0$. □

2.2 Varieties and The Nullstellensatz

Source Reference:

Affine Varieties

Let $\mathbb{K}$ be an algebraically closed field. Let $R = \mathbb{K}[x_1, \ldots, x_n]$.

Definition 2.2.1: Affine Variety

Let $I \subseteq R$ be an ideal. The **affine variety** defined by I, denoted $\mathbf{V}(I)$, is the set of all common zeros of polynomials in I:

$$\mathbf{V}(I) = \{\mathbf{a} \in \mathbb{K}^n \mid f(\mathbf{a}) = 0 \quad \forall f \in I\}.$$

Remark 2.2.1: Generators Suffice If $I = \langle g_1, \ldots, g_m \rangle$, then $\mathbf{a} \in \mathbf{V}(I)$ if and only if $g_i(\mathbf{a}) = 0$ for all $i = 1, \ldots, m$.

Properties of Varieties

Let I and J be ideals in R. We have the following properties relating algebraic operations on ideals to geometric operations on varieties.

Proposition 2.2.1: Properties

1. $I \subseteq J \implies \mathbf{V}(J) \subseteq \mathbf{V}(I)$ (order-reversing).
2. $\mathbf{V}(I \cap J) = \mathbf{V}(IJ) = \mathbf{V}(I) \cup \mathbf{V}(J)$.
3. $\mathbf{V}(I + J) = \mathbf{V}(I) \cap \mathbf{V}(J)$.
4. $\mathbf{V}(\sqrt{I}) = \mathbf{V}(I)$.

Selected Proofs. **Proof of (2):** $\mathbf{V}(IJ) = \mathbf{V}(I) \cup \mathbf{V}(J)$. Since $IJ \subseteq I \cap J \subseteq I$, we have $\mathbf{V}(I) \subseteq \mathbf{V}(I \cap J) \subseteq \mathbf{V}(IJ)$. Similarly $\mathbf{V}(J) \subseteq \mathbf{V}(IJ)$. Thus $\mathbf{V}(I) \cup \mathbf{V}(J) \subseteq \mathbf{V}(IJ)$.

Conversely, let $\mathbf{a} \in \mathbf{V}(IJ)$. Suppose $\mathbf{a} \notin \mathbf{V}(I)$. Then there exists $f \in I$ such that $f(\mathbf{a}) \neq 0$. For any $g \in J$, the product $fg \in IJ$, so $(fg)(\mathbf{a}) = f(\mathbf{a})g(\mathbf{a}) = 0$. Since $f(\mathbf{a}) \neq 0$, we must have $g(\mathbf{a}) = 0$. Since this holds for all $g \in J$, $\mathbf{a} \in \mathbf{V}(J)$. Thus $\mathbf{V}(IJ) \subseteq \mathbf{V}(I) \cup \mathbf{V}(J)$.

Proof of (3): $\mathbf{V}(I+J) = \mathbf{V}(I) \cap \mathbf{V}(J)$. $I \subseteq I+J$ implies $\mathbf{V}(I+J) \subseteq \mathbf{V}(I)$. Similarly $\mathbf{V}(I+J) \subseteq \mathbf{V}(J)$. Hence $\mathbf{V}(I+J) \subseteq \mathbf{V}(I) \cap \mathbf{V}(J)$. Conversely, if $\mathbf{a} \in \mathbf{V}(I) \cap \mathbf{V}(J)$, then $f(\mathbf{a}) = 0$ for all $f \in I$ and $g(\mathbf{a}) = 0$ for all $g \in J$. Any element in $I + J$ is of the form $f + g$, and $(f+g)(\mathbf{a}) = f(\mathbf{a}) + g(\mathbf{a}) = 0$. Thus $\mathbf{a} \in \mathbf{V}(I + J)$. □

Weak Nullstellensatz

The fundamental link between algebra and geometry is Hilbert's Nullstellensatz. We start with the "Weak" version.

Theorem 2.2.1: Weak Nullstellensatz

Let $\mathbb{K}$ be an algebraically closed field and $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be an ideal. Then:

$$\mathbf{V}(I) = \emptyset \iff I = R \quad \text{(i.e., } 1 \in I).$$

Corollary 2.2.1: Consistency of SystemsA system of polynomial equations $f_1 = 0, \ldots, f_m = 0$ has a solution in $\mathbb{K}^n$ (where $\mathbb{K}$ is algebraically closed) if and only if $1 \notin \langle f_1, \ldots, f_m \rangle$. Equivalently, the reduced Gröbner basis of I is not $\{1\}$.

2.3 Versions of Nullstellensatz

Source Reference:

We explore the connection between maximal ideals and points in $\mathbb{K}^n$.

Theorem 2.3.1: Nullstellensatz Version 2 (Maximal Ideals)

Let $\mathbb{K}$ be an algebraically closed field. Let $\mathfrak{m}$ be a maximal ideal of $R = \mathbb{K}[x_1, \ldots, x_n]$. Then there exists a point $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{K}^n$ such that:

$$\mathfrak{m} = \langle x_1 - a_1, \ldots, x_n - a_n \rangle.$$

Remark 2.3.1: Points define Maximal Ideals For any field $\mathbb{K}$ (not necessarily algebraically closed), the ideal $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ is always maximal. **Proof:** Consider the evaluation homomorphism $ev_{\mathbf{a}} : R \to \mathbb{K}$ defined by $f \mapsto f(\mathbf{a})$. This map is surjective. The kernel is exactly $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$. By the First Isomorphism Theorem, $R/\ker(ev_{\mathbf{a}}) \cong \mathbb{K}$. Since $\mathbb{K}$ is a field, the kernel is maximal.

Proof of Nullstellensatz Version 2 (assuming Weak NS)

Let $\mathfrak{m}$ be a maximal ideal. Since $\mathfrak{m} \neq R$, by the Weak Nullstellensatz, $\mathbf{V}(\mathfrak{m}) \neq \emptyset$. Let $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbf{V}(\mathfrak{m})$. Consider the ideal corresponding to the point $\mathbf{a}$, denoted $I_{\mathbf{a}} = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$. Since $\mathbf{a} \in \mathbf{V}(\mathfrak{m})$, every function $f \in \mathfrak{m}$ vanishes at $\mathbf{a}$. However, $I_{\mathbf{a}}$ consists of *all* polynomials vanishing at $\mathbf{a}$. Thus, $\mathfrak{m} \subseteq I_{\mathbf{a}}$. Since $\mathfrak{m}$ is maximal and $I_{\mathbf{a}} \neq R$, we must have $\mathfrak{m} = I_{\mathbf{a}}$.

Proof of Weak NS (assuming Version 2)

Suppose $I \neq R$. We want to show $\mathbf{V}(I) \neq \emptyset$. Since R is Noetherian, every proper ideal is contained in a maximal ideal $\mathfrak{m}$. By Version 2, $\mathfrak{m} = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ for some $\mathbf{a}$. Thus $I \subseteq \mathfrak{m}$. Since every $f \in \mathfrak{m}$ vanishes at $\mathbf{a}$, and $I \subseteq \mathfrak{m}$, every $f \in I$ vanishes at $\mathbf{a}$. Therefore, $\mathbf{a} \in \mathbf{V}(I)$, so $\mathbf{V}(I) \neq \emptyset$.

2.4 The Classical Nullstellensatz

Source Reference:

Theorem 2.4.1: Hilbert's Strong Nullstellensatz

Let $\mathbb{K}$ be an algebraically closed field and $I \subseteq R$ be an ideal. Then:

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

> That is, if a polynomial f vanishes at all points where polynomials in I vanish, then some power of f belongs to I.

*

Proof (Rabinowitsch Trick) Let $I = \langle f_1, \dots, f_r \rangle \subseteq \mathbb{K}[x_1, \dots, x_n]$. Let $f \in \mathbf{I}(\mathbf{V}(I))$. We want to show $f \in \sqrt{I}$, i.e., $f^m \in I$ for some m.

Introduce a new variable Y. Consider the ring $S = \mathbb{K}[x_1, \dots, x_n, Y]$. Let J be the ideal in S generated by I and the polynomial $1 - Yf$:

$$J = \langle f_1, \dots, f_r, 1 - Yf \rangle \subseteq S.$$

We claim $\mathbf{V}(J) = \emptyset$ in $\mathbb{K}^{n+1}$. Suppose there exists a point $(\mathbf{a}, b) \in \mathbf{V}(J)$. Then $f_i(\mathbf{a}) = 0$ for all i, which implies $\mathbf{a} \in \mathbf{V}(I)$. By assumption, f vanishes on $\mathbf{V}(I)$, so $f(\mathbf{a}) = 0$. However, the condition $1 - Yf = 0$ at this point implies $1 - b \cdot f(\mathbf{a}) = 1 - b \cdot 0 = 1 \neq 0$. Contradiction.

By the Weak Nullstellensatz applied to S, $J = S$, so $1 \in J$. Therefore, we can write:

$$1 = \sum_{i=1}^{r} A_i(x_1, \dots, Y) f_i + B(x_1, \dots, Y)(1 - Yf).$$

Now consider the homomorphism $S \to \mathbb{K}(x_1, \dots, x_n)$ mapping $Y \mapsto 1/f$. Under this map, $1 - Yf \mapsto 0$. The equation becomes:

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

Multiplying by a sufficiently high power of f (say f^m) to clear denominators, we get:

$$f^m = \sum_{i=1}^{r} (\text{poly}) f_i \in I.$$

Thus $f \in \sqrt{I}$.

2.5 Buchberger's Algorithm and Quotient Rings

Source Reference:

How do we actually compute Gröbner bases?

S-Polynomials

Definition 2.5.1: S-Polynomial

Let $f, g \in R$ be non-zero polynomials. Let $x^\alpha = \mathrm{LM}(f)$ and $x^\beta = \mathrm{LM}(g)$. Let $x^\gamma = \mathrm{lcm}(x^\alpha, x^\beta)$. The **S-polynomial** of f and g is:

$$S(f, g) = \frac{x^\gamma}{\mathrm{LT}(f)} \cdot f - \frac{x^\gamma}{\mathrm{LT}(g)} \cdot g.$$

The S-polynomial is designed to cancel the leading terms of f and g.

Buchberger's Criterion and Algorithm

Theorem 2.5.1: Buchberger's Criterion

A set $G = \{g_1, \ldots, g_m\}$ is a Gröbner basis for the ideal $I = \langle G \rangle$ if and only if for all pairs $i \neq j$,

$$\mathrm{rem}_G(S(g_i, g_j)) = 0.$$

Definition 2.5.2: Buchberger's Algorithm

Input: $F = \{f_1, \ldots, f_r\}$. **Output:** A Gröbner basis G for $\langle F \rangle$.

```
set $G := F$.
REPEAT:
    Select a pair $f, g \in G$ not yet considered.
    Compute $h = \mathrm{rem}_G(S(f, g))$.
    If $h \neq 0$, add $h$ to $G$ ($G := G \cup \{h\}$).
UNTIL all pairs satisfy $\mathrm{rem}_G(S(f, g)) = 0$.
```

This process terminates because R is Noetherian (ideals cannot grow strictly strictly indefinitely).

Quotient Rings and Vector Space Bases

Gröbner bases allow us to understand the structure of the quotient ring R/I.

Proposition 2.5.1: Macaulay's Basis Theorem

Let $I \subseteq R$ be an ideal and fixing a monomial order $>$. The set of monomials

$$B = \{x^\alpha \mid x^\alpha \notin \mathrm{LT}(I)\}$$

forms a $\mathbb{K}$-vector space basis for the quotient ring R/I. Note: $\mathrm{LT}(I)$ is the ideal generated by leading terms of all elements in I (which equals $\langle \mathrm{LT}(g) \mid g \in G \rangle$).

Proof. **Linear Independence:** Suppose $\sum c_i m_i = 0$ in R/I where $m_i \in B$. Then $f = \sum c_i m_i \in I$. If $f \neq 0$, then $\mathrm{LT}(f) \in \mathrm{LT}(I)$. But $\mathrm{LT}(f)$ is one of the m_i, which are defined to be outside $\mathrm{LT}(I)$. Contradiction. **Spanning:** For any $f \in R$, $f = q + r$ where $r = \mathrm{rem}_G(f)$. The terms of r are not in $\mathrm{LT}(I)$, so r is a linear combination of elements in B. Since $f \equiv r \pmod{I}$, B spans R/I. □

Finiteness of Variety

Theorem 2.5.2: Finiteness Criterion

Let $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ where $\mathbb{K}$ is algebraically closed. The following are equivalent:

1. $\mathbf{V}(I)$ is a finite set.
2. $\dim_{\mathbb{K}}(R/I) < \infty$.
3. For each $i \in \{1, \ldots, n\}$, there exists $m_i \geq 0$ such that $x_i^{m_i} \in \mathrm{LT}(I)$.
4. If G is a GB for I, then for each i, there is some $g \in G$ such that $\mathrm{LM}(g) = x_i^k$ for some k.

2.6 Elimination Theory

Source Reference:

Elimination theory generalizes Gaussian elimination to higher degree polynomials. We want to eliminate variables $x_1, \ldots, x_k$ from an ideal I to find relations among the remaining variables.

Elimination Ideals

Definition 2.6.1: Elimination Ideal

Given $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$, the k-th **elimination ideal** is:

$$I_k = I \cap \mathbb{K}[x_{k+1}, \ldots, x_n].$$

The Elimination Theorem

Theorem 2.6.1: Elimination Theorem

Let $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ and let G be a Gröbner basis for I with respect to the **lexicographic order** where $x_1 > x_2 > \cdots > x_n$. Then for any $0 \leq k < n$, the set

$$G_k = G \cap \mathbb{K}[x_{k+1}, \ldots, x_n]$$

is a Gröbner basis for the k-th elimination ideal I_k.

Proof. Clearly $G_k \subseteq I_k$. We need to show that $\langle \mathrm{LT}(G_k) \rangle = \mathrm{LT}(I_k)$. Let $f \in I_k$. Then $f \in I$, so $\mathrm{LT}(f)$ is divisible by $\mathrm{LT}(g)$ for some $g \in G$. Since $f \in \mathbb{K}[x_{k+1}, \ldots, x_n]$, $\mathrm{LT}(f)$ involves only variables $x_{k+1}, \ldots, x_n$. Because of the lexicographic order ($x_1 > \cdots > x_k > \ldots$), if $\mathrm{LT}(g)$ divides a term involving only $x_{k+1}, \ldots, x_n$, then $\mathrm{LT}(g)$ itself can only involve $x_{k+1}, \ldots, x_n$. Since $g \in G$, this implies $g \in \mathbb{K}[x_{k+1}, \ldots, x_n]$ (any term with $x_1, \ldots, x_k$ would be greater than $\mathrm{LT}(g)$, which is impossible). Thus $g \in G_k$. Therefore, $\mathrm{LT}(f)$ is divisible by $\mathrm{LT}(g)$ where $g \in G_k$, proving G_k is a GB for I_k. □

Application: Kernel of Ring Homomorphisms

Let $\phi : R = \mathbb{K}[y_1, \ldots, y_m] \to S = \mathbb{K}[x_1, \ldots, x_n]$ be a ring homomorphism defined by $\phi(y_i) = f_i(x_1, \ldots, x_n)$. We want to find $\ker(\phi)$.

Consider the ideal J in $\mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_m]$ generated by the graphs of the maps:

$$J = \langle y_1 - f_1, \ldots, y_m - f_m \rangle.$$

Then:

$$\ker(\phi) = J \cap \mathbb{K}[y_1, \ldots, y_m].$$

To compute this, calculate a Gröbner basis for J using an elimination order where x's $> y$'s. The elements of the GB that contain only y variables generate the kernel.

CHAPTER 3

MODULES AND LOCALIZATION

3.1 Modules

Definition and Basic Examples

Definition 3.1.1: R-Module

Let R be a ring. By an **R-module**, we mean an abelian group $(M, +)$ equipped with an action by R (scalar multiplication) $R \times M \to M$, denoted $(r, m) \mapsto r \cdot m$, satisfying the following axioms for all $r, r_1, r_2 \in R$ and $x, x_1, x_2 \in M$:

1. $1_R \cdot x = x$ (Identity).
2. $(r_1 + r_2) \cdot x = r_1 \cdot x + r_2 \cdot x$ (Distributivity in R).
3. $r \cdot (x_1 + x_2) = r \cdot x_1 + r \cdot x_2$ (Distributivity in M).
4. $(r_1 r_2) \cdot x = r_1 \cdot (r_2 \cdot x)$ (Associativity).

Example 3.1.1: Standard Examples

1. If $R = k$ is a field, a k-module is exactly a **k-vector space**.
2. If $R = \mathbb{Z}$, a $\mathbb{Z}$-module is exactly an **abelian group**.
3. If R is any ring, R itself is an R-module (via ring multiplication).
4. If $I \subseteq R$ is an ideal, then I is an R-module. Furthermore, the quotient ring R/I is an R-module via the action $r \cdot (r' + I) := rr' + I$.

Example 3.1.2: Modules via Algebras Let R and S be rings. If S is an **R-algebra** (i.e., there exists a ring homomorphism $\varphi : R \to S$), then S becomes an R-module via the action:

$$r \cdot s := \varphi(r)s$$

where the product on the right is the ring product in S.

Furthermore, if N is an S-module, it naturally becomes an R-module through φ, defined by:

$$r \cdot y := \varphi(r)y \quad \text{for } r \in R, y \in N.$$

Module Homomorphisms

Definition 3.1.2: R-Module Homomorphism

Let M and N be R-modules. An **R-module homomorphism** (or R-linear map) is a function $f : M \to N$ such that:

1. f is a group homomorphism: $f(x + y) = f(x) + f(y)$.
2. f preserves scalars: $f(rx) = rf(x)$ for all $r \in R, x \in M$.

