University of Zurich

Master Thesis

Castelnuovo–Mumford Regularity and the Complexity of Gröbner Basis Algorithms

Author:
Andreia Venzin

Supervisor:
Professor Dr. Joachim Rosenthal

Co-supervisor:
Dr. Karan Khathuria

Universität Zürich[UZH]

Faculty of Science
Department of Mathematics

March 3, 2021

Abstract

Solving systems of polynomial equations in multiple variables is a classical problem in various areas of mathematics. The solutions of such a system can be obtained from the lexicographic Gröbner basis of the ideal generated by the polynomials of the system. An important application originates from multivariate public-key cryptosystems, whose security is based on the hardness of solving such systems. Thus, estimating the complexity of Gröbner basis algorithms is central in the security analysis of multivariate cryptosystems.
Many Gröbner basis algorithms base the computation on Gaussian elimination of so-called Macaulay matrices. Under certain assumptions, the complexity-estimation of such algorithms can be done by means of an algebraic invariant called Castelnuovo–Mumford regularity.
However, due to the use of concepts from several different areas of mathematics and a lot of preliminaries, many research papers regarding this topic have a high entry-level, and are not easily accessible to many students even at a master level.
The purpose of this thesis is to collect the background information and give an overview of the different mathematical topics and underlying concepts needed in the theory of Gröbner bases and Castelnuovo–Mumford regularity. Furthermore, we show how to connect the complexity of Gröbner basis algorithms and Castelnuovo–Mumford regularity. Finally, we compare this approach with a similar concept called the degree of regularity that is often used in literature.

Acknowledgements

First and foremost, I would like to thank the supervisor of this thesis, Professor Dr. Joachim Rosenthal, for enabling me to write my master thesis on such a current and interesting topic. I'm extremely thankful for the many interesting lectures he and his team held during my time at the university.

Furthermore, I wish to express my sincere gratitude to Dr. Karan Khaturia, for his continuous enthusiasm, patience and support. He was always available for discussions, when I needed help or raised concerns. It was a pleasure to have him as a co-supervisor.

Also, I am very grateful to my fellow students, for creating a great atmosphere to study and discuss mathematics over the years.

Finally, I am deeply grateful to my friends and family for their unconditional support. Without them, this thesis would not have been possible.

Thank you!

Contents

Abstract **i**

Acknowledgements **ii**

1 Introduction **1**
1.1 Background . . . 1
1.2 Notation . . . 3

2 Ideals and Modules **4**
2.1 Ideals . . . 4
2.1.1 Basics . . . 4
2.1.2 Noetherian Rings . . . 8
2.1.3 Primary Decomposition . . . 9
2.1.4 Localization . . . 12
2.2 Modules . . . 15
2.2.1 Basics . . . 15
2.2.2 Noetherian Modules . . . 17
2.2.3 Associated Primes . . . 18
2.3 Graded Rings and Modules . . . 20
2.4 Krull Dimension . . . 24
2.4.1 The Ungraded Case . . . 24
2.4.2 The Graded Case . . . 25
2.5 Monomials and Monomial Ideals . . . 26
2.5.1 Monomials and Polynomials . . . 26
2.5.2 Monomial Ideals . . . 28

3 Homological Algebra **31**
3.1 Exact Sequences . . . 31
3.2 Free Resolutions . . . 35
3.3 Injective Resolutions . . . 39
3.4 Local Cohomology . . . 43

4 Algebraic Geometry **49**
4.1 Affine Space . . . 49
4.2 Projective Space . . . 53
4.3 Homogenization and Dehomogenization . . . 56
4.4 Zariski Topology . . . 58
4.5 Dimension of Varieties . . . 60

5 Gröbner Bases **65**
5.1 Monomial Orders . . . 65
5.2 Gröbner Bases . . . 70
5.3 Buchberger's Algorithm . . . 73

5.4 Extending Monomial Orders and Homogeneous Gröbner Bases 77
5.5 Solving Systems with Finitely Many Solutions 79
5.6 Macaulay Matrices 82
5.7 Gröbner Bases for Modules 86

6 Hilbert Function **93**
6.1 Hilbert Function for Ideals 93
6.1.1 The Affine Hilbert Function 93
6.1.2 The Projective Hilbert Function 95
6.1.3 Hilbert Polynomial and Krull Dimension 97
6.2 Hilbert Function for Modules 100

7 Castelnuovo–Mumford Regularity **104**
7.1 Definition and Properties of Regularity 104
7.2 Criterion for m-regularity 110

8 Complexity of Gröbner Basis Algorithms **113**
8.1 Generic Initial Ideals 113
8.2 Solving Degree 117
8.3 Degree of Regularity 120
8.4 First Fall Degree 125

Bibliography **127**

A Appendix **130**
A.1 Zorn's Lemma 130
A.2 Inclusion-Exclusion Principle 130
A.3 Proof of Generic Initial Ideals 130

Chapter 1

Introduction

1.1 Background

Solving polynomial systems has been an important problem in various parts of mathematics such as coding theory or cryptography. The problem itself can be formulated as follows.

PoSSo Problem (Polynomial System Solving): *Given a system of non-linear polynomials* $\mathcal{F} = \{f_1, \ldots, f_r\} \subseteq k[x_1, \ldots, x_n]$ *find values* $a_1, \ldots, a_n \in k$ *s.t.*

$$f_1(a_1, \ldots, a_n) = \cdots = f_r(a_1, \ldots, a_n) = 0.$$

The PoSSo problem is proven to be NP-hard even in the simplest cases of quadratic polynomials [28]. This thesis is motivated by the PoSSo problem in the context of multivariate cryptography. While the security of communication has been important for many centuries, the rise of the internet and digital communication has increased the need for such secure communication by a lot and will likely increase further in the future.

Nowadays, the security of many cryptosystems is based on the difficulty of factoring integers or solving the discrete logarithm problem like RSA [44] or ECC [39], respectively. However, with the construction of quantum computers in the future, solving those problems will eventually become feasible, respectively, these systems will become insecure. Multivariate cryptography on the other hand is (still) believed to be a secure alternative against attacks from quantum computers and is therefore of big interest in research. For example, the Rainbow Signature Scheme proposed by J. Ding and D. Schmidt [17] is considered by the National Institute of Standards and Technology (NIST) as a post-quantum cryptographic scheme for standardization.

In a Multivariate Public Key Cryptosystem (MPKC), the standard method to construct the public key is to the compose a polynomial system $\mathcal{F}$ that is easy to solve with two affine invertible maps $\mathcal{S}$ and $\mathcal{T}$ to get the public key $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$. For a given plaintext $\mathbf{m} = (m_1, \ldots, m_n)$ one computes the ciphertext $(c_1, \ldots, c_r) = \mathbf{c} = \mathcal{P}(\mathbf{m}) = (p_1(\mathbf{m}), \ldots, p_r(\mathbf{m}))$ [19].
One way for an attacker to recover the original plaintext $\mathbf{m}$ from $\mathbf{c}$ that is always possible against such systems is the *direct* resp. *algebraic* attack. There, the plaintext $\mathbf{m}$ is recovered by solving the polynomial system:

$$\begin{aligned} 0 &= c_1 - p_1(x_1, \ldots, x_n) \\ &\vdots \\ 0 &= c_r - p_r(x_1, \ldots, x_n) \end{aligned}$$

Thus, for the security analysis of such systems, it is important to be able to estimate the complexity of solving the system $\mathcal{P}$ directly.

A key contribution to tackling the PoSSo problem has been the introduction of the concept of Gröbner basis in 1965, by Bruno Buchberger in his PhD thesis [9]. A Gröbner basis G of an ideal I that is generated by multivariate polynomials, is a set of generators of I that has the property

that the initial monomials of G generate the same ideal as the initial monomials of all elements of the ideal I. These bases have a lot of useful properties and are helpful in many problems regarding algebraic properties of polynomial ideals and their affine varieties [15]. A central property concerning the PoSSo problem is that from a lexicographic Gröbner basis of a polynomial ideal, the solutions of the associated system can be obtained. Buchberger introduced the first algorithm to compute such bases, by adding certain elements to the original set of polynomials, until it is a Gröbner basis. Computationally this is not very efficient and numerous improvements have been made and new algorithms created. One class of such algorithms are those that base the computation of a Gröbner basis on Gaussian elimination of Macaulay matrices. If these matrices are chosen large enough, Gaussian elimination yields a Gröbner basis [49].

The complexity of these algorithms can be described by the solving degree, which depends on the size of these matrices [11]. Since the minimal size of the Macaulay matrix that is needed is not known beforehand, having upper bounds on the solving degree is very useful in estimating the complexity.

A. Caminata and E. Gorla have shown in [11] that in generic coordinates it is possible to bound the solving degree of a system of polynomials $\mathcal{F} = \{f_1, \dots, f_r\}$ with finitely many projective solutions by the Castelnuovo–Mumford regularity of the ideal $\langle f_1^h, \dots, f_r^h \rangle$, generated by the homogenized polynomials. To be in generic coordinates informally means that a random linear change of coordinates has been applied, which usually is the case for public keys in MPKCs.

The concept of Castelnuovo–Mumford regularity was first introduced in 1966 by D. Mumford [40] in the context of coherent sheaves based on ideas in the work of G. Castelnuovo [12] in 1893. It has since been adapted to commutative algebra, where it can be seen as a measure of how complicated an ideal generated by homogeneous elements, is in terms of its minimal free resolution

$$0 \to F_p \to \cdots \to F_1 \to F_0 \to I \to 0.$$

There exists another equivalent definition in terms of local cohomology, where the regularity is the smallest positive integer $m \in \mathbb{Z}_{\geq 0}$ s.t. the degree-d-component of the i-th local cohomology module vanishes for all $d \geq m - i + 1$.
By obtaining bound for the Castelnuovo–Mumford regularity, we then also get bounds for the solving degree.

This area of research is important and will likely become increasingly important in the future. However, since it combines concepts and results from several different areas, research papers on this subject often have a high entry-level and require a lot of preliminary results. Thus, despite being very interesting, they are not easily accessible to many students, even at a graduate level. This thesis is devoted to providing a mostly self-contained overview of the theoretical background required w.r.t Gröbner basis theory and Castelnuovo–Mumford regularity. Moreover, we recover some of the main results of the paper of A. Caminata and E. Gorla [11].

The remainder of this thesis is divided into seven chapters and is organized as follows.

Chapter 2 summarizes fundamental material regarding polynomials and ideals. First, in Section 2.1 we give basic results about ideals and present the concepts of localization and primary decomposition. In Section 2.2 we recall the notion of modules and some of the most important facts about them. Section 2.3 is dedicated to graded rings and modules. After introducing the concepts of Krull dimension in Section 2.4, we focus on monomial ideals in Section 2.5.

Chapter 3 offers an introduction to homological algebra. We start in Section 3.1, with introducing exact sequences and some useful results like the snake lemma. Then, in Section 3.2 we present free resolutions and look at how to obtain them. Section 3.3 deals with injective resolutions. Section 3.4 contains the concept of the I-torsion functor, which is then used to define the notion of local cohomology.

Chapter 4 offers a presentation of the most important notions of algebraic geometry. Section 4.1 handles varieties in the affine space and contains fundamental results like the Nullstellensatz.

In Section 4.2 we adapt the concepts from the previous section to the projective space. The relationship between affine and projective space is explained in Section 4.3, where we study the concept of homogenization and dehomogenization. The notion of Zariski topology is the topic of Section 4.4. The last section of Chapter 4 introduces the dimension of affine and projective varieties.

Chapter 5 is devoted to the study of Gröbner basis theory. It begins with Section 5.1, where we introduce monomial orders and initial ideals. Also, we present the division algorithm for multivariate polynomials. In Section 5.2, Gröbner bases are defined and we present their properties and how to obtain them with Buchberger's algorithm. Section 5.3 explores the connection between Gröbner bases and their homogenization resp. dehomogenization and we show that for certain monomial orders, homogenizing a Gröbner basis yields the Gröbner basis of the homogenized ideal. Section 5.4 consists of elimination theory and studies how it can be used to solve systems with finitely many solutions over the algebraic closure. In Section 5.5 Macaulay matrices are defined and a basic algorithm to compute a Gröbner basis by doing Gaussian elimination on them is presented. We conclude Chapter 5 with Section 5.6, where we generalize the concept of Gröbner bases to the setting of modules and restate some of the results in this context, since they are used in the proof of the Hilbert syzygy theorem.

We continue with Chapter 6, where we introduce the Hilbert function and Hilbert polynomials. In Section 6.1 we do so in the context of ideals and relate it to the notions of Krull dimension Section 6.2 generalizes the Hilbert function to modules and we show some important results.

Chapter 7 is dedicated to the notion of Castelnuovo–Mumford regularity. In Section 7.1 we combine previous results, to define Castelnuovo–Mumford regularity by means of minimal graded free resolutions. Moreover, we show the equivalence to a definition based on local cohomology and present some useful properties. In Section 7.2 we present a criterion for m-regularity.

Chapter 8 is the final theoretical chapter and connects results from previous chapters and is overall concerned with the complexity of Gröbner basis algorithms. First, Section 8.1 deals with the regularity of the generic initial ideal w.r.t the degree-reverse lexicographic order. In Section 8.2 we introduce the notion of solving degree and show how it can be bounded by regularity. Section 8.3 introduces two other notions that are frequently used in literature to estimate complexity and show their relation to the solving degree.

1.2 Notation

For this thesis, it is assumed that the reader is familiar with basic mathematical concepts such as *rings*, *ideals* and *modules*. Otherwise, this material can be looked up in many introductory books like [26]. Throughout this thesis the following notation is frequently used:

- $\mathbb{Z}$ denotes the ring of integers.
- $\mathbb{Q}$ denotes the field of rational numbers.
- $\mathbb{R}$ denotes the field of real numbers.
- R denotes an arbitrary commutative ring with identity element 1.
- k denotes an arbitrary field.
- $\bar{k}$ denotes the algebraic closure of the field k.
- $k[x_1, \ldots, x_n]$ denotes the ring of polynomials with coefficients in k and variables $x_1, \ldots, x_n$.
- $\mathbb{F}_q$ denotes a finite field with q elements.
- $\mathrm{Hom}_R(A, B)$ denotes the set of all R-module homomorphisms from A to B.

Chapter 2

Ideals and Modules

This chapter contains mostly basic results about ideals and modules that become useful tools in later chapters. We start by recalling some definitions and concepts regarding ideals that are used throughout the thesis. We continue by giving some fundamental background on modules and then introduce the notion of graded rings and modules. After giving a short introduction to the concept of Krull dimension, we conclude the chapter by looking at monomial ideals.

2.1 Ideals

This fundamental introduction about ideals is mainly based on the contents of [46, Chapters 2–5] and [2, Chapters 1 and 4]

2.1.1 Basics

Definition 2.1.1. Let R be a commutative ring. A subset $I \subseteq R$ is called an *ideal* of R when the following conditions are satisfied:

(a) $0 \in I$,

(b) if $a, b \in I$, then $a + b \in I$,

(c) if $a \in I$ and $r \in R$, then $ra \in I$.

Given elements $a_\lambda \in R$, $\lambda \in \Lambda$ for a set of indices Λ, the ideal $\langle a_\lambda \rangle_{\lambda \in \Lambda}$ is defined to be the set of all finite linear combinations $\sum_{\lambda \in \Lambda} r_\lambda a_\lambda$ with $r_\lambda \in R$, which is equal to the smallest ideal containing all the generators a_λ. If Λ is finite, e.g. $\Lambda = \{1, \ldots, n\}$, one writes $I = \langle a_1, \ldots, a_n \rangle$ and I is called *finitely generated*.

Let I, J be ideals in R. We recall some of the most basic operations on ideals:

- Intersection: $I \cap J = \{c \in R : c \in I \text{ and } c \in J\}$.
- Addition: $I + J = \{a + b \in R : a \in I \text{ and } b \in J\}$.
- Product: $IJ = \{\sum_{i=1}^{n} a_i b_i : n \in \mathbb{N},\ a_i \in I \text{ and } b_i \in J \text{ for all } i = 1, \ldots, n\}$.
- Colon ideal: $(I : J) = \{r \in R \ : \ r \cdot J \subseteq I\}$, where $r \cdot J = \{r \cdot b \ : \ b \in J\}$.

If $R \subseteq S$ is a ring extension and I is an ideal in R, then $IS \subseteq S$ denotes the ideal of S generated by the set I.

Next, we recall some important types of ideals.

Definition 2.1.2. An ideal $\mathfrak{p} \subseteq R$ is called *prime* if $1 \notin \mathfrak{p}$ and $xy \in \mathfrak{p}$ implies $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$ for all $x, y \in R$. The set of all prime ideals of R is called the *spectrum of* R denoted by $\operatorname{Spec}(R)$.
An ideal $\mathfrak{m} \subseteq R$ is called *maximal* if $1 \notin \mathfrak{m}$ and there is no other proper ideal I of R s.t. $\mathfrak{m} \subsetneq I$.

The following facts are well known but also very important:

(a) An ideal $\mathfrak{p}$ is prime if and only if $R/\mathfrak{p}$ is an integral domain.

(b) An ideal $\mathfrak{m}$ is maximal if and only if $R/\mathfrak{m}$ is a field.

The following result turns out to be very useful and will be used frequently throughout the remaining thesis.

Proposition 2.1.3 ([2], Proposition 1.11)**.**

(a) *Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \operatorname{Spec}(R)$. Let I be an ideal of R s.t. $I \subseteq \bigcup_{i=1}^n \mathfrak{p}_i$. Then $I \subseteq \mathfrak{p}_i$ for some i.*

(b) *Let $I_1, \ldots, I_n$ be ideals of R and let $\mathfrak{p} \in \operatorname{Spec}(R)$ s.t. $\bigcap_{i=1}^n I_i \subseteq \mathfrak{p}$. Then $I_i \subseteq \mathfrak{p}$ for some i. If $\mathfrak{p} = \bigcap_{i=1}^n I_i$, then $\mathfrak{p} = I_i$ for some i.*

Proof. (a) We prove the contrapositive by induction on n:

$$I \nsubseteq \mathfrak{p}_i,\ i = 1, \ldots, n \implies I \nsubseteq \bigcup_{i=1}^n \mathfrak{p}_i.$$

The statement clearly holds for $n = 1$. Let $n > 1$ and assume the result holds for $n - 1$. By induction hypothesis we have that for each $i = 1, \ldots, n$ there is $x_i \in I$ s.t. $x_i \notin \mathfrak{p}_j$ for all $j \neq i$. If $x_i \notin \mathfrak{p}_i$ for some i, the statement follows. Otherwise, we have that $x_i \in \mathfrak{p}_i$ for all i. Then, for

$$y = \sum_{i=1}^n x_1 x_2 \cdots x_{i-1} x_{i+1} x_{i+2} \cdots x_n$$

we have that $y \in I$ but $y \notin \mathfrak{p}_i$ for $i = 1, \ldots, n$. Thus, $I \nsubseteq \bigcup_{i=1}^n \mathfrak{p}_i$.

(b) If $I_i \nsubseteq \mathfrak{p}$ for $i = 1, \ldots, n$, then there are elements $x_i \in I_i$ s.t. $x_i \notin \mathfrak{p}$ for all i. Thus, $\prod_{i=1}^n x_i \in \prod_{i=1}^n I_i \subseteq \bigcap_{i=1}^n I_i$. But on the other hand $\prod_{i=1}^n x_i \notin \mathfrak{p}$, since $\mathfrak{p}$ is prime. Thus, $\bigcap_{i=1}^n I_i \nsubseteq \mathfrak{p}$. Now, if $\bigcap_{i=1}^n I_i = \mathfrak{p}$, then $\mathfrak{p} \subseteq I_i$ for all i and therefore $\mathfrak{p} = I_i$ for some i, which concludes the proof. □

An important kind of ideals are those in quotient rings, but they behave rather well.

Theorem 2.1.4 ([46], Theorem 2.37)**.** *Let I be an ideal of R.*

(a) *If J is an ideal s.t. $I \subseteq J$, then J/I is an ideal of R/I. Also, $r + I \in J/I$ if and only if $r \in J$.*

(b) *Any ideal $\bar{J}$ of R/I can be expressed as J/I for exactly one ideal J of R s.t. $I \subseteq J$.*

Proof. (a) Clearly, $J/I \subseteq R/I$ s.t. J/I is an additive subgroup of R/I. Also, for all $r \in R$ and $a \in J$ one has that $(r + I)(a + I) = ra + I \in J/I$. Thus, J/I is an ideal of R/I. If $r \in R$ s.t. $r + I = j + I$ for some $j \in J$, then $r = (r - j) + j$ and $r - j \in J$. Thus, $r \in J$.

(b) Consider $J = \{a \in R :\ a + I \in \bar{J}\}$ for an ideal $\bar{J}$ of R/I. Clearly, $I \subseteq J$. Let $a, b \in J$ and $r \in R$. Then $a + I, b + I \in \bar{J}$ s.t. $(a + b) + I, ra + I \in \bar{J}$. Therefore, $a + b, ra \in J$, so J is an ideal of R. Thus, $J/I = \bar{J}$. Suppose that there is a different ideal K of R s.t. $I \subseteq K$ and $K/I = \bar{J}$. Let $a \in K$, then $a + I \in K/I = \bar{J}$ and so $a \in J$ by definition of J. Conversely, let $b \in J$. Then $b + I \in \bar{J} = K/I$ and (a) implies that $b \in K$. It follows that $J = K$. □

The previous result allows us to look at prime ideals in quotient rings.

Lemma 2.1.5 ([46], Lemma 3.28)**.** *Let $I \subseteq R$ be an ideal and let $J \subseteq R$ be an ideal with $I \subseteq J$. Then $J/I \in \mathrm{Spec}(R/I)$ if and only if $J \in \mathrm{Spec}(R)$.*

Proof. By the well known isomorphism theorem for commutative rings one has

$$(R/I)/(J/I) \cong R/J,$$

where one is an integral domain if and only if the other one is. So the result follows. □

Next, we introduce two frequently used but easy ways to obtain new ideals.

Definition 2.1.6. Let I, J be ideals of R. The *saturation* of I w.r.t J is the ideal

$$I_J^{sat} = (I : J^\infty) = \bigcup_{n \geq 1} (I : J^n) = \{f \in R : fJ^n \subseteq I \text{ for some } n \geq 1\}.$$

The *radical of* I is the defined to be set

$$\sqrt{I} = \{a \in R : a^m \in I \text{ for some } m \geq 1\}.$$

An ideal I is said to be a *radical ideal* if $\sqrt{I} = I$. The set $\mathrm{Nil}(R) = \sqrt{\langle 0 \rangle}$ is called the *nilradical* of R and consists of all nilpotent elements of R.

The radical of an ideal satisfies some simple but useful properties.

Lemma 2.1.7 ([46], Lemma 3.46)**.** *Let I be an ideal. Then $\sqrt{I}$ is an ideal containing I.*

Proof. Clearly, $I \subseteq \sqrt{I}$ and $ra \in \sqrt{I}$ for all $r \in R$, $a \in \sqrt{I}$. Let $a, b \in \sqrt{I}$, i.e. $a^n, b^m \in I$ for some $m, n \in \mathbb{N}$. Thus,

$$(a+b)^{n+m-1} = \sum_{i=0}^{n+m-1} \binom{n+m-1}{i} a^{n+m-1-i} b^i.$$

But for all $i = 0, \ldots, n+m-1$ we either have $n+m-1-i \geq n$ or $i \geq m$, s.t. either $a^{n+m-1-i} \in \sqrt{I}$ or $b^i \in \sqrt{I}$. Thus, $(a+b)^{n+m-1} \in I$ and $a+b \in \sqrt{I}$. □

Lemma 2.1.8 ([15], Proposition 16, Chapter 4.3)**.** *Let I, J be ideals of R. Then $\sqrt{IJ} = \sqrt{I \cap J}$.*

Proof. ($\subseteq$) This is immediate as $IJ \subseteq I \cap J$.

($\supseteq$) Let $f \in \sqrt{I \cap J}$, so $f^m \in I \cap J$ for some m. But then, since $f^m \in I$ and $f^m \in J$, we have that $f^{2m} \in IJ$. □

Theorem 2.1.9 ([1], Proposition 3.12)**.** *Let I be an ideal of R and let S be a multiplicatively closed subset of R s.t. $I \cap S = \emptyset$. Then the set*

$$\mathcal{S} = \{\textit{Ideals } J | I \subseteq J \textit{ and } J \cap S = \emptyset\}$$

has a maximal element $\mathfrak{p}$ and $\mathfrak{p} \in \mathrm{Spec}(R)$.

Proof. The set $\mathcal{S}$ is nonempty as $I \in \mathcal{S}$ and is partially ordered by inclusion. Every chain of the form $J_1 \subseteq J_2 \subseteq \ldots$ in $\mathcal{S}$ has an upper bound $J = \bigcup_i J_i$. Thus, $\mathcal{S}$ has a maximal element $\mathfrak{p}$ by Zorn's lemma A.1.1. Let $x, y \in R \setminus \mathfrak{p}$. Then, $\langle \mathfrak{p}, x \rangle$ and $\langle \mathfrak{p}, y \rangle$ are ideals properly containing $\mathfrak{p}$. Thus, they are not disjoint to $\mathcal{S}$, which implies that there are $p, q \in \mathfrak{p}$ and $a, b \in R$ with $p + ax \in \mathcal{S}$ and $q + by \in \mathcal{S}$. We have that $pq + pby + qax + abxy \in \mathcal{S}$ as $\mathcal{S}$ is multiplicatively closed. But $pq + pby + qax \in \mathfrak{p}$, so $xy \notin \mathfrak{p}$, which implies that $\mathfrak{p}$ is prime. □

This allows us to express the radical of an ideal as an intersection of prime ideals.

Proposition 2.1.10 ([1], Theorem 3.29)**.** *Let I be an ideal of R. Then*

$$\sqrt{I} = \bigcap_{\substack{\mathfrak{p}\in \mathrm{Spec}(R) \\ I\subseteq\mathfrak{p}}} \mathfrak{p}.$$

Proof. ($\supseteq$) Define the multiplicative set $\mathcal{S} = \{1, x, x^2, \ldots\}$ for an element $x \notin \sqrt{I}$. $\mathcal{S}$ clearly satisfies $I \cap \mathcal{S} = \emptyset$. By Theorem 2.1.9 there is $\mathfrak{p} \in \mathrm{Spec}(R)$ s.t. $I \subseteq \mathfrak{p}$, but $x \notin \mathfrak{p}$. Thus, $x \notin \bigcap_{\substack{\mathfrak{p}\in \mathrm{Spec}(R) \\ I\subseteq\mathfrak{p}}} \mathfrak{p}$.

($\subseteq$) Let $x \in \sqrt{I}$, i.e. $x^n \in I$. Thus, $x \in \mathfrak{p}$ for all $\mathfrak{p} \in \mathrm{Spec}(R)$ containing I. □

Corollary 2.1.11 ([46], Corollary 3.49)**.** *The nilradical* $\mathrm{Nil}(R)$ *satisfies*

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

Proof. This follows directly from Proposition 2.1.10, since the zero ideal is contained in every prime ideal of R. □

Definition 2.1.12. A prime ideal $\mathfrak{p} \in \mathrm{Spec}(R)$ containing I is called a *minimal prime of* I if it is minimal w.r.t inclusion among all prime ideals containing I. The set of all minimal primes of an ideal I is denoted by $\mathrm{Min}(I)$. The minimal primes of $\langle 0\rangle$ are called *the minimal primes of* R.

