Commutative Algebra

LICENSE, DISCLAIMER OF LIABILITY, AND LIMITED WARRANTY

By purchasing or using this book (the "Work"), you agree that this license grants permission to use the contents contained herein, but does not give you the right of ownership to any of the textual content in the book or ownership to any of the information or products contained in it. *This license does not permit uploading of the Work onto the Internet or on a network (of any kind) without the written consent of the Publisher.* Duplication or dissemination of any text, code, simulations, images, etc. contained herein is limited to and subject to licensing terms for the respective products, and permission must be obtained from the Publisher or the owner of the content, etc., in order to reproduce or network any portion of the textual material (in any media) that is contained in the Work.

Mercury Learning And Information ("MLI" or "the Publisher") and anyone involved in the creation, writing, or production of the companion disc, accompanying algorithms, code, or computer programs ("the software"), and any accompanying Web site or software of the Work, cannot and do not warrant the performance or results that might be obtained by using the contents of the Work. The author, developers, and the Publisher have used their best efforts to insure the accuracy and functionality of the textual material and/or programs contained in this package; we, however, make no warranty of any kind, express or implied, regarding the performance of these contents or programs. The Work is sold "as is" without warranty (except for defective materials used in manufacturing the book or due to faulty workmanship).

The author, developers, and the publisher of any accompanying content, and anyone involved in the composition, production, and manufacturing of this work will not be liable for damages of any kind arising out of the use of (or the inability to use) the algorithms, source code, computer programs, or textual material contained in this publication. This includes, but is not limited to, loss of revenue or profit, or other incidental, physical, or consequential damages arising out of the use of this Work.

The sole remedy in the event of a claim of any kind is expressly limited to replacement of the book, and only at the discretion of the Publisher. The use of "implied warranty" and certain "exclusions" vary from state to state, and might not apply to the purchaser of this product.

Commutative Algebra
An Introduction

J. William Hoffman
(Louisiana State University)

Xiaohong Jia
(Chinese Academy of Sciences)

Haohao Wang
(Southeast Missouri State University)

Mercury Learning and Information
Dulles, Virginia
Boston, Massachusetts
New Delhi

Publisher: David Pallai
Mercury Learning And Information
22841 Quicksilver Drive
Dulles, VA 20166
info@merclearning.com
www.merclearning.com
(800) 232-0223

J. W. Hoffman, X. Jia, H. Wang. *Commutative Algebra. An Introduction.*
ISBN: 978-1-944534-60-8

Cover image: "Kummer Surface" by Paul Aspinwall/Duke University.
Used with permission.

Library of Congress Control Number: 2016935954

161718321 This book is printed on acid-free paper.

Our titles are available for adoption, license, or bulk purchase by institutions, corporations, etc.

For additional information, please contact the Customer Service Dept. at 800-232-0223(toll free).

All of our titles are available in digital format at authorcloudware.com and other digital vendors. The sole obligation of Mercury Learning And Information to the purchaser is to replace the book, based on defective materials or faulty workmanship, but not based on the operation or functionality of the product.

CONTENTS

PREFACE

The purpose of this book is twofold: to present some basic ideas in commutative algebra and algebraic geometry and to introduce some interesting topics of current research centered around the themes of Gröbner bases, resultants and syzygies. There are many good introductory texts on commutative algebra and algebraic geometry, and the intention of this book is to be a supplement to those texts with the aim of pointing the reader toward possible future research directions. The presentation of the material combines definitions and proofs with an emphasis on concrete examples. We also illustrate the use of software such as Mathematica and Singular.

The design of the text in each chapter consists of two parts: the fundamentals and the applications, which make it suitable for courses of various lengths, levels, and topics based on the mathematical background of the students. The fundamentals portion of the chapter is intended for an average graduate student to read with minimal outside assistance, and to learn some of the most useful tools in commutative algebra. The applications of the chapter are to provide a glimpse of the advanced mathematical research where the topics and results are related to the material presented in the fundamentals. In the applications, we allow ourselves to present a number of results from a wide range of sources without detailed proofs. The applications portion of the chapter is suitable for a reader who knows a little commutative algebra and algebraic geometry already, and serves as a guide to some interesting research topics.

The prerequisite for this book is a standard first year graduate course in abstract algebra. In Chapter 2 and Chapter 3 we start with a quick review of the fundamental concepts of rings and modules. Via the notion of localization, we make contact with sheaf theory. We do not develop sheaf theory

systematically in this book, but we use these ideas, especially on the interesting topics. Therefore, a brief explanation is given concerning the relation between rings and modules on the one hand, and affine schemes and quasi-coherent sheaves on the other.

Since the idea of graded rings and modules is necessary to do projective geometry, it is essential to understand the algebra, and therefore, in Chapter 4, we extend some concepts such as dimensions, lengths, and free resolutions to the graded rings and modules. The connection between graded modules and sheaves on projective space is briefly recalled. In mathematics, a syzygy is a relation between the generators of a module. Hilbert's syzygy theorem is a keystone result. Among the applications in Chapter 4, we present the results of several recent research papers which utilize syzygy techniques in the study of curves and surfaces.

In the study of algebra and geometry, homological algebra is a common thread which ties many things together. For example, we use homological techniques in commutative algebra by studying the notion of depth by means of Ext. This leads to the Buchsbaum-Eisenbud criterion of exactness of finite free complexes. Many computational techniques, such as finding the implicit equations or the defining equations of Rees algebra of certain ideals, involve homological algebra. Hence, in Chapter 5, we include the construction of the functors of importance in the homological aspects of commutative ring theory. As applications, we discuss the topics such as regularity, determinants, and approximation complexes.

As mentioned earlier, we have attempted to keep the necessary prerequisites for this book to a minimum. It is important for a reader to be familiar with the conceptual background. The fundamentals in each of the chapters can be used as a quick introduction or refresher course on commutative algebra and algebraic geometry. However, many readers might want to have a look at some of the applications.

This book should be thought of as an introduction to more advanced texts and research topics. The novelty of this book, we hope, is that the material presented here is a unique combination of the essential methods and the current research results. Our goal is to equip our students with the fundamental classical algebra and geometry tools, ignite their research interests, and initiate some potential research projects in the related areas.

LIST OF FIGURES

1. Introduction

One of the interesting problems concerning rational curves and surfaces is the implicitization problem. To understand the motivation of implicitization, we start with a simple example. The curve in Figure 1.1 is given by the following parametric equations with parameter t:

$$\begin{aligned} x &= t^2 - 1, \\ y &= t(t^2 - 1). \end{aligned}$$

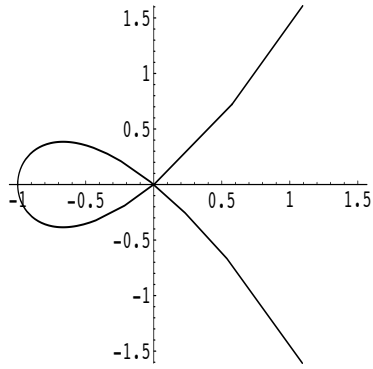


Figure 1.1: Curve

The implicitization problem is to convert the parametrization into a defining equation for the curve, which we find is:

$$y^2 - x^2 - x^3 = 0.$$

Parametric surfaces are widely used in computer aided design projects since it is easy to describe the points of the surface by means of the parameter values.

Given the parametric equations of a surface, the computer can evaluate at different parameter values, and then plot the points of the surface. But it is hard to determine whether a point is on the surface given by the parametric representation. For example the graph in Figure 1.2 is plotted by using the parametric representation:

$$\begin{aligned} x &= t(u^2 - t^2), \\ y &= u, \\ z &= u^2 - t^2 \end{aligned}$$

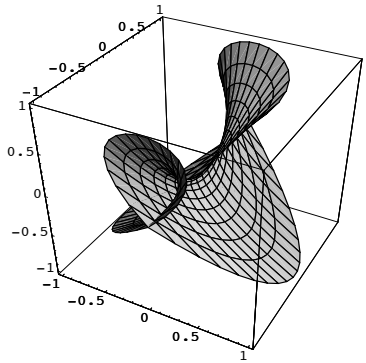


Figure 1.2: Surface

To answer the following question, it is useful to have an implicit representation of a variety.

Question: *Is the point* (x_0, y_0, z_0) *on the above surface?*

Answer:

To answer this question from the knowledge of the parametric equations, we need to solve the equations

$$\begin{aligned} x_0 &= t(u^2 - t^2), \\ y_0 &= u, \\ z_0 &= u^2 - t^2, \end{aligned}$$

for t, u, if possible.

Trying to solve these equations leads to

$$x_0^2 - y_0^2 z_0^2 + z_0^3 = 0,$$

as a criterion for the solvability of the parametric equations. The implicit equation $x^2 - y^2z^2 + z^3 = 0$ gives the Zariski closure of the image of the parametrization, which is an easily checked criterion for deciding if a point (x_0, y_0, z_0) is on the parametrized surface. For example, $(1, 2, -1)$ is not on the surface since

$$1^2 - 2^2(-1)^2 + (-1)^3 = 1 - 4 - 1 = -1 \neq 0,$$

while $(10, 3, 5)$ is on the surface since

$$10^2 - 3^2 5^2 + 5^3 = 0.$$

To describe the set of points which are common to two different parametrically represented surfaces is a difficult problem using the parametric descriptions. If the surfaces are described by implicit equations, then to find the set of common points of two surfaces reduces to the problem of finding the common solutions of two explicitly given polynomial equations. This is a problem which can be handled relatively easily. For example, let's consider the following question:

Question: *What is the intersection of the parametric surfaces S_1 and S_2?*

The surfaces S_1 and S_2 (see Figure 1.3) are given by the following parametric representations:

$$S_1: \begin{cases} x &= \frac{1-u^2}{1+u^2}, \\ y &= \frac{2u}{1+u^2}, \\ z &= v; \end{cases} \qquad S_2: \begin{cases} x &= uv, \\ y &= v, \\ z &= u^2. \end{cases}$$

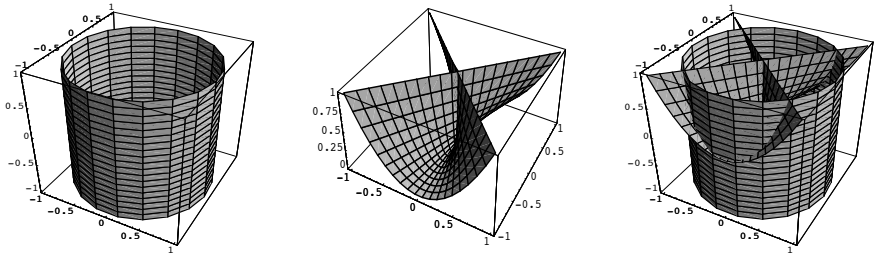


Figure 1.3: S_1 (Left), S_2 (Middle), $S_1 \cap S_2$ (Right)

It is not easy to describe the intersection of surfaces S_1 and S_2 (see Figure 1.3) if the surfaces are represented parametrically. In general, the

intersection of two surfaces might consist of several curves and these might be curves of genus greater than 0, in which case no rational parametrization of $S_1 \cap S_2$ is possible. If we use implicit equations to describe the surfaces, then finding intersection is just to find the solutions of the two polynomial equations:

$$\begin{aligned} x^2 + y^2 &= 1, \\ y^2 z - x^2 &= 0. \end{aligned}$$

The solution set is:

$$\left\{ \left(\pm\sqrt{1-y^2},\, y,\, \frac{1-y^2}{y^2} \right) \,:\, 0 < |y| \leq 1 \right\}.$$

Thus, there is a need for being able to go back and forth between a parametric and an implicit description of a surface. This is, in essence, the *implicitization problem* - describe algorithms to produce an implicit equation of a surface for which one knows a parametric description.

For any parametrization, we can find the implicit equation via elimination of the parameters. In practice, there are four major methods used: resultants, Gröbner bases, syzygies, and approximation complexes.

Resultant computations are based on the methods developed by Macaulay [Mac23], Cayley [Cay65], Bézout, Dixon [Dix08]. The resultant can tell us whether two polynomials have a common factor. To find an implicit equation via resultants is to eliminate a subset of variables from a set of polynomials.

For example, we can rewrite the parametric equations of Figure 1.1 as the following equations:

$$\begin{aligned} t^2 - (1+x) &= 0, \\ t^3 - t - y &= 0. \end{aligned}$$

Then the *Sylvester resultant* of the above equation with respect to t can be written as a determinant of 5×5 matrix N,

$$N = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ -(1+x) & 0 & 1 & -1 & 0 \\ 0 & -(1+x) & 0 & -y & -1 \\ 0 & 0 & -(1+x) & 0 & -y \end{bmatrix}$$

and the implicit equation for the curve is $|N| = -x^2 - x^3 + y^2 = 0$.

It is not an easy task to compute the implicit equations via resultants. It often involves an extraneous factor and requires a polynomial division to eliminate the extraneous factor.

It is known that the resultants can eliminate several variables simultaneously, and reduce system solving over the complex numbers to univariate polynomial factorization. One of the research directions is to seek the smallest possible resultant matrix such that its determinant is precisely equal to the resultant. Many people have attempted to construct the smallest possible determinantal formula for multi-homogeneous resultants, ranging from the classical matrices, namely Sylvester's and Bézout's, to the hybrid type of these two.

Gröbner bases were proposed by Buchberger [Buc85] for efficient computation in polynomial rings. Many problems about ideals in polynomial rings can be solved by Gröbner bases. Gröbner bases can be used to find solutions to a set of polynomials, compute projections of their variety into lower dimensional spaces, and test polynomials for ideal membership. With Gröbner bases, we can compute the equations satisfied by given elements of an affine or homogeneous coordinate ring. Geometrically, this is the computation of the closure of the image of an affine or projective variety under a morphism. This method requires an ordering of the monomials in the polynomial ring. The algorithm gives a basis of the ideal generated by the parametric equations. This method will produce the implicit equation without any extraneous factor [BW93]. Let's use the example of the equations of Figure 1.1 again. We will take the lex order in the ring $\mathbb{K}[x, y, t]$ by the variable ordering $t > x > y$, where $\mathbb{K}$ is an algebraically closed field. Using Mathematica, we find the Gröbner basis of the ideal

$$\tilde{I} = \langle x - (t^2 - 1), y - t(t^2 - 1) \rangle$$

is:

$$\{x^2 + x^3 - y^2, -x - x^2 + ty, tx - y, 1 - t^2 + x\}$$

The implicit equation is:

$$y^2 - x^2 - x^3 = 0.$$

The first polynomial in the Gröbner basis eliminates the variable t, since t is the largest in the monomial order. This polynomial is the implicit equation of our curve.

Recently, applications of Gröbner bases for ideals for various fields have been studied. In commutative algebra, there many problems can be solved by Gröbner bases approaches, for example

- solving algebraic systems of equations,
- ideal and radical membership decision,
- syzygy computations,
- Hilbert functions,
- implicitiziation problems.

However, in practice, Gröbner bases calculations in the elimination problems require more time and memory than resultant calculations (see [KS95] and [Stu98]). Resultants are still the preferred choice to compute the implicit equations.

Syzygy techniques are developed recent years as tools for finding implicit equations. The first introduction of syzygy-like techniques in the implicitization problem was the use of moving lines to produce implicit equations for curves by Sederberg and Chen [SC95]. The syzygy method uses determinants of smaller matrices than the classical methods to find the implicit equation of the parametrized curve. There are many open problems in the area of syzygies, for example:

- the Castelnuovo-Mumford regularity,
- characterization of Hilbert functions,
- extremal Betti numbers and lower bounds,
- free resolutions and Hilbert functions of points in $\mathbb{P}^n$.

The method of approximation complexes is motivated by the interest in computing explicit formulas for resultants and discriminants initiated by Bézout, Cayley and Sylvester, and is emphasized in the recent years due to the increase of computing power.

Approximation complexes were developed by Jürgen Herzog, Aron Simis and Wolmer V. Vasconcelos [HSV83b], [HSV82], and [HSV83a] in the beginning of the 80's to study the syzygies of the conormal modules.

In 2003, approximation complexes were first used in elimination theory by Laurent Busé and Jean-Pierre Jouanolou [BJ03] to provide an alternative method to compute the implicit equations of parametrized surfaces or curves.

The spirit behind the approximation complexes method consists of taking the determinant of a graded strand of a complex. This idea is similar to the one used for the computation of a Macaulay resultant of n homogeneous

polynomials in n variables, which is by taking the determinant of a graded branch of a Koszul complex.

Recently, based on computing the determinant of a multi-graded Koszul complex, Botbol [Bot11] showed that the classical study of Macaulay resultants and Koszul complexes coincides. Furthermore, he provided a geometric interpretation for the acyclicity condition of approximation complexes, and gave algebraic and geometric criteria for computing the implicit equations of rationally parametrized hypersurfaces in projective toric varieties.

This book is developed with the central focus being Gröbner bases, resultants, syzygies, and approximation complexes. In each chapter, we first provide the necessary background knowledge and useful tools in commutative algebra in order to start mathematical research in these areas, then we give a glimpse of the advanced mathematical topics originating in these themes. We hope this book will equip graduate students with background knowledge, ignite their research interests, and initiate some potential research projects in related domains.

2. Rings and Ideals

2.1 Rings and Ideals

This chapter, we start with the most basic definitions and fundamental properties of rings and ideals.

Definition 2.1.1. Unless stated to the contrary, a **ring** is a **commutative ring with identity**. A homomorphism φ of rings always preserves the identity: $\varphi(1) = 1$

Definition 2.1.2. A **field** is a commutative ring with identity $1 \neq 0$ that satisfies the condition:

$$\text{for each } a \neq 0 \text{ in } R, \text{ the equation } ax = 1 \text{ has a solution in } R.$$

Definition 2.1.3. An element a in a ring R with identity is called a **unit** if there exists $u \in R$ such that $au = 1 = ua$. In this case, the element u is called the **multiplicative inverse** of a and is denoted a^{-1}.

Example 2.1.4. Let $\mathbb{K}$ be a field and $\mathbb{K}[x] = \{f(x) = \sum_{k=0}^{n} a_k x^k \mid a_k \in \mathbb{K}\}$ be a polynomial ring in one variable x with coefficients in the field $\mathbb{K}$. The most important example is the field $\mathbb{K} = \mathbb{C}$ of complex numbers. It is easy to see that this is a commutative ring. For any $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{K}[x]$ where $a_n \neq 0$, the elements $a_i \in \mathbb{K}$ are called *coefficients* of the polynomial. If the polynomial contains no terms of the form $a_m x^m$ with $m > n$, then the non-negative n is called the *degree* of the polynomial (denoted by $\deg(f) = n$), a_n is called *leading coefficient* of the polynomial (denoted by $\mathrm{LC}(f) = a_n$), and $a_n x^n$ is called *leading term* of the polynomial (denoted by $\mathrm{LT}(f) = a_n x^n$).

The ring $\mathbb{K}[x]$ has the property that the product of two nonzero elements is always nonzero, and this type of rings is called an *integral domain*.

Definition 2.1.5. An **integral domain** is a commutative ring R with identity $1 \neq 0$ that satisfies the condition:

$$\text{whenever } a, b \in R, \text{ and } ab = 0, \text{ then } a = 0, \text{ or } b = 0.$$

Example 2.1.6. Any field is an integral domain. The ring $\mathbb{Z}$ of integers is an integral domain. If p is a prime, then $\mathbb{Z}/p$ is a field, hence an integral domain. But $\mathbb{Z}/6$ is not an integral domain since $2 \cdot 3 = 0$, even though $2 \neq 0$ and $3 \neq 0$.

Definition 2.1.7. An element a in a ring R is a **zero divisor** if

$$a \neq 0, \text{ and there exists } 0 \neq c \in R \text{ such that } ac = 0.$$

An element $r \in R$ is called **nilpotent** if $r^n = 0$ for some $n > 0$. A nilpotent element is a zero divisor.

Example 2.1.8. We can see that $2, 3$ in the ring $\mathbb{Z}/6$ are zero divisors.

Remark 2.1.9. An integral domain contains no zero divisors. A polynomial ring $\mathbb{K}[x_1, \ldots, x_n]$ does not contain any zero divisors, and it is an integral domain.

Example 2.1.10. We can check that the unit elements $\mathbb{Z}_6$ are $1, 5$, and $5 \cdot 5 \cong 1$, hence $5^{-1} = 5$.

Definition 2.1.11. A subset I of a ring R is an **ideal** provided

1. For all $a, b \in I$, $a - b \in I$;
2. For all $r \in R$ and $a \in I$, $ra \in I$.

Given a set of elements $a_j,\ j \in J$ of R, there is a smallest ideal containing these elements, denoted $\langle ..., a_j, ... \rangle$. This consists of all finite linear combinations

$$\sum_{j \in J} r_j a_j, \quad r_j \in R$$

where in the above expression, all but finitely many r_j are 0.

Let I be an ideal of the ring R, then the quotient group R/I is also a ring, it is the *quotient ring* R/I. The elements of R/I are the cosets of I in R, and the mapping $f : R \to R/I$ defined by $f(r) = r + I$ for all $r \in R$ is a surjective ring homomorphism. Let R and S be two rings, and $f : R \to S$ a ring homomorphism, then $\ker(f) = \{r \in R \mid f(r) = 0\}$, the *the kernel of* f, is an ideal of R; $\mathrm{im}(f) = f(R)$, the *image of* f, is a subring of S; and f induces a ring homomorphism $\mathrm{im}(f) \cong R/\ker(f)$.

Proposition 2.1.12. *Let R be a non-zero ring. The the following are equivalent:*

1. *R is a field;*
2. *The only ideals in R are $\langle 0\rangle$ and $\langle 1\rangle$;*
3. *Every homomorphism of R into a non-zero ring S is injective.*

Proof. In any ring R, an ideal $I = R$ if and only if I contains a unit of R.

$(1 \Rightarrow 2)$ Let $I \neq \langle 0\rangle$, then $\langle 1\rangle \subset I \subset \langle 1\rangle$, thus $I = \langle 1\rangle$.

$(2 \Rightarrow 3)$ Let $f : R \to S$ be a ring homomorphism, since $\ker(f)$ is an ideal in R, and $\ker(f) = 0$. Thus f is injective.

$(3 \Rightarrow 1)$ Let I be a non-zero ideal of R, and $f : R \to R/I$ is a surjective homomorphism, since it is also injective, thus $\ker(f) = I = \langle 0\rangle$. □

Definition 2.1.13. Let I_j for all $j \in J$ be a finite family of ideals in a ring R, the **sum** $\sum_{j\in J} I_j = \{\sum_{j\in J} a_j \mid a_j \in I_j\}$, is the smallest ideal of R which contains all I_j. If two ideals $I, J \subset R$, and $I + J = R$, then we say I, J are **coprime**. The **intersection** $\bigcap_{j\in J} I_j$ is an ideal. The **product** of any finite family of ideals $\Pi_{j\in J} I_j = \{\sum(\prod_{j\in J} a_j) \mid a_j \in I_j\}$. Conventionally, $I^0 = \langle 1\rangle$.

Remark 2.1.14. Clearly, $I, J \subset R$ are coprime if and only if there exist $a \in I$ and $b \in J$ such that $a + b = 1$. If I, J are coprime, then $I \cap J = IJ$, since

$$IJ \subseteq I \cap J = I \cap J(I + J) = (I \cap J)I + (I \cap J)J \subseteq JI + IJ \subseteq IJ.$$

Definition 2.1.15. An ideal $\mathfrak{p} \subset R$, $\mathfrak{p} \neq R$ is **prime** if either of the equivalent conditions holds:

1. For any $a, b \in R$, $ab \in \mathfrak{p}$ implies either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$,
2. $R/\mathfrak{p}$ is an integral domain.

An ideal $\mathfrak{m} \neq R$ is called **maximal** if either of the equivalent conditions holds:

1. Any ideal I such that $\mathfrak{m} \subset I \subset R$ must have either $\mathfrak{m} = I$ or $I = R$,
2. $R/\mathfrak{m}$ is a field.

Since a field is an integral domain, every maximal ideal is prime. We let $\mathrm{Spec}(R)$ be the set of prime ideals of R and $\mathrm{Max}(R) \subset \mathrm{Spec}(R)$ the subset of maximal ideals. In section 2.7 we will show how to put a topology on these sets as well as a sheaf of rings.

Theorem 2.1.16. *If I is a proper ideal in a non-zero ring R, then there exists at least one maximal ideal containing I.*

Proof. Let $\sum = \{$proper ideals in R that contain I $\}$, and order $\sum$ by inclusion. We check that $\sum$ satisfies the conditions of Zorn's lemma, hence $\sum$ has a maximal element. □

As consequences of this theorem, we see that every ideal $I \neq \langle 1 \rangle$ is contained in some maximal ideal of R, and every non-unit of the ring R is contained in a maximal ideal.

Definition 2.1.17. There is a special type of ring which has exactly one maximal ideal, namely, a **local ring**. For example a field is a local ring. If $(R, \mathfrak{m})$ is a local ring, then $\mathbb{K} = R/\mathfrak{m}$ is called the **residue field of** R. A ring with finitely many maximal ideals is called **semi-local ring**.

Definition 2.1.18. A subset S of a ring R is **multiplicative** or **multiplicatively closed** if

1. $x, y \in S$ implies that $xy \in S$;
2. $1 \in S$.

Theorem 2.1.19. *Let S be a multiplicatively closed set, and I an ideal disjoint from S, then there exists a prime ideal containing I and disjoint from S.*

Proof. By an argument similar to the proof of theorem 2.1.16, the set of ideals containing I and disjoint from S has a maximal element. If $\mathfrak{p}$ is such a maximal element, we will show it is a prime ideal. Let $ab \in \mathfrak{p}$, suppose if $a, b \notin \mathfrak{p}$, then $\mathfrak{p} + aR, \mathfrak{p} + bR$ meet S due to the maximality of $\mathfrak{p}$, hence the product $(\mathfrak{p}+aR)(\mathfrak{p}+bR) \subset \mathfrak{p}+abR$ must meet S, because S is multiplicatively closed. Thus we must have $ab \notin \mathfrak{p}$, contradicting the assumption. Therefore, either a or b is in $\mathfrak{p}$, and $\mathfrak{p}$ is a prime ideal. □

Proposition 2.1.20. *Let $I_1, \ldots, I_n \subset R$ be ideals, and a homomorphism $f : R \to \prod_{i=1}^{n}(R/I_i)$ defined by $f(r) = (r + I_1, \ldots, r + I_n)$, then*

1. *If I_i, I_j are coprime whenever $i \neq j$, then $\prod I_i = \bigcap I_i$;*
2. *f is surjective if and only if I_i and I_j are coprime whenever $i \neq j$; in particular, if $I_1, \ldots, I_n$ are coprime ideals in the ring R, then*

$$R/I_1 \cdots I_n = R/I_1 \times \cdots \times R/I_n.$$

3. f is injective if and only if $\bigcap I_i = \langle 0 \rangle$.

Proof. (1.) We will prove the first claim by induction on n. The case $n = 2$ is proved in Remark 2.1.14. Suppose $n > 2$ and the result holds for $n-1$, then we let $J = \prod_{i=1}^{n-1} I_i = \bigcap_{i=1}^{n-1} I_i$. Since $I_i + I_n = \langle 1 \rangle$ for all $i = 1, \ldots, n-1$, we have the equation $a_i + b_i = 1$ for some $a_i \in I_i$ and $b_i \in I_n$, and therefore, we have

$$\prod_{i=1}^{n-1} a_i = \prod_{i=1}^{n-1} (1 - b_i) \equiv 1 \ (\bmod I_n) \quad \Rightarrow \quad I_n + J = \langle 1 \rangle.$$

Therefore, the claim follows directly by the following

$$\bigcap_{i=1}^{n} I_i = I_n \cap (\bigcap_{i=1}^{n-1} I_i) = I_n \cap J = I_n J = I_n (\prod_{i=1}^{n-1} I_i) = \prod_{i=1}^{n} I_i.$$

(2.) Let $f : R \to \prod_{i=1}^{n} (R/I_i)$. Since f is surjective, there exists $a \in I_i$ such that $f(a) = (0, \ldots, 0, 1, 0, \ldots 0)$ where 1 is in the i-th position, thus $a \equiv 1 \pmod{I_i}$ and $a \equiv 0 \pmod{I_j}$ for all $j \neq i$). Hence, we have $1 = (1 - a) + a \in I_i + I_j$. Therefore I_i and I_j are coprime.

On the other hand, if I_i and I_j are coprime, then we have $a_i + b_j = 1$ for some $a_i \in I_i$ and $b_j \in I_j$. Set $b = \prod_{k \neq i} b_k$, and $b = \prod (1 - b_k) \equiv 1 \pmod{I_i}$; and $b \equiv 0 \pmod{I_j}$ for all $j \neq i$). Hence we have that $f(b) = (0, \ldots, 0, 1, 0, \ldots 0)$ where 1 is in the i-th position. Thus f is surjective.

Furthermore, the kernel of the map $f : R \to R/I_1 \times \cdots R/I_n$ is

$$\begin{aligned} \ker(f) &= \{r \in R \mid r = 0 \bmod I_i, i = 1, \ldots, n\} \\ &= \{r \in R \mid r \in I_i, i = 1, \ldots, n\} = \bigcap_{i=1}^{n} I_i, \quad \text{hence} \\ R/\ker(f) &= R/\bigcap_{i=1}^{n} I_i = R/I_1 \cdots I_n = R/I_1 \times \cdots R/I_n. \end{aligned}$$

(3.) Since $\ker(f) = \bigcap I_j$, f is injective if and only if $\cap I_i = \langle 0 \rangle$.

□

Definition 2.1.21. Let I be an ideal in a commutative ring R, the **radical of** I, denoted by $\sqrt{I}$ is defined as

$$\sqrt{I} = \{r \in R \mid r^n \in I, \text{ for some } n \in \mathbb{N}\}.$$

We call $\sqrt{\langle 0 \rangle} = \{r \in R \mid r^n = 0, \text{ for some } n \in \mathbb{N}\}$ is the set of **nilpotent elements of** R, and is also called **nilradical of** R, and denoted by $\mathfrak{N}$.

Proposition 2.1.22. *The set $\mathfrak{N}$ of all nilpotent elements in a ring R is an ideal, and $R/\mathfrak{N}$ has no non-zero nilpotent element.*

Proof. It is easy to see that for if $a \in \mathfrak{N}$ such that $a^m = 0$, then $ra \in \mathfrak{N}$ for all $r \in R$, and if $a, b \in \mathfrak{N}$ such that $a^m = 0$ and $b^n = 0$, then

$$(a+b)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} a^i b^{m+n-i} = 0, \text{ since } \begin{cases} a^i = 0, & \forall\, i \geq m; \\ b^{m+n-i} = 0, & \forall i \leq m. \end{cases}$$

Therefore $\mathfrak{N}$ is an ideal.

Moreover, let $\bar{r} = r + \mathfrak{N} \in R/\mathfrak{N}$, then $(\bar{r})^n = r^n + \mathfrak{N} = 0$ means $r^n \in \mathfrak{N}$. Therefore, $(r^n)^m = 0$ for some $m > 0$, hence $r^{mn} = 0$ thus $r \in \mathfrak{N}$, thus $\bar{r} = 0$. □

Proposition 2.1.23. *The nilradical of R, $\mathfrak{N} = \sqrt{\langle 0 \rangle}$, is the intersection of all prime ideals of R, i.e.*

$$\mathfrak{N} = \bigcap_{\mathfrak{p} \in \mathrm{Spec}(R)} \mathfrak{p}.$$

Proof. If $f \in \mathfrak{N}$, then f is such that $f^n = 0$ for some $n > 0$. It follows that $f \in \mathfrak{p}$ for every prime ideal $\mathfrak{p}$ in R. Hence $f \in \bigcap_{\mathfrak{p} \in \mathrm{Spec}(R)} \mathfrak{p}$.

To show the other inclusion, suppose $f \notin \mathfrak{N}$, and thus $f^n \neq 0$ for all $n > 0$. Let $\sum = \{I \text{ ideal in } R \mid f^n \notin I \text{ for all } n > 0\}$. Order this set by inclusion, then $0 \in \sum$, and by Zorn's lemma, there is a maximal element $\mathfrak{p} \in \sum$. We claim $\mathfrak{p}$ is a prime ideal. To see this let $a, b \notin \mathfrak{p}$, then $\mathfrak{p} \subset \mathfrak{p} + \langle a \rangle$ and $\mathfrak{p} \subset \mathfrak{p} + \langle b \rangle$, therefore $\mathfrak{p} + \langle a \rangle$ and $\mathfrak{p} + \langle b \rangle$ do not belong to $\sum$, hence $f^m \in \mathfrak{p} + \langle a \rangle$ and $f^n \in \mathfrak{p} + \langle b \rangle$ for some $m, n > 0$. This means $f^{m+n} \in \mathfrak{p} + \langle ab \rangle$. Since $\mathfrak{p}$ is the maximal element of $\sum$, we must have $\mathfrak{p} + \langle ab \rangle \notin \sum$, and $ab \notin \mathfrak{p}$. Thus $\mathfrak{p}$ is a prime, and $f \notin \mathfrak{p}$. Therefore, $\cap_{\mathfrak{p} \subset R} \mathfrak{p} \subset \mathfrak{N}$. □

Definition 2.1.24. We say that a ring R is **reduced** if the nilradical $\mathfrak{N}$ of R, is 0. Hence $R/\mathfrak{N}$ is a reduced ring.

Proposition 2.1.25. *The radical of an ideal I is the intersection of the prime ideals which contain I. For any ideal I, define $\mathbb{V}(I) \subset \mathrm{Spec}(R)$ to be the set of primes that contain I, i.e., $\mathfrak{p} \supset I$. Then*

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

Proof. Since $\sqrt{I} = \{r \in R \mid \bar{r} \text{ is a nilpotent element in } R/I\}$ which is the nilradical ideal $\mathfrak{N}$ of R/I. By Proposition 2.1.23, we have the $\mathfrak{N}$ of R/I is the intersection of all prime ideals contains I. □

Now, we discuss some properties of radicals of ideals.

Proposition 2.1.26. *Let $I, J \subset R$ be two ideals. Then*

1. *If $I \subseteq J$, then $\sqrt{I} \subseteq \sqrt{J}$.*
2. *$\sqrt{I} = \sqrt{\sqrt{I}}$.*
3. *$\sqrt{I+J} = \sqrt{\sqrt{I} + \sqrt{J}}$.*
4. *$\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.*
5. *$I + J = R$ if and only if $\sqrt{I} + \sqrt{J} = R$.*

Proof. (1.) Let $a \in \sqrt{I}$. Then $a^n \in I \subseteq J$ for some $n \in \mathbb{N}$, thus $a \in \sqrt{J}$.

(2.) It is obvious that $\sqrt{I} \subseteq \sqrt{\sqrt{I}}$. To show the other inclusion, let $a \in \sqrt{\sqrt{I}}$, then $a^n \in \sqrt{I}$ for some $n \in N$, and $(a^n)^m \in I$ for some $m \in N$. Thus, $a^{mn} \in I$, hence $a \in \sqrt{I}$.

(3.) It is easy to see that $\sqrt{I+J} \subseteq \sqrt{\sqrt{I} + \sqrt{J}}$. On the other hand, $\sqrt{I} \subseteq \sqrt{I+J}$ and $\sqrt{J} \subseteq \sqrt{I+J}$ implies $\sqrt{I} + \sqrt{J} \subseteq \sqrt{I+J}$. Thus $\sqrt{\sqrt{I} + \sqrt{J}} \subseteq \sqrt{\sqrt{I+J}} = \sqrt{I+J}$.

(4.) It is clear that $\sqrt{I \cap J} \subseteq \sqrt{I} \cap \sqrt{J}$. To show the other inclusion, let $a \in \sqrt{I} \cap \sqrt{J}$, then $a^n \in I$ and $a^m \cap J$ for some $m, n \in \mathbb{N}$. Therefore, $a^{m+n} \in I \cap J$, thus $a \in \sqrt{I \cap J}$.

(5.) If $I+J = R$, then $\sqrt{I}+\sqrt{J} = R$. On the other hand, if $\sqrt{I}+\sqrt{J} = R$, then $a + b = 1$ for some $a \in \sqrt{I}$ and $b \in \sqrt{J}$, and $a^n \in I$ and $b^m \in J$ for some $m, n \in \mathbb{N}$. But

$$1 = 1^{m+n} = (a+b)^{m+n} = \sum_{i=1}^{m+n} \binom{m+n}{i} a^i b^{m+n-i} = c + d,$$

where

$$c = \sum_{i \mid i<n} a^i b^{m+n-1} \in J, \text{ and } d = \sum_{i \mid i \geq n} a^i b^{m+n-i} \in I.$$

Thus, $I + J = R$. □

Definition 2.1.27. An ideal is called a **radical** ideal if $I = \sqrt{I}$.

Definition 2.1.28. The intersection of all the maximal ideals of R is called **Jacobson radical** of R, and we denote this ideal by $\mathfrak{J}$.

Recall that semi-local ring has finitely many maximal ideals. If $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ are all the maximal ideals of a semi-local ring, then the Jacobson radical $\mathfrak{J} = \bigcap_{i=1}^{s} \mathfrak{m}_i$.

The Jacobson radical has the property that

Proposition 2.1.29. *$a \in \mathfrak{J}$ if and only if $1 - ab$ is a unit in R for all $b \in R$.*

Proof. ($\Rightarrow$) Suppose $1 - ab$ is not a unit in R. Then $1 - ab$ is contained in some maximal ideal $\mathfrak{m} \subset R$. The fact that $a \in \mathfrak{J}$ implies $a \in \mathfrak{m}$, and hence $1 \in \mathfrak{m}$, which is absurd. Thus, $1 - ab \notin \mathfrak{m}$ must be a unit.

($\Leftarrow$) Suppose $a \notin \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$, then for some $b \in \mathfrak{m}$ and some $r \in R$ we have $b + ra = 1$. Hence $1 - ra \in \mathfrak{m}$ which is not a unit. □

We discussed the intersection, sum of ideals, and now, let's consider the union of ideals. In general, the union of two ideals is not an ideal.

Proposition 2.1.30. *(Prime Avoidance Theorem) The first claim is called the Prime Avoidance Theorem.*

1. *Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be prime ideals, and I an ideal such that $I \subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i$. Then $I \subseteq \mathfrak{p}_i$ for some i.*

2. *Let $I_1, \ldots, I_n$ be ideals, and $\mathfrak{p}$ a prime ideal such that $\bigcap_{i=1}^{n} I_i \subseteq \mathfrak{p}$. Then $I_i \subseteq \mathfrak{p}$ for some i. If $\bigcap_{i=1}^{n} I_i = \mathfrak{p}$, then $\mathfrak{p} = I_i$ for some i*

Proof. (1.) To prove the claim is equivalent to prove the claim that if $I \not\subseteq \mathfrak{p}_i$ for all $i = 1, \ldots, n$, then $I \not\subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i$. We will prove this by induction on n. It is obviously true for $n = 1$. If $n > 1$, we assume the result is true for $n - 1$, then there exists an $a_i \in I \setminus \mathfrak{p}_j$ for all $j \neq i$. Consider the element

$$b = \sum_{i=1}^{n} a_1 a_2 \cdots a_{i-1} a_{i+1} a_{i+2} \cdots a_n$$

Note that $a_1 a_2 \cdots a_{i-1} a_{i+1} a_{i+2} \notin \mathfrak{p}_i$ since $\mathfrak{p}_i$ is a prime. Therefore, $b \in I \setminus \mathfrak{p}_i$ for all $i = 1, 2, \ldots, n$. Hence $I \not\subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i$.

(2.) Let $I_i \not\subseteq \mathfrak{p}$ for $i = 1, \ldots, n$. Then there exist $a_i \in I_i \setminus \mathfrak{p}$ for $i = 1, \ldots, n$, and $\prod_{i=1}^{n} a_i \in \prod_{i=1}^{n} I_i \subseteq \bigcap_{i=1}^{n} I_i$. But $\prod_{i=1}^{n} a_i \notin \mathfrak{p}$ since $\mathfrak{p}$ is a prime, contradicting the given condition $\bigcap_{i=1}^{n} I_i \subseteq \mathfrak{p}$. Therefore, $I_i \subseteq \mathfrak{p}$ for some i. If $\bigcap_{i=1}^{n} I_i = \mathfrak{p}$, then $\mathfrak{p} \subseteq I_i$ for all i, hence $\mathfrak{p} = I_i$ for some i. □

Definition 2.1.31. If I, J are ideals in a ring R, the **ideal quotient** is

$$(I : J) = \{r \in R \mid rJ \subseteq I\}.$$

The ideal quotient is also an ideal. In particular, the **annihilator of** J, denoted by $\mathrm{Ann}(J)$ is defined by

$$\mathrm{Ann}(J) = (0 : J) = \{r \in R \mid rJ = \langle 0 \rangle\}.$$

Remark 2.1.32. Let D be the set of all zero-divisors in R, then $D = \bigcup_{a \neq 0} \mathrm{Ann}(a)$. In general D is a not an ideal, but

$$D = \sqrt{D} = \sqrt{\bigcup_{a \neq 0} \mathrm{Ann}(a)} = \bigcup_{a \neq 0} \sqrt{\mathrm{Ann}(a)}.$$

Definition 2.1.33. A ring R is called **Noetherian** if it satisfies the following equivalent conditions:

1. Every non-empty set of ideals in R has a maximal element;
2. Every ascending chain of ideals in R is stationary;
3. Every ideal in R is finitely generated.

Here are some properties of Noetherian rings.

Proposition 2.1.34. *If R is Noetherian ring, and f is an homomorphism of R onto a ring S, then S is Noetherian.*

Proof. Consider $f : R \twoheadrightarrow S$, then $S \cong R/\ker(f)$, hence every ascending chain in S is obtained from an ascending chain in R, we have that S is Noetherian. □

Definition 2.1.35. An ideal I is said to be **irreducible** if

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

Proposition 2.1.36. *In Noetherian ring R every ideal is a finite intersection of irreducible ideals.*

Proof. Suppose there exists at least one ideal in R such that this ideal is not a finite intersection of irreducible ideals. The fact that R is Noetherian implies that the set of ideals which is not a finite intersection of irreducible ideals has an maximal element, namely, an ideal I. Since I is reducible, then $I = I_1 \cap I_2$ where $I_i \supset I$ for $i = 1, 2$. Thus I_i are finite intersection of irreducible ideals, but this would imply that I is a finite intersection of irreducible ideals, a contradiction. Thus, every ideal is a finite intersection of irreducible ideals. □

Definition 2.1.37. Let $\mathfrak{q} \subsetneq R$ be an ideal of a ring R. The following are equivalent:

1. For all $x, y \in R$, if $xy \in \mathfrak{q}$ then either $x \in \mathfrak{q}$ or $y^n \in \mathfrak{q}$ for some integer $n \geq 1$.
2. $R/\mathfrak{q} \neq 0$ and every zero divisor in $R/\mathfrak{q}$ is nilpotent.

An ideal $\mathfrak{q}$ with either of these properties is called **primary**.

Remark 2.1.38.
1. If $\mathfrak{q}$ is primary, then $\sqrt{\mathfrak{q}} = \mathfrak{p}$ is a prime ideal, and it is the smallest prime ideal containing $\mathfrak{q}$. We say that $\mathfrak{q}$ is $\mathfrak{p}$-*primary*.
2. If the ring $R = \mathbb{Z}$, then every ideal is principal, $I = \langle n \rangle$ for some $n \in \mathbb{Z}$, and I is primary if and only if $n = \pm p^a$ is a power of a prime number. Similarly in $R = \mathbb{K}[t]$, a polynomial ring in one variable over a field $\mathbb{K}$, every ideal is principal $I = \langle f(t) \rangle$ and I is primary if and only if the generator $f(t)$ is the power of an irreducible polynomial $g(t)$, i.e., $f(t) = g(t)^a$ for some $a \in \mathbb{Z}_{\geq 0}$.
3. It is not necessarily true that the power of a prime ideal is primary. For example: $\mathfrak{p} = \langle \bar{x}, \bar{z} \rangle \subset R = \mathbb{K}[x, y, z]/\langle xy - z^2 \rangle = \mathbb{K}[\bar{x}, \bar{y}, \bar{z}]$ is prime because $R/\mathfrak{p} \cong \mathbb{K}[y]$ is an integral domain. But $\bar{x}\bar{y} = \bar{z}^2 \in \mathfrak{p}^2$, yet $x \notin \mathfrak{q} = \mathfrak{p}^2$ and $y \notin \sqrt{\mathfrak{q}} = \mathfrak{p}$, so $\mathfrak{p}^2$ is not primary.
4. A power of a maximal ideal is primary. If fact, any ideal whose radical is a maximal ideal $\mathfrak{m}$ is $\mathfrak{m}$-primary.

Theorem 2.1.39. *Let R be a Noetherian ring. Then every ideal I in R has a* **primary decomposition**. *That is, we have an expression*

$$I = \bigcap_{i=1}^{s} \mathfrak{q}_i, \quad \text{each } \mathfrak{q}_i \text{ is primary.}$$

Such a decomposition can be chosen to be irredundant in the following sense:

1. *The radicals $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ are distinct: $\mathfrak{p}_i \neq \mathfrak{p}_j$ if $i \neq j$.*
2. *For all $1 \leq i \leq s$, $\mathfrak{q}_i \not\supseteq \bigcap_{j \neq i} \mathfrak{q}_j$*

This decomposition has the following uniqueness properties:

3. *The primes $\mathfrak{p}_i$ are unique. In fact they are precisely the prime ideals that occur among the radicals of the ideals*

$$(I :_R x) = \{y \in R \mid yx \in I\}, \quad x \in R.$$

We say that these primes are associated to I.

4. *The ideals $\mathfrak{q}_i$ belong to minimal associated primes, i.e., those associated primes $\mathfrak{p}_i$ such that there are no other associated primes $\mathfrak{p}_j$ such that $\mathfrak{p}_j \subset \mathfrak{p}_i$.*

Example 2.1.40. $I = \langle x^2, xy \rangle \subset \mathbb{K}[x, y]$. Then $I = \mathfrak{p}_1 \cap \mathfrak{p}_2^2$ where $\mathfrak{p}_1 = \langle x \rangle$ and $\mathfrak{p}_2 = \langle x, y \rangle$. $\mathfrak{p}_2^2$ is the square of the maximal ideal $\mathfrak{p}_2$, so it is a primary ideal. We have $\mathfrak{p}_1 \subset \mathfrak{p}_2$, so there is only one minimal associated prime, namely $\mathfrak{p}_1$. We say that $\mathfrak{p}_2$ is an embedded prime. The primary component $\mathfrak{p}_2^2$ is not unique: we have $I = \mathfrak{p}_1 \cap \mathfrak{q}$ where $\mathfrak{q} = \langle x^2, xy, y^n \rangle$ for any $n \geq 1$.

2.2 Localization of a Ring

Let R be a commutative ring with identity, and $S \subseteq R$ a multiplicatively closed set (i.e., $1 \in S$ and S is closed under multiplication). We define an equivalence relation $\equiv$ in the set $R \times S$:

$$(r, s) \equiv (r', s') \;\Leftrightarrow\; (rs' - r's)t = 0 \;\text{ for some } t \in S.$$

This relation is reflexive, symmetric and transitive. We denote the r/s be the equivalence class of (r, s), and give $S^{-1}R$ a ring structure by defining addition and multiplication by the following:

$$(r/s) + (r'/s') = (rs' + r's)/(ss'), \quad (r/s) \cdot (r'/s') = (rr')/(ss').$$

This definition is independent of the choices of representative (r/s) and (r'/s'), and $S^{-1}R$ satisfies the axioms of a commutative ring with identity. Moreover, we have a ring homomorphism $f : R \to S^{-1}R$ defined by $f(r) = r/1$. In general, this map is not injective. If R is an integral domain, and $S = R \backslash \{0\}$, then $S^{-1}R$ is the field of fractions of R. The ring $S^{-1}R$ is called **ring of fractions** of R with respect to the multiplicative closed subset S, and sometimes we write R_S. If $S = R \setminus \mathfrak{p}$ is the complement of a prime ideal $\mathfrak{p}$, then we write $R_{\mathfrak{p}} = S^{-1}R$, and if $S = \{f^n\}_{n \geq 0}$, then we write $R_f = S^{-1}R$.

Proposition 2.2.1. *Let R be a ring, and $S \subseteq R$ a multiplicatively closed set. If $f : R \to S^{-1}R$ is a ring homomorphism defined by $f(r) = r/1$, and $g : R \to R'$ is a ring homomorphism such that $g(s)$ is a unit in R' for all $s \in S$. Then there exists a unique ring homomorphism $h : S^{-1}R \to R'$ such that $g = h \circ f$.*

Proof. (Existence) Let $h(r/s) = g(r)g(s)^{-1}$, we will show that h is well-defined. Let $r/s = r'/s'$, then there exists a $t \in S$ such that $(rs' - r's)t = 0$, thus

$$(g(r)g(s') - g(r')g(s))g(t) = 0.$$

Since $t \in S$, $g(t)$ is a unit in R', $g(r)g(s') = g(r')g(s)$, and $g(r)g(s)^{-1} = g(r')g(s')^{-1}$. Thus $h(r/s) = h(r'/s')$, i.e., h is well-defined. It is easy to see that h is a ring homomorphism.

(Uniqueness) If h satisfies the given condition, then $h(r/1) = hf(r) = g(r)$ for all $r \in R$. For all $s \in S$,

$$h(1/s) = h((s/1)^{-1}) = h(s/1)^{-1} = g(s)^{-1},$$

thus,

$$h(r/s) = h(r/1)h(1/s) = g(r)g(s)^{-1}.$$

Therefore, h is uniquely determined. □

We have seen that the ring homomorphism: $f : R \to S^{-1}R$ has the following properties:

1. If $s \in S$, then $f(s)$ is a unit in $S^{-1}R$;
2. $f(r) = 0$ implies that $rs = 0$ for some $s \in S$;
3. Every element in $S^{-1}R$ is the form $f(r)f(s)^{-1}$ for some $r \in R$ and $s \in S$.

Any such f determines a ring $S^{-1}R$ up to isomorphism.

Definition 2.2.2. Let $R \to T$ be any ring homomorphism, I an ideal of R, and J an ideal of T. We write IT or I^e for the ideal $f(I)T \subset T$, and call this ideal the **extension of I to T**, or the **extended ideal**. We write $J \cap R$ or J^c for the ideal $f^{-1}(J)R \subset R$, and call this ideal the **contracted ideal of J**.

Remark 2.2.3. 1. $I^{ec} \subset I, \quad J^{ce} \subset J.$

2. From the above inclusion,

$$I^{ece} \subset I^e \subset (I^e)^{ce} = I^{ece} \;\Rightarrow\; I^e = I^{ece}, \text{ similarly, } J^{cec} = J^c.$$

   Hence, there is a canonical bijection between the sets $\{I^e\}$ and $\{J^c\}$.

3. If $\mathfrak{p}$ is a prime in T, then $T/\mathfrak{p}$ is an integral domain. Since $R/\mathfrak{p}^c$ is a subring of $T/\mathfrak{p}$, it is also an integral domain. Thus, $\mathfrak{p}^c$ is a prime ideal.

Theorem 2.2.4. *Let S be a multiplicative closed set in the ring R. Then:*

1. *All the ideals of R_S are of the form IR_S where I is an ideal of R;*

2. *Every prime ideal of R_S is of the form $\mathfrak{p}R_S$ where $\mathfrak{p}$ is a prime ideal of R disjoint from S. Conversely, $\mathfrak{p}R_S$ is a prime in R_S for every such $\mathfrak{p}$. Exactly the same holds for primary ideals.*

Proof. (1.) Let J be an ideal in R_S, set $I = J \cap R = J^c$. By part 1 of Remark 2.2.3, $IR_S = J^{ce} \subset J$. If $f : R \to R_S$ is the localization map, and $x = a/s \in J$, then $f(a) = xf(s) \in J$, hence $a \in I$. Thus $x = (1/s) \cdot f(a) \in IR_S$, that is $J \subset IR_S$. Therefore, $J = IR_S$, and all the ideals of R_S are of the form IR_S where I is an ideal of R.

(2.) If P is a prime ideal in R_S, let $\mathfrak{p} = P \cap R$, then $\mathfrak{p}$ is a prime ideal of R. By the first claim, $P = \mathfrak{p}R_S$. Since P does not contain a unit in R_S, $\mathfrak{p} \cap S = \emptyset$.

On the other hand, if $\mathfrak{p}$ is a prime ideal of R and disjoint from S, then

$$(a/s)(b/t) \in \mathfrak{p}R_S, \quad s,t \in S \;\Rightarrow\; rab \in \mathfrak{p} \text{ for some } r \in S.$$

Since $r \notin \mathfrak{p}$, and $\mathfrak{p}$ is a prime, we must have $ab \in \mathfrak{p}$, thus either a or b is in $\mathfrak{p}$. Therefore, either a/s or b/t is in $\mathfrak{p}R_S$. Thus $\mathfrak{p}R_S$ is a prime ideal of R_S.

Similar proof will show that exactly the same holds for primary ideals. □

Remark 2.2.5. If $\mathfrak{p} \subset R$ is a prime ideal, then it follows from the above that $R_\mathfrak{p}$ is a local ring with (unique) maximal ideal $\mathfrak{p}R_\mathfrak{p}$. The reason is that the lattice of prime ideals in $R_\mathfrak{p}$ is isomorphic to the lattice of the prime ideals in R that are disjoint from $R \setminus \mathfrak{p}$. But these are just the prime ideals contained in $\mathfrak{p}$. There must be a unique maximal element, namely $\mathfrak{p}$.

Theorem 2.2.6. *Let R be a ring, $S \subset R$ a multiplicatively closed set, I an ideal in R, and $\bar{S}$ the image of S in R/I. Then*

$$R_S/IR_S \cong (R/I)_{\bar{S}}.$$

Proof. The composite map $R \to R/I \to (R/I)_{\bar{S}}$ sends every element of S to a unit, and sends I to zero. Therefore it induces a map $R_S \to (R/I)_{\bar{S}}$ which factors through a map $R_S/IR_S \to (R/I)_{\bar{S}}$. On the other hand, the map $R \to R_S \to R_S/IR_S$ sends I to zero, and therefore induces a map $R/I \to R_S/IR_S$. This map sends every element of $\bar{S}$ to a unit, and hence induces a map $(R/I)_{\bar{S}} \to R_S/IR_S$. These two constructed maps are inverses of each other. □

Remark 2.2.7. If $\mathfrak{p} \subset R$ is a prime ideal, then $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ is the fraction field of the integral domain $R/\mathfrak{p}$, because $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} = (R/\mathfrak{p})_{\bar{S}_\mathfrak{p}}$, and $\bar{S}_\mathfrak{p} = (R/\mathfrak{p}) \setminus 0$.

Theorem 2.2.8. *Let R be a ring, S a multiplicatively closed set in R, and $f : R \to R_S$ the canonical map. Suppose that R' is another ring, and $g : R \to R'$ and $h : R' \to R_S$ are maps such that $f = h \circ g$. Suppose further that for every $r' \in R'$, there exists an $s \in S$ such that $g(s)r' \in g(R)$. Then R_S can be regarded as a localization of the ring R'. In particular,*

$$R_S = R'_{g(S)} = R'_T, \quad \textit{where } T = \{t \in R' \mid h(t) \textit{ is a unit in } R_S\}.$$

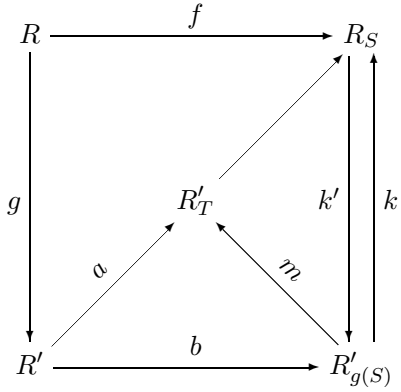
Proof. Observe that $g(S)$ is a multiplicatively closed subset of R', so we have a localization $b : R' \to R'_{g(S)}$. Since $f = h \circ g$, and f inverts S, we see that h inverts $g(S)$, so $g(S) \subset T$. Therefore we have a factorization of $a : R' \xrightarrow{b} R'_{g(S)} \xrightarrow{m} R'_T$. Since h inverts $g(S)$, the map h factors as $R' \to R'_{g(S)} \xrightarrow{k} R_S$. The composite $R \to R' \to R'_{g(S)}$ inverts S, so we can factor it as $R \xrightarrow{f} R_S \xrightarrow{k'} R'_{g(S)}$. We calculate

$$k(k'(f(a)/f(s))) = k(g(a)/g(s)) = h(g(a))/h(g(s)) = f(a)/f(s),$$

and since every element of R_S is of the shape $f(a)/f(s)$, $k \circ k' = \mathrm{id}_{R_S}$. On the other hand, k' is a surjective map by our hypothesis, and hence, k, k' are inverse isomorphisms. To see that R'_T and $R'_{g(S)}$ are isomorphic, we construct an inverse to the map m above. Note that the composite $R' \xrightarrow{h} R_S \xrightarrow{k'} R'_{g(S)}$ inverts T, and therefore factors as $R' \to R'_T \xrightarrow{n} R'_{g(S)}$. We claim that $m \circ n = 1$ and $n \circ m = 1$. For instance

$$m(n(a(r')/a(t))) = m(b(r')/b(t)) = a(r')/a(t),$$

and since every element of R'_T is of the form $a(r')/a(t)$, we get that $m \circ n = 1$. The proof for $n \circ m = 1$ is similar.



□

We will try to understand the localization from another point of view. First, we will provide an extension of the polynomial division theorem.

Theorem 2.2.9. *Let R be a ring, $f \in R$, and y a new indeterminate such that $0 \neq g(y) \in R[y]$. Then there exists a $q(y) \in R[y]$ such that*

$$f^{\deg(g)} g(y) = q(y)(fy - 1) + r, \text{ where } r \in R.$$

Proof. We can write $g(y) = \sum_{i=0}^{k} r_i y^i$ for some $r_i \in R$, and $\deg(g) = k$. Then

$$f^{\deg(g)} g(y) = \sum_{i=0}^{k} f^k r_i y^i = \sum_{i=0}^{k} f^{k-i} r_i (fy)^i := G(fy), \text{ where } G(y) \in R[y].$$

Note

$$\begin{aligned}
G(y) &= \sum_{i=0}^{k} f^{k-i} r_i (y)^i, \\
G(y+1) &= \sum_{i=0}^{k} f^{k-i} r_i (y+1)^i = Q(y)y + r, \\
&\quad \text{where } Q(y) \in R[y],\ r \in R, \text{ substitute } y = fy - 1 \\
f^{\deg(g)} g(y) &:= G(fy) \\
&= Q(fy-1)(fy-1) + r = q(y)(fy-1) + r, \\
&\quad \text{where } q(y) = Q(fy-1) \in R[y].
\end{aligned}$$

□

With this result, we can view the localization this way:

Theorem 2.2.10. *Let R be a ring, $0 \neq f \in R$, and y an indeterminate. Then there exists an isomorphism of R-algebra*

$$R_f \cong R[y]/\langle fy - 1 \rangle.$$

Proof. Let $\phi : R[y] \to R_f$ be an R-algebra homomorphism defined by $\phi(y) = \frac{1}{f}$. It is easy to see that $fy - 1 \in \ker(\phi)$. We will show that $\ker(\phi) \subset \langle fy - 1 \rangle$. To do so, let $0 \neq g(y) \in \ker(\phi)$, then by Theorem 2.2.9,

$$f^k g(y) = q(y)(fy - 1) + r, \text{ where } k = \deg(g),\ q(y) \in R[y],\ r \in R.$$

Since $g(y) \in \ker(\phi)$,

$$0 = \phi(f^k g(y)) = \phi(q(y)(fy - 1) + r) = r \in R_f,$$

therefore, there exists $t > 0$ such that $f^t r = 0 \in R$. Thus,

$$f^{k+t} g(y) = f^t q(y)(fy-1) + f^t r = f^t q(y)(fy-1).$$

This shows that

$$\begin{aligned} g(y) &= f^{k+t} y^{k+t} g(y) - (f^{k+t} y^{k+t} - 1) g(y) \\ &= y^{k+t} f^t q(y)(fy-1) - (fy-1) \left(\sum_{i=0}^{k+t-1} f^i y^i \right) g(y) \\ &\in \langle fy - 1 \rangle. \end{aligned}$$

Thus $\ker(\phi) = \langle fy - 1 \rangle$. □

Localization is also related to a concept called saturation.

Definition 2.2.11. Let R be a ring, $J, I \subset R$ be ideals. Then the set

$$(J :_R I^\infty) = \bigcup_{i \in \mathbb{N}} J :_R I^i = \{ r \in R \mid I^i r \subseteq J, \text{ for some } i \in \mathbb{N} \}$$

is an ideal in R, and is called the **saturation of J by I in R.**

Remark 2.2.12. Let R be a Noetherian ring. If $k = \min\{ i \in \mathbb{N} \mid J :_R I^i = J :_R I^{i+1} \}$, then

$$(J :_R I^\infty) = (J :_R I^k) = (J :_R I^{k+1}) = \cdots .$$

Moreover, $(J :_R f^\infty) = J_f \cap R$.

Proof. To show the first claim, we observe that $r \in R$ is such that $I^i r \subseteq J$ for some $i \geq 0$, then $I^{i+1} r \subseteq J$. Hence we have a increasing chain

$$(J :_R I) \subseteq (J :_R I^2) \subseteq \cdots \subseteq \cdots \subseteq (J :_R I^\infty),$$

which is stable since R is a Noetherian ring. Thus, we must have that $(J :_R I^i) = (J :_R I^{i+1})$ for some i. Therefore, the claim holds.

To show the second claim, we first prove $(J :_R f^\infty) \subseteq J_f \cap R$. Observe that $r \in R$ such that $f^i r \subseteq J$ for some $i \in \mathbb{N}$ suggests $\frac{r}{1} = \frac{1}{f^i} \cdot f^i r \in J_f$. On the other hand to show $J_f \cap R \subseteq (J :_R f^\infty)$, let r R such that $\frac{r}{1} = \frac{a}{f^k}$ for some $a \in J$ and $k \in \mathbb{N}$, we have $f^k r = a \in J$. Thus $r \in (J :_R f^\infty)$, and we proved the claim. □

Theorem 2.2.13. *Let R be a Noetherian ring, I, J ideals in R, and y an indeterminate.*

1. *Suppose* $I = \langle f \rangle$. *Then*
$$(J :_R f^\infty) = (JR[y] + \langle fy - 1 \rangle R[y]) \cap R.$$

2. *Let* $\{f_1, \ldots, f_s\}$ *be a system of generators of* I, *then*
$$(J :_R I^\infty) = \bigcap_{i=1}^{s} (J :_R f_i^\infty).$$

3. *Let* $\{f_1, \ldots, f_s\}$ *be a system of generators of* I, *and* $f(y) = \sum_{i=1}^{s} f_i y^{i-1}$. *Then*
$$(J :_R I^\infty) = \left(JR[y] :_{R[y]} f(y)^\infty\right) \cap R.$$

Proof. (1.) Let $r \in R$ be such that $f^i r \in J$ for some $i \in \mathbb{N}$. Then
$$r = f^i y^i r - \left(\sum_{s=0}^{i-1} f^s y^s\right)(fy - 1)r \in (JR[y] + \langle fy - 1 \rangle R[y]) \cap R.$$
On the other hand, let $r \in (JR[y] + \langle fy - 1 \rangle R[y]) \cap R$, and $\{a_1, \ldots, a_t\}$ a system of generators of J, then
$$r = \sum_{i=1}^{s} a_i g_i + (fy - 1)g, \text{ for some } g, g_1, \ldots, g_s \in R[y].$$
Replacing $y = \frac{1}{f}$, we have
$$r = \sum_{i=1}^{s} a_i g_i \left(\frac{1}{f}\right), \text{ for some } g, g_1, \ldots, g_s \in R[y].$$
Clear the denominator, we obtain
$$f^t r = \sum_{i=1}^{s} a_i g_i' \in J, \text{ for some } g_i' \in R.$$
Thus $f \in (J :_R f^t) \subseteq (J :_R f^\infty)$.

(2.) The second claim is done by induction on s. First, we claim that
$$(J :_R f^\infty) \cap (J :_R g^\infty) = (J :_R \langle f, g \rangle^\infty).$$
It is easy to see that if $r \in (J :_R \langle f, g \rangle^\infty)$, then there exists $t \in \mathbb{N}$ such that $\langle f, g \rangle^t r \subseteq J$. Since $f^t, g^t \in \langle f, g \rangle^t$, we must have
$$f^t r,\, g^t r \subseteq \langle f, g \rangle^t r \subseteq J,$$

and

$$r \in (J :_R f^\infty) \cap (J :_R g^\infty).$$

On the other hand, let $r \in (J :_R f^\infty) \cap (J :_R g^\infty)$, then there exist $k, t \in \mathbb{N}$ such that

$$f^t r,\, g^k r \subseteq J.$$

This shows that

$$\langle f, g\rangle^{t+k+1} r \in J, \text{ hence } r \in J :_R \langle f, g\rangle^\infty.$$

Repeat this, we obtain the second result.

(3.) To show $(J :_R I^\infty) \subseteq \big(JR[y] :_{R[y]} f(y)^\infty\big) \cap R$, we observe that second claim yields that

$$(J :_R I^\infty) = \bigcap_{i=1}^{s} (J :_R f_i^\infty),$$

which means that if $r \in (J :_R I^\infty)$, then $f_1^w r, \ldots, f_s^w r \in J$ for some sufficiently large integer w. Hence for some $t \in \mathbb{N}$, we have

$$f(y)^t r = (f_1 + f_2 y + \cdots + f_s y^{s-1})^t r \in JR[y].$$

Thus, we showed the desired inclusion

On the other hand, assume $r \in \big(JR[y] :_{R[y]} f(y)^\infty\big) \cap R$, then for some $t \in \mathbb{N}$, we have that

$$f(y)^t r = (f_1 + f_2 y + \cdots + f_s y^{s-1})^t r \in JR[y].$$

By looking at coefficients of powers of y, and by the second claim, we have that

$$r \in \bigcap_{i=1}^{s} (J :_R f_i^\infty) = (J :_R I^\infty).$$

□

As an application, we may check radical membership via localizations.

Remark 2.2.14. Let R be a Noetherian ring and $I \subseteq R$ an ideal. Let $0 \neq f \in R$ and y a new indeterminate. Then the following are equivalent:

1. $f \in \sqrt{I}$,
2. $IR_f = R_f$,

3. $1 \in (I :_R f^\infty)$,

4. $1 \in IR[y] + (fy - 1)$ in the ring $R[y]$,

Proof. To prove the claims we can observe that $f \in \sqrt{I}$ means that $f^i \in I$ for some $i \in \mathbb{N}$. Then $1 = f_i \cdot \frac{1}{f^i} \in IR_f$. Moreover, if $1 \in IR_f$, then there exists $g \in I$, and $i \in \mathbb{N}$ such that $1 = \frac{g}{f^i}$, which means $f^i = g \in I$. This shows the equivalence of the first two claims.

Since $(I :_R f^\infty) = I_f \cap R$, we have $(2 \Leftrightarrow 3)$.

Finally, Theorems 2.2.10 and 2.2.13 show $(3 \Leftrightarrow 4)$. □

2.3 Ideals in a Polynomial Ring

Recall:

Lemma 2.3.1. *Let $\mathbb{K}$ be a field, and I an ideal in the polynomial ring $\mathbb{K}[x]$. Then there exists $f \in \mathbb{K}[x]$ such that $I = \langle f \rangle$. This means that any ideal in $\mathbb{K}[x]$ is a principal ideal.*

This is proved using the division algorithm:

Lemma 2.3.2. *Let $\mathbb{K}$ be a field, and $f \in \mathbb{K}[x]$ a non-zero polynomial with coefficients in $\mathbb{K}$. Then, given any polynomial $h \in \mathbb{K}[x]$, there exist unique polynomials q and $r \in \mathbb{K}[x]$ such that $h = fq + r$ where $r = 0$ or $\deg r < \deg f$.*

Definition 2.3.3. Polynomials $f_1, f_2, \ldots, f_n \in \mathbb{K}[x]$ for some field $\mathbb{K}$ are said to be **coprime** if there is no non-constant that divides all of them.

Lemma 2.3.4. *Let $f_1, f_2, \ldots, f_n \in \mathbb{K}[x]$ be coprime polynomials in some field $\mathbb{K}$. Then there exist polynomials $g_1, g_2, \ldots, g_n$ such that $f_1 g_1 + f_2 g_2 + \cdots f_n g_n = 1$.*

Proof. Let $I = \langle f_1, f_2, \ldots, f_n \rangle$, then Lemma 2.3.1 shows there exists a polynomial $f \in I$ such that $I = \langle f \rangle$. Hence, for $i = 1, 2, \ldots, n$, $f_i = c_i f$ for some $c_i \in \mathbb{K}[x]$. Moreover, the condition that f_i's are coprime yields that f must be a constant. Thus, there exist $g_1, g_2, \ldots, g_n$ such that $f_1 g_1 + f_2 g_2 + \cdots f_n g_n = 1$. □

Lemma 2.3.5. *Let $f, g \in \mathbb{K}[x]$ be polynomials with $\deg f = \ell > 0$ and $\deg g = m > 0$. Then f and g have a common factor if and only if there are polynomials $A, B \in \mathbb{K}[x]$ such that:*

1. *A and B are not both zero,*
2. *$\deg A \le m-1$ and $\deg B \le \ell - 1$,*
3. *$Af + Bg = 0$.*

Proof. First, suppose f and g have a common factor, and let $h = \gcd(f,g) \in \mathbb{K}[x]$. Then $f = hf_1$ and $g = hg_1$ with $f_1, g_1 \in \mathbb{K}[x]$, $\deg f_1 \le \ell - 1$, $\deg g_1 \le m-1$, and $\gcd(f_1, g_1) = 1$. Then $g_1 f + (-f_1)g = g_1(hf_1) + (-f_1)hg_1 = 0$. Set $A = g_1$ and $B = -f_1$, we obtain the required properties.

Conversely, let A and B be polynomials with the required properties. Without loss of generality, by the first property, let $B \neq 0$. If $\gcd(f,g) = 1$, then by Lemma 2.3.4, we can find polynomials $A', B' \in \mathbb{K}[x]$ such that $A'f + B'g = 1$. Multiply both sides by B, and use property 3, $Bg = -Af$, we have

$$B = B(A'f + B'g) = A'Bf + B'Bg = A'Bf - AB'f = (A'B - AB')f.$$

Since $B \neq 0$, this shows that $\deg B \ge \deg f = \ell$, contradicting property 2. Hence, there must be a common factor of positive degree. □

Now, write

$$\begin{aligned} A &= c_0 x^{m-1} + \cdots + c_{m-1}, \\ B &= d_0 x^{\ell-1} + \cdots + d_{\ell-1}, \\ f &= a_0 x^{\ell} + \cdots + a_{\ell}, \quad a_0 \neq 0, \\ g &= b_0 x^{m} + \cdots + b_{m}, \quad b_0 \neq 0, \end{aligned}$$

and regard $c_0, \ldots, c_{m-1}, d_0, \ldots, d_{\ell-1}$ as $\ell + m$ unknowns. Then the equation $Af + Bg = 0$ gives the following matrix equations

$$\begin{bmatrix} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ a_2 & a_1 & \ddots & & b_2 & b_1 & \ddots & b_0 \\ \vdots & \vdots & \ddots & a_0 & \vdots & \vdots & \ddots & \vdots \\ a_\ell & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ & a_\ell & \ddots & \vdots & b_m & \vdots & \ddots & \vdots \\ & & \ddots & \vdots & & b_m & \ddots & \vdots \\ & & & a_\ell & & & & b_m \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{m-1} \\ d_0 \\ \vdots \\ d_{\ell-1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Since there are $\ell + m$ linear equations and $\ell + m$ unknowns, there is non-trivial solution if and only if the coefficient matrix has zero determinant.

Definition 2.3.6. Given $f, g \in \mathbb{K}[x]$, and

$$\begin{aligned} f &= a_0 x^\ell + \cdots + a_\ell, \quad a_0 \neq 0, \\ g &= b_0 x^m + \cdots + b_m, \quad b_0 \neq 0. \end{aligned}$$

The **Sylvester matrix** of f and g with respect to x, denoted $\mathrm{Syl}(f, g, x)$ is an $(\ell + m) \times (\ell + m)$ matrix:

$$\mathrm{Syl}(f,g,x) = \begin{bmatrix} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ a_2 & a_1 & \ddots & & b_2 & b_1 & \ddots & b_0 \\ \vdots & \vdots & \ddots & a_0 & \vdots & \vdots & \ddots & \vdots \\ a_\ell & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ & a_\ell & \ddots & \vdots & b_m & \vdots & \ddots & \vdots \\ & & \ddots & \vdots & & b_m & \ddots & \vdots \\ & & & a_\ell & & & & b_m \end{bmatrix}$$

The **Resultant** of f and g with respect to x, denoted $\mathrm{Res}(f, g, x)$, is the determinant of the Sylvester matrix.

$$\mathrm{Res}(f,g,x) = \det(\mathrm{Syl}(f,g,x)).$$

A polynomial is called an *integer polynomial* provided all of its coefficients are integers.

Proposition 2.3.7. *Given $f, g \in \mathbb{K}[x]$ of positive degree, then Res(f, g, x) is an integer polynomial in the coefficients of f and g. Furthermore, f and g have a common factor in $\mathbb{K}[x]$ if and only if Res$(f, g, x) = 0$.*

Proposition 2.3.8. *Given $f, g \in \mathbb{K}[x]$ of positive degree, then there are polynomials $A, B \in \mathbb{K}[x]$ such that $Af + Bg =$ Res(f, g, x). Furthermore, the coefficients of A and B are integer polynomials in the coefficients of f and g.*

Proof. If $\mathrm{Res}(f, g, x) = 0$, then we can choose $A = B = 0$.

On the other hand, if $\mathrm{Res}(f, g, x) \neq 0$, then by Proposition 2.3.7 and Lemma 2.3.4, there exist A' and B' such that $A'f + B'g = 1$. Write

$$\begin{aligned} A' &= c_0 x^{m-1} + \cdots + c_{m-1}, \\ B' &= d_0 x^{\ell-1} + \cdots + d_{\ell-1}, \\ f &= a_0 x^\ell + \cdots + a_\ell, \quad a_0 \neq 0, \\ g &= b_0 x^m + \cdots + b_m, \quad b_0 \neq 0, \end{aligned}$$

and $A'f + B'f = 1$ if and only if

$$\mathrm{Syl}(f, g, x)(c_0, c_1, \ldots, c_{m-1}, d_0, d_1, \ldots, d_\ell)^t = (0, 0, 0, \ldots, 0, 1)^t.$$

Then by Cramer's rule, we can solve

$$c_0 = \frac{1}{\mathrm{Res}(f, g, x)} \begin{bmatrix} 0 & & & & b_0 & & & \\ 0 & a_0 & & & b_1 & b_0 & & \\ 0 & a_1 & \ddots & & b_2 & b_1 & \ddots & b_0 \\ \vdots & \vdots & \ddots & a_0 & \vdots & \vdots & \ddots & \vdots \\ 0 & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & a_\ell & \ddots & \vdots & b_m & \vdots & \ddots & \vdots \\ 0 & & \ddots & \vdots & & b_m & \ddots & \vdots \\ 1 & & & a_\ell & & & & b_m \end{bmatrix},$$

and similar solution for other c_i's and d_i's. Hence, we have

$$A' = \frac{A}{\mathrm{Res}(f, g, x)}, \; B' = \frac{B}{\mathrm{Res}(f, g, x)}$$

where A, B are integer polynomials in a_i, b_i, and $A'f + B'g = 1$ shows $Af + Bg = \mathrm{Res}(f, g, x)$. □

Remark 2.3.9. If $f, g \in \mathbb{K}[x]$ have positive degree in x. Then $\mathrm{Res}(f, g, x) \in \langle f, g \rangle$.

Definition 2.3.10. A non-constant polynomial $f \in R[x]$ where R is ring is said to be **irreducible** over R if there does not exist any non-constant polynomial that divides f whose degree is less than that of f.