Remark 3.1.1: Structure of Hom The set of all R-linear maps from M to N is denoted by $\mathrm{Hom}_R(M, N)$. This set itself forms an R-module defined by pointwise addition and scalar multiplication:

- $(f + g)(x) = f(x) + g(x)$
- $(r \cdot f)(x) = f(rx)$ (Note: if R is commutative).

Definition 3.1.3: Isomorphism

An R-linear map $f : M \to N$ is an **isomorphism** if there exists an R-linear map $g : N \to M$ such that $f \circ g = \mathrm{id}_N$ and $g \circ f = \mathrm{id}_M$. This is equivalent to f being bijective.

Direct Sums and Free Modules

Definition 3.1.4: Direct Sum

Let $\{M_\lambda\}_{\lambda \in \Lambda}$ be a family of R-modules. The **direct sum** is defined as:

$$\bigoplus_{\lambda \in \Lambda} M_\lambda = \{(x_\lambda)_{\lambda \in \Lambda} \mid x_\lambda \in M_\lambda, \text{ and } x_\lambda = 0 \text{ for all but finitely many } \lambda\}$$

Example 3.1.3: Polynomial Ring The polynomial ring $R[x_1, \ldots, x_n]$ can be viewed as a direct sum of copies of R indexed by monomials, or simply as R-modules.

Definition 3.1.5: Free Module

An R-module M is said to be **free** if it is isomorphic to a direct sum of copies of

R:

$$M \cong \bigoplus_{\lambda \in \Lambda} R$$

for some index set Λ. The set corresponding to the basis elements e_λ is called a **basis**.

Example 3.1.4: Free vs Non-Free

1. If k is a field, every k-vector space is a free module.
2. If R has a non-zero proper ideal I, then R/I is **not** a free R-module (due to torsion: for any $a \in I$, $a \cdot \bar{1} = \bar{0}$ in R/I).

Finitely Generated and Finitely Presented Modules

Definition 3.1.6: Finitely Generated (f.g.)

An R-module M is **finitely generated** if there exists a finite subset $\{x_1, \dots, x_n\} \subseteq M$ such that every $y \in M$ can be written as:

$$y = \sum_{i=1}^{n} r_i x_i, \quad r_i \in R.$$

This is equivalent to the existence of a surjective R-linear map:

$$\varphi : R^n \to M \twoheadrightarrow 0.$$

Definition 3.1.7: Finitely Presented (f.p.)

An R-module M is **finitely presented** if there exists an exact sequence:

$$R^m \xrightarrow{\psi} R^n \xrightarrow{\varphi} M \to 0$$

for finite integers m, n. Equivalently, M is finitely generated ($M \cong R^n / \ker \varphi$) and the kernel of the surjection, $\ker \varphi$, is also finitely generated.

Remark 3.1.2: Presentation Matrix If M is finitely presented, $M \cong \operatorname{coker}(\psi)$. The map $\psi : R^m \to R^n$ can be represented by an $n \times m$ matrix $A = (a_{ij})$ where $\psi(e_j) = \sum_i a_{ij} e_i$.

3.2 Modules II - Exact Sequences and Noetherian Modules

Exact Sequences

Definition 3.2.1: Exact Sequence

A sequence of R-modules and homomorphisms:

$$\cdots \to M_{i-1} \xrightarrow{f} M_i \xrightarrow{g} M_{i+1} \to \ldots$$

is said to be **exact at M_i** if $\mathrm{Im}(f) = \ker(g)$.

Definition 3.2.2: Short Exact Sequence

A sequence $0 \to N \xrightarrow{f} M \xrightarrow{g} P \to 0$ is a **short exact sequence** if:

- f is injective (exact at N).
- g is surjective (exact at P).
- $\mathrm{Im}(f) = \ker(g)$ (exact at M).

This implies $P \cong M/N$ (identifying N with $\mathrm{Im}(f)$).

Noetherian Modules

Proposition 3.2.1: Equivalent Conditions for Noetherian Modules

Let M be an R-module. The following are equivalent (FAE):

1. **ACC:** Every ascending chain of submodules $M_1 \subseteq M_2 \subseteq \ldots$ stabilizes (i.e., $\exists n$ such that $M_n = M_{n+1} = \ldots$).
2. **Maximum Condition:** Every non-empty collection of submodules has a maximal element (with respect to inclusion).
3. **Finite Generation:** Every submodule of M is finitely generated.

If these conditions hold, M is called a **Noetherian Module**.

Remark 3.2.1: Ring vs ModuleA ring R is a Noetherian ring if it is a Noetherian module over itself (i.e., every ideal is finitely generated).

Proposition 3.2.2: Exactness and Noetherian Property

Consider a short exact sequence $0 \to M_1 \to M_2 \to M_3 \to 0$. Then:

$$M_2 \text{ is Noetherian} \iff M_1 \text{ and } M_3 \text{ are Noetherian.}$$

Proposition 3.2.3: Relation between f.g. and f.p.

Let R be a ring and M an R-module.

1. If R is Noetherian and M is finitely generated, then M is finitely presented. (Because the kernel of the surjection $R^n \to M$ is a submodule of a Noetherian module R^n, hence f.g.).
2. Generally: M is f.p. $\iff$ M is f.g. and $\ker(R^n \to M)$ is f.g.

3.3 Localization

Construction

Definition 3.3.1: Multiplicatively Closed Set

A subset $U \subseteq R$ is **multiplicatively closed** if:

1. $1 \in U$.
2. If $u, v \in U$, then $uv \in U$.

Example 3.3.1: Examples of U

1. If R is a domain, $U = R \setminus \{0\}$.
2. If $\mathfrak{p}$ is a prime ideal, $U = R \setminus \mathfrak{p}$.
3. If $a \in R$ is not nilpotent, $U = \{1, a, a^2, \dots\}$.

Definition 3.3.2: Localization $U^{-1}R$

Let $U \subseteq R$ be multiplicatively closed. The **localization** $U^{-1}R$ is the set of equivalence classes of pairs $(r, u) \in R \times U$, denoted $\frac{r}{u}$, under the relation:

$$(r, u) \sim (r', u') \iff \exists u'' \in U \text{ such that } u''(ru' - r'u) = 0.$$

This forms a ring with standard addition and multiplication of fractions.

Remark 3.3.1: Notation

- If $U = R \setminus \mathfrak{p}$, we write $R_{\mathfrak{p}}$ (Localization at a prime).
- If $U = \{1, a, a^2, \dots\}$, we write R_a or $R[1/a]$.

Properties of Localization

Proposition 3.3.1: Ideals in Localization

Let $\phi : R \to U^{-1}R$ be the canonical map $r \mapsto r/1$.

1. Every ideal $J \subseteq U^{-1}R$ is an **extended ideal**, meaning $J = U^{-1}I$ for some ideal $I \subseteq R$ (specifically $I = \phi^{-1}(J)$).

2. **Prime Correspondence:** There is a bijection between prime ideals of $U^{-1}R$ and prime ideals of R that do not intersect U:

$$\{\mathfrak{q} \in \operatorname{Spec}(U^{-1}R)\} \longleftrightarrow \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \cap U = \emptyset\}.$$

   Specifically, $\mathfrak{q} \mapsto \phi^{-1}(\mathfrak{q})$ and $\mathfrak{p} \mapsto U^{-1}\mathfrak{p}$.

Corollary 3.3.1: Noetherian Preservation If R is a Noetherian ring, then $U^{-1}R$ is a Noetherian ring.

Localization of Modules

Definition 3.3.3: Localized Module

For an R-module M, define $U^{-1}M$ similarly as pairs (m, u) modulo equivalence:

$$\frac{m}{u} = \frac{m'}{u'} \iff \exists s \in U, s(u'm - um') = 0.$$

$U^{-1}M$ is a $U^{-1}R$-module. Localization is an exact functor (it preserves exact sequences).

Local Rings

Definition 3.3.4: Local Ring

A ring R is a **local ring** if it has a unique maximal ideal $\mathfrak{m}$. We often denote this as $(R, \mathfrak{m})$.

Example 3.3.2: Examples

1. $R_{\mathfrak{p}}$ is a local ring with unique maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$.

2. The power series ring $k[[x]]$ is a local ring with maximal ideal (x). (Note: Elements $a_0 + a_1x + \dots$ are units iff $a_0 \neq 0$).

3. **Non-example:** The polynomial ring $k[x]$ is not local (has many maximal

ideals corresponding to irreducible polynomials).

3.4 Determinant Trick and Nakayama's Lemma

The Determinant Trick

Proposition 3.4.1: Cayley-Hamilton for Modules

Let M be a finitely generated R-module generated by n elements. Let I be an ideal of R and $\varphi : M \to M$ be an R-linear map such that $\varphi(M) \subseteq IM$. Then there exist $a_1, \dots, a_n$ with $a_j \in I^j$ such that:

$$\varphi^n + a_1\varphi^{n-1} + \cdots + a_{n-1}\varphi + a_n \cdot \mathrm{id}_M = 0$$

as an operator on M.

Proof. Let M be generated by $x_1, \dots, x_n$. Since $\varphi(x_i) \in IM$, we can write:

$$\varphi(x_i) = \sum_{j=1}^{n} a_{ij}x_j, \quad \text{with } a_{ij} \in I.$$

This can be rewritten as a system:

$$\sum_{j=1}^{n}(\delta_{ij}\varphi - a_{ij})x_j = 0$$

Let A be the matrix $(\delta_{ij}\varphi - a_{ij})$ with entries in the ring $R[\varphi]$. By multiplying by the adjugate matrix $\mathrm{adj}(A)$, we get:

$$\det(A) \cdot x_k = 0 \quad \text{for all } k.$$

Since the x_k generate M, $\det(A)$ is the zero operator on M. Expanding the determinant gives the characteristic polynomial of the form stated. □

Corollary 3.4.1: Annihilator Let M be a finitely generated R-module. If $IM = M$, then there exists $x \equiv 1 \pmod{I}$ such that $xM = 0$.

Proof. Apply the proposition with $\varphi = \mathrm{id}_M$. Since $\mathrm{id}_M(M) \subseteq IM$, we get an equation:

$$1 + a_1 + \cdots + a_n = 0 \text{ on } M, \quad a_i \in I.$$

Let $x = 1 + \sum a_i$. Then $x \in 1 + I$ and $xM = 0$. □

Nakayama's Lemma (NAK)

Lemma 3.4.1: Nakayama's Lemma

Let $(R, \mathfrak{m})$ be a local ring and M be a finitely generated R-module. If $M = \mathfrak{m}M$, then $M = 0$.

Proof. By the previous corollary, if $M = \mathfrak{m}M$, there exists $x \in 1 + \mathfrak{m}$ such that $xM = 0$. Since R is local, elements in $1 + \mathfrak{m}$ are units (invertible). Thus x is a unit, so $x^{-1}xM = 0 \implies M = 0$. □

Corollary 3.4.2: Lifting Generators Let $(R, \mathfrak{m})$ be a local ring and M a finitely generated R-module. Let $\bar{x}_1, \dots, \bar{x}_n$ be elements of $M/\mathfrak{m}M$ that generate it as an $R/\mathfrak{m}$-vector space. If $x_1, \dots, x_n$ are lifts of these elements to M, then $x_1, \dots, x_n$ generate M as an R-module.

Proof. Let N be the submodule generated by $x_1, \dots, x_n$. Then $M = N + \mathfrak{m}M$. Consider the quotient module M/N. We have:

$$\mathfrak{m}(M/N) = (\mathfrak{m}M + N)/N = M/N$$

Since M is f.g., M/N is f.g. By Nakayama's Lemma, $M/N = 0$, so $M = N$. □

3.5 Spectrum and Irreducible Components

The Spectrum of a Ring

Definition 3.5.1: Spec R

Let R be a ring. The **spectrum** of R, denoted $\mathrm{Spec}(R)$, is the set of all prime ideals of R.

$$\mathrm{Spec}(R) = \{\mathfrak{p} \subset R \mid \mathfrak{p} \text{ is a prime ideal}\}.$$

We also define the Maximal Spectrum $\mathrm{mSpec}(R)$ as the set of maximal ideals.

The Zariski Topology

Definition 3.5.2: Vanishing Set V(I)

For any ideal $I \subseteq R$, define the subset $V(I) \subseteq \mathrm{Spec}(R)$ as:

$$V(I) = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid I \subseteq \mathfrak{p}\}.$$

These sets satisfy the axioms of closed sets for a topology:

1. $V(R) = \emptyset$, $V(0) = \mathrm{Spec}(R)$.
2. $V(I) \cup V(J) = V(IJ) = V(I \cap J)$.
3. $\bigcap_\lambda V(I_\lambda) = V(\sum_\lambda I_\lambda)$.

The topology defined by these closed sets is called the **Zariski Topology**.

Remark 3.5.1: Closed Sets of Quotients There is a natural homeomorphism between $\mathrm{Spec}(R/I)$ and the closed set $V(I) \subseteq \mathrm{Spec}(R)$.

Irreducibility and Minimal Primes

Definition 3.5.3: Irreducible Space

A topological space X is **irreducible** if it cannot be written as the union of two proper closed subsets. i.e., if $X = F_1 \cup F_2$ with F_i closed, then $X = F_1$ or $X = F_2$.

Proposition 3.5.1: Irreducibility of Spec R

$\mathrm{Spec}(R)$ is irreducible if and only if the nilradical $\sqrt{0}$ is a prime ideal. (For domains, $\mathrm{Spec}(R)$ is always irreducible). Specifically, $V(\mathfrak{p})$ is an irreducible closed subset for any prime $\mathfrak{p}$.

Definition 3.5.4: Minimal Primes

A prime ideal $\mathfrak{p}$ is **minimal** if it does not contain any other prime ideal. By Zorn's Lemma, every ring has minimal prime ideals.

Theorem 3.5.1: Irreducible Decomposition

The space $\mathrm{Spec}(R)$ can be written as the union of irreducible closed sets corresponding to the minimal primes of R:

$$\mathrm{Spec}(R) = \bigcup_{\mathfrak{p} \in \min(R)} V(\mathfrak{p}).$$

These $V(\mathfrak{p})$ are called the **irreducible components** of $\mathrm{Spec}(R)$.

CHAPTER 4

IRREDUCIBLE DECOMPOSITIONS AND ASSOCIATED PRIMES

4.1 Irreducible Decompositions and Spectrum

The Spectrum of a Ring and Radical Ideals

Recall that for a commutative ring R, the spectrum $\mathrm{Spec}(R)$ is the set of all prime ideals of R. For any ideal $I \subseteq R$, we define the closed set $V(I)$ as:

$$V(I) = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \supseteq I\}.$$

Proposition 4.1.1: : Radical Ideals and $V(I)$

Let I be an ideal of R. Then:

$$\bigcap_{\mathfrak{p} \in V(I)} \mathfrak{p} = \sqrt{I},$$

where $\sqrt{I} = \{r \in R \mid r^n \in I \text{ for some } n \geq 1\}$ is the radical of I. Consequently, $V(I) = V(\sqrt{I})$.

Proof. If $\mathfrak{p} \supseteq I$, since $\mathfrak{p}$ is prime, it must contain $\sqrt{I}$. Thus $V(I) \subseteq V(\sqrt{I})$. Conversely, since $I \subseteq \sqrt{I}$, $V(\sqrt{I}) \subseteq V(I)$. The equality $\bigcap_{\mathfrak{p} \supseteq I} \mathfrak{p} = \sqrt{I}$ is a standard result: the intersection of all prime ideals containing I is exactly the radical of I. □

Remark 4.1.1: Applying this to the zero ideal $I = (0)$, the intersection of all prime ideals in R is the **nilradical** of R (the set of nilpotent elements).

Localization and Spectrum

Consider an element $a \in R$. We denote $R_a = S^{-1}R$ where $S = \{1, a, a^2, \dots\}$. The prime ideals of the localization R_a correspond to prime ideals of R that do not intersect S.

Definition 4.1.1:

$$\mathrm{Spec}(R_a) \cong \{\mathfrak{p} \in \mathrm{Spec}(R) \mid a \notin \mathfrak{p}\} = D(a).$$

This set $D(a)$ is an open set in the Zariski topology on $\mathrm{Spec}(R)$.

Note that in the ring R_a, $\frac{1}{1} = \frac{0}{1}$ if and only if $0 \in S$, which implies a is nilpotent.

Nullstellensatz and Correspondence

Let k be an algebraically closed field and let $R = k[x_1, \ldots, x_n]$. Let I be an ideal and $S = R/I$.

Definition 4.1.2: : Zero Sets

For an ideal $J \subseteq R$, we define the zero set in affine space:

$$Z(J) = \{\mathbf{a} \in k^n \mid f(\mathbf{a}) = 0 \quad \forall f \in J\}.$$

There is a correspondence between geometric objects and algebraic ones:

- $\mathrm{MaxSpec}(S) \subseteq \mathrm{Spec}(S)$ corresponds to points in the variety.
- $V(J)$ in $\mathrm{Spec}(S)$ corresponds to closed subvarieties.

Theorem 4.1.1: : Hilbert's Nullstellensatz (Geometric version)

If k is algebraically closed, then for any ideal $J \subseteq k[x_1, \ldots, x_n]$:

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

Furthermore, maximal ideals $\mathfrak{m} \subset k[x_1, \ldots, x_n]$ are of the form $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$ for some point $(a_1, \ldots, a_n) \in k^n$.

Topological Irreducibility

Definition 4.1.3: : Irreducible Space

A topological space X is **irreducible** if $X \neq \emptyset$ and X cannot be written as the union of two proper closed subsets. That is, if $X = Z_1 \cup Z_2$ with Z_i closed, then $X = Z_1$ or $X = Z_2$.

Proposition 4.1.2: : Irreducibility of Spectrum

Let S be a ring. The space $\mathrm{Spec}(S)$ is irreducible if and only if the nilradical of S is a prime ideal. If S is a domain, $\mathrm{Spec}(S)$ is irreducible.

In the geometric context ($R = k[x_1, \ldots, x_n]/I$), the variety $Z(I)$ is irreducible if and only if the ideal I is prime (or more generally, $\sqrt{I}$ is prime).