Lemma 2.1.13 ([46], Theorem 3.52)**.** *Every prime ideal $\mathfrak{p}$ containing I contains a minimal prime of I.*

Proof. Consider the set $\mathcal{S} = \{\mathfrak{q} \in \mathrm{Spec}(R) |\ I \subseteq \mathfrak{q} \subseteq \mathfrak{p}\}$ ordered by reverse inclusion. Then $\mathfrak{p} \in \mathcal{S}$, so $\mathcal{S} \neq \emptyset$. Consider a chain $\{\mathfrak{q}_\lambda\}_{\lambda\in\Lambda}$ in $\mathcal{S}$. Then $\mathfrak{q} = \bigcap_{\lambda\in\Lambda} \mathfrak{q}_\lambda$ is prime. Indeed, let $ab \in \mathfrak{q}$ for $a, b \in R \setminus \mathfrak{q}$. Then there exist $j, k \in \Lambda$ s.t. $a \notin \mathfrak{q}_j$, $b \notin \mathfrak{q}_k$, where without loss of generality, we may assume that $\mathfrak{q}_k \subseteq \mathfrak{q}_j$. Thus, $ab \in \mathfrak{q}$ implies $ab \in \mathfrak{q}_j$, but neither a nor b is contained in $\mathfrak{q}_j$. So $ab \notin \mathfrak{q}$ and $\mathfrak{q}$ is prime. Now, $\mathfrak{q}$ is an upper bound of the chain $\{\mathfrak{q}_\lambda\}_{\lambda\in\Lambda}$ in $\mathcal{S}$, so $\mathcal{S}$ has by Zorn's lemma A.1.1 a maximal element, which is in $\mathrm{Min}(I)$. □

With minimal primes, we can refine the expression of the radical of an ideal I as the intersection of all minimal primes containing I.

Corollary 2.1.14 ([46], Corollary 3.54)**.** *Let I be an ideal of R. Then*

$$\sqrt{I} = \bigcap_{\mathfrak{p}\in \mathrm{Min}(I)} \mathfrak{p}.$$

Proof. ($\subseteq$) Since all elements of $\mathrm{Min}(I)$ are prime ideals containing I, this inclusion follows from Proposition 2.1.10.

($\supseteq$) Since by Lemma 2.1.13 every prime containing I contains a minimal prime of I, the reverse inclusion also follows. □

2.1.2 Noetherian Rings

Often it is desired that the commutative rings we work with, satisfy some finiteness properties. We now introduce some of the most important types of rings that are used very frequently throughout the rest of the thesis.

Definition 2.1.15. A ring R is called *Noetherian* if every ideal of R is finitely generated.

Example 2.1.16. Every principal ideal domain (PID) is Noetherian as every ideal is generated by one element.

Definition 2.1.17. A ring R satisfies the *ascending chain condition (ACC)* if every ascending chain of ideals $I_0 \subseteq I_1 \subseteq \cdots$ *stabilizes*, i.e. there is a $j \geq 0$ s.t.

$$I_j = I_{j+1} = \cdots .$$

The *maximal condition (MaxC)* is satisfied if every nonemtpy set of ideals $\mathcal{S}$ contains a maximal element w.r.t to inclusion.

Lemma 2.1.18 ([1], Lemma 16.4)**.** *ACC is satisfied if and only if MaxC is satisfied*

Proof. ($\Leftarrow$) Consider a chain of ideals $I_0 \subseteq I_1 \subseteq \cdots$ with I_j maximal w.r.t. inclusion. Then $I_j = I_{j+1} = \cdots$.

($\Rightarrow$) We prove the contrapositive: Suppose there is a nonempty set $\mathcal{S}$ that has no maximal element. Since $\mathcal{S}$ is nonempty, there is $I_0 \in \mathcal{S}$. For each $j \geq 0$, there is $I_{j+1} \in \mathcal{S}$ with $I_j \subsetneq I_{j+1}$. This yields a chain $I_0 \subsetneq I_1 \subsetneq \cdots$ that does not stabilize. □

These conditions can be used to equivalently define Noetherian rings.

Proposition 2.1.19 ([1], Proposition 16.5)**.** *The following conditions are equivalent:*

(a) *R is Noetherian,*

(b) *ACC is satisfied,*

(c) *MaxC is satisfied.*

Proof. ($a \Rightarrow b$) Let $I_0 \subseteq I_1 \subseteq \cdots$ be a chain of ideals and set $I = \bigcup_{i \geq 0} I_i$. I is an ideal and finitely generated by hypothesis i.e. $I = \langle x_1, \ldots, x_r \rangle$. There is j_i with $x_i \in I_{j_i}$ for each i. Let $j = \max_i\{j_i\}$, then $x_i \in I_j$ for all i, which implies that $I \subseteq I_j \subseteq I_{j+1} \subseteq \cdots \subseteq I$. Thus, $I_j = I_{j+1} = \cdots$.

($b \Rightarrow c$) This follows by Lemma 2.1.18.

($c \Rightarrow a$) Let I be an ideal generated by $x_\lambda, \lambda \in \Lambda$. Define $\mathcal{S}$ to be the set of ideals that are generated by finitely many x_λ. Let J be a maximal element of $\mathcal{S}$ generated by $x_{\lambda_1}, \ldots, x_{\lambda_m}$. Then, $J \subseteq \langle J, x_\lambda \rangle$ for each $\lambda \in \Lambda$. Thus, it holds that $J = \langle J, x_\lambda \rangle$ as J is maximal. Therefore, $x_\lambda \in J$, which implies that $J = I$ and I is finitely generated. □

Noetherian rings have a lot of useful properties. We now state one that we use throughout the thesis.

Lemma 2.1.20 ([46], Lemma 8.21)**.** *Let I be an ideal in a Noetherian ring R. Then I contains a power of its radical.*

Proof. $\sqrt{I}$ is finitely generated by say $x_1, \ldots, x_t$ as R is Noetherian. Since $x_i \in \sqrt{I}$, there exists $n_i \in \mathbb{N}$ s.t. $x_i^{n_i} \in \sqrt{I}$. Let $N = n_1 + \cdots + n_t$ and observe that $\sqrt{I}^N$ is generated by elements of the form $x_1^{r_1} \cdots x_t^{r_t}$ where $r_1 + \cdots + r_t = N$. For each such element $r_i \geq n_i$ for some i and therefore $x_1^{r_1} \cdots x_t^{r_t} \in I$. Thus, $\sqrt{I}^N \subseteq I$, since each of its generators is contained in I. □

2.1.3 Primary Decomposition

Primary decomposition generalizes the factorization of an integer into prime powers. One of the goals of this section is to show that every proper ideal in R has a primary decomposition. To do so, we have to introduce some basic definitions.

Definition 2.1.21. An ideal $\mathfrak{q}$ of R is called a *primary ideal* of R if

(a) $1 \notin \mathfrak{q}$,

(b) whenever $a, b \in R$ with $ab \in \mathfrak{q}$ but $a \notin \mathfrak{q}$, then $b \in \sqrt{\mathfrak{q}}$.

Remark 2.1.22. Clearly, every prime ideal is primary. However, the converse is not necessarily true.

Lemma 2.1.23 ([46], Lemma 4.5)**.** *Let $\mathfrak{q}$ be a primary ideal. Then $\mathfrak{p} = \sqrt{\mathfrak{q}} \in \operatorname{Spec}(R)$. Moreover, it is the smallest prime ideal containing $\mathfrak{q}$, i.e. the unique minimal prime of $\mathfrak{q}$.*

Proof. We know that $1 \notin \mathfrak{p} = \sqrt{\mathfrak{q}}$, since $1 \notin \mathfrak{q}$. Let $a, b \in R$ with $ab \in \mathfrak{p}$ and $a \notin \mathfrak{p}$. Then there is $n \in \mathbb{N}$ s.t. $(ab)^n = a^n b^n \in \mathfrak{q}$. But no positive power of a is contained in $\mathfrak{q}$, so no power of a^n lies in $\mathfrak{q}$. As $\mathfrak{q}$ is primary, this implies that $b^{nm} \in \mathfrak{q}$ for some m, i.e. $b \in \mathfrak{p}$ so $\mathfrak{p} \in \operatorname{Spec}(R)$.
Note that for $\mathfrak{p}' \in \operatorname{Spec}(R)$ and $\mathfrak{q} \subseteq \mathfrak{p}'$, we have $\mathfrak{p}' = \sqrt{\mathfrak{p}'} \supseteq \sqrt{\mathfrak{q}} = \mathfrak{p}$. □

Definition 2.1.24. Let $\mathfrak{q}$ be a primary ideal and let $\mathfrak{p} \in \operatorname{Spec}(R)$ s.t. $\sqrt{\mathfrak{q}} = \mathfrak{p}$. Then $\mathfrak{q}$ is called a $\mathfrak{p}$-*primary* ideal.

Example 2.1.25. The primary ideals of $\mathbb{Z}$ are $\langle 0 \rangle$ and those of the form $p^i\mathbb{Z}$ for a prime number $p \in \mathbb{Z}$ and $i > 0$. Clearly $p^i\mathbb{Z}$ is $p\mathbb{Z}$-primary.

Lemma 2.1.26 ([46], Lemma 4.13)**.** *The intersection of $\mathfrak{p}$-primary ideals is $\mathfrak{p}$-primary.*

Proof. Let $\mathfrak{q}_i$ for $i = 1, \ldots, n$ be $\mathfrak{p}$-primary and set $\mathfrak{q} = \bigcap_{i=1}^n \mathfrak{q}_i$. Then, Lemma 2.1.8 implies $\sqrt{\mathfrak{q}} = \sqrt{\bigcap_{i=1}^n \mathfrak{q}_i} = \bigcap_{i=1}^n \sqrt{\mathfrak{q}_i} = \bigcap_{i=1}^n \mathfrak{p} = \mathfrak{p}$.
Let $ab \in \mathfrak{q}$ and $a \notin \mathfrak{q}$. Then for some i, we have that $ab \in \mathfrak{q}_i$ but $a \notin \mathfrak{q}_i$. Thus, $b \in \sqrt{\mathfrak{q}_i} = \mathfrak{p} = \sqrt{\mathfrak{q}}$.
So $\mathfrak{q}$ is $\mathfrak{p}$-primary. □

Lemma 2.1.27 ([2], Lemma 4.4)**.** *Let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal and let a be an element of R. Then:*

(a) *If $a \in \mathfrak{q}$, then $(\mathfrak{q} : a) = R$.*

(b) *If $a \notin \mathfrak{q}$, then $(\mathfrak{q} : a)$ is $\mathfrak{p}$-primary.*

(c) *If $a \notin \mathfrak{p}$, then $(\mathfrak{q} : a) = \mathfrak{q}$.*

Proof. (a) This follows immediately from the definition.

(b) Let $b \in (\mathfrak{q} : a)$. Then $ab \in \mathfrak{q}$ and $b \in \mathfrak{p}$, since $a \notin \mathfrak{q}$. Thus, $\mathfrak{q} \subseteq (\mathfrak{q} : a) \subseteq \mathfrak{p}$, i.e. $\sqrt{(\mathfrak{q} : a)} = \mathfrak{p}$ when taking radicals. Let $bc \in (\mathfrak{q} : a)$ with $b \notin \mathfrak{p}$, then $abc \in \mathfrak{q}$. Thus, $ac \in \mathfrak{q}$, so $c \in (\mathfrak{q} : a)$.

(c) Let $b \in (\mathfrak{q} : a)$. Then $ab \in \mathfrak{q}$. But $a \notin \mathfrak{p}$, so $b \in \mathfrak{q}$. □

Definition 2.1.28. Let I be a proper ideal of R. A *primary decomposition* of I is an expression of I as a finite intersection of primary ideals, i.e.

$$I = \bigcap_{i=1}^{n} \mathfrak{q}_i \text{ with } \sqrt{\mathfrak{q}_i} = \mathfrak{p}_i \text{ for } i = 1, \ldots, n.$$

Such a decomposition is called a *minimal primary decomposition* of I when

(a) $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are n different prime ideals of R,

(b) for all $j = 1, \ldots, n$ we have

$$\mathfrak{q}_j \not\supseteq \bigcap_{\substack{i=1 \\ i \neq j}}^{n} \mathfrak{q}_i.$$

An ideal I is called *decomposable* if it has a primary decomposition.

Remark 2.1.29. By repeatedly applying Lemma 2.1.26, (a) is easily achievable. Condition (b) can be achieved by omitting all the superfluous terms. Thus, every decomposable ideal of R does also have a minimal primary decomposition.

While primary ideals $\mathfrak{q}_i$ in a minimal primary decomposition may not be unique, there is some uniqueness to it.

Theorem 2.1.30 (1st Uniqueness Theorem, [2], Theorem 4.5)**.** *Let I be a decomposable ideal of R with a minimal primary decomposition $I = \bigcap_{i=1}^{n} \mathfrak{q}_i$. Let $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ for $i = 1, \ldots, n$. Then the $\mathfrak{p}_i$ are exactly the prime ideals which occur in the set $\{\sqrt{(I : x)} : x \in R\}$. Thus, they are independent of the minimal primary decomposition of I.*

Proof. $(I : x) = (\bigcap_{i=1}^{n} \mathfrak{q}_i : x) = \bigcap_{i=1}^{n} (\mathfrak{q}_i : x)$ for any $x \in R$. Thus, $\sqrt{(I : x)} = \bigcap_{i=1}^{n} \sqrt{(\mathfrak{q}_i : x)}$, which implies that $\sqrt{(I : x)} = \bigcap_{x \notin \mathfrak{q}_j} \mathfrak{p}_j$ by Lemma 2.1.27. Now, suppose that it is prime, i.e. $\sqrt{(I : x)} \in \operatorname{Spec}(R)$. Then, Proposition 2.1.3 implies that $\sqrt{(I : x)} = \mathfrak{p}_j$ for some j.

On the other hand, as the decomposition is minimal, for each $i = 1, \ldots, n$, there is $x_i \notin \mathfrak{q}_i$ with $x_i \in \bigcap_{i \neq j} \mathfrak{q}_j$. Then, Lemma 2.1.27 implies that $\sqrt{(I : x_i)} = \mathfrak{p}_i$. □

Remark 2.1.31. The last part of the proof of Theorem 2.1.30 combined with Lemma 2.1.27 implies that for each i, there exists an element $x_i \in R$ s.t. $(I : x_i)$ is $\mathfrak{p}_i$-primary.

Definition 2.1.32. The prime ideals of the decomposition in Proposition 2.1.28 are said to *belong* to I.

Example 2.1.33. Consider the ideal $180\mathbb{Z}$ of $\mathbb{Z}$. It is easy to see that

$$180\mathbb{Z} = 4\mathbb{Z} \cap 9\mathbb{Z} \cap 5\mathbb{Z},$$

so the prime ideals belonging to $180\mathbb{Z}$ are $2\mathbb{Z}, 3\mathbb{Z}$ and $5\mathbb{Z}$.

In the previous example, the ideals belonging to I are precisely the minimal prime ideals containing I. These actually always belong to I.

Proposition 2.1.34 ([2], Proposition 4.6)**.** *Let I be a decomposable ideal of R. Then, any prime ideal $\mathfrak{p} \supseteq I$ contains a minimal prime ideal belonging to I.*

Proof. If $\mathfrak{p} \supseteq I = \bigcap_{i=1}^{n} \mathfrak{q}_i$, then $\mathfrak{p} = \sqrt{\mathfrak{p}} \supseteq \bigcap_{i=1}^{n} \sqrt{\mathfrak{q}_i} = \bigcap_{i=1}^{n} \mathfrak{p}_i$. Thus, Proposition 2.1.3 implies that $\mathfrak{p} \supseteq \mathfrak{p}_i$ for some i and therefore $\mathfrak{p}$ contains a minimal prime ideal of I. □

Next, we look at the relationship between prime ideals belonging to I and the colon ideal. To do so, we introduce a particular type of colon ideal.

Definition 2.1.35. The *annihilator of* I is defined to be the set $\operatorname{Ann}(I) = (0 : I)$.

Proposition 2.1.36 ([46], Proposition 8.22)**.** *Let I be a decomposable ideal of R and let $\mathfrak{p}$ be a prime ideal. Then the following are equivalent:*

(a) *$\mathfrak{p}$ belongs to I.*

(b) *There exists $a \in R$ s.t. $(I : a) = \mathfrak{p}$.*

(c) *There exists $\lambda \in R/I$ s.t. $\mathrm{Ann}(\lambda) = \mathfrak{p}$.*

Proof. $(b \Rightarrow a)$ If there is $a \in R$ s.t. $(I : a) = \mathfrak{p}$, then clearly $(I : a)$ is $\mathfrak{p}$-primary and by Theorem 2.1.30 it belongs to I.

$(a \Rightarrow b)$ Consider I with a minimal primary decomposition $I = \bigcap_{i=1}^{n} \mathfrak{q}_i$ with $\sqrt{\mathfrak{q}_i} = \mathfrak{p}_i$ for $i = 1, \ldots, n$. Let $j \in \mathbb{N}$ with $1 \leq j \leq n$ and set

$$I_j = \bigcap_{\substack{i=1 \\ i \neq j}}^{n} \mathfrak{q}_i,$$

s.t. $I \subsetneq I_j \not\subseteq \mathfrak{q}_j$ as the primary decomposition was chosen minimal. There exists $t \in \mathbb{N}$ s.t. $\mathfrak{p}_j^t \subseteq \mathfrak{q}_j$ by Lemma 2.1.20. Therefore, we have

$$\mathfrak{p}_j^t I_j \subseteq \mathfrak{q}_j I_j \subseteq \mathfrak{q}_j \cap I_j = I.$$

Let u be the smallest $t \in \mathbb{N}$ s.t. $\mathfrak{p}_j^t I_j \subseteq I$ holds. Then, $\mathfrak{p}_j^u I_j \subseteq I$ and $\mathfrak{p}_j^{u-1} I_j \not\subseteq I$. (Also for $u = 1$ as $I_j \not\subseteq I$). Choose $a \in \mathfrak{p}_j^{u-1} I_j \setminus I$ s.t. $a \in I_j \setminus I$. Then

$$(I : a) = (\bigcap_{i=1}^{n} \mathfrak{q}_i : a) = \bigcap_{i=1}^{n} (\mathfrak{q}_i : a) = (\mathfrak{q}_j : a),$$

which is $\mathfrak{p}_j$-primary by Lemma 2.1.27. Since $a\mathfrak{p}_j \subseteq \mathfrak{p}_j^u I_j \subseteq I$, one has that $\mathfrak{p}_j \subseteq (I : a) \subseteq \mathfrak{p}_j$ and thus $\mathfrak{p}_j = (I : a)$.

$(b \Leftrightarrow c)$ This equivalence is immediate, as for $x \in R$ one has $\mathrm{Ann}_{R/I}(x + I) = (I : x)$. □

To show that a primary decomposition always exists we introduce irreducible ideals.

Definition 2.1.37. An ideal I of R is called *irreducible* if I is a proper ideal that cannot be expressed as the intersection of two strictly larger ideals.

Proposition 2.1.38 ([46], Proposition 4.33)**.** *Let R be Noetherian and let I be a proper ideal of R. Then I can be expressed as an intersection of finitely many irreducible ideals of R.*

Proof. Suppose by contradiction that there exist ideals that cannot be expressed in such a way. Let $\mathcal{S}$ be the set of all such ideals. Then $\mathcal{S}$ has a maximal element, say I, as R is Noetherian. Clearly, I cannot be irreducible, as otherwise $I = I \cap I$, which would imply $I \notin \mathcal{S}$. Therefore I can be written as $I = I_1 \cap I_2$ for some ideals I_1, I_2 of R that properly contain I. By maximality of I, both these ideals are not in $\mathcal{S}$ and thus, can be expressed as intersections of finitely many irreducible ideals of R. But then $I = I_1 \cap I_2$ is also a intersection of finitely many irreducible ideals, which is a contradiction. Therefore, $\mathcal{S} = \emptyset$. □

Proposition 2.1.39 ([46], Proposition 4.34)**.** *Let R be Noetherian. If an ideal I is irreducible, then it is primary.*

Proof. Let $a, b \in R$ s.t. $ab \in I$ but $b \notin I$. Clearly, we have

$$(I : a) \subseteq (I : a^2) \subseteq \cdots \subseteq (I : a^i) \subseteq \cdots .$$

This ascending chain eventually stabilizes, as R is Noetherian. Then $(I : a^n) = (I : a^{n+i})$ for some $n \in \mathbb{N}$ and all $i \in \mathbb{N}$. Also, we have that $I \subseteq \langle I, a^n\rangle \cap \langle I, b\rangle$. Let $r \in \langle I, a^n\rangle \cap \langle I, b\rangle$. Then $r = g + ca^n = h + db$ for some $g, h \in I, c, d \in R$. Therefore, $ra = ga + ca^{n+1} = ha + dab$ s.t. $ca^{n+1} = ha + dab - ga \in I$, since $ab, g, h \in I$. This implies that $c \in (I : a^{n+1}) = (I : a^n)$ s.t. $r = g + ca^n \in I$. Thus, we have that $I = \langle I, a^n\rangle \cap \langle I, b\rangle$. Since I is irreducible and $I \subsetneq \langle I, b\rangle$, it follows that $I = \langle I, a^n\rangle$, i.e. $a^n \in I$. Thus I is primary. □

The results above ensure that every proper ideal I of a Noetherian ring R has a primary decomposition. By Remark 2.1.29, it follows that all such I have a minimal decomposition.

2.1.4 Localization

Localization is the procedure of inverting certain elements in a ring and generalizes the construction of the field of fractions of an integral domain. It is a very useful tool and has many applications beyond what we use in this thesis.
First, we introduce some conventions regarding notation.

Definition 2.1.40. Let R and S be commutative rings with a ring homomorphism $f : R \to S$.

(a) For an ideal I of R, the ideal $f(I)S$ of S is called the *extension* of I to S and will be denoted I^e.

(b) For an ideal J of S, the ideal $f^{-1}(J) = \{r \in R : f(r) \in J\}$ of R is called the *contraction* of J to R and will be denoted J^c.

Lemma 2.1.41 ([46], Lemma 2.44)**.** *Let I be and ideal of R, J an ideal of S and let $f : R \to S$ be a ring homomorphism. Then:*

(a) $I \subseteq I^{ec}$,

(b) $J^{ce} \subseteq J$.

Proof. (a) Let $r \in I$. Then $f(r) \in f(I) \subseteq f(I)S = I^e$.

(b) Since $f(f^{-1}(J)) \subseteq J$ and J is an ideal of S, it follows that $J^{ce} \subseteq J$. □

Example 2.1.42. Let $f : \mathbb{Z} \to \mathbb{Q}$ be the inclusion and $I = 2\mathbb{Z}$. Then $I^e = \mathbb{Q}$.
Let $f : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}, a + 6\mathbb{Z} \mapsto a + 2\mathbb{Z}$ and $J = \langle 0 + 2\mathbb{Z}\rangle \subseteq \mathbb{Z}/2\mathbb{Z}$. Then $J^c = f^{-1}(0) = 2\mathbb{Z}/6\mathbb{Z}$.

Lemma 2.1.43 ([46], Remark 3.27)**.** *Let $J \in \operatorname{Spec}(S)$ and let $f : R \to S$ be a ring homomorphism. Then $J^c \in \operatorname{Spec}(R)$.*

Proof. The kernel of the composition

$$R \xrightarrow{f} S \to S/J,$$

where $S \to S/J$ is the natural epimorphism, is $J^c = \{r \in R : f(r) \in J\}$. Thus, $R/J^c \cong S/J$, but S/J is an integral domain, so R/J^c is too. □

Definition 2.1.44. A subset $S \subseteq R$ is called a multiplicative set, if $1 \in S$ and if $x, y \in S$ implies that $xy \in S$.

Remark 2.1.45. It is easy to see that for $\mathfrak{p} \in \operatorname{Spec}(R)$, $R \setminus \mathfrak{p}$ is a multiplicative set.

Lemma 2.1.46 ([46], Lemma 5.1)**.** *Let $S \subseteq R$ be a multiplicative subset of R. Define the relation $\sim$ on $R \times S$ as follows. For $(a,s),(b,t) \in R \times S$ one writes*

$$(a,s) \sim (b,t) \iff \exists u \in S \text{ with } u(ta - sb) = 0.$$

Then $\sim$ is an equivalence relation on $R \times S$.

Proof. Reflexivity is easy as $1 \in S$. Symmetry is also trivial. Let (a,s), (b,t), $(c,u) \in R \times S$ s.t. $(a,s) \sim (b,t)$ and $(b,t) \sim (c,u)$. Then $v(ta - sb) = 0 = w(ub - tc)$ for some $v, w \in S$. This implies that $wuvta = wuvsb$ and $vswub = vswtc$. Thus,

$$wtv(ua - sc) = 0 \text{ and } wtv \in S.$$

This implies that $(a,s) \sim (c,u)$, i.e $\sim$ is transitive and therefore an equivalence relation. □

Using this equivalence relation, we now can introduce the notion of localization.

Definition 2.1.47. Let $S \subseteq R$ be a multiplicative set. For $(r,s) \in R \times S$ denote the equivalence class of $\sim$, which contains (r,s), by $\frac{r}{s}$ or r/s and denote the set of all equivalence classes by $S^{-1}R = \{\frac{r}{s} : r \in R, s \in S\}$.
$S^{-1}R$ is called the *localization* of R at S. If $S = R \setminus \mathfrak{p}$ for a prime ideal $\mathfrak{p}$, then $S^{-1}R$ is also denoted by $R_{\mathfrak{p}}$ and said to be the *localization of R at $\mathfrak{p}$*

Lemma 2.1.48 ([46], Proposition 5.2)**.** *For a multiplicative set $S \subseteq R$, $S^{-1}R$ has the structure of a commutative ring under operations for which*

$$\frac{a}{s} + \frac{b}{t} = \frac{ta + sb}{st}, \quad \frac{a}{s}\frac{b}{t} = \frac{ab}{st}$$

for all $a, b \in R$ and $s, t \in S$. The zero element is $\frac{0}{1}$ and the multiplicative identity is $\frac{1}{1}$.

Proof. We only check if the operations are well-defined. The rest consists of straight-forward checking of ring-axioms.
Let $a, a', b, b' \in R$ and $s, s', t, t' \in S$ be chosen in such a way that in $S^{-1}R$ we have

$$\frac{a}{s} = \frac{a'}{s'} \text{ and } \frac{b}{t} = \frac{b'}{t'}.$$

Then $u(s'a - sa') = 0 = v(t'b - tb')$ for some $u, v \in S$. This yields that

$$uv(s't'ta - stt'a') = 0 = uv(s't'sb - sts'b').$$

Summing up yields

$$uv(s't'(ta + sb) - st(t'a' + s'b')) = 0.$$

As $uv \in S$, we get $\frac{ta+sb}{st} = \frac{t'a'+s'b'}{s't'}$.
Similarly, let $\frac{b}{t} \in S^{-1}R$ and $\frac{a}{s} = \frac{a'}{s'}$. Then there exists $u \in S$ s.t. $us'a = usa'$ and therefore also $btus'a = btusa'$, which implies that $\frac{ba}{st} = \frac{ba'}{s't}$. So multiplication is also well-defined. □

There is a natural ring homomorphism $f : R \to S^{-1}R$ given by $f(r) = r/1$ for all $r \in R$.

Example 2.1.49. Let $2\mathbb{Z} \in \operatorname{Spec}(\mathbb{Z})$ and define the multiplicative set $S = \mathbb{Z} \setminus 2\mathbb{Z}$ consisting of all odd integers. Then $\mathbb{Z}_{2\mathbb{Z}}$ corresponds to the subset of $\mathbb{Q}$ of all rational numbers with odd denominator.

Next, we show that ideals behave rather well under localization.

Lemma 2.1.50 ([46], Lemma 5.24)**.** *Let $S \subseteq R$ be a multiplicative set and let $f : R \to S^{-1}R$ be the natural homomorphism. Let J be an ideal of $S^{-1}R$. Then $J = J^{ce}$.*

Proof. ($\subseteq$) Let $\lambda \in J$. We can write $\lambda = a/s$ for some $a \in R, s \in S$. Then we have that $f(a) = \frac{a}{1} = \frac{s}{1}\frac{a}{s} \in J$, which implies that $a \in J^c$. Thus, $\lambda = a/s = (1/s)f(a) \in J^{ce}$

($\supseteq$) The other inclusion is immediate by Lemma 2.1.41. □

Lemma 2.1.51 ([46], Lemma 5.25)**.** *Let $S \subseteq R$ be a multiplicative set and let $f : R \to S^{-1}R$ be the natural homomorphism. Let I be an ideal of R. Then*

$$I^e = \{\lambda \in S^{-1}R : \lambda = \frac{a}{s} \text{ for some } a \in I, s \in S\}.$$

Proof. ($\supseteq$) For all $a \in I$ and $s \in S$, one has $a/s = (1/s)f(a) \in I^e$.