Proposition 2.3.11. *Let $f, g, h \in \mathbb{K}[x]$ over some field $\mathbb{K}$. Suppose that f is irreducible over $\mathbb{K}$ such that $f \mid (gh)$. Then either $f \mid g$ or $f \mid h$.*

Proof. Suppose $f \nmid g$, we will show that $f \mid h$. First, we note since f is irreducible, g, f must be coprime. By Lemma 2.3.4, there exist $p, q \in K[x]$ such that $pf + qg = 1$. This shows that $pfh + qgh = h$. Since $f \mid (gh)$, $gh = fc$ for some $c \in \mathbb{K}[x]$. Thus, $pfh + qgh = (ph + qc)f = h$, and $f \mid h$. □

Let $R = \mathbb{K}[x_1, x_2, \ldots, x_n]$ be a multivariate polynomial ring over a field $\mathbb{K}$, and $\mathbb{M}$ the set of all monomials $\{\mathbf{x}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}\}$. Any element $f \in R$ can be written as

$$f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha \mathbf{x}^\alpha, \text{ where } \mathbf{x}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}, \text{ where } \mathbb{N} = \{0, 1, 2, \ldots\}.$$

Theorem 2.3.12. *Let $f \in \mathbb{K}[x_1, \ldots, x_n]$ be irreducible over the field $\mathbb{K}$, and suppose that f divides the product gh, where $g, h \in \mathbb{K}[x_1, \ldots, x_n]$. Then f divides either g or h.*

Proof. The claim can be shown by induction on the number of variables, we omit the prove here, but we note if $n = 1$, then the theorem is in fact Proposition 2.3.11. □

Corollary 2.3.13. *Suppose that $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ have positive degree in x_1. Then f and g have a common factor in $\mathbb{K}[x_1, \ldots, x_n]$ of positive degree in x_1 if and only if they have a common factor in $\mathbb{K}(x_2, \ldots, x_n)[x_1]$ that has a positive degree in x_1.*

Proof. If f and g have a common factor in $\mathbb{K}[x_1, \ldots, x_n]$ of positive degree in x_1, then they definitely have a common factor in the $\mathbb{K}(x_2, \ldots, x_n)[x_1]$. On the other hand, if f and g have a common factor $h \in \mathbb{K}(x_2, \ldots, x_n)[x_1]$ of positive degree in x_1, then

$$f = hf_1,\ g = hg_1,\ f_1, g_1, h \in \mathbb{K}(x_2, \ldots, x_n)[x_1].$$

Now, let $d \in \mathbb{K}[x_2, \ldots, x_n]$ be a common denominator of f_1, g_1, h, and define elements of $\mathbb{K}[x_1, ..., x_n]$:

$$H = dh,\ F_1 = df_1,\ G_1 = dg_1.$$

Then

$$d^2 f = d^2 h f_1 = HF_1,\ d^2 g = d^2 h g_1 = HG_1,\ H, F_1, G_1 \in \mathbb{K}[x_1, x_2, \ldots, x_n].$$

Since $h = H/d$ has a positive degree in x_1, there exists an irreducible factor h' of H with positive degree in x_1, thus $h' \mid d^2 f$ (since $d^2 f = HF_1$). Note that $h' \nmid d^2$ since $d \in \mathbb{K}[x_2, \ldots, x_n]$, hence, $h' \mid f$ in $\mathbb{K}[x_1, \ldots, x_n]$. By similar argument, $h' \mid g$ in $\mathbb{K}[x_1, \ldots, x_n]$. Thus, f and g has a common factor $h' \in \mathbb{K}[x_1, \ldots, x_n]$ with positive degree in x_1. □

Theorem 2.3.12 implies that there is a unique factorization of a polynomial in a polynomial ring.

Theorem 2.3.14. *Every non-constant polynomial $f \in \mathbb{K}[x_1, \ldots, x_n]$ can be written as a product $f = f_1 \cdot f_2 \cdots f_r$ of irreducible polynomials over $\mathbb{K}$. Furthermore, if $f = g_1 \cdot g_2 \cdots g_s$ is another factorization into irreducibles over $\mathbb{K}$, then $r = s$ and with some permutation, each f_i can be written as a constant multiple of g_i.*

Theorem 2.3.15. (Hilbert's Basis Theorem) *A polynomial ring in one indeterminate over a Noetherian ring is itself Noetherian. In particular, by iteration, the polynomial ring $\mathbb{K}[x_1, \ldots, x_n]$ over a field $\mathbb{K}$ is Noetherian. Every finitely generated $\mathbb{K}$-algebra is Noetherian.*

Proof. Let I be an ideal in the ring $R[x]$. The leading coefficients of the polynomials in I form an ideal J in R. Since R is Noetherian, J is finitely generated, and let $J = \langle a_1, \ldots, a_n \rangle$. For each $i = 1, \ldots, n$, there is a polynomial $f_i \in R[x]$ of the form $f_i = a_i x^{\alpha_i} + \text{lower terms}$. Let $\alpha = \max\{\alpha_i\}_{i=1}^n$. The f_i's generate an ideal $I' \subseteq I \subset R[x]$.

Let $f = ax^m + \text{lower terms} \in I$, then $a \in J$ and a is generated by a_i's. If $m \geq \alpha$, then $a = \sum_{i=1}^n c_i a_i$ where $c_i \in R$, and $g = f - \sum_{i=1}^n c_i f_i x^{m-\alpha_i} \in I$ with $\deg(g) < m$. Continuing in this way, we can write $f = g + h$ where $h \in I'$ and $g \in I$ has degree $\leq \alpha - 1$. The elements of I of degree $\leq \alpha - 1$ form a sub R-module of the free R-module generated by $1, x, \ldots, x^{\alpha-1}$. Since R is Noetherian, this submodule is finitely generated. Let $g_1, \ldots, g_t$ be generators. Then the above argument shows that $f_1, \ldots, f_s, g_1, \ldots, g_t$ generate I. Hence, I is finitely generated. □

2.4 Gröbner Basis of an Ideal

Definition 2.4.1. A **partial order** is a binary relation $\geq$ on a set S which is reflexive, antisymmetric, and transitive, i.e., for all a, b, and c in S:

1. $a \geq a$ (reflexivity);
2. If $a \geq b$ and $b \geq a$ then $a = b$ (antisymmetry);
3. If $a \geq b$ and $b \geq c$ then $a \geq c$ (transitivity).

A set with a partial order is called a **partially ordered set**. A **total order** is a binary relation that satisfies the conditions for a partial order plus an additional condition known as the comparability condition

4. For any $a, b \in S$, either $a \geq b$ or $b \geq a$ (Comparability).

A set with a total order is called a **totally ordered set**.

We are interested in orderings on the set $\mathbb{M}$ of monomials in a polynomial ring $\mathbb{K}[x_1, \cdots, x_n]$.

Definition 2.4.2. An **admissible partial order** T is a partial order $>_T$ on $\mathbb{M}$ with the properties:

1. $m >_T 1$ for any non constant monomial m;
2. If $m_1 > m_2$, and $m_3 \in \mathbb{M}$, then $m_1 \cdot m_3 > m_2 \cdot m_3$.

If $>_T$ is a total order, we say that it is a **term order** or **a monomial ordering**.

For multivariate monomials $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ and $x^\beta = x_1^{\beta_1} \cdots x_n^{\beta_n}$ in the polynomial ring $\mathbb{K}[x_1, \cdots, x_n]$, with $\alpha = (\alpha_1, \cdots, \alpha_n)$ and $\beta = (\beta_1, \cdots, \beta_n)$ in $\mathbb{N}^n$, where $\mathbb{N}$ is the set of non-negative integers, any ordering on $\mathbb{N}^n$ will give an ordering on the monomials. If $\alpha > \beta$, we will say $x^\alpha > x^\beta$.

Definition 2.4.3. We say $\alpha > \beta$ with **Lexicographic order**, or **lex order**, if in the vector difference $\alpha - \beta \in \mathbb{Z}^n$, the left-most nonzero entry is positive. We will write $x^\alpha > x^\beta$ if $\alpha > \beta$.

Definition 2.4.4. Let $f = \sum_\alpha a_\alpha x^\alpha$ be a nonzero polynomial in $\mathbb{K}[x_1, \cdots, x_n]$ and let $>$ be a monomial order. The **multidegree** of f is

$$\deg(f) = \max\{\alpha \in \mathbb{N}^n : a_\alpha \neq 0\}.$$

The **leading coefficient** of f is

$$\mathrm{LC}(f) = a_{\deg(f)} \in \mathbb{K}.$$

The **leading monomial** of f is

$$\mathrm{LM}(f) = x^{\deg(f)} \text{ with coefficient } 1.$$

The **leading term** of f is

$$\mathrm{LT}(f) = \mathrm{LC}(f) \cdot \mathrm{LM}(f).$$

Example 2.4.5. This example illustrates lex order and the monomial order corresponding to different variable order.

1. $(1, 1, 3) > (0, 3, 4)$ since $(1, 1, 3) - (0, 3, 4) = (1, -2, -1)$.
2. There are many lex orders corresponding to how the variables are ordered.

   Let $f = xy^2z^3 + 4x^2yz^4 \in \mathbb{K}[x, y, z]$

   a) If $x > y > z$, we can order the terms of f in decreasing order:

   $$f = 4x^2yz^4 + xy^2z^3, \text{ since } (2, 1, 4) > (1, 2, 3).$$

   $$\deg(f) = (2, 1, 4),\ \mathrm{LC}(f) = 4,\ \mathrm{LM}(f) = x^2yz^4,\ \mathrm{LT}(f) = 4x^2yz^4.$$

b) If $y > x > z$, we can order the terms of f in decreasing order:

$$f = y^2xz^3 + 4yx^2z^4, \text{ since } (2,1,3) > (1,2,4).$$

$$\deg(f) = (2,1,3),\ \mathrm{LC}(f) = 1,\ \mathrm{LM}(f) = y^2xz^3,\ \mathrm{LT}(f) = y^2xz^3.$$

Definition 2.4.6. Let I be an ideal in a polynomial ring R, the ideal generated by the leading monomials of all polynomials of I is called the **initial ideal** and denoted $\mathrm{in}(I) = \langle \mathrm{LM}(f) \mid f \in I \rangle$. We will write $\mathrm{in}_>(I)$ if we would like to emphasize the monomial order used.

The following is known as Dickson's Lemma:

Lemma 2.4.7. *Every monomial ideal is generated by finitely many monomials.*

Proof. Let G be a set of monomials (may not be a finite set) generating the ideal $I = \langle g \mid g \in G \rangle$ in the polynomial ring $R = \mathbb{K}[x_1, \ldots, x_n]$. Without loss of generality we may assume G consists of minimal elements with respect to divisibility, which means that if two monomials $x, y \in G$ such that $x \mid y$, then we exclude y from the set G. We see that

$$I = \langle I_0 \cup x_1 I_1 \cup x_1^2 I_2 \cup x_1^3 I_3 \cup \cdots \rangle, \text{ where } I_i \text{ ideals in } \mathbb{K}[x_2, \ldots, x_n]$$

such that

$$\{x_1^i \mathbf{x}^{\beta_2 \cdots \beta_n} \mid \mathbf{x}^{\beta_2 \cdots \beta_n} \in \mathrm{in}(I_i)\} = \{\mathbf{x}^{\alpha_1 \alpha_2 \cdots \alpha_n} \in \mathrm{in}(I) \mid \alpha_1 = i\}.$$

We do induction on n. It is obvious that the result is true for $n = 1$. If $n > 1$, we assume that result is true for $n - 1$. Thus, $I_i \subset K[x_2, \ldots, n]$ is generated by G_i consisting finitely many monomials, for $i = 0, \ldots, n$.

Since $I_1 \subseteq I_2 \subseteq \cdots$ is an ascending chain of ideals in a Noetherian ring, there is a maximal element. Let I_k be the maximal element such that $I_1 \subseteq I_2 \subseteq \cdots \subset I_k = I_{k+1} = \cdots$. Thus, we have

$$\begin{aligned} I &= \langle I_0 \cup x_1 I_1 \cup x_1^2 I_2 \cup x_1^3 I_3 \cup \cdots x^k I_k \rangle \\ &= \langle G_0 \cup x_1 G_1 \cup x_1^2 G_2 \cup x_1^3 G_3 \cup \cdots x^k G_k \rangle. \end{aligned}$$

Hence I is generated by finitely many monomials. □

Definition 2.4.8. Let $\mathbb{K}[x_0, x_1, \ldots, x_n]$ be a polynomial ring. Suppose $I = \langle f_1, \ldots, f_m \rangle$ is an ideal of R. For a fixed monomial order, a finite subset $G = \{g_1, \cdots, g_s\}$ of an ideal I is said to be a **Gröbner basis** if

$$\langle \mathrm{LT}(g_1), \cdots, \mathrm{LT}(g_s) \rangle = \langle \mathrm{LT}(I) \rangle,$$

where $\langle \mathrm{LT}(I) \rangle$ is the ideal generated by the leading terms of all the elements in I.

The process for calculating this basis is known as Buchberger's Algorithm. For details, see [Page 84, [Cla04], Page 108-110, [CLO95]]. This algorithm, while relatively easy to understand, is not usually conducive to hand computation, so a Computer Algebra System is the means by which a Gröbner basis is most often calculated.

Example 2.4.9. This example is shown in [Page 75, [CLO95]]. Assume Lex order with $x > y$. Let $f, g \in R = \mathbb{C}[x, y]$ and $\{f, g\} = \{x^3 - 2xy, x^2y - 2y^2 + x\}$. We claim $\{f, g\}$ is not a Gröbner basis for $I = \langle f, g \rangle$. Since

$$\begin{aligned} xg - yf &= x(x^2y - 2y^2 + x) - y(x^3 - 2xy) \\ &= x^3y - 2xy^2 + x^2 - x^3y - 2xy^2 \\ &= x^2, \end{aligned}$$

then $x^2 \in \langle \mathrm{LT}(I) \rangle$, but $x^2 \notin \langle \mathrm{LT}(f), \mathrm{LT}(g) \rangle = \langle x^3, x^2y \rangle$.

We can find the Gröbner basis for I by using the following command in Mathematica [Wol15]:

$$\mathrm{GroebnerBasis}[\{x^3 - 2xy, x^2y - 2y^2y + x\}, \{x, y\}],$$

and the Gröbner basis for I is

$$\{-y^4 + 2y^7 - 4y^8 + 2y^9, x - 2y^3 + 4y^5 - 8y^6 + 4y^7\}$$

Theorem 2.4.10 (Corollary 6, Page 76; Theorem 2, Page 89; [CLO95])**.** *Fix a monomial order. Then every nonzero ideal $I \subset k[x_1, \cdots, x_n]$ has a Gröbner basis. Any Gröbner basis of an ideal I is a basis for I. Furthermore, the Gröbner basis can be constructed by Buchberger's Algorithm.*

We will sketch out Buchberger algorithm below. The detailed treatment can be find in [CLO95] and [TB93]. Before we introduce the algorithm, let us first recall a notion involved all the stages of finding the Gröbner basis process.

Given a set of generators for a polynomial ideal, one can obtain a Gröbner basis with respect to some monomial order via Buchberger's algorithm. The method was invented by Austrian mathematician Bruno Buchberger, which can be viewed as a generalization of the Euclidean algorithm for univariate GCD computation and of Gaussian elimination for linear systems. One of the key components of the algorithm is the polynomial reduction, the most computationally intensive part of the algorithm. The *polynomial reduction* can be viewed as a generalized division. In general, a polynomial g reduces to another polynomial h modulo a set of polynomials $F = \{f_1, \ldots, f_m\}$, denoted by $g \to_F h$, if and only if there exists $f \in F$ such that the $\mathrm{LT}(g)$ can be eliminated by the subtraction of an appropriate multiple of f, i.e., $h = \frac{\mathrm{LCM}\{\mathrm{LT}(g),\mathrm{LT}(f)\}}{\mathrm{LT}(g)} g - \frac{\mathrm{LCM}\{\mathrm{LT}(g),\mathrm{LT}(f)\}}{\mathrm{LT}(f)} f$ where $\deg h < \deg g$. Polynomial g is called *irreducible modulo* F if no leading monomial of an element of F divides the leading monomial of g. On the other hand if g is reducible modulo F then we can subtract from it a multiple of an element of F to eliminate its leading monomial and to get a new leading monomial less than the leading monomial of g. This new polynomial is equivalent to g with respect to the ideal generated by F.

Example 2.4.11. Consider lexical order with $x > y$, and $F = \{f_1, f_2\}$, where

$$f_1 = xy - 1,\ f_2 = y^2 - 1,\ g = x^2y + xy^2 + y^2.$$

Then,

$$g = (x + y)f_1 + 1 \cdot f_2 + (x + y + 1),\ \text{ let } h = x + y + 1.$$

Hence,

$$g \to_F h,\ \text{ where } h = x + y + 1.$$

Algorithm 2.4.12. Buchberger's Algorithm:
Input: A set of polynomials $F = \{f_1, \ldots, f_m\}$ that generates the ideal I in the polynomial ring $\mathbb{K}[x_1, \ldots, x_n]$ over some field $\mathbb{K}$.
Output: A Gröbner basis G for I

step 1. $G := F$;

step 2. For every $f_i, f_j \in G$, let $a_{ij} = \mathrm{LCM}\{\mathrm{LT}(f_i), \mathrm{LT}(f_j)\}$ with respect to the given ordering;

step 3. Choose two polynomials in G and let $S_{ij} = \frac{a_{ij}}{\mathrm{LT}(f_i)} f_i - \frac{a_{ij}}{\mathrm{LT}(f_j)} f_j$;

step 4. Reduce S_{ij} with the multivariate division algorithm relative to the set G until the result is not further reducible. If the result is non-zero, add it to G;

step 5. Repeat steps 1-4 until all possible pairs are considered, including those involving the new polynomials added in step 4.

The polynomial S_{ij} is commonly referred to as the **S-polynomial** . The algorithm terminates by the Hilbert basis theorem. Sometimes, Gröbner bases can be extremely large, and hard to compute.

Example 2.4.13. Consider lexical order with $x > y$, the ideal $I = \langle f_1, f_2 \rangle$ with

$$f_1 = 2x^2 - 4x + y^2 - 4y + 3,\ f_2 = x^2 - 2x + 3y^2 - 12y + 9.$$

Since

$$S_{12} = \frac{-5}{2}y^2 + 10y - \frac{15}{2}$$

and the remainder on dividing f_1, f_2 is still S_{12}, we let

$$f_3 = S_{12} = \frac{-5}{2}y^2 + 10y - \frac{15}{2}.$$

Now,

$$\begin{aligned} S_{13} &= 4x^2y - 3x^2 - 2xy^2 + \frac{y^4}{2} - 2y^3 + \frac{3y^2}{2} \\ &= \left(2y - \frac{3}{2}\right) f_1 + \left(\frac{4x}{5} - \frac{y^2}{5} + \frac{4y}{5} - \frac{3}{5}\right) f_3, \\ S_{23} &= 4x^2y - 3x^2 - 2xy^2 + 3y^4 - 12y^3 + 9y^2 \\ &= \left(2y - \frac{3}{2}\right) f_1 + \left(\frac{4x}{5} - \frac{6y^2}{5} + \frac{4y}{5} - \frac{3}{5}\right) f_3. \end{aligned}$$

Hence the Gröbner basis $G = \{f_1, f_2, f_3\}$.

It is easy to see that if $F = \{f_1, \ldots, f_m\}$ is a finite set of polynomials, and I is the ideal generated by F, then the following are equivalent:

1. F is a Gröbner basis;
2. For all i, j, $S_{ij} \to_F 0$, i.e., the S-polynomial of f_i, f_j reduces to zero modulo F;
3. Any $f \in I$, $f \to_F 0$, i.e., any f of I reduces to zero modulo F.

2.5 Elimination and Extension

In commutative algebra and algebraic geometry, elimination theory is the classical name for algorithmic approaches to eliminating some variables between polynomials of several variables. One of the important applications in elimination theory is to find the implicit equations of a given set of parametric expressions.

Definition 2.5.1. Let $I = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{K}[x_1, \ldots, x_n]$. The **$\ell$-th elimination ideal** I_ℓ is the ideal of $\mathbb{K}[x_{\ell+1}, \ldots, x_n]$ defined by

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

Theorem 2.5.2. (Elimination Theorem) *Let $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be an ideal, and let G be a Gröbner basis of I with respect to lex order where $x_1 > x_2 > \cdots > x_n$. Then, for every $0 \leq \ell \leq n$, the set*

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

is a Gröbner basis of the ℓ-th elimination idea I_ℓ.

Proof. Fix ℓ. By definition of Gröbner basis, it suffices to show that

$$\langle \mathrm{LT}(I_\ell) \rangle = \langle \mathrm{LT}(G_\ell) \rangle.$$

By construction, $G_\ell \subset I_\ell$, we only need to show that $\langle \mathrm{LT}(I_\ell) \rangle \subseteq \langle \mathrm{LT}(G_\ell) \rangle$. Let $f \in I_\ell \subset I$, then $f \in I$ shows $\mathrm{LT}(f)$ is divisible by some $\mathrm{LT}(g)$ for some $g \in G$, and $f \in I_\ell$ yields that $\mathrm{LT}(f)$ involves only the variables $x_{\ell+1}, \ldots, x_n$. Using lex order with $x_1 > x_2 > \ldots > x_n$, we must have that $\mathrm{LT}(g) \in \mathbb{K}[x_{\ell+1}, \ldots, x_n]$, hence $g \in \mathbb{K}[x_{\ell+1}, \ldots, x_n]$, and thus we proved theorem. □

Let us restrict our attention to the case where we eliminate just the first variable x_1. We want to know if a partial solution $(a_2, \ldots, a_n) \in \mathbb{V}(I_1)$ can be extended to a solution $(a_1, a_2, \ldots, a_n) \in \mathbb{V}(I)$. We note that if $f, g \in \mathbb{K}[x_1, \ldots, x_n]$, then we can write

$$f = a_0 x_1^\ell + \cdots + a_\ell, \quad a_0 \neq 0, \tag{2.1}$$
$$g = b_0 x_1^m + \cdots + b_m, \quad b_0 \neq 0, \tag{2.2}$$

where $a_i, b_i \in \mathbb{K}[x_2, \ldots, x_n]$. Now we use what we learned about resultants:

Proposition 2.5.3. *Let $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ have positive degree in x_1. Then:*

1. *$Res(f, g, x_1)$ is in the first elimination ideal $\langle f, g\rangle \cap \mathbb{K}[x_1, \ldots, x_n]$,*
2. *$Res(f, g, x_1) = 0$ if and only if f, g have a common factor in $\mathbb{K}[x_1, \ldots, x_n]$ which has a positive degree in x_1.*

We will prove the extension theorem by relating the resultants and the partial solutions.

Proposition 2.5.4. *$f, g \in \mathbb{C}[x_1, \ldots, x_n]$ have degree ℓ, m in x_1 respectively, and let $\mathbf{c} = (c_2, \ldots, c_n) \in \mathbb{C}^{n-1}$ satisfy the following conditions:*

1. *$f(x_1, \mathbf{c}) \in \mathbb{C}[x_1]$ has degree ℓ,*
2. *$g(x_1, \mathbf{c}) \in \mathbb{C}[x_1]$ has degree $p \leq m$.*

Then the polynomial $h = Res(f, g, x_1) \in \mathbb{C}[x_2, \ldots, x_n]$ satisfies $h(\mathbf{c}) = a_0(\mathbf{c})^{m-p} Res(f(x_1, \mathbf{c}), g(x_1, \mathbf{c}), x_1)$ where a_0 is in Equation (2.1).

Proof. Substituting $\mathbf{c} = (c_2, \ldots, c_n)$ in place of $x_2, \ldots, x_n$ in the $\mathrm{Res}(f, g, x_1)$, we obtain

$$h(\mathbf{c}) = \det \begin{bmatrix} a_0(\mathbf{c}) & & & & b_0(\mathbf{c}) & & & \\ a_1(\mathbf{c}) & a_0(\mathbf{c}) & & & b_1(\mathbf{c}) & b_0(\mathbf{c}) & & \\ a_2(\mathbf{c}) & a_1(\mathbf{c}) & \ddots & & b_2(\mathbf{c}) & b_1(\mathbf{c}) & \ddots & b_0(\mathbf{c}) \\ \vdots & \vdots & \ddots & a_0(\mathbf{c}) & \vdots & \vdots & \ddots & \vdots \\ a_\ell(\mathbf{c}) & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ & a_\ell(\mathbf{c}) & \ddots & \vdots & b_m(\mathbf{c}) & \vdots & \ddots & \vdots \\ & & \ddots & \vdots & & b_m(\mathbf{c}) & \ddots & \vdots \\ & & & a_\ell(\mathbf{c}) & & & & b_m(\mathbf{c}) \end{bmatrix}.$$

If $\deg(g(x_1, \mathbf{c})) = p = m$, then $h(\mathbf{c}) = \mathrm{Res}(f(x_1, \mathbf{c}), g(x_1, \mathbf{c}), x_1)$. On the other hand, if $\deg(g(x_1, \mathbf{c})) = p < m$, then $h(\mathbf{c}) \neq \mathrm{Res}(f(x_1, \mathbf{c}), g(x_1, \mathbf{c}), x_1)$, but we can obtain the desired resultant by repeatedly expanding along the first row. □

In the following, we take $\mathbb{K} = \mathbb{C}$, but any algebraically closed field will do.

Theorem 2.5.5. (The Extension Theorem) *Let $I = \langle f_1, \ldots, f_s\rangle \subseteq \mathbb{C}[x_1, \ldots, x_n]$, and I_1 the first elimination ideal of I. For each $1 \leq i \leq s$, we write*

$$f_i = g_i(x_2, \ldots, x_n) x_1^{N_i} + \text{ terms in which } x_1 \text{ has degree } < N_i,\ g_i \neq 0,\ N_i \geq 0.$$

Suppose we have a partial solution $(a_2, \ldots, a_n) \in \mathbb{V}(I_1)$. *If* $(a_2, \ldots, a_n) \notin \mathbb{V}(g_1, \ldots, g_s)$, *then there exists* $a_1 \in \mathbb{C}$ *such that* $(a_1, a_2, \ldots, a_n) \in \mathbb{V}(I)$.

Proof. Here we only give a sketch of the proof. First, let $\mathbf{c} = (c_2, \ldots, c_n)$ and note that we have a ring homomorphism

$$\mathbb{C}[x_1, \ldots, x_n] \to \mathbb{C}[x_1] \text{ defined by } f(x_1, \ldots, x_n) = f(x_1, \mathbf{c}).$$

The image of the ideal I is an ideal in $\mathbb{C}[x_1]$ generated $g(x_1) \in \mathbb{C}[x_1]$. If $g(x_1)$ is a non-constant polynomial, by Fundamental Theorem of Algebra, there exists $c_1 \in \mathbb{C}$ such that $g(c_1) = 0$, which yields that $f(c_1, \mathbf{c}) = 0$ for all $f \in I$. Thus, $(c_1, \mathbf{c}) = (c_1, c_2, \ldots, c_n) \in \mathbb{V}(I)$. Now, we will show that it is impossible for $g(x_1)$ to be a non-zero constant. Suppose the contrary, and we will deduce a contradiction. Because of the form of f_i, there must be some $f \in I$ such that $f(x_1, \mathbf{c}) = g(x_1) = k$, a non-zero constant.

By the given condition $\mathbf{c} \notin \mathbb{V}(g_1, \ldots, g_s)$, there must be an index i such that $g_i(\mathbf{c}) \neq 0$. Consider

$$h = \text{Res}(f_i, f, x_1) \in \mathbb{C}[x_2, \ldots, x_n],$$

Apply Proposition 2.5.4, we have

$$h(\mathbf{c}) = g_i(\mathbf{c})^{\deg f} \text{Res}(f_i(x_1, \mathbf{c}), f(x_1, \mathbf{c}), x_1) = g_i(\mathbf{c})^{\deg f} k^N \neq 0.$$

But this contradicts the fact that $h \in I_1$, and $\mathbf{c} \in \mathbb{V}(I_1)$. Thus, it is impossible for $g(x_1)$ to be a non-zero constant.

Hence, we can always extend the partial solution. □

The Extension Theorem tells us that the extension step can fail only when the leading coefficients vanish simultaneously. The variety $\mathbb{V}(g_1, \ldots, g_s)$ where the leading coefficient vanish depends on the basis $\{f_1, \ldots, f_s\}$ of I. There is a method to choose $\{f_1, \ldots, f_s\}$ so that $\mathbb{V}(g_1, \ldots, g_s)$ is as small as possible.

As an application of Gröbner bases, we will find the implicit equations of a set of polynomial parametric equations.

Given a set of parametric expression in $t_1, \ldots, t_m$,

$$\begin{aligned} x_1 &= f_1(t_1, \cdots, t_m) \\ &\vdots \\ x_n &= f_n(t_1, \cdots, t_m) \end{aligned}$$

with Lex order $t_1 > \cdots > t_m > x_1 > \cdots > x_n$ in $\mathbb{K}[t_1, \cdots, t_m, x_1, \cdots, x_n]$. Consider the ideal

$$\tilde{I} = \langle x_1 - f_1(t_1, \cdots, t_m), \cdots, x_n - f_n(t_1, \cdots, t_m) \rangle \subset k[t_1, \cdots, t_m, x_1, \cdots, x_n].$$

The Gröbner basis of the m-th elimination ideal give the implicit equations for the variables $x_1, ..., x_n$.

Example 2.5.6. Consider the parametric equations:

$$\begin{aligned} x &= t^2 - 1, \\ y &= t(t^2 - 1), \end{aligned}$$

Assume the lex order in the ring $\mathbb{C}[x, y, t]$ is $t > x > y$.

$$\tilde{I} = \langle x - (t^2 - 1), y - t(t^2 - 1) \rangle$$

Using Mathematica [Wol15], we find the Gröbner basis of the ideal is:

$$\{x^2 + x^3 - y^2, -x - x^2 + ty, tx - y, 1 - t^2 + x\},$$

and the implicit equation is:

$$y^2 - x^2 - x^3 = 0.$$

To demonstrate why the above algorithm really works, we need to understand the geometry behind the Gröbner basis method. We start by introducing basic terminology of algebraic geometry. Later in Section **??** we will relate this to the theory of schemes.

Definition 2.5.7. Let $\mathbb{K}$ be an algebraically closed field.

1. Let $I = \langle f_1, ..., f_s \rangle \subset \mathbb{K}[x_1, \cdots, x_n]$ be an ideal. Define

$$\mathbb{V}(I) = \{(a_1, \cdots, a_n) \in \mathbb{K}^n : f(a_1, \cdots, a_n) = 0, \quad \forall f \in I\}.$$

Note that this is the same set as

$$\mathbb{V}(f_1, \cdots, f_s) = \{(a_1, \cdots, a_n) \in \mathbb{K}^n : f_i(a_1, \cdots, a_n) = 0, \quad 1 \leq i \leq s\}.$$

This is called the **affine variety** defined by $f_1, \cdots, f_s$, or by the ideal I. If the polynomials f_i have coefficients belonging to a subfield $k \subset \mathbb{K}$, we say that this variety is defined over k. The map $I \mapsto \mathbb{V}(I)$ is order-reversing.

2. Let $X \subset \mathbb{K}^n$ be a subset. Define

$$\mathbb{I}(X) = \{f \in \mathbb{K}[x_1, ..., x_n] : f(x) = 0,\ \forall x \in X\}.$$

This is an ideal in $\mathbb{K}[x_1, ..., x_n]$. The map $X \mapsto \mathbb{I}(X)$ is order-reversing.

3. The sets $\mathbb{V}(I)$ with I ranging over the ideals of $\mathbb{K}[x_1, ..., x_n]$ form a topology on the set $\mathbb{K}^n$ called the **Zariski topology**. This topology is coarse in the sense that it is rarely Hausdorff, but it is **quasicompact**, i.e., any cover of $\mathbb{K}^n$ has a finite subcover.

4. We have

   a. $\mathbb{V}(\mathbb{I}(X)) = \bar{X}$, closure in the Zariski topology.
   b. $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$, Hilbert's Nullstellensatz .

5. The assignments $I \mapsto \mathbb{V}(I)$ and $X \mapsto \mathbb{I}(X)$ set up an order-reversing bijection between the sets

$$\{\text{radical ideals in } \mathbb{K}[x_1, ..., x_n]\} \leftrightarrow \{\text{affine subvarieties of } \mathbb{K}^n\}.$$

6. If $X = \mathbb{V}(I) \subset \mathbb{K}^n$ is an affine variety, the ring

$$\mathbb{K}[X] = \mathbb{K}[x_1, ..., x_n]/\sqrt{I}$$

is called the affine coordinate ring of X. It is a reduced $\mathbb{K}$-algebra of finite type, and every reduced $\mathbb{K}$-algebra of finite type is the affine coordinate ring of an affine variety.

7. If $X \subset \mathbb{K}^n$ and $Y \subset \mathbb{K}^m$ are affine varieties, a morphism $f : X \to Y$ is a map induced by polynomials $f_1(x_1, ..., x_n), ..., f_m(x_1, ..., x_n)$. This sets up a bijection

$$\text{Hom}_{\text{varieties}}(X, Y) = \text{Hom}_{\mathbb{K}-\text{algebras}}(\mathbb{K}[Y], \mathbb{K}[X]),$$

given by

$$f \mapsto (g(y_1, ..., y_m) \mapsto g(f_1(x_1, ..., x_n), ..., f_m(x_1, ..., x_n))).$$

Example 2.5.8. Let us consider several varieties defined over $\mathbb{R}$. As is usual, we only draw the $\mathbb{R}$-valued points:

$$\mathbb{V}_1(x^2 + y^2 - 1) = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 - 1 = 0\},$$

$$\mathbb{V}_2 = \mathbb{V}(y - x^2) = \{(x, y) \in \mathbb{R}^2 : y - x^2 = 0\},$$

$$\mathbb{V}_3 = \mathbb{V}(x^2 + y^2 - 1, y - x^2) = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 - 1 = 0, \quad y - x^2 = 0\}.$$

$\mathbb{V}_1$ and $\mathbb{V}_2$ are represented by the first two graphs, the unit circle and the parabola in the real plane, in Figure 2.1 below. But $\mathbb{V}_3 = \mathbb{V}_1 \cap \mathbb{V}_2$ is the two points of intersection of the unit circle and the parabola, which is given as the last graph in Figure 2.1.

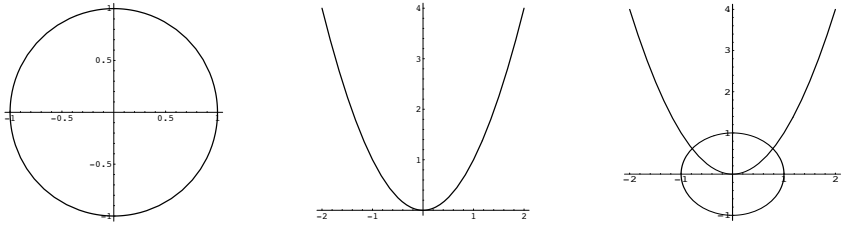


Figure 2.1: $\mathbb{V}(x^2 + y^2 - 1)$, $\mathbb{V}(y - x^2)$, and $\mathbb{V}(x^2 + y^2 - 1, y - x^2)$

Example 2.5.9. Consider $V = \{(1)\} \subset \mathbb{K}$. Then $\mathbb{I}(V) = \langle x - 1 \rangle$. This can be observed if $f \in \langle x - 1 \rangle$, then $f = A(x)(x - 1)$, and $f(1) = 0$, therefore, $f \in \mathbb{I}(V)$. On the other hand, if $f \in \mathbb{I}(V)$, then $f(1) = 0$, and $(x - 1)|f$. Thus $f \in \langle x - 1 \rangle$.

Definition 2.5.10. Given $V = \mathbb{V}(f_1, \cdots, f_s) \subset \mathbb{C}^n$, we define the *projection map* as follows:

$$\pi_\ell : \mathbb{C}^n \to \mathbb{C}^{n-\ell}$$

$$(a_1, \cdots, a_n) \to (a_{\ell+1}, \cdots, a_n).$$

$$\pi_\ell(V) \subset \mathbb{C}^{n-\ell}.$$

Example 2.5.11. Let $V = \mathbb{V}(xy - 1) = \{(a, 1/a) \in \mathbb{C}^2 : a \neq 0\}$, $\pi_1(V) = \{1/a \in \mathbb{C} : a \neq 0\}$. In Figure 2.2 below, the graph projects to the y-axis. $\pi_1(V)$ is the y-axis without origin. Moreover, if we let $I = \langle xy - 1, xz - 1 \rangle \subset \mathbb{C}[x, y, z]$, and fix a lex order with $x > y > z$, then Mathematica [Wol15] gives the Gröbner basis of the ideal as

$$G = \{-y + z, -1 + xz\}, \; G_1 = G \cap \mathbb{C}[y, z] = \{-y + z\}, \; I_1 = \langle -y + z \rangle.$$

Theorem 2.5.12. *If $V = \mathbb{V}(I)$, then $\pi_\ell(V) \subset \mathbb{V}(I_\ell)$.*

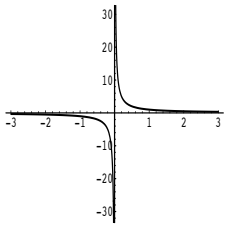


Figure 2.2: Projection

Proof. Let $(a_1, \ldots, a_n) \in V = \mathbb{V}(I)$, then $(a_{\ell+1}, \ldots, a_n) \in \pi_\ell(V)$. To show $\pi_\ell(V) \subset V(I_\ell)$ is to show that $f(a_{\ell+1}, \ldots, a_n) = 0$ for all $f \in I_\ell$.

Let $f \in I_\ell \subset I$, then $f \in I$ shows that $f(a_1, \ldots, a_n) = 0$, and $f \in I_\ell$ means that $f \in \mathbb{K}[x_{\ell+1}, \ldots, x_n]$. Hence,

$$f(a_{\ell+1}, \ldots, a_n) = f(\pi_\ell(a_1, \ldots, a_n)) = 0.$$

Therefore, f vanishes at all points on $\pi_l(V)$. Thus, we have shown $\pi_\ell(V) \subset \mathbb{V}(I_\ell)$. □

Theorem 2.5.13. (The Closure Theorem) *Let $V = \mathbb{V}(f_1, \cdots, f_s) \subset \mathbb{C}^n$, and I_ℓ the ℓ-th elimination ideal of $\langle f_1, \cdots, f_s \rangle$. Then:*

1. *$\mathbb{V}(I_\ell)$ is the smallest affine variety containing $\pi_\ell(V) \subset \mathbb{C}^{n-\ell}$.*
2. *When $V \neq \emptyset$, there is an affine variety $W \subset \mathbb{V}(I_\ell)$ such that $\mathbb{V}(I_\ell) - W \subset \pi_\ell(V)$.*

Proof. For details see [Theorem 3, page 123,[CLO95]] □

We will use the following example to illustrate the Closure Theorem.

Example 2.5.14. If $I = \langle xy - 1, xz - 1 \rangle \subset \mathbb{C}[x, y, z]$, then by Gröbner basis calculation, we obtain that

$$I_1 = \langle -y + z \rangle, \quad \text{therefore,} \quad \mathbb{V}(I_1) = \{(a, a) \in \mathbb{C}^2\}.$$

The graph on the left in Figure 2.3 below shows $\mathbb{V}(I)$ and the graph on the right in Figure 2.3 shows the first projection map $\pi_1(V)$. This map projects to the y, z-plane without the origin. Note that $\pi_1(V)$ is contained in $\mathbb{V}(I_1)$, and the missing point is the origin.

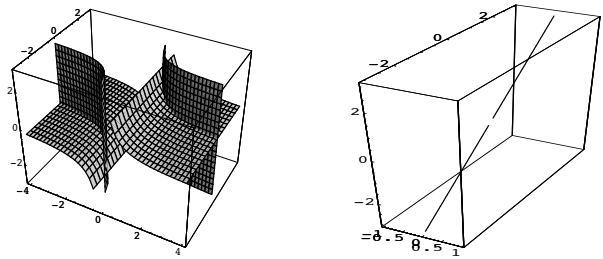


Figure 2.3: $V = \mathbb{V}(I)$ and $\pi_1(V) = \{(a, a) \neq (0, 0) \in \mathbb{C}^2\}$

2.6 Implicitization

Now, we have the necessary background knowledge to understand the Gröbner basis method for elimination, we return to our original goal of finding the implicit equation of the following polynomial parametrization in $\mathbb{C}^n$ given by $x_i = f_i(t_1, \cdots, t_m)$ for $i = 1, \ldots, n$, where each $f_i \in \mathbb{C}[t_1, \cdots, t_m]$. Geometrically, we can think of this as the function:

$$F : \mathbb{C}^m \to \mathbb{C}^n$$

$$F(t_1, \cdots, t_m) = (f_1(t_1, \cdots, t_m), \cdots, f_n(t_1, \cdots, t_m)).$$

The image $F(\mathbb{C}^m) \subset \mathbb{C}^n$ is parametrized by the above equation. $F(\mathbb{C}^m)$ may not be an affine variety. The implicitization problem is to find the smallest affine variety that contains $F(\mathbb{C}^m)$. The elimination theorem helps us to find implicit equations (for information see [Page 127, [CLO95]]). Set

$$V = \mathbb{V}(x_1 - f_1, \cdots, x_n - f_n) \subset \mathbb{C}^{n+m}.$$

Points of V can be written in the form:

$$(t_1, \cdots, t_m, f_1(t_1, \cdots, t_m), \cdots, f_n(t_1, \cdots, t_m)).$$

Let us consider the following maps:

$$\mathbb{C}^m \xrightarrow{\ i\ } \mathbb{C}^{m+n} \xrightarrow{\ \pi\ } \mathbb{C}^n.$$

The first is the inclusion map,

$$i(t_1, \cdots, t_m) = ((t_1, \cdots, t_m, f_1(t_1, \cdots, t_m), \cdots, f_n(t_1, \cdots, t_m));$$

and the second one is a projection map

$$\pi_m(t_1, \cdots, t_m, x_1, \cdots, x_n) = (x_1, \cdots, x_n).$$

Therefore, F is the composition of these two maps, and

$$F(\mathbb{C}^m) = \pi_m(i(k^m)) = \pi_m(V).$$

If we let I be the ideal

$$I = \langle x_1 - f_1, \cdots, x_n - f_n \rangle \subset \mathbb{C}[t_1, \cdots, t_m, x_1, \cdots, x_n],$$

and let

$$I_m = I \cap k[x_1, \cdots, x_n]$$

be the m-th elimination, then $\mathbb{V}(I_m)$ is the smallest variety in $\mathbb{C}^n$ containing $\pi_m(V) = F(\mathbb{C}^m)$. Therefore, to find the implicit equation is to find the m-th elimination ideal. So in summary, to find the implicit equation via the Gröbner basis method is to find the m-th elimination ideal, which is the ideal generated by those polynomials in the Gröbner basis that do not contain the parameters.

Theorem 2.6.1. (Polynomial Implicitization) *If $\mathbb{K}$ is an infinite field, let $F : \mathbb{K}^m \to \mathbb{K}^n$ be the function determined by the polynomial parametrization*

$$\begin{aligned} x_1 &= f_1(t_1, \cdots, t_m) \\ &\vdots \\ x_n &= f_n(t_1, \cdots, t_m). \end{aligned}$$

Let $I = \langle x_1 - f_1, \ldots, x_n - f_n \rangle$ be an ideal of the ring $\mathbb{K}[t_1, \ldots, t_m, x_1, \ldots, x_n]$, and $I_m = I \cap \mathbb{K}[x_1, \ldots, x_n]$ the m-th elimination ideal. Then $\mathbb{V}(I_m)$ is the smallest variety in $\mathbb{K}^n$ containing $F(\mathbb{K}^m)$.

Example 2.6.2. Let us find the implicit equation of the parametrized surface S given by:

$$\begin{aligned} x &= uv \\ y &= uv^2 \\ z &= u^2 \end{aligned}$$

$$I = \langle x - uv, y - uv^2, z - u^2 \rangle.$$

Using lex order $u > v > x > y > z$, the Gröbner basis G for I is

$$\{x^4 - y^2z, -x^3 + vyz, vx - y, x^2 - v^2z, -x^2 + uy, -ux + x, -u^2 + z\}$$

To eliminate our parameters u, v, we find G_2 and the 2nd elimination ideal I_2 to be:

$$G_2 = G \cap k[x, y, z] = \{x^4 - y^2z\}$$
$$I_2 = \langle x^4 - y^2z \rangle,$$

so the implicit equation for the surface is $x^4 - y^2z = 0$. Figure 2.4 below shows the implicit equation of the surface. Please note that $(0, 1, 0)$ is on $\mathbb{V}(I_2)$, but not on S.

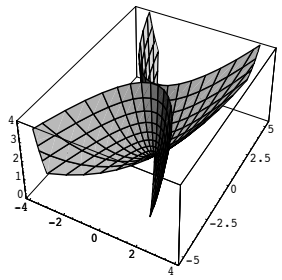


Figure 2.4: $\mathbb{V}(x^4 - y^2z)$

In a more general setting of rational parametrization, $x_i = \frac{f_i}{g_i}$ for $i = 1, \ldots, n$. If $W = \mathbb{V}(g_1 \cdots g_n)$, then this defines a map

$$F(t_1, \ldots, t_m) = \left(\frac{f_1(t_1, \cdots, t_m)}{g_1(t_1, \ldots, t_m)}, \ldots, \frac{f_n(t_1, \cdots, t_m)}{g_n(t_1, \ldots, t_m)} \right) : \mathbb{K}^m - W \to \mathbb{K}^n.$$

The *implicitization problem* is to find the smallest variety containing $F(\mathbb{K}^m - W)$. We obtain the following theorem for rational parametrization.

Theorem 2.6.3. (Rational Implicitization) *Let $\mathbb{K}$ be an infinite field, let $F : \mathbb{K}^m \setminus W \to \mathbb{K}^n$ be the function determined by a rational parametrization*

$$\begin{aligned} x_1 &= \frac{f_1(t_1, \cdots, t_m)}{g_1(t_1, \ldots, t_m)}, \\ &\vdots \\ x_n &= \frac{f_n(t_1, \cdots, t_m)}{g_n(t_1, \ldots, t_m)}. \end{aligned}$$

Let ideal $J = \langle x_1 g_1 - f_1, \ldots, x_n g_n - f_n, 1 - gy \rangle \subseteq \mathbb{K}[y, t_1, \ldots, t_m, x_1, \ldots, x_n]$, *where* $g = g_1 \cdots g_n$, *and* $W = \mathbb{V}(g)$. *Let* $J_{m+1} = J \cap \mathbb{K}[x_1, \ldots, x_n]$ *be the* $(m+1)$*-th elimination ideal of* I. *Then* $\mathbb{V}(J_{m+1}$ *is the smallest variety containing* $F(\mathbb{K}^m - W)$.

Proof. See [Page 134, Theorem 2, [CLO95]] for the detailed proof. □

2.7 Schemes

We briefly recall the ideas of schemes and sheaves, which are essential to modern algebraic geometry. A standard reference is [Har97].

Definition 2.7.1. If A is a commutative ring, then $\mathrm{Spec}(A)$ is the set of prime ideals of A. We let $\mathrm{Max}(A) \subset \mathrm{Spec}(A)$ be the subset of maximal ideals. We define the **Zariski topology** on $X = \mathrm{Spec}(A)$ by declaring that a subset $Z \subset X$ is closed if and only if $Z = \mathbb{V}(I)$ for an ideal $I \subset A$ where

$$\mathbb{V}(I) = \{\mathfrak{p} \mid \mathfrak{p} \supset I\}.$$

Sometimes to distinguish between $\mathfrak{p}$ as a prime ideal in A and $\mathfrak{p}$ as a point in X, we use the notation $x = [\mathfrak{p}]$. $\mathrm{Max}(A)$ inherits a topology as a subset of $\mathrm{Spec}(A)$. One proves:

1. The $\mathbb{V}(I)$ for I ranging over the ideals of A do satisfy the axioms for closed sets in a topological space.
2. $\mathbb{V}(I) = V(J)$ if and only if $\sqrt{I} = \sqrt{J}$.
3. The sets
$$X_a = X \setminus \mathbb{V}(a) = \{x = [\mathfrak{p}] \mid a \notin \mathfrak{p}\}$$
as a ranges through the elements of A form a basis of open sets for the Zariski topology.
4. Let $\varphi : A \to B$ be a ring homomorphism. There is a map
$$f : Y = \mathrm{Spec}(B) \longrightarrow X = \mathrm{Spec}(A), \quad y = [\mathfrak{q}] \mapsto [\varphi^{-1}\mathfrak{q}] = f(y);$$
that is, if $\mathfrak{q}$ is a prime ideal of B, then $\varphi^{-1}\mathfrak{q}$ is a prime ideal of A. This map is continuous. On basic open sets we have, for all $a \in A$,
$$f^{-1}(X_a) = Y_{\varphi(a)}.$$

5. For all $a \in A$, if A_a is the localization of A in the multiplicative set $\{1, a, a^2, ...\}$, the natural map $A \to A_a$ induces a map $\mathrm{Spec}(A_a) \to \mathrm{Spec}(A)$. This map is a homeomorphism onto the open subset X_a. More generally, if $S \subset A$ is any multiplicative set, the natural map $\mathrm{Spec}(S^{-1}A) \to \mathrm{Spec}(A)$ is a homeomorphism onto the subset

$$\{[\mathfrak{p}] \in \mathrm{Spec}(A) \mid \mathfrak{p} \cap S = \emptyset\}.$$

There is a **sheaf** of rings $\mathcal{O}_X$ on X such that the pair $(X, \mathcal{O}_X)$ defines a **scheme**. These terms will be explained later.

Next recall Hilbert's Nullstellensatz.

Theorem 2.7.2. *Let $\mathbb{K}$ be an algebraically closed field, and $A = \mathbb{K}[x_1, ..., x_n]$ a polynomial ring. There is a canonical bijection*

$$\mathbb{K}^n \longrightarrow \mathrm{Max}(A), \quad a = (a_1, ..., a_n) \mapsto \mathfrak{m}_a = \langle x_1 - a_1, ..., x_n - a_n \rangle.$$

More generally, for any ideal $I \subset A$ (finitely generated by Hilbert's basis theorem), the map $a \mapsto \mathfrak{m}_a$ induces a bijection $\mathbb{V}(I) \cong \mathrm{Max}(A/I)$ where

$$\mathbb{V}(I) = \{a \in \mathbb{K}^n \mid g(a) = 0, \textit{for all } g \in I\}.$$

In classical algebraic geometry, one considers sets like $\mathbb{V}(J) \subset \mathbb{K}^n$ and calls them **algebraic varieties** (see 2.5.7). The set $\mathbb{K}^n = \mathbb{A}^n(\mathbb{K})$ is called affine n-space over $\mathbb{K}$, but in the theory of **schemes** we define affine n-space over $\mathbb{K}$ to be $\mathrm{Spec}(\mathbb{K}[x_1, ..., x_n]) = \mathbb{A}^n_{\mathbb{K}}$. (Note the subtle difference in notation. Strictly speaking, we need to define a sheaf of rings on $\mathrm{Spec}(\mathbb{K}[x_1, ..., x_n])$ to give it the structure of a scheme. This will be defined next.) More generally, for any ring k (for instance $k = \mathbb{Z}$) one defines $\mathrm{Spec}(k[x_1, ..., x_n]) = \mathbb{A}^n_k$, which will be a scheme once the sheaf of rings is defined, and $k^n = \mathbb{A}^n(k)$, which is only a set of points. Methodologically, in classical algebraic geometry one usually fixed an algebraically closed field $\mathbb{K}$ and considered varieties as subsets of $\mathbb{K}^n$, or as subsets of projective space $\mathbb{P}^n(\mathbb{K})$, which are solutions to a system of polynomial equations $f = 0$ for all f in some ideal J. In modern algebraic geometry, one usually fixes a ground ring k (or a ground scheme S) and considers, for instance an ideal $J \subset k[x_1, ..., x_n]$ as before, but now one looks at solutions with coordinates in all k-algebras R. If we temporarily call this solution set $\mathrm{Sol}(J; R)$, then we think of the assignment $R \mapsto \mathrm{Sol}(J; R)$ as a **functor** from the category Alg_k of k-algebras to Set, the category of sets. This is an example of the functor of points defined by a scheme.

Definition 2.7.3. Let X be a topological space. A **presheaf** of abelian groups $\mathcal{F}$ on X is an assignment of an abelian group $\mathcal{F}(U)$ for every open subset $U \subset X$. Moreover, for every inclusion of open sets $V \subset U$ there is a homomorphism of abelian groups

$$\mathrm{res}^{\mathcal{F}}_{VU} : \mathcal{F}(U) \longrightarrow \mathcal{F}(V)$$

subject to the axioms

1. For all U, $\mathrm{res}^{\mathcal{F}}_{UU} = \mathrm{Id}_{\mathcal{F}(U)}$;
2. For all $W \subset V \subset U$, $\mathrm{res}^{\mathcal{F}}_{WV} \circ \mathrm{res}^{\mathcal{F}}_{VU} = \mathrm{res}^{\mathcal{F}}_{WU}$.

To simplify notation, the map $\mathrm{res}^{\mathcal{F}}_{VU}$ is often written $s \mapsto s \mid V$ for $s \in \mathcal{F}(U)$. If $x \in X$, the **stalk** at x is the abelian group

$$\mathcal{F}_x = \varinjlim_{x \in U} \mathcal{F}(U),$$

where the direct limit is taken over all the open neighborhoods of U. By definition, the elements of $\mathcal{F}_x$ are equivalence classes of pairs (U, s) where U is an open neighborhood of x and $s \in \mathcal{F}(U)$. The equivalence relation is

$$(U, s) \sim (V, t) \Leftrightarrow \exists W \subset U \cap V, x \in W, \text{such that } s \mid W = t \mid W.$$

There is a homomorphism $s \mapsto s_x : \mathcal{F}(U) \to \mathcal{F}_x$ for all $x \in U$. A **morphism** of sheaves of abelian groups on X, denoted $\alpha : \mathcal{F} \to \mathcal{G}$ is an assignment of a homomorphism of abelian groups $\alpha(U) : \mathcal{F}(U) \to \mathcal{G}(U)$ for every open $U \subset X$, subject to the axiom that for all $W \subset U$, the diagram commutes:

$$\begin{array}{ccc} \mathcal{F}(U) & \xrightarrow{\mathrm{res}^{\mathcal{F}}_{WU}} & \mathcal{F}(W) \\ {\scriptstyle \alpha(U)}\downarrow & & \downarrow{\scriptstyle \alpha(W)} \\ \mathcal{G}(U) & \xrightarrow{\mathrm{res}^{\mathcal{G}}_{WU}} & \mathcal{G}(W) \end{array}$$

Finally, a presheaf is a **sheaf** if $\mathcal{F}(\emptyset) = 0$, and it satisfies the gluing axiom:

3. Given an open set $U \subset X$, a covering of U by open sets U_i, $i \in I$, and for each index i an element $s_i \in \mathcal{F}(U_i)$ with the property that

$$s_i \mid U_i \cap U_j = s_j \mid U_i \cap U_j, \quad \forall i, j,$$

then there exists a unique $s \in \mathcal{F}(U)$ such that $s_i = s \mid U_i$ for all i.

The elements of $\mathcal{F}(U)$ are called **sections** of $\mathcal{F}$ over U.

Remark 2.7.4. 1. Roughly speaking, the gluing condition in the definition of a sheaf $\mathcal{F}$ means that the sections of $\mathcal{F}$ are defined by *local conditions*. For example, let X be any topological space and define a presheaf $\mathbb{R}_X$ on X by the rule that for any open set $U \subset X$

$$\mathbb{R}_X(U) = \{f : U \to \mathbb{R} \mid f \text{ is continuous.}\},$$

with the obvious restriction maps when $V \subset U$. Then $\mathbb{R}_X$ is a sheaf, i.e., the gluing condition holds. The reason is that a function is continuous if and only if it is continuous in a neighborhood of any point in its domain, that is, continuity is a local property.

2. We can define a presheaf of abelian groups on X as a contravariant functor

$$\mathcal{F} : \mathsf{Open}_X^{\mathsf{op}} \longrightarrow \mathsf{Ab}.$$

Here Ab is the category of abelian groups, and Open_X is the category (poset) of open subsets of X. A morphism of presheaves is then a natural transformation of functors $\alpha : \mathcal{F} \to \mathcal{G}$.

3. The (pre)sheaves of abelian groups on a topological space X form a category $\mathsf{AbPreShv}_X$, AbShv_X. In fact, AbShv_X is an example of an **abelian category**. Without giving the formal definition, what this means is that all the general constructions available in the category of abelian groups, e.g., kernels and cokernels of maps, direct sums, etc., are also available in the category of sheaves of abelian groups.

4. One can give the definition of sheaves of other kinds of mathematical structures, e.g., sheaves of rings, sheaves of groups, sheaves of sets, sheaves of modules over a given ring R.

Theorem 2.7.5. *Let A be a commutative ring and let $X = \mathrm{Spec}(A)$ with the Zariski topology. There is a unique sheaf of rings $\mathcal{O}_X$ on X with the properties that*

1. *For every $f \in A$, $\mathcal{O}_X(X_f) = A_f$.*

2. *For $f, g \in A$, if $X_g \subset X_f$, then the restriction map $\mathcal{O}_X(X_f) \to \mathcal{O}_X(X_g)$ is the localization $A_f \to A_g$.*

Note that the second condition is meaningful: $X_g \subset X_f$ if and only if $V(f) \subset V(g)$ if and only if $g \in \sqrt{f}$. We can write $g^\mu = af$ for some $\mu \geq 1$, $a \in A$. The map $A_f \to A_g$ is then $b/f^\nu \mapsto ba^\nu/g^{\mu\nu}$, and one checks that this is well-defined, i.e., independent of the expression $g^\mu = af$. This is a sheaf of local rings in the sense that each stalk $\mathcal{O}_{X,x}$ is a local ring: if $x = [\mathfrak{p}]$ then $\mathcal{O}_{X,x} = A_\mathfrak{p}$.

The pair $(X, \mathcal{O}_X)$ is an **affine scheme**. Its construction is functorial in the ring A: given a ring homomorphism $\varphi : A \to B$ there is a morphism $(Y, \mathcal{O}_Y) \to (X, \mathcal{O}_X)$, where $Y = \mathrm{Spec}(B)$. We have already seen (2.7.1) that we have a continuous map $f : Y \to X$. There is also a map of sheaves of rings on X, $\varphi^\sharp : \mathcal{O}_X \to f_*\mathcal{O}_Y$, where the direct image of sheaves is defined (for any continuous map of topological spaces $f : Y \to X$, and any sheaf $\mathcal{F}$ on Y) as

$$f_*\mathcal{F}(U) := \mathcal{F}(f^{-1}U), \quad \text{for all open } U \subset X.$$

In fact, $\varphi^\sharp$ is defined on basic open sets as $h/a^\nu \mapsto \varphi(h)/\varphi(a)^\nu$:

$$A_a = \mathcal{O}_X(X_a) \longrightarrow f_*\mathcal{O}_Y(X_a) = \mathcal{O}_Y(f^{-1}(X_a)) = \mathcal{O}_Y(Y_{\varphi(a)}) = B_{\varphi(a)}.$$

Intuitively we think of $\varphi^\sharp$ as "pulling back functions on X to functions on Y along f". In this way we obtain the category of affine schemes SchAff.

Theorem 2.7.6. *The map $A \mapsto (\mathrm{Spec}(A), \mathcal{O}_{\mathrm{Spec}(A)})$ is a contravariant functor. It induces an antiequivalence of categories: $\mathsf{Ring}^{\mathsf{op}} \to \mathsf{SchAff}$.*

The construction of the sheaf $\mathcal{O}_X$ from the ring A generalizes as follows: given any A-module M we define a sheaf $\mathcal{M} = \tilde{M}$ which on basic open sets takes the value $\tilde{M}(X_a) = M_a$, the localization of the module M in the set $\{1, a, a^2, ...\}$. This is a sheaf of $\mathcal{O}_X$-modules in an obvious sense. Sheaves of this type are called **quasi-coherent** sheaves.

Theorem 2.7.7. *Let $X = \mathrm{Spec}(A)$, the map $M \mapsto \tilde{M}$ is a covariant functor. It induces an equivalence of categories*

$$\mathsf{Mod}_A \to \mathsf{QCoh}_X.$$

We can summarize this by saying that, in some sense, the theory of commutative rings and modules is equivalent to the theory of affine scheme and quasi-coherent sheaves. Often we let $\mathrm{Spec}(A)$ mean the scheme attached to A (the sheaf of rings being understood). For instance if k is a field, $\mathrm{Spec}(k)$ will denote the one-point space $\mathrm{Spec}(k) = \{[0]\}$ together with the sheaf whose value is just k itself over the unique open set $[0]$.

Definition 2.7.8. A **locally ringed space** is a pair $(X, \mathcal{O}_X)$ consisting of a topological space X and a sheaf of rings $\mathcal{O}_X$ on X such that each stalk $\mathcal{O}_{X,x}$ is a local ring (with maximal ideal $\mathfrak{m}_{X,x}$). A morphism $(Y, \mathcal{O}_Y) \to (X, \mathcal{O}_X)$ is a pair (f, ψ) where $f : Y \to X$ is a continuous map, and $\psi : \mathcal{O}_X \to f_*\mathcal{O}_Y$ is a homomorphism of sheaves of rings on X such that, for all $y \in Y$, the canonical map $\psi_y : \mathcal{O}_{X,f(y)} \to \mathcal{O}_{Y,y}$ is a *local homomorphism* of local rings. That is, $\psi_y(\mathfrak{m}_{X,f(y)}) \subset \mathfrak{m}_{Y,y}$. To explicate this last condition, if U runs over the set of open neighborhoods of $f(y)$, then $f^{-1}(U)$ forms a system of open neighborhoods of y. We then have maps

$$\psi_y : \mathcal{O}_{X,f(y)} = \varinjlim_U \mathcal{O}_X(U) \xrightarrow{\varinjlim \psi(U)} \varinjlim_U \mathcal{O}_Y(f^{-1}U) \xrightarrow{\text{canonical}} \mathcal{O}_{Y,y}$$

A **scheme** is a locally ringed space $(X, \mathcal{O}_X)$ which has a covering of open sets each of which is isomorphic to $(\mathrm{Spec}(A), \mathcal{O}_{\mathrm{Spec}(A)})$.

In the practice of algebraic geometry, one usually works with a fixed base field (or base ring) k, and these are "constants". In the theory of schemes one accomplishes this by fixing a base scheme S (for instance $S = \mathrm{Spec}(k)$) and works in the category Sch_S of schemes over S, which are just schemes X with a distinguished morphism $X \to S$, and whose morphisms are commutative diagrams of schemes and morphisms:

$$\begin{array}{ccc} X & \longrightarrow & Y \\ & \searrow \quad \swarrow & \\ & S & \end{array}$$

2.8 Gröbner Basis Applications

Gröbner bases and the Buchberger Algorithm for finding them are fundamental notions in algebra. Using Gröbner bases, one can perform more advanced computations in algebraic geometry such as elimination theory and cohomology.

Since polynomial models are widely used in the sciences and engineering, Gröbner bases have been used to solve problems in many different areas of mathematics and applied sciences. For example, researchers in optimization, coding, robotics, control theory, statistics, molecular biology, and many other fields. Below, we list a few applications of Gröbner Bases in applied science areas.

- Computer Aided Geometry Design (CAGD) visualization problems for intersections of curves and surfaces, implicitizations, [Ago05].

- Kinematic problems in robotics, and generating efficient kinematic solutions for the dynamic simulation of mechanisms, [UM12].
- Integral programming, [CT91].
- Optimization and Code, [BP09].
- Signal and image processing, [LXW04].

We will discuss three examples in some detail.

2.8.1 Solving Systems of Equations

One of the important applications of Gröbner basis is to solve systems of equations. Suppose we have a linear system of equations, then this system can be solved by Gaussian elimination. That is to write the linear system of equations as $M\mathbf{x} = \mathbf{0}$ where M is the coefficient matrix corresponding to the system, and then transform M into a row echelon form by elementary row operations, finally use back-substitution to solve for $x_1, \ldots, x_n$. In Gaussian elimination, we eliminate variables in the linear system in order to work with a simpler system of equations with same solution set as the original one. For non-linear systems, we can solve via Gröbner basis, a device similar to Gaussian elimination for a system of nonlinear multivariate polynomials. The reason behind this application is that is if the ideal I, generated by polynomials $f_1, \ldots, f_m$ in variables $x_1, \ldots, x_n$, is zero-dimensional for the lexicographical order $x_n > \cdots > x_1$, then the situation is similar to the linear case. That is the Gröbner basis $\{g_1, \ldots, g_s\}$ is such that g_1 contains only x_1, g_2 contains only x_1, x_2, and so forth until g_s. Therefore, we solve $g_1(x_1) = 0$ for x_1, and substitute into g_2 to solve x_2, and so on.

Example 2.8.1. The real numbers x, y and z satisfy the system of equations:

$$\begin{aligned} x^2 - x &= yz + 1 \\ y^2 - y &= xz + 1 \\ z^2 - z &= xy + 1. \end{aligned}$$

Find all solutions (x, y, z) of the system and determine all possible values of $xy + yz + xz + x + y + z$ where (x, y, z) is a solution of the system.

Proof. The solutions are: $(-1, -1, -1)$ and

$$\left(\frac{1 - y \mp \sqrt{-(3y^2 - 2y - 5)}}{2},\ y,\ \frac{1 - y \pm \sqrt{-(3y^2 - 2y - 5)}}{2} \right),\ -1 \leq y \leq \frac{5}{3}.$$

Moreover, $xy + yz + zx + x + y + z = 0$, when (x, y, z) is a solution of the system.

To see this, first, a simple computation via Mathematica [Wol15] with lexicographic order $z > y > x$ gives that

$$-1-y+y^2-2z+y^2z+yz^2+z^3,\ -y-y^2+y^3+z+z^2-z^3,\ -2+x+y^2+yz+z^2$$

are the Gröbner basis for the ideal generated by the polynomials $x^2 - x - yz - 1$, $y^2 - y - xz - 1$, and $z^2 - z - xy - 1$.

Therefore, the solutions to the system of equations:

$$\begin{aligned} -1 - y + y^2 - 2z + y^2z + yz^2 + z^3 &= 0 \\ -y - y^2 + y^3 + z + z^2 - z^3 &= 0 \\ -2 + x + y^2 + yz + z^2 &= 0. \end{aligned}$$

are exactly the solutions to the original problem.

We observe that

$$-y - y^2 + y^3 + z + z^2 - z^3 = (z - y)(1 + z + y - z^2 - zy - y^2) = 0,$$

suggests either $z - y = 0$ or $1 + z + y - z^2 - zy - y^2 = 0$.

If $z - y = 0$, then $z = y$ and

$$-1-y+y^2-2z+y^2z+yz^2+z^3 = -1-3y+y^2+3y^2 = (1+3y)(y+1)(y-1) = 0.$$

Hence, $y = 1$, or $y = -1$, or $y = -1/3$.

Thus, the last equation $-2 + x + y^2 + yz + z^2 = 0$ implies the solutions are

$$(-1, 1, 1),\ (-1, -1, -1),\ (5/3, -1/3, -1/3).$$

If $1 + z + y - z^2 - zy - y^2 = 0$, then $z^2 + (y-1)z + (y^2 - y - 1) = 0$, and

$$z = \frac{1 - y \pm \sqrt{-(3y^2 - 2y - 5)}}{2}, \quad \text{where} \quad -1 \le y \le \frac{5}{3}.$$

Since $1 + z + y - z^2 - zy - y^2 = 0$ suggests

$$-1 - y + y^2 - 2z + y^2z + yz^2 + z^3 = -z(1 + z + y - y^2 - yz - z^2) = 0,$$

which doesn't contribute to the solution; but

$$-2 + x + y^2 + yz + z^2 = -2 + x + y^2 + (1 + z + y - y^2) = -1 + x + y + z = 0$$

implies that

$$x = 1-y-z = 1-y-\frac{1-y\pm\sqrt{-(3y^2-2y-5)}}{2} = \frac{1-y\mp\sqrt{-(3y^2-2y-5)}}{2}.$$

Therefore, we have the solutions are

$$\left(\frac{1-y\mp\sqrt{-(3y^2-2y-5)}}{2},\ y,\ \frac{1-y\pm\sqrt{-(3y^2-2y-5)}}{2}\right),\ -1\le y\le\frac{5}{3}.$$

Combining the above two cases, the solutions for the given systems of equations are: $(-1,-1,-1)$ and

$$\left(\frac{1-y\mp\sqrt{-(3y^2-2y-5)}}{2},\ y,\ \frac{1-y\pm\sqrt{-(3y^2-2y-5)}}{2}\right),\ -1\le y\le\frac{5}{3}.$$

It is easy to check that if $(x,y,z)=(-1,-1,-1)$, then $xy+yz+zx+x+y+z=0$.

If $(x,y,z)=\left(\frac{1-y\mp\sqrt{-(3y^2-2y-5)}}{2},\ y,\ \frac{1-y\pm\sqrt{-(3y^2-2y-5)}}{2}\right)$, where $-1\le y\le\frac{5}{3}$, then

$$\begin{aligned} xy+yz+zx+x+y+z &= y(x+z)+zx+y+(x+z)\\ &= (x+z)(y+1)+zx+y\\ &= (1-y)(1+y)+zx+y\\ &= 1-y^2+(y^2-y-1)+y\\ &= 0. \end{aligned}$$

Thus, we conclude $xy+yz+zx+x+y+z=0$, when (x,y,z) is a solution of the system. □

2.8.2 Orthogonal Projection

Elimination via Gröbner basis can also help us solving the problem concerning the orthogonal projection of a rational space curve to a rational surface. A rational parametrized curve $\mathcal{C}$ is defined as the image of

$$F(t):\mathbb{R}\to\mathbb{R}^3,\ t\to\left(\frac{f_1(t)}{f_0(t)},\ \frac{f_2(t)}{f_0(t)},\ \frac{f_3(t)}{f_0(t)}\right)$$

where $f_i(t) \in \mathbb{R}[t]$, polynomials for $i = 0, 1, 2, 3$. A rational parametrized surface $\mathcal{S}$ is defined as the image of

$$G(u,v) : \mathbb{R}^2 \to \mathbb{R}^3,\ (u,v) \to \left(\frac{g_1(u,v)}{g_0(u,v)}, \frac{g_2(u,v)}{g_0(u,v)}, \frac{g_3(u,v)}{g_0(u,v)}\right)$$

where $g_i(u,v) \in \mathbb{R}[u,v]$, polynomials for $i = 0, 1, 2, 3$.

The *orthogonal projection* of $\mathcal{C}$ onto $\mathcal{S}$ is defined to be the set H such that

$$H = \{(u,v,t) \in \mathbb{R}^3 \mid (G(u,v) - F(t)) \times N(u,v) = 0\}, \tag{2.3}$$

where $N(u,v)$ is the normal vector of $G(u,v)$. In particular, we can focus our attention to the two dimensional space and study the set

$$P = \{(u,v) \in \mathbb{R}^2 \mid (u,v,t) \in H\}, \tag{2.4}$$

since this set provides the same information in a lower dimension.

Since $N(u,v) = G_u(u,v) \times G_v(u,v)$, we must have that

$$(G(u,v) - F(t)) \cdot G_u(u,v) = 0, \quad \text{and} \quad (G(u,v) - F(t)) \cdot G_v(u,v) = 0;$$

which can be further simplified as

$$\begin{cases} \dfrac{\sum_{i=1}^{3}(g_i f_0 - f_i g_0)(g_{iu} g_0 - g_i g_{0u})}{g_0^3 f_0} = 0, \\ \dfrac{\sum_{i=1}^{3}(g_i f_0 - f_i g_0)(g_{iv} g_0 - g_i g_{0v})}{g_0^3 f_0} = 0. \end{cases} \tag{2.5}$$

Thus we have the following result concerning the orthogonal projection.

Corollary 2.8.2. *Given a rational parametrized curve $\mathcal{C}$*

$$F(t) : \mathbb{R} \to \mathbb{R}^3,\ t \to \left(\frac{f_1(t)}{f_0(t)}, \frac{f_2(t)}{f_0(t)}, \frac{f_3(t)}{f_0(t)}\right)$$

and a rational parametrized surface $\mathcal{S}$

$$G(u,v) : \mathbb{R}^2 \to \mathbb{R}^3,\ (u,v) \to \left(\frac{g_1(u,v)}{g_0(u,v)}, \frac{g_2(u,v)}{g_0(u,v)}, \frac{g_3(u,v)}{g_0(u,v)}\right)$$

where $f_i(t) \in \mathbb{R}[t]$, $g_i(u,v) \in \mathbb{R}[u,v]$ are polynomials for $i = 0, 1, 2, 3$. Fix a monomial order with $y > t > u > v$, and let G be a Gröbner basis of the ideal

$$\left\langle \sum_{i=1}^{3}(g_i f_0 - f_i g_0)(g_{iu} g_0 - g_i g_{0u}), \sum_{i=1}^{3}(g_i f_0 - f_i g_0)(g_{iv} g_0 - g_i g_{0v}), y f_0 g_0 - 1 \right\rangle.$$

Then H, the orthogonal projection of $\mathcal{C}$ onto $\mathcal{S}$, is the variety of the first elimination ideal,

$$H = \mathbb{V}(G \cap \mathbb{R}[u, v, t]), \quad \textit{moreover,} \quad E = \mathbb{V}(G \cap \mathbb{R}[u, v]).$$

Proof. The result follows directly from the elimination theorem. □

Example 2.8.3. Let the space curve $\mathcal{C}$ and the surface $\mathcal{S}$ be given as

$$\begin{aligned} F &= \left(\frac{t^3}{t+1}, \frac{t^2}{t+1}, \frac{t}{t+1}\right), \\ G &= \left(\frac{uv}{u+v}, \frac{uv^2}{u+v}, \frac{u^2}{u+v}\right). \end{aligned}$$

Then by the above result, we obtain

$$\begin{aligned} G \cap \mathbb{R}[u, v] &= -u^{12} + u^9 v - 2u^{10} v - 4u^{11} v + 2u^{12} v + 5u^8 v^2 \\ &\quad -8u^9 v^2 - 9u^{10} v^2 + 7u^{11} v^2 + 10u^7 v^3 - 12u^8 v^3 \\ &\quad -11u^9 v^3 + 4u^{10} v^3 + 2u^{11} v^3 + 10u^6 v^4 - 8u^7 v^4 \\ &\quad -2u^8 v^4 - 14u^9 v^4 + 7u^{10} v^4 + 5u^5 v^5 - 2u^6 v^5 \\ &\quad +14u^7 v^5 - 30u^8 v^5 + 7u^9 v^5 + u^4 v^6 + 26u^6 v^6 \\ &\quad -26u^7 v^6 - 11u^8 v^6 - 4u^9 v^6 + 26u^5 v^7 - 8u^6 v^7 \\ &\quad -25u^7 v^7 - 14u^8 v^7 + 14u^4 v^8 + 2u^5 v^8 - 3u^6 v^8 \\ &\quad -18u^7 v^8 - 4u^8 v^8 + 3u^3 v^9 + 27u^5 v^9 - 9u^6 v^9 \\ &\quad -10u^7 v^9 - u^3 v^{10} + 30u^4 v^{10} + 3u^5 v^{10} - 9u^6 v^{10} \\ &\quad +11u^3 v^{11} + u^4 v^{11} + 2u^5 v^{11} + 2u^6 v^{11} - u^2 v^{12} \\ &\quad -3u^3 v^{12} + 11u^4 v^{12} + 3u^5 v^{12} + 6u^3 v^{13} + 2u^5 v^{13} \\ &\quad +u^3 v^{14} + 3u^4 v^{14} + u^3 v^{15}; \\ E &= \mathbb{V}(G \cap \mathbb{R}[u, v]). \end{aligned}$$

Figure 2.8.3 shows the three dimensional space curve and the surface, and the orthogonal projection image in the plane.

2.8.3 Poncelet's Algebraic Correspondence

There are many interesting applications using Gröbner basis. Here, we present one topic related to Poncelet's theorem and relations to certain kinds of classical invariants.

Let C and D be two nonsingular projective plane conics. Start from a point $P = P_0 \in C$, draw a tangent line $\ell = \ell_0$ to D from P and let $P_1 \in C$

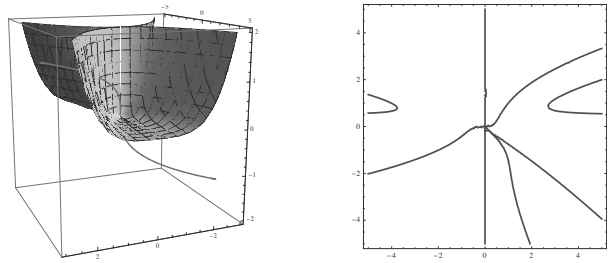


Figure 2.5: Curve $\mathcal{C}$, surface $\mathcal{S}$, and orthogonal projection

be the other intersection of ℓ and C. Continue this process with P_0 replaced by P_1; we obtain in this way a sequence (P_i, ℓ_i) of points of C and tangent lines to D: $\ell_i = P_i P_{i+1}$. If there is an n such that $P_n = P_0$, we say we have a Poncelet n-gon. Note that this n-gon can be degenerate: if one of the tangent lines ℓ_i to D is also tangent to C, then $P_i = P_{i+1}$. Also, if P_{i+1} is an intersection of C and D, then $\ell_i = \ell_{i+1}$. Poncelet's theorem is that if one gets an n-gon starting from a general point $P \in C$, then one gets an n-gon, possibly degenerate, starting from any other point of C. Cayley gave a proof of this using the theory of elliptic curves (see [GH78] for a modern exposition). More generally, any sequence (P_i, ℓ_i), whether it repeats or not, is called a Poncelet chain.

Let $D^* \subset \mathbb{P}^{2*}$ be the dual variety of tangent lines to D. This is also a conic. Let

$$E = \{(P, \ell) \in C \times D^* : P \in \ell\},$$

the incidence correspondence. Assuming that C and D meet transversally in four distinct points, one can show that E is nonsingular, that the projection $\pi : E \to C$ is two-to-one with four branch points over $C \cap D$, hence it is a curve of genus 1. For $P \in C$, $\pi^{-1}(P)$ are the two tangents to D from P. Similarly the projection $\rho : E \to D^*$ is two-to-one: $\rho^{-1}(\ell)$ are the two points $P, Q \in C$ such that $\ell \cap C = \{P, Q\}$. If we take $O = (P_O, \ell_O) \in C \times D^*$ such that P_O is one of the four points $C \cap D$ and ℓ_O is the unique tangent to D there, then we can take O as the origin for group-law on the elliptic curve (E, O). Let $S = (P_S, \ell_S) \in E$ be the point defined by $\ell_O \cap C = \{P_O, P_S\}$, and ℓ_S the other tangent line to D through P_S, i.e., other than ℓ_O. Then the successive points in a Poncelet chain result from translation by S in the group-law of E:

$$(P_i, \ell_i) + (P_S, \ell_S) = (P_{i+1}, \ell_{i+1}), \text{ addition in } E.$$

Thus, we have a Poncelet n-gon if and only if $S \in E$ is a point of order n, and Poncelet's theorem is now clear: starting from any point $M = (P_M, \ell_M) \in E$, translation n times by S brings you back to M. Remark that we have not assumed that either C or D has a $\mathbb{K}$-rational point. In general, we must enlarge $\mathbb{K}$ to so that we can define an origin O for an elliptic curve E.