4.2 Irreducible Ideals

Irreducible Ideals

Definition 4.2.1: : Irreducible Ideal

An ideal I in a ring R is called **irreducible** if I cannot be written as an intersection of two strictly larger ideals.

$$I = I_1 \cap I_2 \implies I = I_1 \text{ or } I = I_2.$$

Proposition 4.2.1: : Decomposition in Noetherian Rings

Let R be a Noetherian ring. Then every ideal $I \subseteq R$ can be written as a finite intersection of irreducible ideals:

$$I = \bigcap_{i=1}^{m} J_i,$$

where each J_i is irreducible.

Proof. Suppose the set of ideals that cannot be written as a finite intersection of irreducible ideals is non-empty. Since R is Noetherian, this set has a maximal element, say I. I itself cannot be irreducible (otherwise it is an intersection of length 1). Thus, $I = I_1 \cap I_2$ with $I \subsetneq I_1$ and $I \subsetneq I_2$. By the maximality of I, both I_1 and I_2 must have irreducible decompositions. Substituting these back gives a decomposition for I, a contradiction. □

Example 4.2.1: : Decomposition in $\mathbb{Z}$Let $R = \mathbb{Z}$ and $n = p_1^{e_1} \dots p_r^{e_r}$ be a prime factorization. The ideal (n) has the irreducible decomposition:

$$(n) = (p_1^{e_1}) \cap (p_2^{e_2}) \cap \dots \cap (p_r^{e_r}).$$

In a PID like $\mathbb{Z}$, irreducible ideals are powers of prime ideals.

Introduction to Associated Primes

Let M be an R-module.

Definition 4.2.2: : Colon Ideals

For submodules $N \subseteq M$ and an element $x \in M$, define:

$$(N :_R x) = \{r \in R \mid rx \in N\}.$$

This is an ideal of R. The **annihilator** of x is $\operatorname{Ann}_R(x) = (0 :_R x) = \{r \in R \mid rx = 0\}$.

Definition 4.2.3: : Associated Prime

A prime ideal $\mathfrak{p} \in \operatorname{Spec}(R)$ is **associated** to M if $\mathfrak{p} = \operatorname{Ann}_R(x)$ for some non-zero element $x \in M$. The set of associated primes is denoted $\operatorname{Ass}_R(M)$.

Remark 4.2.1: $\mathfrak{p} \in \operatorname{Ass}_R(M) \iff$ there exists an injective R-linear map $R/\mathfrak{p} \hookrightarrow M$.

4.3 Associated Primes and Primary Decomposition

Existence of Associated Primes

Proposition 4.3.1:

Let R be a Noetherian ring and M a non-zero finitely generated R-module. Let $\mathcal{F}$ be the family of ideals:

$$\mathcal{F} = \{\operatorname{Ann}_R(x) \mid x \in M, x \neq 0\}.$$

Then any maximal element of $\mathcal{F}$ is a prime ideal. Consequently, $\operatorname{Ass}_R(M) \neq \emptyset$.

Proof. Let $I = \operatorname{Ann}(x)$ be maximal in $\mathcal{F}$. Let $a, b \in R$ such that $ab \in I$ but $b \notin I$. Then $abx = 0$ but $bx \neq 0$. Consider the element bx. We have $\operatorname{Ann}(bx) \supseteq \operatorname{Ann}(x) = I$. Also, $a \in \operatorname{Ann}(bx)$ implies $\operatorname{Ann}(bx) \supseteq (I, a)$. Since I is maximal in $\mathcal{F}$, we must have $\operatorname{Ann}(bx) = I$ is impossible if we assume strict inclusion. Actually, to show I is prime: Since $b \notin I$, $bx \neq 0$. The ideal $\operatorname{Ann}(bx)$ is in $\mathcal{F}$ (or contained in one). Since $I = \operatorname{Ann}(x) \subseteq \operatorname{Ann}(bx)$ and I is maximal, we must have $I = \operatorname{Ann}(bx)$. Since $abx = 0$, $a \in \operatorname{Ann}(bx) = I$. Thus I is prime. □

Behavior under Exact Sequences

Proposition 4.3.2:

Let $0 \to M_1 \xrightarrow{\phi} M_2 \xrightarrow{\psi} M_3 \to 0$ be a short exact sequence of R-modules. Then:

$$\operatorname{Ass}(M_1) \subseteq \operatorname{Ass}(M_2) \subseteq \operatorname{Ass}(M_1) \cup \operatorname{Ass}(M_3).$$

Proof. **1.** $\operatorname{Ass}(M_1) \subseteq \operatorname{Ass}(M_2)$**:** Let $\mathfrak{p} \in \operatorname{Ass}(M_1)$. Then $R/\mathfrak{p} \hookrightarrow M_1$. Composing with ϕ gives $R/\mathfrak{p} \hookrightarrow M_2$, so $\mathfrak{p} \in \operatorname{Ass}(M_2)$.

2. $\operatorname{Ass}(M_2) \subseteq \operatorname{Ass}(M_1) \cup \operatorname{Ass}(M_3)$**:** Let $\mathfrak{p} \in \operatorname{Ass}(M_2)$, so $\mathfrak{p} = \operatorname{Ann}(x)$ for some $x \in M_2$. Case 1: $Rx \cap M_1 \neq 0$. Let $y \in Rx \cap M_1, y \neq 0$. Since $y = rx$ for some r, $\operatorname{Ann}(y) \supseteq \operatorname{Ann}(x) = \mathfrak{p}$. In fact, over a Noetherian ring, or by localized argument, one can show $\mathfrak{p} \in \operatorname{Ass}(M_1)$. (Specifically, $r \notin \mathfrak{p} \implies \operatorname{Ann}(rx) = \mathfrak{p}$). Case 2: $Rx \cap M_1 = 0$. Then ψ maps Rx isomorphically into M_3. Thus $R/\mathfrak{p} \cong Rx \hookrightarrow M_3$, so $\mathfrak{p} \in \operatorname{Ass}(M_3)$. □

Primary Submodules

Definition 4.3.1: : Primary Submodule

A submodule $N \subseteq M$ is **primary** if $\mathrm{Ass}_R(M/N)$ consists of exactly one prime ideal, say $\mathfrak{p}$. We say N is $\mathfrak{p}$-primary.

Proposition 4.3.3: : Irreducible Implies Primary

Let R be Noetherian and $N \subseteq M$ an irreducible submodule. Then N is primary.

Proof. Consider $M' = M/N$. Since N is irreducible in M, the zero submodule 0 is irreducible in M'. We must show $\mathrm{Ass}(M')$ is a singleton. Let $\mathfrak{p}_1, \mathfrak{p}_2 \in \mathrm{Ass}(M')$. Then there exist submodules $R\bar{x} \cong R/\mathfrak{p}_1$ and $R\bar{y} \cong R/\mathfrak{p}_2$ in M'. If $\mathfrak{p}_1 \neq \mathfrak{p}_2$, these submodules intersect at 0 (non-trivial intersection would require common annihilator properties impossible for distinct primes). But if intersection is 0, this contradicts the irreducibility of 0 in M' (unless one is zero, which is not allowed for Assoc primes). Therefore $\mathfrak{p}_1 = \mathfrak{p}_2$. □

Primary Decomposition Theorem

Theorem 4.3.1: : Primary Decomposition

Let R be Noetherian and M finitely generated. Any submodule $N \subseteq M$ has a **primary decomposition**:

$$N = Q_1 \cap Q_2 \cap \cdots \cap Q_n,$$

where each Q_i is a primary submodule.

Proof. Since M is Noetherian (as R is Noetherian and M is f.g.), N admits a decomposition into irreducible submodules: $N = \bigcap M_i$. By the previous proposition, each irreducible submodule M_i is primary. □

Proposition 4.3.4: Intersection of Primary Submodules

If Q_1 and Q_2 are both $\mathfrak{p}$-primary, then $Q_1 \cap Q_2$ is $\mathfrak{p}$-primary.

Proof sketch: $\mathrm{Ass}(M/(Q_1 \cap Q_2)) \subseteq \mathrm{Ass}(M/Q_1 \oplus M/Q_2) \subseteq \{\mathfrak{p}\}$.

This allows us to form a **minimal** primary decomposition where distinct Q_i have distinct associated primes.

4.4 Support and Minimal Primes

Relation between Associated Primes and Zero Divisors

Proposition 4.4.1: Relation between Associated Primes and Zero Divisors

Let R be Noetherian and M finitely generated. Let $\mathcal{Z}(M)$ be the set of zero-divisors on M (elements $r \in R$ such that $rm = 0$ for some $m \neq 0$). Then:

$$\mathcal{Z}(M) = \bigcup_{\mathfrak{p} \in \operatorname{Ass}(M)} \mathfrak{p}.$$

Support of a Module

Definition 4.4.1: Support

The **support** of a module M is defined as:

$$\operatorname{Supp}(M) = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid M_{\mathfrak{p}} \neq 0\}.$$

Definition 4.4.2: Minimal Primes

Let $I = \operatorname{Ann}_R(M)$. The minimal primes of M, denoted $\operatorname{Min}(M)$, are the minimal primes over the ideal $\operatorname{Ann}_R(M)$. Alternatively, $\operatorname{Min}(M)$ are the minimal elements of the set $\operatorname{Supp}(M)$.

Proposition 4.4.2: Relations between Ass, Supp, Min

Let R be Noetherian and M finitely generated.

1. $\operatorname{Supp}(M) = V(\operatorname{Ann}_R(M))$.
2. $\operatorname{Ass}(M) \subseteq \operatorname{Supp}(M)$.
3. $\operatorname{Min}(M) \subseteq \operatorname{Ass}(M)$.
4. $\operatorname{rad}(\operatorname{Ann}_R(M)) = \bigcap_{\mathfrak{p} \in \operatorname{Ass}(M)} \mathfrak{p} = \bigcap_{\mathfrak{p} \in \operatorname{Min}(M)} \mathfrak{p}$.

Localization of Associated Primes

Proposition 4.4.3: Ass and Localization

Let S be a multiplicatively closed subset of R.

1. If $\mathfrak{p} \in \operatorname{Ass}_R(M)$ and $\mathfrak{p} \cap S = \emptyset$, then $S^{-1}\mathfrak{p} \in \operatorname{Ass}_{S^{-1}R}(S^{-1}M)$.
2. The map $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$ induces a bijection:

$$\operatorname{Ass}_R(M) \cap \{\mathfrak{p} \mid \mathfrak{p} \cap S = \emptyset\} \longleftrightarrow \operatorname{Ass}_{S^{-1}R}(S^{-1}M).$$

Proof. If $\mathfrak{p} = \operatorname{Ann}(x)$, and $S \cap \mathfrak{p} = \emptyset$, then in $S^{-1}M$, the annihilator of $x/1$ is $S^{-1}\mathfrak{p}$.

Conversely, if $\mathcal{Q} \in \mathrm{Ass}(S^{-1}M)$, then $\mathcal{Q} = \mathrm{Ann}(x/s)$. We can clear denominators to find an element in M whose annihilator in R contracts to a prime that corresponds to $\mathcal{Q}$. □

Minimal Primes are Associated

> **Corollary 4.4.1: Minimal Primes are Associated**If R is Noetherian, then $\mathrm{Min}(M) \subseteq \mathrm{Ass}(M)$.

Proof. Let $\mathfrak{p} \in \mathrm{Min}(M)$. Since $\mathfrak{p}$ is a minimal element of $\mathrm{Supp}(M)$, upon localizing at $\mathfrak{p}$, the support of $M_{\mathfrak{p}}$ over $R_{\mathfrak{p}}$ contains only the maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$ (nilradical behavior). Since $M_{\mathfrak{p}} \neq 0$ and R is Noetherian, $\mathrm{Ass}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}})$ is non-empty. The only possible prime is $\mathfrak{p}R_{\mathfrak{p}}$. By the correspondence of associated primes under localization, $\mathfrak{p} \in \mathrm{Ass}_R(M)$. □

CHAPTER 5

PRIMARY DECOMPOSITION

5.1 Primary Ideals and Their Properties

We begin by recalling the definition and basic properties of primary ideals in a Noetherian ring R.

Definition 5.1.1: Primary Ideal

An ideal Q in a ring R is called **primary** if $Q \neq R$ and for every zero divisor in R/Q is nilpotent.
Equivalently, if $xy \in Q$ and $x \notin Q$, then $y^n \in Q$ for some $n > 0$ (i.e., $y \in \sqrt{Q}$).

If Q is a primary ideal, then its radical $\sqrt{Q} = p$ is a prime ideal. In this case, we say that Q is p-**primary**.

Proposition 5.1.1: Radical of Primary Ideals

Let R be a Noetherian ring. If Q is a p-primary ideal, then:

$$\mathrm{Ass}(R/Q) = \{p\}.$$

Moreover, $\sqrt{\mathrm{Ann}(R/Q)} = p$.

Warning 5.1.1: Converse Falsehood If $\sqrt{I} = p$ is a prime ideal, it does **not** necessarily imply that I is a p-primary ideal.

Example 5.1.1: Non-primary ideal with prime radical Consider the ring $R = k[X, Y]$. Let $I = (X^2, XY)$.
1. **Calculate Radical:** Note that $X^2 \in I \implies X \in \sqrt{I}$. Also, $XY \in I$. The radical is $\sqrt{I} = (X)$, which is a prime ideal.
2. **Check Primality:** In the quotient ring R/I, we have $\bar{X} \neq 0$ and $\bar{Y} \neq 0$. However, their product $\bar{X}\bar{Y} = 0$. For I to be primary, one of these must be nilpotent. $\bar{X}^2 = 0$, so $\bar{X}$ is nilpotent. However, considering the definition via elements: $XY \in I$, $X \notin I$, but is $Y^n \in I$ for any n? No. Y is not in the radical (X).

3. **Associated Primes:** Let's calculate $\text{Ass}(R/I)$. We look for prime ideals that are annihilators of elements.

- $\text{Ann}_R(\bar{X}) = \{f \in R \mid fX \in (X^2, XY)\}$. Write $fX = AX^2 + BXY \implies f = AX + BY$. Thus, $\text{Ann}_R(\bar{X}) = (X, Y)$, which is a maximal ideal. Let $m = (X, Y)$. Since m is prime, $m \in \text{Ass}(R/I)$.
- $\text{Ann}_R(\bar{Y}) = (X)$ (since $XY \in I$ and $X^2 \nmid Y$). (X) is prime, so $(X) \in \text{Ass}(R/I)$.

Therefore, $\text{Ass}(R/I) = \{(X), (X, Y)\}$. Since there are two associated primes, I is not primary (a primary ideal has exactly one associated prime).
Conclusion: $I = (X) \cap (X^2, Y)$ is a primary decomposition, but I itself is not primary.

Proposition 5.1.2: Maximal Radical implies Primary

Let R be a Noetherian ring and m be a maximal ideal. Let I be an ideal such that $\sqrt{I} = m$. Then I is m-primary.

Proof. We know that $\text{Ass}(R/I) \subseteq \text{Supp}(R/I) = V(\text{Ann}(R/I)) = V(\sqrt{I}) = V(m) = \{m\}$. Since R is Noetherian, $\text{Ass}(R/I)$ is non-empty. Thus, $\text{Ass}(R/I) = \{m\}$. This implies I is m-primary. □

5.2 Primary Decomposition of Modules

We extend the concept of primary decomposition to modules over a Noetherian ring R.

Definition 5.2.1: Primary Submodule

Let M be an R-module and $N \subseteq M$ a submodule. N is called **p-primary** if $\text{Ass}(M/N) = \{p\}$.

Theorem 5.2.1: Lasker-Noether Decomposition

Let R be a Noetherian ring and M a finitely generated R-module. Any proper submodule $N \subsetneq M$ has a primary decomposition:

$$N = \bigcap_{i=1}^{m} Q_i,$$

where Q_i is a p_i-primary submodule.

A decomposition is called **irredundant** (or minimal) if: 1. No Q_i contains the intersection of the others. 2. The associated primes $p_i = \sqrt{\text{Ann}(M/Q_i)}$ are all distinct.

Proposition 5.2.1: Structure of Associated Primes

If $N = \bigcap_{i=1}^m Q_i$ is an irredundant primary decomposition with Q_i being p_i-primary, then:

$$\text{Ass}(M/N) = \{p_1, p_2, \ldots, p_m\}.$$

Proof. We have an embedding $M/N \hookrightarrow \bigoplus_{i=1}^m M/Q_i$. Since $\text{Ass}(\bigoplus M/Q_i) = \bigcup \text{Ass}(M/Q_i) = \{p_1, \ldots, p_m\}$, we have $\text{Ass}(M/N) \subseteq \{p_1, \ldots, p_m\}$.

For the reverse inclusion, since the decomposition is irredundant, we can find elements in the intersection of all but one Q_i that map to non-zero elements annihilated by p_i, showing $p_i \in \text{Ass}(M/N)$. □

Minimal and Embedded Primes

Let $\text{Ass}(M/N) = \{p_1, \ldots, p_m\}$. The elements that are minimal with respect to inclusion are called **minimal primes** (or isolated primes). The others are called **embedded primes**.

Example 5.2.1: Revisiting $I = (X^2, XY)$In $R = k[X, Y]$, we found $\text{Ass}(R/I) = \{(X), (X, Y)\}$.

- (X) is a **minimal prime**. It corresponds to the geometric component (the line $x = 0$).
- (X, Y) is an **embedded prime**. It corresponds to the "embedded point" at the origin.

The primary decomposition is $I = (X) \cap (X^2, Y)$. Note that (X) is (X)-primary and (X^2, Y) is (X, Y)-primary.