($\subseteq$) Let $\lambda \in I^e$. There exist $n \in \mathbb{N}, h_1, \ldots, h_n \in I$ and $g_1, \ldots, g_n \in S^{-1}R$ s.t. $\lambda = \sum_{i=1}^n g_i f(h_i)$. There also exist $a_1, \ldots, a_n \in R$ and $s_1, \ldots, s_n \in S$ s.t. $g_i = a_i/s_i$ for $i = 1, \ldots, n$. Therefore, we have

$$\lambda = \sum_{i=1}^n \frac{a_i}{s_i}\frac{h_i}{1} = \sum_{i=1}^n \frac{a_i h_i}{s_i}.$$

After putting the RHS on a common denominator $s \in S$, it is clear that $\lambda = a/s$ for some $a \in I$ and $s \in S$. □

Prime ideals satisfy some additional properties.

Lemma 2.1.52 ([46], Corollary 5.30)**.** *Let $S \subseteq R$ be a multiplicative set and let $\mathfrak{p} \in \operatorname{Spec}(R)$ be s.t. $\mathfrak{p} \cap S = \emptyset$. Let $\lambda \in \mathfrak{p}^e$. Then, every representation $\lambda = a/s$ has $a \in \mathfrak{p}$. Further, it holds that $\mathfrak{p}^{ec} = \mathfrak{p}$.*

Proof. Let $\lambda = a/s, a \in R, s \in S$ be some representation of λ. Then $\lambda = b/t = a/s$ for some $b \in \mathfrak{p}, t \in S$, since $\lambda \in \mathfrak{p}^e$. Thus, there is $u \in S$ s.t. $u(sb - ta) = 0$. Therefore, $(ut)a = usb \in \mathfrak{p}$, where $ut \in S$, which is disjoint from $\mathfrak{p}$. Therefore, $a \in \mathfrak{p}$.

The inclusion $\mathfrak{p} \subseteq \mathfrak{p}^{ec}$ is clear by Lemma 2.1.41.
Conversely, let $a \in \mathfrak{p}^{ec}$. Then $a/1 \in \mathfrak{p}^e$, which implies that $a \in \mathfrak{p}$. So $\mathfrak{p}^{ec} \subseteq \mathfrak{p}$. □

Lemma 2.1.53 ([46], Lemma 5.31)**.** *Let $S \subseteq R$ be a multiplicative set and let I be an ideal of R. Then $I^e = S^{-1}R$ if and only if $I \cap S \neq \emptyset$.*

Proof. ($\Rightarrow$) If $I^e = S^{-1}R$, we have $1/1 \in I^e$ and there is $a \in I, s, t \in S$ s.t. $t(s1 - a1) = 0$. Thus, $ts = ta \in I \cap S \neq \emptyset$.

($\Leftarrow$) Suppose there is $s \in I \cap S$. Then $1/1 = (s/1)(1/s) \in I^e$. □

This allows us to describe the prime ideals of localized rings.

Theorem 2.1.54 ([46], Theorem 5.32)**.** *Let $S \subseteq R$ be a multiplicative set and let $\mathfrak{p}$ be an ideal of R.*

(a) *If $\mathfrak{p} \in \operatorname{Spec}(R)$ and $\mathfrak{p} \cap S = \emptyset$, then $\mathfrak{p}^e \in \operatorname{Spec}(S^{-1}R)$.*

(b) *If $\mathfrak{q} \in \operatorname{Spec}(S^{-1}R)$, then $\mathfrak{q}^c \in \operatorname{Spec}(R)$ and $\mathfrak{q}^c \cap S = \emptyset$.*

(c) *$\operatorname{Spec}(S^{-1}R)$ is precisely the set of ideals $\mathfrak{p}^e$, where $\mathfrak{p} \in \operatorname{Spec}(R)$ s.t. $\mathfrak{p} \cap S = \emptyset$. In fact, each prime ideal of $S^{-1}R$ is of the form $\mathfrak{p}^e$ for exactly one $\mathfrak{p} \in \operatorname{Spec}(R)$ s.t. $\mathfrak{p} \cap S = \emptyset$.*

Proof. (a) We have $\mathfrak{p}^{ec} = \mathfrak{p}$ by Lemma 2.1.52. Thus, $\mathfrak{p}^e \subsetneq S^{-1}R$, as otherwise we would have $\mathfrak{p}^{ec} = (S^{-1}R)^c = R \neq \mathfrak{p}$.
Let $\lambda = a/s, g = b/t \in S^{-1}R$, where $a, b \in R, s, t \in S$ s.t. $\lambda g \in \mathfrak{p}^e$, i.e. $\frac{ab}{st} \in \mathfrak{p}^e$. Then $ab \in \mathfrak{p}$ by Lemma 2.1.52. So either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, which implies that either $\lambda = a/s \in \mathfrak{p}^e$ or $g = b/t \in \mathfrak{p}^e$. Thus, $\mathfrak{p}^e \in \operatorname{Spec}(S^{-1}R)$.

(b) If $\mathfrak{q} \in \operatorname{Spec}(S^{-1}R)$, then $\mathfrak{q}^c \in \operatorname{Spec}(R)$ by Lemma 2.1.43 and also $\mathfrak{q} = \mathfrak{q}^{ce}$. Thus, $\mathfrak{q}^c \cap S = \emptyset$ as otherwise we would have that $\mathfrak{q}^{ce} = S^{-1}R$.

(c) If $\mathfrak{q} \in \operatorname{Spec}(S^{-1}R)$, then $\mathfrak{q} = \mathfrak{p}^e$ for some $\mathfrak{p} \in \operatorname{Spec}(R)$ s.t. $\mathfrak{p} \cap S = \emptyset$ as was shown in (b). Further, if $\mathfrak{p}, \mathfrak{p}' \in \operatorname{Spec}(R)$ with $\mathfrak{p} \cap S = \mathfrak{p}' \cap S = \emptyset$ and $\mathfrak{p}^e = \mathfrak{p}'^e$, then Lemma 2.1.52 implies that $\mathfrak{p} = \mathfrak{p}^{ec} = \mathfrak{p}'^{ec} = \mathfrak{p}'$, which concludes the second part of the statement. □

The results of the previous theorem can be summarized as follows.

Corollary 2.1.55 ([46], Remark 5.33)**.** *There is an inclusion-preserving bijective mapping*

$$\{\ \mathfrak{p} \in \operatorname{Spec}(R) : \mathfrak{p} \cap S = \emptyset\ \} \leftrightarrow \operatorname{Spec}(S^{-1}R)$$

given by extension and contraction of ideals.

We conclude this section by showing that a PID keeps its useful properties after localization.

Lemma 2.1.56. *Let R be a PID and S be a multiplicative set of R. Then $S^{-1}R$ is also a PID.*

Proof. By Theorem 2.1.54, it easy to see that $S^{-1}R$ is an integral domain, as $\langle 0 \rangle^e \in \operatorname{Spec}(S^{-1}R)$ if $0 \cap S = \emptyset$ and $S^{-1}R = 0$ otherwise by Lemma 2.1.53.
Let J be an ideal of $S^{-1}R$. Then there exists an ideal I of R s.t. $J = I^e$. Now, since R is a PID, there exists $r \in R$ s.t. $I = \langle r \rangle$. Let J' be the ideal in $S^{-1}R$ generated by $r/1$. If $\lambda \in J'$, then $\lambda = \frac{a}{s}\frac{r}{1}$, where $\frac{a}{s} \in S^{-1}R$ and so $\lambda \in I^e = J$.
On the other hand, let $y \in J$. Then $y = \frac{a}{s}\frac{x}{1}$, where $x \in J, \frac{a}{s} \in S^{-1}R$. Thus, $x = nr$ for some $n \in R$ and $y = \frac{nr}{1}\frac{a}{s}$. But then we have $y = \frac{na}{s}\frac{r}{1} \in J'$. So J is a principal ideal and since it was chosen arbitrarily, $S^{-1}R$ is a PID. □

2.2 Modules

For a lot of results, it makes sense to generalize the concept of ideals to modules. We start by recalling the most important definitions and facts. This section mainly follows [1, Chapters 4, 16 and 17].

2.2.1 Basics

Definition 2.2.1. An *R-module* M is an additive abelian group with a scalar multiplication $\cdot : R \times M \to M$, that for $m, n \in M, a, b \in R$ satisfies

(a) $a(m + n) = am + an$,

(b) $(a + b)m = am + bm$,

(c) $(ab)m = a(bm)$,

(d) $1 \cdot m = m$.

A subset N of M, which satisfies the properties of an R-module is called a *submodule* of M. Clearly, the set of cosets M/N inherits the R-module structure.
Let $J \subseteq M$, then

$$\sum_{m \in J} Rm = \left\{ \sum_{i=1}^{n} r_i m_i : n \in \mathbb{N}, r_1, \ldots, r_n \in R, m_1, \ldots, m_n \in J \right\}$$

is called the submodule of M *generated* by the set J, denoted $M = \langle J \rangle$.

As in the ideal case, there are some common operations on modules.

Definition 2.2.2. Let M be an R-module and let N be a submodule of M. Let $J \subseteq M$ be a subset of M.
The ideal $\{r \in R : rj \in N \text{ for all } j \in J\}$ will be denoted $(N : J)$. Clearly, $(N : J) = (N : \langle J \rangle)$.
The ideal $(0 : M)$ is called the *annihilator* of M, denoted $\mathrm{Ann}(M)$.

Definition 2.2.3. Let M, N be R-modules. An R-module homomorphism ϕ is an R-linear map, i.e. $\phi : M \to N$ s.t.

$$\phi(am + bn) = a\phi(m) + b\phi(n) \text{ for } a, b \in R, m, n \in M.$$

If N is a submodule of M, then $\phi : M \to M/N, m \mapsto m + N$ is called the *canonical* homomorphism.
Note that $\ker(\phi) = \phi^{-1}(0) \subseteq M$ and $\mathrm{Im}(\phi) = \phi(M) \subseteq N$ are clearly submodules of M and N respectively.
The *cokernel* of ϕ is defined to be $\mathrm{coker}(\phi) = N/\mathrm{Im}(\phi)$.

Some very important modules that we use frequently throughout this thesis are free modules.

Definition 2.2.4. An R-module F is said to be a *free* module if F has a generating set consisting of linearly independent elements. Such a generating set is called a (module-) basis.

The *rank* of a free module F is defined to be the minimal number of elements in a basis, i.e. $\mathrm{rk}(F) = \min\{|B| : B \text{ is a basis of } F\}$. If $\mathrm{rk}(F) < \infty$, then F is said to be of *finite rank*. Since any two bases of a free module have the same cardinality, the rank is just the cardinality of a basis.

Example 2.2.5. $\bigoplus_{i \in B} R \cong R^{|B|}$ is a free module with the *standard basis* $(e_i)_{i \in B}$, where for each $j \in B$, the basis vector $e_j = (0, \ldots, 0, 1, 0 \ldots, 0) \in \bigoplus_{i \in B} R_i$ has a 1 in the j-th component and all its other components are zero.

Next, we state some basic properties of free modules that can be found in most textbooks. For the proof of these results, we refer to [46, Chapter 6].

Lemma 2.2.6. *Let M be an R-module.*

(a) *M is free if and only if M is isomorphic to an R-module of the form $\bigoplus_{i \in B} R_i$, with standard basis $(e_i)_{i \in B}$ and $R_i = R$ for all $i \in B$.*

(b) *There always exists a free module $F \cong R^n$ and a surjective homomorphism $\varphi : F \to M$. If M is finitely generated by n elements $m_1, \ldots, m_n$, F can be chosen of rank n and we will usually choose $\varphi : R^n \to M, e_i \mapsto m_i$ as the epimorphism.*

(c) *Between free modules, homomorphisms can be seen as multiplication by matrices. Let $\phi : R^m \to R^n$ be a map. Then, ϕ is a module-homomorphism if and only if there exists a $n \times m$ matrix A with coefficients in R s.t. $\phi(f) = Af^\top$ for all $f \in R^m$.*

2.2.2 Noetherian Modules

As Noetherian rings become very important it makes sense to generalize this notion to modules.

Definition 2.2.7. Let M be an R-module.

(a) M is *Noetherian* if every submodule is finitely generated.

(b) The *ascending chain condition (ACC)* is satisfied in M if every ascending chain of submodules $M_0 \subseteq M_1 \subseteq \cdots$ eventually stabilizes.

(c) The *maximal condition (MaxC)* is satisfied in M if every nonempty set of submodules contains a maximal ideal.

It is very simple to generalize Proposition 2.1.19 and show the following result.

Proposition 2.2.8. *Let M be an R-module. Then the following are equivalent:*

(a) *M is Noetherian,*

(b) *ACC is satisfied in M,*

(c) *MaxC is satisfied in M.*

To show that submodules and quotient modules of Noetherian modules inherit these properties we need a preliminary result.

Lemma 2.2.9 ([1], Lemma 16.14)**.** *Let N be a submodule of M and let $M_1 \subseteq M_2$ be submodules of M. If*

$$M_1 \cap N = M_2 \cap N \text{ and } (M_1 + N)/N = (M_2 + N)/N,$$

then $M_1 = M_2$.

Proof. Let $m_2 \in M_2$. There exists $m_1 \in M_1$ s.t. $n = m_2 - m_1 \in N$. Then $n \in M_2 \cap N = M_1 \cap N$. Thus, $m_2 \in M_1$, which implies that $M_1 = M_2$. □

Proposition 2.2.10 ([1], Proposition 16.16)**.** *Let N be a submodule of the R-module M. Then M is Noetherian if and only if N and M/N are Noetherian.*

Proof. ($\Rightarrow$) Since M is Noetherian, and every submodule of N is a submodule of M and thus finitely generated, it follows that N is Noetherian. Any ascending chain in M/N is the image of a chain in M that stabilizes, since M is Noetherian. Thus, this chain stabilizes too.

($\Leftarrow$) For a chain $M_1 \subseteq M_2 \subseteq \cdots \subseteq M$, both of the chains $(M_1 \cap N) \subseteq (M_2 \cap N) \subseteq \cdots$ and $(M_1 + N)/N \subseteq (M_2 + N)/N \subseteq \cdots$ stabilize. Choose $j \in \mathbb{N}$ s.t. $M_j \cap N = M_{j+1} \cap N = \cdots$ and $(M_j + N)/N = (M_{j+1} + N)/N = \cdots$. Then, $M_j = M_{j+1} = \cdots$ by Lemma 2.2.9, which implies that M is Noetherian. □

Iteratively applying Proposition 2.2.10 to the direct sum of modules gives the following useful results, which basically show that all submodules of a free R-module of finite rank are finitely generated.

Corollary 2.2.11 ([1], Corollary 16.17)**.** *The R-modules $M_1, \ldots, M_r$ are Noetherian if and only if $M_1 \oplus \cdots \oplus M_r$ is Noetherian.*

Theorem 2.2.12 ([1], Theorem 16.19)**.** *Let R be a Noetherian ring and M be an R-module. Then M is Noetherian if and only if M is finitely generated.*

Proof. ($\Rightarrow$) This is immediate, as M is a submodule of itself.

($\Leftarrow$) As M is finitely generated, there is a free module F and an epimorphism $\phi : F \to M$. Let $K = \ker(\phi)$. Since by hypothesis R is Noetherian, it follows by Lemma 2.2.6 that $F \cong R^n$ is Noetherian, where $n = \mathrm{rk}(F)$. Thus, K and F/K are Noetherian by Proposition 2.2.10, but $M \cong F/K$, so M is Noetherian. □

In later chapters, we will be interested in relations among the elements generating a module. Thus it makes sense to introduce the following terminology.

Definition 2.2.13. Let M be an R-module and $\mathcal{S} = (m_1, \ldots, m_t)$ be a t-tuple of elements $m_i \in M$. Then a t-tuple $(a_1, \ldots, a_t) \in R^t$ satisfying the relation

$$a_1 m_1 + \cdots + a_t m_t = 0$$

is called a *syzygy* on $\mathcal{S}$.
The set of all syzygies on $\mathcal{S}$ is called the (1st) *syzygy-module* of $\mathcal{S}$ and is denoted $\mathrm{Syz}(m_1, \ldots, m_t)$.

As the kernel of the epimorphism $\varphi : R^t \to M$, $e_i \to m_i$, it is easy to see that $\mathrm{Syz}(m_1, \ldots, m_t)$ is a submodule of R^t and finitely generated, as R^t is Noetherian.

2.2.3 Associated Primes

Next, we introduce a certain type of prime ideals that arise as annihilators and have special properties w.r.t to a module M.

Definition 2.2.14. A prime ideal $\mathfrak{p}$ is said to be *associated to* M if there is a nonzero $m \in M$ s.t. $\mathrm{Ann}(m) = \mathfrak{p}$. The set of all associated primes of M is denoted $\mathrm{Ass}(M)$.

Remark 2.2.15. Suppose I is an ideal of R. Proposition 2.1.36 implies that $\mathfrak{p} \in \mathrm{Ass}(R/I)$ if and only if $\mathfrak{p}$ belongs to I.

Lemma 2.2.16 ([1], Lemma 17.2)**.** *Let M be a R-module and $\mathfrak{p} \in \mathrm{Spec}(R)$. Then $\mathfrak{p} \in \mathrm{Ass}(M)$ if and only if there exists a monomorphism $R/\mathfrak{p} \hookrightarrow M$.*

Proof. ($\Rightarrow$) Suppose $\mathfrak{p} = \mathrm{Ann}(m)$ for some $m \in M$. Define the map $R \to M, x \mapsto xm$. This map clearly induces a monomorphism $R/\mathfrak{p} \hookrightarrow M$.

($\Leftarrow$) Let $m \in M$ be the image of 1 of the given injection. Then $\mathrm{Ann}(m) = \mathfrak{p}$, i.e. $\mathfrak{p} \in \mathrm{Ass}(M)$. □

Lemma 2.2.17 ([1], Lemma 17.4)**.** *Let $\mathfrak{p} \in \mathrm{Spec}(R)$ and let $m \in R/\mathfrak{p}$ be nonzero. Then:*

(a) $\mathrm{Ann}(m) = \mathfrak{p}$,

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

Proof. (a) Let $m \in R/\mathfrak{p}$ be the residue class of an element $y \in R$ and let $x \in R$. Then, $xm = 0$ if and only if $xy \in \mathfrak{p}$, which is only the case if $x \in \mathfrak{p}$ as $\mathfrak{p} \in \mathrm{Spec}(R)$ and $m \neq 0$.

(b) This follows directly from (a). □

Proposition 2.2.18 ([1], Proposition 17.5)**.** *Let M be an R-module and N a submodule. Then:*

$$\mathrm{Ass}(N) \subseteq \mathrm{Ass}(M) \subseteq \mathrm{Ass}(N) \cup \mathrm{Ass}(M/N).$$

Proof. Let $m \in N \subseteq M$. $\mathrm{Ann}(m)$ does not change whether m is seen as an element in M or in N. Thus, $\mathrm{Ass}(N) \subseteq \mathrm{Ass}(M)$.

Let $\mathfrak{p} \in \mathrm{Ass}(M)$. Then, by Lemma 2.2.16, there is an injective map $R/\mathfrak{p} \hookrightarrow M$. Let E be the image of $R/\mathfrak{p}$ in M.
If $E \cap N = 0$, then $R/\mathfrak{p} \hookrightarrow M \to M/N$ is injective. So, Lemma 2.2.16 implies that $\mathfrak{p} \in \mathrm{Ass}(M/N)$.
If $E \cap N \neq 0$, choose $m \in E \cap N$ nonzero. Lemma 2.2.17 implies $\mathrm{Ann}(m) = \mathfrak{p}$. But $m \in N$, which implies that $\mathfrak{p} \in \mathrm{Ass}(N)$. □

Lemma 2.2.19 ([1], Lemma 17.12)**.** *Let M be an R-module and $\mathfrak{p}$ an ideal of R. If $\mathfrak{p}$ is maximal in the set of annihilators of nonzero elements m of M, then $\mathfrak{p} \in \mathrm{Ass}(M)$.*

Proof. Let $\mathfrak{p} = \mathrm{Ann}(m)$ for some nonzero $m \in M$. Clearly, $1 \notin \mathfrak{p}$ as $m \neq 0$. Let $b, c \in R$ s.t. $bc \in \mathfrak{p}$, but $c \notin \mathfrak{p}$, i.e. $bcm = 0$, but $cm \neq 0$. Then, $\mathfrak{p} \subseteq \mathrm{Ann}(cm)$. Thus, $\mathfrak{p} = \mathrm{Ann}(cm)$ by maximality. But $b \in \mathrm{Ann}(cm)$, so $b \in \mathfrak{p}$. Therefore, $\mathfrak{p}$ is prime. □

Proposition 2.2.20 ([1], Proposition 17.13)**.** *Let R be Noetherian and let M be an R-module. Then $M = 0$ if and only if $\mathrm{Ass}(M) = \emptyset$.*

Proof. ($\Rightarrow$) This is immediate.

($\Leftarrow$) Suppose $M \neq 0$ and define $\mathcal{S} = \{\mathrm{Ann}(m) : m \in M \setminus \{0\}\}$. The set $\mathcal{S}$ has a maximal element $\mathfrak{p}$ by Proposition 2.2.8, which is in $\mathrm{Ass}(M)$ by Lemma 2.2.19. Thus, $\mathrm{Ass}(M) \neq \emptyset$. □

Definition 2.2.21. Let M be an R-module and let $x \in R$. The element x is called a *zerodivisor* on M if there is a nonzero $m \in M$ with $xm = 0$. Otherwise, x is said to be a *nonzerodivisor* (or *M-regular*). The set of all zerodivisors of M is denoted $\mathrm{z.div}(M)$.

Definition 2.2.22. Let M be an R-module and $a_1, \ldots, a_r \in R$. The sequence $(a_1, \ldots, a_r)$ is called M-regular, when

(a) $M \neq (a_1, \ldots, a_r)M$,

(b) a_i is a nonzerodivisor on $M/(a_1, \ldots, a_{i-1})M$ for all $i = 1, \ldots, r$.

As associated primes are annihilators of elements, there clearly is some relationship between associated primes and zerodivisors. As we show next, the set of zerodivisors is actually the union of all associated prime ideals.

Proposition 2.2.23 ([1], Proposition 17.15)**.** *Let R be Noetherian and let M be an R-module. Then*

$$\mathrm{z.div}(M) = \bigcup_{\mathfrak{p} \in \mathrm{Ass}(M)} \mathfrak{p}.$$

Proof. ($\supseteq$) This is clear by definition.

($\subseteq$) Let $x \in \mathrm{z.div}(M)$, i.e. $xm = 0$ for a nonzero element $m \in M$. Then $x \in \mathrm{Ann}(m)$, where $\mathrm{Ann}(m) \subseteq \mathfrak{p}$ for some ideal $\mathfrak{p}$ that is maximal in the set $\mathcal{S} = \{\mathrm{Ann}(m) : m \in M \setminus \{0\}\}$. So, $\mathfrak{p} \in \mathrm{Ass}(M)$ by Lemma 2.2.19 and thus, $x \subseteq \bigcup_{\mathfrak{p} \in \mathrm{Ass}(M)} \mathfrak{p}$. □

The following result implies that this is indeed a finite union of prime ideals as there are only finitely many associated primes.

Lemma 2.2.24 ([1], Lemma 17.20)**.** *Let R be Noetherian and let M be a finitely generated R-module. Then there exists a chain of submodules*

$$0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_{n-1} \subseteq M_n = M,$$

with $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ for some prime ideals $\mathfrak{p}_i, i = 1, \ldots, n$. Moreover, $\mathrm{Ass}(M) \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$.

Proof. Since M is finitely generated, it is Noetherian by Theorem 2.2.12. Therefore, among the submodules of M with such a chain, there exists a maximal one w.r.t inclusion, say N. If $M/N \neq 0$, then, $\mathrm{Ass}(M/N) \neq 0$ by Proposition 2.2.20. So Lemma 2.2.16 implies that there exists a submodule N'/N of M/N s.t. $N'/N \cong R/\mathfrak{p}$ for some $\mathfrak{p} \in \mathrm{Spec}(R)$. But then $N \subsetneq N'$, which contradicts the maximality of N. Thus, $M = N$ and such a chain exists.

By Proposition 2.2.18, one has $\mathrm{Ass}(M) \subseteq \mathrm{Ass}(M_{n-1}) \cup \mathrm{Ass}(M_n/M_{n-1}) = \mathrm{Ass}(M_{n-1}) \cup \{\mathfrak{p}_n\}$. Iteratively we get $\mathrm{Ass}(M) \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. □

Corollary 2.2.25 ([1], Theorem 17.21)**.** *Let R be Noetherian and let M be a finitely generated R-module. Then $\mathrm{Ass}(M)$ is finite.*

Proof. This follows immediately by Lemma 2.2.24 as $\mathrm{Ass}(M) \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. □

Example 2.2.26. We have seen that the prime ideals belonging to $180\mathbb{Z}$ are $2\mathbb{Z}, 3\mathbb{Z}, 5\mathbb{Z}$. Therefore, by Remark 2.2.15 we have $\mathrm{Ass}(\mathbb{Z}/180\mathbb{Z}) = \{2\mathbb{Z}, 3\mathbb{Z}, 5\mathbb{Z}\}$. A chain of submodules as in Lemma 2.2.24 is given by

$$0 = 180\mathbb{Z}/180\mathbb{Z} \subseteq 90\mathbb{Z}/180\mathbb{Z} \subseteq 45\mathbb{Z}/180\mathbb{Z} \subseteq 15\mathbb{Z}/180\mathbb{Z} \subseteq 5\mathbb{Z}/180\mathbb{Z} \subseteq \mathbb{Z}/180\mathbb{Z}.$$

2.3 Graded Rings and Modules

The grading of rings and modules will become an important tool to study their structure. For the introduction in this section, we refer to [8, Chapter 1.5] and [33, Chapter 1.7].

Definition 2.3.1.

(a) A ring R is *$\mathbb{Z}$-graded* (or just *graded*) if there exists a family of abelian groups $\{R_d\}_{d\in\mathbb{Z}}$ s.t.

- $R = \bigoplus_{d\in\mathbb{Z}} R_d$,
- $R_d \cdot R_{d'} \subseteq R_{d+d'}$ for all $d, d' \in \mathbb{Z}$.

(b) The elements of R_d are called *homogeneous of degree d*. For $r \in R_d$ we write $\deg(r) = d$.

(c) If $r \in R$ and $r = \sum_{d\in\mathbb{Z}} r_d$ is the decomposition of r according to (a), where $r_d \in R_d$, then r_d is called the *homogeneous component* of degree d of r.

Since a graded ring R can be written as a direct sum of abelian groups, the decomposition into homogeneous components in (c) is actually unique. Furthermore, the property in (b) gives R_d the structure of an R_0-module for every $d \in \mathbb{Z}$.

The concept of grading can also be applied to modules.

Definition 2.3.2. Let R be a graded ring. A finitely generated R-module M is called a *graded R-module* if there exists a family of abelian groups $\{M_d\}_{d\in\mathbb{Z}}$ s.t.

(a) $M = \bigoplus_{d\in\mathbb{Z}} M_d$,

(b) $R_d \cdot M_{d'} \subseteq M_{d+d'}$ for all $d, d' \in \mathbb{Z}$.

As before, we call $u \in M$ *homogeneous of degree d* if $u \in M_d$ for some $d \in \mathbb{Z}$ and write $\deg(u) = d$. For $u \in M$ we have again a unique decomposition into *homogeneous components*.
A submodule $N \subseteq M$ is called a *graded submodule* if $N = \bigoplus_{d\in\mathbb{Z}}(N \cap M_d)$.

The following result shows that graded submodules can be characterized by several equivalent properties.

Proposition 2.3.3 ([33], Proposition 1.7.10)**.** *Let M be a graded R-module, let $N \subseteq M$ be a submodule and let $N_d = N \cap M_d$ for all $d \in \mathbb{Z}$. Then the following are equivalent:*

(a) *N is a graded submodule.*

(b) *If $n \in N$, then every homogeneous component of n is in N.*

(c) *N has a homogeneous system of generators.*

Proof. $(a \Rightarrow b)$ Let $n = \sum_{d\in\mathbb{Z}} n_d \in N$, where $n_d \in N_d$ for all $d \in \mathbb{Z}$. Since $n_d \in N_d \subseteq M_d$, this is equal to the decomposition of n into its homogeneous elements as an element of M. Thus, $n_d \in N$.