We define an algebraic correspondence T on C:

$$T = \{(P, Q) \in C \times C : \ell = PQ \in D^* = \text{the set of tangents to } D\}.$$

There are two projections $T \to C$ each of which is two-to-one and branched over $C \cap D$. If $\mathbb{K}$ is a field of definition of C and D, the curve T is $\mathbb{K}$-isomorphic to the curve E, by the map $(P, Q) \mapsto (P, PQ)$. The correspondence is symmetric under exchange of P and Q. We can view this correspondence as a mulitvalued map $C \to C : P \mapsto P_1 + P_2$ where PP_1 and PP_2 are the two tangents to D from P. More precisely we view T as inducing an endomorphism of the group $\mathrm{Div}(C)$ of divisors of C. From now on, we will assume that C contains a $\mathbb{K}$-rational point. As is well-known, this means that we have an isomorphism of C with $\mathbb{P}^1$. Also it is well-known that we may choose coordinates in $\mathbb{P}^2$ such that $y = x^2$ is an affine equation of C.

Lemma 2.8.4. *([Sak10, Ch.2]) Let two conics C, D in $\mathbb{P}^2$ be defined by*

$$C : \ y = x^2, \quad D : \ c_1x^2 + c_3xy + c_2y^2 + c_4x + c_5y + c_6 = 0,$$

then the algebraic correspondence T on C is defined by $A(x, z) = 0$, where

$$\begin{aligned}
A(x,z) &= a_1x^2z^2 + a_2xz(x+z) + a_3(x+z)^2 + a_4xz + +a_5(x+z) + a_6,\\
a_1 &= -4c_1c_2 + c_3^2,\\
a_2 &= -2(2c_2c_4 - c_3c_5),\\
a_3 &= c_5^2 - 4c_2c_6,\\
a_4 &= -2c_3c_4 - 2c_1c_5,\\
a_5 &= 2(c_4c_5 - 2c_3c_6),\\
a_6 &= c_4^2 - 4c_1c_6.
\end{aligned}$$

That is, the line connecting the points (x, x^2) and (z, z^2) is tangent to D if and only if $A(x, z) = 0$. The map $(c_1, ..., c_6) \to (a_1, ..., a_6)$ is a birational

transformation $\mathbb{P}^5 \to \mathbb{P}^5$ *with inverse*

$$\begin{aligned}
\lambda c_1 &= (a_4^2 - 4a_1a_6)/2,\\
\lambda c_2 &= (a_2^2 - 4a_1a_3)/2,\\
\lambda c_3 &= a_2a_4 - 2a_1a_5,\\
\lambda c_4 &= a_4a_5 - 2a_2a_6,\\
\lambda c_5 &= 2a_3a_4 - a_2a_5,\\
\lambda c_6 &= (a_5^2 - 4a_3a_6)/2\\
\lambda &= -8(c_2c_4^2 - c_3c_4c_5 + c_1c_5^2 - 4c_1c_2c_6 + c_3^2c_6)
\end{aligned}$$

To emphasize dependence on the parameters a_i*, we write this as* $A(a, x, z)$*.*

Proof. Write the equation for the line connecting $(x, x^2), (z, z^2)$. Plug this equation into the equation for D. The tangent condition is that this quadratic equation should have a double root, or in other words, that its discriminant should be a square. These conditions lead to the above expressions. The last assertion can be checked by direct substitution. □

Remark 2.8.5. The birational correspondence between $c = (c_1, \ldots, c_6)$ and $a = (a_1, \ldots, a_6)$ enables us to describe the Poncelet configurations either with the a-coordinates, or the c-coordinates.

We can consider the iterates of $T = T_1$, $T^2 = T \circ T$, etc. Notice that $T^2P = 2P + T_2P$, for a correspondence T_2 of degree 2. We define T_3 by the equation $T_3P = T_1T_2P - T_1P$, T_4 by the equation $T_4P = T_2^2P - 2P$. In general, $TT_n = T_{n+1} + T_{n-1}$ is the recursion for $n \geq 2$. These are all of degree 2. One can see that each T_n is defined by an equation $A_n(x, z) = A(a^{(n)}, x, z) = 0$ where the entries in the vector $a^{(n)}$ are homogeneous polynomials of degree n^2 in $a_1, ..., a_6$.

Lemma 2.8.6. *Let* C, D *in* $\mathbb{P}^2$ *be defined by*

$$C: \ y = x^2, \quad D: \ c_1x^2 + c_3xy + c_2y^2 + c_4x + c_5y + c_6 = 0,$$

and let $P_0, \ldots, P_7 = P_0 \in C$ *be a Poncelet 7-gon. Then the following are the*

algebraic correspondences on C:

$$\begin{aligned}
A_2(x,z) &= \frac{\mathrm{Res}\,(A_1(x,u),A_1(z,u),u)}{(x-z)^2},\\
A_2(x,z) &= 0 \textit{ is the equation of } T_2 : P_0 \to \{P_2, P_5\}\\
A_3(x,z) &= \frac{\mathrm{Res}\,(A_1(x,u),A_2(u,z),u)}{A_1(x,z)},\\
A_3(x,z) &= 0 \textit{ is the equation of } T_3 : P_0 \to \{P_3, P_4\}\\
A_4(x,z) &= \frac{\mathrm{Res}\,(A_2(x,u),A_2(z,u),u)}{(x-z)^2},\\
A_4(x,z) &= 0 \textit{ is the equation of } T_4 : P_0 \to \{P_3, P_4\}.
\end{aligned}$$

Therefore, we have a Poncelet 7-gon if and only if $A_4(x,z) = \alpha A_3(x,z)$ for a constant α.

Proof. Since the identity correspondence is defined by $x - z = 0$ and the composition of correspondences is defined by the resultant expressions, we see that $T_2 = T^2 - 2\,\mathrm{id}$ is defined by the given expression. Similar arguments give the expressions for T_3 and T_4. One has a Poncelet 7-gon if and only if $T_3 = T_4$ which proves the last claim.

□

Given conics C and D as above, they define Poncelet 7-gons if and only if the equation $A_4(x,z) = \alpha A_3(x,z)$ holds for a constant α. This gives a set of polynomial relations $G_j(a_1, ..., a_6, \alpha) = 0$ for $1 \le j \le 6$ in α and the coefficients $a_1, a_2, \ldots, a_6$ associated to the conic D as in Lemma 2.8.4, namely the coefficients of $1, x+z, xz, (x+z)^2, xz(x+z)$, and x^2z^2. We eliminate α from these equations by taking the resultants of pairs of these equations relative to α. These resultants have a GCD, $F_7(a_1, ..., a_6)$, a polynomial of degree 12, 260 monomial terms, with integer coefficients.

We have proved:

Proposition 2.8.7. *Given a pair of conics C, D as above, these give rise to Poncelet 7-gons if and only if $F_7(a_1, ..., a_6) = 0$, for the coefficients a as in Lemma 2.8.4.*

3. Modules

3.1 Modules

In abstract algebra, the concept of a module over a ring is a generalization of the notion of vector space over a field, wherein the corresponding scalars are the elements of an arbitrary ring.

Definition 3.1.1. Let R be a commutative ring. Then M is a **module** over R (or an **R-module**) if M has an operation $+$ of addition and a zero element 0 so that

1. The operation $+$ is both commutative and associative. That is $x+y = y+x$; $x+(y+z) = (x+y)+z$ for all $x, y, z \in M$.
2. For all $x \in M$, we have $0+x = x+0 = x$.
3. There is an operation of multiplication, that is multiplying elements of M by elements of the base ring R, so that multiplication distributes over addition. That is

   $$(r_1+r_2)x = r_1x+r_2x,\ r(x_1+x_2) = rx_1+rx_2,\ r_1, r_2, r \in R,\ x, x_1, x_2 \in M.$$

4. Finally we assume that if 1 is the unit element of R that $x \cdot 1 = 1 \cdot x = x$ for all $x \in M$.

Definition 3.1.2. Let M, N be R-modules. A mapping $f : M \to N$ is an **R-module homomorphism** or **R-linear** if $\forall\, m_1, m_2, m \in M$, and $\forall\, r \in R$

$$f(m_1+m_2) = f(m_2)+f(m_2),\ \text{ and }\ f(rm) = rf(m).$$

An **endomorphism** is an homomorphism from an object to itself.

We see that if R is a field, then an R-module homomorphism is indeed a linear transformation of vector spaces.

Definition 3.1.3. Moreover, we can consider the set of all R-module homomorphisms from M to N as an R-module. For all $m \in M$ and $r \in R$, define

$$(f+g)(m) = f(m) + g(m), \text{ and } (rf)(x) = r \cdot f(m).$$

We can check this is indeed an R-module, and we denote this module by $\mathrm{Hom}_R(M, N)$, or just $\mathrm{Hom}(M, N)$.

Example 3.1.4. Let M be an R-module, then $\mathrm{Hom}(R, M) \cong M$ by mapping $f \mapsto f(1)$.

Further more, the homomorphisms $s : M' \to M$ and $t : N \to N'$ induce R-module homomorphisms:

$$s' : \mathrm{Hom}(M, N) \to \mathrm{Hom}(M', N), \text{ and } t' : \mathrm{Hom}(M, N) \to \mathrm{Hom}(M, N')$$

where

$$s'(f) = f \circ s, \text{ and } t'(g) = t \circ g.$$

A submodule of an R-module is defined just as a subspace of a vector space is defined.

Definition 3.1.5. Let R be a module over the commutative ring R. Then $N \subset M$ is a **submodule** of M if for all $x_1, x_2 \in N$, and $r_1, r_2 \in R$, we have $r_1 x_1 + r_2 x_2 \in N$. That is, N is closed under linear combinations where the scalars are in the base ring R.

Example 3.1.6. If R is a commutative ring, and let $M = R$, then R is a module over itself. A subset N of R is a submodule if it is an ideal of R.

Example 3.1.7. Let R be a ring, then the set of n-tuples R^n is an R-module with the usual operations.

Example 3.1.8. Let $\mathbb{F}$ be a field and, V a vector space over $\mathbb{F}$. Let $T : V \to V$ be a linear map from V to V. We can consider V is a module over the ring $\mathbb{F}[x]$ by the operation

$$f(x) \cdot v = f(T)v, \quad \text{where } f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{F}[x], \ v \in V.$$

Definition 3.1.9. Let M be an R-module, and N a submodule of M. A factor group M/N as additive commutative group can be made into an R-module by defining $r(m + N) = rm + N$ for every coset $m + N \in M/N$. The natural map of M to M/N is a R module homomorphism.

It is easy to check that given a R-module homomorphism $f : M \to N$, then the *kernel of* f, $\ker(f) = \{m \in M \mid f(m) = 0\}$, is a submodule of M; the *image of* f, $\mathrm{im}(f) = f(M)$, is a submodule of N; the *cokernel of* f, $\mathrm{coker}(f) = N/\mathrm{im}(f)$, is a quotient module of N.

The operations on modules are similar to the operations on ideals. Let M be an R-module and let $\{M_i\}_{i\in I}$ be a family of submodules of M. Then *sum* $\sum M_i$ is the set of all finite sums $\sum_{i\in I} m_i$ for $m_i \in M_i$ with almost all but finitely many $m_i \neq 0$. $\sum M_i$ is the smallest submodule of M containing all the M_i. The *intersection* $\cap_{i\in I} M_i$ is also a submodule of M.

The following are known results which we will state as exercises and leave the reader to complete the proof.

Exercise 3.1.10. *1. If $N \subseteq M \subseteq L$ are R-modules, then*

$$(L/N)/(M/N) \cong L/N.$$

2. If M_1, M_2 are submodules of M, then

$$(M_1 + M_2)/M_1 \cong M_2/(M_1 \cap M_2).$$

Definition 3.1.11. Let M be an R-module and N, P submodules of M. We define

$$(N : P) = \{r \in R \mid rP \subset N\}, \text{ this is an ideal in } R.$$

In particular, $(0 : M)$ is the set of all $r \in R$ such that $rM = 0$; this ideal is called the **annihilator of** M, denoted by $\mathrm{Ann}(M)$. An R-module is **faithful** if $\mathrm{Ann}(M) = 0$. If $m \in M$, then we write $\mathrm{Ann}(m) = \{r \in R \mid rm = 0\}$.

Remark 3.1.12. If $I \subseteq \mathrm{Ann}(M)$, then M can be considered as an R/I-module. If $\mathrm{Ann}(M) = I$, then M is a faithful R/I-module.

Definition 3.1.13. Suppose $\{M_i\}_{i\in I}$ is a family of R-modules. The **direct sum** $\oplus_{i\in I} M_i$ is defined as a set of tuples with i-th entry in M_i with only finitely many non-zeros

$$\oplus_{i\in I} M_i = \{(m_i)_{i\in I} \mid m_i \in M_i\}.$$

The addition and multiplication of the elements are componentwise. The **direct product** $\prod_{i\in I} M_i$ is defined similar to direct sum without the condition only finitely many non-zeros. In case that I is a finite set, direct sum and direct product are the same.

Definition 3.1.14. A **free** R-module M is an R-module is of the form $M \cong \oplus_{i\in I} M_i$ where $M_i \cong R$ as an R-module. A **finitely generated free R-module** is isomorphic to $R^n = \oplus_{i=1}^n R$, where R^0 is the zero module.

Let $m_1, \ldots, m_n$ generate M. Define a R-module homomorphism $f : R^n \to M$ by $f(r_1, \ldots, r_n) = (r_1 m_1, \ldots, r_n m_n)$. The readers can prove the following theorems.

Exercise 3.1.15. *1. M is a finitely generated R-module if and only if M is isomorphic to a quotient of R^n for some $n > 0$.*

2. Let M be a finitely generated R-module, let I be an ideal of R, and f be an R-module endomorphism of M such that $f(M) \subseteq IM$. Then f satisfies and equation of the form

$$f^n + a_1 f^{n-1} + \cdots + a_n = 0, \text{ where } a_i \in I.$$

One of the consequence of this result is that if $IM = M$, then there exists $r \cong 1 \pmod I$ such that $rM = 0$. This can be shown by taking the map f to be the identity map, then the result in the above exercise becomes

$$f^n + a_1 f^{n-1} + \cdots + a_n = 1 + a_1 + \cdots + a_n = 0.$$

Let $r = 1 + a_1 + \cdots + a_n$, we see that $r \cong 1 \pmod I$ and $rM = 0$. Suppose the ideal I is contained in the Jacobson radical of R, then $r \cong 1 \pmod I$ means that r is a unit in R, thus $M = 0$. Hence, we have the following well-known Nakayama's lemma.

Proposition 3.1.16. *(Nakayama's lemma) Let M be a finitely generated R-module and I and ideal of R such that I is contained in the Jacobson radical of R. Then $IM = M$ implies $M = 0$.*

As exercises, one can derive the following corollaries from Nakayama's lemma.

Exercise 3.1.17. *1. Let M be a finitely generated R-module, N a submodule of M, and ideal $I \subset R$ is contained in the Jacobson radical of R. Then $M = IM + N$ implies that $M = N$.*

2. Let $(R, \mathfrak{m})$ be a local ring, M finitely generated R-module, and let $m_i \in M$ for $i = 1, \ldots, n$ whose images in $M/\mathfrak{m}M$ form a basis of this vector space. Then m_i generate M.

Let us recall the definition of the *ascending chain condition* or *the maximal condition*: for a partially ordered set $(\sum, \leq)$, every increasing sequence $x_1 \leq x_2 \leq \cdots$ in this set is stationary. This hypothesis is also equivalent to the statement that every non-empty subset of $\sum$ has a maximal element. A module that satisfies the a.c.c. for the set $\sum$ of submodules ordered by inclusions $\subseteq$ called **Noetherian**. On the other hand, if it is ordered by $\supseteq$, then we say it satisfies the *descending chain condition* if every sequence $x_1 \supseteq x_2 \supseteq \cdots$ in $\sum$ is stationary. A module that satisfies d.c.c for submodules is called **Artinian**.

We see that a polynomial ring $\mathbb{K}[x]$ with $\mathbb{K}$ a field satisfies the ascending chain condition on ideals, hence, it is a Noetherian. But the polynomial ring with infinitely many variables is not Noetherian since ideal chain $\langle x_1 \rangle \subset \langle x_1, x_2 \rangle \subset \cdots$ does not terminate.

Using the ascending chain condition one can prove the following theorem.

Exercise 3.1.18. *M is a Noetherian R-module if and only if every submodule of M is finitely generated.*

3.2 Exact Sequences and Commutative Diagrams

A chain of modules connected by maps $M_1 \to M_2 \to M_3 \to \cdots$ is called exact at M_i if the kernel of the map $M_i \to M_{i+1}$ is precisely the image of the map $M_{i-1} \to M_i$. This implies, but is stronger than, the condition that the composite map $M_{i-1} \to M_i \to M_{i+1}$ is zero. A sequence is called *exact* if it is exact at each module which has a map from left and right. A sequence $0 \to M \to N$ is exact if and only if $M \to N$ is injective, and a sequence $M \to N \to 0$ is exact if and only if $M \to N$ is surjective. A sequence $0 \to M \to N \to 0$ is exact if and only if $M \cong N$. For vector spaces $0 \to V_1 \to V_2 \to V_3 \to 0$ is exact if and only if $V_2 \cong V_1 \oplus V_3$.

Using the ascending chain condition one can prove the following result.

Exercise 3.2.1. *1. Let*

$$0 \to N \xrightarrow{f} M \xrightarrow{g} P \to 0$$

be an exact sequence of R-modules. Then M is Noetherian (or Artinian) if and only if N and P are Noetherian (or Artinian).

2. If M_i for $i = 1, \ldots, n$ are Noetherian (or Artinian) R-module so is $\bigoplus_{i=1}^{n} M_i$.

3. *If R is a Noetherian (or Artinian) ring, and M is a finitely generated R-module, then M is Noetherian (or Artinian).*

Definition 3.2.2. A diagram of homomorphisms of the form

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle f'}\downarrow & & \downarrow{\scriptstyle g} \\ C & \xrightarrow{g'} & D \end{array}$$

is **commutative** if $g \circ f = g' \circ f'$.

Proposition 3.2.3. *Let*

$$\begin{array}{ccccccccc} & & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\ & & {\scriptstyle h'}\downarrow & & {\scriptstyle h}\downarrow & & {\scriptstyle h''}\downarrow & & \\ 0 & \longrightarrow & N' & \xrightarrow{f'} & N & \xrightarrow{g'} & N'' & & \end{array}$$

be commutative diagram with exact rows and assume that both h' and h'' are isomorphisms. Then h is an isomorphism.

Proof. We will first show that h is an injective map. Let $m \in M$ such that $h(m) = 0$. Then $h''(g(m)) = g'(h(m)) = 0$. Since h'' is injective, we must have that $g(m) = 0$. The exactness of the first row yields that $\ker(g) = \mathrm{im}(f)$, and there exists a $m' \in M'$ such that $f(m') = m$. Hence $h(f(m')) = f'(h'(m')) = 0$. Since both f' and h' are injective, this means that $f' \circ h'$ is injective, hence $m' = 0$. Thus $m = f(m') = 0$. Therefore, h is injective.

Now, we will show that h is surjective. Let $n \in N$. Since h'' is surjective, there exists $m'' \in M''$ such that $h''(m'') = g'(n)$. Since g is surjective, we must have that there exists a $m \in M$ such that $g(m) = m''$. Therefore,

$$g'(n - h(m)) = g'(n) - g'(h(m)) = g'(n) - h''(g(m)) = g'(n) - h''(m'') = 0.$$

But the $\ker(g') = \mathrm{im}(f')$, thus there exists $n' \in N'$ such that $f'(n') = n - h(m)$. Since h' is surjective, there must be a $m' \in M'$ such that $h'(m') = n'$. Thus $n = f'(n') + h(m) = f'(h'(m')) + h(m) = h(f(n')) + h(m) = h(f(n') + m)$, and h is surjective. ∎

Definition 3.2.4. A short exact sequence

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

splits if there exists a homomorphism $h : M'' \to M$ with the property that $g \circ h$ is the identity map on M''. The homomorphism h is called a **splitting**.

For any modules M, N, the short exact sequence

$$0 \longrightarrow M \xrightarrow{i_M} M \oplus N \xrightarrow{\pi_N} N \longrightarrow 0,$$

where $i_M(m) = (m, 0)$, $\pi_N(m, n) = n$, splits. The converse is true as well.

Proposition 3.2.5. *If the short exact sequence*

$$0 \longrightarrow M \xrightarrow{f} P \xrightarrow{g} N \longrightarrow 0$$

splits, then $P \cong M \oplus N$.

Proof. Let the splitting be $h : N \to P$, and define a homomorphism $\phi : M \oplus N \to P$ be such $\phi((m, n)) = f(m) + h(n)$.

First, $\phi(i_M(m)) = \phi(m, 0) = f(m) + h(0) = f(m)$, and $g(\phi((m, n)) = g(f(m)+h(n)) = g(f(m))+g(h(n)) = 0+g(h(n)) = \mathrm{id}_N(n) = n = \pi_N(m, n)$. Hence, the commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M & \xrightarrow{i_M} & M \oplus N & \xrightarrow{\pi_N} & N & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathrm{id}_M} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \mathrm{id}_N} & & \\
0 & \longrightarrow & M & \xrightarrow{f} & P & \xrightarrow{g} & N & \longrightarrow & 0.
\end{array}$$

Hence the map ϕ is an isomorphism. □

Proposition 3.2.6. *Let I, J be two ideals in R such that $I + J = R$, then $I \oplus J \cong R \oplus IJ$.*

Proof. Consider the short exact sequence:

$$0 \to I \cap J \to I \oplus J \to I + J \to 0.$$

Since $I + J = R$, this exact sequence becomes

$$0 \to IJ \to I \oplus J \to R \to 0.$$

Since R is free, we have that the sequence split, that is $I \oplus J \cong R \oplus IJ$. □

Perform diagram chasing, we have the following lemmas.

Lemma 3.2.7. *(Four Lemmas)*

1. *If the rows in the commutative diagram*

$$\begin{array}{ccccccc} B & \xrightarrow{g} & C & \xrightarrow{h} & D & \xrightarrow{j} & E \\ {\scriptstyle m}\downarrow & & {\scriptstyle n}\downarrow & & {\scriptstyle p}\downarrow & & {\scriptstyle q}\downarrow \\ B' & \xrightarrow{s} & C' & \xrightarrow{t} & D' & \xrightarrow{u} & E' \end{array}$$

are exact, and m and p are epimorphisms, and q is a monomorphism, then n is an epimorphism.

2. *If the rows in the commutative diagram*

$$\begin{array}{ccccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C & \xrightarrow{h} & D \\ {\scriptstyle \ell}\downarrow & & {\scriptstyle m}\downarrow & & {\scriptstyle n}\downarrow & & {\scriptstyle p}\downarrow \\ A' & \xrightarrow{r} & B' & \xrightarrow{s} & C' & \xrightarrow{t} & D' \end{array}$$

are exact, and m and p are monomorphisms, and ℓ is an epimorphism, then n is a monomorphism.

Lemma 3.2.8. *(Five Lemma) If the rows in the commutative diagram*

$$\begin{array}{ccccccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C & \xrightarrow{h} & D & \xrightarrow{j} & E \\ {\scriptstyle \ell}\downarrow & & {\scriptstyle m}\downarrow & & {\scriptstyle n}\downarrow & & {\scriptstyle p}\downarrow & & {\scriptstyle q}\downarrow \\ A' & \xrightarrow{r} & B' & \xrightarrow{s} & C' & \xrightarrow{t} & D' & \xrightarrow{u} & E' \end{array}$$

are exact, m and p are isomorphisms, ℓ is an epimorphism, and q is a monomorphism, then n is also an isomorphism.

In particular, the well-known result named Snake's Lemma is obtained by diagram-chasing

Proposition 3.2.9. *(Snake's Lemma) Let*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow[f]{} & M & \xrightarrow[g]{} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle h'} & & \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle h''} & & \\ 0 & \longrightarrow & N' & \xrightarrow[f']{} & N & \xrightarrow[g']{} & N'' & \longrightarrow & 0 \end{array}$$

be a commutative diagram of R-modules and homomorphisms, with the rows exact. Then there exists an exact sequence

$$0 \to \ker(f') \to \ker(f) \to \ker(f'') \to \operatorname{coker}(f') \to \operatorname{coker}(f) \to \operatorname{coker}(f'') \to 0.$$

Use the diagram chasing techniques showed in the previous proofs, please prove the following theorems.

Exercise 3.2.10. *1. Let*

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

be a sequence of R-modules and homomorphisms. Then this sequence is exact if and only if for all R-module N, the following sequence is exact:

$$0 \longrightarrow \mathrm{Hom}(N, M') \xrightarrow{f'} \mathrm{Hom}(N, M) \xrightarrow{g'} \mathrm{Hom}(N, M'').$$

2. Let

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

be a sequence of R-modules and homomorphisms. Then this sequence is exact if and only if for all R-module N, the following sequence is exact:

$$0 \longrightarrow \mathrm{Hom}(M'', N) \xrightarrow{g'} \mathrm{Hom}(M, N) \xrightarrow{f'} \mathrm{Hom}(M', N).$$

Remark 3.2.11. The short exact sequence $0 \to M' \to M \to M'' \to 0$ does not in general induce a short exact sequence of the $\mathrm{Hom}(N, *)$ or the $\mathrm{Hom}(*, N)$. This will be addressed in more detail in the last chapter. For example $0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0$ is an exact sequence where the map $\mathbb{Z} \to \mathbb{Z}$ is just multiplication by n. If we let $N = \mathbb{Z}/n\mathbb{Z}$, then $0 = \mathrm{Hom}(N, \mathbb{Z}) \to \mathrm{Hom}(N, \mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$ is not surjective.

3.3 Projective and Injective Modules

The concept of a *projective module* over a ring R is a generalization of the idea of a free module. The usual definition in line with category theory is the property of lifting that carries over from free to projective modules.

Definition 3.3.1. A module P is **projective** if and only if for every surjective module homomorphism $f : N \twoheadrightarrow M$ and every module homomorphism $g : P \to M$, there exists a homomorphism $h : P \to N$ such that $f \circ h = g$.

Exercise 3.3.2. *Every free module is projective.*

It is not obvious that there exist projective modules which are not free.

Proposition 3.3.3. *A direct sum of modules $P_1 \oplus P_2$ is projective if and only if P_i for $i = 1, 2$ are both projective. Hence, $\bigoplus_{i\in I} P_i$ is projective if and only if all P_i's are projective.*

Proof. First, we assume that $P_1 \oplus P_2$ is projective, we will show that P_1 is projective, and the similar proof will show that P_2 is projective. Let $g : M \to N$ is a surjective homomorphism, and a homomorphism $h : P_1 \to N$. We define a map $h' : P_1 \oplus P_2 \to N$ be such that $h'((p_1, p_2)) = h(p_1)$. h' is a homomorphism. Moreover, since $P_1 \oplus P_2$ is projective, there exists a map $k : P_1 \oplus P_2 \to M$ such that $g \circ k = h'$. Let $k_1(p_1) = k((p_1, 0))$

$$g(k_1(p_1)) = (g \circ k)((p_1, 0)) = h'((p_1, 0)) = h(p_1).$$

Thus, the map $k_1 : P_1 \to M$ is such that $g \circ k_1 = h$. By definition, P_1 is projective.

Now, we assume that P_1, P_2 are projective, we will show that $P_1 \oplus P_2$ is projective. Let $g : M \to N$ be a surjective map, and homomorphisms $h : P_1 \oplus P_2 \to N$, $h_i : P_i \to N$ where $h_1(p_1) = h(p_1, 0)$ and $h_2(p_2) = h(0, p_2)$. Since P_i's are projective, there are maps $f_i : P_i \to M$ such that $g \circ f_i = h_i$. Hence, we define $f : P_1 \oplus P_2 \to M$ such that $f((p_1, p_2)) = f((p_1, 0)+(0, p_2)) = f_1(p_1)+f_2(p_2)$, hence have $(g\circ f)((p_1, p_2)) = g(f_1(p_1))+ g(f_2(p_2)) = h_1(p_1) + h_2(p_2) = h((p_1, 0) + (0, p_2)) = h(p_1, p_2)$. Thus by definition, $P_1 \oplus P_2$ is projective. □

As an exercise, we will leave the reader to prove the following equivalent statements.

Exercise 3.3.4. *If P is a module, then the following are equivalent:*

1. *P is projective;*
2. *For every short exact sequence*

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

sequence of R-modules and homomorphisms, the following induced sequence of $\mathbb{Z}$-modules is exact.

$$0 \to \mathrm{Hom}(P, M') \xrightarrow{f'} \mathrm{Hom}(P, M) \xrightarrow{g'} \mathrm{Hom}(P, M'') \to 0$$

3. *For every surjective homomorphism $f : M \twoheadrightarrow P$, there exists $g : P \to M$ such that $g \circ h = id_P$. (That is every exact sequence $0 \to N \to M \to P \to 0$ splits, i.e., $M \cong P \oplus N$).*

4. *P is a direct summand in every module of which it is a quotient.*

5. *P is direct summand in a free module (That is there exists a free module F, and another module N such that $F \cong P \oplus N$.)*

As a consequence of Theorem 3.3.4, we have

Corollary 3.3.5. *(Schanuel's Lemma) If P, P' are projective modules with $P/M \cong P'/M'$, then $P \oplus M' \cong P' \oplus M$.*

Proof. Consider the following commutative diagram (since P is projective, t exists),

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{i} & P & \longrightarrow & P/M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle s} & & \downarrow{\scriptstyle t} & & \downarrow{\scriptstyle f} & & \\ 0 & \longrightarrow & M' & \xrightarrow{j} & P' & \longrightarrow & P'/M' & \longrightarrow & 0, \end{array}$$

and the sequence:

$$0 \longrightarrow M \xrightarrow{\alpha} P \oplus M' \xrightarrow{\beta} P' \longrightarrow 0,$$

where $\alpha(m) = (i(m), s(m))$ and $\beta(p, q) = t(p) - j(q)$. Since the diagram is commutative, $\beta(\alpha(m)) = ti(m) - js(m) = 0$, thus $\mathrm{im}(\alpha) \subset \ker(\beta)$. On the other hand, $\ker(\beta) = \{(p, q) \mid t(p) = j(q), p \in P, q \in M'\}$. Again, since the diagram is commutative there exists a $m \in M$ such that $p = i(m)$, and $q = s(m)$. Therefore, $\ker(\beta) \in \mathrm{im}(\alpha)$. Thus, the sequence is exact. Since P' is projective, by Theorem 3.3.4, the exact sequence splits, and $P \oplus M' \cong P' \oplus M$. □

Let $P = \bigoplus_{i \in I} Rp_i$ be a free R-module, $f : N \twoheadrightarrow M$ any surjective homomorphism, and any homomorphism $g : P \to M$. We can prove the following theorem by definition.

Proposition 3.3.6. *A finitely generated projective module M over a Noetherian local ring R is free.*

Proof. Let $\mathfrak{m}$ be the unique maximal ideal in R. Let $m_1, \ldots, m_n \in M$ so that $\bar{m}_1, \ldots, \bar{m}_n$ are a basis for the vector space $M/\mathfrak{m}M$ over the field $R/\mathfrak{m}$. Let $f : R^n \to M$ be defined by $f(r_1, \ldots, r_n) = \sum_{i=1}^n r_i m_i$. Then, M is generated by m_i for $i = 1, \ldots, n$, by Exercise 3.1.17 (2). Thus f is surjective.

Since M is a projective module, $R^n = \ker(f) \oplus M$, and $\ker(f)$ is finitely generated, since R is Noetherian. Moreover, the map f induces an isomorphism $R^n/\mathfrak{m}R^n \cong M/\mathfrak{m}M$. Hence $\ker(f)/\mathfrak{m}\ker(f) \oplus M/\mathfrak{m}M = M/\mathfrak{m}M$.

The fact that these are finite dimensional vector space over the field $R/\mathfrak{m}$ shows that $\ker(f)/\mathfrak{m}\ker(f) = 0$. Thus $\ker(f) = 0$ by Nakayama's Lemma. Thus, f is injective, hence an isomorphism. Thus $M \cong R^n$ is free. □

Exercise 3.3.7. *Every exact sequence* $0 \to A' \to A \to A'' \to 0$ *can be imbedded in a commutative diagram*

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P' & \longrightarrow & P & \longrightarrow & P'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A' & \longrightarrow & A & \longrightarrow & A'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

in which all rows and columns are exact, the middle row splits and consists of projective modules. In fact, the following are exact sequences

$$0 \to M' \to P' \to A' \to 0, \quad 0 \to M'' \to P'' \to A'' \to 0,$$

with P' *and* P'' *projective.*

Definition 3.3.8. Let M be an R-module. A sequence of R-modules and R-module homomorphisms:

$$\mathcal{P}: \quad \cdots \to P_2 \xrightarrow{f_2} P_1 \xrightarrow{f_1} P_0 \xrightarrow{\pi} M \to 0$$

is called a **projective resolution of** M, if for all $i \geq 0$, P_i's are projective R-module, and $\mathrm{im}(f_{i+1}) = \ker(f_i)$. Any R-module admits a projective resolution.

Definition 3.3.9. A module Q is **injective** if and only if for every injective module homomorphism $f : N \hookrightarrow M$ and every module homomorphism $g : N \to Q$, there exists a homomorphism $h : M \to Q$ such that $h \circ f = g$.

Exercise 3.3.10. *The following a equivalent for an* R*-module* Q*.*

1. Q *is injective;*

2. Every exact sequence $0 \to Q \to B \to C \to 0$ *splits, that is* $B \cong Q \oplus C$*;*

3. $\mathrm{Hom}_R(*, Q)$ *is exact.*

Exercise 3.3.11. *Every exact sequence* $0 \to A' \to A \to A'' \to 0$ *can be imbedded in a commutative diagram*

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A' & \longrightarrow & A & \longrightarrow & A'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & Q' & \longrightarrow & Q & \longrightarrow & Q'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

in which all rows and columns are exact, the middle row splits and consists of injective modules. In fact, the following are exact sequences

$$0 \to A' \to Q' \to N' \to 0, \quad 0 \to A'' \to Q'' \to N'' \to 0,$$

with Q' *and* Q'' *projective.*

3.4 Tensor Product of Modules

Definition 3.4.1. Let M, N, P be three R-modules. A mapping $f : M \times N \to P$ is said to be a R**-bilinear** if for each $m \in M$ the mapping $n \to f(m, n)$ of T into P is R-linear, and for each $n \in N$, the mapping $m \to f(m, n)$ of M into P is R-linear.

We can construct an R-module R, namely, the **tensor product of** M **and** N with the property that the R-bilinear mapping $M \times N \to P$ are in a natural one-to-one correspondence with the R-linear mappings $T \to P$, for all R-modules P.

We can summarize this property as the following

Proposition 3.4.2. *Let* M *and* N *be* R*-modules. Then there exists a pair* (T, g) *consisting of an* R*-module* T *and an* R*-bilinear map* $g : M \times N \to T$ *with the following properties:*

1. *Given any R-module P and any R-bilinear map $f : M \times N \to P$, there exists a unique R-linear mapping $h : T \to P$, such that $f = h \circ g$.*

2. *If (T, g) and (T, g') are two pairs with this property, then there exists a unique isomorphism $k : T \to T'$ such that $k \circ g = g'$.*

Proof. (Existence:) Let B denote the free R-module, and the elements of B are formal linear combinations of elements of $M \times N$ with coefficients in R, i.e., $\sum_{i=1}^{s} r_i(m_i, n_i)$ where $r_i \in R$, $m_i \in M$ and $n_i \in N$. Let C be a submodule of B generated by the elements of B of the following form:

$$(m + m', n) - (m, n) - (m', n);\ (m, n + n',) - (m, n) - (m, n');$$

$$(am, n) - a(m, n);\ (m, an) - a(m, n).$$

Let $T = B/C$. If $(m, n) \in B$ is a basis element of C, then let $m \otimes n$ be its image in T. Then T is generated by the elements of the form $m \otimes n$, and we have

$$(m + m') \otimes n = m \otimes n + m' \otimes n,\ m \otimes (n + n') = m \otimes n + m \otimes n',$$

$$am \otimes n = m \otimes an = a(m \otimes n).$$

This mapping $g : M \times N \to T$ defined by $g(m, n) = m \otimes n$ is R-bilinear.

Any map f of $M \times N$ into an R-module P extends by linearity to an R-module homomorphism $h : B \to P$. If f is R-bilinear, then h vanishes on all the generators of C. Hence h is a well-defined R-homomorphism of $T = B/C$ into P such that $h(m \otimes n) = f(m, n)$. The mapping h is uniquely defined by this condition, and the pair (T, g) satisfies the condition (1).

(Uniqueness) Replace (P, f) by (T', g') we get a unique map $k : T \to T'$ such that $g' = k \circ g$. Exchange T and T', we have $k : T' \to T$ such that $g = k' \circ g'$. Hence the composition $k \circ k'$ and $k' \circ k$ are identities. Thus, we must have that k is an isomorphism. □

The result of Proposition 3.4.2 can be extend to the situation of $M_1, \ldots, M_r$ R-modules.

We need to note that suppose M' and N' are submodules of M and N, $m \in M'$ and $n \in N'$. Then $m \otimes n$ can be zero in $M \otimes N$, but non-zero in $M' \otimes N'$. For example, let $R = \mathbb{Z}$, $M = \mathbb{Z}$, $N = \mathbb{Z}/2\mathbb{Z}$, $M' = 2\mathbb{Z}$, and $N' = N$, then $2 \oplus 1 = 1 \oplus 2 = 0 \in M \otimes N$, but $2 \otimes 1 \neq 0 \in M' \otimes N'$.

Remark 3.4.3. 1. Let M, N, P be R-modules. Then there exist unique homomorphisms:

a. $M \otimes N \to N \otimes M$ by $m \otimes n \to n \otimes m$.

b. $(M \otimes N) \otimes P \to M \otimes (N \otimes P) \to M \otimes N \otimes P$ by $(m \otimes n) \otimes p \to m \otimes (n \otimes p) \to m \otimes n \otimes p$;

c. $(M \oplus N) \otimes P \to (M \otimes P) \oplus (N \otimes P)$ by $(m \oplus n) \otimes p \to (m \otimes p) \oplus (n \otimes p)$;

d. $R \otimes M \to M$ by $r \otimes m \to rm$.

2. Let R, S be rings, and let M be an R-module, P an S-module, and N an $(R.S)$-module, that is N is simultaneously R-module and S-module, and $r(ns) = (rn)s$ for all $r \in R$, $s \in S$ and $n \in N$. Then $M \otimes_R N$ is a S-module, and $N \otimes_S P$ an R-module, and we have

$$(M \otimes_R N) \otimes_S P \cong M \otimes_R (N \otimes_S P).$$

3. Let $f : M \to M'$, $g : N \to N'$ be homomorphisms of R-modules. Define $h : M \times N \to M' \otimes N'$ by $f(m, n) = f(m) \otimes g(n)$. h is R-bilinear, and induces an R-module homomorphism: $f \otimes g : M \times N \to M' \otimes N'$ such that $(f \otimes g)(m, n) = f(m) \otimes g(n)$ for all $m \in M$ and $n \in N$. Moreover, if $f' : M' \to M''$ and $g' : N' \to N''$ are homomorphisms of R-modules. Then $((f' \circ f) \otimes (g' \circ g))(m \otimes n) = ((f' \otimes g') \circ (f \otimes g))(m \otimes n)$ for all $m \otimes n \in M \otimes N$.

Let $f : R \to S$ be a ring homomorphism, and N a S-module. Then N has an R-module structure defined by $r \in R$, $n \in N$, and rn is defined to be $f(r)n$. This R-module structure is obtained from N by *restriction of scalars*. In this way, f defines an R-module structure on S.

Hence, if $n_1, \ldots, n_p$ generate N over S, and let $s_1, \ldots, s_q$ generate S as an R-module. Then the product $n_i s_j$ for $i = 1, \ldots, p$ and $j = 1, \ldots q$ generate N over R. Therefore, we have the following result:

Proposition 3.4.4. *Suppose N is finitely generated as a S-module, and S is finitely generated as an R-module, then N is finitely generated as an R-module.*

On the other hand, if M is an R-module, and we can consider S as an R-module, thus we can form an R-module $M_S = S \otimes M$, where M_S carries a S-module structure such that $s(s' \otimes m) = ss' \otimes m$ for all $s, s' \in S$ and $m \in M$. The S-module structure of M_S is obtained from M by *extension of scalars*.

Hence, if $m_1, \ldots, m_p$ generate M over R, then the elements $1 \otimes m_i$ generate M over S. Thus, we have the following result:

Proposition 3.4.5. *If M is finitely generated as an R-module, then M_S is finitely generated as a S-module.*

Let $f : M \times N \to P$ be an R-bilinear mapping, then f gives rise to an R-linear mapping $M \to \mathrm{Hom}(N, P)$ since for each $m \in M$, the mapping $n \in N \to f(m, n) \in P$ is R-linear, and on the other hand, every R-homomorphism $\phi : M \to \mathrm{Hom}_R(N, P)$ defines a bilinear map $(m, n) \in M \times N \to \phi(m)(n) \in P$. Hence the set of R-bilinear mapping $M \times N \to P$ is one-to-one correspondence with $\mathrm{Hom}(M \otimes N, P)$ by the property of the tensor product, hence there is an isomorphism

$$\mathrm{Hom}(M \otimes N, P) \cong \mathrm{Hom}(M, \mathrm{Hom}(N, P)).$$

Use the above property, and the condition that $M' \to M \to M'' \to 0$ is an exact if and only if

$$0 \to \mathrm{Hom}(M'', \mathrm{Hom}(N, P)) \to \mathrm{Hom}(M, \mathrm{Hom}(N, P)) \to \mathrm{Hom}(M', \mathrm{Hom}(N, P))$$

is exact, we can show

Exercise 3.4.6. *Let*

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

be an exact sequence of R-modules and homomorphisms, and let N be an R-module. Then the following sequence is exact:

$$M' \otimes N \xrightarrow{f \otimes 1} M \otimes N \xrightarrow{g \otimes 1} M'' \otimes N \longrightarrow 0.$$

Note, in general, tensor does not preserve the exactness, that is it is not true that if $M' \to M \to M''$ is an exact sequence then $M' \otimes N \to M \otimes N \to M'' \otimes N$ is exact. If $T_N : M \to M \otimes N$ preserves the exact sequence, then N is called *flat* R-module. In the following section, we will discuss about the flat modules.

3.5 Flatness

Definition 3.5.1. Let R be a ring, and M an R-module. We let $C_\bullet$ be a sequence

$$C_\bullet : \quad \cdots \to N' \to N \to N'' \to \cdots$$

of R-modules and R-module homomorphisms, we let $C_\bullet \otimes_R M$, or simply $C_\bullet \otimes M$ be the induced sequence

$$C_\bullet \otimes M : \quad \cdots \to N' \otimes M \to N \otimes M \to N'' \otimes M \to \cdots .$$

Then M is **flat over** R or R **flat** if for every exact sequence $C_\bullet$, the sequence $C_\bullet \otimes_R M$ is again exact. Moreover, we call M is **faithfully flat** if for every sequence $C_\bullet$, we have

$$C_\bullet \text{ is exact} \quad \Leftrightarrow \quad C_\bullet \otimes_R M \text{ is exact.}$$

Exercise 3.5.2. *The following are equivalent for an R-module N:*

1. *N is flat.*
2. *If $0 \to M' \to M \to M'' \to 0$ is an exact sequence of R-modules, then the tensor sequence $0 \to M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$ is exact.*
3. *If $f : M' \to M$ is injective, then $f \otimes 1 : M' \otimes N \to M \otimes N$ is injective.*
4. *If $f : M' \to M$ is injective and M', M are finitely generated, then $f \otimes 1 : M' \otimes N \to M \otimes N$ is injective.*

Definition 3.5.3. If $f : R \to S$ is a homomorphism of rings and S is flat as an R-module, we say f is **flat homomorphism**, or S is a **flat R-algebra**.

Due to the tensor product property $(C_\bullet \otimes_R S) \otimes_S M = C_\bullet \otimes_R M$ for any sequence of R-module, we have the following results of "Transitivity": Let S be an R-algebra, and M a S-module. Then the following holds:

1. If S is flat over R, and M is flat over S, then M is flat over R.
2. If S is faithfully flat over R, and M is faithfully flat over S, then M is faithfully flat over R.
3. If M is faithfully flat over both R and S, then S is faithfully flat over R.

Furthermore, due to the fact that $C_\bullet \otimes_S (S \otimes_R M) = C_\bullet \otimes_R M$, we have the following results of "Changing of coefficient ring":

1. If M is flat over R, then $M \otimes_R S$ is flat over S.
2. If M is faithfully flat over R, then $M \otimes_R S$ is faithfully flat over S.

Exercise 3.5.4. *Let R be a ring and M be an R-module. Then the following are equivalent:*

1. *M is faithfully flat over R;*

2. *M is R-flat, and $N \otimes_R M \neq 0$ for any non-zero R-module N;*

3. *M is R-flat, and $\mathfrak{m}M \neq M$ for every maximal ideal $\mathfrak{m}$ in R.*

Exercise 3.5.5. 1. *Let R be a ring, M a flat R-module, and N', N'' two submodules of an R-module N. Then as submodules of $N \otimes M$, we have*

$$(N' \cap N'') \otimes M = (N' \otimes M) \cap (N'' \otimes M).$$

2. *Let $R \to S$ be a flat ring homomorphism, and let I, J be ideals of R. Then*

$$(I \cap J)S = IS \cap JS.$$

3. *If in addition J is finitely generated, then*

$$(I : J)S = IS : JS.$$

Exercise 3.5.6. *Let $f : R \to S$ be a faithfully flat ring homomorphism.*

1. *For any R-module M, the map $M \to M \otimes_R S$ defined by $m \to m \otimes 1$ is injective; in particular, $f : R \to S$ is injective.*

2. *If I is an ideal of R, then $IS \cap R = I$.*

3.6 Localization

In algebraic geometry, the localization of a module is a construction to introduce denominators in a module for a ring. More precisely, it is a systematic way to construct a new module $S^{-1}M$ out of a given module M containing algebraic fractions $\frac{m}{s}$ where $s \in S \subset R$.

The technique of localization has become fundamental, particularly in algebraic geometry, as the link between modules and sheaf theory. Localization of a module generalizes localization of a ring.

If S is a multiplicatively closed set of a ring R, and M is an R-module, we call $S^{-1}M$ the **localization** of M with respect to S. This $S^{-1}M$ is a $S^{-1}R$ module with the obvious addition and scalar multiplication. If $S = R \setminus \mathfrak{p}$ is the complement of a prime ideal $\mathfrak{p}$, then we write $M_{\mathfrak{p}} = S^{-1}M$, and if $S = \{f^n\}_{n \geq 0}$, then we write $M_f = S^{-1}M$. $S^{-1}R$-module homomorphism $S^{-1}g : S^{-1}M \to S^{-1}N$ which maps $S^{-1}g(m/s) = g(m)/s$, moreover, $S^{-1}(g \circ g') = (S^{-1}g) \circ (S^{-1}g')$.

Proposition 3.6.1. *The operation S^{-1} is exact, that is, if*

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

is exact at M, then

$$S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$$

is exact at $S^{-1}M$.

Proof. We first see that $\mathrm{im}(S^{-1}f) \subseteq \ker(S^{-1}g)$, since $g \circ f = 0$ implies that $S^{-1}(g \circ f) = (S^{-1}g) \circ (S^{-1}f) = 0$.

To prove the other inclusion, let $m/s \in \ker(S^{-1}g)$, then $g(m)/s = 0$ in $S^{-1}M$, thus there exists a $t \in S$ such that $tg(m) = 0$ in M''. But since g is a ring homomorphism, $tg(m) = g(tm) = 0$, which suggests that $tm \in \ker(g) = \mathrm{im}(f)$. Hence $tm = f(m')$ for some $m' \in M'$, and in $S^{-1}M$, we have $m/s = f(m')/(st) = (S^{-1}f)(m'/(st)) \in \mathrm{im}(S^{-1}f)$. Therefore, $\ker(S^{-1}g) \subseteq \mathrm{im}(S^{-1}f)$. □

Use the property that localization preserves the exactness, we can show the following:

Exercise 3.6.2. *If M is a finitely generated module over a Noetherian ring R, then every R-module N and multiplicatively closed set S, the map*

$$S^{-1}\mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(S^{-1}M, S^{-1}N), \text{ is an isomorphism.}$$

This result suggests that if M' is a submodule of M, then $M' \to M$ is injective, and $S^{-1}M' \to S^{-1}M$ is injective, thus $S^{-1}M'$ is a submodule of $S^{-1}M$. Hence, if N, P are submodules of an R-module M, then

1. $S^{-1}(N \oplus P) = S^{-1}(N) \oplus S^{-1}(P)$;
2. $S^{-1}(N \cap P) = S^{-1}(N) \cap S^{-1}(P)$;
3. $S^{-1}(M/N) \cong S^{-1}(M)/S^{-1}(N)$ as a $S^{-1}R$-modules.

Proposition 3.6.3. *Let M be an R-module. Then the $S^{-1}R$-modules $S^{-1}M$ and $S^{-1}R \otimes M$ are isomorphic. That is there exists a unique isomorphism*

$$f : S^{-1}R \otimes M \to S^{-1}M, \ f((r/s) \otimes m) = rm/s, \ \forall\, r \in R,\, m \in M,\, s \in S.$$

Thus $S^{-1}R$ is a flat R-module.

Proof. The mapping

$$S^{-1}R \times M \to S^{-1}M \text{ defined by } (r/s, m) \to rm/s$$

is R-bilinear, and then by the universal property of the tensor product, we have an R-homomorphism

$$f : S^{-1}R \otimes_R M \to S^{-1}M,\ f((r/s) \otimes m) = rm/s,\ \forall\, r \in R,\, m \in M,\, s \in S.$$

It is clear that f is surjective, and uniquely defined.

To show f is injective, let $\sum_i (r_i/s_i) \otimes m_i \in S^{-1}R \otimes M$, $s = \prod_i s_i \in S$, and $t_i = \prod_{j \neq i} s_i \in S$, we have that

$$\sum_i (r_i/s_i) \otimes m_i = \sum_i (r_i t_i)/s \otimes m_i = \sum_i 1/s \otimes r_i t_i m_i = 1/s \otimes \sum_i r_i t_i m_i.$$

Let $m = \sum_i r_i t_i m_i$, then one obtains $1/s \otimes m$. Suppose $f((1/s) \otimes m) = 0$, then $m/s = 0$, and $tm = 0$ for some $t \in S$. Thus

$$1/s \otimes m = t/(st) \otimes m = 1/(st) \otimes tm = 1/(st) \otimes 0 = 0.$$

f is injective. Therefore, f is an isomorphism. And by definition, $S^{-1}M$ is a flat R-module. □

Now, if we replace M by $M \otimes N$, the there is a unique isomorphism $f : S^{-1}R \otimes (M \otimes N) = S^{-1}M \otimes_{S^{-1}R} S^{-1}N \to S^{-1}(M \otimes N)$, and hence, as a consequence of this result, we have

Exercise 3.6.4. *If M and N are R-modules, and S is multiplicative set, then*

1. $\mathrm{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N) = \mathrm{Hom}_R(S^{-1}M, S^{-1}N) = \mathrm{Hom}_R(M, S^{-1}N)$.
2. $S^{-1}M \otimes_{S^{-1}R} S^{-1}N = S^{-1}M \otimes_R S^{-1}N$.

3.7 Local Property

Definition 3.7.1. A property P of a ring R or an R-module M is said to be a **local property** if the following is true: R or M has P if and only if $R_\mathfrak{p}$ or $M_\mathfrak{p}$ has P for each prime ideal $\mathfrak{p} \subset R$.

Proposition 3.7.2. *Let M be an R-module. Then the following are equivalent.*

1. $M = 0$;
2. $M_{\mathfrak{p}} = 0$ *for all prime ideals* $\mathfrak{p} \subset R$;
3. $M_{\mathfrak{m}} = 0$ *for all maximal ideals* $\mathfrak{m} \subset R$.

Proof. The implication of 1. to 2. to 3. are clear. We will show that 3. implies 1.

Suppose that $M \neq 0$. Let $I = \mathrm{Ann}(m)$ for some $0 \neq m \in M$, where $I \subsetneq R$ is an ideal and is contained in some maximal ideal $\mathfrak{m}$. Consider $m/1 \in M_{\mathfrak{m}} = 0$, that means there exists $a \in R \setminus \mathfrak{m}$ such that $am = 0$, but this means that $a \in I \subset \mathfrak{m}$ which is impossible. Thus, $M = 0$. □

Since localization preserves the exactness, we can show

Exercise 3.7.3. *Let $\phi : M \to N$ be an R-module homomorphism. Then the following are equivalent:*

1. *ϕ is injective (or surjective);*
2. *$\phi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is injective (or surjective) for all prime ideals $\mathfrak{p} \subset R$;*
3. *$\phi_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective (or surjective) for all maximal ideals $\mathfrak{m} \subset R$.*

We need to note that in general $M_{\mathfrak{m}} \cong N_{\mathfrak{m}}$ for all maximal ideals $\mathfrak{m}$ does not imply that $M \cong N$.

Proposition 3.7.4. *(Chinese Remainder Theorem) Let $I_1, \ldots, I_n$ be ideals in a commutative ring with identity R such that $I_i + I_j = R$ for all $i \neq j$. Let M be an R-module. Then*

$$\frac{M}{\cap I_i M} \cong \bigoplus_{i=1}^{n} \frac{M}{I_i M}.$$

Proof. For each k, there is a map $\dfrac{M}{\cap I_i M} \to \dfrac{M}{I_k M}$, and thus there is a map $\dfrac{M}{\cap I_i M} \to \bigoplus_{i=1}^{n} \dfrac{M}{I_i M}$. This is easily seen to be injective, and we will show that this is an isomorphism, by localizing at every prime ideal of R. For each prime $\mathfrak{p}$, there is a unique index k such that $\mathfrak{p} \supset I_k$, but $I_i \not\subseteq \mathfrak{p}_k$ for $i \neq k$. This follows from the condition $I_i + I_j = R$ for all $i \neq j$. Moreover, for each k, we can find a prime $\mathfrak{p}_k$ which contains I_k. Thus,

$$(\cap I_i M)_{\mathfrak{p}_k} = M_{\mathfrak{p}_k} \cap I_k M_{\mathfrak{p}_k} = I_k M_{\mathfrak{p}_k}, \quad \text{and} \quad M_{\mathfrak{p}_k}/I_i M_{\mathfrak{p}_k} = 0, \, \forall\, i \neq k.$$

Thus,

$$\left(\frac{M}{\cap I_i M}\right)_{\mathfrak{p}_k} = \frac{M_{\mathfrak{p}_k}}{I_k M_{\mathfrak{p}_k}} \cong \left(\frac{M}{I_k M}\right)_{\mathfrak{p}_k} = \left(\bigoplus_{i=1}^{n} \frac{M}{I_i M}\right)_{\mathfrak{p}_k}.$$

Since localization preserves exactness, we have

$$\frac{M}{\cap I_i M} \cong \bigoplus_{i=1}^{n} \frac{M}{I_i M}.$$

□

Again, since localization preserves the exactness, the flat property is also a local property.

Exercise 3.7.5. *For any R-module M, the following are equivalent:*

1. *M is a flat R-module;*
2. *$M_{\mathfrak{p}}$ is a flat $R_{\mathfrak{p}}$-module for all prime ideals $\mathfrak{p} \subset R$;*
3. *$M_{\mathfrak{m}}$ is a flat $R_{\mathfrak{m}}$-module for all maximal ideals $\mathfrak{m} \subset R$.*

Proposition 3.7.6. *A finitely generated module M over a Noetherian ring R is projective if and only if $M_{\mathfrak{p}}$ is a free $R_{\mathfrak{p}}$ module for all prime ideals $\mathfrak{p}$.*

Proof. ($\Rightarrow$) M is a projective module, hence M is the direct summand of a free module. The localization of projective R-module at $\mathfrak{p}$ is a projective module over $R_{\mathfrak{p}}$. Thus it is free.

($\Leftarrow$) Let M be finitely generated R-module, and $M_{\mathfrak{p}}$ is a free $R_{\mathfrak{p}}$ module for all prime ideals $\mathfrak{p}$ in R. To show that M is projective, we will show that every surjective map $f : X \to Y$, the induced map $f' : \mathrm{Hom}_R(M, X) \to \mathrm{Hom}_R(M, Y)$ is surjective. By 3.7.3, we only need to show that for all maximal ideals $\mathfrak{m}$, the map $f'_{\mathfrak{m}} : (\mathrm{Hom}_R(M, X))_{\mathfrak{m}} \to (\mathrm{Hom}_R(M, Y))_{\mathfrak{m}}$ is surjective. Since M is finitely generated, we have the following commutative diagram

$$\begin{array}{ccccc} (\mathrm{Hom}_R(M,X))_{\mathfrak{m}} & \longrightarrow & (\mathrm{Hom}_R(M,Y))_{\mathfrak{m}} & & \\ \downarrow\cong & & \downarrow\cong & & \\ \mathrm{Hom}_{R_{\mathfrak{m}}}(M_{\mathfrak{m}}, X_{\mathfrak{m}}) & \longrightarrow & \mathrm{Hom}_{R_{\mathfrak{m}}}(M_{\mathfrak{m}}, Y_{\mathfrak{m}}) & \longrightarrow & 0 \end{array}$$

where the vertical map are isomorphic, and the bottom map is surjective since $M_{\mathfrak{m}}$ is projective $R_{\mathfrak{m}}$-module. Thus, the top map is a surjective map. Hence M is a projective module. □

Definition 3.7.7. An R-module M is **finitely presented** if it is finitely generated and the kernel of the surjection from some finitely generated free module onto M is finitely generated.

Proposition 3.7.8. *Let R be a commutative ring, and P a finitely presented R-module. Then P is projective if and only if $P_{\mathfrak{p}}$ is projective for all prime ideals $\mathfrak{p} \subset R$, and this holds if and only if $P_{\mathfrak{m}}$ is projective for all maximal ideal $\mathfrak{m}$ in R.*

Proof. Let $0 \to K \to R^n \to P \to 0$ be a short exact sequence with K finitely generated. P is projective if and only if $\mathrm{Hom}_R(P, R^n) \to \mathrm{Hom}_R(P, P)$ is onto. By the property of localization, this map is onto if and only if it is onto after localization at all prime ideals or all maximal ideals. Since P is finitely presented, for any multiplicatively closed set $S \subset R$, we have $S^{-1}\mathrm{Hom}_R(P, *)) = \mathrm{Hom}_{S^{-1}R}(S^{-1}P, S^{-1}*)$. Therefore, we have proved the claim. □

3.8 Associated Primes

For modules over a commutative ring, we are interested in the concepts of *annihilators* of an element, and the set of *associated primes*.

Definition 3.8.1. Let M be an R-module, and $m \in M$, we define

$$\mathrm{Ann}(m) = \{r \in R \mid rm = 0\},$$

$$\mathrm{Ann}(M) = \{r \in R \mid \forall\, m \in M, rm = 0\} = \bigcap_{m \in M} \mathrm{Ann}(m),$$

where $\mathrm{Ann}(m)$ is the **annihilator of** $m \in M$, and $\mathrm{Ann}(M)$ is the annihilator of M.

Lemma 3.8.2. *Let $m \in M$, and $\mathfrak{p} \subset R$ a prime ideal. Then $0 \neq m/1 \in M_{\mathfrak{p}}$ if and only if $\mathrm{Ann}(m) \subseteq \mathfrak{p}$.*

Proof. Suppose $m/1 = 0$ if and only if there exists $r \in R \setminus \mathfrak{p}$ such that $rm = 0$ if and only if $r \in \mathrm{Ann}(m)$ if and only if $\mathrm{Ann}(m) \nsubseteq \mathfrak{p}$. □

Definition 3.8.3. A prime ideal $\mathfrak{p}$ is called an **associated prime** for M if there exists $m \in M$ such that $\mathfrak{p} = \mathrm{Ann}(m)$. We write $\mathrm{Ass}(M)$ for the set of associated primes of M. $\mathrm{Ass}(M) = \{\mathfrak{p} \mid \mathfrak{p} = \mathrm{Ann}(m) \text{ for some } m \in M\}$. A prime ideal $\mathfrak{p} \in \mathrm{Ass}(M)$ is called a **embedded prime** if $\mathfrak{p}$ is not a minimal element in $\mathrm{Ass}(M)$.

Remark 3.8.4. If $\mathfrak{p} \in \mathrm{Ass}(M)$, then there exists a $m \in M$ such that $\mathfrak{p} = \mathrm{Ann}(m)$, not just $\mathfrak{p} \supseteq \mathrm{Ann}(m)$.

Example 3.8.5. Consider $R = \mathbb{K}[x, y]$, and $M = \mathbb{K}[x, y]/(x^2, xy)$. Then the ideal (x) and (x, y) both belong to $\mathrm{Ass}(M)$, but (x, y) is an embedded prime since we have a chain $(x) \subset (x, y)$.

Definition 3.8.6. A module is called a **cyclic module** if it is generated by one element.

Lemma 3.8.7. *A prime $\mathfrak{p}$ is an associated prime for M if and only if M contains a submodule isomorphic to $R/\mathfrak{p}$.*

Proof. Let $m \in M$, if $\mathfrak{p} = \mathrm{Ann}(m)$, then $R/\mathfrak{p} \cong Rm$ where Rm is a cyclic submodule of M. □

Lemma 3.8.8. *If $\mathfrak{p}$ is a prime ideal, then* $\mathrm{Ass}(R/\mathfrak{p}) = \{\mathfrak{p}\}$.

Proof. It is obvious that $\mathfrak{p} \in \mathrm{Ass}(R/\mathfrak{p})$. We only need to show there is no other associated primes. Suppose $\mathfrak{q} \in \mathrm{Ass}(R/\mathfrak{p})$, then $R/\mathfrak{p}$ would contain a submodule N, and by previous lemma, we have $N \cong R/\mathfrak{q}$, and N is cyclic. This means that N is a principal ideal in the integral domain $R/\mathfrak{p}$. Hence $R/\mathfrak{p} \cong N$, and $\mathfrak{q} = \mathrm{Ann}(N) = \mathrm{Ann}(R/\mathfrak{p}) = \mathfrak{p}$. □

We also recall that a module M over an integral domain R is *torsion* if for every $m \in M$, there exists $0 \neq r \in R$ such that $rm = 0$; and M is *torsion free* if no non-trivial submodule of M is torsion. Moreover, when $\mathrm{Ann}(M) = 0$, the module M is *faithful*.

Lemma 3.8.9. *Let M be a non-trivial module over a Noetherian integral domain R. Then*

1. *M is torsion if and only if $0 \notin \mathrm{Ass}(M)$.*
2. *M is torsion free if and only if $\mathrm{Ass}(M) = \{0\}$.*

Proof. (1.) M is torsion if and only if for every $m \in M$ there exists $0 \neq r \in R$ such that $rm = 0$, i.e. $0 \neq \mathrm{Ann}(m)$.

(2.) M is torsion free if and only if every $0 \neq m \in M$, $\langle 0 \rangle = \mathrm{Ann}(m)$. □

Lemma 3.8.10. *Let M be a module over a commutative Noetherian ring R, and $0 \neq m \in M$. Let S be a multiplicative closed set in R such that $S \cap \mathrm{Ann}(m) = \emptyset$. Then there exists $\mathfrak{p} \in \mathrm{Ass}(M)$ such that $\mathrm{Ann}(m) \subseteq \mathfrak{p}$ and $S \cap \mathfrak{p} = \emptyset$. In fact, if $\mathfrak{q}$ is any prime ideal such that $\mathrm{Ann}(m) \subseteq \mathfrak{q}$, then there exists $\mathfrak{p} \in \mathrm{Ass}(M)$ with $\mathrm{Ann}(m) \subseteq \mathfrak{p} \subseteq \mathfrak{q}$.*

Proof. Since $\mathrm{Ann}(m) \neq R$, then by Zorn's Lemma, there exists an ideal $\mathfrak{q}$ which is the maximal element with respect to the inclusion $\mathrm{Ann}(m) \subseteq \mathfrak{q}$ and $S \cap \mathfrak{q} = \emptyset$. We claim such an ideal $\mathfrak{q}$ is prime. Let $r, s \notin \mathfrak{q}$, then $S \cap (\langle r \rangle + \mathfrak{q}) \neq \emptyset$ and $S \cap (\langle s \rangle + \mathfrak{q}) \neq \emptyset$ by the maximality of $\mathfrak{q}$. Thus, there exist elements $rr_1 + q_1$ and $sr_2 + q_2$ in S with $r_i \in R$ and $q_i \in \mathfrak{q}$. Then $(rr_1 + q_1)(sr_2 + q_2) = rsr_1r_2 + rr_1q_2 + sr_2q_1 + q_1q_2 \in S$. But since $S \cap \mathfrak{q} = \emptyset$, we must have that $rsr_1r_2 \notin \mathfrak{q}$. Thus $r_1r_2 \notin \mathfrak{q}$. Thus $\mathfrak{q}$ must be a prime ideal.

Now, let $\mathfrak{q} \supseteq \mathrm{Ann}(m)$ be a prime ideal. Since R is Noetherian, among the ideals $\mathfrak{p}$ such that $\mathfrak{p} \subseteq \mathfrak{q}$, and $\mathfrak{p} = \mathrm{Ann}(rm)$ for $r \in R$ and $rm \neq 0$, there exists a maximal ideal which has such a property. Let $\mathfrak{p}$ be such an ideal. $\mathrm{Ann}(m) \subseteq \mathrm{Ann}(rm) = \mathfrak{p}$. We claim that $\mathfrak{p}$ is a prime. Suppose if $r_1r_2 \in \mathfrak{p}$, and $r_2 \notin \mathfrak{p}$, then $r_2rm \neq 0$, and $\mathfrak{p} \subseteq \mathfrak{p} + \langle r_1 \rangle \subseteq \mathrm{Ann}(r_2rm) \subseteq \mathfrak{q}$. By the maximality of $\mathfrak{p}$, we must have that $\mathfrak{p} + \langle r_1 \rangle = \mathfrak{p}$, that is $r_1 \in \mathfrak{p}$. Therefore, $\mathfrak{p}$ is a prime. Since $\mathfrak{p} = \mathrm{Ann}(rm)$, $\mathfrak{p} \in \mathrm{Ass}(M)$ such that $\mathrm{Ann}(m) \subseteq \mathrm{Ann}(rm) = \mathfrak{p} \subseteq \mathfrak{q}$. □

Lemma 3.8.11. *If R is Noetherian ring, then $\mathrm{Ass}(M) = \emptyset$ if and only if $M = 0$.*

Proof. It is clear that if $M = 0$, then $\mathrm{Ass}(M) = \emptyset$. Thus, we only need to prove the other direction of the implication. Assume that $M \neq 0$, let $0 \neq m \in M$, then there exists $\mathfrak{p} \supseteq \mathrm{Ann}(m)$, hence $\mathrm{Ass}(M) \neq \emptyset$. □

Therefore, over a Noetherian ring to check whether a module is trivial or not, we only need to check whether there is a associated primes or not.

Proposition 3.8.12. *If $m \in M$, then $m = 0$ if and only if $m/1 = 0 \in M_{\mathfrak{p}}$ for all prime ideals $\mathfrak{p} \in \mathrm{Ass}(M)$.*

Proof. If $0 \neq m \in M$, then there exists a prime ideal $\mathfrak{p} \in \mathrm{Ass}(M)$ such that $\mathrm{Ann}(m) \subseteq \mathfrak{p}$, and hence $0 \neq m/1 \in M_{\mathfrak{p}}$. □

Definition 3.8.13. The **support** of an R-module M is the set of primes such that $M_{\mathfrak{p}} \neq 0$, that is,

$$\mathrm{Supp}(M) = \{\mathfrak{p} \mid M_{\mathfrak{p}} \neq 0\}.$$

Remark 3.8.14. The definition and the property of localization imply:

1. $M_{\mathfrak{p}} = 0$ for all primes $\mathfrak{p}$ if and only if $M = 0$ if and only if $\mathrm{Supp}(M) = \emptyset$.
2. $\mathrm{Supp}_{S^{-1}R} S^{-1}M = \{\mathfrak{p}S^{-1}R \mid \mathfrak{p} \in \mathrm{Supp}(M),\ \mathfrak{p} \cap S = \emptyset\}$;
3. $\mathrm{Ass}_{S^{-1}R} S^{-1}M = \{\mathfrak{p}S^{-1}R \mid \mathfrak{p} \in \mathrm{Ass}(M),\ \mathfrak{p} \cap S = \emptyset\}$;

4. $\mathrm{Ass}_R S^{-1}M = \{\mathfrak{p} \mid \mathfrak{p} \in \mathrm{Ass}(M),\ \mathfrak{p} \cap S = \emptyset\}$.

Proposition 3.8.15. *If M is finitely generated, then*

$$\mathrm{Supp}(M) = \{\mathfrak{p} \mid \mathfrak{p} \text{ is prime and } \mathfrak{p} \supseteq \mathrm{Ann}(M)\}.$$

Proof. First, if $\mathrm{Ann}(M) \nsubseteq \mathfrak{p}$, then there exists an $r \in R \backslash \mathfrak{p}$ such that $rM = 0$, thus $M_\mathfrak{p} = 0$. By the definition of support, we have that $\mathfrak{p} \notin \mathrm{Supp}(M)$.

Now, since M is finitely generated, let $m_1, \ldots, m_n$ be the generators of M. Let $\mathfrak{p}$ be a prime ideal such that $\mathrm{Ann}(M) = \cap_{i=1}^n \mathrm{Ann}(m_i) \subseteq \mathfrak{p}$. Since $\mathfrak{p}$ is prime, by Prime Avoidance Theorem, we must have that $\mathrm{Ann}(m_i) \subseteq \mathfrak{p}$ for some i. Thus for all $r \in R \setminus \mathfrak{p}$, we must have that $r \notin \mathrm{Ann}(m_i)$, and hence $rm_i \neq 0$. Thus, $0 \neq rm_i/1 \in M_\mathfrak{p}$, and $M_\mathfrak{p} \neq 0$. By definition, $\mathfrak{p} \in \mathrm{Supp}(M)$. □

Proposition 3.8.16. *If M is finitely generated R-module and $\mathfrak{p} \in \mathrm{Supp}(M)$, then $\mathfrak{p}M \neq M$.*

Proof. If $\mathfrak{p}M = M$, then localization yields $\mathfrak{p}M_\mathfrak{p} = M_\mathfrak{p}$. Consider M as an $R_\mathfrak{p}$-module, by Nakayama's Lemma, $M_\mathfrak{p} = 0$, thus $\mathfrak{p} \notin \mathrm{Supp}(M)$. □

Corollary 3.8.17. $\mathrm{Ass}(M) \subseteq \mathrm{Supp}(M)$. *On the other hand, if $\mathfrak{q} \in \mathrm{Supp}(M)$, then there exists a $\mathfrak{p} \in \mathrm{Ass}(M)$ such that $\mathfrak{p} \subseteq \mathfrak{q}$. Moreover, if $\mathrm{Ass}(M)$ consists of maximal ideals, the $\mathrm{Supp}(M) = \mathrm{Ass}(M)$.*

Proof. To prove $\mathrm{Ass}(M) \subseteq \mathrm{Supp}(M)$, we let $\mathfrak{p} \in \mathrm{Ass}(M)$, then M contains a submodule N such that $N \cong R/\mathfrak{p}$. Thus $0 \neq N_\mathfrak{p} \subset M_\mathfrak{p}$, hence $\mathfrak{p} \in \mathrm{Supp}(M)$.

To prove the second claim, we let $\mathfrak{q} \in \mathrm{Supp}(M)$, then $M_\mathfrak{q} \neq 0$, hence there exists $m \in M$ such that $0 \neq m/1 \in M_\mathfrak{q}$. Thus, by Lemma 3.8.10, there exists $\mathfrak{p} \in \mathrm{Ass}(M)$ such that $\mathrm{Ann}(m) \subseteq \mathfrak{p} \subseteq \mathfrak{q}$.

The last claim follows directly from the second claim since $\mathfrak{p} \in \mathrm{Ass}(M)$ is the maximal ideal, hence $\mathfrak{p} = \mathfrak{q}$ for each $\mathfrak{q} \in \mathrm{Supp}(M)$. □

Proposition 3.8.18. *If $N \subseteq M$ is a submodule of an R-module M, then* $\mathrm{Ass}(N) \subseteq \mathrm{Ass}(M) \subseteq \mathrm{Ass}(N) \cup \mathrm{Ass}(M/N)$.

Proof. Let $\mathfrak{p} \in \mathrm{Ass}(N)$, then $\mathfrak{p} = \mathrm{Ann}(n)$ for some $n \in N \subseteq M$, hence $\mathfrak{p} \in \mathrm{Ass}(M)$.

Now let $\mathfrak{p} \in \mathrm{Ass}(M) \setminus \mathrm{Ass}(N)$, then there exists $m \in M \setminus N$, such that $0 \neq \bar{m} \in M/N$ and $\mathfrak{p} = \mathrm{Ann}(\bar{m}) \in \mathrm{Ass}(M/N)$. □

Proposition 3.8.19. *If M is finitely generated module over a commutative Noetherian ring, then $\mathrm{Ass}(M)$ is a finite set. (In general, $\mathrm{Supp}(M)$ is not finite.)*

Proof. M is finitely generated over Noetherian ring, then M is Noetherian, hence there exists a submodule N of M maximal with respect to the property that $\mathrm{Ass}(N)$ is finite. We know that $N \neq 0$, since for each $\mathfrak{p} \in \mathrm{Ass}(M)$, there exists a submodule of M which is isomorphic to $R/\mathfrak{p}$ with $\mathrm{Ass}(R/\mathfrak{p}) = \{\mathfrak{p}\}$. Now, we repeat this process to the module M/N. Thus, there is a submodule P/N of M/N such that the $\mathrm{Ass}(P/N)$ is finite. By Proposition 3.8.18, we have that $\mathrm{Ass}(P) \subseteq \mathrm{Ass}(N) \cup \mathrm{Ass}(P/N)$, but this contradicts the maximality of $\mathrm{Ass}(N)$. Hence, $N = M$, and $\mathrm{Ass}(M)$ is finite. □

3.9 Primary Decomposition of Modules

We studied primary ideals, the concepts can be generalized to modules.

Definition 3.9.1. A module M is **$\mathfrak{p}$-primary** if $\mathrm{Ass}(M) = \{\mathfrak{p}\}$.

Proposition 3.9.2. *1. If $\mathfrak{p}$ is a maximal ideal, then for all $n > 0$ the cyclic module $R/\mathfrak{p}^n$ is $\mathfrak{p}$-primary.*

2. If $\mathfrak{p}$ is minimal in $\mathrm{Ass}(M)$, then $M_\mathfrak{p}$ is $\mathfrak{p}$-primary.

3. Let R be a Noetherian ring, M an R-module, and $\mathfrak{p}$ a prime ideal. Then M is $\mathfrak{p}$-primary if and only if the natural map $f : M \to M_\mathfrak{p}$ is one-to-one, and for all $m \in M$ there exists $k \geq 1$ such that $\mathfrak{p}^k m = 0$.

Proof. (1.) Let $\mathfrak{q}$ be a prime, then $\mathfrak{q} \in \mathrm{Supp}(R/\mathfrak{p}^n)$ if and only if $\mathfrak{p}^n \subseteq \mathfrak{q}$. Since $\mathfrak{q}$ is prime and $\mathfrak{p}$ is maximal ideal, we must have that $\mathfrak{p} \subseteq \mathfrak{q} \subseteq \mathfrak{p}$. Thus $\mathfrak{p} = \mathfrak{q}$. Thus $\mathrm{Supp}(R/\mathfrak{p}^n) = \{\mathfrak{p}\}$. Moreover, $\emptyset \neq \mathrm{Ass}(R/\mathfrak{p}^n) \subseteq \mathrm{Supp}(R/\mathfrak{p}^n)$, we must have that $\mathrm{Ass}(R/\mathfrak{p}^n) = \{\mathfrak{p}\}$, and $R/\mathfrak{p}^n$ is $\mathfrak{p}$-primary.

(2.) Since $\mathrm{Ass}(M_\mathfrak{p}) = \{\mathfrak{q} \in \mathrm{Ass}(M) \mid \mathfrak{q} \subset \mathfrak{p}\}$. By minimality of $\mathfrak{p}$, we must have that $\mathrm{Ass}(M_\mathfrak{p}) = \{\mathfrak{p}\}$, hence $M_\mathfrak{p}$ is $\mathfrak{p}$-primary.