Zero Divisors and Prime Avoidance

Proposition 5.2.2: Zero Divisors

Let R be Noetherian and M finitely generated. The set of zero divisors on M, denoted $Z(M)$, is the union of the associated primes:

$$Z(M) = \bigcup_{p \in \text{Ass}(M)} p.$$

Lemma 5.2.1: Prime Avoidance

Let $p_1, \ldots, p_n$ be prime ideals and I be an ideal. If $I \subseteq \bigcup_{i=1}^n p_i$, then $I \subseteq p_i$ for some i.

Proof. (Sketch) By induction on n. For $n = 2$, if $I \not\subseteq p_1$ and $I \not\subseteq p_2$, pick $x_1 \in I \setminus p_2$ and $x_2 \in I \setminus p_1$. Then $x_1 + x_2 \in I$ but is in neither p_1 nor p_2 (standard check), contradiction. The general case follows similar logic; if I is not contained in the union of any $n - 1$, we can construct an element in I avoiding all p_i. □

Example: Computing Primary Decomposition

Example 5.2.2: Ideal in 4 variables Let $R = k[u, v, x, y]$ and $I = (ux, vy, uy + vx)$.
1. **Find Minimal Primes:** Since $ux \in I \subseteq p$, either $u \in p$ or $x \in p$. Similarly, $v \in p$ or $y \in p$. From $uy + vx \in p$:

- Case 1: $u \in p, v \in p \implies 0 \in p$. This gives minimal prime $p_1 = (u, v)$.
- Case 2: $x \in p, y \in p \implies 0 \in p$. This gives minimal prime $p_2 = (x, y)$.
- Mixed cases (e.g., $u, y \in p$) force the other variables or lead to non-minimal primes.

Thus $\text{Min}(R/I) = \{(u, v), (x, y)\}$.
2. **Embedded Primes?** Consider the element uy. $uy \notin I$ (check degrees/terms). $(I : uy) = (x, v, uy + vx : uy) = (x, v, u, y) = m$. The maximal ideal $m = (u, v, x, y)$ is an associated prime because it annihilates the class of uy mod I (modulo simplification). Specifically, we look at the decomposition. $I = (u, v) \cap (x, y) \cap Q_{emb}$. Actually, $I = (u, v) \cap (x, y) \cap (ux, vy, uy + vx, \text{something else})$.
Let's check intersections: $(u, v) \cap (x, y) = (ux, uy, vx, vy)$. Our ideal I contains ux, vy and $uy + vx$. Notice $uy \notin I$ and $vx \notin I$, but their sum is. In $(u, v) \cap (x, y)$, both uy and vx are present. So $I \subsetneq (u, v) \cap (x, y)$. The quotient $((u, v) \cap (x, y))/I$ is annihilated by (u, v, x, y). Thus $m = (u, v, x, y)$ is an embedded prime.
Decomposition: $I = (u, v) \cap (x, y) \cap (u, v, x, y)^2 + I$ (conceptually). A valid decomposition is $I = (u, v) \cap (x, y) \cap (ux, vy, uy + vx, x^2, y^2, u^2, v^2 \dots)$.

5.3 Radical Ideals and Irreducibility

Proposition 5.3.1: Radical Ideals have no Embedded Primes

Let R be Noetherian and I be a radical ideal (i.e., $I = \sqrt{I}$). Then I has no embedded primes.

$$I = \bigcap_{p \in \text{Min}(R/I)} p.$$

Proof. Since I is radical, $I = \bigcap_{p \in V(I)} p$. In a Noetherian ring, this intersection is finite and reduces to the intersection of the minimal primes over I. If there were an embedded prime P, the primary component Q corresponding to P would not be needed to describe the radical intersection. □

Geometric Interpretation

Let k be an algebraically closed field.

1. There is a bijection between algebraic sets $Z(I)$ and radical ideals $\sqrt{I}$.
2. $Z(I)$ is irreducible if and only if $\sqrt{I}$ is prime.
3. The primary decomposition of a radical ideal $I = p_1 \cap \cdots \cap p_n$ corresponds to the decomposition of the algebraic set into irreducible components:

$$Z(I) = Z(p_1) \cup Z(p_2) \cup \cdots \cup Z(p_n).$$

5.4 Saturation and Localization

Often we want to remove certain components from an algebraic set (e.g., removing the "embedded points" or components contained in a specific subvariety). This is achieved algebraically via saturation.

Definition 5.4.1: Saturation

Let I, J be ideals in a Noetherian ring R. The **saturation** of I with respect to J is:

$$I : J^\infty = \bigcup_{n=1}^{\infty} (I : J^n) = \{r \in R \mid \exists n, rJ^n \subseteq I\}.$$

Since R is Noetherian, the chain $I : J \subseteq I : J^2 \subseteq \dots$ stabilizes. Thus $I : J^\infty = I : J^N$ for sufficiently large N.

Theorem 5.4.1: Saturation and Associated Primes

Let I, J be ideals. Then:

$$\mathrm{Ass}(R/(I : J^\infty)) = \{p \in \mathrm{Ass}(R/I) \mid J \not\subseteq p\}.$$

Proof. Let $I = \bigcap_{i=1}^m Q_i$ be a primary decomposition of I, where Q_i is p_i-primary. We recall that $(Q_i : J^\infty) = R$ if $J \subseteq p_i$ (or rather, if elements of J are nilpotent modulo Q_i? No, if $J \cap (R \setminus p_i) \neq \emptyset$, then we invert elements). Actually, let's look at the property:

- If $J \subseteq p_i$, then elements of J are topologically "close" to zero divisors. But saturation removes components where J is **not** a zero divisor.
- Correct Logic: If $J \not\subseteq p_i$, then J contains an element $s \notin p_i$. s is not a zero divisor on R/Q_i. Thus $Q_i : s^\infty = Q_i$. So $Q_i : J^\infty = Q_i$.

- If $J \subseteq p_i$, does it imply $Q_i : J^\infty = R$? Not necessarily immediately, but if p_i is minimal, yes, locally. For primary ideals, if $J \subseteq \sqrt{Q_i}$, then $J^n \subseteq Q_i$ for large n, so $Q_i : J^\infty = R$.

Thus, $I : J^\infty = \bigcap(Q_i : J^\infty)$. The terms where $J \subseteq p_i$ become R and disappear from the intersection. The terms where $J \not\subseteq p_i$ remain as Q_i. So the associated primes of the saturation are exactly those original associated primes that do **not** contain J. □

Corollary 5.4.1: Geometric Meaning$V(I : J^\infty)$ is the closure of $V(I) \setminus V(J)$ in the Zariski topology. Saturation removes the components of $V(I)$ that are contained in $V(J)$.

5.5 Computing Saturation and Intersection

How do we compute $I : J^\infty$ or $I \cap J$ computationally? We use Gröbner bases (referencing Cox, Little, O'Shea).

Intersection via Elimination Theory

Proposition 5.5.1: Intersection Trick

Let $I, J \subseteq k[x_1, \dots, x_n]$. Let t be a new variable. Consider the ideal K in $k[t, x_1, \dots, x_n]$ generated by:

$$K = tI + (1-t)J = \{tf + (1-t)g \mid f \in I, g \in J\}.$$

Then:

$$I \cap J = K \cap k[x_1, \dots, x_n].$$

Proof. ($\subseteq$) Let $h \in I \cap J$. Then $h = th + (1-t)h \in tI + (1-t)J = K$. Since h has no t, $h \in K \cap k[x]$.

($\supseteq$) Let $h(x) \in K$. Then $h(x) = \sum a_i(t,x)tf_i(x) + \sum b_j(t,x)(1-t)g_j(x)$. Set $t = 0$: $h(x) = \sum b_j(0,x)g_j(x) \in J$. Set $t = 1$: $h(x) = \sum a_i(1,x)f_i(x) \in I$. Thus $h \in I \cap J$. □

Algorithm: Compute a Gröbner basis for $\langle tf_1, \dots, (1-t)g_m \rangle$ with respect to an elimination order eliminating t. The elements not involving t generate $I \cap J$.

Computing Saturation

To compute $I : g^\infty$, we can use the "Rabinowitsch Trick" variable.

$$I : g^\infty = (I, 1 - yg) \cap R \quad \text{(where } y \text{ is a new variable).}$$

Or, if $J = (g_1, \dots, g_k)$, then $I : J^\infty = \bigcap (I : g_i^\infty)$.

In the notes, a method for $I : (g)$ in a domain is mentioned: Write $I \cap (g) = (h_1 g, \dots, h_m g)$. Then $I : (g) = (h_1, \dots, h_m)$.

5.6 Morphisms

We briefly touch upon morphisms between affine varieties.

Let $\phi : R \to S$ be a ring homomorphism. This induces a map on spectra:

$$\phi^* : \mathrm{Spec}(S) \to \mathrm{Spec}(R), \quad Q \mapsto \phi^{-1}(Q).$$

Proposition 5.6.1: Contraction of Primes

If Q is a prime ideal in S, its contraction $P = \phi^{-1}(Q)$ is a prime ideal in R.

This corresponds geometrically to the fact that polynomial maps send algebraic sets to algebraic sets (under certain conditions, e.g., Chevalley's Theorem on constructible sets, though the preimage is always defined).

CHAPTER 6

INTEGRAL ELEMENTS AND EXTENSIONS

6.1 Integral Elements and Extensions

We begin by examining the relationship between rings and geometry, specifically focusing on the concept of integral extensions.

Geometric Motivation

Consider the polynomial ring $k[X, Y]$. Let us analyze the quotient ring $S = k[X, Y]/(XY)$. Geometrically, the ideal (XY) corresponds to the union of the X-axis and the Y-axis in the affine plane $\mathbb{A}^2_k$.

Consider the inclusion map from the subring $k[X]$ to S:

$$\varphi : k[X] \hookrightarrow \frac{k[X, Y]}{(XY)}$$

This ring homomorphism corresponds to a map of spectra in the opposite direction:

$$f : \operatorname{Spec}\left(\frac{k[X, Y]}{(XY)}\right) \to \operatorname{Spec}(k[X]) \cong \mathbb{A}^1_k$$

Geometrically, this is the projection of the union of the axes onto the X-axis.

- For a point $\alpha \neq 0$ on the X-axis, the fiber over α is the point $(\alpha, 0)$.
- For the origin $\alpha = 0$, the fiber is the entire Y-axis (since if $x = 0$, y can be anything).

This disparity in fibers (finite vs. infinite) motivates the study of **integral extensions**, which generalize the notion of "finite" covers in geometry.

Example 6.1.1: Contrasting Examples

1. **Infinite Fiber:** In the map $k[X] \to k[X, Y]/(XY)$, the element Y represents a "direction" that is not constrained by a monic polynomial over $k[X]$.
2. **Finite Fiber:** Consider the ring $k[X, Y]/(X^2 - Y^3)$ or a map where variables satisfy monic equations. If S is a finite R-module, the geometric fibers are

finite sets.

Definition of Integral Elements

Let $R \to S$ be a ring map (making S an R-algebra). We identify R with its image in S.

Definition 6.1.1: Integral Element

Let $R \subseteq S$. An element $s \in S$ is said to be **integral** over R if s is the root of a **monic** polynomial with coefficients in R. That is, there exist $r_1, \dots, r_n \in R$ such that:

$$s^n + r_1 s^{n-1} + \cdots + r_n = 0$$

Example 6.1.2: Examples of Integrality

1. Let k be a field and F a field extension. Then $\alpha \in F$ is integral over k if and only if α is **algebraic** over k.
2. Let $R = \mathbb{Z}$ and $S = \mathbb{Q}$. The element $1/2 \in \mathbb{Q}$ is **not** integral over $\mathbb{Z}$. (Rational numbers integral over $\mathbb{Z}$ are exactly the integers).
3. Consider $R = k[t^2]$ and $S = k[t^2, t^3] \subseteq k[t]$. The element t^3 satisfies $X^2 - (t^2)^3 = 0$, so it is integral over R. Actually, t is integral over $k[t^2]$ because it satisfies $X^2 - t^2 = 0$.

6.2 Properties of Integral Extensions

We now establish the relationship between integral elements and finite modules.

Proposition 6.2.1: Characterization of Integral Elements

Let $R \subseteq S$ be rings and $s \in S$. The following are equivalent:

1. s is integral over R.
2. The subalgebra $R[s]$ is a finitely generated R-module.
3. There exists a faithful $R[s]$-module M which is finitely generated as an R-module. (Faithful means $\mathrm{Ann}(M) = 0$).

Proof. **(1) ⇒ (2):** Since s is integral, $s^n = -\sum_{i=1}^n r_i s^{n-i}$. Thus, any power s^k for $k \geq n$ can be reduced to a linear combination of $1, s, \dots, s^{n-1}$. Hence, $R[s]$ is generated as an R-module by $\{1, s, \dots, s^{n-1}\}$.

(2) ⇒ (3): Take $M = R[s]$. Since $1 \in M$, it is faithful.

(3) ⇒ (1): (The Determinant Trick). Let M be generated by $m_1, \dots, m_k$ as an R-module. Multiplication by s is an R-linear map $\varphi : M \to M$. We can write:

$$s \cdot m_i = \sum_{j=1}^{k} a_{ij} m_j$$

where $a_{ij} \in R$. This gives a system of equations $\sum_j (s\delta_{ij} - a_{ij})m_j = 0$. Let A be the matrix $(s\delta_{ij} - a_{ij})$. By Cramer's rule/determinant properties, $\det(A) \cdot M = 0$. Since M is faithful, $\det(A) = 0$. Expanding the determinant gives a monic polynomial in s with coefficients in R. □

Corollary 6.2.1: Finite Algebras If S is a finite R-algebra (i.e., finitely generated as an R-module), then S is integral over R.

Proposition 6.2.2: Transitivity of Integrality

1. If $s_1, \dots, s_n \in S$ are integral over R, then $R[s_1, \dots, s_n]$ is a finite R-module.
2. **Transitivity:** Let $R \subseteq S \subseteq T$. If S is integral over R and T is integral over S, then T is integral over R.
3. The set $\bar{R} = \{s \in S \mid s \text{ is integral over } R\}$ is a subring of S containing R. This is called the **integral closure** of R in S.

Proof. (1) follows by induction on n, using the tower law for finite modules. (2) Let $t \in T$. It satisfies $t^n + s_1 t^{n-1} + \cdots + s_n = 0$ with $s_i \in S$. Let $S' = R[s_1, \dots, s_n]$. S' is finite over R. Since t is integral over S', $S'[t]$ is finite over S'. Thus $S'[t]$ is finite over R, implying t is integral over R. (3) follows from (1): if $x, y \in \bar{R}$, then $R[x, y]$ is a finite module, so $x \pm y$ and xy are integral. □

6.3 Integral Closure and Normalization

Definition 6.3.1: Integrally Closed Domain

Let R be a domain with field of fractions K.

- The **integral closure** of R is the integral closure of R in K, denoted $\bar{R}$.
- R is said to be **integrally closed** (or **normal**) if $\bar{R} = R$.

Example 6.3.1: Examples

1. $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$.
2. **Geometric Counter-example (Cusp):** Let $R = k[X, Y]/(Y^2 - X^3)$. This

ring is isomorphic to $k[t^2, t^3] \subset k[t]$. The fraction field is $k(t)$. The element $t = Y/X$ is in the fraction field. Note that $t^2 - (t^2) = 0$ is trivial, but t satisfies the monic equation $Z^2 - t^2 = 0$ (where coefficients must be in R). More simply, $t = Y/X$ satisfies $z^2 - X = 0$? No, $t^2 = X \in R$. Wait, t is a root of $Z^2 - t^2 = 0$ is not a valid polynomial over R unless $t^2 \in R$. Yes, $t^2 = X$. So t satisfies $Z^2 - X = 0$. Thus t is integral over R, but $t \notin k[t^2, t^3]$. Hence, $k[t^2, t^3]$ is **not** integrally closed. Its normalization is $k[t]$.

6.4 Noether Normalization Lemma

The Noether Normalization Lemma (NNL) is a fundamental result connecting dimension theory and geometry.

Definition 6.4.1: Algebraic Independence

Elements $z_1, \dots, z_d$ in a k-algebra R are **algebraically independent** over k if the map $k[T_1, \dots, T_d] \to R$ sending $T_i \mapsto z_i$ is injective. In this case, $k[z_1, \dots, z_d]$ is isomorphic to a polynomial ring.

Theorem 6.4.1: Noether Normalization Lemma

Let k be a field and R be a finitely generated k-algebra. Then there exist elements $z_1, \dots, z_d \in R$ such that:

1. $z_1, \dots, z_d$ are algebraically independent over k.

2. R is integral (and thus finite) over the polynomial subring $A = k[z_1, \dots, z_d]$.

The integer d is the Krull dimension of R.

Proof of Noether Normalization

We assume k is infinite (the finite field case requires a slightly different change of variables).

Proof. Let $R = k[y_1, \dots, y_n]$. We proceed by induction on n. If $y_1, \dots, y_n$ are algebraically independent, we are done ($d = n, R = A$). If not, there exists a non-zero polynomial $f \in k[T_1, \dots, T_n]$ such that $f(y_1, \dots, y_n) = 0$.

We aim to perform a change of variables so that f becomes **monic** in one variable (up to a scalar). Let us shift the variables:

$$y_i' = y_i - y_n^{r_i} \quad \text{for } 1 \leq i \leq n-1$$

and set $y'_n = y_n$. Substituting these into f, a term $cy_1^{e_1} \dots y_n^{e_n}$ becomes:

$$c(y'_1 + (y'_n)^{r_1})^{e_1} \dots (y'_n)^{e_n}$$

The highest degree term in y'_n from this expansion will have exponent $e_n + e_1 r_1 + \cdots + e_{n-1} r_{n-1}$. To ensure a unique highest degree term (so no cancellation occurs), we choose integers r_i such that the sums $\sum e_i r_i$ are distinct for all multi-indices occurring in f. We can choose $r_i = s^i$ for a sufficiently large integer s (larger than any exponent appearing in f).