$(b \Rightarrow c)$ Consider the set of all homogeneous components of all $n \in N$. This is clearly a system of generators.

$(c \Rightarrow a)$ Let $(n_\lambda)_{\lambda\in\Lambda}$ be a homogeneous system of generators of N and let $N' = \sum_{d\in\mathbb{Z}}(N \cap M_d)$. Clearly, $n_\lambda \in M_d$ for some d since they are homogeneous. Thus,

$$N' \subseteq N \subseteq \sum_{d\in\mathbb{Z}} Rn_\lambda \subseteq N'.$$

This implies that $N = \bigoplus_{d\in\mathbb{Z}} N_d$, i.e. N is a graded submodule. □

Since every ideal $I \subseteq R$ can be regarded as an R-module, the preceding definition also characterizes *graded ideals*, which are ideals that can be written as $I = \bigoplus_{d\in\mathbb{Z}} I_d$ with $I_d = I \cap R_d$. A particular graded ideal we frequently use is the one generated by all elements of positive degree.

Definition 2.3.4. For a graded ring $R = \bigoplus_{d\geq 0} R_d$, the ideal $R_+ := \bigoplus_{d>0} R_d$ consisting of all elements of degree greater than zero, is called the *irrelevant ideal*.

Definition 2.3.5. A *homogeneous ideal* I of a graded ring R is an ideal that is generated by homogeneous elements of R.

Thus, Proposition 2.3.3 implies that the notion of graded and homogeneous ideals coincide.

Remark 2.3.6. Note that homogeneous ideals can contain a lot of non-homogeneous elements, since the sum of homogeneous elements is not necessarily homogeneous.

Given a collection of graded R-modules $M^{(1)}, \ldots, M^{(n)}$, it is possible to regard the direct sum $N = M^{(1)} \oplus \cdots \oplus M^{(n)}$ as a graded module by taking $N_d = (M^{(1)})_d \oplus \cdots \oplus (M^{(n)})_d$ for all $d \in \mathbb{Z}$. If $N \subseteq M$ is a graded submodule of the graded module M, then one can equip the quotient module M/N with the structure of graded module by taking $(M/N)_d = M_d/N_d$.

Definition 2.3.7. Let R be a graded ring, let M and N be finitely generated graded modules and let $\varphi : M \to N$ be an R-linear map. Then φ is said to be *homogeneous of degree d'* if $\varphi(M_d) \subseteq N_{d+d'}$ for all $d \in \mathbb{Z}$. If φ is homogeneous of degree 0, φ is said to be *homogeneous*.

An easy way to create more graded modules is by *shifting degrees*. These modules are called *twists* and are an important tool for constructing graded free resolutions in Chapter 3.

Definition 2.3.8. Given a graded R-module M, the same R-module but with the grading $M(d')_d = M_{d'+d}$ is called the *twist* $M(d')$ or the *twist of M by d'*.

This procedure together with Remark 2.3.6 yields *twisted free graded* modules of the form $R(d_1) \oplus \cdots \oplus R(d_n)$, where the standard basis vectors e_i are homogeneous of degree $-d_i$ for all $i = 1, \ldots, n$.

The concept of twisted free graded modules allows us to turn module-homomorphisms into homogeneous module homomorphisms. Let M be a finitely generated graded R-module generated by homogeneous elements $m_1, \dots, m_n$ of degrees $d_1, \dots, d_n$. Then there exists a surjective homomorphism $\varphi : R^n \to M$ taking e_i to m_i. By twisting the free module accordingly, the homomorphism $\varphi : R(-d_1) \oplus \cdots \oplus R(-d_n) \to M$ is homogeneous since the basis vectors e_i are now also of degree d_i.
By Lemma 2.2.6, homomorphisms between free modules $\varphi : R^m \to R^n$ can be represented by $n \times m$-matrices with entries in R.

Definition 2.3.9. Let $\varphi : R(-d_1) \oplus \cdots \oplus R(-d_m) \to R(-c_1) \oplus \cdots \oplus R(-c_n)$ be a homogeneous homomorphism. Then φ is represented by a matrix A, where the ij-th entry $a_{ij} \in R$ is homogeneous of degree $d_j - c_i$. A matrix satisfying these conditions for a collection of degrees $d_1, \dots, d_m, c_1, \dots, c_n$ is called a *graded matrix*.

A useful result regarding the generating sets of graded modules is the graded version of Nakayama's lemma.

Theorem 2.3.10 (Graded Nakayama's Lemma, [23], Lemma 1.4)**.** *Let M be a finitely generated graded R-module and let $m_1, \dots, m_n \in M$ be homogeneous elements. Then $m_1, \dots, m_n$ generate M if and only if their residue classes $\overline{m}_1, \dots, \overline{m}_n$ generate $M/(R_+M)$.*

Proof. ($\Rightarrow$) This is immediate.

($\Leftarrow$) Let $\overline{M} = M/(\sum_i Rm_i)$. If M/R_+M is generated by $\overline{m}_1, \dots, \overline{m}_n$, then $\overline{M}/R_+\overline{M} = 0$, i.e. $R_+\overline{M} = \overline{M}$. Suppose $\overline{M} \neq 0$, then there exists a nonzero element of least degree in $\overline{M}$ as $\overline{M}$ is finitely generated. But this element cannot be in $R_+\overline{M}$, so $\overline{M} = 0$. Thus, the m_i generate the module M. □

Next, we show that graded ideals stay graded when applying some operations.

Lemma 2.3.11 ([27], Lemma 6, Chapter 8.1)**.** *Let R be a graded ring. Let I, J be homogeneous ideals of R. Then the ideals $\sqrt{I}, I + J, IJ$ and $I \cap J$ are homogeneous.*

Proof. I, J are generated by homogeneous elements, say $I = \langle a_1, \dots, a_s \rangle, J = \langle b_1, \dots, b_t \rangle$.

Let $x \in \sqrt{I}$, i.e. $x^m \in I$ for some m. Take the component x_k of highest degree of x. Then it is clear that $x_k^m \in I$, i.e. $x_k \in \sqrt{I}$. Therefore, $x - x_k \in \sqrt{I}$ and we can repeat the argument to see that all homogeneous components of x lie in $\sqrt{I}$. Thus, $\sqrt{I}$ is homogeneous.

$I + J = \langle a_1, \dots, a_s, b_1, \dots, b_t \rangle$ is generated by homogeneous elements and thus homogeneous.

Let $a \in I \cap J$. Then $a \in I$ and $a \in J$, so all homogeneous components of a are contained in I respectively are contained in J. Thus all homogeneous components of a are contained in $I \cap J$, which implies that $I \cap J$ is homogeneous.

$IJ = \langle a_i b_j : i = 1, \dots, s,\ j = 1, \dots, t \rangle$ is generated by homogeneous elements and is therefore homogeneous. □

Now, we look at what happens when we localize graded rings. They have the useful property that they remain equipped with a grading after localization.

Lemma 2.3.12 ([6], Lemma 3.19)**.** *Let R be a graded ring and let S be a multiplicative set of nonzero homogeneous elements in R. Then $S^{-1}R$ is a graded ring.*

Proof. If $a \in R$ is homogeneous and $\frac{a}{s} \in S^{-1}R$, let $\deg(\frac{a}{s}) = \deg(a) - \deg(s)$ and define a grading on $S^{-1}R$ by setting $(S^{-1}R)_d = \{\frac{a}{s} \in S^{-1}R : a \text{ homogeneous}, \deg(\frac{a}{s}) = d\}$. This satisfies the conditions to be a graded ring. □

As in the ungraded case, it is often of interest to look at prime ideals. As it turns out, to check if a homogeneous ideal is prime, we only need to study its properties on homogeneous elements.

Lemma 2.3.13 ([6], Lemma 3.10)**.** *A homogeneous ideal $\mathfrak{p}$ is prime if and only if for all homogeneous elements $f, g \in R$ with $fg \in \mathfrak{p}$, either $f \in \mathfrak{p}$ or $g \in \mathfrak{p}$.*

Proof. ($\Rightarrow$) This direction is immediate.

($\Leftarrow$) We show the contrapositive. Suppose $\mathfrak{p} \notin \operatorname{Spec}(R)$, so there exist $a, b \in R$ s.t. $ab \in \mathfrak{p}$ but $a, b \notin \mathfrak{p}$. Choose a, b s.t. their compositions into homogeneous components $a = \sum_{i=1}^{n} a_i$ and $b = \sum_{i=1}^{m} b_i$ have a minimal number of homogeneous components. We may assume that $\deg(a_1) < \deg(a_2) < \cdots < \deg(a_n)$ and $\deg(b_1) < \deg(b_2) < \cdots < \deg(b_m)$. Clearly, $a_1 b_1$ is the homogeneous component of ab of smallest degree and therefore in $\mathfrak{p}$ as $\mathfrak{p}$ is homogeneous. Thus one of $a_1, b_1 \in \mathfrak{p}$, say a_1. Then $a' = a - a_1$ satisfies $a'b$ in $\mathfrak{p}$ but $a', b \notin \mathfrak{p}$, which is a contradiction to the choice of a, b since a' has fewer homogeneous components. □

Lemma 2.3.14 ([6], Lemma 3.11)**.** *Let M be a finitely generated graded R-module. Then $\operatorname{Ann}(M)$ is a graded ideal of R.*

Proof. Let $r \in \operatorname{Ann}(M)$ and choose an arbitrary homogeneous generator m of M. Decompose r into homogeneous components $r = \sum_{i=1}^{n} r_i$ s.t. $\deg(r_1) < \deg(r_2) < \cdots < \deg(r_n)$. Then $r_1 m$ is the homogeneous component of smallest degree of rm. Thus $r_1 m = 0$ and $r' = r - r_1 \in \operatorname{Ann}(M)$. Iteratively applying the same argument we see that each homogeneous component of r lies in $\operatorname{Ann}(M)$. □

We can show the same for associated primes.

Proposition 2.3.15 ([6], Proposition 3.14)**.** *Let R be graded and M a finitely generated graded R-module. If $\mathfrak{p} \in \operatorname{Ass}(M)$, then $\mathfrak{p}$ is a graded ideal of R.*

Proof. Let $\mathfrak{p} \in \operatorname{Ass}(M)$, then $\mathfrak{p} = \operatorname{Ann}(m)$ for some nonzero $m \in M$. Let $f = \sum_{j=1}^{s} f_j$ be the decomposition into homogeneous components of $f \in \mathfrak{p}$ s.t. $\deg(f_1) < \deg(f_2) < \cdots < \deg(f_s)$. Similarly decompose $m = \sum_{i=1}^{t} m_i$ s.t. $\deg(m_1) < \deg(m_2) < \cdots < \deg(m_t)$. Observe that $f_1 m_1 = 0$ as the unique term of lowest degree in $fm = 0$.

Now we use induction on t. If $t = 1$, then $m = m_1$, so $f_1 m_1 = f_1 m = 0$, which implies that $f_1 \in \operatorname{Ann}(m)$.
Suppose $t > 1$ and that for all $n \in M$ with $t - 1$ or fewer nonzero homogeneous components s.t. $\operatorname{Ann}(n) \in \operatorname{Spec}(R)$, it holds that $\operatorname{Ann}(n)$ is a graded ideal. Now, suppose by contradiction that $f_1 \notin \mathfrak{p}$ thus, $f_1 m \neq 0$ and $\mathfrak{p}$ is not graded. Note that $f_1 m = \sum_{i=2}^{t} f_1 m_i$, because $f_1 m_1 = 0$ and let $I = \operatorname{Ann}(f_1 m)$. I is proper since $f_1 m \neq 0$. I is also a prime ideal, since if $a, b \in R$ and $ab \in I$, then $abf_1 m = 0$ so, $abf_1 \in \mathfrak{p}$, where $f_1 \notin \mathfrak{p}$. Thus, $ab \in \mathfrak{p}$, so $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. Say $a \in \mathfrak{p}$, i.e. $am = 0$ and therefore $af_1 m = 0$. Then, $a \in I$ and I is prime. By induction hypothesis, I is a graded prime ideal. Also $\mathfrak{p} \subsetneq I$, where the inclusion is strict, since I is graded and $\mathfrak{p}$ is not. Thus, there exists $g \in I \setminus \mathfrak{p}$, which satisfies $gf_1 m = 0$, s.t. $gf_1 \in \mathfrak{p}$. But $\mathfrak{p}$ is prime, so $g \in \mathfrak{p}$, which is a contradiction. Thus, $f_1 \in \mathfrak{p}$.
Iteratively applying the same argument we can conclude that $f_i \in \operatorname{Ann}(m)$ for all $i = 1, \ldots, s$. □

When working with graded rings, we are mainly interested in graded ideals. Thus, for prime ideals that are not necessarily graded we define a graded prime ideal that is closely related.

Definition 2.3.16. For a graded ring R and a prime ideal $\mathfrak{p} \in \operatorname{Spec}(R)$ (not necessarily graded), define $\mathfrak{p}^*$ to be the largest graded ideal contained in $\mathfrak{p}$, i.e. $\mathfrak{p}^*$ is the ideal generated by all homogeneous elements contained in $\mathfrak{p}$.

Lemma 2.3.17 ([8], Lemma 1.5.6)**.** *Let R be a graded ring and let $\mathfrak{p} \in \operatorname{Spec}(R)$. Then $\mathfrak{p}^* \in \operatorname{Spec}(R)$.*

Proof. Clearly, $\mathfrak{p}^*$ is a graded ideal. If $a, b \in R$ are homogeneous elements s.t. $ab \in \mathfrak{p}^* \subseteq \mathfrak{p}$, then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. Since a, b are homogeneous, we have either $a \in \mathfrak{p}^*$ or $b \in \mathfrak{p}^*$. □

With this definition, we can redefine the nilradical in the setting of graded rings.

Lemma 2.3.18. *If R is a graded ring, then* $\mathrm{Nil}(R)$ *is the intersection of all graded prime ideals.*

Proof. Clearly, one has

$$\mathrm{Nil}(R) = \bigcap_{\mathfrak{p} \in \mathrm{Spec}(R)} \mathfrak{p} \subseteq \bigcap_{\substack{\mathfrak{p} \in \mathrm{Spec}(R) \\ \mathfrak{p} \text{ graded}}} \mathfrak{p}.$$

On the other hand, since $\mathfrak{p}^* \subseteq \mathfrak{p}$ is a graded prime ideal for all $\mathfrak{p} \in \mathrm{Spec}(R)$, we have

$$\bigcap_{\substack{\mathfrak{p} \in \mathrm{Spec}(R) \\ \mathfrak{p} \text{ graded}}} \mathfrak{p} \subseteq \bigcap_{\mathfrak{p} \in \mathrm{Spec}(R)} \mathfrak{p}^* \subseteq \bigcap_{\mathfrak{p} \in \mathrm{Spec}(R)} \mathfrak{p} = \mathrm{Nil}(R). \qquad \square$$

While in a field, every nonzero element is invertible, it is also interesting to look at graded rings, where all nonzero homogeneous elements are invertible.

Definition 2.3.19. A *graded field* is a graded ring R, in which every nonzero homogeneous element is invertible.

Lemma 2.3.20 ([8], Lemma 1.5.7)**.** *Let R be a graded field. Then R_0 is a field and either $R_i = 0$ for all $i \neq 0$ or $R \cong R_0[t, t^{-1}]$ as a graded ring with* $\deg(t) > 0$.

Proof. Every nonzero homogeneous element is invertible, so clearly R_0 is a field, say k. If $R = R_0$, then R is a field. Otherwise, $\deg(t) > 0$ for some nonzero homogeneous element t of minimal positive degree. Since t is invertible, there is a homomorphism $\varphi : k[T, T^{-1}] \to R$, where φ is the identity on $k \to R_0$ and $\varphi(T) = t$. $k[T, T^{-1}]$ is equipped with a grading by setting $\deg(T) = d$.

Let $f \in \ker(\varphi), f = \sum_{i \in \mathbb{Z}} a_i T^i, a_i \in k$. Then $0 = \varphi(f) = \sum_{i \in \mathbb{Z}} a_i t^i$, so $a_i t^i = 0$ for all $i \in \mathbb{Z}$. Thus, $a_i = (a_i t^i) t^{-i} = 0$ for all $i \in \mathbb{Z}$ since t is invertible. Thus, $f = 0$, i.e. φ is injective.

Let $a \in R$ be a nonzero homogeneous elements of degree i. If $i = 0$, then $a \in \mathrm{Im}(\varphi)$. Otherwise $i \neq 0$ and write $i = jd + r$, with $0 \leq r < d$. Clearly, at^{-j} has degree r. So $r = 0$ as d was chosen to be minimal. Therefore, $a = bt^j$ for some $b \in R_0$, i.e. $a = \varphi(bT^j) \in \mathrm{Im}(\varphi)$.
Thus, φ is an isomorphism. □

Remark 2.3.21. Let k be a field and let $S = \{t^i : i \in \mathbb{Z}_{\geq 0}\}$ be a multiplicative set of $R = k[t]$. Then $S^{-1}R \cong K[t, t^{-1}]$, which is a PID, since R is a PID by Lemma 2.1.56.

2.4 Krull Dimension

We now introduce the concept of Krull dimension, which is an important invariant of rings and modules. The main results are based on [6, Chapters 2 and 3].

2.4.1 The Ungraded Case

First, we look at the general case without grading.

Definition 2.4.1. A *chain of prime ideals* in R is a sequence of prime ideals $(\mathfrak{p}_i)_{i \geq 0}^l$ in R s.t. $\mathfrak{p}_i \subsetneq \mathfrak{p}_{i+1}$ for all $i = 1, \ldots, l$.
The number l is called the *length* of the chain $(\mathfrak{p}_i)_{i \geq 0}^l$ and corresponds to the number of proper inclusions in the chain.
A prime ideal chain $(\mathfrak{p}_i)_{i \geq 0}^l$ with $\mathfrak{p}_l = \mathfrak{p}$ is said to be *below* $\mathfrak{p}$.

Definition 2.4.2. The *Krull dimension* of a ring R is the supremum of the lengths of all chains of prime ideals in R, i.e.

$$\operatorname{kdim}(R) = \sup\{l \in \mathbb{Z}_{\geq 0} : (\mathfrak{p}_i)_{i\geq 0}^{l} \text{ is a prime ideal chain in } R\}.$$

The Krull dimension of an R-module M is defined to be $\operatorname{kdim}(M) = \operatorname{kdim}(R/\operatorname{Ann}(M))$.

Remark 2.4.3. Clearly, all Noetherian rings and modules have finite Krull dimension.

Lemma 2.4.4. *Let R be a PID that is not a field. Then* $\operatorname{kdim}(R) = 1$.

Proof. Since R is a domain, $\langle 0\rangle$ is a prime ideal, which is contained in any other prime ideal of R. Since R is not a field, there are nonzero prime ideals. Let $\mathfrak{p}$ be such a nonzero prime ideal and suppose it is not maximal. Then, there exists a maximal ideal $\mathfrak{q} \in \operatorname{Spec}(R)$ properly containing $\mathfrak{p}$. Since R is a PID, there exists $b \in \mathfrak{q}$ and $a \in \mathfrak{p}$ s.t. $\mathfrak{q} = \langle b\rangle$ and $\mathfrak{p} = \langle a\rangle$ and one can write $a = br$ for some $r \in R$. $\mathfrak{p}$ is prime and $b \notin \mathfrak{p}$, thus $r \in \mathfrak{p}$ and one can write $r = as$ for some $s \in R$. This gives $a = a(bs)$ i.e. $a(1 - bs) = 0$. Since R is a domain and $\mathfrak{p} \neq 0$, this forces $bs = 1 \in \mathfrak{q}$, which is a contradiction, since $\mathfrak{q}$ is a proper maximal ideal. Therefore, the longest chain of prime ideals of R is $\langle 0\rangle \subsetneq \mathfrak{p}$, i.e. $\operatorname{kdim}(R) = 1$. □

It is also of interest to look at chains of prime ideals contained in an ideal.

Definition 2.4.5. Given a prime ideal $\mathfrak{p} \in \operatorname{Spec}(R)$, the *height* of $\mathfrak{p}$ is defined to be the supremum of lengths of chains of prime ideals below $\mathfrak{p}$, i.e.

$$\operatorname{ht}(\mathfrak{p}) = \sup\{l \in \mathbb{Z}_{\geq 0} : (\mathfrak{p}_i)_{i\geq 0}^{l} \text{ is a prime ideal chain below } \mathfrak{p}\}.$$

The height of an ideal I is the infimum of all heights of prime ideals containing I, i.e.

$$\operatorname{ht}(I) = \inf\{\operatorname{ht}(\mathfrak{p}) : I \subseteq \mathfrak{p} \in \operatorname{Spec}(R)\}.$$

2.4.2 The Graded Case

We now look at prime ideal chains in graded rings. Since not all maximal chains in a ring necessarily have the same length, it is not trivially true that the Krull dimension equals the length of the longest chain of graded prime ideals. We show that this is indeed the case nevertheless.

To do so, recall the definition of $\mathfrak{p}^*$ from Definition 2.3.16.

Lemma 2.4.6 ([6], Lemma 3.21)**.** *Let R be a graded ring and let $\mathfrak{p} \in \operatorname{Spec}(R)$. If $\mathfrak{q} \in \operatorname{Spec}(R)$ and $\mathfrak{p}^* \subseteq \mathfrak{q} \subseteq \mathfrak{p}$, then either $\mathfrak{q} = \mathfrak{p}$ or $\mathfrak{q} = \mathfrak{p}^*$.*

Proof. If $\mathfrak{p}$ is graded, then $\mathfrak{p}^* = \mathfrak{p}$ and the result follows.

Suppose that $\mathfrak{p}$ is not graded, i.e. $\mathfrak{p}^* \subsetneq \mathfrak{p}$. The inclusion preserving correspondence for primes containing $\mathfrak{p}^*$ yields a set of primes in $R/\mathfrak{p}^*$:

$$\mathfrak{p}^* \subseteq \mathfrak{q} \subseteq \mathfrak{p} \leftrightarrow \mathfrak{p}^*/\mathfrak{p}^* \subseteq \mathfrak{q}/\mathfrak{p}^* \subseteq \mathfrak{p}/\mathfrak{p}^*.$$

Thus, by replacing R by $R/\mathfrak{p}^*$, we may assume that R is an integral domain and $\mathfrak{p}^* = 0$, which gives $\langle 0\rangle \subseteq \mathfrak{q} \subseteq \mathfrak{p}$. Let $S = \{s \in R : s \text{ homogeneous}, \ s \neq 0\}$, which is a multiplicative set of homogeneous elements in R, not containing 0. So by 2.3.12, one can construct the graded ring $S^{-1}R$. Since $\mathfrak{p}^* = 0$, $\mathfrak{p}$ contains no nonzero homogeneous elements, i.e. $S \cap \mathfrak{p} = \emptyset$. By Corollary 2.1.55, there is a bijection between the set of prime ideals (graded or not) in $S^{-1}R$ and the set of prime ideals in R not intersecting S. The ring $S^{-1}R$ is graded and by the choice of S, every homogeneous element in $S^{-1}R$ has an inverse. Therefore, $S^{-1}R$ is a graded field. So by Remark 2.3.21 and Lemma 2.3.20, it is either a field or a PID, which means that the Krull dimension is either 0 or 1, respectively.
But since $\langle 0\rangle \subseteq S^{-1}\mathfrak{q} \subseteq S^{-1}\mathfrak{p}$ is a chain of prime ideals, either $S^{-1}\mathfrak{q} = 0$ or $S^{-1}\mathfrak{q} = S^{-1}\mathfrak{p}$. So using the usual correspondence again, we have either $\mathfrak{q} = 0 = \mathfrak{p}^*$ or $\mathfrak{q} = \mathfrak{p}$. □

Proposition 2.4.7 ([8], Theorem 1.5.8)**.** *Let R be a graded ring, $\mathfrak{p} \in \operatorname{Spec}(R)$ and let $d = \operatorname{ht}(\mathfrak{p})$. There exists a chain of prime ideals*

$$\mathfrak{q}_0 \subsetneq \cdots \subsetneq \mathfrak{q}_d = \mathfrak{p}$$

s.t. $\mathfrak{q}_0, \ldots, \mathfrak{q}_{d-1}$ are all graded.

Proof. This is shown by induction on d.

If $d = 1$, there is a chain $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 = \mathfrak{p}$ that cannot be elongated below $\mathfrak{p}$. Thus, $\mathfrak{p}_0 \in \operatorname{Min}(R)$ and $\mathfrak{p}_0 \in \operatorname{Ass}(R)$ is graded by Proposition 2.3.15.

Let $d > 1$ and assume by induction that the claim holds for $d-1$. Let $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_d = \mathfrak{p}$ be a prime ideal chain below $\mathfrak{p}$ that cannot be elongated. It is clear that $\operatorname{ht}(\mathfrak{p}_{d-1}) = d-1$. By induction hypothesis, there exists a chain $\mathfrak{q}_0 \subsetneq \cdots \subsetneq \mathfrak{q}_{d-2} \subsetneq \mathfrak{p}_{d-1} \subsetneq \mathfrak{p}_d$, where all the $\mathfrak{q}_i$ are graded prime ideals. We distinguish two cases.

(*case 1*) $\mathfrak{p}_d = \mathfrak{p}$ not graded. By $\mathfrak{q}_{d-2} \subsetneq \mathfrak{p}_{d-1}$ one gets that $\mathfrak{q}_{d-2}^* \subseteq \mathfrak{p}_{d-1}^*$, where $\mathfrak{q}_{d-2} = \mathfrak{q}_{d-2}^*$ as it is graded. Therefore, we have

$$\mathfrak{q}_{d-2} \subseteq \mathfrak{p}_{d-1}^* \subseteq \mathfrak{p}_d^* \subsetneq \mathfrak{p}_d,$$

where the last inclusion is proper, since $\mathfrak{p}_d$ is not graded. Suppose, $\mathfrak{p}_d^* = \mathfrak{q}_{d-2}$, then we get $\mathfrak{p}_d^* \subseteq \mathfrak{p}_{d-1} \subsetneq \mathfrak{p}_d$. But $\mathfrak{p}_{d-1} \neq \mathfrak{q}_{d-2}$ and $\mathfrak{p}_{d-1} \neq \mathfrak{p}_d$, which is a contradiction to Lemma 2.4.6. Therefore, $\mathfrak{q}_{d-2} \subsetneq \mathfrak{p}_d^* \subsetneq \mathfrak{p}_d$. So by taking $\mathfrak{q}_{d-1} = \mathfrak{p}_d^*$ we can conclude this case.

(*case 2*) $\mathfrak{p}_d = \mathfrak{p}$ graded. Since $\mathfrak{q}_{d-2} \subsetneq \mathfrak{p}_d$ are graded, we can choose a nonzero homogeneous element $a \in \mathfrak{p}_d \setminus \mathfrak{q}_{d-2}$. Let $I = \langle \mathfrak{q}_{d-2}, a \rangle \subseteq \mathfrak{p}_d$, which is graded. There is a minimal prime $\mathfrak{q}_{d-1}$ over I, which is contained in $\mathfrak{p}_d$. But is also graded, since it is a minimal prime in R/I and therefore in $\operatorname{Ass}(R/I)$. As $I/\mathfrak{q}_{d-2}$ is a principal ideal generated by $a + \mathfrak{q}_{d-2}$ in the integral domain $R/\mathfrak{q}_{d-2}$ and $\mathfrak{q}_{d-1}/\mathfrak{q}_{d-2}$ is minimal over $I/\mathfrak{q}_{d-2}$, it follows that $\operatorname{ht}(\mathfrak{q}_{d-1}) = \operatorname{ht}(\mathfrak{q}_{d-2}) + 1 = d-1$. As $\operatorname{ht}(\mathfrak{p}_d) = d$, it follows that $\mathfrak{q}_{d-1} \subsetneq \mathfrak{p}_d$. This yields a chain $\mathfrak{q}_0 \subsetneq \cdots \subsetneq \mathfrak{q}_{d-1} \subsetneq \mathfrak{q}_d = \mathfrak{p}_d = \mathfrak{p}$, where all $\mathfrak{q}_i$ are graded prime ideals. □

2.5 Monomials and Monomial Ideals

After introducing grading, we can look at a fundamental case of graded ideals, the monomial ideals. Monomial ideals will be central to the study of Gröbner bases in Chapter 5. The following section is based on [30, Chapter 1].