(3.) Suppose M is $\mathfrak{p}$-primary, then $\mathrm{Ass}(M) = \{\mathfrak{p}\}$. If $0 = f(m) \in M_\mathfrak{p}$ then $rm = 0$ for some $r \notin \mathfrak{p}$, which shows that $\mathrm{Ann}(m)$ is not contained in the only associated prime $\mathfrak{p}$. This is impossible unless $m = 0$, so f is injective. Now let $r \in \mathfrak{p}$, and let $S = \{r^k \mid k \geq 1\}$. Since $\mathrm{Ass}(S^{-1}M) = \{\mathfrak{p} \mid \mathfrak{p} \in \mathrm{Ass}(M), \mathfrak{p} \cap S = \emptyset\}$, we must have that $\mathfrak{p} \notin \mathrm{Ass}(S^{-1}M)$, hence $\mathrm{Ass}(S^{-1}M) = \emptyset$. This in turn shows that $S^{-1}M = 0$, which means that for each $m \in M$ there exists $r^k \in S$ such that $r^k m = 0$ for some $k \geq 1$.

Now, suppose that $f : M \to M_\mathfrak{p}$ is one-to-one. By Proposition 3.8.18, we have that $\mathrm{Ass}(M) \subseteq \mathrm{Ass}(M_\mathfrak{p})$. It is suffices to show that $\mathrm{Ass}(M_\mathfrak{p}) = \{\mathfrak{p}\}$. Without loss of generality, we assume $M = M_\mathfrak{p}$. Let $\mathfrak{q} \in \mathrm{Ass}(M)$, then $\mathfrak{q} \subseteq \mathfrak{p}$ and $\mathfrak{q} = \mathrm{Ann}(m)$ for some $0 \neq m \in M$. By the given condition,

$\mathfrak{p}^k \subseteq \mathrm{Ann}(m) = \mathfrak{q} \subseteq \mathfrak{p}$. since $\mathfrak{p}$ is a prime, we must have that $\mathfrak{p} = \mathfrak{q}$. Thus M is $\mathfrak{p}$-primary. □

Definition 3.9.3. We call $r \in R$ such that $rm = 0$ for some $0 \neq m \in M$ a **zero divisor on** M.

Proposition 3.9.4. *If R is Noetherian, then $\bigcup\{\mathfrak{p} \mid \mathfrak{p} \in \mathrm{Ass}(M)\}$ is the set of elements in M which are zero divisors.*

Proof. Let $Z \subseteq R$ be the set of zero divisors on M. It is obvious that $\cup\{\mathfrak{p} \mid \mathfrak{p} \in \mathrm{Ass}(M)\} \subseteq Z$. We only need to show the other inclusion. Let $r \in Z$, then $rm = 0$ for some $0 \neq m \in M$, then $r \in \mathrm{Ann}(m) \subseteq \mathfrak{p}$ for some $\mathfrak{p} \in \mathrm{Ass}(M)$. □

Definition 3.9.5. Let R be a Noetherian ring and M a finitely generated R-module. A submodule $N \subseteq M$ is said to be **primary** if $N \neq M$ and whenever $r \in R$, $m \in M \setminus N$, and $rm \in N$, then there exists a positive integer such that $r^n M \subset N$.

Lemma 3.9.6. *Let $N \subseteq M$ be a primary submodule, then $\sqrt{N :_R M}$ is a prime ideal.*

Proof. Let $r, s \in R$ such that $rs \in \sqrt{N :_R M}$, but $s \notin \sqrt{N :_R M}$. Then there exists a positive integer n such that $(rs)^n M = r^n(s^n M) \subseteq N$. Since $s^n M \subsetneq N$, then there exists a $m \in M$ such that $s^n m \in M \setminus N$, and $r^n M \subset N$ since N is primary in M. Thus $r \in \sqrt{N :_R M}$. □

Definition 3.9.7. Let $N \subseteq M$ be a primary submodule. Then N is **$\mathfrak{p}$-primary** where $\mathfrak{p}$ is the prime ideal $\mathfrak{p} = \sqrt{N :_R M}$.

Lemma 3.9.8. *Let R be a ring, $\mathfrak{p}$ a prime ideal in R, M an R-module, and N a $\mathfrak{p}$-primary submodule of M. Then $N :_R M$ is a $\mathfrak{p}$-primary ideal.*

Proof. Let $I = N :_R M$. Then $\sqrt{I} = \mathfrak{p}$. Let $r, s \in R$ such that $rs \in I$ and $s \notin \mathfrak{p}$. We need to show that $r \in I$. Because $\mathfrak{p}$ is a prime, we see that $r \in \mathfrak{p}$. Thus for a positive integer n, $r^n \in I$. Choose n to be smallest possible with this property: therefore $r^{n-1} M \subsetneq N$. There exists $m \in M$ such that $r^{n-1} m \notin N$. Suppose $n > 1$, then because $rs \in I$, $sr^{n-1} m \in N$ and therefore $s^\ell M \subseteq N$ for some ℓ since N is primary to M. This means that $s^\ell \in I \subseteq \mathfrak{p}$, hence $s \in \mathfrak{p}$. This contradicts the assumption that $s \notin \mathfrak{p}$. Therefore, $n = 1$, hence $r \in \mathfrak{p}$, and $\mathfrak{p}$ is prime ideal. □

Lemma 3.9.9. *The intersection of any two $\mathfrak{p}$-primary submodule of M is $\mathfrak{p}$-primary.*

Proof. Let N, P be two $\mathfrak{p}$-primary submodules of M, then $\mathfrak{p} = \sqrt{N :_R M} = \sqrt{P :_R M}$. We will show that $\mathfrak{p} = \sqrt{(N \cap P) :_R M}$.

Let $r \in \mathfrak{p}$, and $m \in M \setminus (N \cap P)$ such that $rm \in N \cap P$. Then there exist two positive integers a, b such that $r^a M \subseteq N$ and $r^b M \subseteq P$, we let $c = \max\{a, b\}$, then $r^c M \subseteq (N \cap P)$. Thus $r \in \sqrt{(N \cap P) :_R M}$.

On the other hand, $\sqrt{(N \cap P) :_R M} \subseteq \sqrt{N :_R M} \cap \sqrt{P :_R M} = \mathfrak{p}$. Thus we proved both sides of inclusion. □

Definition 3.9.10. Let R be a ring, M an R-module and N a submodule. A **primary decomposition** of N is to write

$$N = N_1 \cap N_2 \cap \cdots \cap N_s, \quad \text{where } N_i\text{'s are primary in } M.$$

In Noetherian ring, every ideal has a primary decomposition, similarly, every module also has a primary decomposition.

Theorem 3.9.11. *Let R be a Noetherian ring, and M a finitely generated R-module. Then every proper submodule N of M has a primary decomposition.*

Definition 3.9.12. A primary decomposition $N = \cap_{i=1}^s N_i$ of a submodule N of M is **irredundant** or **minimal** if the prime ideals $\sqrt{N_i :_R M}$ are distinct for $i = 1, \ldots, n$, and for all $j = 1, \ldots n$, $N \neq \cap_{i \neq j} N_i$.

For minimal decompositions, the primes of the primary modules are uniquely determined: they are the associated primes of M/N. Moreover the primary submodules associated to the *minimal* or *isolated associated primes* (those not containing any other associated primes) are also unique. However the primary submodules associated to the non-minimal associated primes, called *embedded primes* for geometric reasons need not be unique.

Example 3.9.13. Let $N = R = \mathbb{K}[x, y]$ for some field $\mathbb{K}$, and let M be the ideal $\langle xy, y^2 \rangle$. Then M has two different minimal primary decompositions

$$M = \langle y \rangle \cap \langle x, y^2 \rangle = \langle y \rangle \cap \langle x + y, y^2 \rangle.$$

The minimal prime is $\langle y \rangle$ and the embedded prime is $\langle x, y \rangle$.

Minimal primes are important. We note that $\mathrm{Ass}(M/N)$ contains all primes minimal over $\mathrm{Ann}(M/N)$. Hence, to compute $\mathrm{Ass}(M/N)$, we only need to compute the minimal primes of $\mathrm{Ann}(M/N)$, but it is not obvious that the minimal primes of M/N and $\mathrm{Ann}(M/N)$ coincide. As an exercise, one can show the following.

Exercise 3.9.14.

$$\min(\mathrm{Ass}(M/N)) = \min(\mathrm{Ass}(\mathrm{Ann}(M/N))) = \min(\mathrm{Ass}(R/\mathrm{Ann}(M/N))).$$

Similar to ideals, the modules have irredundant primary decomposition as well. This can be done once the decomposition is written, one can remove the component which does not satisfy the conditions one a time. Repeat the process, we obtain an irredundant primary decomposition. Hence, we have the following property.

Proposition 3.9.15. *Let R be a ring, M be an R-module and N a submodule of M. If N has a primary decomposition, then N has an irredundant primary decomposition.*

3.10 Modules of Finite Length

Definition 3.10.1. A module is called a **simple module** if there is no submodule except zero and itself. Let R be a Noetherian commutative ring, and M an R-module. We say that M has **finite length** if and only if it has a **composition series**

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_k = M, \text{ where } M_i/M_{i-1} \text{ is a simple module.}$$

The **length** of the chain is k, the number of links. A composition series is a maximal chain, i.e., length is the maximal.

Proposition 3.10.2. *Suppose that M has a composition series of length n. Then every composition series of M has length n, and every chain in M can be extended to a composition series.*

Proof. Let $\ell(M)$ denote the least length of a composition series of a module M. $\ell(M) = \infty$ means that M has no composition series.

If $N \subset M$, then $\ell(N) < \ell(M)$. Let (M_i) be a composition series of M of minimum length, and let $N_i = N \cap M_i$. Since $N_i/N_{i-1} \subset M_i/M_{i-1}$ and the latter is a simple module, we have either $N_i/N_{i-1} = M_i/M_{i-1}$ or zero. Hence, we can remove the repeated terms and obtain a composition series of N, thus $\ell(N) \leq \ell(M)$. If $\ell(N) = \ell(M)$, then $N_i/N_{i-1} = M_i/M_{i-1}$, for each i, hence $N_i = M_i$.

Any chain in M has length at most $\ell(M)$. Let $0 = M_0 \subseteq M_1 \subseteq M_2 \cdots \subseteq M_k = M$, then we have that $\ell(M) \geq \ell(M_{k-1}) \geq \cdots \geq \ell(M_0) = 0$. Thus $\ell(M) \geq k$.

Consider any composition series of M. If it has length k, then $k \leq \ell(M)$, hence $k = \ell(M)$. Hence all composition series have the same length.

For any chain, if its length is $\ell(M)$, then it must be a composition series; if it length $< \ell(M)$, then it is not a composition series, hence we may insert links to obtain a maximal link. □

Proposition 3.10.3. *M has a composition series if and only if M is both Artinian and Noetherian.*

Proof. If M has a composition series, then the maximal chain is bounded, hence M satisfies both a.c.c. and d.c.c.. Thus M is both Noetherian and Artinian.

On the other hand, we will construct a composition series. Let $M = M_0$, and it has a maximal submodule $M = M_0 \supsetneq M_1$, and so on. Thus we have a strictly decreasing sequence $M = M_0 \supsetneq M_1 \supsetneq \cdots$, since M is Artinian, the chain stationary, that is, there exists M_k such that $M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_k$, this is the composition series. □

Remark 3.10.4. A module is of finite length if it satisfies both the a.c.c and d.c.c. The finite length of the module is denoted by $\ell(M)$, which is the length of any composition series. Jordan-Hölder Theorem asserts that the length of a module M is independent of the particular composition.

Proposition 3.10.5. *Let R be a ring in which $\langle 0 \rangle = \mathfrak{m}_1 \cdots \mathfrak{m}_n$ where $\mathfrak{m}_i$ for $i = 1, \ldots, n$, are maximal ideals. Then R is Noetherian if and only if R is Artinian.*

Proof. The chain $R \supset \mathfrak{m}_1 \supset \mathfrak{m}_1\mathfrak{m}_2 \supset \cdots \supset \mathfrak{m}_1 \cdots \mathfrak{m}_n = 0$, hence this chain satisfies both a.c.c. and d.c.c.. Moreover $\prod_{i=1}^{k} \mathfrak{m}_i / \prod_{i=1}^{k+1} \mathfrak{m}_i$ is a vector space over the field $R/\mathfrak{m}_{k+1}$. Hence, the a.c.c. if and only if d.c.c. for each of the factors, which in turn for the ring R. □

Theorem 3.10.6. *Let R be a Noetherian ring, and M an R-module such that all the associated primes of M are maximal, then $\mathrm{Ass}(M) = \mathrm{Supp}(M)$, and for each $\mathfrak{p} \in \mathrm{Ass}(M)$, the canonical map $M \to M_{\mathfrak{p}}$ is surjective and $M_{\mathfrak{p}}$ is isomorphic to the $\mathfrak{p}$-primary component of M, i.e., $\{m \in M \mid \mathfrak{p}^k m = 0$, for some $k \geq 1\}$. Furthermore, M is the direct sum of its $\mathfrak{p}$-primary components.*

Proof. By Proposition 3.7.3, we only need to show that $M_{\mathfrak{m}} \to (M_{\mathfrak{p}})_{\mathfrak{m}}$ is surjective for every maximal ideal $\mathfrak{m}$. But since $\mathfrak{p}$ is maximal, if $\mathfrak{p} \neq \mathfrak{m}$, then $\mathfrak{m} \notin \mathrm{Ass}(M_{\mathfrak{p}}) = \mathrm{Supp}(M_{\mathfrak{p}})$, so $(M_{\mathfrak{p}})_{\mathfrak{m}} = 0$, so $M_{\mathfrak{m}} \to (M_{\mathfrak{p}})_{\mathfrak{m}}$ is surjective;

if $\mathfrak{p} = \mathfrak{m}$, then $M_\mathfrak{m} \to (M_\mathfrak{p})_\mathfrak{m}$ is the identity map, hence a surjective. Since $M \to M_\mathfrak{p}$ is an injective, we have the map $M \to M_\mathfrak{p}$ is an isomorphism. Therefore, for each maximal ideal $\mathfrak{m}$, the map $M_\mathfrak{m} \to (\oplus_{\mathfrak{p}\in \mathrm{Ass}(M)} M_\mathfrak{p})_\mathfrak{m}$ is isomorphism, hence, $M \to \oplus_{\mathfrak{p}\in \mathrm{Ass}(M)} M_\mathfrak{p}$ is isomorphism.

Now, given $\mathfrak{p} \in \mathrm{Ass}(M)$, since $\mathfrak{p}$ is maximal, we have that $\mathfrak{p} \in \mathrm{Ass}(M_\mathfrak{p}) \subseteq \{\mathfrak{p}\}$. Thus, $\{\mathfrak{p}\} = \mathrm{Ass}(M_\mathfrak{p})$, and $M_\mathfrak{p}$ is $\mathfrak{p}$-primary. By Property 3.9.2, we have that $M_\mathfrak{p} \cong \{m \in M \mid \mathfrak{p}^k m = 0, \text{ for some } k \geq 1\}$. □

Corollary 3.10.7. *If* $\mathrm{Ass}(M)$ *consists of maximal ideals, and* $M_\mathfrak{p} \cong N_\mathfrak{p}$ *for every maximal ideal* $\mathfrak{p}$*, then* $M \cong N$*.*

Proof. If $M_\mathfrak{p} \cong N_\mathfrak{p}$ for every maximal ideal $\mathfrak{p}$, then it is true for every prime ideal $\mathfrak{p}$. Thus $\mathrm{Ass}(M) = \mathrm{Ass}(N)$. By Theorem 3.10.6

$$M \cong \bigoplus_{\mathfrak{p}\in \mathrm{Ass}(M)} M_\mathfrak{p} \cong \bigoplus_{\mathfrak{p}\in \mathrm{Ass}(N)} N_\mathfrak{p} \cong N.$$

□

Proposition 3.10.8. *If* M *is an Artinian module, then* $\mathrm{Ass}(M)$ *is finite, and consists of maximal ideals.*

Proof. If $\mathfrak{p} \in \mathrm{Ass}(M)$, then M contains a submodule which is isomorphic to $R/\mathfrak{p}$. Thus M is Artinian implies that $R/\mathfrak{p}$ is Artinian. As an Artinian integral domain $R/\mathfrak{p}$ is a field, thus $\mathfrak{p}$ is a maximal ideal.

By Theorem 3.10.6, we have $M \cong \oplus_{\mathfrak{p}\in \mathrm{Ass}(M)} M_\mathfrak{p}$, $M_\mathfrak{p} \neq 0$ for all $\mathfrak{p} \in \mathrm{Ass}(M)$, and as Artinian, the direct sum has only finitely many components. Thus $\mathrm{Ass}(M)$ is finite. □

Theorem 3.10.9. *A module* M *over a Noetherian ring* R *has finite length if and only if it is finitely generated and* $\mathrm{Ass}(M)$ *consists of only maximal ideals.*

Proof. M has finite length if and only if M is both Noetherian and Artinian, hence by Proposition 3.10.8, $\mathrm{Ass}(M)$ is finite and consists of maximal ideals.

On the other hand, if M is finitely generated, then it is Noetherian. So there exists a submodule N of M which is maximal with respect to the property of finite length. If $\mathrm{Ass}(M)$ consists of maximal ideals, then $\mathrm{Ass}(M) = \mathrm{Supp}(M)$. Since $\mathrm{Supp}(M/N) \subseteq \mathrm{Supp}(M)$, we must have that $\mathrm{Supp}(M/N)$ consists of maximal ideals, and so $\mathrm{Ass}(M/N) = \mathrm{Supp}(M/N)$. If $\mathfrak{p} \in \mathrm{Ass}(M/N)$, then M/N contains a submodule P/N such that $P \supseteq N$ and $P/N \cong R/\mathfrak{p}$. Since $\mathfrak{p}$ is maximal, P/N is isomorphic to a field, hence it

is simple. Since N has finite length, then P has finite length, contradicting to the maximality of N. Thus $\mathrm{Ass}(M/N) = \emptyset$, so $M/N = 0$, hence $M = N$. Thus, $\mathrm{Ass}(M)$ consists of only maximal ideals. □

Proposition 3.10.10. *Let M over a Noetherian ring have finite length, and $I = \mathrm{Ann}(M)$. Then $\mathrm{Ass}(M)$ consists of prime ideals containing I. Furthermore, length of M is no less than the length of R/I, $\ell(M) \geq \ell(R/I)$.*

Proof. M is over a Noetherian ring with finite length, then $\mathrm{Ass}(M)$ consists of maximal ideals. This means that $\mathrm{Ass}(M) = \mathrm{Supp}(M)$, but by definition $\mathrm{Supp}(M) = \{\mathfrak{p} \text{ prime ideal } \mid \mathfrak{p} \supseteq \mathrm{Ann}(M) = I\}$. Therefore, $\mathrm{Ass}(M) = \mathrm{Ass}(R/I)$. This means that $\mathrm{Ass}(R/I)$ only consists of maximal ideals, and R/I is finitely generated, hence R/I is finite length.

Since $M \cong \oplus_{\mathfrak{p}\in\mathrm{Ass}(M)} M_{\mathfrak{p}}$ and $R/I \cong \oplus_{\mathfrak{p}\in\mathrm{Ass}(R/I)} (R/I)_{\mathfrak{p}}$, we only need to show that $\ell(M_{\mathfrak{p}}) \geq \ell(R/I)_{\mathfrak{p}}$. Without loss of generality, we let R be a local ring, and $I = \mathfrak{p}^k$ where $\mathfrak{p}^{k-1}M \neq 0$. Then for $i < k$, by Nakayama's Lemma, $\mathfrak{p}^{i+1}M \subsetneq \mathfrak{p}^i M$, and the series

$$0 = \mathfrak{p}^k M \subsetneq \mathfrak{p}^{k-1} M \subsetneq \cdots \subsetneq \mathfrak{p}M \subsetneq M$$

of length k can be refined to a composition series, so that $k = \ell(R/I) \leq \ell(M)$. □

We can summarize

Remark 3.10.11. Let R be a commutative Noetherian local ring with the unique maximal ideal $\mathfrak{m}$. Then the following are equivalent:

1. R is Artinian;
2. R has finite length as an R-module;
3. $\mathfrak{m}$ is the only prime ideal in R;
4. $\mathrm{Ass}(R) = \{\mathfrak{m}\}$;
5. $\mathfrak{m}^k = 0$ for some $k \geq 1$;

3.11 Krull Dimension of a Ring

Definition 3.11.1. Let R be a ring. The **spectrum** of R, denoted $\mathrm{Spec}\, R$ is the set of prime ideals of R with the **Zariski topology**, the topology where the closed sets are

$$\mathbb{V}(I) = \{\mathfrak{p} \in \mathrm{Spec}\, R \mid I \subseteq \mathfrak{p}, \text{ for ideals } I \subseteq R\}.$$

Definition 3.11.2. The **height** of a prime ideal $\mathfrak{p}$, denoted $\mathrm{ht}\mathfrak{p}$ is the supremum of integers t such that there exists a chain of prime ideals

$$\mathfrak{p} = \mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \mathfrak{p}_2 \supsetneq \cdots \supsetneq \mathfrak{p}_t, \text{ where } \mathfrak{p}_i \in \operatorname{Spec} R.$$

The **coheight** of $\mathfrak{p}$, denoted by $\mathrm{coht}\mathfrak{p}$, is the supremum of the lengths of the chain

$$\mathfrak{p} = \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \cdots \subsetneq \mathfrak{p}_t, \text{ where } \mathfrak{p}_i \in \operatorname{Spec} R.$$

The height of an arbitrary ideal $I \subseteq R$ is

$$\mathrm{ht} I = \inf\{\mathrm{ht}\mathfrak{p} \mid I \subset \mathfrak{p},\, \mathfrak{p} \in \operatorname{Spec} R\}.$$

The **Krull dimension** of R is

$$\dim R = \sup\{\mathrm{ht}\mathfrak{p} \mid \mathfrak{p} \in \operatorname{Spec} R\}.$$

Remark 3.11.3. It follows from the definition, we have

$$\mathrm{ht}\mathfrak{p} = \dim R_{\mathfrak{p}}, \quad \mathrm{coht}\mathfrak{p} = \dim R/\mathfrak{p}, \quad \mathrm{ht}\mathfrak{p} + \mathrm{coht}\mathfrak{p} \leq \dim R.$$

Theorem 3.11.4. *(Krull Height Theorem) Let R be a Noetherian ring. If an ideal $I \subseteq R$ is generated by n elements, then each minimal prime of I has height at most n. In particular, every ideal $I \subsetneq R$ has finite height.*

Proof. Let $r_1, \ldots, r_n \in R$ and $\mathfrak{p}$ a minimal prime over $(r_1, \ldots, r_n)$. Since localization does not change the height of a prime ideal, without loss of generality, we assume that $\mathfrak{p}$ is the unique maximal ideal in R.

If $n = 0$, then $\mathrm{ht}\mathfrak{p} = 0$.

If $n = 1$, we will prove by contradiction. Suppose $\mathrm{ht}\mathfrak{p} > 1$, that is there exists a prime ideal $\mathfrak{q}$ such that $\mathfrak{p}_0 \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}$, we will show that $\mathfrak{q}R_{\mathfrak{q}}$ is of height 0, hence a contradiction.

Since $\mathfrak{p}$ is minimal over (r_1), then $R/(r_1)$ has only one prime ideal, and $R/(r_1)$ is Artinian, hence the descending chain stabilizes:

$$\mathfrak{q}+(r_1) \supseteq \mathfrak{q}^2R_{\mathfrak{q}} \cap R + (r_1) \supseteq \cdots \supseteq \mathfrak{q}^nR_{\mathfrak{q}} \cap R + (r_1) = \mathfrak{q}^{n+1}R_{\mathfrak{q}} \cap R + (r_1) = \cdots.$$

Thus, we have the following inclusion:

$$\begin{aligned} \mathfrak{q}^nR_{\mathfrak{q}} \cap R &\subseteq \mathfrak{q}^nR_{\mathfrak{q}} \cap R + (r_1) \\ &\subseteq (\mathfrak{q}^{n+1}R_{\mathfrak{q}} \cap R + (r_1)) \cap (\mathfrak{q}^nR_{\mathfrak{q}} \cap R) \\ &= \mathfrak{q}^{n+1}R_{\mathfrak{q}} \cap R + (r_1) \cap \mathfrak{q}^nR_{\mathfrak{q}} \cap R. \end{aligned}$$

Since $\mathfrak{q}^n R_{\mathfrak{q}}$ is primary in $R_{\mathfrak{q}}$, we must have $\mathfrak{q}^n R_{\mathfrak{q}} \cap R$ is primary in R. But $r_1 \notin \mathfrak{q}$, hence it is a non-zero divisor in the ring $R/(\mathfrak{q}R_{\mathfrak{p}} \cap R)$. Thus

$$(r_1) \cap \mathfrak{q}^n R_{\mathfrak{q}} \cap R = r_1(\mathfrak{q}^n R_{\mathfrak{q}} \cap R).$$

Thus

$$\begin{aligned} \mathfrak{q}^n R_{\mathfrak{q}} \cap R &\subseteq \mathfrak{q}^{n+1} R_{\mathfrak{q}} \cap R + (r_1) \cap \mathfrak{q}^n R_{\mathfrak{q}} \cap R \\ &= \mathfrak{q}^{n+1} R_{\mathfrak{q}} \cap R + r_1(\mathfrak{q}^n R_{\mathfrak{q}} \cap R) \\ &\subseteq \mathfrak{q}^n R_{\mathfrak{q}} \cap R. \end{aligned}$$

Thus

$$\mathfrak{q}^n R_{\mathfrak{q}} \cap R = \mathfrak{q}^{n+1} R_{\mathfrak{q}} \cap R = \mathfrak{q}(\mathfrak{q}^n R_{\mathfrak{q}} \cap R) \quad \Rightarrow \quad \mathfrak{q}^n R_{\mathfrak{q}} = \mathfrak{q}(\mathfrak{q}^n R_{\mathfrak{q}}),$$

and by Nakayama's lemma, we must have that $\mathfrak{q}^n R_{\mathfrak{q}} = 0$. Hence, in the Noetherian local ring $(R_{\mathfrak{q}}, \mathfrak{q})$, the maximal ideal $\mathfrak{q}$ is nilpotent, thus $R_{\mathfrak{q}}$ is Artinian, and $\mathfrak{q}R_{\mathfrak{q}}$ must have height zero. Therefore, there is no $\mathfrak{p}_0 \subsetneq \mathfrak{q}$, contradicting the assumption. Hence, $\mathrm{ht}\mathfrak{p} \leq 1$.

For the general case, we can assume by localizing at $\mathfrak{p}$ that R is a local ring with maximal ideal $\mathfrak{p}$. Since $\mathfrak{p}$ is minimal over $(r_1, ..., r_n)$, the ideal $\mathfrak{p}$ is nilpotent modulo the ideal $(r_1, ..., r_n)$ (see Remark 3.10.11). Let $\mathfrak{p}_1 \subsetneq \mathfrak{p}$ be any prime such that there is no prime in-between $\mathfrak{p}$ and $\mathfrak{p}_1$. We will now show that $\mathfrak{p}_1$ is minimal over an ideal generated by $n-1$ elements. If so, then by induction on n, we have $\mathrm{ht}\mathfrak{p}_1 \leq n-1$, and we conclude that $\mathrm{ht}\mathfrak{p} \leq n$ as desired. There must be one of the r_i which is not in $\mathfrak{p}_1$, say $r_1 \notin \mathfrak{p}_1$. Then $\mathfrak{p}$ is minimal over $(\mathfrak{p}_1, r_1)$, and thus $\mathfrak{p}$ is nilpotent modulo $(\mathfrak{p}_1, r_1)$. We therefore have equations $r_i^n = a_i r_1 + s_i$, for $i = 2, ..., n$, $a_i \in R$, $s_i \in \mathfrak{p}_1$, for some $n \geq 1$. We can see that $\mathfrak{p}_1$ is minimal over the ideal $(s_2, ..., s_n)$ as follows. By construction, $\mathfrak{p}$ is nilpotent modulo $(r_1, s_2, ..., s_n)$. This implies that the image $\bar{\mathfrak{p}}$ of $\mathfrak{p}$ in $\bar{R} = R/(s_2, ..., s_n)$ is minimal over $r_1\bar{R}$, and by the case $n = 1$ of this theorem, we get that $\mathrm{ht}\bar{\mathfrak{p}} \leq 1$. But $\bar{\mathfrak{p}}_1 \subsetneq \bar{\mathfrak{p}}$, so we must have $\mathrm{ht}\bar{\mathfrak{p}}_1 = 0$, which shows that $\mathfrak{p}_1$ is minimal over the ideal $(s_2, ..., s_n)$ as required.

□

Theorem 3.11.5. *(Converse of Krull Height Theorem) Let R be a Noetherian ring, and $\mathfrak{p}$ a prime ideal in R with $\mathrm{ht}\mathfrak{p} = n$. Then there exist $r_1, \ldots, r_n \in \mathfrak{p}$ such that $\mathfrak{p}$ is minimal over $(r_1, \ldots, r_n)$.*

Proof. Without loss of generality, we assume that R is a local ring with maximal ideal $\mathfrak{p}$.

If $n = 0$, it is true, we will show the case for $n > 0$.

If $n = 1$, by Primary Decomposition theorem, there exist finite many minimal prime ideals in R

$$(0) = \bigcap_{i=1}^{t} \mathfrak{q}_i,\ \mathfrak{p}_i = \sqrt{\mathfrak{q}_i} \text{ are minimal prime ideals in } R,$$

and by Prime Avoidance theorem, there exists $r_1 \in \mathfrak{p}$ that avoids all the minimal prime ideals. Since $\mathrm{ht}\mathfrak{p} = n = 1$, then it is the only prime ideal in addition to the minimal prime ideals, so $\mathfrak{p}$ is minimal over (r_1).

If $n = 2$, then by Primary Decomposition theorem, there exists finite many minimal prime ideals over (r_1) in R

$$(r_1) = \bigcap_{i=1}^{t} \mathfrak{q}_i,\ \mathfrak{p}_i = \sqrt{\mathfrak{q}_i} \text{ are minimal prime ideals over } (r_1) \text{ in } R,$$

and by Prime Avoidance theorem, there exists $r_2 \in \mathfrak{p}$ that avoids all the minimal prime ideals.

We can continue this process, and obtain $(r_1, \ldots, r_n)$ such that $\mathfrak{p}$ is minimal over $(r_1, \ldots, r_n)$. □

Remark 3.11.6. The above theorems show that in a Noetherian ring, the set of prime ideals satisfies the descending chain condition. In fact, any chain of primes descending from $\mathfrak{p}$ is bounded in length by the number of generators of $\mathfrak{p}$. Nonetheless, a Noetherian ring can have infinite dimension (an example, due to Nagata, can be found in chapter 11, exercise 4 of [AM97]).

3.12 Dimension of Modules

We know that the *Krull dimension* of a ring, denoted by $\dim R$ is the maximum length n of a chain $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ of prime ideals of R. If there is no upper bound on the length of the chain such as in the ring $\mathbb{K}[x_1, x_2, \cdots]$ over the field $\mathbb{K}$, then we let $\dim R = \infty$. We also call the *height* of a prime ideal $\mathfrak{p}$ as the maximum length n of the chain $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n = \mathfrak{p}$. The height of $\mathfrak{p}$ in fact is the dimension of the local ring $R_{\mathfrak{p}}$. The *coheight* of a prime ideal $\mathfrak{p}$ is the maximum length n of a chain of prime ideals $\mathfrak{p} = \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$. It follows from the correspondence theorem, the coheight of $\mathfrak{p}$ in fact is the dimension of the quotient ring $R/\mathfrak{p}$. If I is an arbitrary ideal of R, we define the height of I is the infimum of the heights

of prime ideals $\mathfrak{p} \supseteq I$. The coheight of I is the supremum of the coheight of prime ideals $\mathfrak{p} \subseteq I$.

Similarly, we define the **dimension** of an R-module to be the length of the chains of prime ideals which are related to M as the following.

Definition 3.12.1. We define the **Krull dimension** or **dimension of an R-module** M to be

$$\dim M = \dim R/\mathrm{Ann}(M), \text{ if } M \neq 0. \quad \dim M = 0, \text{ if } M = 0.$$

Suppose M is a nonzero and finitely generated module over the Noetherian ring R.

$$\mathfrak{p} \supseteq \mathrm{Ann}M \text{ if and only if } \mathfrak{p} \in \mathrm{Supp}M,$$

hence

$$\dim M = \sup\{\mathrm{coht}\ \mathfrak{p} \mid \mathfrak{p} \in \mathrm{Supp}M\}.$$

Remark 3.12.2. The following conditions are equivalent:

1. $\dim M = 0$;
2. Every prime ideal in $\mathrm{Supp}M$ is maximal;
3. Every associated prime ideal of M is maximal;
4. The length of M as an R-module is finite;
5. If R is a local ring with maximal ideal $\mathfrak{m}$, then

$$\mathrm{Supp}(M/\mathfrak{m}M) = \mathrm{Ann}(M/\mathfrak{m}M).$$

Definition 3.12.3. Over the Noetherian ring local $(R, \mathfrak{m})$, there exists a smallest positive integer r, called **Chevalley dimension**, $\delta(M)$, such that there exists $a_1, \ldots, a_r \in \mathfrak{m}$, such that the length $\ell(M/(a_1, \ldots, a_r)M) < \infty$. If $M = 0$, then $\delta(M) = -1$.

Definition 3.12.4. Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$. And ideal I of R is said to be an **ideal of definition** if $\mathfrak{m}^n \subseteq I \subseteq \mathfrak{m}$ for some $n \geq 1$. Equivalently, R/I is an Artinian ring.

If $\ell(M) < \infty$, then $\delta(M) = 0$. If I is any ideal of definition of the ring R, then $\ell(M/IM) < \infty$, and $\delta(M)$ is the number of the generators of the ideal I. If R is a local ring with the maximal ideal $\mathfrak{m}$, and $M = R$, then $\ell(R/I) < \infty$ if and only if I is $\mathfrak{m}$-primary. Thus $\delta(R)$ is the minimum of the number of generators of $\mathfrak{m}$-primary ideals.

If $\mathcal{M}$ is a class of R-modules, and let ℓ be a function on $\mathcal{M}$ with values in $\mathbb{Z}$. The function ℓ is called *additive* if for each exact sequence with $M', M, M'' \in \mathcal{M}$

$$0 \to M' \to M \to M'' \to 0 \quad \Rightarrow \quad \ell(M') - \ell(M) + \ell(M'') = 0.$$

For example, the class of finite-dimensional vector spaces V, the dimension is and additive function.

Since one can split long exact sequence into short exact sequences, we obtain the following property:

Exercise 3.12.5. *Let*

$$0 \to M_0 \to M_1 \to \cdots \to M_n \to 0$$

be an exact sequence of R-modules where all M_i and the kernels of all the homomorphism belong to a class of R-modules $\mathcal{M}$. Then for any additive function ℓ on $\mathcal{M}$, we have

$$\sum_{i=0}^{n} (-1)^i \ell(M_i) = 0.$$

Proposition 3.12.6. *Let I be an ideal of definition of the Noetherian local ring R, and let M be an R-module of finite type. Then there is a polynomial $p(x)$ with rational coefficients such that*

$$p(n) = \ell(M/I^n M)$$

for all integers n sufficiently large. We call this the **Hilbert-Samuel polynomial** *and denote it*

$$s_I(M, n) = \ell(M/I^n M), \quad n \gg 0.$$

The Hilbert-Samuel polynomial $s_I(M, n)$ depends on the particular ideal of definition I, but the degree $d(M)$ of $s_I(M, n)$ is the same for all possible choices. To see this let t be an integer such that $\mathfrak{m}^t \subseteq I \subseteq \mathfrak{m}$. Then for all $n \geq 1$, we have $\mathfrak{m}^{tn} \subseteq I^n \subseteq \mathfrak{m}^n$, so we have

$$s_{\mathfrak{m}}(M, tn) \geq s_I(M, n) \geq s_{\mathfrak{m}}(M, n).$$

Hence the three degrees coincide. Moreover,

Exercise 3.12.7. *Let I be an ideal of definition of the Noetherian local ring R, and suppose $0 \to M' \to M \to M'' \to 0$ is an exact sequence of finitely generated R-modules. Then*

$$s_I(M', n) + s_I(M'', n) = s_I(M, n) + r(n),$$

where $r(n)$ is a polynomial of degree less than $d(M) = \deg(s_I(M, n))$, and the leading coefficient of $r(n)$ is nonnegative.

As a direct consequence, if M' is a submodule of M where M is finitely generated module over the Noetherian local ring R, then $d(M') \leq d(M)$.

It can be shown that $\dim M \leq d(M) \leq \delta(M) \leq \dim M$, and therefore

Theorem 3.12.8. *Let M be a finitely generated module over the Noetherian local ring R. Then the following are the same*

1. *The dimension $\dim M$ of the module M;*
2. *The degree $d(M)$ of the Hilbert-Samuel polynomial $s_I(M, n)$, where I is any ideal of definition of R.*
3. *The Chevalley dimension $\delta(M)$ (i.e., least number of generators of an $\mathfrak{m}$-primary ideal of R).*

Hence, as direct consequences of the above result 3.12.8, we have

1. Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$. If M is a finitely generated R-module, then $\dim M < \infty$, and $\dim R < \infty$. Moreover, the dimension of R is the minimum over all ideals I of definition of R, of the number of generators of I.
2. Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$, and residue field $\mathbb{K} = R/\mathfrak{m}$. Then $\dim R \leq \dim_{\mathbb{K}}(\mathfrak{m}/\mathfrak{m}^2)$.
3. If R is a Noetherian ring, then the prime ideals of R satisfy the descending chain condition.
4. Let $\mathfrak{p}$ be a prime ideal of the Noetherian ring R. Then the height of $\mathfrak{p}$ is at most n if only if there is an ideal $I \subseteq R$ that is generated by n elements such that $\mathfrak{p}$ is a minimal prime ideal over I.
5. Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$, and let $a \in \mathfrak{m}$ be a non-zero divisor. Then $\dim R/Ra = \dim R - 1$.

3.13 Rank of Modules

This section, we need some of the homological knowledge, especially, Ext, and we refer the reader to the chapter concerning homological method.

First, we recall the **projective dimension** of an R-module, denoted by $\mathrm{pdim}(M)$, is the length of its minimal projective resolution. If $\mathrm{pdim}(M) = 1$, then the minimal projective resolution is of the form $0 \to P_1 \to P_0 \to M \to 0$. where P_0, P_1 are both finitely generated projective modules. Moreover, we note that $\mathrm{Hom}(*, R)$ is left exact, and since P_0 is projective $\mathrm{Ext}^1_R(P_0, R) = 0$, we have the long exact sequence

$$0 \to \mathrm{Hom}(M, R) \to \mathrm{Hom}(P_0, R) \to \mathrm{Hom}(P_1, R) \to \mathrm{Ext}^1_R(M, R) \to 0.$$

Definition 3.13.1. For a finitely generated R-module M, the **rank of** M, $\mathrm{rank}(M)$ is defined as

$$\mathrm{rank}(M) = \inf\{\mu(M_{\mathfrak{p}}) \mid \ \mathfrak{p} \text{ is a prime ideal in } R\},$$

where $\mu(M_{\mathfrak{p}})$ means the number of the generators of $M_{\mathfrak{p}}$.

Theorem 3.13.2. *(Serre - Murthy Theorem) If M is a finitely generated R-module with $\mathrm{pdim}(M) = 1$. Then the following positive integers are equal.*

1. $\inf\{t \mid \exists$ *exact sequence* $0 \to R^t \to P \to M \to 0,\ P$ *is projective*$\}$.
2. $\inf\{\mu(P_1) \mid \exists$ *exact sequence* $0 \to P_1 \to P \to M \to 0,\ P_1$ *is projective*$\}$.
3. $\mu(\mathrm{Ext}^1_R(M, R))$.

Proof. Let

$m = \inf\{t \mid \exists$ exact sequence $0 \to R^t \to P \to M \to 0,\ P$ is projective$\}$,

$n = \inf\{\mu(P_1) \mid \exists$ exact sequence $0 \to P_1 \to P_0 \to M \to 0,\ P_i$ are projective$\}$,

and $s = \mu(\mathrm{Ext}^1_R(M, R))$.

$(1 \Rightarrow 2)$ Since the exact sequence in (1) is of the form of (2), this shows that $n \leq m$.

On the other hand, given any sequence of the form (2), let $u = \mu(P_1)$. Then there is a surjection $R^u \to P_1$, and we get a splitting $P_1 \oplus Q \cong R^u$. We can construct an exact sequence $0 \to R^u \to P_0 \oplus Q \to M \to 0$ with $P_0 \oplus Q$ a finitely generated projective module. The sequences of type (1) obtained this way must have $u \geq m$; therefore $n \geq m$, because n is the infimum of these u.

Therefore, $m = n$.

$(1 \Rightarrow 3)$ Given condition (1), we obtain an exact sequence

$$0 \to \mathrm{Hom}(M,R) \to \mathrm{Hom}(P,R) \to \mathrm{Hom}(R^m,R) \to \mathrm{Ext}^1_R(M,R) \to 0.$$

$s \leq m$ since the map $\mathrm{Hom}(R^m,R) \to \mathrm{Ext}^1_R(M,R)$ is surjective.

$\mathrm{pdim}(M) = 1$ yields $m = n \geq 1$, and because $\mathrm{Ext}^1_R(M,R) \neq 0$, $s \geq 1$. To show $m \leq s$, it suffice to show that there exists an exact sequence of the form $0 \to R^s \to P \to M \to 0$ with P projective. Let $E_1, \ldots, E_s$ generate $\mathrm{Ext}^1_R(M,R)$, and we will prove this by induction on s. Now any element of $[L] \in \mathrm{Ext}^1_R(M,R)$ corresponds to an exact sequence $0 \to R \to L \to M \to 0$. From this we deduce the long exact sequence

$$\begin{aligned} 0 \longrightarrow \mathrm{Hom}(M,R) &\longrightarrow \mathrm{Hom}(L,R) \longrightarrow \mathrm{Hom}(R,R) \\ &\xrightarrow{g} \mathrm{Ext}^1_R(M,R) \xrightarrow{f} \mathrm{Ext}^1_R(L,R) \longrightarrow 0 \end{aligned}$$

The class of the extension $[L] \in \mathrm{Ext}^1_R(M,R)$ is $g(1)$, $1 \in \mathrm{Hom}(R,R)$, and thus $f([L]) = 0$. Now take $[L]$ to be one of the generators, say, E_1. Because $f(E_1) = 0$, from the above exact sequence we have $\mu(\mathrm{Ext}^1_R(L,R)) < s$. If $s = 1$, we see $\mu(\mathrm{Ext}^1_R(L,R)) = 0$, or in other words, $\mathrm{Ext}^1_R(L,R) = 0$. Let X be any finitely generated R-module. Write a presentation $0 \to Y \to R^a \to X \to 0$, and consider the long exact sequence of $\mathrm{Ext}_R(L,*)$, a segment of which is

$$\mathrm{Ext}^1_R(L,R^a) \to \mathrm{Ext}^1_R(L,X) \to \mathrm{Ext}^2_R(L,Y).$$

We have shown that the left-hand side is zero, so the right-hand arrow is injective. Recall that in any exact sequence $0 \to A \to B \to C \to 0$ of R-modules, we have

$$\mathrm{pdim}(B) \leq \sup\left(\mathrm{pdim}(A), \mathrm{pdim}(C)\right).$$

Applied to $0 \to R \to L \to M \to 0$, we see $\mathrm{pdim}(L) \leq 1$, since we are assuming that $\mathrm{pdim}(M) = 1$. This shows that $\mathrm{Ext}^2_R(L,Y) = 0$, and consequently $\mathrm{Ext}^1_R(L,X) = 0$ for every finitely generated R-module X. This shows that L is a projective module, and we have now constructed an exact sequence $0 \to R \to L \to M \to 0$ with L projective, which is what we set out to do. This completes the step $s = 1$ in the induction.

Now let $s > 1$. By induction hypothesis, we have an exact sequence

$$0 \to R^q \to Q \to L \to 0 \text{ where } Q \text{ is projective, and } q \leq s-1.$$

Thus, consider the following commutative diagram,

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & R^q & & R^q & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & K & \longrightarrow & Q & \xrightarrow{f\circ g} & M \to 0, & \quad K = \ker(f\circ g) \cong R^q \oplus R & \\
 & & \downarrow & & {\scriptstyle f}\downarrow & & & & \\
0 & \longrightarrow & R & \longrightarrow & L & \xrightarrow{g} & M \to 0 & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0 & & & &
\end{array}$$

and by the snake lemma, $0 \to R^{q+1} \to Q \to M \to 0$ is the desired exact sequence, and $q+1 \leq s$. Thus we must have that $s \geq m$.

Therefore, we have shown that $s = m$. □

Theorem 3.13.2 generalizes to any finitely generated R-module of finite projective dimension.

Theorem 3.13.3. *If M is a finitely generated R-module with* $\operatorname{pdim}(M) < \infty$. *Then the following positive integers are equal.*

1. $\inf\{t \mid \exists$ *exact sequence* $0 \to R^t \to P_{n-1} \to \cdots \to P_0 \to M \to 0\}$, *where P_i's are finitely generated projective modules.*

2. $\inf\{\mu(P_n) \mid \exists$ *exact sequence* $0 \to P_n \to \cdots \to P_0 \to M \to 0\}$, *where P_i's are finitely generated projective modules.*

3. $\mu(\operatorname{Ext}^n_R(M, R))$.

3.14 Computational Applications

3.14.1 Tensor Products

There are many applications of tensor product. We will first show how to compute simple tensor products.

Example 3.14.1. Compute $\mathbb{Z}/n \otimes_{\mathbb{Z}} \mathbb{Q}$ where $0 < n \in \mathbb{Z}$.

We claim $\mathbb{Z}/n \otimes_{\mathbb{Z}} \mathbb{Q} = 0$. This is true since for any $x \in \mathbb{Z}/n$ and $y \in \mathbb{Q}$,

$$x \otimes y = x \otimes (n \cdot \frac{y}{n}) = nx \otimes \frac{y}{n} = 0 \otimes \frac{y}{n} = 0.$$

Now, we see how to use tensor product to change the base rings.

Example 3.14.2. For any R-module M the tensor product $M \otimes_R S$ has a natural S-module structure given by

$$s \cdot (m \otimes t) = m \otimes (st) \quad \text{for} \quad s, t \in S,\ m \in M.$$

This is a good way to convert an R-module M into an S-module, since there is a natural isomorphism of abelian groups

$$\mathrm{Hom}_S(M \otimes_R S, N) \cong \mathrm{Hom}_R(M, N), \quad N \text{ is an } S\text{-module},$$

where the maps are given as

$F \in \mathrm{Hom}_S(M \otimes_R S, N) \to f_F \in \mathrm{Hom}_R(M, N)$ such that $f_F(m) = F_f(m \otimes 1)$,

hence $F_f(m \otimes n) = n \cdot f(m)$, and

$f \in \mathrm{Hom}_R(M, N) \to F_f \in \mathrm{Hom}_S(M \otimes_R S, N)$ such that $F_f(m \otimes n) = n \cdot f(m)$.

These two maps are inverses of each other.

Example 3.14.3. $\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{C}$ this generated as a $\mathbb{Q}$-module by $1, i$, hence $\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{R}$ is generated as an $\mathbb{R}$-module by $1 \otimes 1$, $i \otimes 1$. Hence, we can write

$$x(1 \otimes 1) + y(i \otimes 1) = x + yi, \ \ x, y \in \mathbb{R}.$$

Example 3.14.4. We have an isomorphism $R[x] \otimes_R S \cong S[x]$.

Example 3.14.5. Moreover, we claim that $R[x, y] \cong R[x] \otimes_R R[y]$ as R-algebras, i.e., that polynomial rings in several variables can be thought of as tensor products of polynomial rings in one variable. To see this, consider the R-module homomorphisms

$$F : R[x] \otimes_R R[y] \to R[x, y], \text{ such that } F(f \otimes g) = fg,\ f \in R[x],\ g \in R[y],$$

with the inverse map

$$G : R[x, y] \to R[x] \otimes_R R[y], \text{ such that } G(\sum a_{ij} x^i y^j) = \sum a_{ij} x^i \otimes y^j.$$

Now, we also can discuss the dimension of the tensor product.

Example 3.14.6. If $\mathbb{K}$ is a field, M is a $\mathbb{K}$-module with basis elements $x_1, \ldots, x_m$ elements, and N is another $\mathbb{K}$-module with basis elements $y_1, \ldots, y_n$ elements, then $M \otimes_{\mathbb{K}} N$ is generated by $x_i \otimes y_j$, hence

$$\dim_{\mathbb{K}} M \otimes N = \dim_{\mathbb{K}} M \cdot \dim_{\mathbb{K}} N = mn.$$

Moreover, the tensor product gives a good definition of extension of scalars.

Example 3.14.7. Let $\mathbb{K}$ be a field extension of a field k. Let V be a finite-dimensional k-vector space. We will show that $V \otimes_k \mathbb{K}$ is a good definition of the extension of scalars of V from k to K, in the sense that for any $\mathbb{K}$-vector space W

$$\mathrm{Hom}_{\mathbb{K}}(V \otimes_k K, W) \cong \mathrm{Hom}_k(V, W).$$

To see this, we note for any k-vector space V the tensor product $V \otimes_k \mathbb{K}$ has a natural K-module structure given by

$$s \cdot (v \otimes t) = v \otimes st, \quad v \in V,\ s, t \in \mathbb{K}.$$

For any $\mathbb{K}$-module W, we have a natural isomorphism of abelian groups

$$\mathrm{Hom}_{\mathbb{K}}(V \otimes_k K, W) \cong \mathrm{Hom}_k(V, W).$$

We have a bijection:

$$F \in \mathrm{Hom}_{\mathbb{K}}(V \otimes_k K, W) \to f_F \in \mathrm{Hom}_k(V, W) \text{ such that } f_F(v) = F(v \otimes 1),$$

hence, $F(v \otimes s) = s \cdot f_F(v)$, and

$$f \in \mathrm{Hom}_k(V, W) \to F_f \in \mathrm{Hom}_{\mathbb{K}}(V \otimes_k K, W) \text{ such that } F_f(v \otimes s) = s \cdot f(v).$$

3.14.2 Primary Decomposition

Primary decomposition can be viewed as an extension of the fundamental theorem of arithmetic, which states that every integer n is uniquely a product of prime powers $p_i^{a_i}$. This can be viewed as the decomposition of ideals in $\mathbb{Z}$, $(n) = (p_1)^{a_1} \cap \ldots (p_s)^{a_s}$. The ideals $(p_i)^{a_i}$ are (p_i)-primary. The primary decomposition theorem is also called the Lasker-Noether theorem, since it was first proven by Emanuel Lasker [Las05] for the special case of polynomial rings and convergent power series rings, and later was proven in its full generality by Emmy Noether [Noe21]. Noether-Lasker theorem plays an

important role in algebraic geometry, by asserting that every algebraic set may be uniquely decomposed into a finite union of irreducible components.

A straightforward extension of Noether-Lasker theorem from ideals to modules states that every submodule of a finitely generated module over a Noetherian ring is a finite intersection of primary submodules. This generalizes the decomposition of an algebraic set into a finite union of (irreducible) varieties. The Lasker-Noether theorem follows immediately from the following three facts:

1. Any submodule of a finitely generated module over a Noetherian ring is an intersection of a finite number of irreducible submodules.

2. If N is an irreducible submodule of a finitely generated module M over a Noetherian ring then M/N has only one associated prime ideal.

3. A finitely generated module over a Noetherian ring is coprimary if and only if it has at most one associated prime.

To find the primary decomposition for a zero-dimensional ideal, we first define something called general position.

Definition 3.14.8. A maximal ideal $\mathfrak{m} \subset R = \mathbb{K}[x_1, \ldots, x_n]$ is called in **general position with respect to** $>_{\text{lex}}$ if $\mathfrak{m} = \langle x_1 + g_1(x_n), \ldots, x_{n-1} + g_{n-1}(x_n), \ldots, g_n(x_n)\rangle$. for suitable polynomials g_i. A zero-dimensional module $N \subseteq M$ (resp. ideal $I \subseteq R$) is called in **general position with respect to** $>_{\text{lex}}$ if all associated primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ are in general position and if $\mathfrak{p}_i \cap \mathbb{K}[x_n] \neq \mathfrak{p}_j \cap \mathbb{K}[x_n]$, for all $i \neq j$.

One can show that zero-dimensional ideal is isomorphic to an ideal in general position, and obtain a primary decomposition from a zero-dimensional ideal in general position.

Exercise 3.14.9. *Let $I \subset R = \mathbb{K}[x_1, \ldots, x_n]$ be a zero-dimensional ideal. Let $\langle g\rangle = I \cap \mathbb{K}[x_n]$; $g = g_1^{r_1} \cdots g_k^{r_k}$, where g_i is prime and $g_i \neq g_j$ for $i \neq j$. Then*

1. *$I = \bigcap \langle I, g_i^{r_i}\rangle$;*

2. *If I is in general position with respect to $>_{\text{lex}}$ then the $\langle I, g_i^{r_i}\rangle$ are primary ideals.*

Moreover, this says that none of the prime ideals $\langle I, g_i^{r_i}\rangle$ can be omitted, hence the primary decomposition is minimal.

We can generalize the primary decomposition algorithm for zero-dimensional ideals to the case of zero-dimensional modules. There is a close relationship between the associated primes of M/N and $\mathrm{Ass}(\mathrm{Ann}M/N)$.

One can show that

Exercise 3.14.10. *Let $N \subset \mathbb{K}[x_1, \ldots, x_n]$ be a zero-dimensional module in general position with respect to $>_{\mathrm{lex}}$, and $N \subset M$.*

Let $\langle g \rangle = \mathrm{Ann}M/N \cap \mathbb{K}[x_n]$; $g = g_1^{r_1} \cdots g_k^{r_k}$, where g_i is prime and $g_i \neq g_j$ for $i \neq j$. Define $h_i = \prod_{i \neq j} g_j^{r_j}$, then

$$N = \bigcap_{i=1} (N : h_i) \quad \textit{is a minimal primary decomposition.}$$

In Singular, the code "zerodec(I)" produces list of primary ideals, the zero-dimensional decomposition of the zero-dimensional ideal I. For example [GPS01],

```
LIB "primdec.lib";
ring r  = 0,(x,y),dp;
ideal i = x2-2,y2-2;
list pr = zerodec(i);
pr;
==> [1]:
==>    _[1]=y2-2
==>    _[2]=xy+2
==>    _[3]=x2-2
==> [2]:
==>    _[1]=y2-2
==>    _[2]=xy-2
==>    _[3]=x2-2
```

Similarly, the code "zeroMod(N)" produces the minimal primary decomposition of a zero-dimensional module N via Gianni-Trager-Zacharias algorithm [Gia88]. For example [GPS01],

```
LIB "mprimdec.lib";
ring r=0,z,dp;
module N=z*gen(1),(z-1)*gen(2),(z+1)*gen(3);
list l=zeroMod(N);
==> 2
l;
==> [1]:
```

```
==>    [1]:
==>       _[1]=gen(1)
==>       _[2]=gen(3)
==>       _[3]=z*gen(2)-gen(2)
==>    [2]:
==>       _[1]=z-1
==> [2]:
==>    [1]:
==>       _[1]=gen(2)
==>       _[2]=gen(3)
==>       _[3]=z*gen(1)
==>    [2]:
==>       _[1]=z
==> [3]:
==>    [1]:
==>       _[1]=gen(1)
==>       _[2]=gen(2)
==>       _[3]=z*gen(3)+gen(3)
==>    [2]:
==>       _[1]=z+1
```

In general, for a non-zero dimensional module (or ideal), one can decompose the module $N \subseteq M$ into an equi-dimensional module N' and another module N''. The primary components of N' can be computed using reduction to dimension zero via localization. The decomposition obtained is minimal for N', the equi-dimensional part of the modules, but we may get redundant components from the decomposition of the module $N + h^r \cdot M$. We avoid computing them if we introduce a module check, which is the intersection of the components computed before.

The Singular code "primdecGTZ(I)" produces a list of primary ideals and their associated primes for a proper ideal I. For example [GPS01],

```
LIB "primdec.lib";
ring  r = 0,(x,y,z),lp;
poly  p = z2+1;
poly  q = z3+2;
ideal i = p*q^2,y-z2;
list pr = primdecGTZ(i);
pr;
==> [1]:
==>    [1]:
```

```
==>       _[1]=z6+4z3+4
==>       _[2]=y-z2
==>    [2]:
==>       _[1]=z3+2
==>       _[2]=y-z2
==> [2]:
==>    [1]:
==>       _[1]=z2+1
==>       _[2]=y-z2
==>    [2]:
==>       _[1]=z2+1
==>       _[2]=y-z2
```

Similarly, the Singular code "PrimdecA (N[, i])" produces a list of (not necessarily minimal) primary decomposition of N via a generalized version of the Shimoyama-Yokoyama algorithm [SY96]. For example [GPS01],

```
LIB "mprimdec.lib";
ring r=0,(x,y,z),dp;
module N=x*gen(1)+ y*gen(2),
x*gen(1)-x2*gen(2);
list l=PrimdecA(N);
l;
==> [1]:
==>    [1]:
==>       _[1]=x*gen(1)+y*gen(2)
==>       _[2]=x*gen(2)-gen(1)
==>    [2]:
==>       _[1]=x2+y
==> [2]:
==>    [1]:
==>       _[1]=gen(2)
==>       _[2]=x*gen(1)
==>    [2]:
==>       _[1]=x
==> [3]:
==>    [1]:
==>       _[1]=y*gen(1)
==>       _[2]=y*gen(2)
==>       _[3]=x*gen(1)
==>       _[4]=x*gen(2)
```

```
==>     [2]:
==>        _[1]=y
==>        _[2]=x
```

3.14.3 Krull Dimension

There is a geometric interpretation of dimension. Let X be a variety over an algebraically closed field $\mathbb{K}$. The coordinate ring of X is

$$\mathbb{K}[X] = \mathbb{K}[x_1, \ldots, x_n]/\mathbb{I}(X)$$

where $\mathbb{I}(X)$ is the radical ideal of all polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ vanishing identically on X. X is irreducible if and only if $\mathbb{I}(X)$ is a prime ideal, which is true if and only if the quotient ring $\mathbb{K}[X]$ is an in integral domain. The quotient field $\mathbb{K}(X)$ of $\mathbb{K}[X]$ is a an extension field of $\mathbb{K}$, and is often called the *function field of* X. One can define the dimension of X as the transcendence degree $\mathrm{tr.deg}_{\mathbb{K}}(\mathbb{K}(X))$.

This notion of dimension coincides with the topological dimension of X when X is considered with the Zariski topology. Recall that the topological dimension of a topological space X is defined to be the supremum over all integers n such that there exists a strictly decreasing chain of irreducible closed subsets X_i of X:

$$X_0 \supsetneq X_1 \supsetneq \cdots \supsetneq X_n \neq \emptyset$$

of irreducible subvarieties of X. This corresponding to a strictly increasing chain of prime ideals in $\mathbb{K}[x_1, \ldots, x_n]$,

$$\mathbb{I}(X_0) \subsetneq \mathbb{I}(X_1) \subsetneq \cdots \subsetneq \mathbb{I}(X_n).$$

The geometric idea behind this definition is that making an irreducible subvariety smaller is only possible by reducing its dimension, so that in a maximal chain as above the dimension of X_i should be $\dim X - i$, with X_n being a point, and X_0 an irreducible component of X.

Similarly, the codimension of an irreducible subvariety $Y \subseteq X$ is the greatest length n of a maximal chain $X_0 \supsetneq X_1 \supsetneq \cdots \supsetneq X_n \supseteq Y$, where X_0 should be an irreducible component of X, and the dimension should drop by 1 in each inclusion in the chain. Moreover, $X_n = Y$ in a maximal chain, so that we can think of n as $\dim X - \dim Y$, and hence as what one would expect geometrically to be the codimension of Y in X.

One of the main obstacles when dealing with dimension is that, in general, the maximal chains of prime ideals may have different length. This can be observed by the corresponding geometry.

For example, $X = \mathbb{V}(xz, yz) \subset \mathbb{K}^3$ is the union of a line (the intersection of the planes $x = 0, y = 0$) and a plane $z = 0$. Then there are two chains of irreducible varieties in X of length one or two:

$$\begin{aligned} X_0 = \mathbb{V}(x,y) \supsetneq X_1 = \mathbb{V}(x,y,z) &\quad\Leftrightarrow\quad \langle x,y\rangle \subsetneq \langle x,y,z\rangle \\ X_0' = \mathbb{V}(z) \supsetneq X_2' = \mathbb{V}(z,y) \supsetneq X_3' = \mathbb{V}(z,y,x) &\quad\Leftrightarrow\quad \langle z\rangle \subsetneq \langle z,y\rangle \subsetneq \langle z,y,x\rangle. \end{aligned}$$

The second chain is longer, and in fact, it is the maximal chain since the plane is of dimension 2.

Moreover, we can compute the associated primes of an ideal via the commend "minAssGTZ", and thus compute the irreducible components of an affine algebraic variety.

```
ring r=0,(x,y,z),dp;
LIB "primdec.lib";
ideal I=xz,yz;
minAssGTZ(I);
==> [1]:
==> _[1]=z
==> [2]:
==> _[1]=y
==> _[2]=x
```

This shows that the affine algebraic variety defined by $\mathbb{V}(xz, yz)$ decomposes as the union of the xy-plane and the z-axis.

The Singular code "dim" computes the dimension of the ideal (resp. module) generated by the leading monomials of the given generators of the ideal (resp. module). This is also the dimension of the ideal if it is represented by a standard basis. Note that the dimension of an ideal I means the Krull dimension of the base ring modulo I, and the dimension of a module is the dimension of its annihilator ideal. For example [GPS01],

```
ring r=32003,(x,y,z),dp;
ideal I=x2-y,x3;
dim(std(I));
==> 1
dim(std(ideal(1)));
==> -1
```

Note, that Singular simply computes the leading terms of the generators and proceeds with these. Thus the ideal I should already be given by a Gröbner basis. In the following example, the ideal I defines a curve

in 3-dimensional space, which is the intersection of three surfaces, we can compute the dimension of the ideal. Moreover, we can check the number of the associated prime ideals by the commend "size(minAssGTZ(I))". In this example, we can confirm that the ideal has only one associate prime, hence I is a prime, and the variety is irreducible.

```
ring r=0,(x,y,z),dp;
ideal I=y2-xz,x2y-z2,x3-yz;
dim(groebner(I));
==> 1
ideal J=lead(groebner(I));
J;
==> J[1]=y2
==> J[2]=x2y
==> J[3]=x3
dim(groebner(J));
==> 1
LIB "primdec.lib";
size(minAssGTZ(I));
==>  1
```

3.14.4 Generators of Syzygy Modules

In mathematics, a syzygy is a relation between the generators of a module M. The set of all such relations form a module and is called the *first syzygy module of* M. A relation between generators of the first syzygy module is called a *second syzygy* of M, and the set of all such relations also form a module and is called the *second syzygy module of* M. Continuing in this way, we derive the n-th syzygy module of M as the set of all relations between generators of the $(n-1)$-th syzygy module of M. If M is finitely generated over a polynomial ring over a field, then the Hilbert's Syzygy Theorem assures this process terminates after a finite number of steps. Moreover, the syzygy modules of M are not unique, and they depend on the choice of generators at each step. In this section, we include the fundamental concepts of syzygies. For the convenience of the reader, we only include the basic definitions and results; for details, we suggest the reader to consult the book [CLO98].

Definition 3.14.11. Let R be a ring and let M be a module generated by $F = \{f_1, \ldots, f_t\}$. The **(first) syzygies** of f_i's are the tuples $(r_1, \ldots, r_t) \in R^t$

such that

$$r_1 f_1 + \cdots + r_t f_t = 0.$$

We denote $\mathrm{Syz}(f_1, \cdots, f_t)$ to be the submodule of R^t generated by the (first) syzygies of f_i. A **Koszul syzygy** is one of the form $(f_j)f_i + (-f_i)f_j = 0$ for $i \neq j$. Let $\mathrm{Kos}(f_1, \cdots, f_t) \subset \mathrm{Syz}(f_1, \cdots, f_t)$ be the submodule generated by the Koszul syzygies. We refer to an arbitrary element of $\mathrm{Kos}(f_1, \cdots, f_t)$ as a Koszul syzygy.

Example 3.14.12. Let $\mathbb{C}^{m\times n}[\mathbf{x}]$ be the set of $m \times n$ matrices with entries in $\mathbb{C}[\mathbf{x}] = \mathbb{C}[x_1, \ldots, x_t]$, the polynomial ring in t-variables with coefficients over the complex numbers $\mathbb{C}$. Let M be a module generated by $\mathbf{f}_1, \ldots, \mathbf{f}_n$ where $\mathbf{f}_i \in \mathbb{C}^{m\times 1}[\mathbf{x}]$. Then a first syzygy of M is a polynomial vector $[h_1, \ldots, h_n]^T$ where each $h_i \in \mathbb{C}[\mathbf{x}]$ such that $\sum_{i=1}^n h_i \mathbf{f}_i = \mathbf{0} \in \mathbb{C}^{m\times 1}[\mathbf{x}]$. If we let F be the matrix $[\mathbf{f}_1, \ldots, \mathbf{f}_n]$, then the first syzygy module of M can be written as $\mathrm{Syz}(F) = \{[h_1, \ldots, h_n]^T \mid F \cdot [h_1, \ldots, h_n]^T = \mathbf{0}\}$. It is easy to see that $\mathrm{Syz}(F)$ is a submodule of $\mathbb{C}^{n\times 1}[\mathbf{x}]$, and it is finitely generated.

Suppose $\mathbf{h}_1, \ldots, \mathbf{h}_s \in \mathbb{C}^{n\times 1}[\mathbf{x}]$ is a generating set of $\mathrm{Syz}(F)$, let $\mathbf{f}_i = [f_{1i}, \ldots, f_{mi}]^T \in \mathbb{C}^{m\times 1}[\mathbf{x}]$, $\mathbf{h}_j = [h_{1j}, \ldots, h_{nj}] \in \mathbb{C}^{n\times 1}[\mathbf{x}]$, and define H to be the matrix $[\mathbf{h}_1, \ldots, \mathbf{h}_s]$. Then

$$F \cdot H = \begin{bmatrix} f_{11} & f_{12} & \cdots & f_{1n} \\ f_{21} & f_{22} & \cdots & f_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ f_{m1} & f_{m2} & \cdots & f_{mn} \end{bmatrix} \cdot \begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1s} \\ h_{12} & h_{22} & \cdots & h_{2s} \\ \vdots & \vdots & \cdots & \vdots \\ h_{n1} & h_{n2} & \cdots & h_{ns} \end{bmatrix} = \mathbf{0}_{m\times s};$$

and for any $\mathbf{h} \in \mathrm{Syz}(F)$, we have

$$\mathbf{h} = \sum_{i=1}^{s} c_i \mathbf{h}_i = \begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1s} \\ h_{12} & h_{22} & \cdots & h_{2s} \\ \vdots & \vdots & \cdots & \vdots \\ h_{n1} & h_{n2} & \cdots & h_{ns} \end{bmatrix} \cdot \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_s \end{bmatrix}.$$

For instance, let $F = [x, y, z] \in \mathbb{C}^{1\times 3}[x, y, z]$. The set of generators of $\mathrm{Syz}(F)$ form a matrix $H \in \mathbb{C}^{3\times 3}[x, y, z]$ where

$$H = \begin{bmatrix} y & z & 0 \\ -x & 0 & z \\ 0 & -x & -y \end{bmatrix}, \quad F \cdot H = \mathbf{0}_{3\times 1}.$$

Note, the columns of H form a generating set for $\mathrm{Syz}(F)$ is proved by [Proposition 6, [Lin99]]. In fact, H is the matrix of $\mathrm{Kos}(F)$, the Koszul syzygies of

F. In this example, $\mathrm{Syz}(F) = \mathrm{Kos}(F)$, the syzygy module is generated by the Koszul syzygies.

Definition 3.14.13. If M is a module spanned by the generators $f_1, \ldots, f_t$, then a **presentation matrix for** M is any matrix whose columns generate $\mathrm{Syz}(f_1, \ldots, f_t)$. If A is a presentation matrix for a module M, then we say that A **presents** the module M. In other words, a presentation of M is an exact sequence

$$R^s \xrightarrow{A} R^t \longrightarrow M \to 0, \quad \text{where } A \text{ is a } t \times s \text{ matrix.}$$

If A is an $\ell \times m$ presentation matrix for an R-module M, then any R-module homomorphism $\phi : M \to R^t$ can be represented by a $t \times \ell$ matrix B such that $BA = 0$, where 0 denotes the $t \times m$ zero matrix. Conversely, if B is any $t \times \ell$ matrix with entries in R such that $BA = 0$, then B defines a homomorphism from $M \to R^t$. To learn more about the syzygy modules, we refer the readers to [CLO98] for details.

Singular code "syz" of an ideal or a module in a ring computes the first syzygy of the ideal or the module. If S is a matrix of a left syzygy module of left submodule given by matrix M, then $S^T \cdot M^T = 0$. For example [GPS01],

```
LIB "ncalg.lib";
def R = makeQso3(3);
setring R;
option(redSB);
// we wish to have completely reduced bases:
option(redTail);
ideal tst;
ideal J = x3+x,x*y*z;
print(syz(J));
==> -yz,
==> x2+1
ideal K = x+y+z,y+z,z;
module S = syz(K);
print(S);
==> (Q-1),        (-Q+1)*z,   (-Q)*y,
==> (Q)*z+(-Q+1),(Q-1)*z+(Q),-x+(Q)*y,
==> y+(-Q)*z,    x+(-Q),     x+(-Q+1)
tst = ideal(transpose(S)*transpose(K));
// check the property of a syzygy module (tst==0):
size(tst);
```

```
==> 0
 // now compute the Groebner basis of K ...
K = std(K);
// ... print a matrix presentation of K ...
print(matrix(K));
==> z,y,x
S = syz(K); // ... and its syzygy module
print(S);
==> y,    x,       (Q-1),
==> (Q)*z,(Q),     x,
==> (Q-1),(-Q+1)*z,(Q)*y
tst = ideal(transpose(S)*transpose(K));
// check the property of a syzygy module (tst==0):
size(tst);
==> 0
// but the "commutative" syzygy property does not hold
size(ideal(matrix(K)*matrix(S)));
==> 3
```

4. Graded and Local Rings and Modules

4.1 Graded Rings and Modules

Definition 4.1.1. Let $\mathbb{K}$ be a field and R be a commutative graded $\mathbb{K}$-algebra, that is $R = \oplus_{i\in\mathbb{N}_0} R_i$ such that $R_0 = \mathbb{K}$, the vector space R_1 has finite dimension and $R_i R_j = R_{i+j}$ for every $i, j \in \mathbb{N}_0$ where $\mathbb{N}_0 = \mathbb{Z}_{\geq 0}$. In general, we say that R is **homogeneous** or **graded ring** if and only if R is generated as an R_0-algebra by its forms of degree 1, that is if and only if $R = R_0[R_1]$. A **homogeneous ideal** I in a graded ring $R = \bigoplus_{n\in\mathbb{N}_0} R_n$ is an ideal generated by a set of homogeneous elements, i.e., each one is contained in only one of the R_n. The ideal generated by the element in R_1 is denoted $R_+ = \oplus_{n\neq 0} R_n$, and is called **irrelevant ideal**. A subring $S \subseteq R$ is called **graded subring** if $S = \sum_n (R_n \cap S)$.

This definition can be enlarged in several ways. We can replace $\mathbb{K}$ by any commutative ring $A = R_0$, then we speak of graded A-algebras. We can also allow graded rings to have negative degrees, thus to be indexed by the integers $\mathbb{Z}$. It is not necessary to assume that R is generated as R_0-algebra by its terms of degree 1. In toric geometry, one naturally considers rings which are graded by an arbitrary finitely generated monoid.

Unless otherwise stated, a graded ring will be an $\mathbb{N}_0$-graded ring generated over a field $R_0 = \mathbb{K}$ by its elements of degree 1.

Example 4.1.2. $\mathbb{Z}[x]$, the polynomial ring in one variable x with coefficients in $\mathbb{Z}$, we note that

$$(\mathbb{Z}[x])_k = \{c\, x^k \mid c \in \mathbb{Z}\}, \text{ note } x^k \cdot x^\ell = x^{k+\ell}, \text{ respect to the grading.}$$

The ideal $I = \langle x^2 \rangle$, i.e., all polynomials with no constant or linear terms, is a homogeneous ideal in $\mathbb{Z}[x]$.

$\mathbb{Z}[x_1, \ldots, x_n]$, the polynomial ring in n variables $x_1, \ldots, x_n$ with coefficient in $\mathbb{Z}$.

$$(\mathbb{Z}[x_1, \ldots, x_n])_k = \left\{ p(x_1, \ldots, x_n) = \sum_{i_1, \ldots, i_n} c_{i_1, \ldots, i_n} x_1^{i_1} \cdots x_n^{i_n} \mid \sum_{j=1}^{n} i_j = k,\ k \in \mathbb{Z}_{\geq 0} \right\}.$$

Definition 4.1.3. Let S, R be graded rings, $f : R \to S$ be a ring homomorphism, then f is said to be **graded** or **homogeneous of degree** d if $f(R_n) \subseteq S_{d+n}$ for all n. If R, S are **isomorphic as graded rings** if there exists a homogeneous ring isomorphism between them.

Definition 4.1.4. A **graded module** over R is a module M with a family of subgroups $\{M_i : i \in \mathbb{Z}\}$ of the additive group of M. The elements of M_i are called the **homogeneous elements** of degree i in the grading, and the M_i must satisfy the following properties:

1. As additive groups
$$M = \bigoplus_{i \in \mathbb{Z}} M_i.$$

2. The decomposition of M in part 1 is compatible with the multiplication by elements of R in the sense that
$$R_j M_i \subset M_{j+i}, \quad \forall j \geq 0, \quad \forall i \in \mathbb{Z}.$$

Any submodule $N \subseteq M$ is **graded** if and only if $N_n = M_n \cap N$.

Definition 4.1.5. Let R be a graded ring, and M, N graded R-modules. Let $f : M \to N$ be an R-module homomorphism, then f is said to be **graded** or **homogeneous of degree** d if $f(M_n) \subseteq N_{d+n}$ for all n. If M, N are **isomorphic as graded modules** if there exists a homogeneous module isomorphism between them.

Remark 4.1.6. Let $(M(d))_t = M_{d+t}$. If $f : M \to N$ is a graded homomorphism of degree d, then $f : M(-d) \to N$ is of degree zero.

Without proof, we provide a few properties here concerning the graded rings, modules, and submodules.

Remark 4.1.7. Let R be a graded ring, M a graded R-module and N a submodule of M (not necessarily graded). Let $N^* \subset M$ be the R-submodule generated by the homogeneous components of the elements of N.

I. Then N^* is the largest graded ideal of R contained in N.

II. The following are equivalent:

1. N is a graded R-module;
2. $N = \sum_n N \cap M_n$;
3. For every $n \in N$, all the homogeneous components of n are in N;
4. N has a homogeneous set of generators.

III. If both M, and N are graded. Then M/N is a graded R-module, and

$$(M/N)_n = (M_n + N)/N = \{m + N \mid m \in M_n\}.$$

Definition 4.1.8. A graded R-module M is **free** if there is an isomorphism of graded R-modules:

$$\phi : \bigoplus_{i \in I} R(n_i) \cong M, \quad n_i \in \mathbb{Z}.$$

Proposition 4.1.9. *Let M be a graded R-module, then M is free if and only if it is generated by an R-linearly independent collection of homogeneous elements.*

Remark 4.1.10. Let $f : R \to S$ be a homomorphism of graded rings. Let $I \subset R$, and $J \subset S$ be homogeneous ideals. Then

I. Both extension $IS \subset S$, and the contraction $f^{-1}(J) \subset R$ are again homogeneous.

II. R/I is graded, and

$$(R/I)_n = (R_n + I)/I = \{(m + I)/I \mid m \in R_n\}.$$

III. There is a one-to-one correspondence between graded ideals containing I and the ideals in R/I.

IV. The radical of I, $\sqrt{I} = \{f \mid f^n \in I\}$, is also a homogeneous ideal.

4.2 Graded Localization

Proposition 4.2.1. *Let $\mathfrak{p} \subset R$ be a prime ideal, then $\mathfrak{p}^*$ (i.e., the ideal generated by the homogeneous components of the elements in $\mathfrak{p}$) is also prime. Moreover, a homogeneous ideal $I \subset R$ is prime if and only if for every pair of homogeneous elements $a, b \in R$ with $ab \in I$ and $a \notin I$, then $b \in I$.*

Proof. Suppose that $a, b \in R$ such that $ab \in \mathfrak{p}^*$. We let a', b' be the homogenous components of the highest degrees of a, b respectively. Then $a'b' \in \mathfrak{p}^* \subset \mathfrak{p}$, since $\mathfrak{p}$ is a prime, then either $a' \in \mathfrak{p}$ or $b' \in \mathfrak{p}$. Since a' and b' are homogeneous, we must have that either $a' \in \mathfrak{p}^*$ or $b' \in \mathfrak{p}^*$.

Without loss of generality, we let $a' \in \mathfrak{p}^*$. Suppose $b' \notin \mathfrak{p}*$, then let a'' be the homogenous component of the highest degree of $(a - a')$, then $a''b' \in \mathfrak{p}^* \subset \mathfrak{p}$. Since $\mathfrak{p}$ is a prime, $a'' \in \mathfrak{p}$, and hence $a'' \in \mathfrak{p}^*$. Repeat the process, we have that $a \in \mathfrak{p}^*$.