With this choice, f rewritten in terms of $y'_1, \dots, y'_n$ looks like:

$$a(y'_n)^N + \text{lower degree terms in } y'_n \text{ with coeffs in } k[y'_1, \dots, y'_{n-1}] = 0$$

where $a \in k^\times$. Dividing by a, we see that y'_n is integral over $k[y'_1, \dots, y'_{n-1}]$.

By the induction hypothesis, the subalgebra $k[y'_1, \dots, y'_{n-1}]$ (generated by $n-1$ elements) contains algebraically independent elements $z_1, \dots, z_d$ such that $k[y'_1, \dots, y'_{n-1}]$ is finite over $k[z_1, \dots, z_d]$. By transitivity of integral extensions (Proposition **??**), R is finite over $k[z_1, \dots, z_d]$. □

Application: Nullstellensatz

Theorem 6.4.2: Hilbert's Nullstellensatz (Weak Version)

Let K be a field and F be a finitely generated K-algebra. If F is a field, then $[F : K] < \infty$. If K is algebraically closed, then $F \cong K$.

Proof. Apply Noether Normalization to F. There exists a polynomial subring $A = K[z_1, \dots, z_d] \subseteq F$ such that F is integral over A. Since F is a field, A must be a field (see Lemma **??**). The only polynomial ring that is a field is when $d = 0$ (i.e., $A = K$). Thus F is finite over K. □

6.5 Dimension Theory

Definition 6.5.1: Krull Dimension

The **Krull dimension** of a ring R, denoted $\dim(R)$, is the supremum of the lengths of chains of prime ideals in R. A chain of length n is:

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$$

Example 6.5.1: Dimension Examples

1. A field k has dimension 0.

2. A Principal Ideal Domain (PID) that is not a field (e.g., $\mathbb{Z}, k[X]$) has dimension 1. The chains are $(0) \subsetneq (p)$.

3. $\dim k[X_1, \ldots, X_n] = n$. The chain $(0) \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq \cdots \subsetneq (X_1, \ldots, X_n)$ has length n.

Definition 6.5.2: Height

For a prime ideal $\mathfrak{p}$, the **height** of $\mathfrak{p}$, denoted $\mathrm{ht}(\mathfrak{p})$, is the supremum of lengths of chains of primes descending from $\mathfrak{p}$:

$$\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_k = \mathfrak{p}$$

Note: $\mathrm{ht}(\mathfrak{p}) = \dim(R_{\mathfrak{p}})$.

6.6 Behavior of Dimension under Integral Extensions

Let $R \subseteq S$ be an integral extension. We compare the prime spectrums of R and S.

Lemma 6.6.1: Field Lemma

Let $R \subseteq S$ be an integral extension where R, S are domains. Then R is a field if and only if S is a field.

Proof. ($\Rightarrow$) Let $s \in S, s \neq 0$. s satisfies $s^n + r_1 s^{n-1} + \cdots + r_n = 0$. Since S is a domain, we can assume $r_n \neq 0$ (divide by s if needed). Then $s(s^{n-1} + \dots) = -r_n$. Since R is a field, r_n is invertible, so s is invertible. ($\Leftarrow$) Let $r \in R, r \neq 0$. Then $r^{-1} \in S$. Since r^{-1} is integral over R, $(r^{-1})^n + a_1(r^{-1})^{n-1} + \cdots + a_n = 0$. Multiplying by r^{n-1}, we find $r^{-1} = -(a_1 + a_2 r + \dots) \in R$. □

Theorem 6.6.1: Lying Over and Going Up

Let $R \subseteq S$ be an integral extension.

1. **Lying Over:** For any prime $\mathfrak{p} \in \mathrm{Spec}(R)$, there exists a prime $Q \in \mathrm{Spec}(S)$ such that $Q \cap R = \mathfrak{p}$.

2. **Incomparability:** If $Q_1 \subseteq Q_2$ are primes in S and $Q_1 \cap R = Q_2 \cap R$, then $Q_1 = Q_2$.

3. **Going Up:** Given a chain of primes $\mathfrak{p}_0 \subseteq \cdots \subseteq \mathfrak{p}_n$ in R and a prime Q_0 in S lying over $\mathfrak{p}_0$, there exists a chain $Q_0 \subseteq \cdots \subseteq Q_n$ in S lying over the chain in R.

Proof. **(1) Lying Over:** We localize at $\mathfrak{p}$. Consider $R_{\mathfrak{p}} \subseteq S_{\mathfrak{p}}$. Let $\mathfrak{m}$ be a maximal ideal of $S_\mathfrak{p}$. The contraction of $\mathfrak{m}$ to $R_\mathfrak{p}$ is the unique maximal ideal $\mathfrak{p}R_\mathfrak{p}$. The contraction of $\mathfrak{m}$ to S gives the desired prime Q.

(3) Going Up: By induction, it suffices to lift one step. Let $\mathfrak{p} \subseteq \mathfrak{p}'$ and Q lie over $\mathfrak{p}$. Consider $\bar{R} = R/\mathfrak{p} \subseteq \bar{S} = S/Q$. This is an integral extension. $\mathfrak{p}'/\mathfrak{p}$ is a prime in $\bar{R}$. By Lying Over applied to $\bar{R} \subseteq \bar{S}$, there exists a prime $\bar{Q}'$ lying over $\mathfrak{p}'/\mathfrak{p}$. Its preimage in S is the desired Q'. □

> **Corollary 6.6.1: Dimension Equality**If $R \subseteq S$ is an integral extension, then $\dim(R) = \dim(S)$.

Proof. By "Lying Over", any chain in R can be lifted to S, so $\dim(S) \geq \dim(R)$. By "Incomparability", a chain in S cannot contract to the same prime twice, so the contraction of a chain in S gives a chain of distinct primes in R of the same length. Thus $\dim(R) \geq \dim(S)$. □

6.7 Artinian Rings

Definition 6.7.1: Artinian Modules and Rings

- An R-module M is **Artinian** if it satisfies the Descending Chain Condition (DCC) on submodules: $M_1 \supseteq M_2 \supseteq \dots$ stabilizes.
- A ring R is **Artinian** if it is Artinian as a module over itself (i.e., DCC on ideals).

Proposition 6.7.1: Properties of Artinian Rings

Let R be an Artinian ring.

1. Every prime ideal in R is maximal (i.e., $\dim(R) = 0$).
2. R has only finitely many maximal ideals.
3. The Jacobson radical $J(R)$ is nilpotent.

Proof. (1) Let $\mathfrak{p}$ be a prime. Then $D = R/\mathfrak{p}$ is an Artinian domain. For any $x \in D, x \neq 0$, the chain $(x) \supseteq (x^2) \supseteq \dots$ stabilizes, so $(x^n) = (x^{n+1})$ for some n. Thus $x^n = yx^{n+1} \implies 1 = xy$, so x is invertible. D is a field, so $\mathfrak{p}$ is maximal. □

CHAPTER 7

ARTINIAN RINGS

7.1 Artinian Rings

Basic Properties of Artinian Rings

We begin by recalling the definition of an Artinian ring. A ring R is Artinian if it satisfies the Descending Chain Condition (DCC) on ideals.

> **Remark 7.1.1: Jacobson Radical**The Jacobson radical of R, denoted $J(R)$, is the intersection of all maximal ideals of R.
>
> $$J(R) = \bigcap_{\mathfrak{m} \in \operatorname{MaxSpec}(R)} \mathfrak{m}$$
>
> Hence, for every Artinian ring R, $J(R)$ is defined similarly.

> **Proposition 7.1.1: Finiteness of Maximal Ideals**
>
> If R is an Artinian ring, then it has only finitely many maximal ideals.

Proof. Let Σ be the collection of all finite intersections of maximal ideals:

$$\Sigma = \{\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k \mid \mathfrak{m}_i \text{ is a maximal ideal}\}.$$

Since R is Artinian, the set Σ has a minimal element with respect to inclusion. Call this minimal element I.

Let $I = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$. Let $\mathfrak{m}$ be any maximal ideal of R. Consider the intersection $I \cap \mathfrak{m}$.

$$I \cap \mathfrak{m} = (\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n) \cap \mathfrak{m}.$$

This element belongs to Σ. Since $I \cap \mathfrak{m} \subseteq I$ and I is minimal, we must have $I \cap \mathfrak{m} = I$. This implies $I \subseteq \mathfrak{m}$.

$$\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n \subseteq \mathfrak{m}.$$

Since $\mathfrak{m}$ is a prime ideal (as it is maximal), by the Prime Avoidance Lemma (or standard properties of prime ideals), $\mathfrak{m}_i \subseteq \mathfrak{m}$ for some i. Since both are maximal, $\mathfrak{m}_i = \mathfrak{m}$. Thus, the only maximal ideals in R are $\mathfrak{m}_1, \dots, \mathfrak{m}_n$. □

Proposition 7.1.2: Nilpotence of the Jacobson Radical

Let R be an Artinian ring. Then the Jacobson radical $J(R)$ is nilpotent. That is, there exists an integer n such that $J(R)^n = 0$.

Proof. Let $\mathfrak{a} = J(R)$. Consider the descending chain:

$$\mathfrak{a} \supseteq \mathfrak{a}^2 \supseteq \mathfrak{a}^3 \supseteq \dots$$

Since R is Artinian, this chain stabilizes. Let $\mathfrak{a}^k = \mathfrak{a}^{k+1} = \cdots = \mathfrak{a}^N$ for large N. Let $I = \mathfrak{a}^N$ be this stable value. Thus $I^2 = I$.

We claim $I = 0$. Suppose $I \neq 0$. Consider the set of ideals:

$$\Lambda = \{K \trianglelefteq R \mid K \cdot I \neq 0\}.$$

Since $I^2 = I \cdot I = I \neq 0$ (assuming $I \neq 0$), $I \in \Lambda$, so Λ is non-empty. Since R is Artinian, Λ has a minimal element, say K_0.

Since $K_0 \in \Lambda$, there exists $a \in K_0$ such that $aI \neq 0$. Note that $(a) \subseteq K_0$. By minimality of K_0, we must have $K_0 = (a)$. Now consider the element a. We have:

$$(aI)I = aI^2 = aI \neq 0.$$

Thus $aI \subseteq (a)$ is in Λ. By minimality, $aI = (a)$. This implies there exists $b \in I$ such that $a = ab$. Substituting repeatedly:

$$a = ab = ab^2 = ab^3 = \dots$$

Since $b \in I \subseteq J(R)$, b belongs to every maximal ideal. However, in an Artinian ring, elements of the Jacobson radical are nilpotent? No, general theory says $1 - b$ is a unit if $b \in J(R)$. Actually, we rely on the property that in an Artinian ring, nilradical equals Jacobson radical. Since R is Artinian, b is nilpotent is not immediate unless we prove $J(R)$ is nil. *Correction from standard text:* The proof typically proceeds by noting $a = ab \implies a(1 - b) = 0$. Since $b \in J(R)$, $1 - b$ is a unit. Thus $a = 0$, a contradiction. Hence, $I = 0$, so $J(R)$ is nilpotent. □

Composition Series and Length

Definition 7.1.1: Composition Series

Let M be an R-module. A **composition series** of M is a descending filtration:

$$M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n = 0$$

such that each quotient M_i/M_{i+1} is a **simple** R-module (i.e., $M_i/M_{i+1} \cong R/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$).

Theorem 7.1.1: Jordan-Hölder Theorem

If M has a composition series of length n, then every composition series of M has length n. This invariant is denoted by $\lambda_R(M)$ (or $\ell(M)$), the **length** of M. If M does not have a composition series, we write $\lambda_R(M) = \infty$.

Proposition 7.1.3: Finite Length and Artinian/Noetherian

An R-module M has a composition series (i.e., finite length) if and only if M is both Noetherian and Artinian.

Proof. **(⇐)** Construct a chain by taking maximal proper submodules. Since M is Noetherian, a maximal submodule $M_1 \subsetneq M$ exists. Continue this process. The chain must terminate at 0 because M is Artinian. **(⇒)** If $\lambda(M) < \infty$, the module satisfies both ACC and DCC. □

Corollary 7.1.1: Artinian Rings are Noetherian An Artinian ring R is Noetherian if and only if $\lambda(R) < \infty$. Since we proved $J(R)$ is nilpotent and $R/J(R)$ is semisimple (product of fields), one can deduce R has finite length. **Conclusion:** Every Artinian ring is Noetherian of dimension 0.

Proposition 7.1.4: Characterization of Artinian Rings

Let R be a Noetherian ring. Then R is Artinian if and only if $\dim(R) = 0$.

Proof. **Sketch:** Use prime filtration. There exists a chain $0 = M_0 \subset \cdots \subset M_r = R$ where $M_i/M_{i-1} \cong R/\mathfrak{p}_i$. If $\dim(R) = 0$, all prime ideals are maximal. Thus $R/\mathfrak{p}_i$ are fields (simple modules). Thus $\lambda(R) < \infty$, implying R is Artinian. □

7.2 Graded Modules and Algebraic Geometry

Artinian Rings in Algebraic Geometry

Proposition 7.2.1: Zero Sets and Artinian Rings

Let k be an algebraically closed field. Let $R = k[X_1, \dots, X_n]$ and $I \subseteq R$ be an ideal. Then R/I is Artinian if and only if the zero set $Z(I) \subseteq \mathbb{A}_k^n$ is finite.

Proof. ($\Rightarrow$) If R/I is Artinian, it is Noetherian and has dimension 0. The prime ideals of R/I are maximal. We know $\operatorname{Min}(R/I) = \operatorname{Ass}(R/I)$ is finite. Let $\operatorname{Min}(R/I) = \{\mathfrak{m}_1, \dots, \mathfrak{m}_r\}$ (minimal primes are maximal since dim is 0). The zero set $Z(I) = V(I) = V(\sqrt{I}) = \bigcup V(\mathfrak{m}_i)$. Since $\mathfrak{m}_i$ are maximal ideals in a polynomial ring over an algebraically closed field, $V(\mathfrak{m}_i)$ is a single point. Thus $Z(I)$ is a finite set of points.

($\Leftarrow$) If $Z(I)$ is finite, say $\{P_1, \dots, P_k\}$, then these points correspond to maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_k$. The radical $\sqrt{I} = \bigcap \mathfrak{m}_i$. $R/\sqrt{I} \cong \prod R/\mathfrak{m}_i \cong k \times \cdots \times k$, which is Artinian. Since $\sqrt{I}$ is nilpotent modulo I (Noetherian ring), R/I is Artinian. □

Graded Rings and Modules

Definition 7.2.1: Graded Ring

A ring S is a **graded ring** if it has a decomposition $S = \bigoplus_{i \in \mathbb{N}} S_i$ (as abelian groups) such that $S_i \cdot S_j \subseteq S_{i+j}$ for all i, j.

Definition 7.2.2: Graded Module

An S-module M is a **graded module** if $M = \bigoplus_{i \in \mathbb{Z}} M_i$ such that $S_i \cdot M_j \subseteq M_{i+j}$. Elements of M_i are called **homogeneous elements** of degree i.

Remark 7.2.1: Finitely Generated Graded Modules If $S = R[X_1, \dots, X_n]$ where R is Artinian local and $\deg(X_i) = 1$, then S is Noetherian. If M is a graded S-module, it has a generating set of homogeneous elements. If M is finitely generated, let $d = \min\{\deg(g) \mid g \in \text{generators}\}$. Then $M_i = 0$ for $i < d$. Furthermore, each graded piece M_i is a finitely generated R-module.

7.3 Hilbert Functions and Hilbert Polynomials

Numerical Polynomials

Definition 7.3.1: Binomial Polynomials

Define the polynomials $P_k(X) := \binom{X}{k}$.

$$P_k(X) = \frac{X(X-1)\dots(X-k+1)}{k!} \in \mathbb{Q}[X].$$

Note that $P_0(X) = 1$, $P_1(X) = X$. These form a basis for $\mathbb{Q}[X]$.

Lemma 7.3.1: Integer-Valued Polynomials

Let $f \in \mathbb{Q}[X]$. The following are equivalent:

1. f is a $\mathbb{Z}$-linear combination of the $P_k(X)$.
2. $f(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$.
3. $f(n) \in \mathbb{Z}$ for all $n \gg 0$.
4. The difference function $\Delta f(n) := f(n+1) - f(n)$ satisfies these properties.

Hilbert Function

Let R be an Artinian local ring and $S = R[X_1, \ldots, X_n]$ with standard grading. Let M be a finitely generated graded S-module. We observed that each M_j is a finitely generated R-module. Since R is Artinian, M_j has finite length $\lambda_R(M_j)$.

Definition 7.3.2: Hilbert Function

The **Hilbert function** of M is defined as:

$$H_M(j) := \lambda_R(M_j) \quad \text{for } j \in \mathbb{Z}.$$

Theorem 7.3.1: Hilbert Polynomial

Let M be a finitely generated graded S-module. There exists a polynomial $P_M(X) \in \mathbb{Q}[X]$ such that:

$$H_M(j) = P_M(j) \quad \text{for all } j \gg 0.$$

This polynomial is called the **Hilbert Polynomial** of M. Furthermore, $\deg(P_M) \leq n-1$.

Proof. We proceed by induction on n (the number of variables in S).

Base case ($n = 0$): $S = R$. M is a finitely generated R-module. Since R is Artinian, M has finite length. Also, since M is graded over $S = R$ (concentrated in degree 0 usually, or finite degrees), $M_j = 0$ for large j. Thus $H_M(j) = 0$ for $j \gg 0$, which is the zero polynomial.

Inductive step: Assume the theorem holds for $n-1$ variables. Consider the multiplication map by X_n:

$$\phi : M \to M(1)$$

defined by $m \mapsto X_n m$. Note: strictly this maps $M_j \to M_{j+1}$. Consider the exact sequence of graded modules:

$$0 \longrightarrow K \longrightarrow M(-1) \xrightarrow{\cdot X_n} M \longrightarrow C \longrightarrow 0$$

where $K = \ker(\phi)$ and $C = \operatorname{coker}(\phi)$. Note that X_n annihilates both K and C. Thus, K and C are modules over $S/X_nS \cong R[X_1, \ldots, X_{n-1}]$. By the inductive hypothesis, $H_K(j)$ and $H_C(j)$ agree with polynomials $P_K(j)$ and $P_C(j)$ for $j \gg 0$.