2.5.1 Monomials and Polynomials

First, we have to introduce the notion of monomials and polynomials that are heavily used throughout the rest of the thesis.

Definition 2.5.1. Let $R = k[x_1, \ldots, x_n]$ be the polynomial ring in n variables. R is equipped with *standard grading*, by setting $\deg(x_1) = \cdots = \deg(x_n) = 1$. This grading turns R into an $\mathbb{N}$-*graded ring*.

Unless mentioned otherwise, we assume that $R = k[x_1, \ldots, x_n]$ is standard graded for the rest of the thesis.

Definition 2.5.2. A *monomial* in the variables $x_1, \ldots, x_n$ is a product of the form

$$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n},$$

where the exponents α_i are nonnegative integers. We can rewrite the notation as x^α, where $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$ is the vector of exponents. The degree of x^α is $|\alpha| = \alpha_1 + \cdots + \alpha_n$. Note that if $\alpha = (0, 0, \ldots, 0)$, then $x^\alpha = 1$. The set of all monomials in R is denoted $\operatorname{Mon}(R)$.

Remark 2.5.3. The set $\mathrm{Mon}(R)$ is clearly a k-basis of R.

Looking at linear combinations of monomials with coefficients in k, we can define multivariate *polynomials*.

Definition 2.5.4. A *polynomial* $f \in R$ is a finite linear combination of monomials with coefficients in k. It can be written in the form

$$f = \sum_\alpha c_\alpha x^\alpha,$$

where the sum is over finitely many n-tuples $\alpha = (\alpha_1, \ldots, \alpha_n)$. The c_α are called the *coefficients of* x^α and the products $c_\alpha x^\alpha$ with $c_\alpha \in k \setminus \{0\}$ are called the *terms of* f. The *total degree of* f is the maximum $|\alpha|$ s.t. $c_\alpha \neq 0$. The total degree of the zero-polynomial $f = 0$ is not defined. The set $\{x^\alpha | c_\alpha \neq 0\}$ is called the *support of* f denoted $\mathrm{Supp}(f)$.
For $d \geq 0$, the set

$$R_d = \{f \in R \mid \deg(t) = d \text{ for all } t \in \mathrm{Supp}(f)\}$$

is a vector space consisting of *homogeneous polynomials of degree* d.

Having introduced these notions, allows us to prove some very important results.

Theorem 2.5.5 (Hilbert Basis Theorem, [1], Lemma 16.11)**.** *If R is Noetherian, then $R[X]$ is Noetherian.*

Proof. Suppose by contradiction that there exists an ideal I of $R[X]$ which cannot be generated by finitely many elements. Set $I_0 = \langle 0 \rangle$. Inductively for each $i \geq 1$, choose a polynomial $f_i \in I \setminus I_{i-1}$ of minimal degree d_i and define $I_i = \langle f_1, \ldots, f_i \rangle$. Let a_i be the coefficient of the highest degree term of f_i and define J to be the ideal, which is generated by all the a_i. We have $J = \langle a_1, \ldots, a_n \rangle$ for some n, as R is Noetherian. Then $a_{n+1} = r_1 a_1 + \cdots + r_n a_n$ for some $r_i \in R$. Clearly, we have $d_i \leq d_{i-1}$ for all i. Now set

$$f = f_{n+1} - (r_1 f_1 x^{d_{n+1}-d_1} + \cdots + r_n f_n x^{d_{n+1}-d_n}).$$

The total degree of f is less than d_{n+1}, so $f \in I_n$. Thus, $f_{n+1} \in I_n$, which is a contradiction. □

Corollary 2.5.6. *If R is notherian, then $R[x_1, \ldots, x_n]$ is Noetherian.*

Proof. This can easily be shown by induction and iteratively using the Hilbert basis theorem 2.5.6 combined with the fact that $R[x_1, \ldots, x_{i-1}][x_i] \cong R[x_1, \ldots, x_{i-1}, x_i]$ for all $i = 1, \ldots, n$. □

Thus, it follows that every ideal $I \subseteq R = k[x_1, \ldots, x_n]$ is finitely generated.
Next, we prove a result that will be useful later.

Theorem 2.5.7 (Artin–Rees Lemma, [37], Theorem 8.5)**.** *Let R be Noetherian and let M be a finitely generated R-module. Let $N \subseteq M$ be a submodule and let I be an ideal over R. Then, there exists a positive integer c s.t. for all $n \geq c$ one has*

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

Proof. ($\supseteq$) This clearly holds for all $c \in \mathbb{Z}_{\geq 0}$.

($\subseteq$) Let $I = \langle a_1, \ldots, a_r \rangle$ and suppose M is generated by $w_1, \ldots, w_s$. Let $B = R[x_1, \ldots, x_n]$ be standard graded. Then an element of $I^n M$ has the form

$$\sum_{i=1}^{s} f_i(a) w_i, \text{ where } f(a) = f(a_1, \ldots, a_r) \in B_n.$$

For $n > 0$, set

$$J_n = \{(f_1, \ldots, f_s) \in B^s : f_i \in B_n \text{ and } \sum_{i=1}^{s} f_i(a)w_i \in N\}.$$

Let $C \subseteq B^s$ be the B-submodule generated by $\bigcup_{n>0} J_n$. As B is a Noetherian ring, C is finitely generated by linear combinations of elements in $\bigcup_{n>0} J_n$, i.e. C is generated by finitely many elements of $\bigcup_{n>0} J_n$. Suppose C is generated by $u_1, \ldots, u_t$, where $u_j = (u_{j1}, \ldots, u_{js}) \in J_{d_j}$ for $i = 1, \ldots, t$. Set $c = \max\{d_1, \ldots, d_t\}$. Now, if $y \in I^n M \cap N$, one can write $y = \sum_{i=1}^{s} f_i(a)w_i$ with $(f_1, \ldots, f_s) \in J_n$, thus $(f_1, \ldots, f_s) = \sum_{j=1}^{t} p_j(x)u_j, p_j \in B, u_j \in J_{d_j}$. Since the LHS consists of elements of degree n, the terms of degree other than n on the RHS must cancel. Therefore, it can be assumed that $p_j(x)$ are homogeneous polynomials of degree $n - d_j$ respectively. Then,

$$y = \sum_{i=1}^{s} f_i(a)w_i = \sum_{j=1}^{t} p_j(a) \sum_{i=1}^{s} u_{ji}(a)w_i, \text{ and } \sum_{i=1}^{s} u_{ji}(a)w_i \in I^{d_j} M \cap N.$$

Thus, if $n \geq c$ then $p_j(a) \in I^{n-c} I^{c-d_j}$ implies that $y \in I^{n-c}(I^c M \cap N)$. □

2.5.2 Monomial Ideals

Monomial ideals are one of the most fundamental cases of graded ideals. For us they are important, as many properties of polynomial ideals can be deduced from the ideal generated by the initial monomials, which we will introduce in Chapter 5.

Definition 2.5.8. An ideal I of R is called a *monomial ideal* if it is generated by monomials. $\mathrm{Mon}(I)$ denotes the set of all monomials contained in I.

Proposition 2.5.9 ([30], Theorem 1.1.2)**.** *Let I be a monomial ideal. Then $\mathrm{Mon}(I)$ is a k-basis of I.*

Proof. The elements of $\mathrm{Mon}(I)$ are clearly linearly independent as $\mathrm{Mon}(I) \subseteq \mathrm{Mon}(R)$, which is a k-basis of R.

Let $f \in I$. Then $f = \sum_{i=1}^{m} f_i u_i$ for some $u_1, \ldots, u_m \in \mathrm{Mon}(I)$ and $f_1, \ldots, f_m \in R$. Thus, $\mathrm{Supp}(f) \subseteq \bigcup_{i=1}^{m} \mathrm{Supp}(f_i u_i)$. Note that $\mathrm{Supp}(f_i u_i) \subseteq \mathrm{Mon}(I)$ for all i, since each $v \in \mathrm{Supp}(f_i u_i)$ is of the form $wu_i \in \mathrm{Mon}(I)$ for some $w \in \mathrm{Mon}(R)$. Thus, $\mathrm{Supp}(f) \subseteq \mathrm{Mon}(I)$, which implies that $\mathrm{Mon}(I)$ is a generating set of the k-space I. □

Monomial ideals can be characterized similarly to homogeneous ideals.

Corollary 2.5.10 ([30], Corollary 1.1.3)**.** *Let I be an ideal of R. The following are equivalent:*

(a) *I is a monomial ideal.*

(b) *For $f \in R$ one has that $f \in I$ if and only if $\mathrm{Supp}(f) \subseteq I$.*

Proof. $(a \Rightarrow b)$ This follows immediately from the proof of Proposition 2.5.9.

$(b \Rightarrow a)$ Suppose I is generated by $f_1, \ldots, f_m \in I$. Then $\bigcup_{i=1}^{m} \mathrm{Supp}(f_i) \subseteq I$, since $\mathrm{Supp}(f_i) \in I$ for $i = 1, \ldots, m$. This is clearly a set of generators of I consisting of monomials. □

Remark 2.5.11. Two monomial ideals are the same if and only if they contain the same monomials.

Corollary 2.5.12 ([30], Corollary 1.1.4)**.** *Let I be a monomial ideal. The residue classes of the monomials not in I form a k-basis of R/I.*

Proof. Let $S = \mathrm{Mon}(R) \setminus \mathrm{Mon}(I)$. Clearly, the set $\bar{S}$ of residue classes of S generates the k-space R/I. Suppose by contradiction that there is some linear relation

$$\sum_{s \in S} a_s \bar{s} = 0.$$

Then, $f = \sum_{s \in S} a_s s \in I$. Corollary 2.5.10 implies that $s \in I$ for all $s \in S$ with $a_s \neq 0$. Thus, the relation is trivial. □

Proposition 2.5.13 ([15], Lemma 2, Chapter 2.4)**.** *Let $I = \langle u \in A \rangle$ for some $A \subseteq \mathrm{Mon}(R)$ be a monomial ideal and let $v \in \mathrm{Mon}(R)$. Then $v \in I$ if and only if $u|v$ for some $u \in A$.*

Proof. ($\Rightarrow$) If $u|v$ for some $u \in A$, then $v \in I$.

($\Leftarrow$) If $v \in I$, then $v = \sum_{u_a \in A} c_a u_a$, where $c_a \in R$. By decomposing each c_a as a sum of terms, one obtains

$$v = \sum_{u_a \in A} c_a u_a = \sum_{u_a \in A} \left(\sum_i b_i w_i \right) u_a = \sum_{u_a \in A, i} b_i w_i u_a,$$

for some $w_i \in \mathrm{Mon}(R)$. On the RHS every term $b_i w_i u_a$ is clearly divisible by some $u_a \in A$. Therefore, the same must hold for the LHS, i.e. v must be divisible by some $u_a \in A$. □

As it turns out, we can always choose a finite set of monomials to generate a monomial ideal.

Theorem 2.5.14 (Dickson's Lemma, [15], Theorem 5, Chapter 2.4)**.** *Let $I = \langle u \in A \rangle$ for some $A \subseteq \mathrm{Mon}(R)$ be a monomial ideal. Then there is a finite subset $B \subseteq A$ s.t. $I = \langle u \in B \rangle$.*

Proof. This is shown by induction on n. If $n = 1$ then I is clearly principal since $k[x]$ is a PID.

Suppose $n > 1$ and the result holds for $n - 1$. Let $J_k = (I : x_n^k) \cap k[x_1, \ldots, x_{n-1}] = \langle B_k \rangle$, where we can choose $B_k \subseteq \mathrm{Mon}(k[x_1, \ldots, x_{n-1}])$ to be finite by induction hypothesis. Clearly, $J_0 \subseteq J_1 \subseteq \cdots \subseteq J_i \subseteq J_{i+1} \subseteq \cdots$. Since $k[x_1, \ldots, x_{n-1}]$ is Noetherian, there is $s \geq 0$ s.t. $J_{s+i} = J_s$ for all $i \geq 0$, i.e. $B_{s+i} = B_s$.
Let $m \in \mathrm{Mon}(I)$. Then $m = m' x_n^k$ for some $k \geq 0$, thus $m' \in J_k = \langle B_k \rangle$, i.e. $m \in \langle x_n^k B_k \rangle$. Therefore, I is generated by the finite set of monomials $B = B_0 \cup x_n B_1 \cup \cdots \cup x_n^s B_s \subseteq A$. □

Not only is it always possible to choose a finite set of monomial generators, but if it is also chosen to be minimal, then it is unique.

Proposition 2.5.15 ([30], Proposition 1.1.6)**.** *A monomial ideal I of R has a unique minimal set of monomial generators.*

Proof. Suppose there are two minimal sets $G_1 = \{u_1, \ldots, u_r\}$ and $G_2 = \{v_1, \ldots, v_s\}$ of monomial generators of I. Since $u_i \in I$, then $u_i = w_1 v_j$ for some monomial w_1 and $v_j \in G_2$. Similarly, there are monomials $u_k \in G_1, w_2$ s.t. $v_j = w_2 u_k$. Therefore, $u_i = w_1 w_2 u_k$. As G_1 is minimal, it follows that $k = i$ and $w_1 w_2 = 1$, i.e. $w_1 = 1$. Thus $u_i = v_j \in G_2$ and therefore $G_1 \subseteq G_2$. Similarly $G_2 \subseteq G_1$, which concludes the proof. □

The unique minimal set of monomial generators of I is denoted by $G(I)$.

Definition 2.5.16. Let $x^\alpha, x^\beta \in \mathrm{Mon}(R)$ with $\alpha = (a_1, \ldots, a_n), \beta = (b_1, \ldots, b_n) \in \mathbb{Z}^n_{\geq 0}$.

(a) Let $d = (d_1, \ldots, d_n) \in \mathbb{Z}^n_{\geq 0}$, with $d_i = \max\{a_i, b_i\}$. Then $\mathrm{lcm}\{x^\alpha, x^\beta\} = x^d$ is called the *least common multiple* (*lcm*) of x^α and x^β.

(b) Let $\eta = (\eta_1, \ldots, \eta) \in \mathbb{Z}^n_{\geq 0}$, with $\eta_i = \min\{a_i, b_i\}$. Then $\gcd\{x^\alpha, x^\beta\} = x^\eta$ is called the *greatest common divisor* (*gcd*) of x^α and x^β.

Proposition 2.5.17 ([30], Propositions 1.2.1 and 1.2.2)**.** *Let I, J be monomial ideals of R. Then*

(a) *$I \cap J$ is a monomial ideal,*

(b) *$(I : J)$ is a monomial ideal.*

Proof. (a) Let $f \in I \cap J$. Then, by Corollary 2.5.10 $\mathrm{Supp}(f) \in I \cap J$. Applying Corollary 2.5.10 again implies that $I \cap J$ is monomial.

(b) Let $f \in (I : J)$. Then $fv \in I$ for all $v \in G(J)$. Clearly, by Corollary 2.5.10, we have $\mathrm{Supp}(f)v = \mathrm{Supp}(fv) \subseteq I$. So $\mathrm{Supp}(f) \subseteq (I : J)$, which implies that $(I : J)$ is monomial. □

To study the primary decomposition of monomial ideals, we first show that a monomial ideal can be expressed as the intersection of monomial ideals that are generated by pure powers of variables.

Theorem 2.5.18 ([30], Theorem 1.3.1)**.** *Let I be a monomial ideal of R. Then $I = \bigcap_{i=1}^{m} \mathfrak{q}_i$, where each $\mathfrak{q}_i$ has the form $(x_{i_1}^{a_1}, \ldots, x_{i_k}^{a_k})$.*

Proof. Let $G(I) = \{u_1, \ldots, u_r\}$. Assume that u_i is not a pure power for some i. We may assume that this is the case for u_1. Then, it is possible to write $u_1 = vw$, for some $v, w \neq 1$, s.t. $\gcd(v, w) = 1$. Now we show that $I = I_1 \cap I_2$, where $I_1 = (v, u_2, \ldots, u_r), I_2 = (w, u_2, \ldots, u_r)$.

Clearly, $I \subseteq I_1 \cap I_2$.

On the other hand let $u \in I_1 \cap I_2$ be a monomial. If $u_i | u$ for some u_i, then $u \in I$. Otherwise u is multiple of v and w. Thus, it is also a multiple of u_1, since $\gcd(v, w) = 1$. Therefore, $u \in I$.

If $G(I_1)$ or $G(I_2)$ contain elements, that are not pure powers, then by iteratively applying the procedure that was just described, we can obtain a presentation of I as an intersection of the desired form. □

Example 2.5.19. Let $I = \langle x^2, xy \rangle \subseteq k[x, y]$ be a monomial ideal. Then

$$I = \langle x^2, x \rangle \cap \langle x^2, y \rangle = \langle x \rangle \cap \langle x^2, y \rangle.$$

Proposition 2.5.20 ([30], Proposition 1.3.7)**.** *A monomial ideal of the form $(x_{i_1}^{a_1}, \ldots, x_{i_k}^{a_k})$ is $(x_{i_1}, \ldots, x_{i_k})$-primary.*

Proof. Let $\mathfrak{q} = (x_{i_1}^{a_1}, \ldots, x_{i_k}^{a_k})$ and $\mathfrak{p} = (x_{i_1}, \ldots, x_{i_k})$. Since $\mathfrak{p} \in \mathrm{Min}(\mathfrak{q})$ it follows that $\mathfrak{p}$ belongs to $\mathfrak{q}$ and thus, $\mathfrak{p} \in \mathrm{Ass}(R/\mathfrak{q})$.
For $m = \sum_{i=1}^{k} a_i$ we have $\mathfrak{p}^m \subseteq \mathfrak{q}$. Thus $\mathfrak{p} = \mathrm{Min}(\mathfrak{q})$. So if $\mathfrak{p}' \in \mathrm{Ass}(R/\mathfrak{q}) \setminus \mathfrak{p}$, then $\mathfrak{p} \subsetneq \mathfrak{p}'$.
If $\mathfrak{p}' \in \mathrm{Ass}(R/\mathfrak{q})$, then by Proposition 2.1.36, one can find $g \in R$ s.t. $\mathfrak{p}' = (\mathfrak{q} : g)$. Now, suppose that $\mathfrak{p}' \neq \mathfrak{p}$, then $\mathfrak{p}'$ contains a polynomial f s.t. $x_{i_j} \nmid u$ for all $u \in \mathrm{Supp}(f)$ and $j = 1, \ldots, k$. Therefore, f is a nonzerodivisor on $R/\mathfrak{q}$. Since $fg \in \mathfrak{q}$, it follows that $g \in \mathfrak{q}$ and thus, by Lemma 2.1.27, we have that $\mathfrak{p}' = R$, which is a contradiction. Thus, $\mathrm{Ass}(R/\mathfrak{q}) = \{\mathfrak{p}\}$, which implies that $\mathfrak{q}$ is $\mathfrak{p}$-primary. □

This shows that the decomposition in Theorem 2.5.18 is a primary decomposition of I. By omitting those ideals containing the intersection of others and using the fact that the intersection of $\mathfrak{p}$-primary ideals is $\mathfrak{p}$-primary, one may construct a minimal primary decomposition of I. From this, the next result follows immediately.

Corollary 2.5.21 ([30], Corollary 1.3.9)**.** *Let I be a monomial ideal. Then $\mathrm{Ass}(I)$ consists of monomial prime ideals.*

Proof. $\mathrm{Ass}(R/I)$ are the prime ideals $\mathfrak{p}_i$ belonging to I of the form $(x_{i_1}, \ldots, x_{i_k})$, which clearly are monomial prime ideals. □

Chapter 3

Homological Algebra

This chapter is an introduction to the concepts of homological algebra used throughout the remaining thesis. We start by presenting the concept of exact sequences and some important results like the snake lemma. Then we study free resolutions and some of their properties. Next, we study injective modules and injective resolutions. Finally, we discuss local cohomology and present some important results.

3.1 Exact Sequences

Exact sequences are a very handy tool that we will use to show many results. The following introduction is based on [48, Chapter 1].

Definition 3.1.1. A *chain complex* is a collection $\mathcal{M} = (M_i)_{i\in\mathbb{Z}}$ of finitely generated R-modules and R-linear maps $\partial = (\partial_i)_{i\in\mathbb{Z}}$ s.t. $\partial_i : M_i \to M_{i-1}$ satisfies $\partial_i \circ \partial_{i+1} = 0$. It is denoted as $(\mathcal{M}, \partial)$ or simply $\mathcal{M}$ and can be written as

$$\cdots \to M_{i+1} \overset{\partial_{i+1}}{\to} M_i \overset{\partial_i}{\to} M_{i-1} \to \cdots$$

It is called *positive* if $M_i = 0$ for all $i < 0$. In other words, it looks like this:

$$\cdots \to M_i \to M_{i-1} \to \cdots \to M_1 \to M_0 \to 0.$$

The morphisms ∂_i are called *boundaries*.
A complex $(\mathcal{N}, d)$ is said to be a *subcomplex* of $(\mathcal{M}, \partial)$ if N_i is a submodule of M_i and $d_i = \partial|_{N_i}$ for all $i \in \mathbb{Z}$.
If $(\mathcal{N}, d)$ is a subcomplex of $(\mathcal{M}, \partial)$, then the quotient complex $(\mathcal{M}/\mathcal{N})$ is defined to be

$$\cdots \to M_{i+1}/N_{i+1} \overset{\bar{\partial}_{i+1}}{\to} M_i/N_i \to \cdots$$

where $\bar{\partial}_{i+1} : m + N_{i+1} \mapsto \partial_{i+1}(m) + N_i$.

Definition 3.1.2. A *cochain complex* is a collection $\mathcal{M} = (M^i)_{i\in\mathbb{Z}}$ of finitely generated R-modules and R-linear maps $\partial = (\partial^i)_{i\in\mathbb{Z}}$ s.t. $\partial^i : M^i \to M^{i+1}$ satisfies $\partial^i \circ \partial^{i-1} = 0$. It is called *positive* if $M^i = 0$ for all $i < 0$. In other words, it looks like this:

$$0 \to M^0 \to M^1 \to \cdots \to M^i \to M^{i+1} \to \cdots .$$

To every chain complex and cochain complex respectively, one can associate some important structures.

Definition 3.1.3.

(a) For a chain complex $\mathcal{M}$ the group $H_i(\mathcal{M}) = \ker(\partial_i)/\operatorname{Im}(\partial_{i+1})$ is called the *i-th homology group* of $\mathcal{M}$.

(b) For a cochain complex $\mathcal{M}$ the group $H^i(\mathcal{M}) = \ker(\partial^i)/\operatorname{Im}(\partial^{i-1})$ is called the *i-th cohomology group* of $\mathcal{M}$.

The cochain complex is the dual notion of the chain complex. Since every cochain complex can be seen as a chain complex, by setting $\partial^i = \partial_{-i}$ and $M^i = M_{-i}$ for all $i \in \mathbb{Z}$. Therefore, we will state and prove most results only for the case of chain complexes. However, a dual result also holds for cochain complexes. From now on, by writing complex, we mean chain complexes.

Definition 3.1.4. A complex $\mathcal{M}$ is said to be

(a) *exact at i-th position* if $H_i(\mathcal{M}) = 0$, i.e. $\ker(\partial_i) = \operatorname{Im}(\partial_{i+1})$,

(b) *exact* if it is exact at i-th position for all i (except possibly the first and last one, if the complex is finite).

An exact complex is also called *exact sequence*.

The most important exact sequences are of the form

$$0 \to A \to B \to C \to 0$$

for some modules A, B, C. Exact sequences of this form are called *short exact sequences*.
It is possible to express many important properties by means of exact sequences.

Proposition 3.1.5 ([31], Corollary 2.18)**.** *Let A, B be R-modules and $\varphi : A \to B$ be an R-module homomorphism.*

(a) $0 \to A \xrightarrow{\varphi} B$ *is exact if and only if φ is injective.*

(b) $A \xrightarrow{\varphi} B \to 0$ *is exact if and only if φ is surjective.*

(c) $0 \to A \xrightarrow{\varphi} B \to 0$ *is exact if and only if φ is an isomorphism.*

Proof. (a) $0 \to A \xrightarrow{\varphi} B$ is exact if and only if $\ker(\varphi) = \operatorname{Im}(0 \to A) = \{0\}$ if and only if φ is injective.

(b) $A \xrightarrow{\varphi} B \to 0$ is exact if and only if $\operatorname{Im}(\varphi) = \ker(B \to 0) = B$ if and only if φ is surjective.

(c) This follows directly from (a) and (b). □

Given a module homomorphism $\varphi : A \to B$ or a submodule $C \subseteq A$, there are easy ways to create exact sequences:

(a) Let $\varphi : A \to B$ an R-module homomorphism, then

$$0 \to \ker(\varphi) \to A \xrightarrow{\varphi} B \to \operatorname{coker}(\varphi) \to 0$$

is an exact sequence.

(b) Let $C \subseteq A$ be a submodule. Then

$$0 \to C \to A \to A/C \to 0$$

is an exact sequence, where the homomorphisms are the natural injections and surjections.

Definition 3.1.6. Let $(\mathcal{A}, \delta), (\mathcal{B}, \partial)$ be complexes. A *morphism of complexes* $\varphi : \mathcal{A} \to \mathcal{B}$ is a collection of morphisms $\varphi_i : A_i \to B_i$ s.t. $\varphi_i \circ \delta_{i+1} = \partial_{i+1} \circ \varphi_{i+1}$, i.e. they fit into the commutative diagram:

$$\begin{array}{ccccccc} \cdots & \longrightarrow & A_{i+1} & \xrightarrow{\delta_{i+1}} & A_i & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle \varphi_{i+1}} & & \downarrow{\scriptstyle \varphi_i} & & \\ \cdots & \longrightarrow & B_{i+1} & \xrightarrow{\partial_{i+1}} & B_i & \longrightarrow & \cdots \end{array}$$

A complex homomorphism φ is surjective, injective, respectively bijective if all the φ_i are. With these maps between complexes, we can consider those that fit into exact sequences themselves.

Definition 3.1.7. Let $(\mathcal{A}, a), (\mathcal{B}, b)$ and $(\mathcal{C}, c)$ be three complexes and let $\varphi : \mathcal{A} \to \mathcal{B}, \psi : \mathcal{B} \to \mathcal{C}$ be two morphisms of complexes s.t. for all i there is a commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_i & \xrightarrow{\varphi_i} & B_i & \xrightarrow{\psi_i} & C_i & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle a_i} & & \downarrow{\scriptstyle b_i} & & \downarrow{\scriptstyle c_i} & & \\ 0 & \longrightarrow & A_{i-1} & \xrightarrow{\varphi_{i-1}} & B_{i-1} & \xrightarrow{\psi_{i-1}} & C_{i-1} & \longrightarrow & 0 \end{array}$$

with short exact sequences as rows, then

$$0 \to \mathcal{A} \xrightarrow{\varphi} \mathcal{B} \xrightarrow{\psi} \mathcal{C} \to 0$$

is called a *short exact sequence of complexes.*

A fundamental tool that we need in many proofs is the so-called *snake lemma.*

Theorem 3.1.8 (Snake Lemma, [31], Corollary 6.12)**.** *Consider the following commutative diagram of R-modules with exact rows:*

$$\begin{array}{ccccccccc} & & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & & \end{array}$$

There exists an exact sequence

$$\ker(\alpha) \xrightarrow{\tilde{f}} \ker(\beta) \xrightarrow{\tilde{g}} \ker(\gamma) \xrightarrow{\delta} \operatorname{coker}(\alpha) \xrightarrow{\overline{f'}} \operatorname{coker}(\beta) \xrightarrow{\overline{g'}} \operatorname{coker}(\gamma).$$

Moreover, if f is injective, so is $\tilde{f}$ and if g is surjective, so is $\overline{g'}$.

Proof. We first have to check that all the maps are well-defined.