If $b' \in \mathfrak{p}^*$, then both $a', b' \in \mathfrak{p}^*$, and $(a - a')(b - b') \in \mathfrak{p}^*$. We choose the highest degree term of a'', b'' of $a - a'$ and $b - b'$, and repeat the above arguments, we obtain that either a or b is in $\mathfrak{p}^*$.

Thus, we have that $\mathfrak{p}^*$ is a prime, and the second statement is the direct consequence of the first statement. □

Definition 4.2.2. Given any multiplicative subset $S \subset R$, and a graded R-module M, we define the **homogeneous localization** to be the module of fractions $U^{-1}M$ where $U \subset S$ is the multiplicative subset consisting of all homogeneous elements. This has a natural grading, for an element $\frac{m}{s}$ with $m \in M$ and $s \in S$ both homogeneous, we let $\deg \frac{m}{s} = \deg m - \deg s$. If $M = R$, then we obtain a graded ring, but now we are allowing a graded ring to have terms of negative degree.

Definition 4.2.3. A graded ring is **local** if it has a unique maximal homogeneous ideal $\mathfrak{m} \neq R$. Note that $\mathfrak{m}$ need not be a maximal ideal: it is simply a maximal element among the homogeneous ideals. The structure of $R/\mathfrak{m}$ is addressed in the next proposition.

Proposition 4.2.4. *The following are equivalent for a graded ring R:*

1. *The only homogeneous ideals of R are 0 and R;*
2. *Every non-zero homogenous element is invertible;*
3. *$R_0 = \mathbb{K}$ is a field, and either $R = \mathbb{K}$, or $R = \mathbb{K}[t, t^{-1}]$ for some indeterminant t of positive degree.*

Proof. It is obvious that $1 \Leftrightarrow 2$ and $3 \Rightarrow 2$. Thus, we only need to show that $2 \Rightarrow 3$. To do so, we assume every non-zero element of R is invertible, thus $R_0 = \mathbb{K}$ a field. If $R = R_0 = \mathbb{K}$, then we are done. Otherwise, let $t \in R$ be a homogeneous element of smallest positive degree d, and t is also invertible, and we have a homomorphism:

$$f : \mathbb{K}[x, x^{-1}] \to R, \quad f(x) = t,\ f(x^{-1}) = t^{-1}.$$

Let $\sum_i a_i x^i \in \ker(f)$. Hence $f(\sum_i a_i x^i) = \sum_i a_i t^i = 0$ which implies that $a_i = 0$. Hence $\ker(f) = 0$. Thus f is injective.

On the other hand, if $a \in R$ of degree i. If $i = 0$, then $a \in R_0$. Otherwise, $i = qd + r$, $0 \leq r < d$. If $r > 0$, then at^{-q} is of degree $r < d$, contradicting the fact that t is of smallest degree. Thus $r = 0$. So $i = qd$, and $a = ct^q = f(cx^q)$ for some $c \in R - 0$. Thus, f is onto.

Therefore, f is an isomorphism, and $R = \mathbb{K}[t, t^{-1}]$. □

Remark 4.2.5. The graded ring $R = \mathbb{K}[t, t^{-1}]$ acts like a field. In particular, if M is a graded R-module, then M is free.

Proposition 4.2.6. *(Graded Nakayama's Lemma) Let $(R, \mathfrak{m})$ be a graded local ring, and let M be a finitely generated graded R-module.*

1. *The minimal number of homogeneous generators for M is equal to the rank of $M/\mathfrak{m}M$ over $R/\mathfrak{m}$.*

2. *If $N \subset M$ is a graded R-submodule such that $M = N + \mathfrak{m}M$, then $N = M$. In particular, if $\mathfrak{m}M = M$, then $M = 0$.*

Proof. We will prove the second claim first. Suppose that $\mathfrak{m}M = M$. Let $\{m_1, \ldots, m_t\}$ be the generators for M with $\deg m_i = r_i$. From the equation $\mathfrak{m}M = M$, we must have $m_t = \sum_{j=1}^{t} a_j m_j$ with $a_j \in \mathfrak{m}$ with $\deg a_j = r_t - r_j$. This gives $\sum_{j=1}^{t-1} a_j m_j + (a_t - 1)m_t = 0$. Now $\deg a_t = 0$ and $a_t - 1 \in R_0 \setminus \mathfrak{m}_0$, therefore $a_t - 1$ is invertible, because $R_0/\mathfrak{m}_0 = \mathbb{K}$ is a field by the previous proposition. Thus, we can remove the generator m_t from the list. Continue in this way, we will have that $t = 1$. Now, if $m_1 = am_1$, then for $a \in \mathfrak{m}$, then $(1 - a)m_1 = 0$ which implies that $m_1 = 0$, so we conclude that $M = 0$.

The second half of part 2 follows by replacing M by M/N.

To prove the first claim, we consider a free basis of $M/\mathfrak{m}M$ over $R/\mathfrak{m}$ (see the above remark). We lift these to elements $\{m_1, \ldots, m_t\} \in M$ and consider the kernel K and cokernel C of the resulting map $\bigoplus_{i=1}^{t} R(-r_i) \to M$. One shows that $K = \mathfrak{m}K$ and $C = \mathfrak{m}C$, thus $K = C = 0$.

□

Definition 4.2.7. A graded ring R is **Noetherian** if it is Noetherian as a ring.

Without proof, we state the following remarks:

Remark 4.2.8. The following are equivalent for a graded ring R.

1. R is a Noetherian ring.
2. Every graded ideal of R is finitely generated.
3. R_0 is Noetherian, and R is a finitely generated R_0 algebra.
4. R_0 is Noetherian, and both $R' = \oplus_{n\geq 0} R_n$ and $R'' = \oplus_{n\leq 0} R_n$ are finitely generated R_0 algebras.

4.3 Graded Associated Primes

First, we recall that if R is a Noetherian ring, M a finitely generated R-module, then a submodule N of M is said to be *primary* if $N \neq M$, and whenever $r \in R$, $m \in M \setminus N$, and $rm \in N$, there exists a positive integer n such that $r^n M \subseteq N$. In other words, N is primary in M if and only if for any $r \in R$, whenever multiplication by r on M/N is not injective, then it is nilpotent as a function. A *primary decomposition of* N is an expression of N as a finite intersection of primary submodules of M, i.e., $N = \cap_{i=1}^{s} N_i$ where N_i is primary in M.

Proposition 4.3.1. *Let R be a graded ring, and M an R-submodule of a graded R-module.*

1. *Then every associated prime $\mathfrak{p}$ of M is homogeneous.*
2. *If M is graded, then there exists a homogeneous element $m \in M$ such that $\mathfrak{p} = 0 : m$.*

Proof. To prove the first claim, let $\mathfrak{p} = 0 : m$ for some $m \in M$. Let $m = \sum_j m_j$, where m_j is a homogeneous element of degree j. Let $h = \max\{j \mid m_j \neq 0\}$. Let $p \in \mathfrak{p}$, write $p = \sum_j p_j$ where p_j is a homogenous element of degree j. Let $k = \max\{j \mid p_j \neq 0\}$. Then $p_k m_h$ is the $k + h$ degree component of the element $pm = 0$, hence $p_k m_h = 0$.

Now, we will show that there exists an i such that $p_k^i m = 0$. The strategy of proving this claim is similar to the above, that is using the $k + j$ degree component. Suppose that for all $j' > j$, we proved that $p_k^i m_{j'} = 0$, and

the term of degree $k+j$ in pm is of the form $\sum_{j' \geq j} p_{k+j-j'} m_{j'}$, so that $p_k^{i+1} m_j = 0$. It follows that for some integer i, $p_k^i \in 0 : m = \mathfrak{p}$. Moreover, since $\mathfrak{p}$ is prime, we must have $p_k \in \mathfrak{p}$. Repeat the process, we get every component of p is in $\mathfrak{p}$, hence $\mathfrak{p}$ is graded.

To prove the second claim, we see if M is graded, then $\mathfrak{p} = 0 : m = \cap_j (0 : m_j)$. Thus, for some j, $\mathfrak{p} = 0 : m_j$.

□

As an exercise, one can show the following consequences of the above proposition.

Exercise 4.3.2. *let R be a graded Noetherian ring, and M a finitely generated graded R-module. Then*

1. *Every prime in $\mathrm{Ass}(M)$ is homogeneous. In particular, the minimal primes of R are homogeneous.*

2. *Given any primary decomposition of a graded submodule $N \subset M$ of the form $N = \cap_{i=1}^t N_i$, the decomposition $N = \cap_{i=1}^t N_i^*$ is also a primary decomposition of N. In particular, we can choose the primary components of N to be homogeneous.*

3. *There is a descending chain of graded submodules*

$$M = M_n \supsetneq M_{n-1} \supsetneq \cdots \supsetneq M_0 = 0,$$

such that there is a homogeneous prime $\mathfrak{p}_i \subset R$ and an integer $n_i \in \mathbb{Z}$ such that

$$M_i / M_{i-1} \cong R/\mathfrak{p}_i(n_i), \quad \forall\, 1 \leq i \leq n.$$

Proposition 4.3.3. *(Graded Prime Avoidance Theorem) Let R be a graded ring and I a homogeneous ideal generated by homogeneous elements of positive degree. Suppose $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are homogeneous prime ideals such that $I \subseteq \cup_{i=1}^n \mathfrak{p}_i$, then there exists an $i \in \{1, 2, \ldots, n\}$ such that $I \subseteq \mathfrak{p}_i$.*

Proof. This follows immediately from the ungraded version of this theorem. □

Definition 4.3.4. Let $N \subset M$ be modules over a ring R. Then the set

$$\{\text{prime ideals } \mathfrak{p} \subset R \mid \mathfrak{p} \text{ is minimal over } N :_R m \text{ for some } m \in M\}$$

is called **the set of weakly associated primes of** M/N, and is denoted by $\widetilde{\mathrm{Ass}}(M/N)$. The set

$$\{\text{prime ideals } \mathfrak{p} \subset R \mid \mathfrak{p} = N :_R m \text{ for some } m \in M\}$$

is called **the set of associated primes of** M/N, and is denoted by $\mathrm{Ass}(M/N)$ or $\mathrm{Ass}_R(M/N)$.

Associated prime ideals plays an important role in primary decomposition in commutative algebra, and we will study some the properties.

Proposition 4.3.5. *Let R be a graded ring, M a graded R-module, and $\mathfrak{p} \in \widetilde{\mathrm{Ass}}_{R_0} M_g$. If $\mathfrak{p}$ is minimal over $0 :_{R_0} m$, then there exists a $\mathfrak{q} \in \widetilde{\mathrm{Ass}}_R M$ such that $\mathfrak{q} \cap R_0 = \mathfrak{p}$ and $\mathfrak{q}$ is minimal over $0 :_R m$. In particular, if $\widetilde{\mathrm{Ass}}_R M$ is finite set, then $\cup_g \widetilde{\mathrm{Ass}}_{R_0} M_g$ is a finite set.*

Proof. Let $m \in M_g$ such that $\mathfrak{p}$ is minimal over $0 :_{R_0} m$, $I = 0 :_R m$, and $R_+ = \oplus_{g>0} R_g$. R_+ is a proper ideal in R, and $I + R_+ \subseteq \mathfrak{p} + R_+$ is a proper ideal in R. Since $R/(\mathfrak{p} + R_+) \cong R_0/\mathfrak{p}$, we must have that $\mathfrak{p} + R_+$ is a prime ideal in R.

Now, let $\mathfrak{q}$ be a prime ideal in R which is minimal over $\mathfrak{p}R$ and contained in $\mathfrak{p} + R_+$. Then $\mathfrak{q} \cap R_0 = \mathfrak{p}$. Suppose that $\mathfrak{q}$ is not minimal over I, then let $\mathfrak{q}'$ be a prime containing I and properly contained in $\mathfrak{q}$. Then by the assumption that $\mathfrak{q}$ is minimal over $\mathfrak{p}$, we must have $\mathfrak{p} \not\subseteq \mathfrak{q}'$. Thus, $I \cap R_0 \subseteq \mathfrak{q}' \cap R_0 \subsetneq \mathfrak{q} \cap R_0 = \mathfrak{p}$, contradicting the minimality of $\mathfrak{p}$ over $I \cap R_0$. Thus, $\mathfrak{q}$ must be minimal over I, hence there exists a $\mathfrak{q} \in \widetilde{\mathrm{Ass}}_R M$.

Thus if $\widetilde{\mathrm{Ass}}_R M$ is finite set, then $\cup_g \widetilde{\mathrm{Ass}}_{R_0} M_g$ is a finite set. □

Proposition 4.3.6. *Let $R = R_0[R_1]$ be a Noetherian $\mathbb{N}$-graded ring generated over R_0 by elements of degree 1. Let M be a finitely generated $\mathbb{N}$-graded R-module. Then there exists an integer s such that for all $n \geq s$, $\mathrm{Ass}_{R_0} M_n = \mathrm{Ass}_{R_0} M_s$.*

Proof. Since R is Noetherian, so is M, and the set of $\mathrm{Ass}_R M$ is finite. Thus, by Proposition 4.3.5, we know that $\cup_n \mathrm{Ass}_{R_0} M_n$ is a finite set. We will show that for each prime ideal $\mathfrak{p} \subset R_0$, there exists s such that for all $n \geq s$, $\mathfrak{p} \in \mathrm{Ass}_{R_0} M_n$ if and only if $\mathfrak{p} \in \mathrm{Ass}_{R_0} M_s$.

To prove these equivalent conditions, without loss of generality, let R_0 be a local ring with maximal ideal $\mathfrak{p}$. Moreover, it is easy to see that if $\mathfrak{p} \in \mathrm{Ass}_{R_0} M_s$, then $\mathfrak{p} \in \mathrm{Ass}_{R_0} M_n$ for all $n \geq s$ as long as s is sufficiently large. Namely, take s to be greater than the degrees of all the finitely many generators $\{m_1, ..., m_t\}$ of M. Then every element of M_s can be written as

a linear combination of expressions $x_1^{a_1}...x_r^{a_r}m_j$, where $\sum a_i + \deg m_j = s$, where the x_i are generators of R_1. Moreover an expression like this appears for every generator m_j by the choice of s. Since $\mathfrak{p} \in \mathrm{Ass}_{R_0} M_s$ and $\mathfrak{p}$ is the maximal ideal of the local ring R_0, we see that $\mathfrak{p}^k x_1^{a_1}...x_r^{a_r}m_j = 0$ for some $k \geq 1$ and all generators $x_1^{a_1}...x_r^{a_r}m_j$ of M_s. But by the choice of s, every generator of M_n, $n \geq s$ is of the form $x_1^{b_1}...x_r^{b_r}m_j$, where $x_1^{a_1}...x_r^{a_r}m_j$ is a generator of M_s and $b_j \geq a_j$ for all j. Thus $\mathfrak{p}^k x_1^{b_1}...x_r^{b_r}m_j = 0$ and we see that $\mathfrak{p} \in \mathrm{Ass}_{R_0} M_n$.

To see the other implication, suppose for some $i \geq 0$, $(0 :_M \mathfrak{p}) \subseteq (0 :_M R_1^i)$. Let s' be the maximal degree of an element in a minimal homogeneous generating set of $0 :_M \mathfrak{p}$, and let $s = s' + i$. If $n \geq s$, and $\mathfrak{p} \in \mathrm{Ass}_{R_0} M_n$, we write $\mathfrak{p} = (0 :_{R_0} b)$ for some $b \in M_n$, then $b \in 0 :_{M_n} \mathfrak{p}$. Thus, for all $n - s \geq i$, $b \in R_{n-s}(0 :_M \mathfrak{p}) = 0$. But this is impossible, since we choose $b \neq 0$. Thus, if a prime ideal is such that for some $i \geq 0$, $(0 :_M \mathfrak{p}) \subseteq (0 :_M R_1^i)$, then $\mathfrak{p} \notin \mathrm{Ass}_{R_0} M_n$ for all $n \geq s$.

Thus, let prime ideal $\mathfrak{p}$ be such that for all $i \geq 0$, $(0 :_M \mathfrak{p}) \not\subseteq (0 :_M R_1^i)$. Fix and i such that for all n, $(0 :_M R_1^n) \subseteq (0 :_M R_1^i)$. Let $m \in M$ be a homogeneous element such that $\mathfrak{p}m = 0$ and $R_1^i m \neq 0$. Then for all n, $R_1^n m \neq 0$. Let $s = \deg m$. For any $n \geq s$, $\mathfrak{p} = (0 :_{R_0} R_1^{n-\deg m} m)$, so that $\mathfrak{p} \in \mathrm{Ass}_{R_0} M_n$ for all $n \geq s$. □

4.4 Filtration

Definition 4.4.1. We call R is a **filtered ring**, if $\{R_n\}$ is a **filtration** of the ring R, i.e., R_n are additive subgroups such that

$$R = R_0 \supseteq R_1 \supseteq R_2 \supseteq \cdots \supseteq R_n \supseteq \cdots$$

with $R_m R_n \subseteq R_{m+n}$.

An R-module M is called a **filtered module** if

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots \supseteq M_n \supseteq \cdots$$

over the filtered ring R with $R_m M_n \subseteq M_{m+n}$.

If I is an ideal of the ring R and M is an R-module, the **I-adic filtration** of R (or of M) is defined by $R_n = I^n$ (or $M_n = I^n M$) where $I^0 = R$ (or $M_0 = M$).

Let M be a filtered R-module with filtration $\{M_n\}$, and I an ideal of R. We say that $\{M_n\}$ is an **I-filtration** if $IM_n \subseteq M_{n+1}$ for all n. An I-filtration with $IM_n = M_{n+1}$ for all sufficiently large n is said to be **I-stable**.

It easy to see that I-adic filtration is I-stable.

Definition 4.4.2. Let $\mathcal{I} = \{I^n\}$ be a I-adic filtration of R. We define the **Rees algebra** $\mathcal{R}(\mathcal{I})$ by

$$\mathcal{R}(\mathcal{I}) = \bigoplus_{n=0}^{\infty} I^n t^n \subset R[t], \text{ where } t \text{ is an indeterminate over } R.$$

Sometimes, we also write $\mathcal{R}(\mathcal{I}) = B_I R$. An alternative way to define $\mathcal{R}(\mathcal{I})$ is to describe it as a subring of the graded ring $R[t]$ with $\deg t = 1$, and

$$\mathcal{R}(\mathcal{I}) = \{a_0 + a_1 t + \cdots + a_n t^n \in R[t] \mid a_i \in I^i, \forall i\}.$$

In case I is an ideal of R, we call $\mathcal{R}(\mathcal{I})$ the **Rees algebra of** I and denote it to be $R[It]$.

Definition 4.4.3. Let $\{R_n\}$ be a filtration of R, the **associated graded ring** of R is defined as

$$\mathrm{gr}R = \bigoplus_{n\geq 0} \mathrm{gr}_n(R), \text{ where } \mathrm{gr}_n(R) = R_n/R_{n+1}.$$

If $a \in R_m$, $b \in R_n$, then $a + R_{m+1} \in R_m/R_{m+1}$ and $b + R_{n+1} \in R_n/R_{n+1}$, and

$$(a + R_{m+1})(b + R_{n+1}) = ab + R_{m+n+1}.$$

Let M be a filtered module over a filtered ring R, the **associated graded module** of M is defined as

$$\mathrm{gr}M = \bigoplus_{n\geq 0} \mathrm{gr}_n(M), \text{ where } \mathrm{gr}_n(M) = M_n/M_{n+1}.$$

If $a \in R_m$, $x \in M_n$, then

$$(a + R_{m+1})(x + M_{n+1}) = ax + M_{m+n+1}, \text{ and}$$

$$(R_m/R_{m+1})(M_n/M_{n+1}) \subseteq M_{m+n}/M_{m+n+1}.$$

$\mathrm{gr}(M)$ is a graded module over the grade ring $\mathrm{gr}(R)$.

Definition 4.4.4. We define the **associated graded ring of a ring** R **with respect to a proper ideal** I is the graded ring:

$$\mathrm{gr}_I R = \bigoplus_{n=0}^{\infty} I^n/I^{n+1}.$$

Similarly, if M is an R-module, then the **associated graded module** is the graded module $\operatorname{gr}_I M$ over $\operatorname{gr}_I R$ where

$$\operatorname{gr}_I M = \bigoplus_0^\infty I^n M / I^{n+1} M.$$

Proposition 4.4.5. *Let $R = \oplus_{d \geq 0} R_d$ be a graded ring. Then R is Noetherian if and only if R_0 is Noetherian and R is finitely generated R_0-algebra.*

Proof. If R_0 is Noetherian, then $R \cong R_0[x_1, \dots, x_n]/I$ for some ideal in $R_0[x_1, \dots, x_n]$, hence R is Noetherian.

If R is Noetherian, then $R_0 \cong R/I$ where $I \subseteq \oplus_{d \geq 1} R_d$ is finitely generated by homogeneous elements $a_1, \dots, a_r$ of degree $n_1, \dots, n_r$. Let $R = R_0[a_1, \dots, a_r]$ be the R_0-algebra generated by the a_i's, we need only to show that $R_n \subset R$ for all $n \geq 0$. We will do so by induction on d. It is obvious that $R_0 \subseteq R$, and assume that $R_d \subseteq R$ for $d \leq n-1$, where $n \geq 1$. For $d = n$, if $a \in R_n$, then $a = \sum_{i=1}^r c_i a_i$ where $\deg(c_i) = \deg(a) - n_i < \deg(a)$. Since $a_i, c_i \in R$, we must have $a \in R$. Thus we proved the claim. □

Proposition 4.4.6. *Let M be a finitely generated module over a Noetherian ring, and $\{M_n\}$ is an I-filtration of M. The following conditions are equivalent:*

1. *$\{M_n\}$ is I-stable;*
2. *Define a graded ring $B_I R$ and a graded $B_I R$-module $B_I M$ by*

$$B_I R = \bigoplus_{n \geq 0} I^n, \quad B_I M = \bigoplus_{n \geq 0} M_n,$$

then $B_I M$ is finitely generated.

Proof. ($\Rightarrow$) Indeed, if the filtration is I-stable, then $B_I M$ is generated by the first $k+1$ terms $M_0, \dots, M_k$ and those terms are finitely generated; thus, $B_I M$ is finitely generated.

($\Leftarrow$) Conversely, if $B_I M$ is finitely generated, say, by $\oplus_0^k M_j$, then, for $n \geq k$, each $f \in M_n$,

$$f = \sum a_{ij} g_{ij}, \quad a_{ij} \in I^{n-j}, \quad \text{with the generators } g_{ij} \in M_j,\ j \leq k.$$

That is, $f \in I^{n-k} M_k$. Thus, $\{M_n\}$ is I-stable. □

Theorem 4.4.7. *(Artin-Rees Lemma) Let I be an ideal in a Noetherian ring R, M a finitely generated R-module, and N a submodule of M. Then there exists an integer $k \geq 1$ so that*

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

Proof. Since R is Noetherian, then $\{M_n\}$ where $M_n = I^n M$ is an I-stable filtration. Thus, by Proposition 4.4.6, $B_I M$ is finitely generated over $B_I R$. Since R is a Noetherian ring, $B_I R$ is also a Noetherian ring, and $B_I M$ is a Noetherian module. Any submodule $B_I N$ is finitely generated over $B_I R$; in particular, $B_I N$ is finitely generated when N is given the induced filtration $\{N_n\}$ where $N_n = M_n \cap N$. Then the induced filtration is I-stable again by the Proposition 4.4.6. Hence, there exists an integer $k \geq 1$ so that

$$M_n \cap N = I^{n-k}(M_k \cap N) \text{ for } n \geq k.$$

□

Theorem 4.4.8. *(Krull's Intersection Theorem) If R is a Noetherian ring, and M is a finitely generated R-module, then for any ideal $I \subsetneq R$, there is an $a \in I$ such that*

$$(1-a)\left(\cap_{n\in\mathbb{N}} I^n M\right) = 0.$$

Proof. Let $E = \cap_{n\in\mathbb{N}} I^n M$. By Artin-Rees Lemma, there exists a k such that

$$E = I^{k+1} M \cap E = I((I^k M) \cap E) = IE.$$

Thus, there exists $a \in I$ such that

$$(1-a)E = (1-a)\left(\cap_{n\in\mathbb{N}} I^n M\right) = 0.$$

□

Corollary 4.4.9. *1. If R is a Noetherian ring, and I is contained in the Jacobson Radical of R, then for any finitely generated R-module M,*

$$\bigcap_{n\in\mathbb{N}} I^n M = 0.$$

2. If $(R, \mathfrak{m})$ is a Noetherian graded local ring, then for any finitely generated R-module M, we have

$$\bigcap_{n\in\mathbb{N}} \mathfrak{m}^n M = 0.$$

Proof. To see the first claim, we note that by Theorem 4.4.8 there exists $a \in I$ such that

$$(1-a)\left(\bigcap_{n\in\mathbb{N}} I^n M\right) = 0.$$

Since I is contained in the Jacobson radical of R, $1-a$ is invertible for any element $a \in I$. Hence, $\bigcap_{n\in\mathbb{N}} I^n M = 0$.

The second claim is an application of the first claim, since R is a local ring and $\mathfrak{m}$ is the only maximal ideal, thus $\bigcap_{n\in\mathbb{N}} \mathfrak{m}^n M = 0$. □

Proposition 4.4.10. *Let R be a Noetherian ring, I an ideal, and M a finitely generated R module. Then $\bigcup_n \mathrm{Ass}(I^n M/I^{n+1}M)$ is a finite set and there exists an integer m such that for all $n \geq m$, $\mathrm{Ass}(I^n M/I^{n+1}M) = \mathrm{Ass}(I^m M/I^{m+1}M)$. Similarly, there exists an integer k such that for all $n \geq k$, $\mathrm{Ass}(M/I^n M) = \mathrm{Ass}(M/I^k M)$.*

Proof. Let S be the Rees algebra $B_I(R)$, and $N = \oplus_n I^n M/I^{n+1}M$ the $\mathbb{N}$-graded S-module, where $N_n = I^n M/I^{n+1}M$. Apply Proposition 4.3.6 to the ring S, we obtain the first claim.

To show the second claim, we consider the short exact sequence:

$$0 \to I^n M/I^{n+1}M \to M/I^{n+1}M \to M/I^n M \to 0.$$

$\mathrm{Ass}(I^n M/I^{n+1}M) \subseteq \mathrm{Ass}(M/I^{n+1}M) \subseteq \mathrm{Ass}(M/I^n M) \cup \mathrm{Ass}(I^n M/I^{n+1}M)$, and by the first claim, there exists an integer m such that for all $n \geq m$, $\mathrm{Ass}(I^n M/I^{n+1}M) = \mathrm{Ass}(I^m M/I^{m+1}M)$. Thus, for all $n \geq m$, we have

$$\mathrm{Ass}(I^n M/I^{n+1}M) \subseteq \mathrm{Ass}(M/I^{n+1}M) \subseteq \mathrm{Ass}(M/I^n M) \cup \mathrm{Ass}(I^n M/I^{n+1}M),$$

and $\cup_n \mathrm{Ass}(M/I^n M)$ is finite. For each $\mathfrak{p} \in \cup_n \mathrm{Ass}(M/I^n M)$, if $\mathfrak{p}$ is associated to only finitely many $M/I^n M$, then let $m_\mathfrak{p}$ be the largest integer such that $\mathfrak{p}$ is associated to $M/I^{k_\mathfrak{p}} M$. Then we choose the maximal of $k = \max\{m, m_\mathfrak{p}\}$, and for all $n \geq k$, we have $\mathrm{Ass}(M/I^n M) = \mathrm{Ass}(M/I^k M)$. □

4.5 System of Parameters

Definition 4.5.1. Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$, and let M be a finitely generated R-module. A **system of parameters** for M is a set $\{a_1, \ldots, a_n\} \subset \mathfrak{m}$ such that $M/(a_1, \ldots, a_n)M$ has finite length.

Definition 4.5.2. Let R be a Noetherian ring, an ideal I is a **complete intersection ideal of height** s if I is generated by a regular sequence $r_1, \ldots, r_s$ of length s; and ideal I is called to be **locally complete intersection ideal of height** s if $I_{\mathfrak{p}}$ is a complete intersection ideal of height s for all prime ideal $\mathfrak{p}$ such that $I \subseteq \mathfrak{p}$. Regular sequences are define in the next section.

If $(R, \mathfrak{m})$ is a Noetherian local ring, let $\mathbb{K} = R/\mathfrak{m}$, then the smallest number of elements needed to generate $\mathfrak{m}$ is equal to the $\dim_{\mathbb{K}} \mathfrak{m}/\mathfrak{m}^2$. In general, if $(R, \mathfrak{m})$ is a Noetherian local ring of $\dim R = n$, then $\dim R \leq \operatorname{rank}_{\mathbb{K}} \mathfrak{m}/\mathfrak{m}^2$, the equality holds when $\mathfrak{m}$ can be generated by n elements. In this case, we call the ring R a *regular local ring.* Below we give a formal definition.

Definition 4.5.3. Let $(R, \mathfrak{m}, \mathbb{K})$ be a Noetherian local ring, and $\mathbb{K} = R/\mathfrak{m}$ be the residue field. If $\dim R = \operatorname{rank}_{\mathbb{K}} \mathfrak{m}/\mathfrak{m}^2 = \dim_{\mathbb{K}} \mathfrak{m}/\mathfrak{m}^2$, then we call R a **regular local ring**. A system of parameters that generate $\mathfrak{m}$ is called a **regular system of parameters**.

Proposition 4.5.4. *Let $(R, \mathfrak{m}, \mathbb{K})$ be a Noetherian local ring. Then R is regular if and only if the* $\dim R = \dim_{\mathbb{K}}(\mathfrak{m}/\mathfrak{m}^2)$

Proof. Let $\dim R = d$. If R is regular, then $a_1, \ldots, a_d \in \mathfrak{m}$ generate $\mathfrak{m}$, and $a_i + \mathfrak{m}^2$ span $\mathfrak{m}/\mathfrak{m}^2$, hence $\dim \mathfrak{m}/\mathfrak{m}^2 \leq d$. But it is always true that $d \leq \dim_{\mathbb{K}}(\mathfrak{m}/\mathfrak{m}^2)$. Thus we have $\dim R = \dim_{\mathbb{K}}(\mathfrak{m}/\mathfrak{m}^2)$.

On the other hand, if $\{a_1 + \mathfrak{m}^2, \ldots, a_d + \mathfrak{m}^2\}$ is a basis for $\mathfrak{m}/\mathfrak{m}^2$, then a_i generate $\mathfrak{m}$, and R is regular. □

Proposition 4.5.5. *Let $(R, \mathfrak{m}, \mathbb{K})$ be a regular local ring of dimension d, let $a_1, \ldots, a_r \in \mathfrak{m}$ where $1 \leq t \leq d$. Then the following are equivalent:*

1. *$a_1, \ldots, a_t$ can be extended to a regular system of parameters in R;*
2. *$\bar{a}_1, \ldots, \bar{a}_t$ are linearly independent over $\mathbb{K}$, where $\bar{a}_i = a_i \ mod\ \mathfrak{m}^2$;*
3. *$R/(a_1, \ldots, a_t)R$ is a regular local ring of dimension $d - t$.*

Proof. $(1 \Leftrightarrow 2)$ This is proved in Proposition 4.5.4. Moreover, $\{a_i\}$ can be extended to a regular system if and only if $\{\bar{a}_i\}$ can be extended to a $\mathbb{K}$-basis of $\mathfrak{m}/\mathfrak{m}^2$.

$(1 \Rightarrow 3)$ Let $a_1, \ldots, a_t, a_{t+1} \ldots, a_d$ be a regular system of parameters for R. Then $\dim(R/(a_1, \ldots, a_t)R) = d - t$, and the $d - t$ elements $\bar{a}_{t+1}, \ldots, \bar{a}_d$ generate $\mathfrak{m}/(a_1, \ldots, a_t)\mathfrak{m}$. Hence $R/(a_1, \ldots, a_t)R$ is regular.

$(3 \Rightarrow 1)$ Let $a_{t+1} \ldots, a_d \in \mathfrak{m}$ such that the images in $\bar{\mathfrak{m}}$ form a regular sequence in $R/(a_1, \ldots, a_t)R$. Let $x \in \mathfrak{m}$, modulo $I = \langle a_1, \ldots, a_t \rangle$, then $x - \sum_{i=t+1}^{d} c_i a_i = 0$ for some $c_i \in R$, and $x - \sum_{i=t+1}^{d} c_i a_i \in I$. Thus, $a_1, \ldots, a_d$ generate $\mathfrak{m}$, R is regular, and $a_1, \ldots, a_t$ extend to a regular system. □

Theorem 4.5.6. *Let $(R, \mathfrak{m}, \mathbb{K})$ be a Noetherian local ring. Then R is regular if and only if $\mathfrak{m}$ can be generated by a regular sequence, the length of any such sequence is* $\dim R$.

Proof. If R is regular with a regular system of parameters $a_1, \ldots, a_d \in R$, and $1 \leq t \leq d$, then $R/(a_1, \ldots, a_t)R$ is regular has dimension $d - t$. By Proposition 4.5.5, $\bar{a}_{t+1}$ is not a zero divisor of $R/(a_1, \ldots, a_t)R$ if and only if a_{t+1} is not a zero divisor of R. By induction, we have $a_1, \ldots, a_d$ form a regular sequence which generate $\mathfrak{m}$.

Suppose $\mathfrak{m}$ is generated by a regular sequence $a_1, \ldots, a_d$, then $\dim R/\mathfrak{m} = \dim R - d$. Since $\dim R/\mathfrak{m} = \dim \mathbb{K} = 0$, we must have that $\dim R = d$. □

Proposition 4.5.7. *If $(R, \mathfrak{m})$ is a Noetherian local ring, and I is a proper ideal in R such that R/I a regular ring, then $I = \sqrt{I}$ and I is locally a complete intersection ideal at all primes $\mathfrak{p}$.*

Proof. We note that R/I is regular if and only if $(R/I)_{\mathfrak{p}}$ is regular for any prime ideal $\mathfrak{p} \supseteq I$, and by Proposition 4.5.5, if and only if the height of $I_{\mathfrak{p}}$ is the same of the number of minimal generators of $I_{\mathfrak{p}}$. Hence I is a local complete intersection by definition.

To show that $I = \sqrt{I}$, we only need to show that $\sqrt{I} \subseteq I$. Let $r \in R/I$ such that $r \in \sqrt{I} \setminus I$. Since $(R/I)_{\mathfrak{p}}$ is a domain for all $\mathfrak{p} \supseteq I$, so $\langle r \rangle_{\mathfrak{p}} = 0$, therefore, $r \in I$. Thus, $I = \sqrt{I}$. □

4.6 Regular and Quasi-regular M-Sequence

Definition 4.6.1. If R is a ring and M an R-module. An element $r \in R$ is said to be **M-regular** if $mr \neq 0$ for all $0 \neq m \in M$. A sequence $r_1, \ldots, r_n \in R$ is an **M-sequence** or **M-regular sequence** if

1. r_1 is M-regular, r_2 is M/r_1M-regular, $\ldots$, r_n is $M/(r_1, \ldots, r_{n-1})M$-regular;
2. $M/(r_1, \ldots, r_n)M \neq 0$

The sequence is said to be a **weak M-sequence** if it only satisfies the first condition.

Remark 4.6.2. By induction on n, one can show that if R is a local ring, and $\{r_1, \ldots, r_n\}$ is a weak M-regular sequence, then for every $i \in \{1, \ldots, n\}$,

$$\dim M/(r_1, \ldots, r_i)M = \dim M - i.$$

Proposition 4.6.3. *Suppose $\mathbf{r} = \{r_1, \ldots, r_n\} \subset I \subset R$ is a weak M-sequence, $f : R \to S$ is a ring homomorphism, and N is a S-module flat over R. Then $f(\mathbf{r})$ is a weak $(M \otimes N)$-sequence in IS. If $\mathbf{r}(M \otimes N) \neq M \otimes N$, then $\mathbf{r}$ is an M-sequence, and $f(\mathbf{r})$ is an $(M \otimes N)$-sequence in IS. If N is faithfully flat over R, then $f(\mathbf{r})$ is an $(M \otimes N)$-sequence if and only if $\mathbf{r}$ is an M-sequence.*

Proof. First, we note that for any ideal $J \subset R$, N/JN is a flat module over R/J, and

$$M/JM \otimes_{R/J} N/JN \cong (M \otimes_R N)/J(M \otimes_R N)$$

preserves the exactness. Let $J = \langle r_1, \ldots, r_i \rangle$ for some $1 \leq i \leq n$. If $\{r_1, \ldots r_i\}$ is a weak M-sequence, then $f(r_1, \ldots r_i)$ is a weak $(M \otimes N)$-sequence in IS.

If $\mathbf{r}(M \otimes N) \neq M \otimes N$, then

$$M/\mathbf{r}M \otimes N/\mathbf{r}N \cong (M \otimes N)/\mathbf{r}(M \otimes N) \neq 0 \;\Rightarrow\; M/\mathbf{r}M \neq 0,$$

thus $\mathbf{r}$ is an M-sequence by definition. Moreover, if $\mathbf{r}$ is an M-sequence, and tensor a flat module preserves the exactness, $f(\mathbf{r})$ is an $(M \otimes N)$-sequence in IS.

To prove the last claim, we only need to show that if $f(\mathbf{r})$ is an $(M \otimes N)$-sequence, then $\mathbf{r}$ is an M-sequence. We will prove such by induction on the length n of the sequence. We will reduce to prove the case when $n = 1$. Since N is faithfully flat,

$$0 \longrightarrow M \otimes N \xrightarrow{r_1 \otimes 1} M \otimes N$$

is exact if and only if

$$0 \longrightarrow M \xrightarrow{r_1} M$$

is exact. Therefore, we have $\mathbf{r}$ is an M-sequence. □

Since localization of R is a flat extension of R, applying the similar argument, we have the following

Remark 4.6.4. If $\mathbf{r} \subset I \subset R$ is a weak M-sequence, and $S \subset R$ is a multiplicatively closed set, then $S^{-1}\mathbf{r} \subset S^{-1}I \subset S^{-1}R$ is a weak $S^{-1}M$-sequence. If $S = R \setminus \mathfrak{p}$ for some prime ideal $\mathfrak{p} \subset R$, and $I \subset \mathfrak{p}$, then $\mathbf{r}_{\mathfrak{p}} \subset I_{\mathfrak{p}}$ is in fact an $M_{\mathfrak{p}}$-sequence in $I_{\mathfrak{p}}$.

Note, the sequence obtained by permuting the elements of an M-sequence may no longer be an M-sequence. In case of a local ring, or more generally, when the sequence lies in the Jacobson radical, the any permutation of an M-sequence results an M-sequence.

Theorem 4.6.5. *If I is in the Jacobson radical of R, and $\mathbf{r} \subset I$ is an M-sequence, then any permutation of $\mathbf{r}$ is also an M-sequence.*

Proof. To prove the claim, we only need to show that if $\{r_1, r_2\}$ is an M-sequence, then $\{r_2, r_1\}$ is also an M-sequence. We will prove that r_2 is not a zero-divisor of M, and r_1 is not a zero-divisor of M/r_2M.

Let $N = (0 :_M r_2)$. To show r_2 is not a zero-divisor of M, we will show $N = 0$. Let $0 \neq m \in N$, then $r_2 m = 0$. The condition that $\{r_1, r_2\}$ is M-regular implies $m \in r_1 M$, and thus, $m = r_1 m'$ for some $0 \neq m' \in M$. Hence, $r_2 m = r_2 r_1 m' = r_1(r_2 m') = 0$. Since r_1 is a non-zero divisor on M, $r_2 m' = 0$, therefore, $m' \in N$. This means for any $m \in N$, $m = r_1 m'$ for some $m' \in N$, i.e., $N \subseteq r_1 N$. Hence, $N = r_1 N$. Since r_1 is in the radical ideal of R, by Nakayama's lemma $N = 0$. Thus, r_2 is a non-zero divisor on M.

Moreover, r_1 is a non-zero divisor on M/r_2M. Otherwise, if there were a non-zero element $m \in M/r_2M$ such that $r_1 m = 0$, then $r_1 m = r_2 m'$ for some $0 \neq m' \in M$. This would imply r_2 is a zero divisor on M/r_1M, contradicting the fact that $\{r_1, r_2\}$ is an M-regular sequence.

Thus, we must have that $\{r_2, r_1\}$ is an M-regular sequence. □

The above theorem is not true if the elements are not coming from the Jacobson radical of R. Without proof, we will state the following known theorem.

Theorem 4.6.6. *If $r_1, \ldots, r_n$ is a regular sequence then so is $r_1^{a_1}, \ldots, r_n^{a_n}$ for any positive integers $a_1, \ldots, a_n$.*

Let $x_1, \ldots, x_n$ be indeterminants over ring R, M an R-module, and $M[x_1, \ldots, x_n] := M \otimes_R R[x_1, \ldots, x_n]$. Then the elements of $M[x_1, \ldots, x_n]$ are polynomials in x_i's with coefficients in M, and $M[x_1, \ldots, x_n]$ can be viewed as either an R-module or an $R[x_1, \ldots, x_n]$-module.

Definition 4.6.7. Let $r_1, \ldots, r_n \in R$, $I = \langle r_1, \ldots, r_n \rangle$ an ideal in R, and M an R-module such that $IM \neq M$. The sequence $r_1, \ldots, r_n$ is **M-quasi-regular** provided that, for all t, $f(x_1, \ldots, x_n) \in M[x_1, \ldots, x_n]$ is homogeneous of degree t and $f(r_1, \ldots, r_n) \in I^{t+1}M$ implies that all the coefficients of f are in IM.

This definition is independent of the order of $r_1, \ldots, r_n$. Moreover, if $r_1, \ldots, r_n$ is M-quasi-regular, then $r_1, \ldots, r_{n-1}$ may not be M-quasi-regular; this is different from an M-regular sequence.

Remark 4.6.8. 1. Define a map $\Phi : M[x_1, \ldots, x_n] \to M$, such that

$$\Phi(f(x_1, \ldots, x_n)) = f(r_1, \ldots, r_n) \quad f \text{ is homogeneous of degree } t.$$

The Definition 4.6.7 is equivalent to the statement that if $f(r_1, \ldots, r_n) = 0$, then the coefficients of f are in IM.

2. Consider a map

$$\phi : (M/IM)[x_1, \ldots, x_n] \to \mathrm{gr}_I M = \oplus_{t \geq 0} I^t M / I^{t+1} M,$$

such that

$$\phi(f(x_1, \ldots, x_n)) = \overline{f(r_1, \ldots, r_n)} \quad f \text{ is homogeneous of degree } t.$$

This is a surjective map, and if ϕ is injective, then $r_1, \ldots, r_n$ is a quasi-regular sequence. Thus Definition 4.6.7 is equivalent to the statement that ϕ is an isomorphism.

Use induction, we can prove the following theorem.

Theorem 4.6.9. *Let R be a ring, M an R-module, and $I = \langle r_1, \ldots, r_n \rangle$ an ideal in R. Then*

1. *If $r_1, \ldots, r_n$ is M-quasi-regular, and $a \in R$ is such that $IM : a = IM$, then $I^t M : a = I^t M$ for any $t > 0$.*

2. *If $r_1, \ldots, r_n$ is M-regular, then it is M-quasi-regular.*

4.7 Proj of a Graded Ring

In the geometry of varieties in affine n-space, the key is in understanding the ideals $I \subset \mathbb{K}[x_1, ..., x_n]$. More generally, modules over $R = \mathbb{K}[x_1, ..., x_n]$ define quasi-coherent shaves on $X = Spec(R)$. In fact, this is an equivalence

of categories: to give a quasi-coherent $\mathcal{O}_X$-module is the same as to give an R-module. Finally, the stalk $\mathcal{O}_{X,x}$ at the point x corresponding to the prime ideal $\mathfrak{p}$ is the local ring $R_{\mathfrak{p}}$.

In projective geometry, a similar role is played by graded rings and modules. Let S be an $\mathbb{N}_0$-graded ring. Define $\operatorname{Proj} S$ to be the set of all homogeneous prime ideals of S not containing S_+. For each positive integer n and each $f \in S_n$, we may view the localization S_f as a graded ring with negative degrees, by placing g/f^k in degree $m - kn$ whenever $g \in S_m$. We may then identify the set

$$D(f) = \{\mathfrak{p} \in \operatorname{Proj} S \mid f \notin \mathfrak{p}\},$$

with $\operatorname{Spec} S_{f,0}$ where $S_{f,0}$ is the degree zero subring of S_f, and glue these to equip $\operatorname{Proj} S$ with the structure of a scheme. In the case $S = \mathbb{K}[x_0, \ldots, x_n]$ with an algebraically closed field $\mathbb{K}$ and where x_i is homogeneous of degree 1, the closed points of this scheme is equal to the usual projective space $\mathbb{P}^n_{\mathbb{K}}$. If I is a graded ideal in S, then S/I can be viewed as a graded ring, and the projection $S \to S/I$ induces a morphism $\operatorname{Proj} S/I \to \operatorname{Proj} S$ which is a closed immersion. The stalk $\mathcal{O}_{X,x}$ at the point x corresponding to the homogeneous prime ideal $\mathfrak{p}$ is the local ring $S_{(\mathfrak{p})}$, where $S_{(\mathfrak{p})}$ denotes the degree 0 homogeneous localization of S at $\mathfrak{p}$, i.e., it consists of fractions x/f of homogeneous elements of the same degree such that $f \notin \mathfrak{p}$.

If M is a graded S-module, we can convert M into a quasi-coherent sheaf $\widetilde{M}$ on $\operatorname{Proj} S$ by doing so on each $D(f)$ and then gluing. Let $0 \leq n \in \mathbb{Z}$, and $M(n)$ the shifted module $M(n)_i = M_{n+i}$. Let $\mathcal{O}_X(n)$ be the quasicoherent sheaf on $X = \operatorname{Proj} S$ defined by the graded module $S(n)$. Then $\mathcal{O}_X(0) = \mathcal{O}_X$. Generally, for any quasicoherent sheaf $\mathcal{F}$ of $\mathcal{O}_X$-modules, set $\mathcal{F}(n) = \mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{O}_X(n)$.

It is proved in [Har97] that suppose that S is generated by S_1 as an S_0-algebra. Then the sheaves $\mathcal{O}_X(n)$ on $\operatorname{Proj} S$ are locally free of rank 1, and $\mathcal{O}_X(m) \otimes_{\mathcal{O}_X} \mathcal{O}_X(n)$ is canonically isomorphic to $\mathcal{O}_X(m+n)$. A locally free quasicoherent sheaf $\mathcal{F}$ of rank one on a locally ringed space X is called an *invertible sheaf* . That is because there is a unique sheaf $\mathcal{F}^\vee$ such that $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{F}^\vee \cong \mathcal{O}_X$ is called the *dual of* $\mathcal{F}$. The dual of $\mathcal{O}_X(n)$ is $\mathcal{O}_X(-n)$.

As a known result proved in [Har97], if S is finitely generated by S_1 as an S_0-algebra, then each quasi-coherent sheaf on $\operatorname{Proj} S$ can be written as $\widetilde{M}$ for a canonical choice of M. This means that from a quasicoherent sheaf $\mathcal{F}$ on M, one can construct a module

$$\Gamma_*(\mathcal{F}) = \oplus_{n \in Z} \Gamma(X, \mathcal{F}(n)).$$

If $1 \leq n \in \mathbb{Z}$ and $S = \mathbb{K}[x_0, \ldots, x_n]$, then $S = \oplus_{n=0}^{\infty} \Gamma(X, \mathcal{O}_X(n))$. Moreover, if $\mathcal{I}$ is an ideal sheaf, then we can construct $\Gamma_*(\mathcal{I})$ as and ideal of $\Gamma_*(\mathcal{O}_X) =$

S. Hence, we see that any closed immersion into $\mathbb{P}^n_{\mathbb{K}}$ is defined by some homogeneous ideal of $\mathbb{K}[x_0, \ldots, x_n]$.

The algebra associated to projective geometry is the algebra of graded rings and modules. However, it is not true that we have an equivalence of categories like we did in the affine case. It can happen that $\operatorname{Proj} S$ can be isomorphic to $\operatorname{Proj} T$ even though S and T are not isomorphic as graded rings. Also two different graded S-modules M and N can define isomorphic quasi-coherent sheaves $\tilde{M}$, $\tilde{N}$. Example: any module M with $M_n = 0$ for $n \gg 0$ has $\tilde{M} = 0$. Another important difference between affine and projective geometry is in sheaf cohomology. If X is an affine scheme then $H^i(X, \mathcal{F}) = 0$ for all $i \geq 0$ for all quasi-coherent sheaves $\mathcal{F}$, a theorem of Serre. But for projective schemes X, the $H^i(X, \mathcal{F})$ are generally nonzero and give interesting invariants of X.

4.8 Graded Free Resolution

In abstract algebra and homological algebra, a resolution is an exact sequence of modules (or any objects in an abelian category), which is used to describe the structure of a specific module (or object) of this category. If M is a graded R-module generated by its elements of positive degree, then M has a free resolution. Among these graded free resolutions, the minimal free resolutions are those for which the number of basis elements of each stage is minimal.

First, let us prove Nakayama's Lemma for the graded modules.

Proposition 4.8.1. *(Graded Nakayama's Lemma) Let $R = R_0[R_1]$ be a non-negatively graded Noetherian ring with R_0 a local ring, $\mathfrak{m}$ the homogeneous maximal ideal of R, and M a finitely generated graded R-module. If $r = \dim_{R/\mathfrak{m}}(M/\mathfrak{m}M)$, then there exists r homogeneous elements which generate M.*

Proof. Let $m_1, \ldots, m_r \in M$ be homogeneous elements whose images form an $R/\mathfrak{m}$-basis in $M/\mathfrak{m}M$. We will show that $m_1, \ldots, m_r$ generate M. Let $N \subset M$ be the submodule generated by $x_1, \ldots, x_r$, then $M = N + \mathfrak{m}M$, and $M/N = \mathfrak{m}(M/N)$. If $M \neq N$, then M/N is a finitely generated non-zero graded R-module. Let s be the smallest integer such that $(M/N)_s \neq 0$. Then $(M/N)_s = \mathfrak{m}'(M/N)_s$ where $\mathfrak{m}'$ is the maximal ideal in R_0. By local version of Nakayama's lemma, $(M/N)_s = 0$, a contradiction. Hence $M = N$. □

With the above notation, let $r = \dim_{R/\mathfrak{m}}(M/\mathfrak{m}M)$ be the minimal number of generators of M. If F is a finitely generated graded free R-module,

then homogeneous elements $m_1, \ldots, m_r$ with $\deg(m_i) = n_i$ form a basis for F. Therefore, there exists a unique set of integers $\{n_1, \ldots, n_r\}$ such that $F \cong \bigoplus_{i=1}^{r} R(-n_i)$.

Definition 4.8.2. Let R be a graded ring and M a graded R-module. A **graded resolution** of M is a complex of free R-modules of the form

$$\cdots \to F_\ell \xrightarrow{\phi_\ell} F_{\ell-1} \to \cdots \to F_1 \xrightarrow{\phi_1} F_0 \xrightarrow{\phi_0} M \to 0,$$

where each $F_\ell = R(-d_1) \oplus \cdots \oplus R(-d_p)$ is a free module, and $(R(d))_t = R_{d+t}$ is **the degree d twisted component of R.** $\ker(\phi_\ell) = \operatorname{im}(\phi_{\ell-1}) \subseteq F_\ell$ is the **ℓ-th syzygy module of M**; and each ϕ_ℓ is a graded homomorphism of degree 0. The resolution is **minimal** if for every $\ell \geq 1$, the nonzero entries of the graded matrix of ϕ_l have positive degree. It is proved that a free resolution is minimal if and only if $\phi_\ell(F_\ell) \subset \mathfrak{m}F_{\ell-1} = \langle x_1, \ldots, x_n \rangle F_{\ell-1}$, $\forall \ell$.

Remark 4.8.3.

1. Every (graded) module has a (graded) free resolution.
2. Every finitely generated module over a principal ideal domain R has a resolution of the form

$$0 \to F_1 \to F_0 \to M \to 0, \quad \text{where } F_i\text{'s are free over } R.$$

$M \cong R^n \oplus R/a_1R \oplus \cdots \oplus R/a_mR$ where a_i's are non-zero units, $F_0 = R^{m+n}$ and $F_1 = R^n$.

Theorem 4.8.4. *(Minimal Resolutions Over Noetherian Local Rings) Let $(R, \mathfrak{m})$ be a Noetherian local ring, and M a finitely generated R-module of projective dimension n. Then, a projective resolution of minimal length may be obtained by constructing a free resolution and taking the minimal possible number of generators of the free modules at each step.*

Proof. Let $b_0 = \mu(M)$ be the number of generators of M, then we have a part of free resolution of M over R as

$$R^{b_0} \xrightarrow{f_0} M \longrightarrow 0.$$

If $b_0 \neq 0$, then take b_1 as the number of the generators of $\ker(f_0)$ to construct the free resolution

$$R^{b_1} \xrightarrow{f_1} R^{b_0} \xrightarrow{f_0} M \longrightarrow 0.$$

We continue this process one at a time, i.e., if $b_i \neq 0$, then take b_{i+1} as the number of the generators of $\ker(f_i)$ to construct the free resolution

$$R^{b_{i+1}} \xrightarrow{f_{i+1}} R^{b_i} \xrightarrow{f_i} R^{b_{i-1}} \to \cdots \to R^{b_0} \xrightarrow{f_0} M \longrightarrow 0.$$

The projective dimension is n implies $b_n \neq 0$, but $b_{n+1} = 0$, and the process terminates. □

We observe that the key idea of constructing a free resolution of a R-module M is to find a system of generators of M first, and then find a generating system of the relations on the generators of M, i.e., the first syzygy module of M, and repeat the process. In fact, building a resolution is to repeatedly solve a system of polynomial equations, i.e., the syzygy modules. Below is an algorithm to construct a free resolution of a finitely generated R-module M.

Algorithm 4.8.5. (Construct a free resolution)

1. Let $M_0 = M$, choose generators $m_1, \ldots, m_r \in M_0$, and set $F_0 = R^r$, let $f_1, \ldots, f_r$ be a basis for F_0, and define

$$d_0 : \quad F_0 \to M, \quad d_0(f_i) = m_i, \quad 1 \leq i \leq r.$$

2. For $i \geq 1$, let $M_i = \ker(d_{i-1})$, choose generators $w_1, \ldots, w_s \in M_i$, and set $F_i = R^s$. Let $g_1, \ldots, g_s$ be a basis in R^s, and define

$$d_i : \quad F_i \to M_i \subset F_{i-1}, \quad d_i(g_j) = w_j, \quad 1 \leq j \leq s.$$

   By construction,

$$\ker(d_{i-1}) = \mathrm{im}(d_i).$$

3. Repeat this process.

This process may or may not terminate; if it terminates, we have a finite free resolution of M, otherwise, we have an infinite free resolution of M.

Remark 4.8.6. A graded resolution can be constructed in the similar way by choosing a set of homogeneous generators of $\ker(d_i)$. Furthermore, a minimal free resolution can be obtained by selecting a minimal system of the generators.

To see this, let

$$\cdots \to F_i \xrightarrow{f_i} F_{i-1} \to \cdots \to M \to 0$$

be the graded free resolution of M, and consider the section of the right exact sequence $F_i \to F_{i-1} \to \mathrm{im} f_{i-1} \to 0$. The complex is minimal if and only if $f_i(F_i) \subset \mathfrak{m}F_{i-1}$. This is equivalent to say that the map

$$\overline{f_i} : \quad F_i/\mathfrak{m}F_i \to F_{i-1}/\mathfrak{m}F_{i-1}$$

is zero. This holds if and only if $F_{i-1}/\mathfrak{m}F_{i-1} \cong (\mathrm{im} f_{i-1})/\mathfrak{m}(\mathrm{im} f_{i-1})$, and by Nakayama's lemma, this is true if and only if F_{i-1} maps to a minimal set of generators of $\mathrm{im} f_{i-1}$.

Theorem 4.8.7. *(Graded Hilbert Syzygy Theorem) Every finitely generated $R = \mathbb{K}[x_1, \ldots, x_n]$-module has a finite graded resolution of length at most n. Any two minimal resolutions are isomorphic.*

Proof. To prove that the resolution terminates at the $(n+1)$-th step, it is necessary and sufficient to show that the n-th syzygy is a free module. We will leave the proof of the first claim to the reader as an exercise. To prove the second statement, let $F_\bullet$ and $G_\bullet$

$$F_\bullet : \quad \cdots \to F_i \xrightarrow{f_i} F_{i-1} \to \cdots \to F_0 \to M \to 0$$

$$G_\bullet : \quad \cdots \to G_j \xrightarrow{g_j} G_{j-1} \to \cdots \to G_0 \to M \to 0$$

be two minimal free resolutions of M. Let m be the length the minimal resolutions. We insert the kernel and the cokernel to the maps $F_i \to F_{i-1}$ and $G_i \to G_{i-1}$. Since $\dim F_0 = \dim G_0$ equals the number of generators of M, $F_0 \cong G_0$, and $\ker(f_0) \cong \ker(g_0)$. According to the construction of the minimal free resolution, $\dim F_1 = \dim G_1$ equals the number of generators in $\ker(f_0) = \ker(g_0)$, hence $F_1 \cong G_1$. Repeat this process, at each stage, $\ker(f_i) \cong \ker(g_i)$, and hence $F_{i+1} \cong G_{i+1}$. Thus, any two minimal resolutions are isomorphic. □

When the polynomial ring has two variables, then the structure of this minimal free resolution has a special form given by the Hilbert-Burch theorem. A modern presentation can be found in the book [Page 263, [CLO98]].

Theorem 4.8.8. *Suppose that $f_1, \ldots, f_m \in \mathbb{K}[x, y]$ are homogeneous polynomials. Then $\mathrm{Syz}(f_1, \ldots, f_m)$ is a twisted free module over $\mathbb{K}[x, y]$. Moreover, if $\deg(f_i) = d$ for all i and $\gcd(f_i) = 1$, then $\mathrm{Syz}(f_1, \ldots, f_s) \cong \oplus_{i=1}^{m-1} R(-\mu_i)$, that is, the generators of the syzygy module are of degrees $\mu_1, \ldots, \mu_{m-1}$ such that $\mu_1 \leq \mu_2 \leq \cdots \leq \mu_{m-1}$ and $\sum_{i=1}^{m-1} \mu_i = d$.*

Cox [Page 279, [CLO98]] sketched the proof of the second statement, and had a nice short literature review of the development on this subject. The set of the generators in Theorem 4.8.8 is called the *μ-basis* of the syzygy module. The basis elements are not unique, but the degrees of the elements are unique.

Remark 4.8.9. Let $\mathbf{F} : \mathbb{P}^1 \to \mathbb{P}^n$ be a generic one-to-one map given by $\mathbf{F}(s,t) = (f_0(s,t), \ldots, f_n(s,t))$ with $\deg(f_i) = d$ and $\gcd(f_i) = 1$. Then the image of the parametrization is a space curve of degree d in $\mathbb{P}^n$.

1. If $n = 2$, then $\mathrm{Syz}(f_0, f_1, f_2)$ is generated by two elements $\mathbf{p}, \mathbf{q}$ of degrees $\mu_1, d-\mu_1$ where $\mu_1 \leq d-\mu_1$. The set $\{\mathbf{p}, \mathbf{q}\}$ is called a μ-basis for the rational planar curve.

2. If $n = 3$, then $\mathrm{Syz}(f_0, f_1, f_2, f_3)$ is generated by three elements $\mathbf{p}, \mathbf{q}, \mathbf{r}$ of degrees $\mu_1 \leq \mu_2 \leq \mu_3$ such that $\sum_{i=1}^{3} \mu_i = d$. The set $\{\mathbf{p}, \mathbf{q}, \mathbf{r}\}$ is called a μ-basis for the rational space curve.

Example 4.8.10. If $R = \mathbb{C}[x,y]$ is a graded ring and $I = \langle x, y \rangle$ is the graded ideal. The minimal graded free resolution of I is

$$0 \to R(-2) \xrightarrow{[y,-x]^T} R(-1) \oplus R(-1) \xrightarrow{[x,y]} I \to 0.$$

There are several useful numerical invariants that can be obtained from the minimal free resolution of a module. The first invariant is called projective dimension, that is the length of the minimal free resolution.

Definition 4.8.11. Let M be a graded R-module with the following free resolution

$$\cdots \to F_\ell \xrightarrow{\phi_\ell} F_{\ell-1} \to \cdots \to F_1 \xrightarrow{\phi_1} F_0 \xrightarrow{\phi_0} M \to 0.$$

The **projective dimension of** M, $\mathrm{pdim}(M)$, is the smallest i such that $F_i \neq 0$ and $F_j = 0$ for all $j > i$. If no such i, then $\mathrm{pdim}(M) = \infty$.

Example 4.8.12. If $R = \mathbb{K}[x,y]/(xy)$ where $\mathbb{K}$ is a field, then $R/(x)$ does not have finite projective dimension over R, since

$$\cdots \xrightarrow{x} R \xrightarrow{y} R \xrightarrow{x} R \xrightarrow{y} R \xrightarrow{x} R \longrightarrow R/(x) \to 0.$$

Remark 4.8.13. Let I be a graded ideal in the graded ring R, then

$$\mathrm{pdim}(R/I) = \mathrm{pdim}(I) + 1.$$

Example 4.8.14. Let $R = \mathbb{K}[x,y]$ and $I = \langle x^2, xy, y^3 \rangle$, then the minimal free resolution of $M = R/I$ is

$$0 \to R(-3) \oplus R(-4) \xrightarrow{\begin{bmatrix} -y & 0 \\ x & -y^2 \\ 0 & x \end{bmatrix}} R^2(-2) \oplus R(-3) \xrightarrow{[x^2, xy, y^3]} R \to M \to 0.$$

It is easy to see that $\mathrm{pdim}(R/I) = 2$.

Betti numbers of M is are other invariants which can be obtained from the minimal free resolution.

Definition 4.8.15. The rank of the i-th syzygy module of the minimal graded free resolution of M over R

$$F_\bullet \quad \cdots \to F_\ell \xrightarrow{\phi_\ell} F_{\ell-1} \to \cdots \to F_1 \xrightarrow{\phi_1} F_0 \xrightarrow{\phi_0} M \to 0 \tag{4.1}$$

is called the **i-th total Betti number** or simply the **i-th Betti number**, and is denoted by

$$\beta_i^R(M) = \operatorname{rank}(F_i).$$

Let $F_i = \bigoplus R(-j)$, then a graded minimal free resolution of M is of the form

$$0 \to \bigoplus_j R(-j)^{\beta_{p,j}} \to \cdots \to \bigoplus_j R(_j)^{\beta_{1,j}} \to \bigoplus_j R(-j)^{\beta_{0,j}} \to M \to 0,$$

where the exponents $\beta_{i,j}$ of the shifted modules $R(-j)$ are called the *graded Betti numbers of M over R*. In fact, $\beta_{ij}^R(M)$ of M is the number of copies of $R(-j)$ that appears in F_i. It is known (and we will see in the next chapter) that

$$\beta_i^R(M) = \dim_{\mathbb{K}} \operatorname{Tor}_i^R(M, \mathbb{K}), \quad \beta_{ij}^R(M) = \dim_{\mathbb{K}} \operatorname{Tor}_i^R(M, \mathbb{K})_j.$$

Since $\beta_{i,j}(M) = 0$ for $j < i$, the graded Betti numbers of an R-module M are often written in a matrix called *the Betti table of M*, where the entry in the i-th column and the j-th row in the matrix is the Betti number $\beta_{i,i+j}(M)$. The Betti table of M is denoted $\beta(M)$ and has the form:

$$\beta(M) = \begin{matrix} \beta_{0,0} & \beta_{1,1} & \cdots & \beta_{p,p} \\ \beta_{0,1} & \beta_{1,2} & \cdots & \beta_{p,p+1} \\ \vdots & \vdots & \cdots & \vdots \\ \beta_{0,r} & \beta_{1,1+r} & \cdots & \beta_{p,p+r}. \end{matrix}$$

Using the Betti numbers, we can identify two important invariants that measure the "growth" of the resolution of M as an R-module. First, the projective dimension of M can be defined in terms of Betti number:

$$\operatorname{pdim}_R(M) = \sup\{i \mid F_i \neq 0\} = \sup\{i \mid \beta_i^R \neq 0\}.$$

Second, the *Castelnuovo-Mumford regularity* or simply the *regularity* of a module can be extracted from the Betti numbers.

Definition 4.8.16. Let $t_i^R(M) = \sup\{j \mid \beta_{i,j}^R(M) \neq 0\}$, the **Castelnuovo-Mumford regularity**, or the **regularity** of M, $\operatorname{reg}_R(M)$, is defined as

$$\operatorname{reg}_R(M) = \sup\{j - i \mid \beta_{i,j}^R(M) \neq 0\} = \sup\{t_i^R(M) - i \mid i \in \mathbb{N}\}.$$

We observe that if M has a minimal free resolution $F_\bullet$ as in (4.1) where $F_i = \oplus_j R(-a_{ij})$, then $\operatorname{reg}_R(M) = \sup_{i,j}\{a_{ij} - i\}$. Moreover, an R-module M has a *linear resolution* if $\beta_{i,j}^R(M) = 0$ if $j \neq d + i$ for some $d \in \mathbb{Z}$. Equivalently, M has a linear resolution as an R-module if it is generated by elements of degree $\operatorname{reg}_R(M)$.

Example 4.8.17. The Betti numbers, Betti table, and regularity of the module M in Example 4.8.14 are

$$\beta_0(M) = 1,\ \beta_1(M) = 3,\ \beta_2(M) = 2,$$

$$\beta_{0,0}(M) = 1,\ \beta_{1,2}(M) = 2,\ \beta_{1,3}(M) = 1,\ \beta_{2,3}(M) = 1,\ \beta_{2,4}(M) = 1.$$

$$\beta(M) = \begin{array}{ccc} 1 & - & - \\ - & 2 & 1 \\ - & 1 & 1. \end{array}$$

$$\operatorname{reg}_R(M) = 2.$$

In general, $\operatorname{reg}_R(M)$ is finite if $\operatorname{pdim}_R(M)$ is finite. But $\operatorname{reg}_R(M)$ can be finite even if $\operatorname{pdim}_R(M)$ is infinite. Following is an example.

Example 4.8.18. Let $R = \mathbb{K}[x]/(x^n)$ with $n > 1$. Then the minimal free resolution of $M = \mathbb{K}$ over R is:

$$\cdots \to R(-2n) \xrightarrow{x^{n-1}} R(-n-1) \xrightarrow{x} R(-n) \xrightarrow{x^{n-1}} R(-1) \xrightarrow{x} R \to M \to 0.$$

Hence $F_{2i} = R(-in)$ and $F_{2i+1} = R(-in-1)$. So $\operatorname{pdim}_R(M) = \infty$ for all $n > 1$. But $\operatorname{reg}_R(M) = 0$ if $n = 2$, and $\operatorname{reg}_R(M) = \infty$ if $n > 2$.

4.9 Dimension and Multiplicity

Lemma 4.9.1. *Let R be a graded ring, and $\mathfrak{p}$ a non-homogeneous prime ideal of R. Then there are no prime ideals properly between $\mathfrak{p}$ and $\mathfrak{p}'$ where $\mathfrak{p}'$ is the ideal generated by all the homogeneous elements contained in $\mathfrak{p}$. Hence,* $\operatorname{ht}(\mathfrak{p}) = \operatorname{ht}(\mathfrak{p}') + 1$.

Proof. By passing to $R/\mathfrak{p}'$, assume R is an integral domain and $\mathfrak{p}' = 0$. Let S be a set of all non-zero homogeneous elements in R, then $\mathfrak{p} \cap S = \emptyset$, and $\mathfrak{p}R_S$ is a non-zero prime ideal in R_S. Since every non-zero homogeneous element of R_S is a unit, $R_S = \mathbb{K}[t^{-1}, t]$, and $\dim R_S = \dim \mathbb{K}[t^{-1}, t] = 1$. Hence, there are no primes properly between $\langle 0 \rangle \subset \mathfrak{p} \subset \mathfrak{p}R_S$. Therefore, there are no primes of R properly between $\langle 0 \rangle \subset \mathfrak{p}$. Thus, $\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\mathfrak{p}') + 1$. □

Corollary 4.9.2. *Let R be a graded ring, and M a finitely generated graded R-module. If $\mathfrak{p} \in \mathrm{Supp}M$ is a non-homogeneous prime ideal, then $\dim M_{\mathfrak{p}} = \dim M_{\mathfrak{p}'} + 1$ where $\mathfrak{p}'$ is the ideal generated by all the homogeneous elements contained in $\mathfrak{p}$.*

Proof. By passing to $R/\mathrm{Ann}_R M$, assume $\mathrm{Ann}_R M = 0$. Then $\dim M_{\mathfrak{p}} = \dim R_{\mathfrak{p}} = \mathrm{ht}(\mathfrak{p})$ for all $\mathfrak{p} \in \mathrm{Supp}M$. By Lemma 4.9.1, $\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\mathfrak{p}') + 1$, thus

$$\dim M_{\mathfrak{p}} = \dim R_{\mathfrak{p}} = \mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\mathfrak{p}') + 1 = \dim R_{\mathfrak{p}'} + 1 = \dim M_{\mathfrak{p}'} + 1.$$

□

Using the technique of passing to $R/\mathfrak{p}'$, one can prove the following results.

Proposition 4.9.3. *Let R be a Noetherian graded ring and $\mathfrak{p}$ a homogeneous prime ideal of height n, then there exists a chain of distinct homogeneous prime ideals*

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n = \mathfrak{p}.$$

Hence, for a non-negatively graded Noetherian ring R,

$$\dim R = \sup_n \{\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n \mid \ \mathfrak{p}_i \text{ are homogeneous primes of } R\}.$$

Lemma 4.9.4. *Let R be a graded ring and M a graded R-module. Then M is simple as an R-module if and only if M is simple as an R_0-module.*

Proof. First, if M is a simple R_0-module, then M must be a simple R-module, hence we only need to show the converse. If M is a simple R-module, then $M \cong R/\mathfrak{m}$ for some homogeneous maximal ideal $\mathfrak{m}$, and $\mathfrak{m} \cong \oplus_{i=-\infty}^{1} R_i + \mathfrak{m}' + \oplus_{i=1}^{\infty} R_i$ for some maximal ideal $\mathfrak{m}' \in R_0$. Thus $M \cong R/\mathfrak{m} \cong R_0/\mathfrak{m}'$, and therefore, M is simple as an R_0-module. □

If M is an R-module, we denote the length of M as and R-module by $\ell_R(M)$, or simply $\ell(M)$.

Theorem 4.9.5. *Let R be a Noetherian graded ring and M a non-zero finitely generated graded R-module. Then there exists a filtration, called quasi-composition series for M,*

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_r = M$$

such that for $i = 1, \ldots, r$, $M_i/M_{i-1} \cong (R/\mathfrak{p}_i)(m_i)$ for some homogeneous prime $\mathfrak{p}_i$, and degree twist $m_i \in \mathbb{Z}$. The set $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ is not uniquely determined by M, but the set of minimal primes in S is the same as the set of minimal associated primes of M over R. Therefore, if $\mathfrak{p}$ is a minimal associated prime of M over R, then the number of times $\mathfrak{p}$ occurs in any quasi-composition series for M is the same as $\ell_{R_\mathfrak{p}}(M_\mathfrak{p})$, the length of $M_\mathfrak{p}$.

Proof. To show the existence of quasi-composition series of M, let

$$\Gamma = \{\text{graded submodule of } M \mid \text{ is zero or has a quasi-composition}\}.$$

Let N be the maximal element of Γ. If $M \neq N$, let $N' = M/N$, then there exists a graded submodule $L \subsetneq N'$ such that $L \cong (R/\mathfrak{q})(m)$ for some $\mathfrak{q} \in \operatorname{Ass}_R N'$, and some degree twist $m \in \mathbb{Z}$. Let M' be the inverse image of L in M, then $M' \supsetneq N$ and $M' \in \Gamma$, contradicting the assumption that N is the maximal element in Γ. Thus, $M = N$.

It is easily verified that for a sufficiently large k,

$$\left[\bigcap_{i=1}^{r} \operatorname{Ann}_R(M_i/M_{i-1})\right]^k \subset \operatorname{Ann}_R(M) \subset \bigcap_{i=1}^{r} \operatorname{Ann}_R(M_i/M_{i-1}) = \bigcap_{i=1}^{r} \mathfrak{p}_i$$

Thus, a prime $\mathfrak{p} \supseteq \operatorname{Ann}_R(M)$ if and only if $\mathfrak{p} \supseteq \operatorname{Ann}_R(M_i/M_{i-1})$ for some i, if and only if $\mathfrak{p}_i \subseteq \mathfrak{p}$ for some i. If $\mathfrak{p}$ is a minimal associated prime of M, then we have $\mathfrak{p}_i = \mathfrak{p}$ for some i.

If $\mathfrak{p}$ is a minimal associated prime of M over R, then localization at $\mathfrak{p}$ gives a composition series for $R_\mathfrak{p}$-module $M_\mathfrak{p}$, and $\ell_{R_\mathfrak{p}}(M_\mathfrak{p})$ is the number of nonzero components in the quasi-composition series of $M_\mathfrak{p}$, which is the number of times that $(R/\mathfrak{p})(m)$ occurs as a component in the quasi-composition series of M. □

Lemma 4.9.6. *Let R be a graded ring and M a graded R-module such that $\ell_R(M) = n$. Then there exists a composition series of M*

$$0 = M_n \subsetneq M_{n-1} \subsetneq \cdots \subsetneq M_0 = M,$$

where M_i/M_{i+1} is a simple R-module and M_i is graded for all i.

Proof. If $n = 0, 1$, then the result is trivial, and let $n > 1$. We will prove the claim by induction on n. Let $0 \neq m \in M$ be a homogeneous element. If $Rm \neq M$, then we are done by induction: pull back a quasi-composition series of M/Rm. If $Rm = M$, then $M \cong R/\mathrm{Ann}(m)$, and $\ell(R/\mathrm{Ann}(m)) = n$. $R/\mathrm{Ann}(m)$ is an Artinian graded ring. If every nonzero homogeneous element were invertible, then the maximal homogeneous ideal is the zero ideal. In other words we would have $n = \ell_R(R/\mathrm{Ann}(m)) = 1$, contradicting the assumption $n > 1$. Thus, there exists a non-zero homogeneous element $r \in R \setminus \mathrm{Ann}(m)$ such that $r + \mathrm{Ann}(m)$ is not a unit in $R/\mathrm{Ann}(m)$. Then $N = R(rx)$ is a non-zero proper graded submodule of M. Hence, we are done by induction. □

Theorem 4.9.7. *Let R be a graded ring and M a graded R-module. Then*

$$\ell_R(M) = \ell_{R_0}(M) = \sum_n \ell_{R_0}(M_n).$$

Proof. If $\ell_R(M) = \infty$, then $\ell_{R_0}(M) = \infty$. Assume that $\ell_R(M) = n < \infty$. By Lemma 4.9.6, there exists a composition series of M

$$0 = M_n \subsetneq M_{n-1} \subsetneq \cdots \subsetneq M_0 = M,$$

where M_i/M_{i+1} is a simple R-module and M_i is graded for all i. By Lemma 4.9.4, these are also simple R_0-modules. Hence, $\ell_{R_0}(M) = n$. □

It follows that if R is a graded ring and M a graded R-module, then $\ell_R(M) < \infty$ as an R-module if and only if each M_n has finite length as an R_0-module, and $M_n = 0$ for $n \gg 0$.

Definition 4.9.8. A graded R-module is called **bounded below** if there exists $k \in \mathbb{Z}$ such that $M_n = 0$ for all $n \leq k$.

Definition 4.9.9. Let R be a graded ring and M a graded R-module. Suppose that $\ell_{R_0}(M_n) < \infty$ for all n, we define that **Hilbert function** $H_M : \mathbb{Z} \to \mathbb{Z}$ of M by

$$H_M(n) = \ell_{R_0}(M_n), \ \forall\, n \in \mathbb{Z}.$$

If M is bounded below, we define the **Hilbert series** or **Poincaré series** of M to be

$$P_M(t) = \sum_{n \in \mathbb{Z}} H_M(n) t^n \in \mathbb{Z}(t).$$

Theorem 4.9.10. *Let $R = \oplus_{i=0}^{\infty} R_i$ be a Noetherian graded ring, where R_0 is a Noetherian ring, and R is generated by homogeneous elements $r_1, \ldots, r_s$ with $\deg(r_i) = k_i > 0$. Let M be a finitely generated graded R-module. The $P_M(t)$ is a rational function in t of the form*

$$P_M(t) = \frac{f(t)}{\prod_{i=1}^{s}(1 - t^{k_i})}, \quad \text{where } f(t) \in \mathbb{Z}[t].$$

Proof. We will prove the claim by induction on s, the number of generators of R over R_0. If $s = 0$, then $R_i = 0$ for all $i \geq 1$, so $R = R_0$, and M is a finitely generated R_0 module, hence $M_i = 0$ for all $i \gg 0$. Thus $P_M(t)$ is a polynomial.