From the additivity of length in exact sequences:

$$\lambda(M_j) - \lambda(M_{j-1}) = \lambda(C_j) - \lambda(K_j)$$

(using the shifted grading).

$$H_M(j) - H_M(j-1) = H_C(j) - H_{K(1)}(j).$$

Let $f(j) = H_M(j)$. Then $\Delta f(j)$ is a polynomial for $j \gg 0$. By the Lemma on numerical polynomials, if the difference function is polynomial, the function itself is a polynomial for $j \gg 0$. □

7.4 Hilbert-Samuel Polynomial

Setup and Definition

Let $(R, \mathfrak{m})$ be a Noetherian local ring. Let I be an $\mathfrak{m}$-primary ideal (i.e., $\sqrt{I} = \mathfrak{m}$). Let M be a finitely generated R-module.

Consider the filtration $M \supseteq IM \supseteq I^2M \supseteq \ldots$. Since $\sqrt{I} = \mathfrak{m}$, R/I is Artinian. Consequently, M/I^nM has finite length.

Definition 7.4.1: Hilbert-Samuel Polynomial

There exists a polynomial $P_{I,M}(X) \in \mathbb{Q}[X]$ such that for $n \gg 0$:

$$\lambda_R(M/I^{n+1}M) = P_{I,M}(n).$$

$P_{I,M}$ is called the **Hilbert-Samuel polynomial** of M with respect to I.

Associated Graded Rings and Modules

To prove the existence of $P_{I,M}$, we construct the associated graded structures.

Definition 7.4.2: Associated Graded Ring

The associated graded ring of R with respect to I is:

$$gr_I(R) := \bigoplus_{n=0}^{\infty} \frac{I^n}{I^{n+1}}.$$

This is a generated by I/I^2 over R/I. Since R/I is Artinian and I is finitely generated, $gr_I(R)$ is a Noetherian graded ring generated in degree 1 over an Artinian ring (R/I).

Definition 7.4.3: Associated Graded Module

The associated graded module of M is:

$$gr_I(M) := \bigoplus_{n=0}^{\infty} \frac{I^n M}{I^{n+1}M}.$$

This is a finitely generated graded module over $gr_I(R)$.

Proof of Existence

Theorem 7.4.1: Existence Theorem

Let $(R, \mathfrak{m})$ be a Noetherian local ring, I an $\mathfrak{m}$-primary ideal, and M a finitely generated R-module. Then the length $\lambda(M/I^{n+1}M)$ agrees with a polynomial for large n.

Proof. Note that:

$$\lambda\left(\frac{M}{I^{n+1}M}\right) = \sum_{j=0}^{n} \lambda\left(\frac{I^j M}{I^{j+1}M}\right).$$

Let $H(n) = \lambda(I^n M/I^{n+1}M)$. This is exactly the Hilbert function of the graded module $gr_I(M)$ over the ring $gr_I(R)$. Since $gr_I(R)$ is a polynomial ring over the Artinian ring R/I (generated by images of generators of I), we can apply the Hilbert Polynomial Theorem from Lecture 38. Thus, $H(n)$ is a polynomial for $n \gg 0$. The function we are interested in is the partial sum (integration) of $H(n)$. If $H(n)$ is a polynomial of degree d, then $\sum_{j=0}^{n} H(j)$ is a polynomial of degree $d+1$. □

Degree and Dimension

Proposition 7.4.1: Degree of Hilbert-Samuel Polynomial

The degree of the Hilbert-Samuel polynomial $P_{I,M}(n)$ is denoted by $d(M)$ or $\delta(M)$.

1. $\deg P_{I,M}$ is independent of the choice of the $\mathfrak{m}$-primary ideal I.

2. $d(M) = \dim(M)$ (the Krull dimension of the module M).

3. Specifically, $\deg P_{I,M} \leq$ minimal number of generators of I.

Proof. **Independence of I:** Since I is $\mathfrak{m}$-primary, there exists k such that $\mathfrak{m}^k \subseteq I \subseteq \mathfrak{m}$. This implies inequalities between the filtrations which, asymptotically, ensures the polynomials have the same degree. □

Remark 7.4.1: System of Parameters The dimension equality relates to the concept of a System of Parameters. $s(M)$ denotes the smallest s such that there exist $x_1, \ldots, x_s$ where $M/(x_1, \ldots, x_s)M$ has finite length. It turns out $s(M) = d(M) = \dim(M)$.

Artin-Rees Lemma

Lemma 7.4.1: Artin-Rees Lemma

Let R be Noetherian, I an ideal, M a finitely generated module, and $N \subseteq M$ a submodule. Then the I-adic topology on N coincides with the topology induced by M. Specifically, there exists k such that for all $n \geq k$:

$$I^n M \cap N = I^{n-k}(I^k M \cap N).$$

CHAPTER 8

DIMENSION THEORY

8.1 The Hilbert-Samuel Polynomial

Warning 8.1.1: Context Setup Let $(R, \mathfrak{m})$ be a Noetherian local ring, and let M be a finitely generated R-module. Let I be an ideal such that the length $l(M/IM) < \infty$. Usually, this implies I is $\mathfrak{m}$-primary, or specifically, $\sqrt{I + \operatorname{Ann}(M)} = \mathfrak{m}$.

Proposition 8.1.1: Additivity of Hilbert Polynomials

Let $(R, \mathfrak{m})$ be a Noetherian local ring and I an ideal as defined above. Let

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

be an exact sequence of finitely generated R-modules. Then:

$$P_{I,M}(n) = P_{I,M'}(n) + P_{I,M''}(n) - Q(n)$$

where $P_{I,M}$ denotes the Hilbert-Samuel polynomial of M with respect to I, and $Q(n)$ is a polynomial with non-negative leading coefficient such that $\deg Q < \deg P_{I,M'}$.

Proof. Given the exact sequence $0 \to M' \to M \to M'' \to 0$, tensoring with R/I^n does not preserve exactness on the left. However, we can analyze the filtration. Consider the induced sequence:

$$\frac{M'}{M' \cap I^n M} \to \frac{M}{I^n M} \to \frac{M''}{I^n M''} \to 0$$

The term on the left requires care. By the Artin-Rees Lemma, the filtration $\{M' \cap I^n M\}$ is I-stable. This implies there exists n_0 such that for $n \geq n_0$,

$$M' \cap I^{n+1} M = I(M' \cap I^n M)$$

Thus, the topology defined by $\{M' \cap I^n M\}$ is equivalent to the I-adic topology on M'.

The length functions satisfy:

$$l\left(\frac{M}{I^nM}\right) = l\left(\frac{M''}{I^nM''}\right) + l\left(\frac{M'}{M' \cap I^nM}\right)$$

We can rewrite the last term:

$$l\left(\frac{M'}{M' \cap I^nM}\right) = l\left(\frac{M'}{I^nM'}\right) - l\left(\frac{M' \cap I^nM}{I^nM'}\right)$$

For large n, $l(M/I^nM)$ agrees with a polynomial $P_{I,M}(n)$. Since the filtration on M' induced by M is stable, the difference term corresponds to a polynomial of lower degree (the "error" term $Q(n)$). Since lengths are non-negative, the leading coefficient of the Hilbert polynomial must be positive. □

> **Corollary 8.1.1: Comparison of Degrees**With notation as in the proposition:
>
> 1. $\deg P_{I,M} = \max(\deg P_{I,M'}, \deg P_{I,M''})$.
> 2. If $\deg P_{I,M'} = \deg P_{I,M''}$, then the leading coefficient of $P_{I,M}$ is the sum of the leading coefficients.
> 3. $\deg P_{I,M'} \leq \deg P_{I,M}$.

> **Corollary 8.1.2: Reduction by Non-Zero Divisors**If $x \in R$ is a non-zero divisor (NZD) on M, then:
> $$\deg P_{I,M/xM} = \deg P_{I,M} - 1$$

Proof. Consider the exact sequence defined by multiplication by x:

$$0 \to M \xrightarrow{x} M \to M/xM \to 0$$

Applying the previous proposition (and adjusting for the shift in degree caused by $I^nM : x$), we find that the leading term of the Hilbert polynomial drops by exactly one degree, similar to taking a finite difference $\Delta P(n) = P(n) - P(n-1)$. □

8.2 Dimension Theory

We define three invariants for a finitely generated module M over a Noetherian local ring $(R, \mathfrak{m})$:

Definition 8.2.1: Dimension Invariants

1. $\delta(M)$: The degree of the Hilbert-Samuel polynomial $P_{\mathfrak{m},M}(n)$.
2. $d(M) = \dim(M)$: The Krull dimension of M, defined as $\dim(R/\text{Ann}(M))$.
3. $s(M)$: The least number of generators of an ideal of definition for M (related to the Chevalley dimension). Specifically, the smallest t such that there exist $x_1, \ldots, x_t \in \mathfrak{m}$ with $l(M/(x_1, \ldots, x_t)M) < \infty$.

Theorem 8.2.1: Fundamental Theorem of Dimension Theory

Let $(R, \mathfrak{m})$ be a Noetherian local ring and M a finitely generated R-module. Then:

$$\delta(M) = d(M) = s(M)$$

Proof. The proof proceeds in a cycle of inequalities: $d(M) \leq \delta(M) \leq s(M) \leq d(M)$.

Step 1: $s(M) \leq d(M)$. Let $d = \dim(M)$. We proceed by induction on d. If $d = 0$, then M has finite length, so $\mathfrak{m}^k M = 0$ for some k. The ideal of definition can be generated by 0 elements (empty set), so $s(M) = 0$. If $d > 0$, we can choose parameters avoiding the minimal primes of maximal dimension to reduce the dimension by 1.

Step 2: $\delta(M) \leq s(M)$. Let $x_1, \ldots, x_t$ be a system of parameters for M, so $s(M) = t$. Let $I = (x_1, \ldots, x_t)$. Consider the associated graded ring $\text{gr}_I(R)$. The Hilbert polynomial corresponds to the growth of the module. Using the Koszul complex or standard reduction arguments on the number of generators, one can show that modding out by one element reduces the degree of the Hilbert polynomial by at most 1 (exactly 1 if it's a non-zero divisor). Thus, $\delta(M) \leq t = s(M)$.

Step 3: $d(M) \leq \delta(M)$. We use induction on $\delta(M)$. If $\delta(M) = 0$, then $P_{\mathfrak{m},M}(n)$ is constant for large n. This implies $l(M/\mathfrak{m}^n M)$ stabilizes, which implies $\mathfrak{m}^n M = 0$ by Nakayama's Lemma (NAK). Thus $\dim M = 0$. Assume $\delta(M) > 0$. We reduce to the case $M = R/\mathfrak{p}$ where $\mathfrak{p} \in \text{Ass}(M)$. Let x be a non-zero divisor on M. Then $\delta(M/xM) = \delta(M) - 1$. By induction, $\dim(M/xM) \leq \delta(M) - 1$. Since x is a NZD, $\dim(M/xM) = \dim(M) - 1$. Therefore, $\dim(M) - 1 \leq \delta(M) - 1 \implies \dim(M) \leq \delta(M)$. □

Corollary 8.2.1: Krull's Principal Ideal Theorem Let R be a Noetherian ring and $x \in R$. Let $\mathfrak{p}$ be a minimal prime over (x). Then:

$$\text{ht}(\mathfrak{p}) \leq 1$$

More generally, if $\mathfrak{p}$ is minimal over $(x_1, \ldots, x_n)$, then $\text{ht}(\mathfrak{p}) \leq n$.

Proof. In the local ring $R_{\mathfrak{p}}$, the ideal $(x_1, \ldots, x_n)R_{\mathfrak{p}}$ is $\mathfrak{p}R_{\mathfrak{p}}$-primary. Thus, $s(R_{\mathfrak{p}}) \leq n$.

By the Fundamental Theorem, $\dim(R_{\mathfrak{p}}) = s(R_{\mathfrak{p}}) \leq n$. Since $\dim(R_{\mathfrak{p}}) = \mathrm{ht}(\mathfrak{p})$, the result follows. □

Proposition 8.2.1: Converse of Principal Ideal Theorem

Let $(R, \mathfrak{m})$ be Noetherian. Let $\mathfrak{p}$ be a prime ideal. The following are equivalent:

1. $\mathrm{ht}(\mathfrak{p}) \leq n$.

2. $\mathfrak{p}$ is minimal over an ideal generated by n elements.

8.3 Dimension of Polynomial Rings

Theorem 8.3.1: Dimension of $R[x]$

Let R be a Noetherian ring. Then:

$$\dim R[x] = \dim R + 1$$

Proof. Let $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_n$ be a chain of primes in R. Then

$$\mathfrak{p}_0 R[x] \subset \cdots \subset \mathfrak{p}_n R[x] \subset \mathfrak{p}_n R[x] + (x)$$

is a chain of length $n+1$ in $R[x]$. Thus $\dim R[x] \geq \dim R + 1$.

For the upper bound, let $Q \subset R[x]$ be a prime ideal and let $P = Q \cap R$. We claim $\mathrm{ht}(Q) \leq \mathrm{ht}(P) + 1$. We can localize at P to assume $(R, \mathfrak{m})$ is local and $P = \mathfrak{m}$. There are two cases:

1. $Q = \mathfrak{m}R[x]$. In this case $\mathrm{ht}(Q) = \mathrm{ht}(\mathfrak{m})$. Wait, this ideal is not maximal in $R[x]$.

2. $Q \supset \mathfrak{m}R[x]$. Then modulo $\mathfrak{m}R[x]$, Q corresponds to a prime in $(R/\mathfrak{m})[x]$, which is a PID. Thus Q is generated by one additional element modulo $\mathfrak{m}R[x]$.

Using the properties of chains and the structure of primes in extensions, we conclude $\dim R[x] \leq \dim R + 1$. □

8.4 Integral Extensions and Going Down

Definition 8.4.1: Noether Normalization

Let k be a field and R a finitely generated k-algebra. Then there exist algebraically independent elements $z_1, \ldots, z_d \in R$ such that R is a finite module over the polynomial subring $A = k[z_1, \ldots, z_d]$. Here $d = \dim R$.

Theorem 8.4.1: Going Down Theorem

Let $A \subseteq B$ be an integral extension of domains with A integrally closed. Let $\mathfrak{p}_1 \subset \mathfrak{p}_2$ be primes in A and let $\mathfrak{q}_2$ be a prime in B such that $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$. Then there exists a prime $\mathfrak{q}_1 \subset \mathfrak{q}_2$ in B such that $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$.

Proof. Consider the localized ring $B_{\mathfrak{q}_2}$. We need to find a prime lying over $\mathfrak{p}_1$. This relates to the surjectivity of the map on spectra for integral extensions, combined with the property that A is integrally closed (which prevents "branching" behavior that would stop the chain from descending). The proof typically involves manipulating the extension of ideals $\mathfrak{p}_1 B_{\mathfrak{q}_2} \cap A$. □

Corollary 8.4.1: Catenary Property of Affine Domains If $R = k[x_1, \dots, x_n]$ is a polynomial ring over a field, then R is catenary. That is, every saturated chain of primes between two prime ideals $\mathfrak{p} \subset \mathfrak{q}$ has the same length.

8.5 Graded Rings and Modules

Definition 8.5.1: Graded Ring

A ring R is $\mathbb{Z}$-graded (or $\mathbb{N}$-graded) if it has a decomposition $R = \bigoplus_{i \in \mathbb{Z}} R_i$ (as abelian groups) such that $R_i R_j \subseteq R_{i+j}$. Elements in R_i are called homogeneous elements of degree i.

Proposition 8.5.1: Homogeneous Annihilators

Let $M = \bigoplus M_n$ be a graded R-module.

1. $\text{Ann}(M)$ is a homogeneous ideal.
2. Any associated prime $\mathfrak{p} \in \text{Ass}(M)$ is a homogeneous ideal.

Proof. Let $f \in \text{Ann}(M)$. Write $f = \sum f_i$ where f_i are homogeneous components. For any homogeneous $m \in M$, $fm = \sum f_i m = 0$. Since $\deg(f_i m)$ are distinct, each $f_i m = 0$. Since M is generated by homogeneous elements, $f_i \in \text{Ann}(M)$ for all i. Thus the ideal is homogeneous. □

Lemma 8.5.1: Structure of Graded Domains

Let $R = \bigoplus_{n \geq 0} R_n$ be a graded domain. Then:

1. Every non-zero homogeneous element is invertible (if R is a field, but usually this characterizes graded fields).
2. If R is a graded field, then R_0 is a field and either $R = R_0$ or $R \cong R_0[t, t^{-1}]$ (if $\mathbb{Z}$-graded) or just R_0 (if $\mathbb{N}$-graded non-trivially).

> 3. (From notes): If R is a graded domain, and we consider the field of fractions $K = Q(R)$, we can define a subfield K_0 of elements of degree 0.

Proof. If $t \in R$ is a homogeneous element of positive degree d, and R is a domain, then purely algebraic relations split into homogeneous components. If R_0 is a field and R contains a transcendental element T of degree 1, then $R \cong R_0[T]$. The notes suggest an argument involving t being transcendental over R_0. □

CHAPTER 9

GRADED RINGS AND MODULES

9.1 Dimension of Graded Rings

Homogeneous Prime Ideals

Recall that in a graded ring $R = \bigoplus_{n\geq 0} R_n$, an ideal I is homogeneous if it is generated by homogeneous elements. Let P be a prime ideal. We denote by P^* (or sometimes $\mathfrak{p}^{hom}$) the ideal generated by the homogeneous elements contained in P.

> **Lemma 9.1.1: Prime Ideals in Graded Rings**
>
> Let R be a graded ring and P be a prime ideal. Let $p = P^*$ be the ideal generated by all homogeneous elements in P. Then:
>
> 1. p is a prime ideal.
> 2. If P is not homogeneous, then $\operatorname{ht}(P/p) = 1$.