$\tilde{f}$ and $\tilde{g}$ are defined as the restrictions $f|_{\ker(\alpha)}, g|_{\ker(\beta)}$ respectively. If $m \in \ker(\alpha)$, then we have $\beta(f(m)) = f'(\alpha(m)) = f'(0) = 0$, i.e. $f(m) \in \ker(\beta)$. Thus, $\tilde{f}$ is well-defined. Similarly for $\tilde{g}$.

$\overline{f'}$ and $\overline{g'}$ are defined as $\overline{f'}(m + \operatorname{Im}(\alpha)) = f'(m) + \operatorname{Im}(\beta)$ and $\overline{g'}(n + \operatorname{Im}(\beta)) = f'(n) + \operatorname{Im}(\gamma)$. If $m + \operatorname{Im}(\alpha) = m' + \operatorname{Im}(\alpha)$, then $m - m' = \alpha(x)$ for some $x \in A$. But then we have that $f'(m - m') = f'(\alpha(x)) = \beta(f(x)) \in \operatorname{Im}(\beta)$, so $f'(m) + \operatorname{Im}(\beta) = f'(m') + \operatorname{Im}(\beta)$. Thus, $\overline{f'}$ is well-defined. Similarly for $\overline{g'}$.

We define the *connecting homomorphism* δ as follows: Let $p \in \ker(\gamma) \subseteq C$. Since g is surjective, we have $p = g(n)$ for some $n \in B$, which implies that $\beta(n) \in B'$. Additionally, we have $g'(\beta(n)) = \gamma(g(n)) = \gamma(p) = 0$, since $p \in \ker(\gamma)$. Thus, $\beta(n) \in \ker(g') = \operatorname{Im}(f')$. Thus, since f' is injective, there is a unique $m \in A'$ s.t. $\beta(n) = f'(m)$.

Now define $\delta(p) = m + \mathrm{Im}(\alpha) = (f')^{-1}(\beta(g^{-1}(p))) + \mathrm{Im}(\alpha)$. To show that δ is well-defined, we note that the only possible ambiguity comes by taking $n = g^{-1}(p)$. Suppose there are $n \neq n'$ s.t. $p = g(n) = g(n')$. As f' is injective, there is a unique $m' \in A'$ s.t. $f'(m') = \beta(n')$. The assumption on n and n' gives $n - n' \in \ker(g) = \mathrm{Im}(f)$, so $n - n' = f(z)$ for some $z \in A$. Therefore, $f'(\alpha(z)) = \beta(f(z)) = \beta(n - n') = f(m - m')$. Then $m - m' = \alpha(z) \in \mathrm{Im}(\alpha)$, since f' is injective. Therefore, $m + \mathrm{Im}(\alpha) = m' + \mathrm{Im}(\alpha)$, which implies that δ is indeed well-defined.

Next, one has to show that the sequence is exact.

(Exactness at $\ker(\beta)$) Clearly, $\tilde{g} \circ \tilde{f} = 0$, as $g \circ f = 0$. Thus $\mathrm{Im}(\tilde{f}) \subseteq \ker(\tilde{g})$. Conversely, let $n \in \ker(\beta)$ with $\tilde{g}(n) = 0$. Then $g(n) = 0$, so $n \in \ker(g) = \mathrm{Im}(f)$. Therefore, there is $m \in A$ s.t. $n = f(m)$. We have $f'(\alpha(m)) = \beta(f(m)) = \beta(n) = 0$ since $n \in \ker(\beta)$. The injectivity of f' implies that $\alpha(m) = 0$ and $m \in \ker(\alpha)$. Thus, $n \in \mathrm{Im}(\tilde{f})$.

(Exactness at $\ker(\gamma)$) Let $n \in \ker(\beta)$. Since $\beta(n) = 0$, this implies that $\beta(n) = f'(0)$. Thus, $\delta(\tilde{g}(n)) = 0 + \mathrm{Im}(\alpha)$, which implies that $\mathrm{Im}(\tilde{g}) \subseteq \ker(\delta)$. On the other hand, let $p \in \ker(\gamma)$ s.t. $p \in \ker(\delta)$. Writing $p = g(n)$gives us $\beta(n) = f'(m)$ s.t. $m \in \mathrm{Im}(\alpha)$, i.e. there exists $x \in A$ s.t. $m = \alpha(x)$. Then $\beta(f(x)) = f'(\alpha(x)) = \beta(n)$. Thus, $n - f(x) \in \ker(\beta)$. Also $\tilde{g}(n - f(x)) = g(n) - g(f(x)) = g(n) = p$, so $n \in \mathrm{Im}(\tilde{g})$ and $\ker(\delta) \subseteq \mathrm{Im}(\tilde{g})$.

(Exactness at $\mathrm{coker}(\alpha)$) Let $p \in \ker(\gamma)$. Write $p = g(n)$ and $\beta(n) = f'(m)$, so $\delta(p) = m + \mathrm{Im}(\alpha)$. Since $f'(m) = \beta(n) \in \mathrm{Im}(\beta)$, we have $\overline{f'}(\delta(p)) = f'(m) + \mathrm{Im}(\beta) = 0$. This implies that $\mathrm{Im}(\delta) \subseteq \ker(\overline{f'})$. Conversely, consider $m + \mathrm{Im}(\alpha) \in \ker(\overline{f'})$, so $f'(m) \in \mathrm{Im}(\beta)$, i.e. there is $n \in B$ s.t. $f'(m) = \beta(n)$. Set $p = g(n)$. Then $\gamma(g(n)) = g'(\beta(n)) = g'(f'(m)) = 0$. Thus, $p \in \ker(\gamma)$ and $\delta(p) = m + \mathrm{Im}(\alpha)$ by definition of δ. Thus, $m + \mathrm{Im}(\alpha) \in \mathrm{Im}(\delta)$, i.e. $\ker(\overline{f'}) \subseteq \mathrm{Im}(\delta)$.

(Exactness at $\mathrm{coker}(\beta)$) Clearly, $\overline{g'} \circ \overline{f'} = 0$. On the other hand, let $n + \mathrm{Im}(\beta) \in \ker(\overline{g'})$. Then we have $g'(n) \in \mathrm{Im}(\gamma)$, thus there is $p \in C$ s.t. $g'(n) = \gamma(p)$. Choose $x \in B$ s.t. $g(x) = p$. One can exchange n with $n - \beta(x)$ as both have the same coset $n + \mathrm{Im}(\beta)$. But we also have that $g'(n - \beta(x)) = g'(n) - g'(\beta(x)) = g'(n) - \gamma(g(x)) = 0$. So we may assume that $g'(n) = 0$. Then we have $n \in \ker(g') = \mathrm{Im}(f')$, so there exists $m \in A'$ s.t. $n = f'(m)$. This implies the equality $n + \mathrm{Im}(\beta) = f'(m) + \mathrm{Im}(\beta) = \overline{f'}(m + \mathrm{Im}(\alpha))$, so $n + \mathrm{Im}(\beta) \in \mathrm{Im}(\overline{f'})$.

Finally, suppose f is injective, then clearly $\tilde{f} = f|_{\ker(\alpha)}$ is injective. When g' is surjective and $p \in \mathrm{Im}(\gamma) \in \mathrm{coker}(\gamma)$, write $p = g'(n)$ for some $n \in B'$. Thus, $p + \mathrm{Im}(\gamma) = \overline{g'}(n + \mathrm{Im}(\beta))$. Therefore, $\overline{g'}$ is surjective. □

A nice result for a short exact sequence of complexes is, that one can obtain long exact sequences of homology from it. We state the following result for cochain complexes and cohomology since we are mostly going to use this version in Chapter 6. Note, however, that an analogous result also holds for chain complexes.

Lemma 3.1.9 ([48], Theorem 1.3.1)**.** *Let $(\mathcal{A}, a), (\mathcal{B}, b)$ and $(\mathcal{C}, c)$ be positive cochain complexes and let $\varphi : \mathcal{A} \to \mathcal{B}, \psi : \mathcal{B} \to \mathcal{C}$ be morphisms of complexes s.t.*

$$0 \to \mathcal{A} \xrightarrow{\varphi} \mathcal{B} \xrightarrow{\psi} \mathcal{C} \to 0$$

form a short exact sequence of complexes. Then, this gives rise to a long exact sequence of cohomology modules

$$0 \to H^0(\mathcal{A}) \to H^0(\mathcal{B}) \to H^0(\mathcal{C}) \to H^1(\mathcal{A}) \to \cdots$$
$$\cdots \to H^n(\mathcal{B}) \to H^n(\mathcal{C}) \to H^{n+1}(\mathcal{A}) \to \cdots .$$

Proof. As seen in the proof of the snake lemma, the short exact sequence

$$0 \to A_n \xrightarrow{\varphi_n} B_n \xrightarrow{\psi_n} C_n \to 0$$

yields an exact sequence

$$0 \to \ker(a_n) \xrightarrow{\varphi'_n} \ker(b_n) \xrightarrow{\psi'_n} \ker(c_n),$$

as well as an exact sequence

$$\operatorname{coker}(a_n) \xrightarrow{\overline{\varphi}_{n+1}} \operatorname{coker}(b_n) \xrightarrow{\overline{\psi}_{n+1}} \operatorname{coker}(c_n) \to 0$$

for all $n \geq 0$. Now, let

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_0 & \xrightarrow{\varphi_0} & B_0 & \xrightarrow{\psi_0} & C_0 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \tilde{a}_0} & & \downarrow{\scriptstyle \tilde{b}_0} & & \downarrow{\scriptstyle \tilde{c}_0} & & \\ 0 & \longrightarrow & \ker(a_1) & \xrightarrow{\varphi'_1} & \ker(b_1) & \xrightarrow{\psi'_1} & \ker(c_1) & & \end{array} \tag{3.1}$$

be a commutative diagram. Checking that all maps are well-defined is done similarly as in the proof of the snake lemma. Applying the snake lemma to (3.1) yields an exact sequence

$$0 \to \ker(a_0) \to \ker(b_0) \to \ker(c_0) \to \operatorname{coker}(\tilde{a}_0) \to \operatorname{coker}(\tilde{b}_0) \to \operatorname{coker}(\tilde{c}_0).$$

By the definition of cohomology one can observe that this is equal to the sequence

$$0 \to H^0(\mathcal{A}) \to H^0(\mathcal{B}) \to H^0(\mathcal{C}) \to H^1(\mathcal{A}) \to H^1(\mathcal{B}) \to H^1(\mathcal{C}).$$

Now, consider this commutative diagram:

$$\begin{array}{ccccccccc} & & \operatorname{coker}(a_0) & \xrightarrow{\overline{\varphi}_1} & \operatorname{coker}(b_0) & \xrightarrow{\overline{\psi}_1} & \operatorname{coker}(c_0) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \tilde{a}_1} & & \downarrow{\scriptstyle \tilde{b}_1} & & \downarrow{\scriptstyle \tilde{c}_1} & & \\ 0 & \longrightarrow & \ker(a_2) & \xrightarrow{\varphi'_2} & \ker(b_2) & \xrightarrow{\psi'_2} & \ker(c_2) & & \end{array} \tag{3.2}$$

where the vertical maps are defined s.t $\tilde{a}_1 : a + \operatorname{Im}(a_0) \mapsto a_1(a)$. Similar for $\tilde{b}_1$ and $\tilde{c}_1$. Again, to show that all the maps are well-defined is straightforward. Applying the snake lemma to (3.2) above yields an exact sequence

$$\ker(\tilde{a}_1) \to \ker(\tilde{b}_1) \to \ker(\tilde{c}_1) \to \operatorname{coker}(\tilde{a}_1) \to \operatorname{coker}(\tilde{b}_1) \to \operatorname{coker}(\tilde{c}_1).$$

By the definition of cohomology one can observe that this is equal to the sequence

$$H^1(\mathcal{A}) \to H^1(\mathcal{B}) \to H^1(\mathcal{C}) \to H^2(\mathcal{A}) \to H^2(\mathcal{B}) \to H^2(\mathcal{C}).$$

Now, observing that these sequences overlap and the maps in the overlapping part actually coincide, one can *glue* the sequences together to obtain a 10-term sequence. Iterating this process we get the desires long exact sequence of cohomology modules. □

3.2 Free Resolutions

Free resolutions are an important tool to describe invariants, which characterize the structure of a module. We need free resolutions to define Castelnuovo–Mumford regularity in Chapter 7. This discussion on free resolutions is based upon [23, Chapter 1] and [16, Chapter 6].

Definition 3.2.1. A *left* resolution of M is a positive chain complex $(\mathcal{F}, \partial)$ together with a map $F_0 \to M$ s.t. the complex

$$\cdots \to F_n \xrightarrow{\partial_n} F_{n-1} \to \cdots \to F_1 \xrightarrow{\partial_1} F_0 \to M \to 0$$

is exact. It is denoted by $\mathcal{F} \to M$.
If each F_n is a free module, the resolution $\mathcal{F} \to M$ is called a *free resolution* of M.
If there exists an $l \geq 0$ s.t. $F_{l+1} = F_{l+2} = \cdots = 0$, but $F_l \neq 0$, the resolution is said to be *finite* of *length* l.

Proposition 3.2.2 ([47], Lemma 3.3)**.** *Every R-module M has a free resolution.*

Proof. For any module M, there exists an epimorphism $\varphi : F_0 \to M$, where F_0 is a free module. Let $M_0 = \ker(\varphi) \subseteq F_0$ and consider an epimorphism $F_1 \to M_0$, where F_1 is free and let $\partial_1 : F_1 \to F_0$ be the composition $F_1 \to M_0 \to F_0$. Clearly, $\mathrm{Im}(F_1 \to F_0) = M_0 = \ker(\varphi)$, which proves exactness at F_0. Setting $M_1 = \ker(F_1 \to F_0)$ and repeating iteratively the construction of F_2 and so on, clearly results in a free resolution of M. □

Lemma 3.2.3 ([16], Proposition 1.12, Chapter 6)**.** *If M has a free resolution in which $\ker(\partial_{l-1})$ is a free module for some l, then M has a finite free resolution of length l.*

Proof. Suppose $\ker(\partial_{l-1})$ is free. Let $F_l = \ker(\partial_{l-1})$ and let $\partial_l : F_l \to F_{l-1}$ be the inclusion. Then we can extend the exact sequence $F_{l-1} \xrightarrow{\partial_{l-1}} F_{l-2} \to \cdots \to F_0 \to M \to 0$ to the finite free resolution

$$0 \to F_l \xrightarrow{\partial_l} F_{l-1} \to \cdots \to F_0 \to M \to 0,$$

which has length l. □

For modules over a polynomial ring $R = k[x_1, \ldots, x_n]$ it can be shown that any finitely generated R-module M has a free resolution of finite length. This is due to the Hilbert syzygy theorem that we will prove in Section 5.7 based on Gröbner bases.

These concepts can also be applied to graded modules. Let $\mathcal{F}$ be a complex, where all the modules are graded. Since each F_i is graded we can write $F_i = \bigoplus_d F_{i,d}$, where $F_{i,d}$ denotes the degree d part of F_i. When the boundaries are homogeneous maps (i.e. of degree 0), we have $\partial_i(F_{i,d}) \subseteq F_{i-1,d}$. Thus, we can look at the d-th graded component of $\mathcal{F}$, which is the sequence of k-vector spaces

$$\cdots \to F_{i+1,d} \to F_{i,d} \to F_{i-1,d} \to \cdots .$$

When the graded complex $\mathcal{F}$ is exact, its graded components form exact sequences of k-vector spaces.

Definition 3.2.4. Let M be a graded R-module. Then a *graded free resolution* of M is a free resolution $\mathcal{F} \to M$, where each F_l is a twisted free graded module of the form

$$R(-d_{l,1}) \oplus \cdots \oplus R(-d_{l,r_l})$$

s.t. each homomorphism φ_l is a graded homogeneous map.

As in the ungraded case, such a resolution always exists.

Lemma 3.2.5 ([42], Construction 4.2)**.** *Every graded R-module has a graded free resolution.*

Proof. The proof is similar to the ungraded case. Since M is a graded module, it is generated by homogeneous elements, say $M = \langle f_1, \ldots, f_s \rangle$, where f_i are homogeneous of degree $d_{0,i}$. Then, as in Proposition 3.2.2, we can construct the usual epimorphism $\varphi_0 : F_0 \to M$, and ensure it is homogeneous by setting $F_0 = \bigoplus_{i=1}^{s} R(-d_{0,i})$. Since $\ker(\varphi_0) \subseteq F_0$ is a graded submodule, it is

generated by a set $G_0 = \{g_1, \dots, g_{t_1}\}$ of homogeneous elements of degree $d_{1,i}$ for $i = 1, \dots, t_1$. Then set $F_1 = \bigoplus_{i=1}^{t_1} R(-d_{1,i})$ and define $\varphi_1 : F_1 \to F_0$ by $e_i \mapsto g_i$ for $i = 1, \dots, t_1$. Clearly, φ is homogeneous and can be represented by a graded $s \times t_1$ matrix, since the ij-th entry has degree $d_{1,j} - d_{0,i}$. Iterating this process we get an exact complex, which satisfies all the properties of a graded free resolution. □

Example 3.2.6. Let $f_1 = x^2 - z^2, f_2 = xy + xz \in R = k[x, y, z]$. A graded free resolution of $I = \langle f_1, f_2 \rangle$ is given by

$$0 \to R(-4) \xrightarrow{\varphi_1} R(-2)^2 \xrightarrow{\varphi_0} I \to 0,$$

where the maps φ_1, φ_2 are given by the graded matrices

$$\varphi_0 = (-xy - xz, x^2 - z^2), \ \varphi_1 = \begin{pmatrix} x^2 - z^2 \\ xy + xz \end{pmatrix}.$$

While such graded free resolutions exist for all graded modules M, they may not be unique. There are, however, some kind of graded free resolutions that will turn out to be unique. Recall the notion of the irrelevant ideal $\mathfrak{m} = R_+$ of the graded ring R.

Definition 3.2.7. A graded free resolution $\mathcal{F} \to M$ of a graded R-module M is called *minimal* if for all $l \geq 1$, we have $\operatorname{Im}(\varphi_l) \subseteq \mathfrak{m}F_{l-1}$.

This definition can be seen as saying that the map φ_l is represented by a matrix, whose entries are all in $\mathfrak{m}$, i.e. have positive degree.

Proposition 3.2.8 ([23], Corollary 1.5)**.** *A graded free resolution $\mathcal{F} \to M$ is minimal if and only if for each l, $\varphi_l(F_l)$ is a minimal system of generators of* $\operatorname{Im}(\varphi_l)$.

Proof. Consider the exact sequence

$$F_{i+1} \xrightarrow{\varphi_{i+1}} F_i \xrightarrow{\varphi_i'} \operatorname{Im}(\varphi_i) \to 0.$$

Then $\mathcal{F}$ is minimal if and only if the map

$$\overline{\varphi}_{i+1} : F_{i+1}/\mathfrak{m}F_{i+1} \to F_i/\mathfrak{m}F_i, \ f + \mathfrak{m}F_{i+1} \mapsto \varphi_{i+1}(f) + \mathfrak{m}F_i$$

is zero for all i. As $\operatorname{Im}(\varphi_{i+1}) = \ker(\varphi_i')$, the above statement is true if and only if the map

$$\overline{\varphi}_i' : F_i/\mathfrak{m}F_i \to \operatorname{Im}(\varphi_i)/\mathfrak{m}\operatorname{Im}(\varphi_i), \ f + \mathfrak{m}F_i \mapsto \varphi_i(f) + \mathfrak{m}\operatorname{Im}(\varphi_i)$$

is an isomorphism, i.e. $F_i/\mathfrak{m}F_i \cong \operatorname{Im}(\varphi_i)/\mathfrak{m}\operatorname{Im}(\varphi_i)$. But a basis $\{f_1, \dots, f_s\}$ of F_i yields a basis $\{\overline{f}_1, \dots, \overline{f}_s\}$ of $F_i/\mathfrak{m}F_i$ by Nakayama's lemma. So by the isomorphism, $\{\overline{\varphi_i}(\overline{f_1}), \dots, \overline{\varphi_i}(\overline{f_s})\}$ is a basis of $\operatorname{Im}(\varphi_i)/\mathfrak{m}\operatorname{Im}(\varphi_i)$. Applying Nakayama's lemma again, yields that $\varphi_i(f_1), \dots, \varphi_i(f_s)$ is a minimal generating system of $\operatorname{Im}(\varphi_i)$. □

We now can show that such a minimal graded free resolution is unique up to isomorphism.

Proposition 3.2.9 ([30], Proposition A.2.3)**.** *Let M be a finitely generated graded R-module. Then any two minimal graded free resolutions of M are isomorphic.*

Proof. Let $\mathcal{F} \to M$ and $\mathcal{G} \to M$ be two minimal graded free resolutions of M. We show that there are isomorphisms $a_i : F_i \to G_i$ s.t. the following diagram commutes:

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & F_i & \longrightarrow & \cdots & \longrightarrow & F_1 & \longrightarrow & F_0 & \longrightarrow & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle a_i} & & & & \downarrow{\scriptstyle a_1} & & \downarrow{\scriptstyle a_0} & & \downarrow{\scriptstyle \mathrm{id}_M} & & \\ \cdots & \longrightarrow & G_i & \longrightarrow & \cdots & \longrightarrow & G_1 & \longrightarrow & G_0 & \longrightarrow & M & \longrightarrow & 0 \end{array} \tag{3.3}$$

First, we show something more general. Let U and V be graded R-modules and let $\varphi : U \to V$ be an isomorphism of finitely generated graded R-modules. Consider $\epsilon : F \to U$ and $\eta : G \to V$ be homogeneous epimorphisms s.t. $\ker(\epsilon) \subseteq \mathfrak{m}F$ resp. $\ker(\eta) \subseteq \mathfrak{m}G$. Suppose $f_1, \dots, f_r$ is a homogeneous basis of F. Then $\varphi(\epsilon(f_1)), \dots, \varphi(\epsilon(f_r))$ is a homogeneous system of generators of V. Since η is surjective and homogeneous, we have $\eta(g_i) = \varphi(\epsilon(f_i))$ for $i = 1, \dots, r$ and some $g_1, \dots, g_r \in G$. Let $\alpha(f_i) = g_i$ for $i = 1, \dots, r$. Then $\alpha : F \to G$ is a homogeneous morphism and the following diagram commutes:

$$\begin{array}{ccc} F & \xrightarrow{\epsilon} & U \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \varphi} \\ G & \xrightarrow{\eta} & V \end{array}$$

Quotienting by $\mathfrak{m}$ yields the following commutative diagram:

$$\begin{array}{ccc} F/\mathfrak{m}F & \xrightarrow{\overline{\epsilon}} & U/\mathfrak{m}U \\ \downarrow{\scriptstyle \overline{\alpha}} & & \downarrow{\scriptstyle \overline{\varphi}} \\ G/\mathfrak{m}G & \xrightarrow{\overline{\eta}} & V/\mathfrak{m}V \end{array}$$

The map $\overline{\epsilon} : F/\mathfrak{m}F \to U/\mathfrak{m}U$ is an isomorphism, since $\ker(\epsilon) \subseteq \mathfrak{m}F$. Similarly $\overline{\eta}$ and $\overline{\varphi}$ are isomorphisms. This implies that also $\overline{\alpha} = \overline{\eta}^{-1} \circ \overline{\varphi} \circ \overline{\epsilon}$ is an isomorphism. Since $\overline{\alpha}$ is an isomorphism, $\overline{\alpha}(\overline{f}_1), \dots, \overline{\alpha}(\overline{f}_1)$ is a basis of $G/\mathfrak{m}G$ and by Nakayama's lemma $\alpha(f_1), \dots, \alpha(f_s)$ is a basis of G. Thus, α is an isomorphism as well.
The existence of isomorphisms α_i in Diagram (3.3) now follows directly with an inductive argument from the comments we just made. □

Not only is the minimal graded free resolution unique, but it can also be obtained from any free resolution.

Proposition 3.2.10 ([23], Theorem 1.6)**.** *Let M be a finitely generated graded R-module. Then, any graded free resolution of M contains the minimal free resolution as a direct summand.*

Proof. Let $\mathcal{F} \to M$ be a graded free resolution of M. If $\mathcal{F}$ is not minimal, then some map φ_i must send a standard basis element of F_i to an element in F_{i-1} that does not lie in $\mathfrak{m}F_{i-1}$. This element may be seen as a basis element of F_{i-1} due to Nakayama's lemma. This, means that there is a subcomplex $\mathcal{G}$ of $\mathcal{F}$ given by

$$\mathcal{G} : \cdots \to 0 \to R(-a) \xrightarrow{c} R(-a) \to 0 \to 0 \to \cdots$$

for some nonzero scalar c. This subcomplex is embedded in $\mathcal{F}$, where the $R(-a)$ are direct summands of F_i and F_{i-1} respectively. Like this, $\mathcal{F}/\mathcal{G}$ is again a free complex. This yields a short exact sequence of complexes

$$0 \to \mathcal{G} \to \mathcal{F} \to \mathcal{F}/\mathcal{G} \to 0,$$

which by the dual version of Lemma 3.1.9 yields a long exact sequence of homology:

$$\begin{aligned} H_0(\mathcal{G}) \to H_0(\mathcal{F}) \to H_0(\mathcal{F}/\mathcal{G}) \to H_1(\mathcal{G}) \to \cdots \\ \cdots \to H_i(\mathcal{F}) \to H_i(\mathcal{F}/\mathcal{G}) \to H_{i+1}(G) \to \cdots \end{aligned}$$

As $\mathcal{G}$ is a trivial complex with no homology, i.e. $H_i(\mathcal{G}) = 0$ for all $i \geq 0$, it follows that $H_i(\mathcal{F}) \cong H_i(\mathcal{F}/\mathcal{G})$ for all $i \geq 0$. Therefore $\mathcal{F}/\mathcal{G}$ has the same homology as $\mathcal{F}$ and is therefore exact, as $\mathcal{F}$ is exact. So if $\mathcal{F}$ is a free resolution of M, then is $\mathcal{F}/\mathcal{G}$ is as well. Proceeding iteratively, one eventually obtains the minimal graded free resolution. □

3.3 Injective Resolutions

A dual notion to free resolutions is the concept of injective resolutions, which we need to define local cohomology later in this chapter. This will then serve as a preparation for the study of Castelnuovo–Mumford regularity in Chapter 7. The majority of the terminology and results is based on [31, Chapters 3 and 6].

First, we introduce the notion of injective modules.

Definition 3.3.1. An R-module M is *injective* if for every injective homomorphism $a : A \to B$ and every homomorphism of R-modules $f : A \to M$, there exists a homomorphism $g : B \to M$ s.t. $f = g \circ a$ as in the following diagram.

$$\begin{array}{ccc} A & \xhookrightarrow{a} & B \\ \downarrow{\scriptstyle f} & \swarrow{\scriptstyle g} & \\ M & & \end{array}$$

Lemma 3.3.2 ([31], Proposition 3.28)**.** *A finite direct sum of injective R-modules is an injective R-module.*

Proof. Let $M = \bigoplus_{i \in I} M_i$, where I is finite and M_i is injective for all $i \in I$. Let $a : A \to B$ be an injective homomorphism and $f : A \to M$ a homomorphism. Then the i-th coordinate of f is a map $f : A \to M_i$, where M_i is injective. Thus, there exists a map $g_i : B \to M_i$ s.t. $f_i = g_i \circ a$. The direct sum $g = \oplus_{i \in I} g_i$ is then a well-defined homomorphism $B \to M$ s.t. $g \circ a = f$. □

Next, we present a criterion for detecting injective modules.

Lemma 3.3.3 (Baer's Criterion, [31], Theorem 3.30)**.** *An R-module M is injective if and only if every homomorphism $f : I \to M$, where $I \subseteq R$ is an ideal, can be extended to R, i.e. there exists $g : R \to M$ s.t. the diagram:*

$$\begin{array}{ccc} I & \xhookrightarrow{i} & R \\ \downarrow{\scriptstyle f} & \swarrow{\scriptstyle g} & \\ M & & \end{array}$$

commutes, where $i : I \to R$ denotes the inclusion.

Proof. ($\Rightarrow$) Assuming M is injective, the existence of g follows directly from the definition of injectivity.