Assume that the claim is true for all $s - 1$, and we will show it is true for s. Consider the following exact sequence:

$$0 \to K_n \to M_n \xrightarrow{r_s} M_{n+k_s} \to L_{n+k_s} \to 0,$$

and let $K = \oplus_n K_n$ and $L = \oplus_n L_n$. Then K and L are finitely generated graded R-module, L is the quotient module of M, both are annihilated by r_s, and they are $R_0[r_1, \ldots, r_{s-1}]$-modules.

$$\ell(K_n) - \ell(M_n) + \ell(M_{n+k_s}) - \ell(L_{n+k_s}) = 0.$$

Multiplying t^{n+k_s}, we have

$$t^{n+k_s}\ell(K_n) - t^{n+k_s}\ell(M_n) + t^{n+k_s}\ell(M_{n+k_s}) - t^{n+k_s}\ell(L_{n+k_s}) = 0,$$

hence,

$$(1 - t^{k_s})P_M(t) = P_L(t) - t^{k_s}P_K(t).$$

Apply induction hypothesis on K and L,

$$(1 - t^{k_s})P_M(t) = \frac{g(t)}{\prod_{i=1}^{s-1}(1 - t^{k_i})} - \frac{t^{k_s}h(t)}{\prod_{i=1}^{s-1}(1 - t^{k_i})}, \text{ where } g(t), h(t) \in \mathbb{Z}[t],$$

thus the claim is true. □

Proposition 4.9.11. *Let $R = \mathbb{K}[x_1, \ldots, x_m]$ be a polynomial ring over a field $\mathbb{K}$ with $\deg(x_i) = 1$ for all i. Then the Hilbert function*

$$H_R(d) = \binom{m + d - 1}{m - 1} = \binom{m + d - 1}{d}, \ \forall d \geq 0.$$

And the Hilbert or Poincaré series of R can be written as

$$P_R(t) = \frac{1}{(1 - t)^m}.$$

Proof. We will prove the first claim by induction on $m + d$. If $m = 1$ or $d = 0$, the claim is clearly true. Suppose that $m > 1$ and $d > 0$. Let $S = \mathbb{K}[x_1, \ldots, x_{m-1}]$, and consider the exact sequence

$$0 \to R_{d-1} \xrightarrow{x_m} R_d \to S_d \to 0.$$

Then apply induction hypothesis on R_{d-1} and S_d,

$$\begin{aligned} H_R(d) &= \dim_{\mathbb{K}} R_d = \dim_{\mathbb{K}} R_{d-1} + \dim_{\mathbb{K}} S_d \\ &= \binom{m + (d-1) - 1}{m-1} + \binom{(m-1) + d - 1}{(m-1) - 1} \\ &= \binom{m+d-2}{m-1} + \binom{m+d-2}{m-2} = \binom{m+d-1}{m-1} = \binom{m+d-1}{d}. \end{aligned}$$

By series expansion,

$$\frac{1}{(1-t)^m} = \sum_d \binom{m+d-1}{d} t^d = \sum_d H_R(d) t^d = P_R(t).$$

□

Corollary 4.9.12. *Let $R = \mathbb{K}[x_1, \ldots, x_m]$ be a graded ring, and M a graded R-module with the following free resolution:*

$$F^\bullet : \quad 0 \to F_s \to F_{s-1} \to \cdots \to F_1 \to F_0 \to M \to 0, \quad F_i = \oplus_j R(-a_{ij}).$$

Then

$$H_M(d) = \sum_{i=0}^{s} (-1)^i \sum_j \binom{m-1+d-a_{ij}}{m-1}.$$

Moreover, there is a polynomial called the **Hilbert polynomial**, *denoted by $HP_M(d)$, such that $HP_M(d) = H_M(d)$ for $d \geq \max_{i,j}\{a_{i,j} - m + 1\}$, and* $\deg(HP_M(d)) = m - 1$.

Proof. By Proposition 4.9.11,

$$H_M(d) = \sum_{i=0}^{s} (-1)^i H_{F_i}(d) = \sum_{i=0}^{s} (-1)^i \sum_j \binom{m-1+d-a_{ij}}{m-1}.$$

If $d \geq \max_{i,j}\{a_{i,j} - m + 1\}$, then $m - 1 + d - a_{ij} \geq 0$, and

$$\begin{aligned} &\binom{m-1+d-a_{ij}}{m-1} \\ = \ &\frac{(m-1+d-a_{ij})(m-1+d-a_{ij}-1)\cdots(d-a_{ij}+1)}{(m-1)!} \end{aligned}$$

is a polynomial of degree $m-1$ in d. Thus, for $d \gg 0$, the Hilbert function is in fact a polynomial, and

$$HP_M(d) = \alpha \cdot d^{m-1} + \text{terms of lower order.}$$

□

Theorem 4.9.13. *Let $R = \mathbb{K}[x_1, \ldots, x_m]$ be a graded ring, M a graded finitely generated R-module. Then the Hilbert polynomial $HP_M(d)$ is of degree* $\dim M - 1$.

Proof. This theorem is proved in [Theorem 4.1.3 [BH93]]. □

Remark 4.9.14. In the setting of Corollary 4.9.12, let $P_{F_i}(t)$ and $P_R(t)$ be the Hilbert or Poincaré series of F_i and R respectively, then

$$\begin{aligned}
& P_M(t) = \sum_d H_M(d)t^d = \sum_d \left(\sum_{i=0}^{s} (-1)^i \dim F_i \right) t^d \\
= & \sum_{i=0}^{s} (-1)^i \left(\sum_d \dim F_i \cdot t^d \right) = \sum_{i=0}^{s} (-1)^i P_{F_i}(t) = \sum_{i=0}^{s} (-1)^i P_{\oplus_j R(-a_{ij})}(t) \\
= & \sum_{i=0}^{s} (-1)^i \left(\sum_j c_{ij} P_R(t) t^{a_{ij}} \right) = P_R(t) \left(\sum_{i=0}^{s} (-1)^i \sum_j c_{ij} t^{a_{ij}} \right) \\
= & \frac{1}{(1-t)^m} \left(\sum_{i=0}^{s} \sum_j (-1)^i c_{ij} t^{a_{ij}} \right).
\end{aligned}$$

Definition 4.9.15. The **Euler polynomial** of the resolution $F^\bullet$ of M in Corollary 4.9.12 is defined as

$$E_{F^\bullet}(t) = \sum_{i \geq 0} \sum_j (-1)^i c_{ij} t^j \in \mathbb{Z}[t].$$

Since every graded free resolution of M is isomorphic to the direct sum of the minimal graded free resolution, the Euler polynomial does not depend on the resolution. If we take the minimal free resolution of M, and let $E_M(t)$ be **Euler polynomial of** M, and

$$E_M(t) = \sum_{i \geq 0} \sum_j (-1)^i c_{ij} t^j.$$

The rank of i-th free module in $F^\bullet$ is $\text{rank}F_i = \sum_j c_{ij} = \beta_i(M)$ where β_i is the i-th Betti number. The **Euler characteristic** of M, $\text{Char}(M)$, is defined as

$$\text{Char}(M) = E_M(1) = \sum_{i\geq 0}\sum_j (-1)^i c_{ij} = \sum_{i\geq 0}(-1)^i \text{rank}F_i = \sum_{i\geq 0}(-1)^i \beta_i(M).$$

Hence, the Hilbert or Poincaré series of M over $R = \mathbb{K}[x_1, \ldots, x_m]$ can be written as

$$P_M(t) = \frac{f(t)}{(1-t)^m} = \frac{E_M(t)}{(1-t)^m}.$$

If $s = \max\{s \in \mathbb{Z} \mid (1-t)^s \mid E_M(t)\}$, let

$$h(t) = \frac{E_M(t)}{(1-t)^s}, \quad \text{and then} \quad P_M(t) = \frac{h(t)}{(1-t)^w}, \quad \text{where } w = m - s.$$

$h(1)$ is called the **(geometric) multiplicity** or **degree** of the module M, and we denote it by $\text{mult}(M)$. If $\dim M = 0$, then $\text{mult}(M)$ is defined to be $\ell(M)$, the length of M.

The following results are proved by Vasconcelos [Mac71] concerning the Euler Characteristic and the annihilator of an R-module M.

Theorem 4.9.16. *Let M be a R-module with a finite free resolution of finite length. Then the Euler characteristic of M, is a non-negative integer, i.e., $0 \leq \text{Char}(M) \in \mathbb{Z}$, and*

1. *If $\text{Char}(M) > 0$ if and only if $\text{Ann}_R(M) = 0$.*
2. *If $\text{Char}(M) = 0$ if and only if $\text{Ann}_R(M) \neq 0$ if and only if $(0 :_R \text{Ann}_R(M)) = 0$.*

With above notation, we conclude the following theorem, and leave the proof as an exercise.

Theorem 4.9.17. *Let $R = \mathbb{K}[x_1, \ldots, x_m]$ be a graded ring, M a finitely generated graded R-module. If M is not Artinian, then*

1. *Hilbert or Poincaré series $P_M(t) = \dfrac{h(t)}{(1-t)^{\dim M}}$.*
2. *The leading coefficient of the Hilbert polynomial $HP_M(d)$ is*

$$\frac{h(1)}{(\dim M - 1)!}$$

3. If $h(t) = h_r t^r + \cdots + h_1 t + h_0$, *then Hilbert polynomial*

$$HP_M(d) = \sum_{0 \le j \le r} h_j \binom{\dim M - 1 + d - j}{\dim M - 1}.$$

4. $\dim(M_d) = HP_M(d)$ *for all* $d \ge \deg(h(t))$.

If M *is Artinian, then* $P_M(t) = h(t)$, *and* $h(1)$ *is the length of* M.

Remark 4.9.18. If the graded Betti numbers of M are known, then we can compute $P_M(t)$, $\dim M$, $HP_M(t)$, and $\text{mult}(M)$, the multiplicity of M.

Example 4.9.19. Let $R = \mathbb{K}[x, y]$, and $M = \mathbb{K}[x, y]/\langle x^2, xy, y^3 \rangle$. Based on the minimal free resolution calculated in Example 4.8.14, Hilbert or Poincaré series is

$$P_M(t) = \frac{1 - 2t^2 - t^3 + t^3 + t^4}{(1-t)^2} = \frac{1 - 2t^2 + t^4}{(1-t)^2} = 1 + 2t + t^2 = h(t).$$

We see that M is an Artinian, and

$$\ell(M) = \text{mult}(M) = h(1) = 4.$$

If $R = \mathbb{K}[x, y, z]$, and $M = \mathbb{K}[x, y, z]/\langle x^2, xy, y^3 \rangle$, then Hilbert or Poincaré series is

$$P_M(t) = \frac{1 - 2t^2 - t^3 + t^3 + t^4}{(1-t)^3} = \frac{1 + 2t + t^2}{1 - t} = 1 + 3t + 4t^2 + \sum_{d \ge 3} 4t^d.$$

$$h(t) = 1 + 2t + t^2,\ h(1) = 4,\ HP_M(d) = 4.$$

Hence,

$$\dim M = 1,\ \text{mult}(M) = 4.$$

Remark 4.9.20. Let the Krull dimension of the module M be $\dim(M) = d$. We will see how to compute the invariant of the module called *multiplicity* or *geometric multiplicity* of M, i.e. $\text{mult}(M)$.

1. The Hilbert or Poincaré series of M is of the form

$$P_M(t) = \sum_{n \in \mathbb{Z}} \dim_{\mathbb{K}}(M_n) t^n = \frac{h(t)}{(1-t)^d}, \quad \text{mult}(M) = h(1).$$

2. The Hilbert polynomial, $HP_M(t)$ of M, is of degree $d-1$ such that $HP_M(n) = \dim_{\mathbb{K}}(M_n)$ for $n \gg 0$, and

$$HP_M(t) = \frac{a_{d-1}}{(d-1)!}t^{d-1} + \text{ terms of lower degrees in } t, \ \text{mult}(M) = a_{d-1}.$$

3. Let R be a graded ring and $\dim R = d$, then the subscheme $\text{Proj}\,(R) \subset \mathbb{P}^r_{\mathbb{K}}$ is of dimension $d-1$. The degree of $\text{Proj}\,(R)$ over $\mathbb{P}^r_{\mathbb{K}}$ is defined to be the number of points obtained by cutting $\text{Proj}\,(R)$ by $d-1$ generic linear forms $L_1, \ldots, L_{d-1}$. The scheme $S = \text{Proj}\,(R/(L_1, \ldots, L_{d-1}))$ is finite and for $n \gg 0$, and

$$\deg_{\mathbb{P}^r_{\mathbb{K}}}(\text{Proj}\,(R)) = \dim_{\mathbb{K}}(\Gamma(S, \mathcal{O}_S)) = \dim_{\mathbb{K}}\left(\frac{R_n}{(L_1, \ldots, L_{d-1})_n}\right).$$

Since we have the following exact sequence

$$0 \to R(-1) \xrightarrow{L_1} R \to R/(L_1) \to 0,$$

$$P_{R/(L_1)}(t) = P_R(t) - P_{R(-1)}(t) = (1-t)P_R(t) = \frac{h(1)}{(1-t)^{d-1}},$$

and by recursion relation, we obtain the geometric degree of R is in fact the multiplicity of R, i.e.,

$$\deg_{\mathbb{P}^r_{\mathbb{K}}}(\text{Proj}\,(R)) = \text{mult}(R) = h(1) = a_{d-1}.$$

Definition 4.9.21. Let $(R, \mathfrak{m})$ be a local ring, $M \neq 0$ a finite R-module, and $I \subset \mathfrak{m}$ an ideal of definition of R such that $\mathfrak{m}^n M \subset IM$ for some $n \in \mathbb{Z}$. The length $\ell(M/I^n M)$ is a polynomial function for a large $n \in \mathbb{N}$. This polynomial is called **Hilbert-Samuel polynomial** of M with respect to I. It is of degree $d = \dim_{\mathbb{K}}(M)$ of the form

$$s_I(M, n) = \ell(M/I^n M) = \frac{e(I, M)}{d!}x^d + \text{ terms of lower degrees in } x.$$

The number $e(I, M)$ is called the **algebraic multiplicity of I in M.**

For a zero-dimensional scheme, one defines the algebraic multiplicity as the follows: let J be a graded ideal of a $\mathbb{N}$-graded ring R, if $T = \text{Proj}\,(R/J)$ is a finite subscheme of $\text{Proj}\,(R)$, then the algebraic multiplicity is

$$e(T, \text{Proj}\,(R)) = \sum_{\mathfrak{p} \in T} e(J_{\mathfrak{p}}, R_{\mathfrak{p}}).$$

Theorem 4.9.22. *(The Associative Formula) Let $R = R_0[R_1]$ be a Noetherian graded ring where R_0 is an Artinian local ring. Let M be a non-zero finitely generated graded R-module and $\dim M = n$. Then*

$$\text{mult}(M) = \sum_{\dim R/\mathfrak{p}=n} \ell(M_{\mathfrak{p}}) \cdot \text{mult}(R/\mathfrak{p}), \quad \textit{where } \mathfrak{p} \textit{ is a prime ideal in } R.$$

Proof. We prove by induction on n. If $\dim M = n = 0$, then by definition of multiplicity, we have that $\text{mult}(M) = \ell(M)$.

Assume $n \geq 1$, and let $0 \subsetneq M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_r = M$ be a quasi-composition series for M, where $M_i/M_{i-1} \cong (R/\mathfrak{p}_i)(m_i)$, and m_i is the degree twists for all $i = 1, \ldots, r$. We note that $\dim R/\mathfrak{p}_i \leq n$ for all i. The exact sequence $0 \to M_{i-1} \to M_i \to R/\mathfrak{p}_i(m_i)$ yields

$$HP_{M_i}(d) - HP_{M_{i-1}}(d) = HP_{(R/\mathfrak{p}_i)(m_i)}(d), \ \forall\, i = 1, \ldots, r.$$

Hence,

$$HP_M(d) - HP_{M_r}(d) = \sum_{i=0}^{r} HP_{(R/\mathfrak{p}_i)(m_i)}(d) = \sum_{i=0}^{r} HP_{(R/\mathfrak{p}_i)}(d + m_i).$$

$\text{mult}(M)$ is the leading coefficient of $HP_M(d)$, i.e., the coefficient of the term d^{n-1}. In order for this to equal to the leading coefficient of the $\sum_{i=0}^{r} HP_{R/\mathfrak{p}_i}(d + m_i)$, the prime ideal $\mathfrak{p}_i$ must be such that $\dim R/\mathfrak{p}_i = n$ for some i. By Theorem 4.9.5, the number of times that $\dim R/\mathfrak{p} = n$ occur in the quasi-composition series is $\ell_{R_0}(M_{\mathfrak{p}})$. Thus

$$\text{mult}(M) = \sum_{\dim R/\mathfrak{p}=n} \ell(M_{\mathfrak{p}}) \cdot \text{mult}(R/\mathfrak{p}), \quad \text{where } \mathfrak{p} \text{ is a prime ideal in } R.$$

□

4.10 Applications

4.10.1 Compute the Free Resolution

A free resolution of a module M can be thought of as the process of approximating M by free modules; it is constructed iteratively by starting with a set of generators for M, then determining the relations among these generators, the so-called first syzygies, then the relations among these relations, the second syzygies, and so forth. If, for some ℓ, there are no relations among

the ℓ-th syzygies, then this process terminates and we say the resolution has length ℓ.

In this section, we will investigate the free resolution of an ideal given by $I = \langle f_0(s,t,u), f_1(s,t,u), f_2(s,t,u), f_3(s,t,u)\rangle$ where f_i are linearly independent homogeneous forms in $R = \mathbb{K}[s,t,u]$ with $\deg(f_i) = 2$ and $\gcd(f_i) = 1$. In fact, our assumption on the ideal I implies that $f_0, \ldots, f_3$ define a morphism

$$\mathbf{f} : (s,t,u) \in \mathbb{P}^2 \to (f_0, f_1, f_2, f_3) \in \mathbb{P}^3 \tag{4.2}$$

of $\mathbb{K}$-varieties that is generically finite-to-one. The image S of this map is a surface in $\mathbb{P}^3$.

The free resolution of the ideal I is affected by *base points* of the projective parametrization.

Definition 4.10.1. $(s_0, t_0, u_0) \in \mathbb{P}^2$ is called a *base point* of the parametrization given by Equation (4.2), if $(s_0, t_0, u_0) \in Z = \mathbb{V}(I)$, i.e., (s_0, t_0, u_0) is a common root of the polynomials f_i for $i = 0, 1, 2, 3$.

Base points play an important role in the image of the parametrization. For a base point $p \in Z$, there are two multiplicities: one is the *algebraic multiplicity*, denoted by $e_p = e(\mathcal{I}_{Z,p}, \mathcal{O}_{\mathbb{P}^2,p})$, where $\mathcal{I}_Z \subset \mathcal{O}_{\mathbb{P}^2}$ is the ideal sheaf of $Z \subset \mathbb{P}^2$. This is the multiplicity of the intersection of two generic combinations of the polynomials f_i's at the base point p. The other multiplicity is the *geometric multiplicity*, also called the *degree* of the point p, defined as $d_p = \dim_{\mathbb{K}} \mathcal{O}_{Z,p}$. In general, if p is a base point, $e_p \geq d_p \geq 1$, but $e_p = d_p$ if and only if p is a local complete intersection. Moreover, if Z consists of finitely many points, and Z is local complete intersection at each point, then $e_p = d_p$ for every $p \in Z$, and for $d \gg 0$

$$\sum_{p\in Z} e_p = \deg Z = \sum_{p\in Z} \dim_{\mathbb{K}} \mathcal{O}_{Z,p} = \dim_{\mathbb{K}} H^0(Z, \mathcal{O}_Z) = \dim_{\mathbb{K}}(R/I)_d.$$

We set $e_p = d_p = 0$ if p is not a base point.

Bézout's Theorem stated below (see [Cox01a] for detailed proof) provides a relationship between the multiplicity of base points and the degree of a variety.

Theorem 4.10.2. *Let S be a surface in projective 3-space given by the image of a generic 1-to-1 rational parametrization as in Equation* (4.2) *with* $\deg(f_i) = d$, *then*

$$\deg(S) = d^2 - \sum_{p\in Z} e_p,$$

where $Z = \mathbb{V}(f_0, f_1, f_2, f_3)$ is the set of base points, and e_p is the algebraic multiplicity of the base point p.

As an application of the Theorem 4.10.2, let us study the degree of a quadratically parametrized surface via study the base points.

Corollary 4.10.3. *Let S be a surface in projective 3-space given by the image of a generic 1-to-1 rational parametrization as in Equation* (4.2) *with* $\deg(f_i) = 2$*, then*

$$\deg Z = \sum_{p \in Z} e_p \leq 2, \quad \textit{i.e., } Z \textit{ is a local complete intersection,}$$

where $Z = \mathbb{V}(f_0, f_1, f_2, f_3)$ is the set of base points, e_p is the algebraic multiplicity of the base point p, and $\deg Z$ is the degree of the variety Z.

Proof. The degree of the image surface cannot be one because that would imply a $\mathbb{K}$-linear dependence among the f_i, which is excluded. Theorem 4.10.2 therefore implies that any generically 1-1 quadratically parametrized surface can be of degree 4, 3 or 2 provided that the parametrization has no base point, total base point multiplicity 1, or 2.

If $Z = \emptyset$, then $\sum_{p \in Z} e_p = \deg Z = 0 \Rightarrow d_p = e_p = 0$.

If $\sum_{p \in Z} e_p = 1$, then $Z = \{p\}$, and the inequality between the algebraic multiplicity and geometric multiplicity, $1 = e_p \geq d_p \geq 1$, forces $e_p = d_p$. Hence $\sum_{p \in Z} e_p = \deg Z = 1$.

If $\sum_{p \in Z} e_p = 2$, then there are two base points of multiplicity one each, or there is one base point of multiplicity two.

First, if $Z = \{p_1, p_2 \mid p_1 \neq p_2\}$, then $e_{p_i} = d_{p_i}$ for $i = 1, 2$. Hence $\sum_{p \in Z} e_p = \deg Z = 2$.

Now, if $Z = \{p\}$, and $e_p = 2$, we claim that $d_p = 2$. Otherwise, $d_p = \dim_{\mathbb{K}} H^0(Z, \mathcal{O}_Z) = \dim_{\mathbb{K}}(\mathcal{O}_{\mathbb{P}^2,p}/\mathcal{I}_{Z,p}) = 1$. This means that $\mathcal{I}_{Z,p}$ is the maximal ideal of the regular local ring $\mathcal{O}_{\mathbb{P}^2,p}$ which implies $e_p = e(\mathcal{I}_{Z,p}, \mathcal{O}_{\mathbb{P}^2,p}) = 1$ (this is well known; it can also be seen from the combinatorial computation of e_p in [Sta99]), a contradiction.

Thus, we conclude in either case $\sum_{p \in Z} e_p = \deg Z$, that is, Z is a local complete intersection. □

Now, we will study the free resolution of the ideal I according to the base points.

Proposition 4.10.4. *Let $I = \langle f_0, f_1, f_2, f_3 \rangle \subset R$ where f_i's are given as in Equation* (4.2) *and* $\deg(f_i) = 2$*, then the projective dimension of I is 2.*

Proof. We will provide a sketch of the proof, and study the free resolution based on the existence of the base point.

Case 1: $\mathbb{V}(I) = \emptyset$. Apply the Auslander-Buchsbaum Formula,

$$\mathrm{pd}(R/I) = \mathrm{depth}(\mathfrak{m}, R) - \mathrm{depth}(\mathfrak{m}, R/I) = 3 - 0 = 3, \quad \mathfrak{m} = \langle s, t, u \rangle.$$

It follows directly that $\mathrm{pd}(I) = \mathrm{pd}(R/I) - 1 = 2$.

Case 2: $\mathbb{V}(I) \neq \emptyset$. Since $\mathrm{pd}(R/I) \leq 3$, $\mathrm{pd}(I) = \mathrm{pd}(R/I) - 1 \leq 2$, and we will show that it is impossible for $\mathrm{pd}(I) < 2$.

$\mathrm{pd}(I) \neq 0$. Otherwise, $I \cong R^m$ for some m, which must be 1 since $I \subset R$, which would imply that I is principal which it is not.

$\mathrm{pd}(I) \neq 1$. Suppose $\mathrm{pd}(I) = 1$, this means that $\mathrm{Syz}(f_0, f_1, f_2, f_3)$ is a free R-module. Then the minimal free resolution of I of the form:

$$0 \to \bigoplus_{i=1}^{m} R(-2 - \mu_i) \to R^4(-2) \xrightarrow{f_0, f_1, f_2, f_3} I \to 0.$$

The above complex is exact, the rank condition requires $m = 3$. Moreover, the Hilbert polynomial computation implies that

$$\mu_1 + \mu_2 + \mu_3 = 2.$$

But this is not possible. Since $\mu_i \geq 0$ for $i = 1, 2, 3$, there must be at least one, say μ_1, is zero. This means that there is a linear relation between f_i, contradicting the assumption that f_i are linearly independent. Therefore, $\mathrm{Syz}(f_0, f_1, f_2, f_3)$ is not a free R-module.

Therefore, $\mathrm{pd}(I) = 2$. □

In addition to know the length of the free resolution, using the property of regularity of an ideal, Hoffman and Wang [HW14] proved the following theorem concerning the exact form of that the free resolution of I.

Theorem 4.10.5. *Let $I = \langle f_0, f_1, f_2, f_3 \rangle \subset R$, where f_i's are given as in Equation (4.2) with $\deg(f_i) = 2$. Then the free resolution of I has the form*

1. *If $\mathbb{V}(I) = \emptyset$, then*

$$0 \to R^2(-5) \to R^2(-3) \bigoplus R^3(-4) \xrightarrow{\mathbf{P}_1, \mathbf{P}_2, \mathbf{P}_3, \mathbf{P}_4, \mathbf{P}_5} R^4(-2) \to I \to 0,$$

where $\deg(\mathbf{P}_1) = \deg(\mathbf{P}_2) = 1$, $\deg(\mathbf{P}_3) = \deg(\mathbf{P}_4) = \deg(\mathbf{P}_5) = 2$ in s, t, u.

2. *If $\deg \mathbb{V}(I) = 1$, then*

$$0 \to R(-5) \to R^3(-3) \bigoplus R(-4) \xrightarrow{\mathbf{P}_1, \mathbf{P}_2, \mathbf{P}_3, \mathbf{P}_4} R^4(-2) \to I \to 0,$$

where $\deg(\mathbf{P}_1) = \deg(\mathbf{P}_2) = \deg(\mathbf{P}_3) = 1$, $\deg(\mathbf{P}_4) = 2$ in s, t, u.

3. *If* $\deg \mathbb{V}(I) = 2$, *then*

$$0 \to R(-4) \to R^4(-3) \xrightarrow{\mathbf{P}_1,\mathbf{P}_2,\mathbf{P}_3,\mathbf{P}_4} R^4(-2) \to I \to 0,$$

where $\deg(\mathbf{P}_1) = \deg(\mathbf{P}_2) = \deg(\mathbf{P}_3) = \deg(\mathbf{P}_4) = 1$ *in* s, t, u.

4.10.2 Implicitization via Syzygies

For a rational variety, there are two standard representations, the implicit representations and the parametric representations. For the purpose of geometric modeling, the rational curves or surfaces are usually represented by parametric equations, since this representation is suitable for plotting the points of the variety, and graphing on the computer screens. On the other hand, if the goal is to see whether a point is on a rational curve or surface, or to determine the intersections of the rational curves or surfaces, then it is more convenient to have implicit representations of the curve or surface in discussion. Thus, there is a need to be able to convert from one representation to the other.

In this section, we will concentrate on the implicitization problem, that is to find an implicit representation of a rational algebraic variety given by parametric equations, i.e. the smallest variety containing the parametrized curves or surfaces. The implicitization problem lies at the heart of several questions in computer-aided geometric design (CAGD) and geometric modeling, including intersection problems and membership queries. There are many advantages of implicit representations, for instance, they encompass a larger class of shapes than parametric ones, and certain operations are closed under the implicit representation but not under it's parametric counterpart.

The implicitization problem is an extremely interesting topic in the elimination theory, there have been many studies done on the topic, for example, [Cha93], [Bot11], [GG91], [Cha06], [BD10], [BJ03], [BC05], [BCD03], [Cox01a], [Cox01b], [CGZ00], [D'A01], [AHW05], and many others.

In general, the basic approach to finding an implicit equation of a parametric representation is to eliminate one or multiple variables. In practice, there are three different methods to find implicit equations of rational parametric curves or surfaces: Gröbner basis, resultant, and syzygy method.

Usually, by clearing denominators, the rational parametrization is converted into a projective parametrization $F : \mathbf{s} \in \mathbb{P}^m \to \mathbf{x} \in \mathbb{P}^n$. Since $\mathbf{0} \notin \mathbb{P}^n$, the parameters $\mathbf{s}$ such that $F(\mathbf{s}) = \mathbf{0}$ are not defined, and called *base points* of the parametrization. When base points are presented in the parametrization, the computation of implicitization becomes more difficult.

Theoretically, the Gröbner basis method will give the smallest variety which contains the image of the parametrization for all degrees and dimensions. But in practice, the computation via Gröbner basis is relatively slow, and machine and memory expensive. Hence, one wants to find other methods to have a faster computation.

Comparing to the Gröbner basis method, the resultant method is to compute the determinant of a certain matrix, which is the implicit presentation of the rational curves or surfaces. In general, it is much faster to compute the resultant than to compute the Gröbner basis. But one of the drawbacks of this method is that the determinant of the resultant matrix need not provide exactly the implicit representation; it can contain extraneous factors. Therefore, the current researches are focused on determining and eliminating the extraneous factors.

The third method for the implicitization of algebraic varieties is the syzygy method, that is the method of moving curves and surfaces. This method allows us to write the implicit equation in terms of certain syzygies, thus creates a smaller matrix, and it generates a more compact form than the resultant matrix.

Syzygy techniques have been developed recently as a tool for finding implicit equations. The first introduction of syzygy-like techniques in the implicitization problem was the use of moving lines to produce implicit equations for curves by Sederberg and Chen [SC95]. We will explain the implicitization problem via syzygy method by the case of rational plane curves.

Let $\mathbb{K}$ be a field, and let a, b, c be linearly independent homogeneous polynomials in the standard $\mathbb{Z}$-graded ring $R := \mathbb{K}[s, u]$ of the same degree d. We also assume that $\gcd(a, b, c) = 1$, which implies that a, b, c define a morphism $\phi : \mathbb{P}^1 \to \mathbb{P}^2$ of $\mathbb{K}$-varieties that is generically finite-to-one. The image C of this map is a curve in $\mathbb{P}^2$ and hence defined by an essentially unique $F \in \mathbb{K}[x_1, x_2, x_3]$, which identically satisfies $F(a, b, c) = 0$. This polynomial is absolutely irreducible (irreducible over the algebraic closure of $\mathbb{K}$). The implicitization problem is then the problem to compute this F by some algorithm. If we assume the stronger condition that the rational map is generically one-to-one, we say that the parametrization is proper (this is not to be confused with a proper morphism in algebraic geometry). In characteristic zero this is equivalent to the condition that the rational map $\mathbb{P}^1 \to C$ is a birational equivalence.

Definition 4.10.6. A **moving line** in $\mathbb{P}^2$ is a linear form

$$A(s, u)x_1 + B(s, u)x_2 + C(s, u)x_3,$$

where $A, B, C \in \mathbb{C}[s,u]$ are homogeneous of the same degree. We say that a moving line has **degree** k if A, B, C are homogeneous of degree k. If

$$A(s,u)a(s,u) + B(s,u)b(s,u) + C(s,u)c(s,u) = 0, \quad \forall (s:u) \in \mathbb{P}^1,$$

then we say **the moving line follows the parametrization** ϕ.

In the language of commutative algebra, the tuple (A, B, C) is a *syzygy* of (a, b, c), and we write this as $(A, B, C) \in \mathrm{Syz}(a, b, c)$, where $\mathrm{Syz}(a, b, c)$ is the *syzygy module* of (a, b, c) over the ring $\mathbb{C}[s, u]$. We let $\mathrm{Syz}(a, b, c)_k$ denote the set of syzygies (A, B, C) with A, B, C homogeneous of degree k. $\mathrm{Syz}(a, b, c)_k$ is a vector space over $\mathbb{C}$ which consists of the moving lines of degree k. The number of linearly independent moving lines of degree k is the dimension of the kernel of the following map:

$$R_k^3 \xrightarrow{(a,b,c)} R_{n+k} \quad \text{where} \quad (A, B, C) \to Aa + Bb + Cc$$

$R = \mathbb{C}[s, u]$ and R_k denotes the homogeneous forms of degree k.

In the case that the parametrization has no base point, i.e., $\mathbb{V}(a, b, c) = \emptyset$, and because $\dim R_{n-1}^3 = 3n$, and $\dim R_{2n-1} = 2n$, one can prove that the map

$$MP: \quad R_{n-1}^3 \xrightarrow{(a,b,c)} R_{2n-1} \text{ has maximal rank,}$$

hence, $\dim \mathrm{Syz}(a, b, c)_{n-1} = n$. This result is related to the regularity we will discuss in the later chapter.

If $k = n-1$, we have n linearly independent moving lines of degree $n-1$ of the form

$$A_i x_1 + B_i x_2 + C_i x_3 = \sum_{j=0}^{n-1} L_{ij}(x_1, x_2, x_3) s^j u^{n-1-j},$$

where $(A_i, B_i, C_i) \in \mathrm{Syz}(a, b, c)_{n-1}$ are homogeneous polynomials in s, u [Cox01b]. We can use these n moving lines to construct an $n \times n$ matrix, where the columns of the matrix are indexed by the monomial bases of R_{n-1}, the rows of the matrix are indexed by the linearly independent moving lines $A_i x_1 + b_i x_2 + C_i x_3$, and the entries of the matrix are the coefficients $L_{ij}(x_1, x_2, x_3)$ of $s^j t^{n-1-j}$ in the moving lines. The following result is proved in [CSC98]:

Theorem 4.10.7. *The implicit equation of ϕ is $F = 0$, where*

$$F^h = \det(L_{ij}(x_1, x_2, x_3)), \quad \textit{and } h \textit{ is the generic degree of } \phi : \mathbb{P}^1 \to \mathbb{P}^2.$$

Now, we will provide a very simple example to illustrate the method.

Example 4.10.8. Let the parametrization of a curve be given as the following:

$$x = s^2 + t^2,\ y = s^2 - t^2,\ z = 2st.$$

There are two moving lines that follow the parametrization:

$$sz - (x + y)t, \quad (-x + y)s + zt$$

Construct the matrix

$$M = \begin{bmatrix} z & -(x+y) \\ -x+y & z \end{bmatrix},$$

and $\det(M) = y^2 + z^2 - x^2$ is the implicit equation.

We also note that use the combination of syzygy and resultant method, we can compute the following example.

Example 4.10.9. Consider

$$a = s^d,\ b = s^{d-1}t,\ c = t^d.$$

$\mathrm{Syz}(a, b, c)$ is a free module generated by two elements p, q, which we write as

$$p = tx - sy \qquad q = t^{d-1}y - s^{d-1}z.$$

Let $\tilde{p} = tx - y$, $\tilde{q} = t^{d-1}y - z$ by setting $s = 1$. Use the property of resultant, i.e., the condition on x, y such that the surface $tx - y = 0$ and $t^{d-1}y - z = 0$ have a common solution,

$$\mathrm{Res}(\tilde{p},\, \tilde{q}) = \mathrm{Res}(tx - y, t^{d-1}y - z) = x^{d-1}z - y^d.$$

Hence, $x^{d-1}z - y^d = 0$ is the implicit equation of the given parametrization.

4.10.3 Compute the Rees Algebra

The Rees algebra of an ideal $I \subset R$ defined as the graded algebra (with the elements of R having degree 0 and the elements of I having degree 1)

$$\mathrm{Rees}(I) = R \oplus I \oplus I^2 \oplus ...$$

is a classical algebraic structure which has been studied for decades by the Commutative Algebra community. One motivation for this study is that it

is related to a classical problem in elimination theory: the implicitization problem.

For instance consider the implicitization problem for rational curves in $\mathbb{P}^2$. Algebraically the problem is this: Given an ideal $I = \langle a, b, c\rangle \subset R$ where the a, b, c are homogeneous polynomials of degree d in the standard $\mathbb{Z}$-graded ring $R := \mathbb{K}[s, t]$ over an infinite field $\mathbb{K}$, find a minimal set of generators for the kernel of the map

$$h : R[x, y, z] \to \text{Rees}(I), \text{ where } h(x) = a,\ h(y) = b,\ h(z) = c.$$

$$\ker(h) = \bigoplus_{r=1}^{\infty} \text{Syz}(I^r),$$

$\ker(h)$ is precisely the moving curve ideal. Under certain general circumstances, the implicit equation F is the element of $\ker(h)$ of degree 0 in the variables s, t.

Elements of $\ker(h)$, under the name of moving lines and moving curves, were introduced into Computer Aided Geometric Design by Sederberg, Cox and their collaborators in order to develop robust. In the past two years, [Bus09], [Cox08], [CHW08], and [HSV08] utilized the method of moving curves and surfaces to determine the defining equations for the Rees algebra of plane algebraic curves. They each develop different methods and algorithms for finding explicit moving curves that are a minimal set of generators for the associated Rees algebra. The approach in [Cox08], [CHW08] is based on iterations of Sylvester determinants, regular sequences, and local cohomology computations

Different computational methods are developed to calculate the Rees algebra. Below, we will provide a procedure to handle a rational planar curve with μ-basis of degree $(1, d-1)$. To be more specific, we assume that the minimal free resolution of the ideal $I = \langle a, b, c\rangle$ has the following form:

$$0 \longrightarrow R(-d-1) \oplus R(-2d+1) \xrightarrow{p,q} R^3(-d) \longrightarrow I \longrightarrow 0.$$

The syzygies $\text{Syz}(a, b, c)$ are generated by two elements p, q with degrees 1, $d-1$ respectively. We can regard p, q as moving lines

$$p = p_x x + p_y y + p_z z, \quad \text{where } \deg(p_x) = \deg(p_y) = \deg(p_z) = 1 \text{ in } s, t$$
$$q = q_x x + q_y y + q_z z, \quad \text{where } \deg(q_x) = \deg(q_y) = \deg(q_z) = d-1 \text{ in } s, t.$$

These two elements p, q are called a μ-basis.

We set $R = \mathbb{K}[s,t]$, $A = \mathbb{K}[x,y,z]$, $C = A[s,t] = R[x,y,z]$. We give C a bigrading by declaring that s,t have bidegree $(0,1)$, and x,y,z have bidegree $(1,0)$. Let $I = \langle a,b,c\rangle \subset R$, $\mathfrak{m} = \langle s,t\rangle \subset C$, and $B = C/\langle p,q\rangle$. Then

$$\ker(h)/\langle p,q\rangle = (\langle p,q\rangle : \mathfrak{m}^\infty)/\langle p,q\rangle = H^0_{\mathfrak{m}}(B) \subset B,$$

where $H^0_{\mathfrak{m}}(B)$ is the zero-th local cohomology of B, which we will introduce in the next chapter. To find the minimal generators of $\ker(h)$, we will study the generators of $H^0_{\mathfrak{m}}(B)$. Using homological method introduced in the later chapter, Cox, Hoffman and Wang [CHW08] proved that there is an isomorphism of A-modules:

$$H^0_{\mathfrak{m}}(B)_\ell = \mathrm{Ker}(H^2_{\mathfrak{m}}(C)_{\ell-d} \xrightarrow{p,q} H^2_{\mathfrak{m}}(C)_{\ell-1} \oplus H^2_{\mathfrak{m}}(C)_{\ell-d+1}),$$

and $H^0_{\mathfrak{m}}(B)_\ell$ is a free module generated by one element. Moreover, they provided the following algorithm to produce the Rees algebra.

Algorithm 4.10.10. Given $a,b,c \in R$ homogeneous of degree $d \geq 3$ with $\mu = 1$ and $\gcd(a,b,c) = 1$, we compute $d+1$ elements of C as follows.

I. Compute a μ-basis p,q of $\mathrm{Syz}(a,b,c)$ with bidegrees $(1,1),(1,d-1)$ respectively when regarded as element of C. Write p,q in the form:

$$\begin{aligned} p &= p_s s + p_t t; \qquad & \mathrm{bideg}(p_s) = \mathrm{bideg}(p_t) &= (1,0) \\ q &= q_{1s} s + q_{1t} t; \qquad & \mathrm{bideg}(q_{1s}) = \mathrm{bideg}(q_{1t}) &= (1,d-2). \end{aligned}$$

II. Compute

$$q_2 := \det \begin{pmatrix} p_s & p_t \\ q_{1s} & q_{1t} \end{pmatrix}, \ \mathrm{bideg}(q_2) = (2,d-2).$$

III. Write $q_2 = q_{2s}s + q_{2t}t$, $\mathrm{bideg}(q_{2s}) = \mathrm{bideg}(q_{2t}) = (2,d-3)$ and compute

$$q_3 := \det \begin{pmatrix} p_s & p_t \\ q_{2s} & q_{2t} \end{pmatrix}, \ \mathrm{bideg}(q_3) = (3,d-3).$$

IV. Repeat this process to obtain

$$q_{i+1} := \det \begin{pmatrix} p_s & p_t \\ q_{is} & q_{it} \end{pmatrix}, \ \mathrm{bideg}(q_{i+1}) = (i+1,d-i-1).$$

V. The algorithm stops when we obtain

$$q_d := \det \begin{pmatrix} p_s & p_t \\ q_{(d-1)s} & q_{(d-1)t} \end{pmatrix}, \ \text{bideg}(q_d) = (d, 0).$$

The following theorem proved that the above algorithm produce exactly $d+1$ generators for Rees algebra associated to the curve.

Theorem 4.10.11 (Theorem 2.3, [CHW08]). *Let $a, b, c \in R := \mathbb{K}[s,t]$ have degree $d \geq 3$, $\mu = 1$, $\gcd(a,b,c) = 1$ and assume that the parametrization is proper. Then Algorithm 4.10.10 gives $d+1$ minimal generators of the ideal $\ker(h)$, that is, $p, q, q_2, \ldots, q_{d-1}, q_d$. Furthermore, $F = q_d$ is the implicit equation of the curve parametrized by a, b, c.*

Here we will the example in [CHW08] to illustrate the computational algorithm.

Example 4.10.12. Consider

$$a = s^d, \ \ b = s^{d-1}t, \ \ c = t^d.$$

Let the ideal $I = \langle a, b, c \rangle \subset R$. The Hilbert-Burch resolution

$$0 \longrightarrow R(-d-1) \oplus R(-2d+1) \longrightarrow R^3(-d) \longrightarrow I \longrightarrow 0$$

shows that $\text{Syz}(a,b,c)$ is a free module generated by two elements p, q, which we write as

$$\begin{aligned} p &= tx - sy \\ q &= t^{d-1}y - s^{d-1}z. \end{aligned}$$

The moving curve ideal K has $d+1$ generators:

I. One moving line of degree 1 in s, t:

$$p = tx - sy.$$

II. One moving line of degree $d-1$ in s, t:

$$q = t^{d-1}y - s^{d-1}z.$$

III. One moving quadric of degree $d-2$ in s,t:

$$q_2 = xzs^{d-2} - y^2t^{d-2}.$$

This is obtained by writing

$$p = -ys + xt,\ \ q = (-zs^{d-2})s + (yt^{d-2})t;$$

and taking the determinant

$$q_2 = \det\begin{pmatrix} -y & x \\ -zs^{d-2} & yt^{d-2} \end{pmatrix} = xzs^{d-2} - y^2t^{d-2}.$$

IV. Continue the process, each time use p, q_i to find the new generators q_{i+1} of degree one less in s,t than q_i. For example:

$$q_3 = \det\begin{pmatrix} -y & x \\ xzs^{d-3} & -y^2t^{d-3} \end{pmatrix} = -x^2zs^{d-3} + y^3t^{d-3}.$$

V. The implicit equation is q_d with degree zero in s,t:

$$F = q_d = x^{d-1}z - y^d.$$

Note, the implicit equation obtained as one of the generators of the Rees algebra is exactly the same as computed via resultant of the μ-basis in Example 4.10.9.

Singular code "ReesAlgebra (I)" returns the Rees algebra $R[It]$ as an affine ring, where I is an ideal in R. For example [GPS01],

```
LIB "reesclos.lib";
ring R = 0,(x,y),dp;
ideal I = x2,xy4,y5;
list L = ReesAlgebra(I);
def Rees = L[1];
setring Rees;
Rees;
==> //   characteristic : 0
==> //   number of vars : 5
==> //        block   1 : ordering dp
==> //                  : names    x y U(1) U(2) U(3)
==> //        block   2 : ordering C
```

```
ker;
==> ker[1]=y*U(2)-x*U(3)
==> ker[2]=y^3*U(1)*U(3)-U(2)^2
==> ker[3]=y^4*U(1)-x*U(2)
==> ker[4]=x*y^2*U(1)*U(3)^2-U(2)^3
==> ker[5]=x^2*y*U(1)*U(3)^3-U(2)^4
==> ker[6]=x^3*U(1)*U(3)^4-U(2)^5
```

4.10.4 Resultants

Elimination Theory deals with the problem of finding conditions on parameters of a polynomial system so that the equations have a common solution in a fixed algebraic set V. In a typical situation of $n+1$ polynomials

$$\begin{cases} f_0(\mathbf{x}) & = \sum_{j=0}^{k_0} c_{0,j}\mathbf{x}^{\alpha_{0,j}} \\ & \vdots \\ f_n(\mathbf{x}) & = \sum_{j=0}^{k_n} c_{n,j}\mathbf{x}^{\alpha_{n,j}}, \end{cases}$$

where $\mathbf{x}^{\alpha_{i,j}}$ is a monomial with exponents a vector $\alpha_{i,j}$. The elimination problem involves to find the necessary and sufficient conditions on the parameters $\mathbf{c} = (c_{i,j})_{i,j=0}^{i=n,j=k_i}$ such that $f_i = 0$ have a common root in $\mathbf{x}$.

Resultants are essential tool in commutative algebra and algebraic geometry in solving system of polynomial equations. They can determine whether or not a system of $n+1$ polynomials in n variables have a common root without explicitly solving for the roots. Resultants are often represented as the determinants of matrices whose entries are polynomials in coefficients of the original polynomial equations. There are a few different constructions of a matrix whose determinant is the resultant or a nontrivial multiple of the resultant.

In the classical situation, in case of the monomials of degree d_i, i.e., f_i are generic homogeneous polynomials of degree d_i and $V = \mathbb{P}^n$, the projective n-dimensional space. Then the necessary and sufficient condition on the parameters $\mathbf{c}$ such that the homogeneous polynomials $f_0 = \cdots = f_n = 0$ have a common root in $V = \mathbb{P}^n$ is $\mathrm{Res}(f_0, \ldots, f_n) = 0$, where $\mathrm{Res}(f_0, \ldots, f_n)$ is the classical projective resultant.

In the geometric point of view, we are searching for the set of parameters $\mathbf{c}$ such that there exists $\mathbf{x} \in V$ such that $f_0 = \cdots = f_n = 0$. The parameters $\mathbf{c}$ form a vector, which is the projection of the point $(\mathbf{c}, \mathbf{x})$ of the variety W_V where

$$W_V = \{(\mathbf{c}, \mathbf{x}) \in \mathbb{P}^{k_0} \times \cdots \times \mathbb{P}^{k_n} \times V \mid f_0 = \cdots = f_n = 0\},$$

and the two projections π_1 and π_2 are

$$\pi_1 : W_V \to \mathbb{P}^{k_0} \times \cdots \times \mathbb{P}^{k_n}, \quad \pi_2 : W_V \to V.$$

The image of π_1 is the set of parameters $\mathbf{c}$ for which the system has a root, and any polynomial in $\mathbf{c}$ which vanishes on the projection $\pi_2(W_V)$ is called an *inertia form*, which is defined in van der Waerden [Wae95].

It is proven in Gelfand, Kapranov and Zelevinsky [GKZ94] that if π_1 is birational and π_2 is of codimension one, then there exists a unique polynomial (up to a scalar) such that $f_0 = \cdots = f_n = 0$ have a solution in V if and only if $\mathrm{Res}(f_0, \ldots, f_n) = 0$. This polynomial is called the *resultant of* $f_0, \ldots, f_n$ *on* V. It is an irreducible polynomial in the variables $\mathbf{c}$, and is invariant under linear transformations of the variables. Moreover, we have a divisibility property:

$$f_0 \ldots, f_n \in \langle b_0, \ldots, b_n \rangle \quad \Rightarrow \quad \mathrm{Res}(b_0, \ldots, b_n) \mid \mathrm{Res}(f_0, \ldots, f_n).$$

There are various resultants corresponding to various V. If $V = \mathbb{P}^n$, then the resultant is called *projective resultant* . If V is the closure $(\overline{\mathbb{K}^*})^n$, then the resultant is called *toric resultant* , also known as the *sparse resultant*, which characterizes the existence of non-trivial common zeros in $(\overline{\mathbb{K}^*})^n$ for a system of $n+1$ (Laurent) polynomials in n variables.

Resultant matrix methods originate in works of Bézout, Sylvester, Cayley and Dixon. In particular, Dixon [Dix08] provided algorithms to construct three different resultant matrices for three bivariate polynomials, namely, Sylvester resultant matrix, Cayley resultant matrix, and Cayley-Sylvester resultant. In [SL05], Sun and Li provide a quick review of the construction of these three classical resultant matrices, and they generalize the construction to a system of $n+1$ polynomials in n-variables, called *generic mixed Cayley-Sylvester matrix*.

One of the classic matrices named Macaulay matrix is a generalization of the Sylvester matrix for a system of $n+1$ polynomials in n-variable. For example, as a special case, the resultant of two polynomials is the determinant of the Sylvester's matrix we discussed in the previous chapters.

Algorithm 4.10.13. *The Macaulay's construction of the resultant of polynomials* $\mathbf{f} = \{f_0, \ldots, f_n\}$ *of degree* $d_0, \ldots, d_n$ *in the variables* $\mathbf{x} = x_1, \ldots, x_n$ *are as follows:*

1. *Let* $v = \sum_{i=0}^{n} d_i - n$, *and* $\mathbf{x}^{\mathcal{B}} = \{\mathbf{x}^{\mathbf{v}} : |\mathbf{v}| = v\}$.
2. *Let* $\mathbf{x}^{\mathcal{B}_0} = \{x_1^{v_1} \cdots x_n^{v_n} : 0 \le v_i \le d_i - 1\}$, *and there is a total of* $d_1 \cdots d_n$ *monomials.*

3. *Let* $\mathbf{x}^{\mathcal{B}_n} = \left\{ \dfrac{x_1^{v_1} \cdots x_n^{v_n}}{x_n^{d_n}} : \begin{array}{l} v_n \geq d_n, \text{ and} \\ 0 \leq v_i \leq d_i - 1, \quad 2 \leq i \leq n-1 \end{array} \right\}$.

4. *Repeat the process, let* $\mathbf{x}^{\mathcal{B}_j} =$

$$\left\{ \frac{x_1^{v_1} \cdots x_n^{v_n}}{x_j^{d_j}} \in \mathbf{x}^{\mathcal{B}} - \cup_{i=j+1}^{n} \mathbf{x}^{\mathcal{B}_i} : \begin{array}{l} v_j \geq d_j, \text{ and} \\ 0 \leq v_i \leq d_i - 1, \quad 1 < i \leq j-1 \end{array} \right\}.$$

5. *The matrix* M *is a square matrix, the size is the same as the number of monomials in* $x_1, \ldots, x_n$ *of total degree* v*, i.e.,* M *is of size* $\binom{v+n}{n} \times \binom{v+n}{n}$*. The columns of the matrix are indexed by the monomials* $\mathbf{x}^{\mathcal{B}}$*; the rows are indexed by the polynomials*

$$\{\mathbf{x}^{\mathcal{B}_0} f_0; \mathbf{x}^{\mathcal{B}_1} f_1; ...; \mathbf{x}^{\mathcal{B}_n} f_n\}.$$

The entries of the matrix are the coefficients $\mathbf{c}$ *of the polynomials* f_i *for* $i = 0, \ldots, n$*.*

The determinant of the matrix, $\det(M)$*, is a non-trivial multiple of the resultant* $\mathrm{Res}(f_0, \ldots, f_n)$*. Moreover,* $\det(M)$ *is homogeneous of degree* $d_1 \cdots d_n$ *in the coefficients of* f_0*. Thus, the resultant* $\mathrm{Res}(f_0, \ldots, f_n)$ *is the GCD of the determinants of all of the matrices obtained this way by a cyclic permutation of the polynomials* $f_0, \ldots, f_n$*.*

Example 4.10.14. Let $n = 2$ and $f_0, f_1, f_2 \in \mathbb{K}[x_1, x_2]$,

$$\begin{aligned} f_0 &= a + bx_1 + cx_2, \\ f_1 &= d + ex_1 + fx_2, \\ f_2 &= m + nx_1^2. \end{aligned}$$

To construct Macaulay's matrix, we have that $v = 1+1+2-2 = 2$, we will construction a matrix M of size $\binom{v+n}{n} \times \binom{v+n}{n} = 6 \times 6$. Thus, the columns of the matrix M are indexed by the monomials of

$$\mathbf{x}^{\mathcal{B}} = \{\mathbf{x}^{\mathbf{v}} : |\mathbf{v}| = v\} = \{1, x_1, x_2, x_1^2, x_1x_2, x_2^2\},$$

$$\mathbf{x}^{\mathcal{B}_0} = \{1, x_2\}, \quad \mathbf{x}^{\mathcal{B}_1} = \{1, x_1, x_2\}, \quad \mathbf{x}^{\mathcal{B}_2} = \{1\}.$$

The rows of the matrix M are indexed by the polynomials

$$\{\mathbf{x}^{\mathcal{B}_0} f_0; \mathbf{x}^{\mathcal{B}_1} f_1; \mathbf{x}^{\mathcal{B}_2} f_2\} = \{f_0, x_2 f_0; f_1, x_1 f_1, x_2 f_1; f_2\}.$$

$$M = \begin{bmatrix} a & b & c & 0 & 0 & 0 \\ 0 & 0 & a & 0 & b & c \\ d & e & f & 0 & 0 & 0 \\ 0 & d & 0 & e & f & 0 \\ 0 & 0 & d & 0 & e & f \\ m & 0 & 0 & 0 & n & 0 \end{bmatrix}.$$

Now, if we do cyclic permutation of the three polynomials, we can construct M_1 and M_2, where the columns still have the same index as M, and

$$\text{rows of } M_1 \text{ are indexed by : } \{f_1, x_1f_1; f_2; f_0, x_1f_0, x_2f_0\}.$$

$$\text{rows of } M_2 \text{ are indexed by : } \{f_2; f_0, x_1f_0, f_1; x_1f_1, x_2f_1, \}.$$

Therefore, we have

$$M_1 = \begin{bmatrix} d & e & f & 0 & 0 & 0 \\ 0 & d & 0 & e & f & 0 \\ m & 0 & 0 & 0 & n & 0 \\ a & b & c & 0 & 0 & 0 \\ 0 & a & 0 & b & c & 0 \\ 0 & 0 & a & 0 & b & c \end{bmatrix} \quad M_2 = \begin{bmatrix} m & 0 & 0 & 0 & n & 0 \\ a & b & c & 0 & 0 & 0 \\ 0 & a & 0 & b & c & 0 \\ 0 & d & 0 & e & f & 0 \\ d & e & f & 0 & 0 & 0 \\ 0 & 0 & d & 0 & e & f \end{bmatrix}.$$

And $\det(M) = Re$, $\det(M_1) = Rc$, and $\det(M_2) = Rb$ where

$$\begin{aligned} R &= \operatorname{Res}(f_0, f_1, f_2) = \gcd(\det(M), \det(M_1), \det(M_2) \\ &= a^2efn - adn(bf + ce) - b^2f^2m + bc(d^2n + 2efm) - c^2e^2m. \end{aligned}$$

In order to reduce the size of the Macaulay matrix, we introduce a new matrix named Bézoutian matrix. We refer [CM96] and [EM96] for the details of the theory of Bezoutians.

Definition 4.10.15. For any sequence of $n+1$ polynomials $\mathbf{f} = \{f_0, \ldots, f_n\}$ of degree $d_0, \ldots, d_n$ in n variables $x_1, \ldots, x_n$, let

$$\mathbf{x}^{(0)} = \mathbf{x} = (x_1, \ldots, x_n),\ \mathbf{x}^{(1)} = (y_1, \ldots, x_n), \ldots,\ \mathbf{x}^{(n)} = \mathbf{y} = (y_1, \ldots, y_n).$$

The **discrete differentiation of** p for any polynomial $p(\mathbf{x})$ is defined as

$$\theta_i = \frac{p(\mathbf{x}^{(i)}) - p(\mathbf{x}^{(i-1)})}{y_i - x_i}.$$

The polynomial $\Theta_{\mathbf{f}}$ constructed below is called **Bézoutian** of $f_0, f_1, \ldots, f_n$:

$$\Theta_{\mathbf{f}}(\mathbf{x}, \mathbf{y}) = \det \begin{pmatrix} f_0(\mathbf{x}) & \theta_1(f_0) & \cdots & \theta_n(f_0) \\ f_1(\mathbf{x}) & \theta_1(f_1) & \cdots & \theta_n(f_1) \\ \vdots & \vdots & & \vdots \\ f_n(\mathbf{x}) & \theta_1(f_n) & \cdots & \theta_n(f_n) \end{pmatrix} = \sum_{\mathbf{a},\mathbf{b}} \theta^{\mathbf{f}}_{\mathbf{a},\mathbf{b}} \mathbf{x}^{\mathbf{a}} \mathbf{y}^{\mathbf{b}}.$$

Moreover,

$$\Theta_{\mathbf{f}}(\mathbf{x}, \mathbf{y}) = \sum_{\mathbf{a} \in E} \mathbf{y}^{\mathbf{a}} w_{\mathbf{a}}(\mathbf{x}),$$

defines a map

$$\Phi : \mathbb{K}^E \to \mathbb{K}[x_1, \ldots, x_n], \quad (\lambda_{\mathbf{a}})_{\mathbf{a} \in E} \to \sum_{\mathbf{a} \in E} \lambda_a w_{\mathbf{a}}.$$

The matrix of this map in the monomial basis is the matrix of the coefficients $B_{\mathbf{f}} = [\theta^{\mathbf{f}}_{\mathbf{a},\mathbf{b}}]_{\mathbf{a},\mathbf{b}}$, and is called **the Bézoutian matrix of f** of the Bézoutian in the monomial basis.

Example 4.10.16. Again, let $n = 2$ and $f_0, f_1, f_2 \in \mathbb{K}[x_1, x_2]$,

$$\begin{aligned} f_0 &= a + bx_1 + cx_2, \\ f_1 &= d + ex_1 + fx_2, \\ f_2 &= m + nx_1^2. \end{aligned}$$

Then, based on the construction described above, we have

$$\begin{aligned} \Theta_{\mathbf{f}} &= \det \begin{pmatrix} a + bx_1 + cx_2 & b & c \\ d + ex_1 + fx_2 & e & f \\ m + nx_1^2 & n(x_1 + y_1) & 0 \end{pmatrix} \\ &= m(bf - ce) + n(cd - af)y_1 + n(cd - af)x_1 + n(ce - bf)y_1x_1. \end{aligned}$$

We will construct the Bézoutian matrix $B_{\mathbf{f}}$ where the columns are indexed by the monomials in the variables $\mathbf{y}$, that is $\{1, y_1\}$ and the rows are indexed by the monomials in $\mathbf{x}$, that is $\{1, x_1\}$.

$$B_{\mathbf{f}} = [\theta^{\mathbf{f}}_{\mathbf{a},\mathbf{b}}]_{\mathbf{a},\mathbf{b}} = \begin{pmatrix} m(bf - ce) & n(cd - af) \\ n(cd - af) & n(ce - bf) \end{pmatrix}.$$

The Bézoutian matrix is usually much smaller than the Macaulay's matrix. Combining Bézoutian matrix and Macaulay matrix, one obtains another new matrix called **Dixon's matrix**. We will refer the reader to [Dix08].

Definition 4.10.17. For any sequence of $n+1$ polynomials $\mathbf{f} = \{f_0, \ldots, f_n\}$ of degree $d_0, \ldots, d_n$ in n variables $x_1, \ldots, x_n$, let

$$\mathbf{x}^{(0)} = \mathbf{x} = (x_1, \ldots, x_n),\ \mathbf{x}^{(1)} = (y_1, \ldots, x_n), \ldots,\ \mathbf{x}^{(n)} = \mathbf{y} = (y_1, \ldots, y_n).$$

The **Dixon polynomial** is

$$\Theta_{\mathbf{f}}(\mathbf{x}, \mathbf{y}) = \frac{\det \begin{pmatrix} f_0(\mathbf{x}) & f_1(\mathbf{x}) & \cdots & f_n(\mathbf{x}) \\ f_0(\mathbf{x}^{(1)}) & f_1(\mathbf{x}^{(1)}) & \cdots & f_n(\mathbf{x}^{(1)}) \\ \vdots & \vdots & & \vdots \\ f_0(\mathbf{x}^{(n)}) & f_2(\mathbf{x}^{(n)}) & \cdots & f_n(\mathbf{x}^{(n)}) \end{pmatrix}}{\prod_{i=1}^{n}(y_i - x_i)} = \overline{\mathbf{y}}^T \times \theta_{\mathbf{f}} \mathbf{x},$$

where $\mathbf{y} = [\mathbf{y}^{\beta_1}, \ldots, \mathbf{y}^{\beta_k}]$ and $\mathbf{x} = [\mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_t}]$ are column vectors. The matrix $\theta_{\mathbf{f}}$ is called the **Dixon matrix**.

Example 4.10.18. Again, let $n = 2$ and $f_0, f_1, f_2 \in \mathbb{K}[x_1, x_2]$,

$$\begin{aligned} f_0 &= a + bx_1 + cx_2, \\ f_1 &= d + ex_1 + fx_2, \\ f_2 &= m + nx_1^2. \end{aligned}$$

Then, based on the construction described above, we have

$$\begin{aligned} & \theta_{\mathbf{f}}(\mathbf{x}, \mathbf{y}) \\ = & \frac{\det \begin{pmatrix} a + bx_1 + cx_2 & a + by_1 + cx_2 & a + by_1 + cy_2 \\ d + ex_1 + fx_2 & d + ey_1 + fx_2 & d + ey_1 + fy_2 \\ m + nx_1^2 & m + ny_1^2 & m + ny_1^2 \end{pmatrix}}{(y_1 - x_1)(y_2 - x_2)} \\ = & m(bf - ce) + n(cd - af)y_1 + n(cd - af)x_1 + n(ce - bf)y_1x_1 \\ = & \mathbf{y}^T \begin{pmatrix} m(bf - ce) & n(cd - af) \\ n(cd - af) & n(ce - bf) \end{pmatrix} \mathbf{x}^T. \end{aligned}$$

The Dixon matrix is

$$\theta_{\mathbf{f}} = \begin{pmatrix} m(bf - ce) & n(cd - af) \\ n(cd - af) & n(ce - bf) \end{pmatrix}.$$

In this example, the Dixon matrix is the same as the Bézoutian matrix.

In general, the size of the Macaulay matrices is larger than the size of Bézout matrices, which is larger than that of the Dixon's matrices. But is more difficult to analyze the structure of a Bézoutian matrix than a structure of a Macaulay matrix. One of the research topics is to construct smaller size matrices and extract information from the determinants of these smaller matrices to determine the resultant.

5. Homological Method

5.1 Complexes

Definition 5.1.1. A **complex** is a collection of (abelian) groups or modules and homomorphisms,

$$\cdots \to M_{i+1} \xrightarrow{d_{i+1}} M_i \xrightarrow{d_i} M_{i-1} \to \cdots$$

where M_i's are groups or modules, and d_i's are group or module homomorphisms, and for all i, $d_i \circ d_{i+1} = 0$. Sometimes, we will use $C_\bullet$, or $M_\bullet$ or $(M_\bullet, d_\bullet)$ to denote the complex. The elements of $Z_n = \ker(d_n)$ are called the **n-th cycles**, and the elements of $B_n = \mathrm{im}(d_{n+1})$ are called the **n-th boundaries**.

A complex is **bounded below** if $M_i = 0$ for all $i \ll 0$; **bounded above** if $M_i = 0$ for all $i \gg 0$; and **bounded** if it is both bounded above and below.

A complex is **exact at the i-th place** if $\ker(d_i) = \mathrm{im}(d_{i+1})$. A complex is **exact** if it is exact for all i.

A complex is **free, flat, projective, injective** if all the M_i's are free, flat, projective, or injective.

Given a complex

$$C_\bullet : \quad \cdots \to M_{i+1} \xrightarrow{d_{i+1}} M_i \xrightarrow{d_i} M_{i-1} \to \cdots,$$

then the **n-th homology group or module of this complex** is

$$H_n(C_\bullet) = \ker(d_n)/\mathrm{im}(d_{n+1}).$$

A **cocomplex** is given and numbered as

$$C^\bullet : \quad \cdots \to M^{i-1} \xrightarrow{d^{i-1}} M^i \xrightarrow{d^i} M^{i+1} \to \cdots,$$

then the **n-th cohomology group or module of this cocomplex** is

$$H^n(C^\bullet) = \ker(d^n)/\mathrm{im}(d^{n-1}).$$

Many results about complexes can be transposed to cocomplexes and vice-versa. If $(C_\bullet, d_\bullet)$ is a complex, we can define a cocomplex $(K^\bullet, \delta^\bullet)$ by the rule $K^i = C_{-i}$ and

$$\delta^i : K^i = C_{-i} \xrightarrow{d_{-i}} C_{-i-1} = K^{i+1}.$$

A **free or projective resolution** of an R-module M is a complex

$$\cdots \to F_{i+1} \xrightarrow{d_{i+1}} F_i \xrightarrow{d_i} F_{i-1} \to \cdots \to F_1 \xrightarrow{d_1} F_0 \to 0,$$

where F_i is free or projective and

$$\cdots \to F_{i+1} \xrightarrow{d_{i+1}} F_i \xrightarrow{d_i} F_{i-1} \to \cdots \to F_1 \xrightarrow{d_1} F_0 \to M \to 0,$$

is exact.

An **injective resolution** of and R-module M is a complex

$$0 \to I^0 \to I^1 \to I^2 \to I^3 \to \cdots,$$

where I^i's are injective R-modules, and

$$0 \to M \to I^0 \to I^1 \to I^2 \to I^3 \to \cdots,$$

is exact.

Given a complex of R-modules

$$C_\bullet \quad \cdots \to C_{i+1} \xrightarrow{d_{i+1}} C_i \xrightarrow{d_i} C_{i-1} \to \cdots,$$

we can derive **homology complex** $H(C_\bullet)$

$$H(C_\bullet): \quad \cdots \to H_{i+1}(C_\bullet) \xrightarrow{0} H_i(C_\bullet) \xrightarrow{0} H_{i-1}(C_\bullet) \to \cdots$$

where the maps are zero maps since $d_i \circ d_{i+1} = 0$.

Definition 5.1.2. A **map of complexes** is a function $f_\bullet : C_\bullet \to C'_\bullet$, where $(C_\bullet, d)$ and $(C'_\bullet, d')$ are complexes, where $f_\bullet$ restricted to C_n is denoted f_n, where f_n maps to C'_n, and such that for all n, $d'_n \circ f_n = f_{n-1} \circ d_n$, or write as $d' \circ f_\bullet = f_\bullet \circ d$, with the commutative diagram

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & C_{n+1} & \xrightarrow{d_{n+1}} & C_n & \xrightarrow{d_n} & C_{n-1} & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle f_{n+1}} & & \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n-1}} & & \\
\cdots & \longrightarrow & C'_{n+1} & \xrightarrow{d'_{n+1}} & C'_n & \xrightarrow{d'_n} & C'_{n-1} & \longrightarrow & \cdots
\end{array}$$

If $f, g : C_\bullet \to C'_\bullet$ are two morphisms, we say that f, g are **homotopic**, denoted by $f \sim g$ if for each n, there is a linear map $h_n : C_n \to C'_{n+1}$ such that

$$f_n - g_n = d'_{n+1}h_n + h_{n-1}d_n.$$

If this occurs, then f, g induce the same map $H_n(C_\bullet) \to H_n(C'_\bullet)$ on homology. Two complex $C_\bullet$ and $C'_\bullet$ are **homotopy equivalent** if there exist morphisms $f : C_\bullet \to C'_\bullet$ and $g : C'_\bullet \to C_\bullet$ such that $gf \sim \mathrm{id}_C$ and $fg \sim \mathrm{id}_{C'}$. Homotopy equivalent complexes have the same homology.

Let $f_\bullet : C_\bullet \to C'_\bullet$ be a map of complexes. Then we get the induced map $f_* : H(C_\bullet) \to H(C'_\bullet)$ of complexes.

Lemma 5.1.3. *Let $0 \to C'_\bullet \to C \to C''_\bullet \to 0$ be a short exact sequence of complexes. If all modules in $C'_\bullet$ and $C''_\bullet$ are projective, so are all the modules in $C_\bullet$.*

Proof. Since $C''_\bullet$ is projective, the short exact sequence splits, and $C_\bullet \cong C'_\bullet \oplus C''_\bullet$. Since $C'_\bullet$ is also projective, we must have that $C_\bullet$ is projective. □

Theorem 5.1.4. *A short exact sequence of complexes yields a long exact sequence of homology sequence. That is, if*

$$0 \to C'_\bullet \xrightarrow{f_\bullet} C_\bullet \xrightarrow{g_\bullet} C''_\bullet \to 0$$

is a short exact sequence of complexes, then we have a long exact sequence on homology

$$\cdots \to H_{n+1}(C''_\bullet) \xrightarrow{\delta_{n+1}} H_n(C'_\bullet) \xrightarrow{f_n} H_n(C_\bullet) \xrightarrow{g_n} H_n(C''_\bullet) \xrightarrow{\delta_n} H_{n-1}(C'_\bullet) \xrightarrow{f_n} H_{n-1}(C_\bullet) \to \cdots$$

where f and g are induced by f and g is the short exact sequence, and δ is the connecting homomorphism.

Proof. First, we note that by assumption of the theorem, we have the following commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & C'_n & \xrightarrow{f_n} & C_n & \xrightarrow{g_n} & C''_n & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d'_n} & & \downarrow{\scriptstyle d_n} & & \downarrow{\scriptstyle d''_n} & & \\
0 & \longrightarrow & C'_{n-1} & \xrightarrow{f_{n-1}} & C_{n-1} & \xrightarrow{g_{n-1}} & C''_{n-1} & \longrightarrow & 0.
\end{array}$$

By the Snake lemma, we have the following exact sequence S_n for all n:

$$\begin{aligned} S_n: \quad 0 \to \ker d'_n &\xrightarrow{f_n} \ker d_n \xrightarrow{g_n} \ker d''_n \\ &\longrightarrow \operatorname{coker} d'_n \xrightarrow{f_n} \operatorname{coker} d_n \xrightarrow{g_n} \operatorname{coker} d''_n \to 0. \end{aligned}$$

There is a mapping from the last three terms of S_n to the first three terms of S_{n-1} as follows:

$$\begin{array}{ccccc} \operatorname{coker} d'_n & \xrightarrow{f_n} & \operatorname{coker} d_n & \xrightarrow{g_n} & \operatorname{coker} d''_n \to 0 \\ \downarrow{\scriptstyle \alpha'_n} & & \downarrow{\scriptstyle \alpha_n} & & \downarrow{\scriptstyle \alpha''_n} \\ 0 \to \ker d'_{n-1} & \xrightarrow{f_{n-1}} & \ker d_{n-1} & \xrightarrow{g_{n-1}} & \ker d''_{n-1}. \end{array}$$

Hence, by the Snake lemma again, we have the following exact sequence;

$$\begin{aligned} \ker \alpha'_n &\xrightarrow{f_n} \ker \alpha_n \xrightarrow{g_n} \ker \alpha''_n \longrightarrow \\ \operatorname{coker} \alpha'_n &\xrightarrow{f_n} \operatorname{coker} \alpha_n \xrightarrow{g_n} \operatorname{coker} \alpha''_n, \end{aligned}$$

where $\ker \alpha'_n = H_n(C'_\bullet)$, $\ker \alpha_n = H_n(C_\bullet)$, $\ker \alpha''_n = H_n(C''_\bullet)$, $\operatorname{coker} \alpha'_n = H_{n-1}(C'_\bullet)$, $\operatorname{coker} \alpha_n = H_{n-1}(C_\bullet)$, and $\operatorname{coker} \alpha''_n = H_{n-1}(C''_\bullet)$. We get the long exact sequence by splicing these together. □

Remark 5.1.5. We observe that if $0 \to C'_\bullet \to C_\bullet \to C''_\bullet \to 0$ is a short exact sequence of complexes, and $C'_\bullet$ and $C''_\bullet$ have zero homology, then $C_\bullet$ also has zero homology.

5.2 Complex of Tor

Let $\mathcal{F} : \mathsf{A} \to \mathsf{B}$ be an additive (covariant) functor between the abelian categories. We say that $\mathcal{F}$ is **left exact** (or **right exact**) if whenever it is applied to a short exact sequence, it produces a complex that is exact everywhere except possibly at the rightmost (or leftmost) non-zero module, i.e.,

$$0 \to M \to N \to P \quad \text{is exact in } \mathsf{A}$$

then

$$0 \to \mathcal{F}(M) \to \mathcal{F}(N) \to \mathcal{F}(P) \quad \text{is exact in } \mathsf{B}.$$

A functor is *exact* if it is both left and right exact.

We recall that if $\mathsf{A} = \mathsf{B} = \mathsf{Mod}_R$ are the categories of R-modules, and M is a fixed R-module, then $\mathcal{F}(T) = T \otimes_R M$ is right exact.

Given a complex of R-modules

$$C_\bullet \quad \cdots \to C_{i+1} \xrightarrow{d_{i+1}} C_i \xrightarrow{d_i} C_{i-1} \to \cdots,$$

then there is a **tensor product complex**:

$$C_\bullet \otimes_R M: \quad \cdots \to C_{i+1} \otimes_R M \xrightarrow{d_{i+1}\otimes \mathrm{id}} C_i \otimes_R M \xrightarrow{d_i \otimes \mathrm{id}} C_{i-1} \otimes_R M \to \cdots.$$

A Hom **from** M **complex** is $\mathrm{Hom}_R(M, C_\bullet)$:

$$\cdots \to \mathrm{Hom}_R(M, C_{i+1}) \xrightarrow{d_{i+1}\circ *} \mathrm{Hom}_R(M, C_i) \xrightarrow{d_i \circ *} \mathrm{Hom}_R(M, C_{i-1}) \to \cdots,$$

and a Hom **into** M **complex** is $\mathrm{Hom}_R(C_\bullet, M)$:

$$\cdots \to \mathrm{Hom}_R(C_{i-1}, M) \xrightarrow{*\circ d_{i-1}} \mathrm{Hom}_R(C_i, M) \xrightarrow{*\circ d_i} \mathrm{Hom}_R(C_{i+1}, M) \to \cdots.$$

If given another complex $K_\bullet$ of R-modules

$$K_\bullet: \quad \cdots \to K_{i+1} \xrightarrow{e_{i+1}} K_i \xrightarrow{e_i} K_{i-1} \to \cdots,$$

then the **tensor product of complexes** is

$$\begin{array}{ccccccc}
 & \downarrow & & \downarrow & & \downarrow & \\
\longrightarrow & C_n \otimes K_m & \longrightarrow & C_{n-1} \otimes K_m & \longrightarrow & C_{n-2} \otimes K_m & \longrightarrow \\
 & {\scriptstyle (-1)^n e_m}\downarrow & & {\scriptstyle (-1)^{n-1} e_m}\downarrow & & {\scriptstyle (-1)^{n-2} e_m}\downarrow & \\
\longrightarrow & C_n \otimes K_{m-1} & \longrightarrow & C_n \otimes K_{m-2} & \longrightarrow & C_n \otimes K_{m-2} & \longrightarrow \\
 & \downarrow & & \downarrow & & \downarrow &
\end{array}$$

The **bicomplex** is a complex along all vertical and along all horizontal strands. We obtain a **total complex** of the tensor product of $C_\bullet$ and $K_\bullet$: the n-th module is $G_n = \sum_i C_i \otimes K_{n-i}$, and the map $g_n : G_n \to G_{n-1}$ is defined $d_i \otimes \mathrm{id}_{K_{n-i}} + (-1)^i \mathrm{id}_{C_i} \otimes e_{n-i}$ where $d_i \otimes \mathrm{id}_{K_{n-i}}$ is in $C_{i-1} \otimes K_{n-i}$ and $(-1)^i \mathrm{id}_{C_i} \otimes e_{n-i}$ is in $C_i \otimes K_{n-i-1}$

$$\begin{aligned}
g_{n-1} \circ g_n|_{C_i \otimes K_{n-i}} &= g_{n-1}(d_i \otimes \mathrm{id}_{K_{n-i}} + (-1)^i \mathrm{id}_{C_i \otimes e_{n-i}}) \\
&= d_{i-1} \circ d_i \otimes \mathrm{id}_{K_{n-i}} + (-1)^{i-1} d_i \otimes e_{n-i} \\
&\quad + (-1)^i d_i \otimes e_{n-i} + (-1)^{2i} \mathrm{id}_{C_i} \otimes e_{n-i-1} \circ e_{n-i} \\
&= 0.
\end{aligned}$$

Definition 5.2.1. Let M, N be R modules, and $P_\bullet$ a projective resolution of M

$$P_\bullet : \quad \cdots \to P_2 \to P_1 \to P_0 \to 0.$$

We define

$$\mathrm{Tor}_i^R(M, N) = H_i(P_\bullet \otimes_R N).$$

Remark 5.2.2. Following are few observations concerning Tor

1. $\mathrm{Tor}_i^R(M, *)$ is independent, up to isomorphism, of the projective resolution $P_\bullet$ of M.
2. Since $P_i = 0$ for all $i < 0$, $\mathrm{Tor}_i^R(M, *) = 0$ for all $i < 0$.
3. $P_1 \to P_0 \to M \to 0$ is exact, so $P_1 \otimes N \to P_0 \otimes N \to M \otimes N \to 0$ is exact, and
$$\mathrm{Tor}_0^R(M, N) = H_0(P_\bullet \otimes N) = (P_0 \otimes N)/\mathrm{im}(P_1 \otimes N) \cong M \otimes N.$$
4. If M is projective, then $P_0 = M$, and $\mathrm{Tor}_i^R(M, *) = 0$ for all $i \geq 1$.
5. If N is flat, then tensoring by N preserves exactness, and $\mathrm{Tor}_i^R(M, N) = 0$ for all $i \geq 1$.
6. Let $0 \to M_n \to P_{n-1} \to \cdots \to P_1 \to P_0 \to M \to 0$ where P_i is projective, and M_n is the *n-th syzygy of* M. Then $\mathrm{Tor}_i^R(M_n, N) = \mathrm{Tor}_{n+i}^R(M, N)$.