Proof. **(1) p is prime:** Let a, b be homogeneous elements such that $ab \in p$. Since $p \subseteq P$ and P is prime, either $a \in P$ or $b \in P$. Since a, b are homogeneous, if $a \in P$ then $a \in P^*$ (by definition of P^*). Thus $a \in p$ or $b \in p$. Since p is generated by homogeneous elements, this suffices to show p is prime.

(2) Height of P/p: Assume P is not homogeneous. We can pass to the quotient ring R/p. Note that R/p is a graded domain. In this domain, the image of P, denoted $\bar{P}$, is a prime ideal that contains no nonzero homogeneous elements.

Consider the localization $U^{-1}(R/p)$, where U is the set of all nonzero homogeneous elements of R/p. Since R/p is a domain, U is a multiplicatively closed set. The ring $S = U^{-1}(R/p)$ is a graded ring where every nonzero homogeneous element is invertible.

- S_0 is a field (let's call it K).
- $S \cong K[t, t^{-1}]$ (if there is a homogeneous element of degree non-zero) or $S = K$ (trivially).

However, structurally, if there are elements of positive degree, S looks like a Laurent polynomial ring over a field. The ideal $\bar{P}S$ is a proper prime ideal in S. Since $\bar{P}$ contains no homogeneous elements, in the localization S, the extension is a prime ideal in a principal ideal domain (or field), which implies the height is limited. Specifically, standard theory (referencing *Cox, Little, O'Shea*) shows that chains of primes in R strictly containing p and consisting of non-homogeneous primes have length at most 1. Thus $\mathrm{ht}(P/p) = 1$. □

> **Example 9.1.1: Spectrum of $k[t]$**Consider $R = k[t]$ with standard grading. $\mathrm{Spec} k[t] = \{(0)\} \cup \{(f(t)) \mid f \text{ is irreducible}\}$. The homogeneous primes are (0) and (t). If $P = (t-1)$, it is not homogeneous. $P^* = (0)$. $\mathrm{ht}(P/P^*) = \mathrm{ht}((t-1)/(0)) = 1$.

Support and Associated Primes

Lemma 9.1.2: Support of Graded Modules

Let R be a Noetherian graded ring and M a graded R-module. If $\mathfrak{p} \in \mathrm{Supp}(M)$, then $\mathfrak{p}^* \in \mathrm{Supp}(M)$.

Proof. $\mathfrak{p} \in \mathrm{Supp}(M) \iff \mathfrak{p} \supseteq \mathrm{Ann}(M)$. Since M is graded, $\mathrm{Ann}(M)$ is a homogeneous ideal. Therefore, if $\mathfrak{p} \supseteq \mathrm{Ann}(M)$, then the homogeneous part $\mathfrak{p}^*$ also contains $\mathrm{Ann}(M)$ (since $\mathrm{Ann}(M)$ is generated by homogeneous elements). Thus $\mathfrak{p}^* \in \mathrm{Supp}(M)$. □

Theorem 9.1.1: Associated Primes are Homogeneous

Let R be a Noetherian graded ring and M a finitely generated graded module.

1. If $\mathfrak{p} \in \mathrm{Ass}(M)$, then $\mathfrak{p}$ is homogeneous.
2. Let $d = \dim M_{\mathfrak{p}}$ (as a module over $R_{\mathfrak{p}}$).
   - If $\mathfrak{p}$ is homogeneous, $\dim M_{\mathfrak{p}}$ is determined by a chain of graded prime ideals.
   - If $\mathfrak{p}$ is not homogeneous, $\dim M_{\mathfrak{p}} = \dim M_{\mathfrak{p}^*} + 1$.

Proof. **(1)** Let $\mathfrak{p} \in \mathrm{Ass}(M)$. Then $\mathfrak{p} = \mathrm{Ann}(m)$ for some $0 \neq m \in M$. By properties of graded modules, $\mathrm{Ann}(m)$ is homogeneous? Not necessarily for arbitrary m. However, we know $\mathfrak{p}^* \in \mathrm{Ass}(M)$ (Standard result: associated primes of graded modules are homogeneous, usually proven by picking a homogeneous nonzero element in the submodule isomorphic to $R/\mathfrak{p}$).

(2) Dimension Relation: Let $\mathfrak{p}$ be non-homogeneous. We have $\mathfrak{p}^* \subsetneq \mathfrak{p}$. Since $\mathrm{ht}(\mathfrak{p}/\mathfrak{p}^*) = 1$, we can form a chain of primes ending at $\mathfrak{p}$ by extending a chain ending at $\mathfrak{p}^*$. Thus $\dim M_{\mathfrak{p}} = \dim M_{\mathfrak{p}^*} + 1$. □

9.2 Graded NAK and Hilbert Series

Graded Nakayama's Lemma

Let $R = k[X_1, \dots, X_n]$ be a graded ring with $\deg(X_i) = 1$. Let $\mathfrak{m} = (X_1, \dots, X_n)$ be the unique homogeneous maximal ideal.

Proposition 9.2.1: Graded NAK

Let M be a finitely generated graded R-module. If $\mathfrak{m}M = M$, then $M = 0$.

Proof. Assume by way of contradiction that $M \neq 0$. Since M is finitely generated and graded, the degrees of homogeneous elements are bounded below. Let d be the minimal degree such that $M_d \neq 0$. Let $m \in M_d$ be nonzero. Since $M = \mathfrak{m}M$, we can write:

$$m = \sum_{i=1}^{n} X_i m_i$$

where $m_i \in M$. For degree reasons:

$$\deg(m) = d$$

$$\deg(X_i m_i) = 1 + \deg(m_i) \implies \deg(m_i) = d - 1$$

But by minimality of d, $M_{d-1} = 0$, so $m_i = 0$. Thus $m = 0$, a contradiction. Therefore $M = 0$. □

Proposition 9.2.2: Graded Free Resolutions

Let M be a finitely generated graded R-module. Then there exists a free resolution:

$$\cdots \to F_1 \to F_0 \to M \to 0$$

where each F_i is a graded free module of the form $\bigoplus_j R(-d_{ij})$ and the maps preserve degrees.

Proof. Let $\{m_1, \dots, m_s\}$ be homogeneous generators of M with $\deg(m_i) = d_i$. Define a map from the free module $F_0 = \bigoplus_{i=1}^{s} R(-d_i)$ to M:

$$\phi : \bigoplus_{i=1}^{s} R(-d_i) \to M$$

mapping the generator e_i (which has degree d_i in the shifted ring) to m_i. This map is degree preserving and surjective. Let $K = \ker(\phi)$. Since R is Noetherian, K is finitely generated. K is a graded submodule. Repeat the process for K to get F_1, and so on. By Hilbert's Syzygy Theorem, this process terminates (i.e., we eventually reach a kernel of 0) in at most n steps. □

Remark 9.2.1: Shifted Modules$R(j)$ denotes the graded module where $R(j)_d = R_{j+d}$. Example: $R(-1)$ is a free module generated by an element in degree 1. $[R(-1)]_0 = R_{-1} = 0$. $[R(-1)]_1 = R_0 = k$. $[R(-1)]_2 = R_1 = k\langle X_1, \dots, X_n\rangle$.

Example 9.2.1: Resolution Example Let $I = (X_1^2, X_1X_2) \subset R = k[X_1, X_2]$. Generators are degree 2. Map $\phi : R(-2) \oplus R(-2) \to I$ given by $e_1 \mapsto X_1^2, e_2 \mapsto X_1X_2$. Kernel relation: $X_2(X_1^2) - X_1(X_1X_2) = 0 \implies X_2e_1 - X_1e_2 \in \ker \phi$. This relation has degree 3. So we need $R(-3)$ to cover the kernel. Resolution: $0 \to R(-3) \to R(-2) \oplus R(-2) \to I \to 0$.

Hilbert Series

Definition 9.2.1: Hilbert Series

Let M be a finitely generated graded module. The Hilbert Series of M is:

$$H_M(t) = \sum_{j\in\mathbb{Z}} (\dim_k M_j) t^j$$

Note: Since M is f.g., $M_j = 0$ for $j \ll 0$.

Proposition 9.2.3: Additivity

Given a short exact sequence of graded modules with degree preserving maps:

$$0 \to M' \to M \to M'' \to 0$$

Then $H_M(t) = H_{M'}(t) + H_{M''}(t)$.

Proof. For each degree j, the sequence of vector spaces $0 \to M'_j \to M_j \to M''_j \to 0$ is exact. Thus $\dim M_j = \dim M'_j + \dim M''_j$. Multiplying by t^j and summing over j gives the result. □

9.3 Dimension and Hilbert Series Form

Theorem 9.3.1: Hilbert Series Rational Function

Let $d = \dim M$. Then there exists a Laurent polynomial $q_M(t) \in \mathbb{Z}[t, t^{-1}]$ such that:

$$H_M(t) = \frac{q_M(t)}{(1-t)^d}$$

Moreover, $q_M(1) > 0$.

Proof. We proceed by induction on $d = \dim M$.

Base Case ($d = 0$): If $\dim M = 0$, then M has finite length (is an Artinian module over R). $M_j = 0$ for $|j| \gg 0$. Thus $H_M(t) = \sum_{j=N_1}^{N_2} (\dim M_j) t^j$ is a polynomial (or Laurent polynomial). Here the denominator is $(1-t)^0 = 1$. $q_M(1) = \sum \dim M_j = \dim_k M > 0$ (assuming $M \neq 0$).

Inductive Step ($d > 0$): Assume the theorem holds for modules of dimension $< d$. We want to find a homogeneous element $f \in R$ of degree 1 that is a non-zero divisor (NZD) on M. However, R might not have such an element if the field k is finite or if all degree 1 elements are in associated primes. Without loss of generality (by extending the field k to be infinite), we can assume there exists $f \in R_1$ such that f is not in any associated prime $\mathfrak{p} \in \operatorname{Ass}(M)$ except possibly $\mathfrak{m}$. Actually, use a filtration. More simply, consider the exact sequence defined by multiplication by f:

$$0 \to K \to M(-1) \xrightarrow{\cdot f} M \to C \to 0$$

where $K = \{m \in M \mid fm = 0\}$ and $C = M/fM$. Since f has degree 1, the map is $M_{j-1} \to M_j$. In terms of Hilbert series:

$$H_K(t) - tH_M(t) + H_M(t) - H_C(t) = 0$$

$$(1-t)H_M(t) = H_C(t) - H_K(t)$$

If f is a NZD, $K = 0$. Then $(1-t)H_M(t) = H_{M/fM}(t)$. Standard dimension theory says $\dim(M/fM) = \dim M - 1 = d - 1$. By induction, $H_{M/fM}(t) = \frac{Q(t)}{(1-t)^{d-1}}$. Then $H_M(t) = \frac{Q(t)}{(1-t)^d}$.

General Case (using filtration): Even if f is not a NZD, the kernel K and cokernel C have dimension $< d$ (related to support arguments). Specifically, we can filter M by prime ideals: $0 = M_0 \subset M_1 \subset \cdots \subset M_k = M$ where $M_i/M_{i-1} \cong (R/\mathfrak{p}_i)(-\ell_i)$. The Hilbert series is additive. $H_{R/\mathfrak{p}}(t)$ for $\mathfrak{p}$ homogeneous. If $\mathfrak{p} = \mathfrak{m}$, dimension is 0. If $\dim(R/\mathfrak{p}) = \delta$, we reduce to the domain case. Ultimately, $H_M(t) = \frac{q_M(t)}{(1-t)^d}$ with $q_M(1) > 0$. □

9.4 Hilbert Polynomial

Definition 9.4.1: Hilbert Polynomial

The Hilbert Series can be expanded. Let $H_M(t) = \frac{q_M(t)}{(1-t)^d}$. Expanding $(1-t)^{-d} = \sum_{n \geq 0} \binom{n+d-1}{d-1} t^n$, we see that for n sufficiently large, $\dim M_n$ is given by a polynomial $P_M(n)$, called the **Hilbert Polynomial**.

Proposition 9.4.1: Polynomial Coefficients

We can write the polynomial $P_M(X)$ in the basis of binomial coefficients:

$$P_M(X) = \sum_{i=0}^{d-1} e_i(M) \binom{X+i}{i}$$

Wait, the notes suggest the form:

$$P_M(X) = \sum_{i=0}^{d-1} (-1)^{d-1-i} e_{d-1-i} \binom{X+i}{i}$$

Or more standardly (matching the notes "Lecture 50"):

$$P_M(X) = \sum_{i=0}^{n-1} e_i(M) P_i(X) \quad \text{where } P_i(X) = \binom{X}{i}$$

Crucially, the leading term is related to the pole at $t = 1$.

$$e_{d-1}(M) = q_M(1)$$

This leading coefficient (normalized) is called the **multiplicity** of M.

Proof. Since $H_M(t) = \frac{q_M(t)}{(1-t)^d}$, write $q_M(t) = \sum a_k t^k$. Then for $n \gg 0$, the coefficient of t^n is a linear combination of terms $\binom{n-k+d-1}{d-1}$. Since $\binom{n}{k}$ is a polynomial in n of degree k, the linear combination is a polynomial of degree $d-1$. The leading coefficient corresponds to the value $q_M(1)$. □

Proposition 9.4.2: Multiplicity Additivity

Let I be a homogeneous ideal. Let $I = \bigcap_{i=1}^{s} J_i$ be an irredundant primary decomposition. Assume $\dim(R/I) = d$. Let $\{J_1, \ldots, J_k\}$ be the primary components such that $\dim(R/J_i) = d$ (the components of top dimension). Then:

$$e_{d-1}(R/I) = \sum_{i=1}^{k} e_{d-1}(R/J_i)$$

Proof. This follows from the additivity of Hilbert series on short exact sequences. Consider the exact sequence:

$$0 \to R/(J_1 \cap \cdots \cap J_s) \to \bigoplus R/J_i \to \ldots$$

Specifically, use induction on the number of components. For two ideals A, B:

$$0 \to R/(A \cap B) \to R/A \oplus R/B \to R/(A+B) \to 0$$

If $\dim(R/(A+B)) < d$, then $e_{d-1}(R/(A+B)) = 0$. Thus $e_{d-1}(R/(A \cap B)) = e_{d-1}(R/A) +$

$e_{d-1}(R/B)$. Applying this to the primary decomposition, terms with lower dimension do not contribute to the multiplicity e_{d-1}. □

9.5 Proj S

Definition 9.5.1: The Proj Construction

Let $S = k[x_0, \dots, x_n]$ be graded. Let $S_+ = \bigoplus_{d \geq 1} S_d = (x_0, \dots, x_n)$ be the irrelevant ideal.

$$\operatorname{Proj} S := \{\mathfrak{p} \in \operatorname{Spec} S \mid \mathfrak{p} \text{ is homogeneous and } S_+ \not\subseteq \mathfrak{p}\}$$

Topology

We define the Zariski topology on $\operatorname{Proj} S$. The closed sets are of the form:

$$V(I) = \{\mathfrak{p} \in \operatorname{Proj} S \mid I \subseteq \mathfrak{p}\}$$

where I is a homogeneous ideal.

Basic Open Sets: For a homogeneous element $f \in S_+$, define:

$$U_f = D_+(f) = \{\mathfrak{p} \in \operatorname{Proj} S \mid f \notin \mathfrak{p}\}$$

These form a basis for the topology.

Proposition 9.5.1: Structure of Basic Open Sets

There is a homeomorphism (and isomorphism of schemes):

$$D_+(f) \cong \operatorname{Spec}(S_{(f)})$$

where $S_{(f)}$ is the degree 0 part of the localization S_f.

$$S_{(f)} = \{\frac{g}{f^k} \mid g \in S \text{ homogeneous}, \deg(g) = k \cdot \deg(f)\}$$

Example 9.5.1: Projective Space$\operatorname{Proj} k[x_0, \dots, x_n] = \mathbb{P}^n_k$. If k is algebraically closed, the closed points correspond to 1-dimensional homogeneous subspaces of k^{n+1} (lines through the origin). Maximal ideals in $S_{(x_i)}$ correspond to points. Example: A point in $\mathbb{P}^n$ is given by homogeneous coordinates $[a_0 : \dots : a_n]$.

Proposition 9.5.2: Dimension of V(I)

1. $V(I) = \emptyset \iff \sqrt{I} \supseteq S_+$.

2. $\dim V(I) = \dim(S/I) - 1$.

Note: The -1 comes from the fact that we exclude the vertex (the irrelevant ideal) which corresponds to the origin in affine space.

Multiplicity and Geometry

Definition 9.5.2: Degree of a Projective Variety

Let $X = V(I) \subset \mathbb{P}^n$ be a projective variety of dimension δ. The **degree** of X is defined as the number of points in the intersection of X with a generic linear subspace of codimension δ.

Theorem 9.5.1: Degree and Multiplicity

Let $M = S/I$. The degree of $V(I)$ is equal to the multiplicity $e_{d-1}(M)$ (where $d = \dim M = \delta + 1$).

$$\deg V(I) = e_{d-1}(S/I)$$

Recall $P_{S/I}(t) = \frac{\deg V(I)}{\delta!} t^\delta + \dots$ (for large t).

Example 9.5.2: Intersection in $\mathbb{P}^2$Two lines L_1, L_2 in $\mathbb{P}^2$ (proj plane). If $L_1 \neq L_2$, they meet at exactly one point. This corresponds to Bezout's Theorem. $\deg(L_1) = 1, \deg(L_2) = 1$. Total intersection multiplicity is $1 \times 1 = 1$.

9.6 Homogenization

Definition 9.6.1: Homogenization

Let $f \in R = k[x_1, \dots, x_n]$ be a polynomial of degree d. The homogenization of f in $S = k[x_1, \dots, x_n, Y]$ is:

$$\tilde{f} = Y^d \cdot f(x_1/Y, \dots, x_n/Y)$$

Essentially, multiply each term of degree e in f by Y^{d-e} to bring total degree to d.