($\Leftarrow$) Let A, B be arbitrary R-modules and suppose $b : A \to M$ is a homomorphism and $a : A \to B$ is an injective homomorphism. We may view A as a submodule of B and a as the inclusion. If A' is a submodule of B containing A, then $b' : A' \to M$ is an *extension* of b if $b'|_A = b$. To show that M is injective, we have to show that there is such an extension of b to B.

By Zorn's lemma A.1.1, there exists a submodule A' and an extension b' of b to A' s.t. it is maximal, meaning that b' cannot be extended any further. If $A' = B$, the result follows.
Otherwise suppose $A' \neq B$. Let $x \in B \setminus A'$ and consider the submodule $A'' = A' + Rx$. Let $I = \{r \in R : rx \in A'\} \subseteq R$. The map $f : I \to M$ defined by $r \mapsto b'(rx) \in M$ extends to a map $g : R \to M$ by assumption. Since $\ker(R \to Rx) \subseteq \ker(g)$, g induces a map $g' : Rx \to M$, where by construction g' agrees with b' on $Rx \cap A'$. Let b'' be an extension of b' to A'' by letting $b''|_{A'} = b'$ and $b''|_{Rx} = g'$. But this contradicts the maximality of A' and B'. □

Definition 3.3.4. Let M be an R-module over an integral domain R. If $r \in R, m \in M$, then m is *divisible* by r if there is some $m' \in M$ with $m = rm'$.
M is called a *divisible* module if each $m \in M$ is divisible by every $r \in R \setminus \{0\}$.

This basically means that M is divisible if $\varphi_r : M \to M, m \mapsto rm$ is surjective for all $r \neq 0$.

Lemma 3.3.5 ([31], Lemma 3.33)**.** *If R is an integral domain, then every injective R-module M is divisible.*

Proof. Suppose M is injective and let $m \in M,\ r_0 \in R \setminus \{0\}$. Set $f : \langle r_0 \rangle \to M$ by $f(rr_0) = rm$, which is well-defined, since R is a domain. There is a map $g : R \to M$ extending f, since M is injective. This means that $m = f(r_0) = g(r_0) = r_0 g(1)$ s.t. $m' = g(1)$ satisfies $m = r_0 m'$. Thus, M is divisible. □

Lemma 3.3.6 ([31], Corollary 3.35)**.** *Let R be a PID and let M be an R-module.*

(a) *M is injective if and only if M is divisible.*

(b) *If M is injective then every quotient of M is injective.*

Proof. (a) ($\Rightarrow$) This follows directly from Lemma 3.3.5.

($\Leftarrow$) Let $f : I \to M$ be a homomorphism, where I is a nonzero ideal of R. Then $I = \langle a \rangle$ for some $a \in I$, since R is a PID. As M is divisible, there exists a $m \in M$ s.t. $f(a) = am$. Let $g : R \to M,\ s \mapsto sm$ for all $s \in R$. Then, g is clearly a homomorphism that extends f, as if $s = ra \in I$, then $g(s) = g(ra) = ram = rf(a) = f(ra)$. Thus, by Baer's criterion, M is injective.

(b) M is divisible, since it is injective. For a submodule $N \subseteq M$, clearly M/N is divisible. Thus, by (a) M/N is injective. □

Example 3.3.7. The homomorphism $\varphi_r : \mathbb{Q} \to \mathbb{Q},\ q \mapsto rq$ is surjective for all $r \neq 0$. Thus $\mathbb{Q}$ is a divisible $\mathbb{Z}$-module. This implies that $\mathbb{Q}$ is an injective $\mathbb{Z}$-module.

Corollary 3.3.8 ([31], Corollary 3.36)**.** *Every abelian group M can be embedded as a subgroup of some injective abelian group.*

Proof. An abelian group is a $\mathbb{Z}$-module. There exists a free $\mathbb{Z}$-module $F = \bigoplus_i \mathbb{Z}_i$, s.t. $M \cong F/K$ for some $K \subseteq F$. Thus,

$$M \cong F/K \cong \left(\bigoplus_i \mathbb{Z}_i \right) / K \subseteq \left(\bigoplus_i \mathbb{Q}_i \right) / K,$$

where copies of $\mathbb{Z}$ are embedded into copies of $\mathbb{Q}$. But $\mathbb{Q}$ is divisible. Thus, by Lemma 3.3.6 $\left(\bigoplus_i \mathbb{Q}_i\right)/K$ is divisible and therefore injective. □

Lemma 3.3.9 ([22], Lemma A.3.8)**.** *Let D be a divisible $\mathbb{Z}$-module. Then $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ is an injective R-module.*

Proof. It is easy to check that $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ is indeed an R-module.
Let $A \subseteq B$ be a submodule and let $f : A \to \mathrm{Hom}_{\mathbb{Z}}(R, D)$ be a homomorphism. We prove that f extends to B.
Consider the natural map of $\mathbb{Z}$-modules $\mathrm{Hom}_{\mathbb{Z}}(R, D) \to D,\ \varphi \mapsto \varphi(1) \in D$. Let $f' : A \to D$ be the composite of f and this natural map. Consider an extension g' of f' to B and set $g : B \to \mathrm{Hom}_{\mathbb{Z}}(R, D)$ by $m \mapsto \varphi_m$, where $\varphi_m(r) = g'(rm)$. Then $g : B \to \mathrm{Hom}_{\mathbb{Z}}(R, D)$ is the desired extension of f. Thus, $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ is injective. □

Theorem 3.3.10 ([31], Theorem 3.38)**.** *Every R-module M can be embedded as a submodule of an injective R-module.*

Proof. First, note that if $i : A \to B$ is injective, then

$$i^* : \mathrm{Hom}(R, A) \to \mathrm{Hom}(R, B), f \mapsto i \circ f$$

is also injective.

View M as an abelian group, i.e. as a $\mathbb{Z}$-module and let $\varphi : M \to \mathrm{Hom}_{\mathbb{Z}}(R, M)$, $m \mapsto \varphi_m$, s.t. $\varphi_m(r) = rm$ for all $r \in R$. Clearly, φ is a $\mathbb{Z}$-homomorphism. If $\varphi_m = \varphi_{m'}$, then $rm = \varphi_m(r) = \varphi_{m'}(r) = rm'$ for all $r \in R$, so also for $r = 1$. Thus, $m = m'$ and φ is injective.
By Lemma 3.3.8, there exists an injective $\mathbb{Z}$-module D and an injective $\mathbb{Z}$-module homomorphism $i : M \to D$. According to the comment at the start, this yields an injective map $i^* : \mathrm{Hom}_{\mathbb{Z}}(R, M) \to \mathrm{Hom}_{\mathbb{Z}}(R, D), f \mapsto i \circ f$. Thus the composite $i^* \circ \varphi$ is also an injective $\mathbb{Z}$-homomorphism.

If $a \in R, m \in M$ then $(i^* \circ \varphi)(am) = i \circ \varphi_{am}$, where $i \circ \varphi_{am} : r \mapsto i(r(am))$. Conversely, $a(i^* \circ \varphi(m)) = a(i \circ \varphi_m)$, where $a(i \circ \varphi_m) : r \mapsto ai(rm) = i(r(am))$. Therefore $i^* \circ \varphi$ is an R-homomorphism. So M can be embedded in $\mathrm{Hom}_{\mathbb{Z}}(R, D)$, which by Lemma 3.3.9, is an injective R-module. □

Now, we have the tools to introduce something similar to free resolutions but for cochain complexes.

Definition 3.3.11. A *right* resolution of M is a positive cochain complex $(\mathcal{E}, d)$ together with a map $\epsilon : M \to E^0$ s.t. the complex

$$0 \to M \to E^0 \xrightarrow{d^0} E^1 \to \cdots \to E^{n-1} \xrightarrow{d^{n-1}} E^n \to \cdots$$

is exact. It is denoted by $M \to \mathcal{E}$. The monomorphism $\epsilon : M \to E^0$, where E^0 is injective is called an *injective representation* of M.
If each E^n is an injective module, the resolution $M \to \mathcal{E}$ is called an *injective resolution* of M.

Proposition 3.3.12 ([31], Proposition 6.4)**.** *Every R-module M has an injective resolution.*

Proof. We can embed every module M as a submodule of an injective module E^0 by a monomorphism ϵ due to Theorem 3.3.10. This yields an exact sequence

$$0 \to M \xrightarrow{\epsilon} E^0 \xrightarrow{\pi} \mathrm{coker}(\epsilon) \to 0,$$

where π is the canonical epimorphism. Embedding $\mathrm{coker}(\epsilon)$ in an injective module E^1 with $\epsilon^1 : \mathrm{coker}(\epsilon) \to E^1$ yields a homomorphism $d^0 = \epsilon^1 \circ \pi : E^0 \to E^1$. As ϵ^1 is injective, we have $\ker(d^0) = \ker(\pi) = \mathrm{Im}(\epsilon)$, so the sequence is exact. Repeating this process of embedding $\mathrm{coker}(d^{n-1})$ in an injective module E^{n+1} yields an injective resolution of M. □

For a short exact sequence of modules, we now present a way to construct injective resolutions that fit into a short exact sequence of complexes.

Proposition 3.3.13 ([41], Proposition 39)**.** *Given a short exact sequence of R-modules*

$$0 \to A \xrightarrow{\varphi} B \xrightarrow{\psi} C \to 0$$

with injective representations

$$\epsilon_A : A \to E_A, \ \epsilon_C : C \to E_C,$$

there exists an injective representation $\epsilon_B : B \to E_B$ fitting into the commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \xrightarrow{\varphi} & B & \xrightarrow{\psi} & C & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \epsilon_A} & & \downarrow{\scriptstyle \epsilon_B} & & \downarrow{\scriptstyle \epsilon_C} & & \\
0 & \longrightarrow & E_A & \xrightarrow{i} & E_B & \xrightarrow{\pi} & E_C & \longrightarrow & 0
\end{array}$$

Proof. Let $E_B = E_A \oplus E_C$, which is injective by Lemma 3.3.2 and let i, π be the inclusion morphism onto the first direct summand, resp. the projection morphism from the second direct summand. We define the maps $\epsilon_B : B \to E_A \oplus E_C$ by components $\epsilon_{B,1} : B \to E_A$ and $\epsilon_{B,2} : B \to E_C$.
Let $\epsilon_{B,2} = \epsilon_C \circ \psi$. For $\epsilon_{B,1}$, note that E_A is injective and φ is a monomorphism. Thus, there exists $\xi : B \to E_A$ s.t. $\epsilon_A = \xi \circ \varphi$. Let $\epsilon_{B,1} = \xi$. It remains to show that ϵ_B is injective. To show this, let $b \in \ker(\epsilon_B)$, i.e. $0 = \epsilon_B(b) = (\epsilon_{B,1}(b), \epsilon_{B,2}(b)) = (\xi(b), \epsilon_C(\psi(b))$. Thus $\epsilon_C(\psi(b)) = 0$, which implies that $\psi(b) = 0$, since ϵ_C is injective. Thus, $b \in \ker(\psi) = \mathrm{Im}(\varphi)$, so there exists $a \in A$ s.t. $\varphi(a) = b$. But then $\epsilon_A(a) = \xi(\varphi(a)) = \xi(b) = \epsilon_{B,1}(b) = 0$. Thus, $a = 0$ since ϵ_A is injective. This implies that $b = \varphi(a) = 0$, so ϵ_B is injective. □

Corollary 3.3.14 ([41], Corollary 40)**.** *Given a short exact sequence of R-modules*

$$0 \to A \xrightarrow{\varphi} B \xrightarrow{\psi} C \to 0$$

with injective resolutions

$$A \to \mathcal{E}_A, C \to \mathcal{E}_C,$$

there exists an injective representation $B \to \mathcal{E}_B$ and an exact sequence of complexes

$$0 \to \mathcal{E}_A \xrightarrow{i} \mathcal{E}_B \xrightarrow{\pi} \mathcal{E}_A \to 0.$$

Proof. By the previous result, there exists an injective representation $\epsilon_B : B \to E_B^0$ s.t.

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A & \xrightarrow{\varphi} & B & \xrightarrow{\psi} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \epsilon_A} & & \downarrow{\scriptstyle \epsilon_B} & & \downarrow{\scriptstyle \epsilon_C} & & \\ 0 & \longrightarrow & E_A^0 & \xrightarrow{i_0} & E_B^0 & \xrightarrow{\pi_0} & E_C^0 & \longrightarrow & 0 \end{array} \tag{3.4}$$

commutes and has exact rows. Thus, by the snake lemma applied to the two exact rows of the diagram, there is an exact sequence

$$0 \to \mathrm{coker}(\epsilon_A) \to \mathrm{coker}(\epsilon_B) \to \mathrm{coker}(\epsilon_C) \to 0.$$

The cokernels $\mathrm{coker}(\epsilon_A)$ and $\mathrm{coker}(\epsilon_C)$ can both be embedded as submodules in the injective modules E_A^1 and E_C^1, respectively, which by Theorem 3.3.10 yields injective representations $\tilde{d_A^0} : \mathrm{coker}(\epsilon_A) \to E_A^1$ and $\tilde{d_C^0} : \mathrm{coker}(\epsilon_C) \to E_C^1$ respectively. Since $\tilde{d_A^0}, \tilde{d_C^0}$ are injective, and the rows of (3.4) are exact, Proposition 3.3.13 yields an injective module $E_B^1 = E_A^1 \oplus E_C^1$ and a monomorphism $\tilde{d_B^0} : \mathrm{coker}(\epsilon_B) \to E_B^1$, with maps $i_1 : E_A^1 \to E_B^1$, $\pi_1 : E_B^1 \to E_C^1$ s.t.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{coker}(\epsilon_A) & \longrightarrow & \mathrm{coker}(\epsilon_B) & \longrightarrow & \mathrm{coker}(\epsilon_C) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \tilde{d_A^0}} & & \downarrow{\scriptstyle \tilde{d_B^0}} & & \downarrow{\scriptstyle \tilde{d_C^0}} & & \\ 0 & \longrightarrow & E_A^1 & \xrightarrow{i_1} & E_B^1 & \xrightarrow{\pi_1} & E_C^1 & \longrightarrow & 0 \end{array} \tag{3.5}$$

commutes and has exact rows. Combining the Diagrams (3.4) and (3.5) with the natural maps $E_A^0 \to \operatorname{coker}(\epsilon_A)$, $E_B^0 \to \operatorname{coker}(\epsilon_B)$ and $E_C^0 \to \operatorname{coker}(\epsilon_C)$ yields the commutative diagram:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A & \xrightarrow{\varphi} & B & \xrightarrow{\psi} & C & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \epsilon_A} & & \downarrow{\scriptstyle \epsilon_B} & & \downarrow{\scriptstyle \epsilon_C} & & \\
0 & \longrightarrow & E_A^0 & \xrightarrow{i_0} & E_B^0 & \xrightarrow{\pi_0} & E_C^0 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d_A^0} & & \downarrow{\scriptstyle d_B^0} & & \downarrow{\scriptstyle d_C^0} & & \\
0 & \longrightarrow & E_A^1 & \xrightarrow{i_1} & E_B^1 & \xrightarrow{\pi_1} & E_C^1 & \longrightarrow & 0
\end{array}$$

with exact rows, where d_A^0 is the composite $E_A^0 \to \operatorname{coker}(\epsilon_A) \xrightarrow{\tilde{d}_A^0} E_A^1$. Similar for d_B^0, d_C^0. Applying the snake lemma again to (3.5), we get an exact sequence

$$0 \to \operatorname{coker}(\tilde{d}_A^0) \to \operatorname{coker}(\tilde{d}_B^0) \to \operatorname{coker}(\tilde{d}_C^0) \to 0.$$

We can iteratively embed the left and right cokernel into injective modules, apply Proposition 3.3.13 to construct the injective module in the middle and the glue the diagrams together to find the desired injective resolution $B \to \mathcal{E}_B$, where $E_B^n = E_A^n \oplus E_C^n$ for all $n \geq 0$ and i_n, π_n are the injection- resp. projection maps. So, also

$$0 \to \mathcal{E}_A \xrightarrow{i} \mathcal{E}_B \xrightarrow{\pi} \mathcal{E}_A \to 0$$

is a short exact sequence of complexes, which completes the proof. □

3.4 Local Cohomology

To define the notion of local cohomology, we first give a very brief introduction to category theory, which we use to define functors. To do so, we follow [30, Section A.1]. The subsequent introduction to local cohomology then follows [7, Chapters 1 and 2].

Definition 3.4.1. A category $\mathcal{C}$ is a class $Obj(\mathcal{C})$ of objects together with a class $Mor(\mathcal{C})$ of morphisms. The set of morphisms from A to B for objects $A, B \in Obj(\mathcal{C})$ is denoted by $\operatorname{Hom}(A, B)$.
For every three objects A, B, C a map

$$\operatorname{Hom}(A, B) \times \operatorname{Hom}(B, C) \to \operatorname{Hom}(A, C), (f, g) \mapsto g \circ f$$

is called the composition of morphism, given the following axioms hold.

(a) (Associativity): If $f : A \to B, g : B \to C, h : C \to D$, then

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

(b) (Identity): For every object A, there is a morphism $\mathrm{id}_A : A \to A$ called the *identity* s.t. for all $f : A \to B$ one has $\mathrm{id}_B \circ f = f \circ \mathrm{id}_A$.

Clearly, the class of R-modules with modules as objects and R-module homomorphisms as morphisms define a category. All results that are stated and used throughout this thesis are used in the case of R-modules.

Definition 3.4.2. A *(covariant) functor* $F(\cdot)$ is a map that assigns to each R-module A an R-module $F(A)$ and to each R-homomorphism $f : A \to B \in \mathrm{Hom}(A, B)$ an R-homomorphism $F(f) : F(A) \to F(B) \in \mathrm{Hom}(F(A), F(B))$ s.t. the following properties hold:

(a) Let $f \in \mathrm{Hom}(A, B), g \in \mathrm{Hom}(B, C)$ then

$$F(g \circ f) = F(f) \circ F(g) \in \mathrm{Hom}(F(A), F(C)).$$

(b) $F(\mathrm{id}_A) = \mathrm{id}_F(A)$ for all R-modules A.

The functor F is called *additive* if additionally $F(f+g) = F(f)+F(g)$ for all $f, g \in \mathrm{Hom}(A, B)$. It is called *$R$-linear* if also $rF(f) = F(rf)$ for all $r \in R$.

Lemma 3.4.3 ([47], Lemma 3.10)**.** *Let M be an R-module. M is a nontrivial direct sum if and only if $id_M = p_1 + p_2$, where p_1, p_2 are nonzero endomorphisms of M s.t. $p_1 \circ p_1 = p_1$ and $p_2 \circ p_2 = p_2$.*

Proof. ($\Rightarrow$) Let $M = A \oplus B$, let p_1 be the projection onto A and let p_2 be the projection onto B. Then these maps clearly satisfy the conditions.

($\Leftarrow$) The properties $\mathrm{id}_M = p_1 + p_2$ and $p_1^2 = p_1$ resp. $p_2^2 = p_2$ imply that $p_1 \circ p_2 = p_2 \circ p_1 = 0$. Set $A = p_1(M)$ and $B = p_2(M)$. The map $(A \oplus B) \to M$, defined by $(a \oplus b) \mapsto a + b$ is clearly surjective since $\mathrm{id}_M = p_1 + p_2$. Let $a \in A \cap B$. Then $a = p_1(m) = p_1^2(m)$ for some $m \in M$ and $a = p_2(n) = p_2^2(n)$ for some $n \in M$. Thus, $a = p_1(p_1(m)) = p_1(p_2(n)) = 0$, so $A \cap B = 0$. Therefore, the map $A \oplus B \to M$ is also injective. □

Lemma 3.4.4 ([47], Lemma 3.10)**.** *Let A, B be two R-modules. If F is an additive functor, then $F(A \oplus B) \cong F(A) \oplus F(B)$.*

Proof. Let $M = A \oplus B$ and define the maps p_1, p_2 as in Lemma 3.4.3. Since F is additive, one has $\mathrm{id}_{F(M)} = F(\mathrm{id}_M) = F(p_1) + F(p_2)$. Moreover, $F(p_1)^2 = F(p_1)$ and $F(p_2)^2 = F(p_2)$. Thus, by Lemma 3.4.3 $F(M) \cong F(p_1)(F(M)) \oplus F(p_2)(F(M)) = F(A) \oplus F(B)$. □

We are interested in those functors that satisfy certain properties when applying them to exact sequences.

Definition 3.4.5. Let A, B, C be R-modules and let

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

be an exact sequence. A functor F is called

(a) *left exact* if $0 \to F(A) \xrightarrow{F(f)} F(B) \xrightarrow{F(g)} F(C)$ is exact,

(b) *right exact* if $F(A) \xrightarrow{F(f)} F(B) \xrightarrow{F(g)} F(C) \to 0$ is exact,

(c) *exact* if it is left-exact and right-exact.

We can now introduce a functor that is fundamental for defining the notion of local cohomology.

Definition 3.4.6. Let M be an R-module and let I be an ideal of R. Let

$$\Gamma_I(M) = \bigcup_{n \in \mathbb{N}} (0 : I^n) = \{m \in M : I^n m = 0 \text{ for some } n \in \mathbb{N}\}.$$

This is called the submodule of M *supported on* I.
For an R-module homomorphism $f : M \to N$, one has $f(\Gamma_I(M)) \subseteq \Gamma_I(N)$, therefore it makes sense to define the map $\Gamma_I(f) : \Gamma_I(M) \to \Gamma_I(N)$, which is the restriction of f to $\Gamma_I(M)$.

It is easy to see that, if $g \in \mathrm{Hom}(M,N), h \in \mathrm{Hom}(N,L)$ are further R-module homomorphisms and $r \in R$, then $\Gamma_I(h \circ f) = \Gamma_I(h) \circ \Gamma_I(f)$, $\Gamma_I(f+g) = \Gamma_I(f) + \Gamma_I(g)$, $\Gamma_I(rf) = r\Gamma_I(f)$ and $\Gamma_I(\mathrm{id}_M) = \mathrm{id}_{\Gamma_I(M)}$.
Thus, $\Gamma_I(\cdot)$ can be seen as an R-linear functor on R-modules and is called the *I-torsion functor*.

Lemma 3.4.7 ([7], Lemma 1.1.6)**.** *The I-torsion functor is left-exact.*

Proof. Consider the exact sequence

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0,$$

where A, B and C are R-modules. Since $\Gamma_I(f)$ agrees with f on $\Gamma_I(A)$ it is clear, that $\Gamma_I(f)$ is injective. Also, $\Gamma_I(g) \circ \Gamma_I(f) = \Gamma_I(g \circ f) = 0$, thus $\mathrm{Im}(\Gamma_I(f)) \subseteq \ker(\Gamma_I(g))$.
Now, let $b \in \ker(\Gamma_I(g))$. Then, $b \in \Gamma_I(B)$ and there exists a nonnegative integer $n \in \mathbb{N}$ s.t. $I^n b = 0$ and $b \in \ker(g) = \mathrm{Im}(f)$. Thus, $f(a) = b$ for some $a \in A$. Note that one has $f(ra) = rf(a) = rb = 0$ for each $r \in I^n$. Thus, $ra = 0$, since f is injective. This implies that $I^n a = 0$ and $a \in \Gamma_I(A)$, i.e. $\ker(\Gamma_I(g)) \subseteq \mathrm{Im}(\Gamma_I(f))$. □

Definition 3.4.8. An R-module M is called

(a) *I-torsion-free* if $\Gamma_I(M) = 0$,

(b) *I-torsion* if $\Gamma_I(M) = M$.

Lemma 3.4.9 ([7], Lemma 2.1.1)**.** *Let M be an R-module and I an ideal.*

(a) *If I contains a nonzerodivisor on M, then $\Gamma_I(M) = 0$.*

(b) *Assume M is finitely generated. Then, $\Gamma_I(M) = 0$ if and only if I contains a nonzerodivisor on M.*

Proof. (a) Let $m \in \Gamma_I(M)$ and suppose $r \in I$ is a nonzerodivisor on M. Then there exists $n \in \mathbb{N}$ s.t. $I^n m = 0$. Thus $r^n m = 0$, which implies that $m = 0$.

(b) ($\Leftarrow$) This follows directly from (a).

($\Rightarrow$) Assume that I contains only zerodivisors. Then $I \subseteq \bigcup_{\mathfrak{p} \in \mathrm{Ass}(M)} \mathfrak{p}$. Also, $\mathrm{Ass}(M)$ is finite, since M is finitely generated. Hence, by Proposition 2.1.3, $I \subseteq \mathfrak{p}$ for some $\mathfrak{p} \in \mathrm{Ass}(M)$. Since there exists a submodule N of M s.t. $\mathrm{Ann}(N) = \mathfrak{p}$, it follows that $(0 : I) \neq 0$, i.e. $\Gamma_I(M) \neq 0$. □

Lemma 3.4.10 ([7], Lemma 2.1.2)**.** *Let M be an R-module and let I be an ideal of R. Then $M/\Gamma_I(M)$ is I-torsion-free.*

Proof. Let $m \in M$ s.t. $m + \Gamma_I(M) \in M/\Gamma_I(M)$ is annihilated by I^n, for some $n \in \mathbb{N}$. Thus, $I^n m \subseteq \Gamma_I(M)$. $I^n m$ is a finitely generated submodule of $\Gamma_I(M)$ and every element of $I^n m$ is annihilated by some power of I. Thus there is $t \in \mathbb{N}$ s.t. $I^t I^n m = 0$. Thus, we get that $m \in (0 : I^{n+t}) \subseteq \Gamma_I(M)$. Therefore, $m \in \Gamma_I(M)$, i.e. $m + \Gamma_I(M) = 0$. □

Remark 3.4.11. If M is I-torsion, then all submmodules of M and all R-homomorphic images of M are also I-torsion.

The I-torsion functor does not only preserve injectivity of homomorphisms, it also preserves the property of an R-module M being injective.

Proposition 3.4.12 ([7], Proposition 2.1.4)**.** *Let R be Noetherian and let M be an injective R-module. Then $\Gamma_I(M)$ is an injective R-module.*

Proof. Let $J \subseteq R$ be an ideal and let $f : J \to \Gamma_I(M) \subseteq M$ be a homomorphism. Since M is injective, f extends to $\tilde{f} : R \to M$. Let $m = \tilde{f}(1) \in M$, then $f(r) = rm$ for all $r \in J$.

$f(J)$ is a finitely generated submodule of $\Gamma_I(M)$ as R is Noetherian. Thus, $I^t f(J) = 0$ for some $t \in \mathbb{N}$. $f(J)$ is also a submodule of the finitely generated R-module Rm. Thus, the Artin–Rees lemma implies that there is $c \in \mathbb{N}$ s.t. for all $n \in \mathbb{N}$ with $n \geq c$ we have

$$I^n(Rm) \cap f(J) = I^{n-c}(I^c(R^m) \cap f(J)).$$

Therefore, $I^{t+c}(Rm \cap f(J)) \subseteq I^t f(J) = 0$. Now, this allows us to define a homomorphism $f' : I^{t+c} + J \to \Gamma_I(J)$, s.t. $f'(s + r) = rm$ for all $s \in I^{t+c}, r \in J$. This is possible, since if $r_1, r_2 \in J$ s.t. $r_1 - r_2 \in I^{t+c}$, then $r_1 m - r_2 m = (r_1 - r_2)m \in I^{t+c}(Rm) \cap f(J) = 0$.

Since M is injective, there is $\tilde{f}' : R \to M$ s.t. $\tilde{f}'$ extends f' and for $w = \tilde{f}'(1)$ one has $f'(r) = rw$ for all $r \in I^{t+c} + J$. Also, f' extends f, as $f'|_J = f$.
Note that for all $s \in I^{t+c}$ we have that $sw = f'(s) = f'(s + 0) = 0$ by the definition of f'. Thus, $w \in \Gamma_I(M)$ and $\tilde{f}'$ extends f. With Baer's criterion 3.3.3, we can now conclude that $\Gamma_I(M)$ is injective. □

Corollary 3.4.13 ([7], Corollary 2.1.6)**.** *Let M be an R-module. If M is I-torsion, then there exists an injective resolution of M consisting entirely of I-torsion modules.*

Proof. Recall, that for an R-module N, there exists an injective presentation $h : N \to \tilde{E}$. As $\Gamma_I(\cdot)$ is left exact, this gives us an injective homomorphism $\Gamma_I(h) : \Gamma_I(N) \to \Gamma_I(\tilde{E})$, where Proposition 3.4.12 implies that $\Gamma_I(\tilde{E})$ is injective.