In addition to these remarks, we will state a few important properties of the functor Tor without detailed proofs. For detailed proofs, one may consult [Wei95].

Theorem 5.2.3. *Let R be a commutative ring, and M and N R-modules. Then*

$$\mathrm{Tor}_n^R(M, N) \cong \mathrm{Tor}_n^R(N, M), \quad \forall\, n.$$

One of the important characterizations of flat modules is done via homological criteria below.

Theorem 5.2.4. *(Homological Criteria for Flat Modules) The following are equivalent for an R-module M.*

1. *M is flat.*
2. *For every R-module N, and every $n \in \mathbb{N}$, $\mathrm{Tor}_n^R(N, M) = 0$.*

3. *For every ideal* $I \subset R$, $\mathrm{Tor}_1(R/I, M) = 0$.

4. *For every ideal* $I \subset R$, *the natural map:*

$$I \otimes_R M \to M \quad \textit{is injection.}$$

5. *For every finitely generated* R*-module* N, $\mathrm{Tor}_1^R(N, M) = 0$.

6. *For every injection* $f : N \to P$, *with* N, P *finitely generated,*

$$f \otimes 1 : N \otimes M \to P \otimes M \quad \textit{is also injective.}$$

Definition 5.2.5. An R-module M is **torsion** if for every $m \in M$, there exists a non-zero divisor $r \in R$ such that $rm = 0$. A module is **torsion free** if no non-zero elements is annihilated by any non-zero divisor in R.

Proposition 5.2.6. *Let* R *be a graded ring, and* $\mathfrak{m} = R_+$ *the irrelevant ideal. Let* $F_\bullet : \cdots \to F_i \to F_{i-1} \to \cdots \to F_1 \to F_0$ *be a minimal graded free resolution of a finitely generated graded* R*-module* M, *and* $\mathbb{K} = R/\mathfrak{m}$ *the residue field. Then any minimal set of homogeneous generators of* F_i *contains precisely* $\dim_{\mathbb{K}} \mathrm{Tor}_i^R(\mathbb{K}, M)_j$ *generators of degree* j.

Proof. The vector space $\mathrm{Tor}_i^R(\mathbb{K}, M)_j$ is the degree j part of the graded vector space of the i-th homology of the complex $\mathbb{K} \otimes_R F_\bullet$. The minimality of the complex yields that the maps in $\mathbb{K} \otimes_R F_\bullet$ are all zero, so $\mathrm{Tor}_i^R(\mathbb{K}, M) = \mathbb{K} \otimes_R F_i$. Hence, by Nakayama's lemma, $\dim \mathrm{Tor}_i^R(\mathbb{K}, M)$ is the number of generators of F_i, hence $\dim \mathrm{Tor}_i^R(\mathbb{K}, M) = \mathrm{rank} F_i$, and $\dim \mathrm{Tor}_i^R(\mathbb{K}, M)_j$ is the number of degree j generators of F_i. □

Remark 5.2.7.

1. Any flat R-module is torsion free. If R is a principal ring, then an R-module is flat if and only if it is torsion free. (This is by item 4 in Theorem 5.2.4.)

2. For any R-module N, and any short exact sequence

$$0 \to F' \to F \to F'' \to 0,$$

where F'' is flat, then the sequence

$$0 \to N \otimes_R F' \to N \otimes_R F \to N \otimes_R F'' \to 0$$

is also exact. (The short sequence tensor by $N\otimes$ gives us the long exact sequence of $\mathrm{Tor}_n(N, *)$, and $\mathrm{Tor}_1(N, F'') = 0$ by item 5 in Theorem 5.2.4. Thus, we have the desired short exact sequence.)

3. Given a short exact sequence

$$0 \to F' \to F \to F'' \to 0.$$

If F'' is flat, then F' is flat if and only if F is flat.

5.3 Koszul Complex

In commutative algebra, if $x \in R$, then multiplication by x is R-linear, and this represents an R-module homomorphism $x : R \to R$, hence, we can construct a complex called the **Koszul complex** of R with respect to x

$$K_\bullet(x): \quad 0 \to R \xrightarrow{x} R \to 0.$$

We note that $H_0(K_\bullet(x)) = R/xR$, and $H_1(K_\bullet(x)) = \mathrm{Ann}(x)$.

Now, if $x_1, x_2, \ldots, x_n \in R$, the Koszul complex of R with respect to $x_1, x_2, \ldots, x_n \in R$, usually denoted $K_\bullet(x_1, x_2, \ldots, x_n)$, is the tensor product over R of the Koszul complexes defined above individually for each i. The Koszul complex is a free chain complex. There are exactly $\binom{n}{j}$ copies of the ring R in the j-th degree in the complex $(0 \le j \le n)$. The matrices involved in the maps can be written down precisely. Let $e_{i_1 \ldots i_p}$ for $1 \le i_1 < \cdots < i_p \le n$ be a free basis of K_p, and define $d : K_p \to K_{p-1}$ as:

$$d(e_{i_1 \ldots i_p}) := \sum_{j=1}^{p} (-1)^{j-1} x_{i_j} e_{i_1 \ldots \widehat{i_j} \ldots i_p}.$$

In the case of two elements x and y, the Koszul complex can then be written down as

$$0 \to R \xrightarrow{d_2} R^2 \xrightarrow{d_1} R \to 0,$$

with the matrices d_1 and d_2 given by

$$d_1 = \begin{bmatrix} x & y \end{bmatrix}, \quad d_2 = \begin{bmatrix} -y \\ x \end{bmatrix}.$$

Note that d_i is applied on the left. The cycles in degree 1 are then exactly the linear relations on the elements x and y, while the boundaries are the trivial relations. The first Koszul homology $H_1(K_\bullet(x, y))$ therefore measures exactly the relations mod the trivial relations.

Proposition 5.3.1. *Let R be a commutative ring, $C_\bullet$ a complex over R, and $K_\bullet = K_\bullet(x;R)$ the Koszul complex of $x \in R$. Then we get a short exact sequence of complexes*

$$0 \to C_\bullet \to C_\bullet \otimes K_\bullet \to C_\bullet[-1] \to 0,$$

and for each n, we have the following maps

$$C_n \xrightarrow{f_n} (C_n \otimes R) \oplus (C_{n-1} \otimes R) \cong C_n \oplus C_{n-1} \xrightarrow{g_n} (C_\bullet[-1])_n = C_{n-1},$$

where $f_n(a) = (a, 0)$ and $g_n(a, b) = b$.

Proof. We define $\delta_n : C_n \oplus C_{n-1} \to C_{n-1} \oplus C_{n-2}$ by

$$\delta(a, b) = (d_n(a) + (-1)^{n-1}xb, d_{n-1}(b)), \ \forall\, n,$$

and this makes $0 \to C_\bullet \to C_\bullet \otimes K_\bullet \to C_\bullet[-1] \to 0$ into an exact sequence of complexes. □

Remark 5.3.2. From the short exact sequence $0 \to C_\bullet \to C_\bullet \otimes K_\bullet \to C_\bullet[-1] \to 0$, we obtain a long exact sequence

$$\begin{aligned} \cdots \xrightarrow{x} \quad & H_n(C_\bullet) \to H_n(C_\bullet \otimes K_\bullet) \to H_n(C_\bullet[-1]) = H_{n-1}(C_\bullet) \\ \xrightarrow{x} \ & H_{n-1}(C_\bullet) \to H_{n-1}(C_\bullet \otimes K_\bullet) \to H_{n-1}(C_\bullet[-1]) = H_{n-2}(C_\bullet). \end{aligned}$$

Moreover, the long exact sequence also breaks into short exact sequences:

$$0 \to H_n(C_\bullet)/xH_n(C_\bullet) \to H_n(C_\bullet \otimes K_\bullet) \to \mathrm{Ann}_{H_{n-1}(C_\bullet)}(x) \to 0.$$

Another construction of Koszul complex is via exterior power.

Definition 5.3.3. If M is an R-module, the **n-fold tensor product of** M is denoted by $M^{\otimes n} = M \otimes \cdots \otimes M$, n-copies. In general, $M^{\otimes 0} = R$, $M^{\otimes 1} = M$, $M^{\otimes 2} = M \otimes M$, $M^{\otimes(n+1)} = M^{\otimes n} \otimes M$. The **$n$-th exterior power of a module** M is

$$\bigwedge^n M = \frac{M^{\otimes n}}{\langle m_1 \otimes \cdots \otimes m_n : m_1, \ldots, m_n \in M, m_i = m_j \text{ for some } i \neq j \rangle}.$$

The image of an element $m_1 \otimes \cdots \otimes m_n \in M^{\otimes n}$ is written as $m_1 \wedge \cdots \wedge m_n$. If $e_1, \ldots, e_t$ form a basis for R^t, then $\wedge^n R^t$ is generated by

$$B = \{e_{i_1} \wedge \cdots \wedge e_{i_n} \mid 1 \leq i_1 < i_2 < \cdots < i_n \leq t\}.$$

Moreover, we can verify that B is a basis for $\wedge^n R^t$, and $\wedge^n R^t \cong R^{\binom{t}{n}}$.

For any $r_1, \dots, r_n \in R$, define a complex $G_\bullet(r_1, \dots, r_n; R)$ as below

$$0 \to \wedge^n R^t \to \wedge^{n-1} R^t \to \cdots \to \wedge^2 R^t \to \wedge^1 R^t \to \wedge^0 R^t \to 0$$

where the map $f_n : \wedge^n R^t \to \wedge^{n-1} R^t$ is given by

$$f_n(e_{i_1} \wedge \cdots \wedge e_{i_n}) = \sum_{j=1}^{n} (-1)^{j+1} x_j e_{i_1} \wedge \cdots \wedge \widehat{e_{i_j}} \wedge \cdots \wedge e_{i_n}.$$

We can check this is exactly the same map as the one given in the Koszul complex, and this is other way to construct a Koszul complex.

$$G_\bullet(r_1, \dots, r_n; R) = K_\bullet(r_1, \dots, r_n; R).$$

With this construction, we can observe the following remark.

Remark 5.3.4. Let M be an R-module, and $r_1, \dots, r_n \in R$. Then

$$H_n(K_\bullet(r_1, \dots, r_n; R)) = H_n(G_\bullet(r_1, \dots, r_n; R)) = \mathrm{Ann}_M(r_1, \dots, r_n).$$

Definition 5.3.5. We say that $r_1, \dots, r_n \in R$ is a **regular sequence** on an R-module M or a M**-regular sequence** if $(r_1, \dots, r_n)M \neq M$ and if for all $i = 1, \dots, n$, r_i is a non-zerodivisor on $M/(x_1, \dots, x_{i-1})M$. We say that $r_1, \dots, r_n \in R$ is a **regular sequence** if it is a regular sequence on the R-module R.

Corollary 5.3.6. *If $r_1, \dots, r_n \in R$ is a regular sequence on a commutative ring R, then*

$$H_i(K_\bullet(r_1, \dots, r_n; R)) = \begin{cases} 0 & \text{if } i > 0 \\ R/(r_1, \dots, r_n) & \text{if } i = 0. \end{cases}$$

Thus $K_\bullet(r_1, \dots, r_n; R)$ is a free resolution of $R/(r_1, \dots, r_n)$.

Proof. We will prove the result by induction on n. If $n = 1$, this is true. We assume the result is true for all $n-1$ and $n \geq 2$. We will prove it is true for n. Let $C_\bullet = K_\bullet(r_1, \dots, r_{n-1}; R)$, and $K_\bullet = K_\bullet(r_n; R)$. Then by induction hypothesis, we have for $i \geq 2$,

$$H_i(r_1, \dots, r_n; R) = H_i(C_\bullet \otimes K_\bullet) = 0.$$

If $i = 1$, we have the short exact sequence

$$0 \to H_1(C_\bullet)/r_n H_1(C_\bullet) \to H_1(C_\bullet \otimes K_\bullet) \to \mathrm{Ann}_{H_0(C_\bullet)}(r_n) \to 0.$$

Since r_n is a non-zero divisor, we have $H_1(C_\bullet)/r_nH_1(C_\bullet) = 0$, and

$$H_1(C_\bullet \otimes K_\bullet) \cong \mathrm{Ann}_{H_0(C_\bullet)}(r_n) = \mathrm{Ann}_{R/(r_1,\ldots,r_{n-1})}(r_n) = 0$$

If $i = 0$, we have

$$\begin{aligned} H_0(K_\bullet(x_1,\ldots,x_n;R)) &\cong H_0(C_\bullet \otimes K_\bullet) \cong H_0(C_\bullet)/r_nH_0(C_\bullet) \\ &\cong R/(r_1,\ldots,r_n). \end{aligned}$$

□

Remark 5.3.7. If R is a graded ring, M a graded R-module, and x_i homogeneous elements with $\deg(x_i) = \alpha_i$, then there are degree shifts in the Koszul complex so that the differentials d_i are all maps of degree zero.

$$K_\bullet(\mathbf{x}, M) = \bigwedge\left(\bigoplus_{i=1}^n Re_i\right), \quad \text{where} \quad \bigoplus_{i=1}^n Re_i \cong \bigoplus_{i=1}^n R(-\alpha_i).$$

Moreover, in the wedge products, we use the convention that $R(-\alpha) \otimes R(-\beta) = R(-\alpha-\beta)$. With this convention, the differentials preserve the degrees.

5.4 Regular Sequences

Definition 5.4.1. Let R be a commutative ring, M an R-module and I an ideal in R. The **I-depth** of M or the **grade of M with respect to I**, denoted by $\mathrm{depth}_I(M)$, is the supremum of the length of the sequence of elements in I which form regular sequences on M, i.e.

$$\mathrm{depth}_I(M) = \sup_n\{n \mid r_1,\ldots,r_n \in I \text{ that form a regular sequence on } M\}.$$

If $(R,\mathfrak{m})$ is local, the **depth** of M is the $\mathfrak{m}$-depth of M.

Proposition 5.4.2. *Let R be a Noetherian ring, M a finitely generated R-module, and $r_1,\ldots,r_n \in \mathfrak{J}$, where $\mathfrak{J}$ is the Jacobson radical of R. If $H_i(K_\bullet(r_1,\ldots,r_n;M)) = 0$ for $i = n, n-1,\ldots,n-\ell+1$, then there exist $s_1,\ldots,s_n \in R$ such that the ideals $\langle r_1,\ldots,r_n\rangle = \langle s_1,\ldots,s_n\rangle$ and $s_1,\ldots,s_\ell$ is a regular sequence on M.*

Proof. Without loss of generality, we assume that $\ell > 0$. By the given condition on H_n and Remark 5.3.4, we have that

$$0 = H_n(K_\bullet(r_1,\ldots,r_n;R)) = \mathrm{Ann}_M(r_1,\ldots,r_n).$$

Therefore, $\langle r_1, \ldots, r_n \rangle$ is not contained in any prime ideals which are associated primes of M. Then by Prime Avoidance, there exists $s_1 \in \langle r_1, \ldots, r_n \rangle$ such that $\mathrm{Ann}_M(s_1) = 0$. Hence, we can let $s_1 = r_1$. If $\ell > 1$, then again by Remark 5.3.4, for $i = n-1, \ldots, n-\ell+1$,

$$H_i(K_\bullet(r_2, \ldots, r_n; M))/r_1 H_i(K_\bullet(r_2, \ldots, r_n; M)) = 0,$$

and Nakayama's lemma shows that $H_i(K_\bullet(r_2, \ldots, r_n; M)) = 0$ for all $i = n-1, \ldots, n-\ell+1$. By induction, we can find elements $s_2, \ldots, s_n \in \langle r_2, \ldots, r_n \rangle$ such that $\langle r_2, \ldots, r_n \rangle = \langle s_2, \ldots, s_n \rangle$ and $s_2, \ldots, s_\ell$ is a regular sequence on M. Now, we are done since we may let $s_1 = r_1$. □

Lemma 5.4.3. *Let $r_1, \ldots, r_n$ be in the Jacobson radical of a Noetherian ring R. If $r_1, \ldots, r_n$ is a regular sequence on a finitely generated R-module M. Then for any permutation of $\{r_1, \ldots, r_n\}$, the new sequence is still a regular sequence.*

Proof. To prove the claim, we will show that if a, b form a regular sequence, then so does b, a.

First, we will show that a is a non-zero divisor on M/bM. If $am = bn$ for some $m, n \in M$. Then $n = az$ for some $z \in M$, so that $am - bn = a(m - bz) = 0$. Since a is a non-zero divisor on M, we must have that $m - bz = 0$, hence $m = bz = 0 \in M/bM$. Thus a is a non-zero divisor on M/bM.

Second, we will show that b is a non-zero divisor on M. If $bm = 0$ for some $m \in M$, since a, b form a regular sequence, we must have $m \in aM$, thus $m = an$ for some $n \in M$. So $0 = bm = ban = a(bn)$, but since a is a non-zero divisor on M, we must have that $bn = 0$. Repeating this process, we know that $n \in aM$, hence $m \in a^2M$, continue the process, we have $m \in a^kM$ for all k, thus $m \in \bigcap_{k=0}^{\infty} a^kM$, this is zero because a is in the Jacobson's radical. Thus, b is a non-zero divisor on M. Thus b, a is a regular sequence. □

Lemma 5.4.4. *Let $r_1, \ldots, r_n$ be in the Jacobson radical of a Noetherian ring R. If $r_1, \ldots, r_n$ is a regular sequence on a finitely generated R-module M. Then the new sequence $\{r_1^{m_1}, \ldots, r_n^{m_n} \mid m_i \in \mathbb{Z}_{>0}\}$ is still a regular sequence.*

Proof. If r_n is a non-zero divisor on $M/(r_1, \ldots, r_{n-1})M$, so is $r_n^{m_n}$, thus $\{r_1, \ldots, r_{n-1}, r_n^{m_n}\}$ is a regular sequence. We can permute the order, and continue the process. □

Proposition 5.4.5. *Let I be an ideal in a Noetherian ring R, M a finitely generated R-module. Let $r_1, \ldots, r_n \in I$ be a maximal regular sequence on M. Then every maximal regular sequence on M of elements in I has length n.*

Proof. Let $s_1, \ldots, s_m \in I$ be another maximal regular sequence on M. Without loss of generality, let $n \leq m$. We will show that $n \geq m$, hence $m = n$.

If $n = 0$, then every element of I is a zero divisor on M, so $m = 0$.

If $n = 1$. Then every element of I is a zero divisor on M/r_1M, then there exists $0 \neq x \in M/r_1M$ such that $xI \subseteq r_1M$. Thus there exists $s_1 \in I$ such that $s_1x = r_1x'$ for some $x' \in M$. We note $x' \notin s_1M$, otherwise, if $x' \in s_1M$, then $x \in r_1M$ since s_i's form a regular sequence, contradicting our assumption that $0 \neq x \in M/r_1M$. Therefore, we must have that $x' \notin s_1M$. Thus, $Ir_1x' = Is_1x \subseteq r_1s_1M$, therefore, $Ix' \subseteq s_1M$, thus every element of I is a zero divisor on M/s_1M. Thus $m = 1$.

Suppose $n > 0$, and $m > n$. Then, there exists a $a \in I$, and a is not a zero divisor on M, M/r_1M, M/s_1M, $M/(r_1, r_2)M$, $M/(s_1, s_2)M$, $\ldots$, $M/(r_1, \ldots, r_{n-1})M$, $M/(s_1, \ldots, s_{n-1})M$, and $M/(s_1, \ldots, s_n)M$, Then $r_1, \ldots, r_{n-1}, a$ and $s_1, \ldots, s_n, a$ form two regular sequences on M. This means that $r_1, \ldots, r_{n-1}$ and $s_1, \ldots, s_n$ are two regular sequences on M/aM. But the induction hypothesis says that $n < n-1$, a contradiction. Therefore, we must have that $m \leq n$. Thus, we must have $m = n$. □

Proposition 5.4.6. *Let M, N be finitely generated modules over a Noetherian local ring $(R, \mathfrak{m})$. If $\mathrm{pd}(M) = n$ is finite, and $\mathfrak{m} \in \mathrm{Ass}(N)$, then $\mathrm{Tor}_n^R(M, N) \neq 0$.*

Proof. We first note that there exists an exact sequence $0 \to R/\mathfrak{m} \to N \to L \to 0$. This short exact sequence gives a long exact sequence

$$\cdots \to \mathrm{Tor}_{n+1}^R(M, L) \to \mathrm{Tor}_n^R(M, R/\mathfrak{m}) \to \mathrm{Tor}_n^R(M, N) \to \mathrm{Tor}_n^R(M, L) \to \cdots$$

Since $\mathrm{pd}(M) = n$, we must have $\mathrm{Tor}_{n+1}^R(M, L) = 0$, and $\mathrm{Tor}_n^R(M, R/\mathfrak{m}) \neq 0$. Thus by exactness of the sequence, we must have that $\mathrm{Tor}_n^R(M, N) \neq 0$. □

Remark 5.4.7. As a direct consequence, if M, N are both finitely generated modules over a Noetherian local ring $(R, \mathfrak{m})$ of finite dimension, and $\mathfrak{m}$ is associated to both, then $\mathrm{pd}(M) = \mathrm{pd}(N)$.

Theorem 5.4.8. *Let M be a finitely generated module of finite projective dimension over a Noetherian local ring $(R, \mathfrak{m})$. Then $\mathrm{depth} M \leq \mathrm{depth} R$.*

Proof. Suppose that $d = \min\{\text{depth}R, \text{depth}M\} = \text{depth}R$. Then there exists a sequence $r_1, \ldots, r_d \in \mathfrak{m}$ that is both regular on R and on M. Therefore, we have free resolutions $K_\bullet(r_1, \ldots, r_d; R)$ of $R/(r_1, \ldots, r_n)R$ and $K_\bullet(r_1, \ldots, r_d; M)$ of $M/(r_1, \ldots, r_d)M$. If $n = \text{pd}M$, because $\mathfrak{m}$ is associated to $R/(r_1, \ldots, r_d)R$, then

$$\begin{aligned} H_n(K_\bullet(r_1, \ldots, r_d; M)) &= H_n(M \otimes K_\bullet(r_1, \ldots, r_d; R)) \\ &= \text{Tor}_n^R(M, R/(r_1, \ldots, r_d)R) \\ &\neq 0, \quad \text{by Proposition 5.4.6,} \end{aligned}$$

which forces $n = 0$. Thus M is a projective R-module, necessarily free since R is a local ring. Hence, $\text{depth}M = \text{depth}R$. □

Theorem 5.4.9. *Let M be a finitely generated module of $\text{pd}_R(M) = n < \infty$ over a Noetherian local ring $(R, \mathfrak{m})$, and $r \in \mathfrak{m}$ a non-zero divisor on R. If $K = \ker(R^{\mu(M)} \to M)$ where $\mu(M)$ is the number of generators of M, then K/rK has projective dimension $n - 1$ over R/rR. In particular, if r is a non-zero divisor on M, then $\text{pd}_{R/rR}(M/rM) = n$.*

Proof. First, we note that if r is not a zero divisor on R, then the exact sequence

$$0 \to R \xrightarrow{r} R \to R/rR \to 0$$

shows that $\text{pd}_R(R/rR) = 1$. Tensor the above exact sequence with M, we obtain a complex

$$N_\bullet : \quad 0 \to M \otimes R \xrightarrow{r} M \otimes R \to M \otimes R/rR \to 0.$$

This says that

$$\begin{aligned} \text{Tor}_0^R(M, R/rR) &= M/rM, \\ \text{Tor}_1^R(M, R/rR) &= (0 :_M r) = 0, \\ \text{Tor}_i^R(M, R/rR) &= 0, \forall i \geq 2. \end{aligned}$$

Consider the long exact sequence of $\text{Tor}(*, R/rR)$ applied to the sequence $0 \to K \to F_0 \to M \to 0$:

$$\cdots \to \text{Tor}_{i+1}^R(M, R/rR) \to \text{Tor}_i^R(K, R/rR) \to \text{Tor}_i^R(F_0, R/rR) \to \cdots .$$

$\text{Tor}_i^R(R, *) = 0$ for all $i \geq 1$, and $\text{Tor}_i(M, R/rR) = 0$ for all $i \geq 2$ yield that $\text{Tor}_i(K, R/rR) = 0$ for all $i \geq 1$.

Consider the long exact sequence

$$M_\bullet \quad 0 \to F_n \to F_{n-1} \to \cdots \to F_1 \to K \to 0.$$

The fact that $\mathrm{Tor}_i(K, R/rR) = 0$ for all $i \geq 1$ means the homology of the complex

$$L_\bullet : \quad 0 \to F_n/rF_n \to F_{n-1}/rF_{n-1} \to \cdots \to F_1/rF_1$$

is zero, i.e., $\mathrm{Tor}_i(K, R/rR) = H_i(M_\bullet \otimes R/rR) = 0$. Thus, the complex $L_\bullet$ is exact. Since $L_\bullet$ is a free resolution of K/rK, $\mathrm{pd}_{R/rR}(K/rK) = n - 1$.

If r is a non-zero divisor on M, then $0 \to K/rK \to F_0/rF_0 \to M/rM \to 0$ is exact. Combining this with the exact sequence

$$0 \to F_n/rF_n \to F_{n-1}/rF_{n-1} \to \cdots \to F_1/rF_1 \to K/rK \to 0,$$

we obtain an exact sequence

$$0 \to F_n/rF_n \to F_{n-1}/rF_{n-1} \to \cdots \to F_1/rF_1 \to F_0/rF_0 \to M/rM \to 0.$$

This is a free resolution of M/rM over R/rR, and $\mathrm{pd}_{R/rR}(M/rM) = n$. □

Theorem 5.4.10. *(Auslander-Buchsbaum Formula) Let M be finitely generated module of $\mathrm{pd}_R(M) = n < \infty$ over a Noetherian local ring $(R, \mathfrak{m})$. Then $\mathrm{pd}_R(M) + \mathrm{depth}M = \mathrm{depth}R$.*

Proof. Let $d = \mathrm{depth}R$, then there exist $r_1, \ldots, r_d \in \mathfrak{m}$ that form a regular sequence on R, and $\mathrm{pd}_R(R/(r_1, \ldots, r_d)R) = d$.

If $\mathrm{depth}M = 0$, then $\mathfrak{m}$ is associated to M, and $\mathfrak{m}$ is associated to $R/(r_1, \ldots, r_d)R$. Therefore, by Remark 5.4.7, we have that $\mathrm{pd}_R(M) = d$, and

$$\mathrm{depth}M + \mathrm{pd}_R(M) = \mathrm{depth}R.$$

If $\mathrm{depth}M > 0$, and by Theorem 5.4.8, $\mathrm{depth}R \geq \mathrm{depth}M > 0$. Since $\mathfrak{m} \neq \left(\bigcup_{\mathfrak{p} \in \mathrm{Ass}M} \mathfrak{p}\right) \bigcup \left(\bigcup_{\mathfrak{p} \in \mathrm{Ass}R} \mathfrak{p}\right)$, there must be an element $r \in \mathfrak{m}$ such that r is a non-zero divisor on M and R. Hence

$$\mathrm{depth}(M) = \mathrm{depth}(M/rM) + 1, \quad \mathrm{depth}(R) = \mathrm{depth}(R/rR) + 1.$$

By Theorem 5.4.9, $\mathrm{pd}_{R/rR}(M/rM) = \mathrm{pd}_R(M)$, and by induction,

$$\mathrm{depth}(M) + \mathrm{pd}_R(M) = \mathrm{depth}R.$$

□

5.5 Regular Rings

Theorem 5.5.1. *Let $(R, \mathfrak{m})$ be a Noetherian local ring. Then the following are equivalent:*

1. $\mathrm{pd}_R(M) \leq n$ *for all finitely generated R-modules M;*
2. $\mathrm{pd}_R(R/\mathfrak{m}) \leq n$;
3. *For all finitely generated R-modules M,* $\mathrm{Tor}_i^R(M, R/\mathfrak{m}) = 0$ *for all* $i > n$.

Proof. $(1 \Rightarrow 2)$ Let $M = R/\mathfrak{m}$, we obtain the result.

$(1 \Rightarrow 3)$ Since $\mathrm{pd}_R(M) \leq n$, $0 \to F_n \to \cdots \to F_1 \to F_0 \to M \to 0$ is a free resolution of M of length $\leq n$. Tensor the following complex $F_\bullet$ with $R/\mathfrak{m}$

$$F_\bullet : \quad 0 \to F_n \to \cdots \to F_1 \to F_0 \to 0,$$

we obtain a complex with zero maps $F_i/\mathfrak{m}F_i \to F_{i-1}/\mathfrak{m}F_{i-1}$ for all $i \geq 1$. Thus $\mathrm{Tor}_i^R(M, R/\mathfrak{m}) = F_i/\mathfrak{m}F_i$. Since $\mathrm{pd}_R(M) \leq n$, $F_i = 0$ for all $i > n$, and therefore, $\mathrm{Tor}_i^R(M, R/\mathfrak{m}) = F_i/\mathfrak{m}F_i = 0$ for all $i > n$.

$(3 \Rightarrow 1)$ Let $0 \to F_m \to \cdots \to F_1 \to F_0 \to M \to 0$ be a free resolution of M, and tensor the complex $F_\bullet$ with $R/\mathfrak{m}$,

$$F_\bullet : \quad 0 \to F_m \to \cdots \to F_1 \to F_0 \to 0,$$

we obtain a complex with zero maps $F_i/\mathfrak{m}F_i \to F_{i-1}/\mathfrak{m}F_{i-1}$ for all $i \geq 1$. Thus $\mathrm{Tor}_i^R(M, R/\mathfrak{m}) = F_i/\mathfrak{m}F_i$. Since $\mathrm{Tor}_i^R(M, R/\mathfrak{m}) = F_i/\mathfrak{m}F_i = 0$ for all $i > n$, and by Nakayama's lemma, $F_i = 0$ for all $i > 0$. Hence $m \leq n$. Therefore, $\mathrm{pd}_R(M) \leq n$.

$(3 \Rightarrow 2)$ Because $0 = \mathrm{Tor}_i^R(M, R/\mathfrak{m}) = \mathrm{Tor}_i^R(R/\mathfrak{m}, M)$ for all $i > n$. We must have that $\mathrm{pd}_R(R/\mathfrak{m}) \leq n$. □

The above theorem can be extended to the graded case, and we obtain the following Hilbert Syzygy Theorem.

Theorem 5.5.2. *(Hilbert Syzygy Theorem) Let R be a polynomial ring with n variables over the field. Then every graded R-module has finite projective dimension at most n.*

Definition 5.5.3. A Noetherian local ring $(R, \mathfrak{m})$ is **regular** if $\mathrm{pd}_R(R/\mathfrak{m}) < \infty$. Hence, it is regular if the number of the minimal generators of $\mathfrak{m}$ is the same as the Krull dimension of R.

Theorem 5.5.4. *Let $(R, \mathfrak{m})$ be a regular local ring. Then for any prime ideal $\mathfrak{p}$ in R, $R_\mathfrak{p}$ is regular.*

Proof. Since $\mathrm{pd}_R(R/\mathfrak{m}) = n < \infty$, we must have that $\mathrm{pd}_R(R/\mathfrak{p}) \leq n$. Let

$$F_\bullet : \quad 0 \to F_n \to \cdots \to F_1 \to F_0 \to R/\mathfrak{p} \to 0,$$

be the free resolution of $R/\mathfrak{p}$, and since localization is flat, thus we obtain a free resolution of $(R/\mathfrak{p})_\mathfrak{p} = R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ over $R_\mathfrak{p}$

$$0 \to (F_n)_\mathfrak{p} \to \cdots \to (F_1)_\mathfrak{p} \to (F_0)_\mathfrak{p} \to (R/\mathfrak{p})_\mathfrak{p} = R_\mathfrak{p}/\mathfrak{p}R_p \to 0.$$

Since $\mathfrak{p}R_\mathfrak{p}$ is the only maximal ideal in $R_\mathfrak{p}$, we have $(R_\mathfrak{p}, \mathfrak{p}R_\mathfrak{p})$ is a Noetherian local ring, and $\mathrm{pd}_{R_\mathfrak{p}}(R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}) = n < \infty$. Thus $R_\mathfrak{p}$ is regular. □

Proposition 5.5.5. *Let R be a Noetherian ring. Suppose $\mathfrak{p} = \langle r_1, \ldots, r_d \rangle$ is a prime ideal of $\mathrm{ht}\mathfrak{p} = d$ that lies in Jacobson radical $\mathfrak{J}$ of R. Then $\langle r_1, \ldots, r_{d-1} \rangle$ is a prime ideal.*

Proof. Let $\mathfrak{q} \subset \mathfrak{p}$ be a prime ideal which is minimal over $\langle r_1, \ldots, r_{d-1} \rangle$. Due to the Krull Height Theorem, $\mathfrak{q} \neq \mathfrak{p}$.

If $\mathfrak{q} \neq \langle r_1, \ldots, r_{d-1} \rangle$, then let $a \in \mathfrak{q} \setminus \langle r_1, \ldots, r_{d-1} \rangle$. Since $a \in \mathfrak{q} \subset \mathfrak{p}$, $a = b + a_1 r_d$ for some $b \in \langle r_1, \ldots, r_{d-1} \rangle \subseteq \mathfrak{q}$, and $a_1 \in R$. Thus $a_1 r_d = a - b \in \mathfrak{q}$, since $r_d \notin \mathfrak{q}$, and $\mathfrak{q}$ is a prime, we must have that $a_1 \in \mathfrak{q}$. We repeat this process, write $a_1 = b_1 + a_2 r_d$ for some $b_1 \in \langle r_1, \ldots, r_{d-1} \rangle \subseteq \mathfrak{q}$, and $a_2 \in R$. Similar argument gives that $a_2 \in \mathfrak{q}$. Thus, we have $a = b_n + a_n r_d^n$ for some $b_n \in \langle r_1, \ldots, r_{d-1} \rangle \subseteq \mathfrak{q}$, and $a_n \in R$. We have shown that

$$a \in \bigcap_{n \geq 1} (\langle r_1, \ldots, r_{d-1} \rangle + r_d^n R) = \langle r_1, \ldots, r_{d-1} \rangle,$$

where the last equality is because $r_d \in \mathfrak{J}$, and every ideal is closed for the r_d-adic topology. But this contradicts our assumption. Thus $\mathfrak{q} = \langle r_1, \ldots, r_{d-1} \rangle$ is a prime. □

Here are some characterizations of a Noetherian regular local ring.

Theorem 5.5.6. *Let $(R, \mathfrak{m})$ be Noetherian local ring. Then the following are equivalent:*

1. $\mathrm{pd}_R(R/\mathfrak{m}) = \dim R$;
2. $\mathrm{pd}_R(M) \leq \dim R$ *for any finitely generated R-module M;*

3. $\mathrm{Tor}_i^R(M, R/\mathfrak{m}) = 0$ *for all* $i > \dim R$ *and all finitely generated* R*-modules* M*;*

4. $\mathrm{pd}_R(R/\mathfrak{m}) \leq n$ *for some integer* n*;*

5. $\mathrm{pd}_R(M) \leq n$ *for all finitely generated* R*-modules* M *and for some integer* n*;*

6. *There exists an integer* n *such that* $\mathrm{Tor}_i^R(M, R/\mathfrak{m}) = 0$ *for all* $i > n$ *and all finitely generated* R*-modules* M*;*

7. *Every minimal generating set of* $\mathfrak{m}$ *is a regular sequence;*

8. $\mathfrak{m}$ *is generated by a regular sequence;*

9. *The minimal number of generators of* $\mathfrak{m}$ *equals* $\dim R$*.*

Proof. First, we see that Theorem 5.5.1 shows that

$$1 \Rightarrow 2 \Leftrightarrow 3 \Rightarrow 4 \Leftrightarrow 5 \Leftrightarrow 6;$$

and

$$7 \Rightarrow 8 \Rightarrow \begin{cases} 9, \text{ by Krull Height Theorem,} \\ 1, \text{ by Auslander-Buchsbaum formula.} \end{cases}$$

$(6 \Rightarrow 7)$ Suppose there exists an integer n such that $\mathrm{Tor}_i^R(M, R/\mathfrak{m}) = 0$ for all $i > n$ and all finitely generated R-module M. Then $\mathrm{pd}_R(M) \leq n < \infty$. By Auslander-Buchsbaum formula, $\mathrm{depth}R = \mathrm{depth}R/\mathfrak{m} + \mathrm{pd}_R(R/\mathfrak{m})$.

If $\mathrm{depth}R = 0$, then $\mathrm{pd}_R(R/\mathfrak{m}) = 0$, which means $R/\mathfrak{m}$ is projective. $R/\mathfrak{m}$ must be free R-module, thus R is a field. Thus 7 is true.

If $\mathrm{depth}R = n > 0$, then let $r_1, \ldots, r_n$ be any minimal generating set of $\mathfrak{m}$. We will show this is a regular sequence. Since $\mathrm{depth}R > 0$, at least one of the generators, say r_1 is a non-zero divisor on R, and the $R/(r_1)$-module $\mathfrak{m}/r_1\mathfrak{m}$ is of finite projective dimension. Thus, every minimal generating set of the ideal $\mathfrak{m}/(r_1)$ in $R/(r_1)$ is a regular sequence by induction. Hence, $r_1, \ldots, r_n$ is a regular sequence, and $n \leq \dim R$. But a minimal generating set of $\mathfrak{m}$ has at least $\dim R$ elements, i.e., $n \geq \dim R$. Therefore, $n = \dim R$.

$(9 \Rightarrow 8)$ Assume that $\dim R > 0$, otherwise, $\dim R = 0$, and the hypothesis of 9 means that R is a field, hence 8 is true.

If $\dim R = 1$, then the hypothesis of 9 means that the ideals in R are generated by one element. We claim that the generator r_1 is not a zero-divisor. Otherwise, if r_1 is a zero-divisor, then $r_1^m = 0$ for some $m > 1$,

and the maximal ideal $\mathfrak{m}$ is nilpotent. Hence, R is an Artinian ring with $\dim R = 0$, a contradiction.

If $\dim R > 1$, and suppose the minimal number of generators of $\mathfrak{m}$ is $\dim R$. Let $r_1 \in \mathfrak{m} \backslash \mathfrak{m}^2$ and avoid all the minimal primes. Let $R' = R/\mathfrak{m}$, and $\mathfrak{m}'$ the maximal ideal of R'. We observe the minimal number of generators of $\mathfrak{m}'$ is $\dim R' = \dim R - 1$. By induction, $\mathfrak{m}'$ is generated by a regular sequence $r_2', \ldots, r_d'$, and lift these elements in R, we obtain $r_2, \ldots, r_d \in \mathfrak{m}$. The ideal $\mathfrak{m} = \langle r_1, r_2, \ldots, r_d \rangle$, and $\{r_1, r_2, \ldots, r_d\}$ form an regular sequence by construction. □

Definition 5.5.7. A Noetherian ring R is **regular** if for all prime ideals $\mathfrak{p}$ in R, $R_\mathfrak{p}$ is regular local ring.

Proposition 5.5.8. *Let R be a Noetherian regular ring. Suppose $\mathfrak{p} = \langle r_1, \ldots, r_d \rangle$ is a prime ideal that lies in the Jacobson radical $\mathfrak{J}$ of R, and $\mathrm{ht}\mathfrak{p} = d$. Then $r_1, \ldots, r_d$ is a regular sequence in R, and $\langle r_1, \ldots, r_i \rangle$ is a prime ideal of height i for all $i = 0, \ldots, d$.*

Proof. By Proposition 5.5.5, $\langle r_1, \ldots, r_{d-1} \rangle$ is a prime ideal. By the definition of a regular ring, $R_\mathfrak{p}$ is a regular local ring of dimension d, and it suffices to show that $\langle r_1, \ldots, r_{d-1} \rangle R_\mathfrak{p}$ is of height $d-1$. By Theorem 5.5.6, we see that $r_1, \ldots, r_d$ is a regular sequence in $R_\mathfrak{p}$, therefore the ideal $\langle r_1, \ldots, r_{d-1} \rangle R_\mathfrak{p}$ is of height $d-1$. Hence $\mathrm{ht}\langle r_1, \ldots, r_{d-1} \rangle = d-1$ in R. The remaining result follows by induction. □

5.6 Complex of Ext

Definition 5.6.1. An **injective resolution** of an R-module M is a cocomplex of injective modules

$$I^\bullet : \quad 0 \to I^0 \to I^1 \to \cdots$$

such that

$$0 \to M \to I^0 \to I^1 \to \cdots$$

is exact.

Similar to projective resolution, we have the following proposition

Proposition 5.6.2. *Let $I'^\bullet$ and $I''^\bullet$ be injective resolutions of M' and M'' respectively. Suppose $0 \to M' \to M \to M'' \to 0$ is a short exact sequence.*

Then there exists an injective resolution $I^\bullet$ such that the following diagram commute and the bottom row is a short exact sequence of complexes.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & I'^\bullet & \longrightarrow & I^\bullet & \longrightarrow & I''^\bullet & \longrightarrow & 0 \end{array}$$

Theorem 5.6.3. *(Theorem - Definition) Let M, N be R-modules. Then for all $n \geq 0$, there are R-modules $\mathrm{Ext}^n_R(M,N)$ uniquely defined by the following properties:*

1. $\mathrm{Ext}^0_R(M,N) = \mathrm{Hom}_R(M,N)$.
2. *If $N \to I^\bullet$ is an injective resolution, then*
$$\mathrm{Ext}^n_R(M,N) = H^n(\mathrm{Hom}_R(M, I^\bullet)).$$
3. *If $P_\bullet \to M$ is a projective resolution, then*
$$\mathrm{Ext}^n_R(M,N) = H^n(\mathrm{Hom}_R(P_\bullet, N)).$$
4. *If $0 \to M' \to M \to M'' \to 0$ is an exact sequence of R-modules, then there is a long exact sequence*
$$\begin{aligned} &0 \to \mathrm{Hom}_R(M'',N) \to \mathrm{Hom}_R(M,N) \to \mathrm{Hom}_R(M',N) \to \cdots \to \\ &\mathrm{Ext}^{n-1}_R(M',N) \to \mathrm{Ext}^n_R(M'',N) \to \mathrm{Ext}^n_R(M,N) \to \cdots . \end{aligned}$$
5. *If $0 \to N' \to N \to N'' \to 0$ is an exact sequence of R-modules, then there is a long exact sequence*
$$\begin{aligned} &0 \to \mathrm{Hom}_R(M,N') \to \mathrm{Hom}_R(M,N) \to \mathrm{Hom}_R(M,N'') \to \cdots \to \\ &\mathrm{Ext}^{n-1}_R(M,N'') \to \mathrm{Ext}^n_R(M,N') \to \mathrm{Ext}^n_R(M,N) \to \cdots . \end{aligned}$$

Lemma 5.6.4. *Let R be a Noetherian ring, M a finitely generated R-module, and N an R-module, then*

$$\mathrm{Ass}_R(\mathrm{Hom}_R(M,N)) = \mathrm{Supp}_R(M) \cap \mathrm{Ass}_R(N).$$

Proof. ($\subseteq$) Let $\mathfrak{p} \in \mathrm{Ass}_R(\mathrm{Hom}_R(M,N))$, then $\mathfrak{p}R_\mathfrak{p} \in \mathrm{Ass}_{R_\mathfrak{p}}(\mathrm{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p}))$. Thus, $\mathrm{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p}) \neq 0$, and $M_\mathfrak{p} \neq 0$. Hence, $\mathfrak{p} \in \mathrm{Supp}_R(M)$, and there is an injection

$$R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} \hookrightarrow \mathrm{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p}).$$

By the adjointness property of Hom and tensor product, i.e., $\mathrm{Hom}(A \otimes B, C) = \mathrm{Hom}(A, \mathrm{Hom}(B, C))$,

$$\mathrm{Hom}_{R_\mathfrak{p}}(R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} \otimes_{R_\mathfrak{p}} M_\mathfrak{p}, N_\mathfrak{p}) \cong \mathrm{Hom}_{R_\mathfrak{p}}(R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}, \mathrm{Hom}_{R/\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p})) \neq 0.$$

Since $M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p} = R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} \otimes_{R_\mathfrak{p}} M_\mathfrak{p}$ is a vector space over $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$, there is a non-zero map $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} \to M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p}$. Thus, $\mathrm{Hom}_{R_\mathfrak{p}}(R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}, N_\mathfrak{p}) \neq 0$, and there is an injective $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} \hookrightarrow N_\mathfrak{p}$. Therefore, $\mathfrak{p}R_\mathfrak{p} \in \mathrm{Ass}_{R_\mathfrak{p}}(N_\mathfrak{p})$, and $\mathfrak{p} \in \mathrm{Ass}_R(N)$.

Therefore, we have shown that $\mathfrak{p} \in \mathrm{Supp}_R(M) \cap \mathrm{Ass}_R(N)$.

($\supseteq$) On the other hand, if $\mathfrak{p} \in \mathrm{Supp}_R(M) \cap \mathrm{Ass}_R(N)$, then $M_\mathfrak{p} \neq 0$, and there is an injective $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} \hookrightarrow N_\mathfrak{p}$. By Nakayama's lemma,

$$M_\mathfrak{p} \otimes_{R_\mathfrak{p}} R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} \cong M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p} \neq 0.$$

Since $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ is a field, and $M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p}$ is a vector space over this field, there is a surjection,

$$M_\mathfrak{p} \otimes_{R_\mathfrak{p}} R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} \twoheadrightarrow R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} \neq 0,$$

which gives a non-zero map $\mathrm{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p} \otimes_{R_\mathfrak{p}} R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}, N_\mathfrak{p})$. Thus,

$$\mathrm{Hom}_{R_\mathfrak{p}}(R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}, \mathrm{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p})) \cong \mathrm{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p} \otimes_{R_\mathfrak{p}} R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}, N_\mathfrak{p})) \neq 0$$

Thus, $\mathfrak{p}R_\mathfrak{p} \in \mathrm{Ass}_{R_\mathfrak{p}}(\mathrm{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p}))$, and $\mathfrak{p} \in \mathrm{Ass}_R(\mathrm{Hom}_R(M, N))$. □

Theorem 5.6.5. *Let R be a Noetherian ring, M a finitely generated R-module, and I an ideal in R such that $IM \neq M$. Let $\mathbb{V}(I)$ be the set of prime ideals in R such that $\mathfrak{p} \supseteq I$. Then the following are equivalent:*

1. $\mathrm{Ext}^i_R(N, M) = 0$ *for all $i < n$, and for all finitely generated R-module N such that* $\mathrm{Supp}_R(N) \subseteq \mathbb{V}(I)$.
2. $\mathrm{Ext}^i_R(N, M) = 0$ *for all $i < n$, and for all finitely generated R-module N such that* $\mathrm{Supp}_R(N) = \mathbb{V}(I)$.
3. $\mathrm{Ext}^i_R(R/I, M) = 0$ *for all $i < n$.*
4. *There exist $r_1, \ldots, r_n \in I$ which form an M-sequence.*

Proof. We see that $1 \Rightarrow 2 \Rightarrow 3$ are clear.

($3 \Rightarrow 4$) We prove by induction on n. If $n = 1$, then the hypothesis means

$$\mathrm{Hom}_R(R/I, M) = 0,$$

and this implies that if $\mathfrak{p}$ a prime ideal in R,

$$\mathfrak{p} \in \mathrm{Ass}_R(M) \Rightarrow \mathfrak{p} \notin \mathbb{V}(I), \quad \text{and} \quad I \not\subseteq \cup_{\mathfrak{p}\in \mathrm{Ass}_R(M)}\mathfrak{p}.$$

Thus, there exists $r_1 \in I$ such that r_1 is a non-zero divisor on M.

If $n > 1$, and $\mathrm{Ext}^i_R(R/I, M) = 0$ for all $i < n-1$. By the above reasoning, there exists $r_1 \in I$ which is a non-zero divisor on M, and

$$0 \to M \xrightarrow{r_1} M \to M/r_1M \to 0.$$

The long exact sequence

$$\cdots \to \mathrm{Ext}^i_R(R/I, M/r_1M) \to \mathrm{Ext}^{i+1}_R(R/I, M) \to \mathrm{Ext}^{i+1}_R(R/I, M) \to \cdots$$

shows us that $\mathrm{Ext}^i_R(R/I, M/r_1M) = 0$ for all $i < n-1$, and by induction hypothesis there is an M/r_1M-sequence $r_2, \ldots, r_n$. Thus, $r_1, \ldots, r_n$ is an M-sequence.

$(4 \Rightarrow 1)$ Suppose $r_1, \ldots, r_n$ is an M-sequence in I. Let N be a finitely generated R-module such that $\mathrm{Supp}_R(N) \subseteq \mathbb{V}(I)$. Let $J = \mathrm{Ann}_R(N)$. $\mathbb{V}(\mathrm{Ann}_R(N)) = \mathrm{Supp}(N)$. Thus $\mathbb{V}(J) \subseteq \mathbb{V}(I)$, and therefore, $\sqrt{I} \subseteq \sqrt{J}$. Hence there exists a t such that $I^t \subseteq J$. Let $f \in \mathrm{Hom}_R(N, M)$, $x \in N$. Then $r_1 \in I$ yields $r_1^t \in J = \mathrm{Ann}_R(N)$, and $r_1^t f(x) = f(r_1^t x) = f(0) = 0$. Since r_1^t is a non-zero divisor on M, $f(x) = 0$, and so $\mathrm{Hom}_R(N, M) = 0$.

Consider the exact sequence

$$0 \to M \xrightarrow{r_1^t} M \to M/r_1^tM \to 0.$$

Since $r_2, \ldots, r_n$ is an M/r_1M-sequence, and by induction hypothesis we have that $\mathrm{Ext}^i_R(N, M/r_1^tM) = 0$ for all $i < n-1$, hence the long exact sequence

$$\mathrm{Ext}^{i-1}_R(N, M/r_1^tM) \to \mathrm{Ext}^i_R(N, M) \xrightarrow{r_1^t} \mathrm{Ext}^i_R(N, M) \to \mathrm{Ext}^i_R(N, M/r_1^tM)$$

implies $\mathrm{Ext}^i_R(N, M) \cong \mathrm{Ext}^i_R(N, M)$ by multiplying r_1^t for all $i < n-1$, and is injection for $i = n-1$, hence this is a zero map for all $i < n$. Thus $\mathrm{Ext}^i_R(N, M) = 0$ for all $0 \le i < n$. □

Definition 5.6.6. An R-module M has **finite injective dimension** if there exists an injective resolution

$$0 \to M \to I^0 \to I^1 \to \cdots \to I^{n-1} \to I^n \to 0$$

of M. The least integer of n is the **injective dimension of** M, denoted by $\mathrm{injdim}M$.

Proposition 5.6.7. *Let R be a Noetherian ring, M a finitely generated R-module, and $I \subset R$ is an ideal such that $IM \neq M$. Then*

$$\operatorname{depth}_I(M) = \min\{\ell \mid \operatorname{Ext}^\ell_R(R/I, M) \neq 0\}.$$

In particular, the length of a maximal M-regular sequence in I does not depend on the sequence.

Proof. Let $d = \operatorname{depth}_I(M)$.

If $d = 0$, then $I \subseteq \mathfrak{p}$ where $\mathfrak{p} \in \operatorname{Ass}(M)$, and $R/\mathfrak{p}$ embeds in M. Thus $0 \neq \operatorname{Hom}_R(R/I, R/\mathfrak{p}) \subseteq \operatorname{Hom}_R(R/I, M) = \operatorname{Ext}^0_R(R/I, M)$, and the equality holds.

If $d > 0$. Let $a \in I$ be a non-zero divisor on M, then the exact sequence

$$0 \to M \xrightarrow{a} M \longrightarrow M/aM \longrightarrow 0$$

gives a long exact sequence

$$\begin{aligned} \cdots \to \quad & \operatorname{Ext}^n_R(R/I, M) \to \operatorname{Ext}^n_R(R/I, M) \to \operatorname{Ext}^n_R(R/I, M/aM) \\ \to \quad & \operatorname{Ext}^{n+1}_R(R/I, M) \to \operatorname{Ext}^{n+1}_R(R/I, M) \to \cdots \end{aligned}$$

Since $a \in I = \operatorname{Ann}(R/I)$, multiplication by a is the zero map, that is $\operatorname{Ext}^n_R(R/I, M) \to \operatorname{Ext}^n_R(R/I, M)$ has image zero for all $n \geq 1$. Therefore,

$$0 \to \operatorname{Ext}^n_R(R/I, M) \to \operatorname{Ext}^n_R(R/I, M/aM) \to \operatorname{Ext}^{n+1}_R(R/I, M) \to 0, \quad (5.1)$$

is exact sequence for all $n \geq 1$. The induction hypothesis $\operatorname{depth}_I(M/aM) = d - 1$ implies $\operatorname{Ext}^d_R(R/I, M/aM) = 0$ for all $n = 0, \ldots, d-1$, hence we have

$$0 \to \operatorname{Ext}^n_R(R/I, M) \to 0 \to \operatorname{Ext}^{n+1}_R(R/I, M) \to 0, \quad n = 0, \ldots, d-1,$$

hence $\operatorname{Ext}^n_R(R/I, M) = 0$ for all $n = 0, \ldots, d$. Let $n = d$, then the exact sequence (5.1) becomes

$$0 \to \operatorname{Ext}^d_R(R/I, M) = 0 \to \operatorname{Ext}^d_R(R/I, M/aM) \neq 0 \to \operatorname{Ext}^{d+1}_R(R/I, M) \to 0,$$

which implies $0 \neq \operatorname{Ext}^d_R(R/I, M/aM) \cong \operatorname{Ext}^{d+1}_R(R/I, M)$. Hence,

$$d = \operatorname{depth}_I M = \min\{\ell \mid \operatorname{Ext}^\ell_R(R/I, M) \neq 0\}.$$

□

Corollary 5.6.8. *If $0 \to M_1 \to M_2 \to M_3 \to 0$ is a short exact sequence of finitely generated R-modules. Set $d_i = \operatorname{depth}_I(M_i)$. Then*

1. $d_1 \geq \min\{d_2, d_3 + 1\}$.
2. $d_2 \geq \min\{d_1, d_3\}$.
3. $d_3 \geq \min\{d_1 - 1, d_2\}$.

Proof. Since the short exact sequence gives a long exact sequence

$$\mathrm{Ext}^i_R(R/I, M_3) \to \mathrm{Ext}^{i+1}_R(R/I, M_1) \to \mathrm{Ext}^{i+1}_R(R/I, M_2) \to \mathrm{Ext}^{i+1}_R(R/I, M_3)$$

The results follows by Proposition 5.6.7. □

Definition 5.6.9. Let R be a Noetherian ring, M a finitely generated R-module, then the **grade** of M is

$$\begin{aligned} \mathrm{grade}(M) &= \inf\{\ell \mid \mathrm{Ext}^\ell_R(M, R) \neq 0\} \\ &= \mathrm{depth}_{\mathrm{Ann}(M)}(R) \\ &= \inf\{\mathrm{depth}(R_\mathfrak{p}) \mid \mathfrak{p} \in \mathrm{Supp}(M)\}. \end{aligned}$$

Theorem 5.6.10. *Let R be a Noetherian ring, M, N finitely generated R-modules where* $\mathrm{grade}(M) = m$, *and* $\mathrm{pdim}_R(N) = n$. *Then*

$$\mathrm{Ext}^i_R(M, N) = 0, \quad \forall\, i < m - n.$$

Proof. We will prove the claim by induction on n.

If $n = 0$, then N is projective, and hence, it is a direct summand of a free R-module. Thus $N \oplus T = R^t$ for some R-module T and some $t \in \mathbb{Z}$. By definition, $\mathrm{grade}(M) = m$ means $\mathrm{Ext}^i_R(M, R) = 0$ for all $i < m$. Thus $\mathrm{Ext}^i_R(M, R^t) = 0$ for all $i < m$, and $\mathrm{Ext}^i_R(M, N) = 0$ for all $i < m$.

Suppose $n > 0$, and let $0 \to N' \to F \to N \to 0$ be a short exact sequence where F is a finitely generated free R-module, i.e. $\mathrm{Ext}^i_R(M, F) = 0$ for all $i < m$. Since $\mathrm{pdim}(N') = n-1$, by the induction hypothesis $\mathrm{Ext}^i_R(M, N') = 0$ for all $i < m - (n-1)$, thus the long exact sequence

$$\mathrm{Ext}^i_R(M, F) \to \mathrm{Ext}^i_R(M, N) \to \mathrm{Ext}^{i+1}_R(M, N')$$

yields $\mathrm{Ext}^i_R(M, N) = 0$ for $i < \min\{m,\, m - (n-1) - 1\} = m - n$.

Therefore, we have shown that

$$\mathrm{Ext}^i_R(M, N) = 0, \quad \forall\, i < m - n.$$

□

Theorem 5.6.11. *Let $(R, \mathfrak{m})$ be a local ring, and M, N finitely generated R-modules with* $\operatorname{depth}(M) = m$, *and* $\dim(N) = n$. *Then*

$$\operatorname{Ext}^i_R(N, M) = 0, \quad \forall\, i < m - n.$$

Proof. We will prove the claim by induction on n.

If $n = 0$, then $\operatorname{Supp}_R(N) = \{\mathfrak{m}\}$. By Theorem 5.6.5, $\operatorname{depth}(M) = m$ is equivalent to $\operatorname{Ext}^i_R(N, M) = 0$ for all $i < m$.

Now, let $n > 0$. Then N has a filtration:

$$N = N_1 \supseteq N_2 \supseteq \cdots \supseteq N_t = 0,\ N_i/N_{i+1} = R/\mathfrak{p}_i,\ i = 1, \ldots, t-1.$$

To show the claim, it is equivalent to show $\operatorname{Ext}^i_R(R/\mathfrak{p}, M) = 0$ for all $i < m - n$. By induction, we only need to show $\operatorname{Ext}^i_R(R/\mathfrak{p}, M) = 0$ for all $i < m - n$ with $\dim R/\mathfrak{p} = n$. Let $r \in \mathfrak{m} \setminus \mathfrak{p}$, then the following sequence is exact

$$0 \to R/\mathfrak{p} \xrightarrow{\ r\ } R/\mathfrak{p} \to R/(\mathfrak{p} + rR) \to 0,$$

$\dim R/(\mathfrak{p} + rR) = n - 1$, and by the induction hypothesis $\operatorname{Ext}^i_R(R/(\mathfrak{p} + rR), M) = 0$ for all $i < m - (n-1)$. Hence the long exact sequence on Ext gives us

$$\operatorname{Ext}^i_R(R/\mathfrak{p}, M) \cong (rR) \cdot \operatorname{Ext}^i_R(R/\mathfrak{p}, M), \quad \forall i < m - n.$$

Since $r \in \mathfrak{m}$, by Nakayama's Theorem, $\operatorname{Ext}^i_R(R/\mathfrak{p}, M) = 0$ for all $i < m - n$. □

Corollary 5.6.12. *Let R be a local ring, $0 \neq N \subseteq M$ finitely generated R-modules. Then*

$$\dim N \geq \operatorname{depth}(M).$$

In particular, $\dim(M) \geq \operatorname{depth}(M)$.

Proof. Since $N \subseteq M$, then there exists a non-zero map $N \to M$, hence $\operatorname{Hom}_R(N, M) \neq 0$. Thus, $\operatorname{Ext}^0_R(N, M) \neq 0$. By Theorem 5.6.11, $m - n \leq 0$. Therefore, $\dim(N) = n \geq m = \operatorname{depth}(M)$ □

As a direct consequence, if M is a finitely generated R-module over a Noetherian local ring $(R, \mathfrak{m})$, then for any ideal I in R, $\operatorname{injdim}_R(M) \geq \operatorname{depth}_I(M)$.

Proposition 5.6.13. *If M is a finitely generated R-module over a Noetherian local ring $(R, \mathfrak{m})$, then* $\operatorname{depth} R \leq \operatorname{injdim}_R(M)$.

Proof. Let $r_1, \ldots, r_d \in \mathfrak{m}$ be a maximal regular sequence on R. Then

$$\begin{aligned} \mathrm{Ext}^d_R(R/(r_1,\ldots,r_d), M) &= H^d(\mathrm{Hom}_R(K_\bullet(r_1,\ldots,r_d;R), M) \\ &\cong M/(r_1,\ldots,r_d)M \neq 0 \end{aligned}$$

so $\mathrm{injdim}_R(M) \geq d = \mathrm{depth}R$. □

Lemma 5.6.14. *Let $(R,\mathfrak{m})$ be a Noetherian local ring, N a finitely generated module, and $n \in \mathbb{N}$. Then $\mathrm{injdim}_R(N) \leq n$ if and only if $\mathrm{Ext}^i_R(M,N) = 0$ for all $i > n$ and for all finitely generated R-modules M.*

Proof. ($\Rightarrow$) It is clear, and we only need to show the other direction.

($\Leftarrow$) Let $0 \to N \to I^0 \to I^1 \cdots \to I^{n-1} \to J \to 0$ be exact with all I^i injective. We will show that J is also injective. First, we observe that $\mathrm{Ext}^i_R(M,J) \cong \mathrm{Ext}^{i+n}_R(M,N)$ for all $i \geq 1$. By the given condition, we have that $\mathrm{Ext}^i_R(M,J) = 0$ for all $i \geq 1$ for all finitely generated R-module M. Hence, for any exact sequence $0 \to M' \to M \to M'' \to 0$, we have the exact long sequence:

$$0 \to \mathrm{Hom}_R(M'',J) \to \mathrm{Hom}_R(M,J) \to \mathrm{Hom}_R(M',J) \to \mathrm{Ext}^1_R(M'',J) = 0.$$

This means that $\mathrm{Hom}_R(*,J)$ is exact on finitely generated modules, then by Proposition 5.6.3, the exactness of $\mathrm{Hom}_R(*,J)$ is equivalent to say that J is an injective module. Therefore, we have at least one injective resolution of N of length n. Thus $\mathrm{injdim}N \leq n$. □

Theorem 5.6.15. *Let $(R,\mathfrak{m})$ be a Noetherian local ring, N a finitely generated R-module. Then*

$$\mathrm{injdim}_R(N) = \sup\{\ell \mid \mathrm{Ext}^\ell_R(R/\mathfrak{m}, N) \neq 0\}.$$

Proof. Without loss of generality, let $\sup\{\ell \mid \mathrm{Ext}^\ell_R(R/\mathfrak{m},N) \neq 0\} = n < \infty$, where $n \in \mathbb{N}$.

First, it is clear that $\mathrm{injdim}_R(N) \geq n$. We will show that $\mathrm{injdim}_R(N) \leq n$, and by Lemma 5.6.14, we only need to show $\mathrm{Ext}^i_R(M,N) = 0$ for all $i > n$ and for all finitely generated R-module M.

If $M = R/\mathfrak{m}$, we are done by hypothesis.

If M is of finite length, we will prove the claim by induction on the length of M. For

$$0 \to R/\mathfrak{m} \to M \to M' \to 0$$

gives the following long exact sequence on Ext, where $\mathrm{Ext}^{\ell}_R(R/\mathfrak{m}, N) = \mathrm{Ext}^i_R(M', N) = 0$ for all $i > n$ by the induction hypothesis.

$$\cdots \to \mathrm{Ext}^i_R(M', N) = 0 \to \mathrm{Ext}^i_R(M, N) \to \mathrm{Ext}^i_R(R/\mathfrak{m}, N) = 0 \to$$
$$\mathrm{Ext}^{i+1}_R(M', N) = 0 \to \mathrm{Ext}^{i+1}_R(M, N) \to \mathrm{Ext}^{i+1}_R(R/\mathfrak{m}, N) = 0 \to \cdots$$

Thus,

$$\mathrm{Ext}^i_R(M, N) = 0, \quad \forall i > n.$$

If M is not of finite length, then we take a prime filtration, $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$, where $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ for some prime ideal $\mathfrak{p}_i$. We will prove by induction on the length of the filtration. If we can show that for any prime ideal $\mathfrak{p}$ in R, $\mathrm{Ext}^i_R(R/\mathfrak{p}, N) = 0$, then the exact sequence

$$0 \to M_{i-1} \to M_i \to R/\mathfrak{p} \to 0$$

will give a long exact sequence of Ext, and by performing the argument similar to the above, we can obtain $\mathrm{Ext}^i_R(M_i, N) = 0$ for all $i > n$.

Therefore, we will show that any prime ideal $\mathfrak{p}$ in R, $\mathrm{Ext}^i_R(R/\mathfrak{p}, N) = 0$. Let $a \in \mathfrak{m} \setminus \mathfrak{p}$, then the short exact sequence

$$0 \to R/\mathfrak{p} \xrightarrow{\ a\ } R/\mathfrak{p} \to L \to 0$$

gives the following long exact sequence on Ext, and $\mathrm{Ext}^i_R(L, N) = 0$ for $i > n$ by the induction hypothesis.

$$0 \to \mathrm{Ext}^i_R(R/\mathfrak{p}, N) \xrightarrow{\ a\ } \mathrm{Ext}^i_R(R/\mathfrak{p}, N) \to 0 \quad \forall\, i > n.$$

Therefore,

$$\mathrm{Ext}^i_R(R/\mathfrak{p}, N) \cong a\,\mathrm{Ext}^i_R(R/\mathfrak{p}, N), \quad \forall i > n,$$

and by Nakayama's lemma,

$$\mathrm{Ext}^i_R(R/\mathfrak{p}, N) = 0, \quad \forall i > n.$$

Hence, we have proved that $\mathrm{injdim}_R(N) \leq n$. □

Theorem 5.6.16. *Let $(R, \mathfrak{m})$ be a Noetherian local ring, N a finitely generated R-module of finite injective dimension. Then* $\mathrm{injdim}_R(N) = \mathrm{depth}R$.

Proof. First, we recall that $0 \leq \mathrm{depth}R \leq \mathrm{injdim}_R(N)$, and we only need to show that $\mathrm{depth}R \geq \mathrm{injdim}_R(N)$.

If $\mathrm{injdim}_R(N) = 0$, then $\mathrm{depth}R = 0$.

If $0 < \mathrm{injdim}_R(N) = n < \infty$. Suppose $\mathrm{depth}R < n$, then let $r_1, \ldots, r_t \in \mathfrak{m}$ be a maximal regular sequence in R where $t < n$. Then the exact sequence

$$0 \to R/\mathfrak{m} \to R/(r_1, \ldots, r_t) \to R/I \to 0, \text{ for some ideal } I \text{ in } R,$$

gives a long exact sequence

$$\mathrm{Ext}^n_R(R/I, N) \to \mathrm{Ext}^n_R(R/(r_1, \ldots, r_t), N) \to \mathrm{Ext}^n_R(R/\mathfrak{m}, N) \to 0,$$

since $\mathrm{Ext}^{n+1}_R(R/I, N) = 0$ by Lemma 5.6.14, and $\mathrm{Ext}^n_R(R/\mathfrak{m}, N) \neq 0$ by Theorem 5.6.15. But this contradicts the fact that $\mathrm{Ext}^n_R(R/(r_1, \ldots, r_t), N) = 0$ for a maximal regular sequence $r_1, \ldots, r_t$ with $t < n$. Thus, $\mathrm{depth}R \geq n$. □

Below is a result concerning the behavior of depth under flat change of rings.

Proposition 5.6.17. *Let $f : (R, \mathfrak{m}, \mathbb{K}) \to (S, \mathfrak{n}, \mathbb{L})$ be a local homomorphism of local rings. If M is finitely generated R-module, and N is a finitely generated S-module that is flat over R, then we have:*

$$\dim_{\mathbb{L}}(\mathrm{Hom}_S(\mathbb{L}, M \otimes N)) = \dim_{\mathbb{K}} \mathrm{Hom}_R(\mathbb{K}, M) \cdot \dim_{\mathbb{L}}(\mathrm{Hom}_S(\mathbb{L}, N/\mathfrak{m}N)).$$

$$\mathrm{depth}_S(M \otimes_R N) = \mathrm{depth}_R M + \mathrm{depth}_S N/\mathfrak{m}N.$$

In particular, if f is a flat map, then

$$\mathrm{depth}S = \mathrm{depth}R + \mathrm{depth}S/\mathfrak{m}S.$$

Proof. To prove the first claim, we check

$$\begin{aligned}
\mathrm{Hom}_S(\mathbb{L}, \mathrm{Hom}_S(S/\mathfrak{m}S, M \otimes N)) &\cong \mathrm{Hom}_S(\mathbb{L} \otimes S/\mathfrak{m}S, M \otimes N) \\
&\cong \mathrm{Hom}_S(\mathbb{L}, M \otimes N); \text{ and} \\
\mathrm{Hom}_S(S/\mathfrak{m}S, M \otimes N) &\cong \mathrm{Hom}_S(\mathbb{K} \otimes S, M \otimes N) \\
&\cong \mathrm{Hom}_R(\mathbb{K}, M) \otimes N \quad \text{since } N \text{ is flat} \\
&\cong (N/\mathfrak{m}N)^{\dim_{\mathbb{K}} \mathrm{Hom}_R(\mathbb{K}, M)}.
\end{aligned}$$

To see the second equality, we note that if $\mathrm{depth}_R M = \mathrm{depth}_S N/\mathfrak{m}N = 0$, then by definition of depth $\mathrm{depth}M = \min\{i : \mathrm{Ext}^i(\mathbb{K}, M) \neq 0\}$ and the first equality,

$$\mathrm{Hom}_R(\mathbb{K}, M) \neq 0, \ \mathrm{Hom}_{\mathbb{L}}(\mathbb{L}, N/\mathfrak{m}N) \neq 0, \ \mathrm{Hom}_S(\mathbb{L}, M \otimes N) \neq 0.$$

Hence, by definition of depth, we have that $\mathrm{depth}_S(M \otimes N) = 0$.

If $\mathbf{c}$ is a maximal M-sequence of length s, and $\mathbf{b}$ is a maximal $N/\mathfrak{m}N$-sequence of length t, then

$$\mathrm{Ext}^s_R(\mathbb{K}, M) \cong \mathrm{Hom}_R(\mathbb{K}, M/\mathbf{c}M) \neq 0,$$

$$\mathrm{Ext}^t_S(\mathbb{L}, N/\mathfrak{m}N) \cong \mathrm{Hom}_S(\mathbb{L}, (N/\mathbf{b}N)/\mathfrak{m}(N/\mathbf{b}N)) \neq 0.$$

Both $M/\mathbf{c}M$ and $(N/\mathbf{b}N)/\mathfrak{m}(N/\mathbf{b}N)$ have depth zero, and $N/\mathbf{b}N$ is R-flat, therefore the depth of $(M/\mathbf{c}M) \otimes (N/\mathbf{b}N)$ is zero. Hence, we have

$$\mathrm{Hom}_S(\mathbb{L}, (M/\mathbf{c}M) \otimes (N/\mathbf{b}N)) \neq 0.$$

And

$$(M/\mathbf{c}M) \otimes (N/\mathbf{b}N) \cong (M \otimes N)/(f(\mathbf{c}) \cup \mathbf{b})(M \otimes N).$$

Thus,

$$\mathrm{Ext}^{s+t}_S(\mathbb{L}, M \otimes N) \cong \mathrm{Hom}_S(\mathbb{L}, (M \otimes N)/(f(\mathbf{c}) \cup \mathbf{b})(M \otimes N)) \neq 0.$$

Since

$$(M \otimes N)/\mathbf{c}(M \otimes N) \cong (M/\mathbf{c}M) \otimes N$$

we have that $\mathbf{b}$ is a $(M \otimes N)/\mathbf{c}(M \otimes N)$-regular sequence. Thus, $f(\mathbf{c}), \mathbf{b}$ is a regular sequence on $M \otimes N$,

$$\mathrm{Ext}^k_S(\mathbb{L}, M \otimes N) = 0, \ \forall\, k < s + t.$$

Thus, again by definition of depth, we have $\mathrm{depth}_S(M \otimes N) = s + t$, hence we proved the second claim. □

5.7 Exactness Criteria for Complexes

Definition 5.7.1. : Let R be a ring, $A = (a_{ij})$ an $m \times n$ matrix with $a_{ij} \in R$, and $I_r(A)$ the ideal in R generated by the determinants of all the $r \times r$ submatrices of A where $r \in \mathbb{Z}_{>0}$. Let $f : R^n \to R^m$ be a module homomorphism, and M an R-module. The **rank of f on M**, denoted by $\mathrm{rank}(f, M)$, is such that

$$\mathrm{rank}(f, M) = \max\{r \mid I_r(f) \not\subseteq \mathrm{Ann}(M)\}.$$

Set

$$I(f, M) = I_r(f, M), \ \text{ where } r = \mathrm{rank}(f, M).$$

Note that if $M = R$, we write $I(f) = I(f, R)$.

We observe that if $N = \min\{m, n\}$, then

$$I_0(A) = A \supseteq I_1(A) \supseteq \cdots \supseteq I_N(A) = \cdots = I_i(A) = \cdots, \quad \forall i \geq N+1,$$

and

$$0 \subseteq (0 :_M I_1(A)) \subseteq (0 :_M I_2(A)) \subseteq \cdots \subseteq (0 :_M I_N(A))$$

are submodules of M.

Theorem 5.7.2. *(McCoy's Theorem) Let R be a commutative ring, M an R-module, and $A = (a_{ij})$ an $m \times n$ matrix with $a_{ij} \in R$. Then the system of equations:*

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + \cdots + a_{2n}x_n = 0 \\ \qquad\vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = 0 \end{cases}$$

has no non-zero solution $(x_1, \ldots, x_n) \in M^n$ if and only if

$$\sup\{\ell \mid (0 :_M I_\ell(A)) = 0\} = n.$$

Proof. Let $d = \sup\{\ell \mid (0 :_M I_\ell(A)) = 0\}$.

If $m < n$, we can always add zero equations, hence, without loss of generality, we assume that $m \geq n$, and $d \leq n$.

First, we will show if the system has no non-zero solution then $\sup\{\ell \mid (0 :_M I_\ell(A)) = 0\} = n$. Suppose $d < n$. Then $(0 :_M I_d(A)) = 0 \subsetneq (0 :_M I_{d+1}(A))$, which shows there exists $m \in M$ such that $mI_{d+1}(A) = 0$. Thus, there exists a $d \times d$ submatrix B such that $m \det B \neq 0$. Without loss of generality, we assume that B is the matrix obtained by taking the first d rows and d columns. Let C be a $(d+1) \times (d+1)$ submatrix of A by taking the first $d+1$ rows and $d+1$ columns. Note $m \det C = 0$. Let $x_j = y_j m$ for $j \leq d+1$, and $x_j = 0$ for $j > d+1$, where y_j is the determinant of the submatrix of C obtained by removing the j-th row and the last columns. Then we see that $(x_1, \ldots, x_n)$ is a solution, because $y_1, \ldots, y_{d+1}$ gives the expansion of $\det C$ along the last column of C, and $m \det C = 0$. Moreover, this is a non-zero solution since $x_{d+1} = y_{d+1}m = m \det B \neq 0$, contradicting the given condition.

Now, we will show the other implication. Suppose $(x_1, \ldots, x_n) \in M^n$ is a non-zero solution, and let B be an $n \times n$ submatrix of A. Then $B \cdot (x_1, \ldots, x_n)^T = \mathbf{0}$, and we know that $\det(B) I_{n\times n} = (\mathrm{adj}B)B$, where $\mathrm{adj}B$ is the adjoint matrix of B. Thus, $0 \neq (0 :_M \det(B))$. Since $\det(B) \in I_n(A)$,

we must have $(0 :_M I_n(A)) \neq 0$. Thus, $d = \sup\{\ell \mid (0 :_M I_\ell(A)) = 0\} > n$ which is absurd.

Hence, to have no non-zero solution $(x_1, \ldots, x_n) \in M^n$ if and only if $d = \sup\{\ell \mid (0 :_M I_\ell(A)) = 0\} = n$. □

The McCoy Theorem states that if $\phi : M \to N$ is a morphism between two finite free R-modules of rank m and n respectively, then ϕ is injective if and only if $(0 :_R \det_m(\phi)) = 0$. Moreover, when this is the case, we have that $m \leq n$.