Definition 9.6.2: Dehomogenization

Let $F \in S$ be homogeneous. The dehomogenization with respect to Y is:

$$f = F(x_1, \dots, x_n, 1)$$

Remark 9.6.1: Ideals If $I \subset R$ is an ideal, its homogenization $I^h \subset S$ is generated by $\{\tilde{f} \mid f \in I\}$. **Warning:** It is NOT generally true that if $I = (f_1, \dots, f_m)$, then $I^h = (\tilde{f}_1, \dots, \tilde{f}_m)$. One needs a Gröbner basis to generate the homogenized ideal properly.

Lemma 9.6.1: Correspondence

Let $\phi : S \to R$ be the evaluation map $Y \mapsto 1$. There is a bijection between prime ideals in R and homogeneous prime ideals in S not containing Y.

$$\mathfrak{p} \subset R \longleftrightarrow \mathfrak{p}^h \subset S$$

$$P \subset S \text{ (homog, } Y \notin P) \longleftrightarrow P^{dehom} \subset R$$

CHAPTER 10

SYZYGIES AND FREE RESOLUTIONS

10.1 Introduction to Syzygies

Preliminaries

Let $R = k[X_1, \dots, X_n]$ be a polynomial ring over a field k. We consider R as a graded ring where $\deg(X_i) = 1$. Let $I \subseteq R$ be a homogeneous ideal.

Definition 10.1.1: Quotient Dimensions

Let $>$ be a monomial order. Then:

$$H_{R/I}(t) = H_{R/\mathrm{in}(I)}(t)$$

In particular:

1. $\dim(R/I) = \dim(R/\mathrm{in}(I))$
2. $\mathrm{multiplicity}(R/I) = \mathrm{multiplicity}(R/\mathrm{in}(I))$

Theorem 10.1.1: Macaulay's Basis Theorem

The set of monomials not in $\mathrm{in}(I)$ (often denoted as the standard monomials) gives a k-basis for R/I and for $R/\mathrm{in}(I)$.

This respects the decomposition of the ring. Specifically,

$$R/I \cong \bigoplus_{d \geq 0} (R/I)_d$$

and

$$\dim_k(R/I)_d = \dim_k(R/\mathrm{in}(I))_d$$

Syzygies of Polynomials

Consider generators $f_1, \dots, f_m \in R$ which are homogeneous elements.

Definition 10.1.2: Syzygy

A **syzygy** of the sequence $(f_1, \dots, f_m)$ is an R-linear relation:

$$\sum_{i=1}^{m} r_i f_i = 0$$

where $r_i \in R$.

Example 10.1.1: Simple Syzygy Let $R = k[X, Y]$. Consider elements X, Y. They have a trivial syzygy (Koszul syzygy):

$$Y \cdot (X) - X \cdot (Y) = 0$$

Here $r_1 = Y$ and $r_2 = -X$.

To formalize this, let $d_i = \deg(f_i)$. We construct a map from a free module to R:

$$\bigoplus_{i=1}^{m} R(-d_i) \xrightarrow{\phi} R$$

where the basis element e_i of the free module maps to $f_i \in R$.

$$e_i \mapsto f_i$$

Note that e_i is a basis element of degree d_i, so the map preserves degrees. The kernel of this map, $\ker(\phi)$, is exactly the module of syzygies.

$$\sum r_i e_i \in \ker(\phi) \iff \sum r_i f_i = 0$$

10.2 Free Resolutions

Constructing Resolutions

Recall that for an ideal $I = \langle f_1, \dots, f_m \rangle \subseteq R$, the R-linear relations among the generating set (syzygies) can be determined by looking at the kernel of a surjective R-linear map.

Let $F_0 = \bigoplus R(-d_i)$. We have a map:

$$F_0 \xrightarrow{\epsilon} I \to 0$$

sending $e_i \mapsto f_i$. Let $M_1 = \ker(\epsilon)$. M_1 is the first syzygy module of I. Since R is Noetherian, M_1 is finitely generated. We can choose generators for M_1 and map a free module F_1 onto it.

$$\begin{tikzcd}
 & F_1 \arrow[d, "\partial_2"] & & \\
M_1 \arrow[r, hook] & F_0 \arrow[r, "\epsilon"] & I \arrow[r] & 0
\end{tikzcd}$$

This process can be iterated.

$$F_2 \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0 \to M \to 0$$

where $\operatorname{Im}(\partial_{i+1}) = \ker(\partial_i)$.

Complexes and Exact Sequences

Definition 10.2.1: Complex

A **chain complex** of R-modules $(C_\bullet, \partial_\bullet)$ is a sequence of R-modules and R-linear maps:

$$\dots \xrightarrow{\partial_{i+1}} C_i \xrightarrow{\partial_i} C_{i-1} \xrightarrow{\partial_{i-1}} \dots$$

satisfying $\partial_i \circ \partial_{i+1} = 0$ for all i.

The condition $\partial \circ \partial = 0$ implies $\operatorname{Im}(\partial_{i+1}) \subseteq \ker(\partial_i)$.

Definition 10.2.2: Homology

The i-th **homology** of a complex $C_\bullet$ is defined as:

$$H_i(C_\bullet) := \frac{\ker(\partial_i)}{\operatorname{Im}(\partial_{i+1})}$$

A complex is **exact** at i if $H_i(C_\bullet) = 0$.

Definition 10.2.3: Free Resolution

A **free resolution** of an R-module M is a complex $F_\bullet$:

$$\dots \to F_2 \to F_1 \to F_0 \to 0$$

such that:

1. Each F_i is a free R-module.

2. The complex is exact everywhere except at F_0, where $H_0(F_\bullet) \cong M$.

Minimal Graded Free Resolutions

Let $R = k[x_1, \dots, x_n]$ be graded with $\deg(x_i) = 1$. Let $\mathfrak{m} = \langle x_1, \dots, x_n \rangle$ be the irrelevant maximal ideal.

Lemma 10.2.1: Minimality Condition

Let $F_\bullet$ be a graded free resolution of a finitely generated graded R-module M. The following are equivalent:

1. $\operatorname{rank}(F_0) = \mu(M)$, the size of a minimal generating set of M.
2. $\partial_i(F_i) \subseteq \mathfrak{m}F_{i-1}$ for all $i \geq 1$.
3. If we represent the maps ∂_i as matrices, all entries are in $\mathfrak{m}$ (i.e., no non-zero constant entries).

Sketch. Consider $F_0 \xrightarrow{\epsilon} M \to 0$. Tensor with $R/\mathfrak{m} \cong k$. Since ϵ is a minimal cover, the induced map $F_0/\mathfrak{m}F_0 \to M/\mathfrak{m}M$ is an isomorphism. This implies $\ker(\epsilon) \subseteq \mathfrak{m}F_0$. □

Theorem 10.2.1: Hilbert Syzygy Theorem

Let $R = k[x_1, \ldots, x_n]$. Every finitely generated graded R-module M has a minimal graded free resolution of length $\leq n$.

Definition 10.2.4: Graded Betti Numbers

The graded Betti numbers $\beta_{i,j}(M)$ are defined as the number of basis elements of degree j in the free module F_i in a minimal free resolution of M.

$$F_i = \bigoplus_j R(-j)^{\beta_{i,j}}$$

Remark 10.2.1: Uniqueness The graded Betti numbers do not depend on the choice of the minimal free resolution. Minimal free resolutions are unique up to isomorphism.

10.3 Computing Syzygies and Gröbner Bases

Gröbner Bases for Modules

We generalize the concept of Gröbner bases from ideals to submodules of a free module. Let $F = \bigoplus_{i=1}^r Re_i$.

Definition 10.3.1: Monomial in Free Module

A **monomial** in F is an element of the form $m \cdot e_i$ where m is a monomial in R and e_i is a standard basis vector of F.

A **monomial submodule** $M \subseteq F$ is a submodule generated by monomials.

$$M = \bigoplus_{i=1}^r I_i e_i$$

where I_i are monomial ideals in R.

We can define a monomial order $>$ on F analogous to R. It must be a total order on monomials me_i respecting multiplication by monomials of R (i.e., if $u > v$, then $mu > mv$).

Computing Syzygies via Gröbner Bases

(Reference: Eisenbud, Commutative Algebra / Cox, Little, O'Shea)

Let $G = \{g_1, \ldots, g_t\} \subseteq F$. For $i \neq j$, define the S-pair notion for modules. Let $m_{ij} = \frac{\operatorname{lcm}(\operatorname{in}(g_i), \operatorname{in}(g_j))}{\operatorname{in}(g_i)}$. The standard reduction relation is:

$$S(g_i, g_j) = m_{ij} g_i - m_{ji} g_j$$

Theorem 10.3.1: Buchberger's Criterion for Modules

A set $G = \{g_1, \ldots, g_t\}$ is a Gröbner basis for the submodule generated by G if and only if for all pairs $i \neq j$, the S-pair $S(g_i, g_j)$ reduces to zero modulo G.

Specifically, if $S(g_i, g_j) = \sum h_k g_k$ (standard representation), then:

$$m_{ij} g_i - m_{ji} g_j - \sum h_k g_k = 0$$

This equation gives a syzygy among the g's.

Key Point: The syzygies produced by the S-pair reductions of a Gröbner basis generate the entire syzygy module of $\operatorname{in}(M)$.

Proof Strategy for Hilbert Syzygy Theorem

1. Reduce to monomial submodules (using Gröbner deformations, since $\beta_{i,j}(M) \leq \beta_{i,j}(\operatorname{in}(M))$). 2. Reduce to monomial ideals. 3. Use the **Horseshoe Lemma** and induction.

Lemma 10.3.1: Horseshoe Lemma

Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence of modules. If $P'_\bullet$ is a resolution of M' and $P''_\bullet$ is a resolution of M'', then there exists a resolution $P_\bullet$ of M such that $P_i \cong P'_i \oplus P''_i$.

For a monomial ideal I, if it is not prime (i.e., not generated by a subset of variables), choose a variable x_i dividing a generator. We have an exact sequence:

$$0 \to \frac{R}{I : x_i}(-1) \xrightarrow{\cdot x_i} \frac{R}{I} \to \frac{R}{I + \langle x_i \rangle} \to 0$$

By induction on the number of variables and degree, we can prove the bound on the resolution length.

10.4 Mapping Cones

Maps of Complexes

Let $(F_\bullet, d_\bullet)$ and $(G_\bullet, \delta_\bullet)$ be complexes. A map of complexes $\phi : F_\bullet \to G_\bullet$ is a family of maps $\phi_i : F_i \to G_i$ such that the diagram commutes:

$$\delta_i \circ \phi_i = \phi_{i-1} \circ d_i$$

The Mapping Cone

Given a map $\phi : F_\bullet \to G_\bullet$, we construct a new complex called the **Mapping Cone**, denoted $C(\phi)_\bullet$ or simply $C_\bullet$.

Definition 10.4.1: Mapping Cone Construction

Let $C_i = G_i \oplus F_{i-1}$. The differential $\Delta_i : C_i \to C_{i-1}$ is defined by the matrix:

$$\Delta_i = \begin{bmatrix} \delta_i & \phi_{i-1} \\ 0 & -d_{i-1} \end{bmatrix}$$

Acting on a vector $\begin{pmatrix} g \\ f \end{pmatrix} \in G_i \oplus F_{i-1}$, we get:

$$\Delta_i(g, f) = (\delta_i(g) + \phi_{i-1}(f), -d_{i-1}(f))$$

We must check $\Delta^2 = 0$:

$$\begin{bmatrix} \delta & \phi \\ 0 & -d \end{bmatrix} \begin{bmatrix} \delta & \phi \\ 0 & -d \end{bmatrix} = \begin{bmatrix} \delta^2 & \delta\phi - \phi d \\ 0 & d^2 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

(Note: indices omitted for brevity, but they match due to the commutativity $\delta\phi = \phi d$).

Short Exact Sequence of Complexes

There is a short exact sequence of complexes:

$$0 \to G_\bullet \to C(\phi)_\bullet \to F_\bullet[-1] \to 0$$

where $F_\bullet[-1]$ is the shifted complex (homological degree shifted by -1).

This induces a long exact sequence in homology:

$$\cdots \to H_i(G) \to H_i(C(\phi)) \to H_{i-1}(F) \xrightarrow{\partial} H_{i-1}(G) \to \dots$$

The connecting homomorphism ∂ is exactly the map induced by ϕ.

10.5 Koszul Complexes

Construction

Let R be a ring. For a single element $f_1 \in R$, the Koszul complex $K(f_1)$ is:

$$0 \to R \xrightarrow{f_1} R \to 0$$

concentrated in homological degrees 1 and 0.

For a sequence $f_1, \ldots, f_r$, the Koszul complex is defined inductively using the mapping cone. Let $K(f_1, \ldots, f_{r-1})$ be denoted by $K_\bullet$. We define:

$$K(f_1, \ldots, f_r) := C(K_\bullet \xrightarrow{f_r} K_\bullet)$$

Specifically, multiplication by f_r induces a map of complexes $K_\bullet \to K_\bullet$. The cone of this map is the Koszul complex for the sequence with f_r added.

Regular Sequences and Homology

Let M be a graded module. $K(f_1, \ldots, f_r; M) \cong K(f_1, \ldots, f_r) \otimes M$.

Definition 10.5.1: Regular Sequence

A sequence $f_1, \ldots, f_r \in \mathfrak{m}$ is a **regular sequence** on M if:

1. f_1 is a non-zero divisor (NZD) on M.
2. f_i is a NZD on $M/\langle f_1, \ldots, f_{i-1}\rangle M$ for $i = 2, \ldots, r$.
3. $M/\langle f_1, \ldots, f_r\rangle M \neq 0$.

Proposition 10.5.1: Koszul Homology and Regular Sequences

Let $f_1, \ldots, f_r$ be homogeneous elements of positive degree. The following are equivalent:

1. $f_1, \ldots, f_r$ is a regular sequence on M.
2. $H_i(K(f_1, \ldots, f_r; M)) = 0$ for all $i \neq 0$.

Remark 10.5.1: Homology at 0$H_0(K(f_1, \ldots, f_r; M)) \cong M/\langle f_1, \ldots, f_r\rangle M$.

Corollary 10.5.1: Minimal Resolution If $f_1, \dots, f_r$ is a regular sequence in R, then the Koszul complex $K(f_1, \dots, f_r)$ is a minimal graded free resolution of $R/\langle f_1, \dots, f_r \rangle$.

Example 10.5.1: Complete Intersection Let $R = k[X, Y, Z]$ and $I = \langle X, Y, Z \rangle$. The Koszul complex $K(X, Y, Z)$ resolves $k \cong R/I$:

$$0 \to R(-3) \to R(-2)^{\oplus 3} \to R(-1)^{\oplus 3} \to R \to k \to 0$$

Projective Dimension

The **projective dimension** of M, $\operatorname{pd}(M)$, is the length of the shortest free resolution of M. In terms of Betti numbers:

$$\operatorname{pd}(M) = \sup\{i \mid \beta_{i,j}(M) \neq 0 \text{ for some } j\}$$

10.6 Castelnuovo-Mumford Regularity

Definition

Let M be a finitely generated graded R-module with a minimal graded free resolution $F_\bullet$.

Definition 10.6.1: Castelnuovo-Mumford Regularity

The **regularity** of M is defined as:

$$\operatorname{reg}(M) := \max\{j - i \mid \beta_{i,j}(M) \neq 0\}$$

This invariant measures the "complexity" of the module. If M is generated in degree 0, the regularity roughly bounds how high the degrees of the generators of the syzygies can get relative to the homological step.

Relation to Hilbert Function

From the exact sequence of the resolution $0 \to F_n \to \cdots \to F_0 \to M \to 0$, we can compute the Hilbert Series. Since $F_i = \bigoplus_j R(-j)^{\beta_{i,j}}$, and $H_R(t) = \frac{1}{(1-t)^n}$, we have:

$$H_M(t) = \frac{\sum_{i=0}^{n} (-1)^i \sum_j \beta_{i,j} t^j}{(1-t)^n} = \frac{K(t)}{(1-t)^n}$$

where $K(t)$ is the K-polynomial.

Proposition 10.6.1: Hilbert Polynomial

For $d \geq \operatorname{reg}(M) + 1$ (note: precise bound may vary by convention, notes suggest $d > \operatorname{reg} M$), the Hilbert Function $H_M(d) = \dim_k M_d$ agrees with the Hilbert Polynomial $P_M(d)$.

Idea. The Hilbert function of M is an alternating sum of the Hilbert functions of the free modules F_i. The Hilbert function of $R(-j)$ is polynomial for $d \geq j - n$. The regularity condition ensures that for large enough d, we fall into the polynomial range for all twists appearing in the resolution. □

10.7 Points in Projective Space

Interpolation Problem

Let k be algebraically closed. Let $X \subseteq \mathbb{P}^n_k$ be a finite set of points, $|X| = m$. A point $p \in \mathbb{P}^n$ is given by coordinates $[a_0 : \cdots : a_n]$. X is defined by an ideal I_X.

Question: When does X impose independent conditions on forms of degree d?

Consider the evaluation map (or restriction map):

$$\rho_d : R_d \to k^{|X|}$$

given by $f \mapsto (f(p))_{p \in X}$. (Note: Since values are not well-defined on projective space, this usually means choosing representatives or looking at the vanishing condition).

More precisely, X imposes independent conditions if this map is surjective. The failure of surjectivity is measured by H^1 of the ideal sheaf, or combinatorially by the Hilbert function.

If the map is surjective, then $H_X(d) = |X| = m$. In general, $H_X(d) = \dim_k(R/I_X)_d$. For large d, this equals the constant polynomial m.

REFERENCES

[1] David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer, 4 edition, 2015.

[2] David Eisenbud. *Commutative Algebra: With a View Toward Algebraic Geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer, 1995.