Theorem 5.7.3. *(Acyclicity Lemma) Let R be Noetherian ring, I an ideal in R. If*

$$M_\bullet : \quad 0 \to M_n \xrightarrow{d_n} M_{n-1} \xrightarrow{d_{n-1}} \cdots \to M_2 \xrightarrow{d_2} M_1 \xrightarrow{d_1} M_0$$

is a complex of R-modules, such that for all $i \geq 1$,

1. $\operatorname{depth}_I(M_i) \geq i$;
2. $H_i(M_\bullet) = 0$ *or* $\operatorname{depth}_I(H_i(M_\bullet)) = 0$.

Then $M_\bullet$ is exact.

Proof. By descending induction on $i \geq 1$ starting with $i = n$, we will show

$$H_i(M_\bullet) = 0, \quad \text{and} \quad \operatorname{depth}_I(\operatorname{im} d_i) \geq i.$$

First, we note that d_n is injective, otherwise, $H_n(M_\bullet) = \ker(d_n) \neq 0$ contradicts the condition 2. Thus, $\operatorname{im} d_n \cong M_n$ and has I-depth at least $n \geq 1$.

If $i < n$, we have complex

$$0 \to \operatorname{im} d_{i+1} \to M_i \to \cdots \to M_1$$

which can be split into two short exact sequences:

$$0 \to \operatorname{im} d_{i+1} \to M_i \to M_i/\operatorname{im} d_{i+1} \to 0,$$

$$0 \to H_i(M_\bullet) \to M_i/\operatorname{im} d_{i+1} \xrightarrow{d_i} \operatorname{im} d_i \to 0.$$

By the induction hypothesis, I-depth of $\operatorname{im} d_{i+1} \geq i + 1$. For all $j \leq i$, the long exact homology sequence induced by the first short exact sequence gives

$$\operatorname{Ext}_R^{j-1}(R/I, M_i) = 0 \to \operatorname{Ext}_R^{j-1}(R/I, M_i/\operatorname{im} d_{i+1}) \to \operatorname{Ext}_R^j(R/I, \operatorname{im} d_{i+1}) = 0$$

so that $\text{depth}_I(M_i/\text{im}d_{i+1}) \geq i$. If $H_i(M_\bullet) = 0$, then $\text{im}d_i$ has I-depth at least i. It is impossible for $H_i(M_\bullet) \neq 0$, since the second short exact sequence gives

$$0 \to \text{Ext}^0_R(R/I, H_i(M_\bullet)) \neq 0 \to \text{Ext}^0_R(R/I, M_i/\text{im}d_{i+1})$$

which yields $\text{Ext}^0_R(R/I, M_i/\text{im}d_{i+1}) \neq 0$, so $\text{depth}_I(M_i/\text{im}d_{i+1}) = 0$, contradicting the condition. □

Lemma 5.7.4. *Let R be a Noetherian ring, and M a non-zero R-module. Let F, G, H be finitely generated free R-modules, and*

$$F \xrightarrow{f} G \xrightarrow{g} H$$

a complex such that $I(f, M) = I(g, M) = R$. Then

$$F \otimes_R M \xrightarrow{f} G \otimes_R M \xrightarrow{g} H \otimes_R M$$

is exact if and only if

$$\text{rank}(f, M) + \text{rank}(g, M) = \text{rank}G.$$

Proof. For any R-module N, by the property of tensor product,

$$N \otimes_R M \cong N \otimes_R M \otimes_{R/\text{Ann}(M)} (R/\text{Ann}(M)) \cong (N/\text{Ann}(M)N) \otimes_{R/\text{Ann}(M)} M.$$

Thus, we may assume $\text{Ann}(M) = 0$. Hence, $\text{rank}(f, M) = \text{rank}(f)$, and $\text{rank}(g, M) = \text{rank}(g)$. Without loss of generality, assume that R is a local ring. Since $I(f) = R$, there must be an invertible $\text{rank}(f) \times \text{rank}(f)$ submatrix. By a change of basis, we can write

$$f = \begin{bmatrix} 1 & 0 \\ 0 & A \end{bmatrix}, \text{ where } A \text{ is invertible of size } (\text{rank}(f) - 1) \times (\text{rank}(f) - 1).$$

By induction, we can write f as a matrix with one in the diagonal entries, and zero elsewhere. Therefore, $\ker f$ and $\text{coker} f$ are free R-modules, and $G \cong \ker f \oplus \text{im}f$.

Since $F \to \ker g \subseteq G$, with the similar method, we can show that $\ker g$ is free, and $\ker g \cong \text{im}f \oplus E$ where E is a free module. The rank of the free module $G/\ker g = \text{rank}g$, and $\text{rank}f = \text{rank}(\text{im}f)$.

Now, $F \otimes_R M \longrightarrow G \otimes_R M \longrightarrow H \otimes_R M$ is exact if and only if $E \otimes_R M = 0$, if and only if $E = 0$ or $M = 0$. Since $M \neq 0$, we must have $E = 0$. Thus $F \otimes_R M \longrightarrow G \otimes_R M \longrightarrow H \otimes_R M$ is exact if and only if $\text{rank}G = \text{rank}(f) + \text{rank}(g)$. □

Theorem 5.7.5. *(Buchsbaum-Eisenbud Exactness Criteria) Let R be a Noetherian ring, and M a non-zero R-module. Suppose $F_\bullet$ is the complex*

$$F_\bullet : \quad 0 \to F_n \xrightarrow{f_n} F_{n-1} \xrightarrow{f_{n-1}} \cdots \to F_2 \xrightarrow{f_2} F_1 \xrightarrow{f_1} F_0,$$

where F_i's are finitely generated free R-modules. Then $F_\bullet \otimes M$ is exact if and only if the following condition hold for all $i \geq 1$

1. $\operatorname{rank}(f_i, M) + \operatorname{rank}(f_{i+1}, M) = \operatorname{rank} F_i$;
2. $\operatorname{depth}_{I(f_i,M)}(M) \geq i$, *that is $I(f_i, M)$ contains a M-regular sequence of length i.*

Proof. For detailed proof, please see [BE73]. □

5.8 Local Cohomology

Let R be a commutative ring, $I \subseteq R$ an ideal, and M an R-module. We define the **global sections with support in** I to be the submodule

$$\Gamma_I(M) = \{m \in M \mid I^n m = 0, \text{ for some } n\}.$$

The reason for this terminology is the following. Let $X = \operatorname{Spec}(R)$, $Y = \mathbb{V}(I) \subset X$ and $\mathcal{F} = \tilde{M}$ be the quasi-coherent sheaf defined by M. Then we can define

$$\Gamma_Y(X, \mathcal{F}) = \{s \in \Gamma(X, \mathcal{F}) \mid \text{ support } (s) \subset Y\}.$$

Then the quasi-coherent sheaf associated to the R-module $\Gamma_I(M)$ is $\Gamma_Y(X, \mathcal{F})$: $\widetilde{\Gamma_I(M)} = \Gamma_Y(X, \mathcal{F})$.

Given any complex $C_\bullet$, we can form a new complex $\Gamma_I(C_\bullet)$

$$\Gamma_I(C_\bullet) : \quad \cdots \to \Gamma_I(C_{i+1}) \to \Gamma_I(C_i) \to \Gamma_I(C_{i-1}) \to \cdots .$$

Now, let $C^\bullet$ be an injective resolution of an R-module M,

$$C^\bullet : \quad 0 \to I^0 \to I^1 \to I^2 \cdots, \text{ where } 0 \to M \to I^0 \to I^1 \to I^2 \cdots \text{ is exact.}$$

Then, apply Γ_I to $C^\bullet$,

$$\Gamma_I(C^\bullet) : \quad 0 \to \Gamma_I(I^0) \to \Gamma_I(I^1) \to \Gamma_I(I^2) \cdots,$$

and then the i-th cohomologies of $\Gamma_I(C^\bullet)$ are the **local cohomology modules** of M with support in I, denoted by $H^i_I(M)$. Up to isomorphism, these

are independent of the choice of the injective resolution of M. They are the right derived functors of the functor $\Gamma_I(M)$. Since Γ_I is a left exact, so $0 \to \Gamma_I(M) \to \Gamma_I(I^0) \to \Gamma_I(I^1)$ is exact, we have that

$$H^0_I(M) = \ker(\Gamma_I(I^0) \to \Gamma_I(I^1))/\mathrm{im}(0 \to \Gamma_I(I^0)) = \Gamma_I(M).$$

Definition 5.8.1. Let $\{I_n\}$ and $\{J_n\}$ be two decreasing chains of ideals. The chains are **cofinal** if for all n, there exists k such that $J_k \subseteq I_n$, and for all m, there exists t such that $I_t \subseteq J_m$. Hence, if $\{I_n\}$ is cofinal with $\{I^n\}$, then

$$H^i_I(M) = \lim_{\to} \mathrm{Hom}_R(R/I_n, M).$$

Another view of the local cohomology is to write

$$\Gamma_I(M) = \bigcup_{i=0}^{n} (0 :_M I^n), \text{ and } (0 :_M I^n) = \mathrm{Hom}_R(R/I^n, M).$$

Hence

$$H^0_I(M) = \Gamma_I(M) = \lim_{\to} \mathrm{Hom}_R(R/I^n, M), \quad H^i_I(M) = \lim_{\to} \mathrm{Ext}^i_R(R/I^n, M).$$

Remark 5.8.2.

$$\Gamma_I(M) = \{m \in M \mid I^n m = 0, \text{ for some } n\} = \Gamma_J(M) \text{ if } \sqrt{I} = \sqrt{J}.$$

Definition 5.8.3. The local cohomology can also be viewed via the **Čech complex** $C^\bullet$. Let $x_1, \ldots, x_n \in R$, and R_x the localization of R at the multiplicatively closed set $\{x^m\}$, then

$$C^\bullet : \quad 0 \to R \to \bigoplus \sum_i R_{x_i} \to \bigoplus \sum_{i<j} R_{x_i x_j} \to \cdots \to R_{x_1 x_2 \cdots x_n} \to 0,$$

where the maps are the natural maps induced from the localization with signs attached.

$$C^\bullet(\mathbf{x}; M) = C^\bullet(x_1, \ldots, x_n; M) = C^\bullet(x_1, \ldots, x_n; R) \otimes M = C^\bullet(\mathbf{x}; R) \otimes M.$$

The ***i*-th Čech cohomology** of M is $H^i_{\mathbf{x}}(M) := H^i(C^\bullet(\mathbf{x}; M))$.

Proposition 5.8.4. *Suppose* $0 \to L \to M \to N \to 0$ *is a short exact sequence of* R*-modules and* $\mathbf{x} = x_1, \ldots, x_n \in R$*. Then there exists a long exact sequence:*

$$\cdots \to H^n_{\mathbf{x}}(L) \to H^n_{\mathbf{x}}(M) \to H^n_{\mathbf{x}}(N) \to H^{n+1}_{\mathbf{x}}(L) \to \cdots$$

Proof. The following commutative diagram (where the exactness of the columns are due to the localization) gives the short exact sequence of cocomplex $0 \to C^\bullet(\mathbf{x}; L) \to C^\bullet(\mathbf{x}; M) \to C^\bullet(\mathbf{x}; N) \to 0$, which in turn gives the desired long exact sequence of the cohomology.

$$\begin{array}{ccccccccccc}
 & & 0 & & 0 & & & & 0 & & \\
 & & \downarrow & & \downarrow & & & & \downarrow & & \\
0 & \longrightarrow & L & \longrightarrow & \bigoplus_i L_{x_i} & \longrightarrow & \cdots & \longrightarrow & L_{x_1 \cdots x_n} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & & & \downarrow & & \\
0 & \longrightarrow & M & \longrightarrow & \bigoplus_i M_{x_i} & \longrightarrow & \cdots & \longrightarrow & M_{x_1 \cdots x_n} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & & & \downarrow & & \\
0 & \longrightarrow & N & \longrightarrow & \bigoplus_i N_{x_i} & \longrightarrow & \cdots & \longrightarrow & N_{x_1 \cdots x_n} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & & & \downarrow & & \\
 & & 0 & & 0 & & & & 0 & &
\end{array}$$

□

Proposition 5.8.5. *Let M be an R-module, $\mathbf{x} = x_1, \ldots, x_n \in R$. If $y \in R$, then there exists a long exact sequence*

$$\cdots \to H^i_{\mathbf{x},y}(M) \to H^i_{\mathbf{x}}(M) \xrightarrow{(-1)^i} H^i_{\mathbf{x}}(M)_y \to H^{i+1}_{\mathbf{x},y}(M) \to \cdots .$$

Proof. Let $C^\bullet = C^\bullet(\mathbf{x}; M)$, and $C^\bullet(y) = C^\bullet(\mathbf{x}, y; M) = C^\bullet(\mathbf{x}; M) \otimes C^\bullet(y; M)$. Then $C^\bullet(y) = C^\bullet \otimes (0 \to R \to R_y \to 0)$. Hence,

$$C^\bullet(y)^n = C^{n-1} \otimes_R R_y \oplus C^n \otimes_R R \cong C^{n-1}_y \oplus C^n,$$

and the following diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & C^{n-1}_y & \longrightarrow & C^{n-1}_y \oplus C^n & \longrightarrow & C^n & \longrightarrow & 0 \\
 & & {\scriptstyle \partial_y}\downarrow & & {\scriptstyle f_{n-1}}\downarrow & & {\scriptstyle \partial}\downarrow & & \\
0 & \longrightarrow & C^n_y & \longrightarrow & C^n_y \oplus C^{n+1} & \longrightarrow & C^{n+1} & \longrightarrow & 0
\end{array}$$

yields a short exact sequence

$$0 \to C^\bullet_y[-1] \to C^\bullet(y) \to C^\bullet \to 0.$$

This short exact sequence gives the long exact sequence

$$\cdots \to H^{i-1}_{\mathbf{x}}(M)_y \to H^i_{\mathbf{x},y}(M) \to H^i_{\mathbf{x}}(M) \xrightarrow{\partial} H^i_{\mathbf{x}}(M)_y \to \cdots$$

where $H^{i-1}_{\mathbf{x}}(M)_y = H^i(C^\bullet_y[-1]) \cong H^{i-1}(C^\bullet_y)$. □

Remark 5.8.6. 1. Let M be an R-module, and $\mathbf{x} = x_1, \ldots, x_n \in R$. If x_i acts as a unit on M for some i, then $H^i_{\mathbf{x}}(M) = 0$ for all i.

2. For any injective module E, $H^i_{\mathbf{x}}(E) = 0$ for all $i \geq 0$.

Proposition 5.8.7. *Let R be a commutative Noetherian ring, I an ideal, and M an R-module. If $\sqrt{I} = \sqrt{(x_1, \ldots, x_n)}$, then*

$$H^i_I(M) \cong H^i_{\mathbf{x}}(M), \ \forall\, i, \quad \textit{and} \quad H^n_I(M) = M_{x_1 \cdots x_n} / \sum_i M_{x_1 \cdots \hat{x}_i \cdots x_n}.$$

Proof. We will prove the results by induction on i. Consider the sequence

$$0 \to M \xrightarrow{f_0} M_{x_1} \oplus \cdots \oplus M_{x_n},$$

and by definition,

$$\begin{aligned} H^0_{\mathbf{x}}(M) &= \ker(f_0) = \{m \in M \mid m x_i^{n_i} = 0, \text{ for some } n_i \in \mathbb{Z}\} \\ &= \Gamma_I(M) = H^0_I(M). \end{aligned}$$

Now, for $i > 0$, let E be an injective resolution of M, then the short exact sequence

$$0 \to M \to E \to C \to 0$$

gives a long exact sequence

$$\begin{array}{ccccccc} \cdots \to H^{i-1}_{\mathbf{x}}(E) & \longrightarrow & H^{i-1}_{\mathbf{x}}(C) & \longrightarrow & H^i_{\mathbf{x}}(M) & \longrightarrow & H^i_{\mathbf{x}}(E) = 0 \\ \cong\downarrow & & \cong\downarrow & & \downarrow & & \downarrow \\ \cdots \to H^{i-1}_I(E) & \longrightarrow & H^{i-1}_I(C) & \longrightarrow & H^i_I(M) & \longrightarrow & H^i_I(E) = 0 \end{array}$$

where the isomorphisms are due to the induction hypothesis. By the Five lemma, $H^i_{\mathbf{x}}(M) \cong H^i_I(M)$.

Finally, consider the complex

$$\textstyle\bigoplus_i M_{x_1 \cdots \hat{x}_i \cdots x_n} \xrightarrow{f} M_{x_1 \cdots x_n} \longrightarrow 0,$$

and by definition

$$H^n_I(M) = M_{x_1 \cdots x_n} / \mathrm{im}(f) = M_{x_1 \cdots x_n} / \sum_i M_{x_1 \cdots \hat{x}_i \cdots x_n}.$$

□

Proposition 5.8.8. *(Change of Rings) Let S be an R-algebra, where R and S are Noetherian. Let I be an ideal in R, and M an S-module. Then*

$$H^i_I(M) \cong H^i_{IS}(M) \quad \forall\, i,$$

where M is considered as a left R-module and a right S-module. Moreover, if S is a flat R-algebra, then

$$H^i_I(M) \otimes_R S \cong H^i_{IS}(M \otimes_R S), \quad \forall\, i \geq 0.$$

Proof. Let $I = (x_1, \ldots, x_n)R$. Then

$$\begin{aligned} C^\bullet_R(\mathbf{x}; M) &= C^\bullet(\mathbf{x}; R) \otimes M = C^\bullet(\mathbf{x}; R) \otimes_R (S \otimes_S M) = C^\bullet(\mathbf{x}; S) \otimes_S M \\ &= C^\bullet_S(\mathbf{x}; M), \end{aligned}$$

and,

$$H^i_I(M) = H^i_{\mathbf{x}}(M) = H^i_{\mathbf{x}S}(M) = H^i_{IS}(M).$$

If S is flat, then

$$\begin{aligned} H^i_I(M) \otimes_R S &= H^i(C^\bullet(\mathbf{x}; M)) \otimes_R S \cong H^i(C^\bullet(\mathbf{x}; M) \otimes_R S) \\ &\cong H^i(C^\bullet(\mathbf{x}S; M \otimes_R S)) = H^i_{\mathbf{x}S}(M \otimes_R S) \\ &= H^i_{IS}(M \otimes_R S). \end{aligned}$$

□

Theorem 5.8.9. *(Mayer-Vietoris Sequence) Let R be a Noetherian ring, I, J ideals in R, and M an R-module. Then there exists a long exact sequence*

$$\cdots \to H^i_{I+J}(M) \to H^i_I(M) \oplus H^i_J(M) \to H^i_{I \cap J}(M) \to \cdots.$$

Proof. Consider the short exact sequence

$$0 \to R/(I^n \cap J^n) \to R/I^n \oplus R/J^n \to R/(I^n + J^n) \to 0.$$

Apply $\mathrm{Hom}_R(*, M)$ to obtain a long exact sequence

$$\begin{aligned} &\cdots \to \mathrm{Ext}^i(R/(I^n + J^n), M) \to \mathrm{Ext}^i(R/I^n, M) \oplus \mathrm{Ext}^i(R/J^n, M) \\ &\to \mathrm{Ext}^i(R/(I^n \cap J^n), M) \to \cdots. \end{aligned}$$

By the Artin-Rees Lemma, there exits a k such that $m \geq k$

$$I^m \cap J^n = I^{m-k}(I^k \cap J^n) \subseteq I^{m-k} J^n,$$

and therefore,

$$\forall\, m \geq n+k,\ I^m \cap J^m \subseteq I^m \cap J^n \subseteq I^{m-k}J^n \subseteq I^n J^n \subseteq (I \cap J)^n.$$

On the other hand $(I \cap J)^n \subseteq I^n \cap J^n$. Thus, $\{I^n \cap J^n\}$ is cofinal with $\{(I \cap J)^n\}$. Moreover,

$$I^n + J^n \subseteq (I+J)^n, \text{ and } (I+J)^{2n} \subseteq I^n + J^n,$$

so $\{I^n + J^n\}$ is cofinal with $\{(I+J)^n\}$. Thus, take the direct limit, we have the desired long exact sequence. □

5.9 Applications

5.9.1 Castelnuovo-Mumford Regularity

In chapter 14 of [Mum66], Mumford introduced the concept of *regularity* for a coherent sheaf $\mathcal{F}$ on projective space $\mathbb{P}^n$: $\mathcal{F}$ is p-regular if, for all $i \geq 1$ we have vanishing for the twists

$$\mathrm{H}^i\left(\mathbb{P}^n,\, \mathcal{F}(k)\right) = 0, \quad \text{for all } k+i = p.$$

This in turn implies the stronger condition of vanishing for $k + i \geq p$. The definition for a finitely generated graded R-module M, which extends that for sheaves was given by Eisenbud and Goto [EG84], and regularity was investigated later by several people, notably Bayer and Mumford [BM93], Bayer and Stillman [BS87], Eisenbud and Goto [EG84], and Ooishi [Ooi82].

Let $R = \mathbb{K}[x_0, ..., x_n]$ with $\deg(x_i) = 1$ be the polynomial algebra in $n+1$ variables over a field $\mathbb{K}$, graded in the usual way. If M is a finitely generated graded R-module, then the *Castelnuovo-Mumford regularity* of M, denoted by $\mathrm{reg}(M)$, is an invariant that measures the "size" of its minimal free resolution and the complexity of the given module. Recall that a graded minimal free resolution of M as the following:

$$0 \to \bigoplus_j R(-j)^{\beta_{p,j}} \to \cdots \to \bigoplus_j R(-j)^{\beta_{1,j}} \to \bigoplus_j R(-j)^{\beta_{0,j}} \to M \to 0,$$

where the exponents $\beta_{i,j}$ of the shifted modules $R(-j)$ are the graded Betti numbers of M over R. Using the Betti number, we identify an important invariant that measure the "growth" of the resolution of M as an R-module.

Definition 5.9.1. Let $t_i^R(M) = \sup\{j \mid \beta_{i,j}^R(M) \neq 0\}$, the **Castelnuovo-Mumford regularity**, or **regularity**, $\mathrm{reg}_R(M)$, is defined as

$$\mathrm{reg}_R(M) = \sup\{j - i \mid \beta_{i,j}^R(M) \neq 0\} = \sup\{t_i^R(M) - i \mid i \in \mathbb{N}\}.$$

We observe that if M has a minimal free resolution of the $F_\bullet$

$$F_\bullet : \quad \cdots \to F_n \to F_{n_1} \to \cdots \to F_1 \to F_0 \to 0$$

where $F_i = \bigoplus_j R(-a_{ij})$, then $\mathrm{reg}_R(M) = \sup_{i,j}\{a_{ij} - i\}$. An important characterization of regularity is:

Theorem 5.9.2. *Suppose $\mathbb{K}$ is a field and M is a graded R-module. Then M is p-regular if and only if the minimal free graded resolution of M has the form*

$$0 \to \bigoplus_{\alpha=1}^{r_s} Re_{\alpha,s} \to \cdots \to \bigoplus_{\alpha=1}^{r_1} Re_{\alpha,1} \to \bigoplus_{\alpha=1}^{r_0} Re_{\alpha,0} \to M \to 0$$

where $\deg(e_{\alpha,i}) \leq p + i$ for all $i \geq 0$.

Thus, if M is a graded R-module of finite length, then

$$\mathrm{reg}(M) = \max\{d \mid M_d \neq 0\}.$$

The most important characterization of Castelnuovol-Mumford regularity is cohomologoical. Eisenbud and Goto [EG84] gave a connection between the regularity for a coherent sheaf and the regularity of graded modules via local cohomology. The following result is proved by Grothendieck, a proof can be found in [Proposition A1.11, [Eis05]]

Proposition 5.9.3. *(Local cohomology and Sheaf Cohomology) Let M be a graded R-module, and $\mathcal{F}$ be the corresponding quasi-coherent sheaf on $\mathbb{P}^n$. Then*

$$0 \to H^0_{\mathfrak{m}}(M) \to M \to \bigoplus_{d\in\mathbb{Z}} H^0(\mathcal{F}(d)) \to H^1_{\mathfrak{m}}(M) \to 0$$

and

$$H^{i+1}_{\mathfrak{m}}(M) = \bigoplus_{d\in\mathbb{Z}} H^i(\mathbb{P}^n, \mathcal{F}(d)), \quad \forall i \geq 1.$$

Since the local cohomology is actually dual to the homology of the complex $\mathrm{Hom}(F_\bullet, R)$, where $F_\bullet$ is a free resolution of M, the regularity can be

formulated in terms of local cohomology. In particular, the local cohomology groups $H^i_{\mathfrak{m}}(M)$ with respect to the ideal $\mathfrak{m} = (x_0, ..., x_n)$ are graded in a natural way and we say that M is **p-regular** if

$$H^i_{\mathfrak{m}}(M)_k = 0 \quad \text{for all } k + i \geq p + 1.$$

If $\mathcal{F}$ is the coherent sheaf on $\mathbb{P}^n$ associated with M in the usual way, we have

$$H^{i+1}_{\mathfrak{m}}(M)_k = \mathrm{H}^i(\mathbb{P}^n, \mathcal{F}(k)) \quad \text{for all } i \geq 1,$$

which shows the compatibility of these definitions. Eisenbud [Theorem 4.3, [Eis05]] provides a characterization of regularity via cohomology.

Theorem 5.9.4. *Let M be a finitely generated graded R-module and*

$$r_i = \max\{j \mid H^i_{\mathfrak{m}}(M)_j \neq 0\}, \quad \textit{for each } i.$$

Then the following are equivalent:

1. $\mathrm{reg}(M) \leq p$;
2. $r_i + i \leq p$ *for all* $i \geq 0$;
3. $r_0 \leq p$ *and* $H^i_{\mathfrak{m}}(M)_{p-i+1} = 0$ *for all* $i > 0$.

Moreover, it is proved in [Eis95] that

Theorem 5.9.5. *If M is a finitely generated graded $R = \mathbb{K}[x_0, \ldots, x_n]$-module, then M is p-regular if and only if*

$$\mathrm{Ext}^i(M, R)_n = 0, \quad \forall\, i,\ \forall\, n \leq -p - i - 1.$$

In addition, if $0 \to A \to B \to C \to 0$ is a short exact sequence of graded finitely generated R-modules, then

1. $\mathrm{reg}A \leq \max(\mathrm{reg}B, \mathrm{reg}C + 1)$;
2. $\mathrm{reg}B \leq \max(\mathrm{reg}A, \mathrm{reg}C)$;
3. $\mathrm{reg}C \leq \max(\mathrm{reg}A - 1, \mathrm{reg}B)$;
4. *If A has finite length, then* $\mathrm{reg}B = \max(\mathrm{reg}B, \mathrm{reg}C)$.

Computer algebra system Singular [GPS01] can compute the regularity of an ideal or module via code “regularity”.

Example 5.9.6. The regularity of the ideal $I = \langle x^2, xy, y^3 \rangle$ is 3.

```
> ring r=0, (x, y, z),dp;
> ideal i=(x^2, x*y, y^3);
> def L=res(i,0);
> regularity(L);
3
```

Note, $\text{reg}(I) = 3$, and $\text{reg}(R/I) = 2$ is obtained in Example 4.8.17.

5.9.2 The MacRae's Invariant

As before, let R be a commutative ring with unit, we will introduce the concept of Fitting ideal and MacRae's invariant. First, we will start with the definition of Fitting ideal.

Definition 5.9.7. Let F be a free R-module of finite rank n, and K a submodule of F (may not be finitely generated). If $r_1, \ldots, r_n \in F$ is a free basis for F, and $k_i = \sum_{j=1}^{n} a_{ij} r_j$ for $i \in I$ is a generating set for K, then $\text{Fitt}^j((r_1, \ldots, r_n)/(k_i,\, i \in I))$ for $j = 0, \ldots, n-1$ is the **j-th Fitting ideal** of R generated by the determinant of $(n-j) \times (n-j)$ minors of the matrix

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \vdots & \vdots & & \vdots \end{pmatrix}.$$

It is proved by Fitting [Page 197, [Fit36]] that if there are two bases $\{r_i\}_{i=1}^n$ and $\{r'_i\}_{i=1}^n$ for F, and two generating sets $\{k_i\}_{i\in I}$ and $\{k'_i\}_{i\in J}$ for K, then

$$\text{Fitt}^j((r_1, \ldots, r_n)/(k_i,\, i \in I)) = \text{Fitt}^j((r'_1, \ldots, r'_n)/(k'_i,\, i \in I)),\ 0 \le j \le n-1,$$

and we denote this ideal to be $\text{Fitt}^j(F/K)$.

A key point is that it is possible to define an invariant of the module M from these Fitting ideals.

Proposition 5.9.8. *Let M be a finitely generated module over a ring R. Suppose that $K \to F \to M \to 0$, and $L \to G \to M \to 0$ are two different presentations of M as quotients of free modules F and G. Then for all $j \ge 0$, $\text{Fitt}^j(F/K) = \text{Fitt}^j(G/L)$. We can define $\text{Fitt}^j(M)$ to be $\text{Fitt}^j(F/K)$ for any presentation of M.*

Here are some useful properties of the Fitting ideals:

Proposition 5.9.9. *Let M be a finitely generated R-module.*

1. *The Fitting ideals of M form an increasing sequence:*

$$\mathrm{Fitt}(M) = \mathrm{Fitt}^0(M) \subseteq \mathrm{Fitt}^1(M) \subseteq \mathrm{Fitt}^2(M) \subseteq \cdots$$

   Moreover, if M is generated by s elements, then $\mathrm{Fitt}^s(M) = R$.

2. *Given any map $R \to S$ of rings, then*

$$\mathrm{Fitt}^t(M \otimes_R S) = (\mathrm{Fitt}^t(M))S, \ \forall t \in \mathbb{N}.$$

3. $\mathrm{Ann}(M)\mathrm{Fitt}^t(M) \subseteq \mathrm{Fitt}^{t-1}(M)$ *for all $t \in \mathbb{N}$. If M can be generated by s elements, then*

$$\mathrm{Ann}(M)^s \subseteq \mathrm{Fitt}(M) \subseteq \mathrm{Ann}(M).$$

4. *If M is finitely presented (i.e, M and its first syzygy module are both finitely generated), then each of its Fitting ideals is a finitely generated ideal of R.*

Note that property 3 above shows that $\mathrm{Fitt}(M)$ is 0 if M is a faithful module. Thus, the study of this invariant is interesting only for unfaithful modules. This leads to the following:

Definition 5.9.10. An R-module M is coherently unfaithful if $(0 :_R M)$ contains a nonzero divisor.

Definition 5.9.11. Let M be an R-module, then the **homological dimension of** M, $\mathrm{hdim}(M)$, is defined as $\mathrm{hdim}(M) = 0$ if M is projective module, or $\mathrm{hdim}(M) = n \geq 1$ if M is not projective, and there exists a short exact sequence $0 \to A \to P \to M \to 0$ where P is a projective module and such that $\mathrm{hdim}(A) = n - 1$.

It is proved by MacRae [Lemma 3.1, [Mac65]] that if R is a Noetherian ring, M is a finitely generated R-module of finite homological dimension, and $(0 :_R M)$ contains a non-zero divisor, then there exists an exact sequence $0 \to F_n \to F_{n-1} \to \cdots \to F_0 \to M \to 0$ where F_i's are finitely generated R-modules of homological dimension at most one, and $(0 :_R F_i)$ contains a non-zero divisor.

Definition 5.9.12. Let M be a finitely generated R-module with R Noetherian, then M is called a **coherent projective** module if there exists a free module F of finite rank such that $M \oplus F$ is also free of finite rank. If there exists an exact sequence

$$0 \to F_n \to F_{n-1} \to \cdots \to F_0 \to M \to 0,$$

where F_i are coherent projective modules, and there exists no shorter such sequence, then we say $\mathrm{hdim}^*(M) = n$. If no such sequence exists, then we say $\mathrm{hdim}^*(M) = \infty$.

Below are some properties between $\mathrm{hdim}(M)$ and $\mathrm{hdim}^*(M)$ proved by MacRae.

Lemma 5.9.13. *Let M be a finitely generated R-module with R Noetherian.*

1. $\mathrm{hdim}(M) \leq \mathrm{hdim}^*(M)$ *and* $\mathrm{hdim}^*(M) < \infty \Rightarrow \mathrm{hdim}(M) = \mathrm{hdim}^*(M)$.
2. *If* $\mathrm{hdim}^*(M) = n < \infty$, *and* $0 \to K \to F_{n-1} \to \cdots \to F_0 \to M \to 0$ *is exact where F_i's are coherent projective modules, then K is also a coherent projective module.*
3. *If* $0 \to A_1 \to A_2 \to A_3 \to 0$ *is an exact sequence of finitely generated R-modules,* $\mathrm{hdim}^*(A_i) < \infty$, *and* $\mathrm{hdim}^*(A_j) < \infty$ *for fixed $i \neq j$, then* $\mathrm{hdim}^*(A_k) < \infty$ *for $k \neq i, j$.*

Proof. See [Lemma 4.3-4.5, [Mac65]]. □

The most important of the Fitting invariants is the first one.
Consider the commutative diagram with exact rows and columns

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & K & & K & & \\
 & & & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & L & \longrightarrow & W & \longrightarrow & R^m & \longrightarrow & 0 \\
 & & & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & L & \longrightarrow & R^n & \longrightarrow & M & \longrightarrow & 0 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 0 & & 0 & &
\end{array}$$

If

$$f \oplus g : R^m \oplus R^n \to M, \quad W = \{(s,t) \in R^m \oplus R^n \mid f(s) = g(t)\},$$

$\pi_1 : W \to R^m$, and $\pi_2 : W \to R^n$ are the two projections, then $K = \ker(\pi_1)$ and $L = \ker(\pi_2)$. MacRae [Mac65] proved that

$$\mathrm{Fitt}^0(R^m/K) = \mathrm{Fitt}^0(R^n/L) = \mathrm{Fitt}^0(R^m \oplus R^n/W).$$

Thus, if M is a finitely generated R-module,we can consider any presentation $K \to R^m \to M \to 0$, and define the **0-th Fitting ideal**, or sometimes **Fitting invariant of** M, $\mathrm{Fitt}(M) = \mathrm{Fitt}^0(M) = \mathrm{Fitt}^0(R^m/K)$. It is proved by MacRae that the Fitting ideal has the following properties:

Theorem 5.9.14. *1. Let M be a finitely generated R-module, and S a multiplicatively closed set in R. Then $\mathrm{Fitt}(M_S) = \mathrm{Fitt}(M)_S$, where the R_S means the localization.*

2. If $0 \to A \to B \to C \to 0$ is a short exact sequence of finitely generated R-modules, then $\mathrm{Fitt}(A)\mathrm{Fitt}(C) \subseteq \mathrm{Fitt}(B)$.

3. If M is a finitely generated R-module, then $\mathrm{Fitt}(M) \subseteq (0 :_R M)$, and $(0 :_R M)^m \subseteq \mathrm{Fitt}(M)$ for some m.

4. If M is a finitely generated of $\mathrm{hdim}(M) \leq 1$, and $(0 :_R M)$ contains a non-zero divisor, then $\mathrm{Fitt}(M)_{\mathfrak{p}}$ is a principal ideal generated by non-zero divisor in $R_{\mathfrak{p}}$ for each prime ideal $\mathfrak{p} \subset R$. Moreover, if R is a Noetherian ring, then $\mathrm{Fitt}(M)$ is an invertible ideal in R.

5. If $0 \to A \to B \to C \to 0$ is a short exact sequence of finitely generated R-modules, $\mathrm{hdim}(C) \leq 1$, and $(0 :_R C)$ contains a non-zero divisor, then $\mathrm{Fitt}(A)\mathrm{Fitt}(C) = \mathrm{Fitt}(B)$.

Proof. For details see [Lemma 2.5 - Proposition 2.11, [Mac65]]. □

The Fitting invariant can be extended to another invariant called *MacRae invariant.*

Definition 5.9.15. Let M be a finitely generated, coherently unfaithful R-module (i.e., $(0 :_R M)$ contains a non-zero divisor). If $0 \to F_n \to F_{n-1} \to \cdots \to F_0 \to M \to 0$ is an exact sequence, where F_i's are finitely generated, coherently unfaithful R-module of homological dimension at most one, then **MacRae invariant of** M is the invertible fractional ideal denoted by $G(M) = \prod_{i=0}^{n} \mathrm{Fitt}(F_i)^{(-1)^i}$.

Definition 5.9.16. An ideal $I \subset R$ is said to have **grade zero** if I is contained in a prime ideal which belongs to the null ideal of R, and the ideal I is said to have **grade** n if there exists a non-zero divisor $a \in I$ such that the ideal $I/\langle a\rangle \subset R/\langle a\rangle$ has grade $n-1$.

The relationship between grade and homological dimension are studied by a few people, here we quote some of the known results:

Remark 5.9.17. 1. If R is a local ring, $\mathfrak{p}$ is its maximal ideal, N is a finitely generated R-module of finite homological dimension, then $\mathrm{hdim}(N) \leq \mathrm{grade}(\mathfrak{p})$, and

$$\mathrm{hdim}(N) = \mathrm{grade}(\mathfrak{p}) \;\Leftrightarrow\; \mathfrak{p} \subset \text{ null submodule of } N.$$

2. If $\mathfrak{p}$ is a prime ideal which belongs to the null submodule of a finitely generated module N, then $\mathrm{grade}(\mathfrak{p}) \leq \mathrm{hdim}(N)$.

3. If $\mathfrak{p}$ is a prime ideal which belongs to the null submodule of a finitely generated module N of finite homological dimension, and S is a multiplicatively closed subset of R disjoint from P, then $\mathrm{grade}(\mathfrak{p}) = \mathrm{grade}(\mathfrak{p}_S)$.

Proof. See [AB57] and [Mac65]. □

MacRae showed that $G(M)$ is independent of the resolution and has the following properties:

Proposition 5.9.18 (Proposition 3.3, [Mac65])**.** *Let M be a finitely generated, coherently unfaithful R-module (i.e., $(0 :_R M)$ contains a non-zero divisor) of finite homological dimension. Then*

1. *If $0 \to F_n \to F_{n-1} \to \cdots \to F_0 \to M \to 0$, and $0 \to E_m \to E_{m-1} \to \cdots \to E_0 \to M \to 0$ are exact sequences with F_i and E_i are finitely generated, coherently unfaithful R-modules of homological dimension at most one, then*

$$\prod_{i=0}^{n} \mathrm{Fitt}(F_i)^{(-1)^i} = \prod_{i=0}^{m} \mathrm{Fitt}(E_i)^{(-1)^i}.$$

2. *If $\mathrm{hdim}(M) \leq 1$, then $G(M) = \mathrm{Fitt}(M)$.*

3. *If S is a multiplicatively closed subset of R then $G(M)_S = G(M_S)$.*

4. *If* $0 \to A \to B \to C \to 0$ *is an exact sequences of finitely generated, coherently unfaithful* R*-modules of finite homological dimension, then* $G(A)G(C) = G(B)$.

5. $G(M)$ *is an invertible ideal of* R*. Moreover, it is a principal ideal generated by a non-zero divisor such that* $\mathrm{Fitt}(M) \subseteq G(M)$*, and it is the smallest one with the property: if* I *is a principal ideal of* R *such that* $\mathrm{Fitt}(M) \subseteq I$*, then* $G(M) \subseteq I$.

6. *The prime ideals which belong to* $G(M)$ *are precisely the same as the grade one prime ideals which belong to the null submodule of* M.

7. *If* $\mathrm{hdim}^*(M) < \infty$*, then* $G(M)$ *is principal ideal generated by a non-zero divisor.*

8. *If* R *is a local ring, the grade of* $(0 :_R M)$ *is at most one, and* $a_1, \ldots, a_n$ *is an* M*-sequence in the maximal ideal of* R*, then* $a_1, \ldots, a_n$ *is an* R*-sequence.*

Definition 5.9.19. Let I be an ideal of R. An invertible ideal J of R is said to be **common divisor of** I if I is contained in J, and is said to be a **greatest common divisor of** I if it is contained in all other common divisors of I.

It is proved by MacRae [Proposition 5.5, [Mac65]] that if I is an ideal of positive grade and finite homological dimension, then $G(R/I)$ is the greatest common divisor of I. As a direct consequence, if I is an ideal of positive grade such that $\mathrm{hdim}^*(I) < \infty$, then any set of generators for I has a greatest common divisor, i.e., $G(R/I)$.

This means that any generator of the MacRae's invariant of M may serve as GCD of any set of generators of $\mathrm{Fitt}(M)$. In particular, when R us a UFD, $G(M)$ is generated by the GCD of a set of generators of $\mathrm{Fitt}(M)$.

Definition 5.9.20. Given an R-module M such that there exists an exact sequence of finite length

$$0 \to K_n \to K_{n-1} \to \cdots \to K_1 \to K_0 \to M \to 0 \tag{5.2}$$

where the R-module K_i's are all **elementary**, (i.e., K_i having a finite free resolution of length one, $0 \to K_i'' \to K_i' \to K_i \to 0$) for all $i = 0, \ldots, n$, then we call the exact sequence (5.2) a **finite elementary resolution of** M.

With the above definition of elementary resolution, we have that an R-module has $\mathrm{hdim}(M) \leq 1$ if and only if M admits a finite free resolution with Euler characteristic $\mathrm{Char}(M) = 0$ and $\mathrm{Ann}(M)$ contains a non-zero divisor.

In general, if R is a commutative domain, and suppose an R-module M admits a finite free resolution of length $n \geq 1$

$$0 \to F_n \xrightarrow{g_n} F_{n-1} \xrightarrow{g_{n-1}} \cdots \longrightarrow F_1 \xrightarrow{g_1} F_0 \xrightarrow{g_0} M \longrightarrow 0$$

with $\mathrm{Char}(M) = \sum_{i=0}^{n}(-1)^i r_i = 0$ where $r_i = \mathrm{rank}F_i$ for all $i = 0, \ldots, n$.

Let $F_n^{(1)} = F_n$ and $F_n^{(0)} = 0$. Since the map $g_n : F_n \to F_{n-1}$ is injective, by McCoy's theorem, we have that F_{n-1} splits into $F_{n-1}^{(0)} \oplus F_{n-1}^{(1)}$ where $\mathrm{rank}F_{n-1}^{(0)} = r_n$, and $\mathrm{rank}F_{n-1}^{(1)} = r_{n-1} - r_n$, and the matrix representation of the map g_n is of the form $\begin{bmatrix} c_n \\ d_n \end{bmatrix}$ with $\det(c_n) \neq 0$.

Since $\mathrm{im}g_n = \ker g_{n-1}$, we have that F_{n-2} splits into $F_{n-2}^{(0)} \oplus F_{n-2}^{(1)}$ where $\mathrm{rank}F_{n-2}^{(0)} = r_{n-1} - r_n$, $\mathrm{rank}F_{n-2}^{(1)} = r_{n-2} - r_{n-1} + r_n$, and the matrix representation of the map g_{n-1} is of the form $\begin{bmatrix} a_{n-1} & c_{n-1} \\ b_{n-1} & d_{n-1} \end{bmatrix}$ with $\det(c_{n-1}) \neq 0$.

Continue this way, we obtain that F_i splits into $F_i^{(0)} \oplus F_i^{(1)}$ where $\mathrm{rank}F_i^{(0)} = \sum_{j=0}^{n-i-1}(-1)^j r_{i+1+j}$, and $\mathrm{rank}F_i^{(1)} = \sum_{j=0}^{n-i}(-1)^j r_{i+j}$, and the matrix representation of g_i is of the form $\begin{bmatrix} a_i & c_i \\ b_i & d_i \end{bmatrix}$ with $\det(c_i) \neq 0$.

Since $\mathrm{Char}(M) = \sum_{i=0}^{n}(-1)^i r_i = 0$, the decomposition ends with the matrix representation of the map g_1 of the form $(a_1 \ c_1)$ with $\det(c_1) \neq 0$.

It is proved by Busé [Proposition 2.12, [Bus06]] that

$$G(M) = \frac{\det(c_1)\det(c_3)\cdots}{\det(c_2)\det(c_4)\cdots}R = \left(\prod_{i=1}^{n}\det(c_i)^{(-1)^{i-1}}\right)R \subset R.$$

Furthermore, if R is graded and M is a graded R-module, then the free resolution is graded, and we have the following graded isomorphism

$$G(M) \cong \bigotimes_{i=0}^{n}\left(\bigwedge^{r_i} F_i\right)^{\otimes(-1)^{i+1}} \cong R(-d).$$

where d is the degree of $\prod_{i=1}^{n}\det(c_i)^{(-1)^{i-1}} \in R$, and $(*)^{\otimes(-1)}$ is the dual module.

For instance, if an R-module M has a free resolution of length one

$$0 \to F_1 \to F_0 \to M \to 0,$$

then $G(M)$ is an homogeneous ideal, and there is a graded isomorphisms of degree zero

$$G(M) \cong \wedge^{\max} F_0^* \otimes_A \wedge^{\max} F_1 \cong R(-d),$$

where d is the degree of the determinant of the map $F_1 \to F_0$, and $\wedge^{\max}(*)$ is the highest non-zero exterior power.

Since $G(M)$ is the smallest principal ideal containing the Fitting ideal $\mathrm{Fitt}(M)$, $G(M)$ is the *codimension one part* of $\mathrm{Fitt}(M)$, and the associated primes of $\mathrm{Fitt}(M)$ are exactly the associated primes of $\mathrm{Ann}_R(M)$. In particular, if R is a UFD, and if $P_1, \ldots, P_r$ are the irreducible factors of a GCD system of generators of $\mathrm{Fitt}(M)$, then $\prod_{i=1}^r P_i^{e_i}$ is a generator of $G(M)$ where e_i are the *multiplicity* of $G(M)$ over $R/\langle P_i \rangle$.

In fact, the Macaulay's resultant corresponds to the case that when n is the number of the homogeneous polynomials, which is the same as the number of the variables. In this case, the resultant ideal is a principal ideal, and is one of the generators of the MacRae's invariant under certain conditions.

Finally, the construction of the MacRae invariant is related to what is called the determinant of a module. These determinants are also constructed for certain kinds of complexes ("perfect complexes") and play an important role in many areas of algebraic geometry and K-theory. See for instance the paper of Knudsen and Mumford, [KM76].

5.9.3 Approximation Complex

The approximation complex was initially developed by Herzog, Simis and Vasconcelos in a sequence of papers [HSV83b], [HSV82], and [HSV83a] to study syzygies in conormal modules. It was first used in elimination theory by Busé and Jouanolou [BJ03] to provide an alternative method to compute the implicit equations of parametrized surfaces or curves. Later on, Chardin [Cha06], Busé and Chardin [BC05], Busé, Chardin and Simis [BCS10] and others applied this tool to study subjects such as regularity and Rees algebra.

The key ingredient of the approximation complexes in elimination theory is to compute the determinants of a graded complex, which is similar to the calculation of a Macaulay resultant of n homogeneous polynomials in n variables.

In this section, we will focus our attention to the basic concepts and properties of approximation complexes which obtained by a series papers by

Herzog, Simis and Vasconcelos. Let R be a Noetherian ring and I an ideal in R. We will write I^m for the usual multiplication of m copies of I for $m \geq 0$, and $I^{\otimes m} = I \otimes_R \cdots \otimes_R I$ m times for $m \geq 0$, where $I^0 = R = I^{\otimes 0}$. In this section, we study presentations for the following algebras:

$$\begin{aligned}
\mathcal{R}_I &= \mathrm{Rees}_R(I) = R[It] = \oplus_{m\geq 0} I^m t^m; \\
\mathcal{S}_I &= \mathrm{Sym}_R(I) = \oplus_{m\geq 0} I^{\otimes m}/(x\otimes y - y\otimes x)_{x,y\in I}; \\
\mathrm{gr}_I(R) &= \oplus_{m\geq 0} I^m/I^{m+1} \cong R/I \otimes_R \mathcal{R}_I; \\
\mathcal{S}_{I/I^2} &= \mathrm{Sym}_{R/I}(I/I^2) = \oplus_{m\geq 0}(I/I^2)^{\otimes m}/(x\otimes y - y\otimes x)_{x,y\in I} \\
&\cong R/I \otimes_R \mathcal{S}_I.
\end{aligned}$$

As a matter of notation, we let $a_1 \cdot a_2 \cdot \ldots \cdot a_m$ denote the image of $a_1 \otimes a_2 \otimes \ldots \otimes a_m \in I^{\otimes m}$ in $\mathcal{S}_I = \mathrm{Sym}_R(I)$. There are several relationships among these algebras, and one of the main themes is to express the comparisons implicit in the canonical diagram

$$\begin{array}{ccc}
\mathcal{S}_I & \xrightarrow{\alpha} & \mathcal{R}_I \\
\downarrow & & \downarrow \\
\mathcal{S}_{I/I^2} & \xrightarrow{\beta} & \mathrm{gr}_I(R)
\end{array}$$

by the approximation complexes. These complexes are constructed over $\mathcal{S}_I$ and $\mathcal{S}_{I/I^2}$, and then related to the homology modules $H_i(\mathbf{f}, R)$ of the regular Koszul complex $\mathcal{K}_\bullet(\mathbf{f}, R)$ built from a sequence $\mathbf{f} = \{f_0, \ldots, f_n\}$ that generates the ideal I.

First, let I be an ideal in a commutative ring R generated by $\mathbf{f} = f_0, \ldots, f_n$. To introduce the measures of comparison between the symmetric and Rees algebra of ideals, we consider the canonical surjection of R-algebras

$$0 \to \mathcal{A} = \ker(\alpha) \to \mathcal{S}_I \xrightarrow{\alpha} \mathcal{R}_I \to 0.$$

Since the ideal I can be presented as

$$0 \to Z_1 \to R^{n+1} \xrightarrow{\phi} I \to 0,$$

ϕ induces surjections h and h', where

$$\begin{aligned}
h: \quad & R[T_0, \ldots, T_n] \to \mathcal{S}_I,\ h(T_i) \to f_i, \\
& \ker(h) = Q = \sum_{i=0}^{n} c_i f_i = 0; \\
h': \quad & R[T_0, \ldots, T_n] \to \mathcal{R}_I,\ h'(T_i) = f_i t, \\
& \ker(h') = Q_\infty = \{F \in R[T_0, \ldots, T_n] \mid F(f_0, \ldots, f_n) = 0\}.
\end{aligned}$$

Therefore, we have the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Q & \longrightarrow & R[T_0,\ldots,T_n] & \xrightarrow{h} & \mathcal{S}_I & \longrightarrow & 0 \\ & & \downarrow & & & & \downarrow{\scriptstyle \alpha} & & \\ 0 & \longrightarrow & Q_\infty & \longrightarrow & R[T_0,\ldots,T_n] & \xrightarrow{h'} & \mathcal{R}_I & \longrightarrow & 0 \end{array}$$

and $\mathcal{A} = \ker(\alpha) = Q_\infty/Q$

Definition 5.9.21. If $\ker(\alpha) = 0$, then α is an isomorphism between $\mathcal{R}_I$ and $\mathcal{S}_I$, and we say that I is of **linear type**.

The ideals of linear type play an important role in the relationship between $\mathcal{S}_I$ and $\mathcal{R}_I$, and it is proven in [HSV83b] that

Theorem 5.9.22. *[Proposition 2.2, [HSV83b]] Let I be an ideal such that $I \cap (0 : I) = (0)$. Then I is of linear type if and only if $\mathcal{S}_I$ has no I-torsion, (i.e., 0 is the only element of $\mathcal{S}_I$ annihilated by I).*

In case of $\mathcal{S}_I \cong \mathcal{R}_I$, the following result holds.

Theorem 5.9.23. *[Proposition 2.4, [HSV83b]] Let I be an ideal of the Noetherian ring R. If $\mathcal{S}_I \cong \mathcal{R}_I$, then for each prime ideal $\mathfrak{p} \supset I$, $I_\mathfrak{p}$ can be generated by* $\mathrm{ht}(\mathfrak{p})$ *elements.*

Since $\mathcal{S}_I$ and $\mathcal{R}_I$ are graded objects, it is useful to check the graded components of the morphism in order to compare $\mathcal{S}_I$ and $\mathcal{R}_I$. Let

$$\alpha_t : (\mathcal{S}_I)_t \to I^t = (\mathcal{R}_I)_t, \quad \mathcal{A}_t = \ker(\alpha_t).$$

It is easy to see that if $i = 0, 1$, then $\alpha_i = \mathrm{id}$, and hence $\mathcal{A}_i = 0$. Let

$$\lambda_t : \quad (\mathcal{S}_I)_{t+1} \to (\mathcal{S}_I)_t, \quad \lambda_t(b_1 \cdot b_2 \cdots b_{t+1}) = b_1(b_2 \cdots b_{t+1})$$

be a connecting homomorphism, then $\mathrm{im}(\lambda_t)$ is a submodule $I((\mathcal{S}_I)_t) \subset (\mathcal{S}_I)_t$, and $I((\mathcal{S}_I)_t) = \ker((\mathcal{S}_I)_t \to (\mathcal{S}_{I/I^2})_t)$. Thus, we obtain the following

commutative exact diagram.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \mathcal{A}_{t+1} & \longrightarrow & \mathcal{A}_t & \longrightarrow & \mathcal{A}_t/\lambda(\mathcal{A}_{t+1}) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & (\mathcal{S}_I)_{t+1} & \xrightarrow{\lambda_t} & (\mathcal{S}_I)_t & \longrightarrow & (\mathcal{S}_{I/I^2})_t & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \alpha_{t+1}} & & \downarrow{\scriptstyle \alpha_t} & & \downarrow{\scriptstyle \beta_t} & & \\
0 & \longrightarrow & I^{t+1} & \longrightarrow & I^t & \longrightarrow & I^t/I^{t+1} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Valla [Val80] discovered following property.

Theorem 5.9.24. *Let I be an ideal of the Noetherian ring R. Then $\alpha : \mathcal{S}_I \to \mathcal{R}_I$ is an isomorphism if and only if the reduction $\beta : \mathcal{S}_I \to \mathrm{gr}_I(R)$ is an isomorphism.*

Following the notation introduced in [HSV83b], we denote the exterior and symmetric algebras of a R-module M by $\bigwedge(M)$ and $\mathrm{Sym}(M)$, and their components of degree t are denoted by $\bigwedge^t(M)$ and $\mathrm{Sym}_t(M)$. Let

$$\begin{array}{ccc}
G & \xrightarrow{\psi} & B \\
{\scriptstyle \phi}\downarrow & & \\
R & &
\end{array}$$

be a diagram of R-module homomorphisms. To make the algebra

$$\bigwedge G \otimes_R \mathrm{Sym}(B)$$

into a double complex with commuting differentials, we let

$$d_\phi = \partial : \quad \bigwedge^r G \otimes \mathrm{Sym}_t(B) \to \bigwedge^{r-1} G \otimes \mathrm{Sym}_t(B),$$

$$\partial(e_1 \wedge \cdots \wedge e_r \otimes w) = \sum (-1)^{r-i} e_1 \wedge \cdots \wedge \hat{e}_i \wedge \cdots \wedge e_r \otimes \phi(e_i) w;$$

$$d_\psi = \partial' : \quad \bigwedge^r G \otimes \mathrm{Sym}_t(B) \to \bigwedge^{r-1} G \otimes \mathrm{Sym}_{t+1}(B),$$

$$\partial'(e_1 \wedge \cdots \wedge e_r \otimes w) = \sum (-1)^{r-i} e_1 \wedge \cdots \wedge \hat{e}_i \wedge \cdots \wedge e_r \otimes \psi(e_i) \cdot w.$$

Changing our notation slightly, let $\mathbf{x} = \{x_1, \ldots, x_n\}$ be a generating set of the ideal I, and

$$\phi: \quad R^n \xrightarrow{[x_1, \cdots, x_n]} R,$$

where $[x_1, \cdots, x_n]$ denotes the mapping defined by the matrix. With this set-up, we are now ready to give the following definition.

Definition 5.9.25. The complex $\mathcal{L} = \mathcal{L}(\phi, \mathrm{id})$ shown below is called the **double Koszul complex** associated to the sequence $\mathbf{x}$.

$$\begin{array}{ccccc}
\bigwedge^{r+2}(R^n) \otimes \mathrm{Sym}_{t-1}(R^n) & \longrightarrow & \bigwedge^{r+1}(R^n) \otimes \mathrm{Sym}_t(R^n) & \longrightarrow & \bigwedge^{r}(R^n) \otimes \mathrm{Sym}_{t+1}(R^n) \\
\downarrow & & \downarrow & & \downarrow \\
\bigwedge^{r+1}(R^n) \otimes \mathrm{Sym}_{t-1}(R^n) & \longrightarrow & \bigwedge^{r}(R^n) \otimes \mathrm{Sym}_t(R^n) & \longrightarrow & \bigwedge^{r-1}(R^n) \otimes \mathrm{Sym}_{t+1}(R^n) \\
\downarrow & & \downarrow & & \downarrow \\
\bigwedge^{r}(R^n) \otimes \mathrm{Sym}_{t-1}(R^n) & \longrightarrow & \bigwedge^{r-1}(R^n) \otimes \mathrm{Sym}_t(R^n) & \longrightarrow & \bigwedge^{r-2}(R^n) \otimes \mathrm{Sym}_{t+1}(R^n)
\end{array}$$

The vertical complex, $\mathcal{L}(\phi)$, is the usual Koszul complex associated to the sequence $\mathbf{x}$ tensored with $S = \mathrm{Sym}(R^n) \cong R[T_1, \ldots, T_n]$, and the horizontal complex $\mathcal{L}(\partial')$ is the Koszul complex over the sequence $\mathbf{T} = \{T_1, \ldots, T_n\}$. We have the grading

$$\mathcal{L}_t = \sum_{r+s=t} \bigwedge^r (R^n) \otimes \mathrm{Sym}_s(R^n).$$

A key property is that the $\mathcal{L}_t$ are exact for $t > 0$, i.e.,

$$H_i(\mathcal{L}_t) = \begin{cases} R & \text{if } i = t = 0 \\ 0 & \text{otherwise.} \end{cases}$$

Given a sequence $\mathbf{x}$ and a R-module M, we can construct an associated double complex $\mathcal{L}(\mathbf{x}, M) = M \otimes \bigwedge(R^n) \otimes S$, where ∂ and ∂' are obtained by considering $\mathcal{L}(\mathbf{x}, M)$ as the Koszul complexes $\mathcal{K}^S(\mathbf{x}, M \otimes_R S)$ and $\mathcal{K}^S(\mathbf{T}, M \otimes_R S)$ respectively. Let $Z = Z(\mathbf{x}, M)$, $B = B(\mathbf{x}, M)$ and $H = H(\mathbf{x}, M)$ be the submodule of cycles, boundaries, and homologies of $\mathcal{K}(\mathbf{x}, M)$, then one can derive several other complexes listed below by the commutativity of ∂ and ∂' from $\mathcal{L}(\mathbf{x}, M)$. $\mathcal{Z}, \mathcal{B}, \mathcal{M}$ are called the **approximation complexes** associated to $\mathbf{x}$ and M.

$$\begin{aligned}
\mathcal{Z} &= \mathcal{Z}(\mathbf{x}, M) = \{Z \otimes S = Z \otimes \mathrm{Sym}(R^n),\ \partial'\}; \\
\mathcal{B} &= \mathcal{B}(\mathbf{x}, M) = \{B \otimes S = B \otimes \mathrm{Sym}(R^n),\ \partial'\}; \\
\mathcal{M} &= \mathcal{M}(\mathbf{x}, M) = \{H \otimes S = H \otimes \mathrm{Sym}(R^n),\ \partial'\}.
\end{aligned}$$

$\mathcal{M}$, $\mathcal{B}$, $\mathcal{Z}$ are complexes of graded modules over the ring $S = R[T_0, \ldots, T_n]$:

$$\mathcal{M}(\mathbf{x}, M): \quad 0 \to H_n \otimes S[-n] \to \cdots \to H_1 \otimes S[-1] \to H_0 \otimes S \to 0,$$

$$\mathcal{Z}(\mathbf{x}, M): \quad 0 \to Z_n \otimes S[-n] \to \cdots \to Z_1 \otimes S[-1] \to Z_0 \otimes S \to 0,$$

where H_i is the i-th homology, and Z_i is the cycles of $\mathcal{K}(\mathbf{x}, M)$. Moreover, $\mathcal{M}$ and $\mathcal{Z}$ are graded. The t-th homogeneous parts $\mathcal{M}_t$ and $\mathcal{Z}_t$ of $\mathcal{M}$ and $\mathcal{Z}$ respectively are the complexes of finitely generated R-modules with the degree one on the variables $T_1, \ldots, T_n$. They are written in the following forms:

$$\mathcal{M}_t: \quad 0 \to H_n \otimes S_{t-n} \to \cdots \to H_1 \otimes S_{t-1} \to H_0 \otimes S_t \to 0;$$

$$\mathcal{Z}_t: \quad 0 \to Z_n \otimes S_{t-n} \to \cdots \to Z_1 \otimes S_{t-1} \to Z_0 \otimes S_t \to 0.$$

First, we will interpret the vanishing of the homology of the $\mathcal{Z}$ and $\mathcal{M}$-complexes, and identify a few isomorphisms.

Theorem 5.9.26.

$$\begin{aligned} H_0(\mathcal{Z}(I, R)) &= \mathrm{Sym}(I), \\ H_0(\mathcal{M}(I, R)) &= \mathrm{Sym}(I/I^2). \end{aligned}$$

Proof. The first claim is obtained by considering the following two sequences

$$0 \to Z_1(\mathcal{K}) \to R^n \to I \to 0,$$

$$Z_1(\mathcal{K}) \otimes \mathrm{Sym}(R^n) \to Z_0(\mathcal{K}) \otimes \mathrm{Syz}(R^n) \to H_0(\mathcal{Z}(I, R)) \to 0.$$

And the similar method can prove the second claim. □

Hence, there are natural surjections:

$$H_0(\mathcal{Z}(I, R)) \to \mathrm{Rees}(I, M) = \oplus_j I^j M,$$

$$H_0(\mathcal{M}(I, R)) \to \mathrm{gr}_I(M) = \oplus_j I^j M / I^{j+1} M,$$

and they are isomorphic in degree zero.

Theorem 5.9.27 ([SV81])**.** *Let $H_i(\mathcal{Z}) := H_i(\mathcal{Z}(I, R))$ and $H_i(\mathcal{M}) := H_i(\mathcal{M}(I, R))$, then $H_i(\mathcal{Z})$ and $H_i(\mathcal{M})$ are independent of the generating set of the ideal I.*

If one considers the following two exact sequences:

$$0 \to \mathcal{Z}_t \to \mathcal{L}_t \to \mathcal{B}_{t-1}[-1] \to 0, \quad 0 \to \mathcal{B}_t \to \mathcal{Z}_t \to \mathcal{M}_t \to 0,$$

where $\mathcal{B}[-1]$ denotes the translation of $\mathcal{B}$ such that $\mathcal{B}[-1]_n = \mathcal{B}_{n-1}$. The first exact sequence gives the following long exact sequence

$$0 = H_{i+1}(\mathcal{L}_t) \to H_{i+1}(\mathcal{B}_{t-1}[-1]) \to H_i(\mathcal{Z}_t) \to H_i(\mathcal{L}_t) = 0, \quad \forall i \geq 1,$$

thus

$$H_{i+1}(\mathcal{B}_{t-1}[-1]) \cong H_i(\mathcal{B}_{t-1}) \cong H_i(\mathcal{Z}_t), \ \forall\, i \geq 1.$$

Apply this in the following long exact sequence induced by the second exact sequence

$$H_{i+1}(\mathcal{M}_t) \to H_i(\mathcal{B}_t) = H_i(\mathcal{Z}_{t+1}) \to H_i(\mathcal{Z}_t) \to H_i(\mathcal{M}_t), \quad \forall\, i > 0.$$

If $H_i(\mathcal{M}) = 0$ for $i \geq 1$, then $H_i(\mathcal{Z}_{t+1}) \cong H_i(\mathcal{Z}_t)$, and since $H_i(\mathcal{Z}_{-1}) = 0$, we have that

$$H_i(\mathcal{Z}_t) = 0, \ \forall\, t, \ \text{and} \ i \geq 1.$$

Since

$$\begin{aligned} H_0(\mathcal{B}_t) &= H_0(\mathcal{Z}_{t+1}) = \mathrm{Sym}_{t+1}(I), \\ H_0(\mathcal{Z}_t) &= \mathrm{Sym}_t(I), \\ H_0(\mathcal{M}_t) &= \mathrm{Sym}_t(I/I^2), \end{aligned}$$

we have the following sequence

$$H_1(\mathcal{M}_t) \xrightarrow{\sigma} \mathrm{Sym}_{t+1}(I) \xrightarrow{\lambda} \mathrm{Sym}_t(I) \to \mathrm{Sym}_t(I/I^2) \to 0,$$

and the commutative diagram

$$\begin{array}{ccccccccc} H_1(\mathcal{M}_t) & \xrightarrow{\sigma} & H_0(\mathcal{Z}_{t+1}) & \xrightarrow{\lambda} & H_0(\mathcal{Z}_t) & \longrightarrow & H_0(\mathcal{M}_t) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha_{t+1}} & & \downarrow{\scriptstyle \alpha_t} & & \downarrow{\scriptstyle \beta_t} & & \\ 0 & \longrightarrow & I^{t+1}M & \longrightarrow & I^tM & \longrightarrow & I^tM/I^{t+1}M & \longrightarrow & 0. \end{array}$$

Theorem 5.9.28 (Corollary 4.6 and Theorem 4.7, [HSV83b])**.** *Suppose that R is a Noetherian ring.*

1. *If $H_i(\mathcal{M}) = 0$ for all $i \geq 1$, then $H_i(\mathcal{Z}) = 0$. $\mathcal{M}$ is acyclic if and only if $\mathcal{Z}$ is also acyclic and λ is an injection.*

2. *σ is a zero map if and only if λ is injective if and only if α is isomorphic.*

Bibliography

[AB57] M. Auslander and D. Buchsbaum, *Homological dimension in local rings*, Trans. Am. math. Soc. **85** (1957), 390–405.

[Ago05] Max K. Agoston, *Computer Graphics and Geometric Modeling: Mathematics*, Springer Verlag, New York, 2005.

[AHW05] W. Adkins, J. W. Hoffman, and H. Wang, *Equations of parametric surfaces with base points via syzygies*, Journal of Symbolic Computation **39** (2005), 73–101.

[AM97] M. F. Atiyah and I. G. MacDonald, *Introduction to Commutative Algebra*, Addision-Wesley Publishing Company, 1997.

[BC05] L. Busé and M. Chardin, *Implicitizing rational hypersurfaces using approximation complexes*, J. Symb. Comp. **40** (2005), 1150–1168.

[BCD03] L. Busé, D. Cox, and C. D'Andrea, *Implicitization of surfaces in $\mathbb{P}^3$ in the presence of base points*, Journal of Algebra and its Applications **2** (2003), 180–214.

[BCS10] L. Busé, M. Chardin, and A. Simis, *Elimination and nonlinear equations of Rees algebra*, Journal of Algebra **324** (2010), no. 6, 1314–1333.

[BD10] T. C. Benítez and C. D'Andrea, *Minimal generators of the defining ideal of the Rees algebra associated to monoid parametrizations*, Computer Aided Geometric Design **27** (2010), no. 6, 461–473.

[BE73] D. Buchsbaum and D. Eisenbud, *What makes a complex exact?*, Journal of Algebra **25** (1973), 259–268.

[BH93] W. Bruns and J. Herzog, *Cohen-Macaulay Rings*, Cambridge studies in advanced mathematics, Cambridge University Press, Cambridge, UK, 1993.

[BJ03] L. Busé and J-P. Jouanolou, *On the closed image of a rational map and the implicitization problem*, J. Algebra **265** (2003), 312–357.

[BM93] D. Bayer and D. Mumford, *What can be computed in algebraic geometry*, Computational Algebraic Geometry and Commutative Algebra (1993), 1–48.

[Bot11] N. Botbol, *The implicit equation of a multigraded hypersurface*, J. Algebra **348** (2011), 381–401.

[BP09] V. Blanco and J. Puerto, *Partial Gröbner bases for multiobjective integer linear optimization*, J. Discrete Math **23** (2009), no. 2, 571–595.

[BS87] D. Bayer and M. Stillman, *A criterion for detecting m-regularity*, Invent. Math. **87** (1987), 1–11.

[Buc85] B. Buchberger, *Gröbner bases: An Algorithmic Method in Polynomial Ideal Theory*, Multidimensional Systems Theory, N.K. Bose, ed., D. Reidel Publ. Co., 1985.

[Bus06] L. Busé, *Elimination theory in codimension one and applications*, INRIA **5918** (2006), 1–47.

[Bus09] ———, *On the equations of the moving curve ideal of a rational algebraic plane curve*, J. Algebra **321** (2009), 2317–2344.

[BW93] T. Becker and V. Weispfenning, *Gröbner bases: A computational approach to commutative algebra*, Springer-Verlag, 1993.

[Cay65] A. Cayley, *On the theory of elimination*, Cambridge and Dublin Mathematical Journal **III** (1865), 210–270.

[CGZ00] D. A. Cox, R. N. Goldman, and M. Zhang, *On the validity of implicitization by moving quadrics for rational surfaces with no base points*, J. Symb. Comput. **29** (2000), 419–440.

[Cha93] M. Chardin, *The resultant via Koszul complex*, Computational Algebraic Geometry (Proc. of MEGA) (1993), 29–39.

[Cha06] ———, *Implicitization using approximation complexes*, Algebraic Geometry and Geometric Modeling Mathematics and Visualization (2006), 23–35.

[CHW08] D. Cox, J. W. Hoffman, and H. Wang, *Syzygies and the Rees algebra*, J. Pure Appl. Algebra **212** (2008), 1787–1796.

[Cla04] J. Clark, *Elementary Gröbner basis theory*, Missouri Journal of Mathematical Sciences **16** (2004), 1–20.

[CLO95] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms*, Undergraduate Texts in Mathematics, vol. 150, Springer-Verlag, 1995.

[CLO98] ———, *Using Algebraic Geometry*, Graduate Texts in Mathematics, vol. 185, Springer-Verlag, 1998.

[CM96] J. P. Cardinal and B. Mourrain, *Algebraic approach of residues and applications*, In J. Renegar, M. Shub and S. Smale Editors, The Mathematics of Numerical Analysis **32** (1996), 189–210.

[Cox01a] D. Cox, *Equations of parametric curves and surfaces via syzygies*, Contemporary Mathematics **286** (2001), 1–20.

[Cox01b] D. A. Cox, *Equations of parametric curves and surfaces via syzygies*, Contemporary Mathematics **286** (2001), 1–20.

[Cox08] D. Cox, *The moving curve ideal and the Rees algebra*, Theoret. Comput. Sci. **392** (2008), 23–36.

[CSC98] D. A. Cox, T. Sederberg, and F. Chen, *The moving line ideal basis of planar rational curves*, Comput. Aided Geom. Des. **15** (1998), 803–827.

[CT91] P. Conti and C. Traverso, *Buchberger Algorithm and Integer Programming*, In: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC-9) (Mattson, et. al, eds.) Lecture Notes in Computer Science, vol. 539, Springer-Verlag, New York, 1991.

[D'A01] C. D'Andrea, *Resultants and moving surfaces*, J. Symbolic Comput. **31** (2001), 585–602.

[Dix08] A. L. Dixon, *The eliminant of three quantics in two independent variables*, Proc. London Mathematical Society **6** (1908), 468–478.

[EG84] D. Eisenbud and S. Goto, *Linear free resolution and minimal multiplicity*, J. Algebra **88** (1984), 89–133.

[Eis95] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, 1995.

[Eis05] ———, *The Geometry of Syzygies: A second course in commutative algebra and algebraic geometry*, Graduate Texts in Mathematics, no. 229, Springer -Verlag, New York, 2005.

[EM96] M. Elkadi and B. Mourrian, *Approche Effective des Résidus Algébriques*, Rapport de Recherch 2884, INRIA, 1996.

[Fit36] H. Fitting, *Die determinantenideale eines moduls*, Jahresbericht Deutsch. Math.-Verein **46** (1936), 195–228.

[GG91] A. Geramita and A. Gimilgliano, *Generators for the defining ideal of certain rational surfaces*, Duke Math. J. **62** (1991), 61–83.

[GH78] P. Griffiths and J. Harris, *On Cayley's explicit solution to Poncelet's porism*, Enseign. Math. **24** (1978), 31–40.

[Gia88] Zacharias Gianni, Trager, *Gröbner bases and primary decomposition of polynomial ideals*, J. Symbolic Computation **6** (1988), 149–167.

[GKZ94] I. M. Gel'fand, M. Kapranov, and A. Zelvinsky, *Discriminants, Resultants, and Multidimensional Determinants: Theory and Applications*, Birkhäuser Boston, Inc., Boston, MA, 1994.

[GPS01] G.-M. Greuel, G. Pfister, and H. Schönemann, SINGULAR *2.0*, A computer algebra system for polynomial computations, Centre for Computer Algebra, University of Kaiserslautern, 2001, `http://www.singular.uni-kl.de`.

[Har97] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, vol. 52, Springer, New York, 1997.

[HSV82] J. Herzog, A. Simis, and W. Vasconcelos, *Approximation complexes of blowing-up rings*, J. Algebra **74** (1982), no. 2, 466–493.

[HSV83a] ———, *Approximation complexes of blowing-up rings. ii*, J. Algebra **82** (1983), no. 1, 53–83.

[HSV83b] ———, *Koszul homology and blowing-up rings*, Commutative algebra (Trento, 1981) **84** (1983), 79–169.

[HSV08] J. Hong, A. Simis, and W. Vasconcelos, *On the homology of two-dimensional elimination*, J. Symb. Comp. **43** (2008), 275–292.

[HW14] J. W. Hoffman and H. Wang, *A note on quadratically parametrized surfaces*, Algebra Colloquium **21** (2014), no. 3, 461–476.

[KM76] F. F. Knudsen and D. Mumford, *The projectivity of the moduli space of stable curves. I. Preliminaries on "det'' and ''Div"*, Math. Scand. **39** (1976), 19–55.

[KS95] D. Kapur and T. Saxena, *Comparison of various multivariate resultant formulations*, Proceedings of International Symposium on Symbolic and Algebraic Computation (ISSAC'95) (1995), 87–194.

[Las05] E. Lasker, *Zur Theorie der Moduln und Ideale*, Math. Ann. **60** (1905), 19–116.

[Lin99] Z. Lin, *On syzygy modules for polynomial matrices*, Linear Algebra and its Applications **298** (1999), 73–86.

[LXW04] Zhiping Lin, Li Xu, and Qinghe We, *Applications of Gröbner bases to signal and image processing: a survey*, Linear Algebra and its Applications **391** (2004), 169–202.

[Mac23] F. C. Macaulay, *Note on the resultant of a number of polynomials of the same degree*, Proc. London Math. Soc. **21** (1923), 14–21.

[Mac65] R. E. MacRae, *On an application of Fitting invariants*, J. Algebra **2** (1965), no. 2, 153–169.

[Mac71] ———, *Annihilators of modules with a finite free resolution*, Proc. Am. Math. Soc. **29** (1971), 440–442.

[Mum66] D. Mumford, *Lectures on curves on an algebraic surface*, Princeton University Press, Princeton, New Jersey, 1966.

[Noe21] E. Noether, *Idealtheorie in Ringbereichen*, Mathematische Annalen **83** (1921), no. 1, 24.

[Ooi82] A. Ooishi, *Castelnuovo's regularity of graded rings and modules*, Hiroshima Math. J. **12** (1982), 627–644.

[Sak10] Y. Sakai, *Construction of genus two curves with real multiplication by Poncelet's theorem*, Ph.D. thesis, Waseda University, 2010.

[SC95] T. W. Sederberg and F. Chen, *Implicitization using moving curves and surfaces*, Proceeding of SIGGRAPH (1995), 301–308.

[SL05] W. Sun and H. Li, *On the construction of generic mixed Cayley-Sylvester resultant matrix*, MM Research Preprints, KLMM, AMSS, Academia Sinica **24** (2005), 117–130.

[Sta99] R. Stanley, *Enumerative Combinatorics*, Cambridge University Press, 1999.

[Stu98] B. Sturmfels, *Introduction to resultanst*, Proceedings of Symposia in Applied Mathematics **39** (1998), 25.

[SV81] A. Simis and W. Vasconcelos, *The syzygies of the conormal module*, Amer. J. Math. **103** (1981), 203–224.

[SY96] T. Shimoyama and K. Yokoyama, *Localization and primary decomposition of polynomial ideals*, J. Symb. Comp. **22** (1996), 247–277.

[TB93] V. Weispfenning T. Bekcer, H. Kredel, *Gröbner Bases*, Springer, Berlin Heidelberg New YorK, 1993.

[UM12] Thomas Uchida and John McPhee, *Using Gröbner bases to generate efficient kinematic solutions for the dynamic simulation of multi-loop mechanisms*, Mechanism and Machine Theory **52** (2012), 144–157.

[Val80] G. Valla, *On the symmetric and Rees algebras of an ideal*, Manuscripta Math. **30** (1980), 239 – 255.

[Wae95] L. Van Der Waerden, *Modern Algebra*, 3rd ed., F. Ungar Publishing Co. New York, 1995.

[Wei95] Charles A. Weibel, *An Introduction to Homological Algebra*, Cambridge Studies in Advanced Mathematics, 38, Cambridge University Press, 1995.

[Wol15] Wolfram, *Mathematica*, 10.3 ed., Wolfram Research, Inc., Champaign, Illinois, 2015, `https://www.wolfram.com`.

Index