If M is I-torsion, then one has $\Gamma_I(M) = M$ s.t. by M can be embedded in an injective I-torsion module $E = \Gamma_I(\tilde{E})$.
Now suppose that $n \in \mathbb{N}$ and we have an exact sequence

$$0 \to M \xrightarrow{\epsilon} E^0 \to \cdots \to E^{n-1} \xrightarrow{d^{n-1}} E^n$$

of R-modules, where all $E^0, \ldots, E^n$ are injective I-torsion R-modules. Set $C = \operatorname{coker}(d^{n-1})$ which is I-torsion as a homomorphic image of E^n. Apply the above procedure to C, to obtain an injective I-torsion module E^{n+1} and a monomorphism $g : C \to E^{n+1}$. Then define the map $d^n : E^n \to E^{n+1}$ to be the composition of the natural epimorphism from E^n to C and g, which elongates our exact sequence by one term. Inductively, we obtain the desired result. □

We now have all the tools to define the notion of *local cohomology*. Let $R = k[x_1, \ldots, x_n]$ be standard graded and let $\mathfrak{m}$ be the irrelevant ideal. Take an injective resolution $M \to \mathcal{E}$ and apply the functor $\Gamma_{\mathfrak{m}}(\cdot)$ to the complex $\mathcal{E}$ to obtain

$$0 \to \Gamma_{\mathfrak{m}}(E^0) \xrightarrow{\Gamma_{\mathfrak{m}}(\epsilon)} \cdots \to \Gamma_{\mathfrak{m}}(E^n) \xrightarrow{\Gamma_{\mathfrak{m}}(d^n)} \Gamma_{\mathfrak{m}}(E^{n+1}) \to \cdots$$

and take the i-th cohomology module of this new complex to obtain

$$H^i(\Gamma_{\mathfrak{m}}(\mathcal{E})) = \ker(\Gamma_{\mathfrak{m}}(d^i))/\operatorname{Im}(\Gamma_{\mathfrak{m}}(d^{i-1})).$$

This leads to the following definition.

Definition 3.4.14. The i-th cohomology module

$$H^i_{\mathfrak{m}}(M) = H^i(\Gamma_{\mathfrak{m}}(\mathcal{E}))$$

of an injective resolution $M \to \mathcal{E}$ is called the *i-th local cohomology module* of M.

By a standard fact of homological algebra $H^i_{\mathfrak{m}}(M)$ does, up to isomorphism, not depend on the choice of injective resolution of M (see e.g. [31, Chapter 6]).

Lemma 3.4.15. *Let M be an R-module. Then $H^0_{\mathfrak{m}}(M) \cong \Gamma_{\mathfrak{m}}(M)$.*

Proof. Since $\Gamma_{\mathfrak{m}}(\cdot)$ is left exact, one has that

$$H^0_{\mathfrak{m}}(M) = \ker(\Gamma_{\mathfrak{m}}(d^0))/\operatorname{Im}(\Gamma_{\mathfrak{m}}(0 \to E^0)) \cong \ker(\Gamma_{\mathfrak{m}}(d^0)) \cong \operatorname{Im}(\Gamma_{\mathfrak{m}}(\epsilon)) \cong \Gamma_{\mathfrak{m}}(M). \qquad \square$$

Lemma 3.4.16. *A short exact sequence of R-modules $0 \to A \to B \to C \to 0$ induces a long exact sequence of local cohomology modules*

$$0 \to H^0_{\mathfrak{m}}(A) \to H^0_{\mathfrak{m}}(B) \to H^0_{\mathfrak{m}}(C) \to H^1_{\mathfrak{m}}(A) \to \cdots$$
$$\cdots \to H^i_{\mathfrak{m}}(B) \to H^i_{\mathfrak{m}}(C) \to H^{i+1}_{\mathfrak{m}}(A) \to \cdots .$$

Proof. By Corollary 3.3.14, there exist injective resolution $\mathcal{E}_A, \mathcal{E}_B$, and $\mathcal{E}_C$ of A, B, and C respectively, s.t. $0 \to \mathcal{E}_A \to \mathcal{E}_B \to \mathcal{E}_C \to 0$ is exact, where $\mathcal{E}^i_B = \mathcal{E}^i_A \oplus \mathcal{E}^i_C$ for all $i \geq 0$. After applying $\Gamma_{\mathfrak{m}}(\cdot)$, this is still exact:

$$0 \to \Gamma_{\mathfrak{m}}(\mathcal{E}^i_A) \to \Gamma_{\mathfrak{m}}(\mathcal{E}^i_A) \oplus \Gamma_{\mathfrak{m}}(\mathcal{E}^i_C) \to \Gamma_{\mathfrak{m}}(\mathcal{E}^i_C) \to 0.$$

Thus,

$$\begin{array}{ccccccccc} & & & & 0 & & 0 & & 0 \\ & & & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \Gamma_{\mathfrak{m}}(\mathcal{E}_A) & \longrightarrow & \Gamma_{\mathfrak{m}}(\mathcal{E}_B) & \longrightarrow & \Gamma_{\mathfrak{m}}(\mathcal{E}_C) & \longrightarrow & 0 \end{array}$$

is a short exact sequence of complexes with exact rows. Applying Lemma 3.1.9 yields the long exact sequence, we were looking for. $\square$

Lemma 3.4.17 ([7], Corollary 2.1.7)**.** *Let M be an R-module.*

(a) *If M is $\mathfrak{m}$-torsion, then $H^i_{\mathfrak{m}}(M) = 0$ for all $i > 0$.*

(b) *For each R-module M, we have $H^i_{\mathfrak{m}}(\Gamma_{\mathfrak{m}}(M)) = 0$ for all $i > 0$.*

(c) *For each R-module M, we have $H^i_{\mathfrak{m}}(M) \cong H^i_{\mathfrak{m}}(M/\Gamma_{\mathfrak{m}}(M))$ for all $i > 0$.*

Proof. (a) Since $H^i_{\mathfrak{m}}(M)$ does not depend on the choice of the injective resolution of M, we can, by Corollary 3.4.13, choose an injective resolution $M \to \mathcal{E}$ s.t. each E^n is an $\mathfrak{m}$-torsion module, i.e. $\Gamma_{\mathfrak{m}}(E^n) = E^n$. for all $n \geq 0$. Since $H^i(\mathcal{E}) = 0$ for all $i > 0$, it follows that $H^i_{\mathfrak{m}}(M) = H^i(\Gamma_{\mathfrak{m}}(M)) = 0$ for all $i > 0$.

(b) Since, $\Gamma_{\mathfrak{m}}(M)$ is $\mathfrak{m}$-torsion, the result follows from (a).

(c) Let $0 \to \Gamma_{\mathfrak{m}}(M) \to M \to M/\Gamma_{\mathfrak{m}}(M) \to$ be a short exact sequence. Then, Lemma 3.4.16 yields a long exact sequence of local cohomology. Since $H^i_{\mathfrak{m}}(\Gamma_{\mathfrak{m}}(M)) = 0$ for all $i > 0$, it follows that $H^i_{\mathfrak{m}}(M) \cong H^i_{\mathfrak{m}}(M/\Gamma_{\mathfrak{m}}(M))$ for all $i > 0$. $\square$

The choice of $\mathfrak{m}$ as the maximal graded ideal of the $\mathbb{Z}$-graded ring R, to define local cohomology, yields the question of whether for a graded module M, the local cohomology is graded too. As is shown in [7, Chapter 12], it is true that every graded module M can be embedded in graded injective modules. Thus, $\Gamma_{\mathfrak{m}}(\cdot)$ can be viewed as a left-exact additive functor on graded R-modules and one can construct an exact sequence

$$0 \to M \to E^0 \to \cdots \to E^{n-1} \xrightarrow{d^{n-1}} E^n \to \cdots ,$$

where all E^n are graded injective modules. Taking the i-th cohomology we get the graded module $H^i_{\mathfrak{m}}(M)$, which is the same module, as when it is constructed without gradings.

There is a useful result regarding zerodivisors in the graded case.

Lemma 3.4.18 ([8], Proposition 1.5.12)**.** *Let M be a finitely generated R-module and assume k is infinite. If $\mathfrak{m}$ contains a nonzerodivisor on M, then it can be chosen linear.*

Proof. As $\mathfrak{m}$ contains a nonzerodivisor we know that $\mathfrak{m}_1 \cap \mathfrak{p}$ is a proper subspace of $\mathfrak{m}_1$ for all $\mathfrak{p} \in \operatorname{Ass}(M)$. Since M is finitely generated, we know by Corollary 2.2.25 that $\operatorname{Ass}(M)$ is a finite set. Because k is infinite, this implies that $\bigcup_{\mathfrak{p}\in\operatorname{Ass}(M)} \mathfrak{m}_1 \cap \mathfrak{p} \subsetneq \mathfrak{m}_1$ as $\mathfrak{m}_1$ cannot be written as a finite union of proper subspaces. Therefore, there exists $x \in \mathfrak{m}_1 \setminus \bigcup_{\mathfrak{p}\in\operatorname{Ass}(M)} \mathfrak{p}$, which by Proposition 2.2.23 is a nonzerodivisor of degree 1. □

If $\mathfrak{m}$ consists of zerodivisors we get another useful result.

Lemma 3.4.19. *Let M be a graded R-module. If $\operatorname{kdim}(M) = 0$, then $H^0_{\mathfrak{m}}(M) = M$.*

Proof. If $\operatorname{kdim}(M) = 0$, then all $\mathfrak{p} \in \operatorname{Spec}(R)$ containing $\operatorname{Ann}(M)$ are maximal and homogeneous by Proposition 2.3.15. Thus, $\sqrt{\operatorname{Ann}(M)} = \mathfrak{m}$ by Lemma 2.3.18. Therefore, there exists $n \in \mathbb{N}$ s.t. $\mathfrak{m}^n \subseteq \operatorname{Ann}(M) \subseteq \mathfrak{m}$ by Lemma 2.1.20, which implies that $\mathfrak{m}^n M = 0$. This shows that $M = \Gamma_{\mathfrak{m}}(M) = H^0_{\mathfrak{m}}(M)$. □

There is a useful result due to A. Grothendieck relating local cohomology with Krull dimension.

Theorem 3.4.20 (Grothendieck's Vanishing Theorem, [7], Theorem 6.1.2)**.** *Let M be a finitely generated graded R-module. Then $H^i_{\mathfrak{m}}(M) = 0$ for all $i > \operatorname{kdim}(M)$.*

Proof. The proof is done by induction on $\operatorname{kdim}(M)$. If $\operatorname{kdim}(M) = 0$, the result follows from the Lemmas 3.4.19 and 3.4.17.

Let $\operatorname{kdim}(M) = n > 0$ and suppose the result holds for $n-1$. By (c) of Lemma 3.4.17, we may assume that M is $\mathfrak{m}$-torsion-free, i.e. contains a nonzerodivisor on M that can be chosen linear by Lemma 3.4.18. This yields the short exact sequence

$$0 \to M(-1) \xrightarrow{x} M \to M/xM \to 0.$$

Let $i > n$. The long exact sequence in local cohomology yields

$$H^{i-1}_{\mathfrak{m}}(M/xM) \to H^i_{\mathfrak{m}}(M(-1)) \xrightarrow{\alpha_x} H^i_{\mathfrak{m}}(M),$$

where α_x is induced by multiplication by x. Since x is a nonzerodivisor, Proposition 6.2.12 implies that $\operatorname{kdim}(M/xM) = n-1$. Thus by our induction hypothesis, $H^{i-1}_{\mathfrak{m}}(M/xM) = 0$. Therefore, α_x is injective and we get a sequence of monomorphisms

$$H^i_{\mathfrak{m}}(M)_d \xrightarrow{\alpha_x} H^i_{\mathfrak{m}}(M)_{d+1} \xrightarrow{\alpha_x} H^i_{\mathfrak{m}}(M)_{d+2} \xrightarrow{\alpha_x} \cdots.$$

But since any element in $H^i_{\mathfrak{m}}(M)$ eventually gets annihilated, we get that $H^i_{\mathfrak{m}}(M)_d = 0$. Since this holds for all d, we have $H^i_{\mathfrak{m}}(M) = 0$. □

Until now we have always considered the local cohomology of modules over the same base ring. But sometimes it is necessary to change the ring. The following result is due to M. Brodmann and R.-Y. Sharp.

Theorem 3.4.21 (Independence Theorem, [7], Theorem 13.1.6)**.** *Let S, R be graded rings, let I be an ideal of S, let M a graded R-module and let $f : S \to R$ be a homogeneous homomorphism. Then*

$$H^i_I(M) \cong H^i_{f(I)R}(M) \text{ for all } i \in \mathbb{Z}_{\geq 0}.$$

Proof. The proof of this result can be looked up in [7, Chapter 13]. □

Chapter 4

Algebraic Geometry

The concepts of algebraic geometry provide us with the tools for the qualitative study of the solutions of systems of polynomial equations and their relationship with polynomial ideals. While algebraic geometry is a very vast subject, this chapter mainly is an introduction to the elementary concepts that are used throughout the subsequent chapters. It begins with a discussion of the affine space, where we show how to represent the set of solutions of a system of polynomials and prove fundamental results like the Nullstellensatz. Then, we adjust these concepts to the projective space and explain the relationship between affine and projective space based on the procedure of homogenization and dehomogenization. Then, we present the concept of Zariski topology. The chapter is concluded with a discussion on the dimension of varieties.

4.1 Affine Space

First, we discuss the affine space, based on [29, Chapter 1] and [43, Chapter 3]. Unless mentioned otherwise, R will denote the polynomial ring $k[x_1, \ldots, x_n]$.

Definition 4.1.1. Let k be a field and $n \in \mathbb{Z}_{>0}$, then the *n-dimensional affine space* is the set

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

Let $P = (a_1, \ldots, a_n) \in k^n$, then P is called a (*k-rational*) *point* and the a_i's are called the *coordinates* of P.

As our main goal is to solve systems of polynomials, it is of great interest to look at the roots of polynomials.

Definition 4.1.2. Let $T \subseteq R$ be a set of polynomials. Then the set of points

$$\mathcal{V}(T) = \{P \in k^n \mid f(P) = 0 \ \forall \ f \in T\}$$

is called the *affine variety* of the set T.

Definition 4.1.3. A set $Y \subseteq k^n$ is called an *algebraic set*, if there exists a set of polynomials $T \subseteq R$ s.t. $Y = \mathcal{V}(T)$. It is called *irreducible*, if it is not the union of two smaller algebraic sets.

Remark 4.1.4. Some references call only irreducible algebraic sets affine varieties. In this thesis, every algebraic set is called affine variety to highlight the fact that it is in the affine space and not in the *projective space*, which will be introduced in the next section.

An affine variety $\mathcal{V}(f_1, \ldots, f_s)$ is therefore simply the set of solutions to the following system of equations:

$$f_1 = \cdots = f_s = 0.$$

Remark 4.1.5. If $\langle T \rangle$ is the ideal generated by the set T, then it is easy to see that $\mathcal{V}(T) = \mathcal{V}(\langle T \rangle)$. Also, since R is Noetherian by the Hilbert basis theorem, the ideal $\langle T \rangle$ is finitely generated and there exists a finite collection of polynomials $f_1, \ldots, f_s$ s.t. $\mathcal{V}(T) = \mathcal{V}(f_1, \ldots, f_s)$. This suggests that it would be convenient to have a way of representing $\mathcal{V}(T)$ by means of polynomials whose roots are easy to find. This will be explored further when we introduce the notion of Gröbner basis in Chapter 5.

First, we focus on the basic properties of varieties.

Proposition 4.1.6 ([27] Proposition 6, Chapter 4.1)**.** *The following properties hold for affine varieties:*

(a) *If $f, g \in R$, then $\mathcal{V}(f, g) = \mathcal{V}(f) \cap \mathcal{V}(g)$.*

(b) *If $S \subseteq T \subseteq R$, then $\mathcal{V}(T) \subseteq \mathcal{V}(S)$.*

(c) *If $I, J \subseteq R$ are ideals, then $\mathcal{V}(I \cup J) = \mathcal{V}(I + J) = \mathcal{V}(I) \cap \mathcal{V}(J)$.*

(d) *If $I, J \subseteq R$ are ideals, then $\mathcal{V}(I \cap J) = \mathcal{V}(IJ) = \mathcal{V}(I) \cup \mathcal{V}(J)$.*

(e) *$\mathcal{V}(0) = k^n, \mathcal{V}(1) = \emptyset$ if k is infinite and $\mathcal{V}(x_1 - a_1, \ldots, x_n - a_n) = (a_1, \ldots, a_n)$ for any point $(a_1, \ldots, a_n) \in k^n$.*

Proof. (a) Let $p \in \mathcal{V}(f, g)$. Then $f(p) = 0$ and $g(p) = 0$. Thus, $p \in \mathcal{V}(f) \cap \mathcal{V}(g)$.

(b) $\mathcal{V}(T) = \bigcap_{f \in T} \mathcal{V}(f) \subseteq \bigcap_{f \in S} \mathcal{V}(f) = \mathcal{V}(S)$.

(c) $\mathcal{V}(I \cup J) = \bigcap_{f \in I \cup J} \mathcal{V}(f) = \bigcap_{f \in I} \mathcal{V}(f) \cap \bigcap_{f \in J} \mathcal{V}(f) = \mathcal{V}(I) \cap \mathcal{V}(J)$.

(d) $\mathcal{V}(IJ) = \bigcap_{f \in IJ} \mathcal{V}(f) = \bigcap_{\substack{g \in I \\ h \in J}} \mathcal{V}(gh) = \bigcap_{g \in I} \mathcal{V}(g) \cup \bigcap_{h \in J} \mathcal{V}(h) = \mathcal{V}(I) \cup \mathcal{V}(J)$, where the third equality holds because $gh = 0$ if and only if either $g = 0$ or $h = 0$.
Since $IJ \subseteq I \cap J$ it follows that $\mathcal{V}(I \cap J) \subseteq \mathcal{V}(IJ) = \mathcal{V}(I) \cup \mathcal{V}(J)$. Since $I \cap J \subseteq I, J$ it follows that $\mathcal{V}(I) \subseteq \mathcal{V}(I \cap J)$. Similarly, $\mathcal{V}(J) \subseteq \mathcal{V}(I \cap J)$. Therefore, $\mathcal{V}(I) \cup \mathcal{V}(J) \subseteq \mathcal{V}(I \cap J)$.

(e) This is immediate. □

Example 4.1.7. Consider the polynomials $f_1 = x^2 - 1, f_2 = xy + x \in \mathbb{R}[x, y]$ as well as $g_1 = x^2 - z^2, g_2 = xy + xz \in \mathbb{R}[x, y, z]$. Then $\mathcal{V}(f_1, f_2) = \{(1, -1), (-1, -1)\}$ and

$$\begin{aligned} \mathcal{V}(g_1, g_2) &= \mathcal{V}((x - z)(x + z), x(y + z)) \\ &= (\mathcal{V}(x - z) \cup \mathcal{V}(x + z)) \cap (\mathcal{V}(x) \cup \mathcal{V}(y + z)) \\ &= \{(0, t, 0), (t, -t, t), (t, t, -t) : t \in \mathbb{R}\}. \end{aligned}$$

To study the algebraic properties of affine varieties, we are also interested in looking at the polynomials that vanish on a set of points.

Definition 4.1.8. Let $Y \subseteq k^n$ be a set of points. Then

$$\mathcal{I}(Y) = \{f \in R \mid f(P) = 0 \ \forall \ P \in Y\}$$

is called the *vanishing ideal of* Y. It is easy to see that $\mathcal{I}(Y)$ is actually an ideal.

Proposition 4.1.9 ([15], Corollary 3, Chapter 4.2)**.** *Let $Y \subseteq k^n$ be a set of points. Then $\mathcal{I}(Y)$ is a radical ideal.*

Proof. Let $f \in \sqrt{\mathcal{I}(Y)}$, then $f^m \in \mathcal{I}(Y)$ for some m. Therefore, $f^m(p) = 0$ for all $p \in Y$. Therefore, $f(p) = 0$ for all $p \in Y$. Thus, $f \in \mathcal{I}(Y)$. It follows that $\sqrt{\mathcal{I}(Y)} = \mathcal{I}(Y)$. □

Proposition 4.1.10. *The following properties hold for vanishing ideals:*

(a) *If $X \subseteq Y \subseteq k^n$, then $\mathcal{I}(Y) \subseteq \mathcal{I}(X)$.*

(b) *If $Y_1, Y_2 \subseteq k^n$, then $\mathcal{I}(Y_1 \cup Y_2) = \mathcal{I}(Y_1) \cap \mathcal{I}(Y_2)$.*

(c) *If $T \subseteq R$, then $T \subseteq \mathcal{I}(\mathcal{V}(T))$.*

(d) *If $Y \subseteq k^n$, then $Y \subseteq \mathcal{V}(\mathcal{I}(Y))$.*

(e) *If $T \subseteq R$, then $\mathcal{V}(\mathcal{I}(\mathcal{V}(T))) = \mathcal{V}(T)$.*

(f) *If $Y \subseteq k^n$, then $\mathcal{I}(\mathcal{V}(\mathcal{I}(Y))) = \mathcal{I}(Y)$.*

(g) *$\mathcal{I}(\emptyset) = R$, $\mathcal{I}(k^n) = 0$ if k is infinite and $\mathcal{I}(\{(a_1, \ldots, a_n)\}) = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ for any point $(a_1, \ldots, a_n) \in k^n$.*

Proof. (a) Let $f \in \mathcal{I}(Y)$. Then $f(p) = 0$ for all $p \in Y \supseteq X$. Thus, $f \in \mathcal{I}(X)$.

(b) ($\subseteq$) Let $f \in \mathcal{I}(Y_1 \cup Y_2)$. Then f vanishes on $Y_1 \cup Y_2$ and therefore also on Y_1, i.e. $f \in \mathcal{I}(Y_1)$. Similarly, $f \in \mathcal{I}(Y_2)$.

($\supseteq$) Let $f \in \mathcal{I}(Y_1) \cap (Y_2)$. Then $f \in \mathcal{I}(Y_1)$, so f vanishes on Y_1. Similarly, f vanishes on Y_2.

(c) Let $f \in T$, then $f(p) = 0$ for all $p \in \mathcal{V}(T)$, which implies that $f \in \mathcal{I}(\mathcal{V}(T))$.

(d) Let $p \in Y$, then $f(p) = 0$ for all $f \in \mathcal{I}(Y)$, which implies that $p \in \mathcal{V}(\mathcal{I}(Y))$.

(e) By (d) we have $\mathcal{V}(T) \subseteq \mathcal{V}(\mathcal{I}(\mathcal{V}(T)))$. On the other hand by (c) we have $T \subseteq \mathcal{I}(\mathcal{V}(T))$. So Proposition 4.1.6 (b) implies that $\mathcal{V}(T) \supseteq \mathcal{V}(\mathcal{I}(\mathcal{V}(T)))$.

(f) By (c) we have $\mathcal{I}(Y) \subseteq \mathcal{I}(\mathcal{V}(\mathcal{I}(Y)))$. On the other hand by (d) we have $Y \subseteq \mathcal{V}(\mathcal{I}(Y))$. So (a) implies that $\mathcal{I}(Y) \supseteq \mathcal{I}(\mathcal{V}(\mathcal{I}(Y)))$.

(g) This is immediate. □

Example 4.1.11. Let $V = \mathcal{V}(x^2 - z^2, xy + xz) \subseteq \mathbb{R}^3$ from the previous example. Then

$$\begin{aligned}\mathcal{I}(V) &= \mathcal{I}(\{(0,t,0) : t \in \mathbb{R}\}) \cap \mathcal{I}(\{(t,-t,t) : t \in \mathbb{R}\}) \cap \mathcal{I}(\{(t,t,-t) : t \in \mathbb{R}\}) \\ &= \langle x, x - z \rangle \cap \langle x - z, y + z \rangle \cap \langle x + z, y + z \rangle \\ &= \langle x - z, x(y + z) \rangle \cap \langle x(y + z), x + z \rangle = \langle x^2 - z^2, xy + xz \rangle.\end{aligned}$$

In this case we see that $\mathcal{I}(\mathcal{V}(I)) = I$. But this is clearly not always true as can easily be seen in $\mathbb{R}[x]$ by $\mathcal{I}(\mathcal{V}(x^2)) = \mathcal{I}(0) = \langle x \rangle$.

We discuss next, when this is the case and study the relationship between varieties and ideals. First, we look at how maximal ideals look like if k is algebraically closed.

Proposition 4.1.12 ([43], Theorem 3.10)**.** *Let k be algebraically closed and let $\mathfrak{m}$ be a maximal ideal in R. Then there exists $(a_1, \ldots, a_n) \in k^n$ s.t.*

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

Proof. Since $\mathfrak{m}$ is a maximal ideal, it is a proper ideal. Next, we use the algebraic fact that $k \subseteq k[x_1, \ldots, x_n]/\mathfrak{m}$ is a finite field extension of k. Since k is algebraically closed, it follows that $k \cong k[x_1, \ldots, x_n]/\mathfrak{m}$. Now, let $\overline{x}_i \in k[x_1, \ldots, x_n]$. Then $\overline{x}_i = x_i + \mathfrak{m} = a_i$ for some $a_i \in k$. Thus, $x_i - a_i \in \mathfrak{m}$ for all $i = 1, \ldots, n$. This implies that $\langle x_1 - a_1, \ldots, x_n - a_n \rangle \subseteq \mathfrak{m}$. But both of these ideals are maximal, thus equality holds. □

To see, which systems of equations actually have solutions, the following theorem will be a helpful tool.

Theorem 4.1.13 (Weak Hilbert Nullstellensatz, [33], Theorem 2.6.13)**.** *Let k be algebraically closed and let I be a proper ideal of R. Then $\mathcal{V}(I) = \emptyset$ if and only if $1 \in I$.*

Proof. ($\Leftarrow$) This is immediate, as if $I = R$, then $\mathcal{V}(I) = \emptyset$.

($\Rightarrow$) The ideal I is contained in a maximal ideal $\mathfrak{m}$, which by Proposition 4.1.12 has the form $\mathfrak{m} = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$. Thus, $\mathcal{V}(\mathfrak{m}) = (a_1, \ldots, a_n) \subseteq \mathcal{V}(I) \neq \emptyset$. □

Theorem 4.1.14 (Strong Hilbert Nullstellensatz, [33], Theorem 2.6.16)**.** *Let k be algebraically closed and let I be a proper ideal of R. Then*

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

Proof. ($\supseteq$) Let $f \in \sqrt{I}$, i.e. $f^m \in I$ for some m and $f^m(p) = 0$ for all $p \in \mathcal{V}(I)$. Thus $f(p) = 0$ for all $p \in \mathcal{V}(I)$ and $f \in \mathcal{I}(\mathcal{V}(I))$.

($\subseteq$) Suppose that $I \neq \emptyset$ and choose $f \in \mathcal{I}(\mathcal{V}(I)) \backslash \{0\}$. Additionally, choose a system of generators $g_1, \ldots, g_r$ of I. Let y be a new variable and consider $J = \langle g_1, \ldots, g_r, yf - 1 \rangle \subseteq R[y]$. For all $(a_1, \ldots, a_{n+1}) \in \mathcal{V}(J)$ one has $a_{n+1} f(a_1, \ldots, a_n) = 1$ and $g_i(a_1, \ldots, a_n) = 0$ for $i = 1, \ldots, r$. But then $(a_1, \ldots, a_n) \in \mathcal{V}(I)$ and $f(a_1, \ldots, a_n) \neq 0$, which is a contradiction to our choice of f. Thus, there is no such point, i.e. $\mathcal{V}(J) = \emptyset$ and the weak Nullstellensatz implies that $1 \in J$. Since $1 \in J$, there exist $h, h_1, \ldots, h_r \in R[y]$ s.t. $\sum_{i=1}^{r} h_i g_i + h(yf - 1) = 1$. Set $y = 1/f$ to get $1 = \sum_{i=1}^{r} h_i(x_1, \ldots, x_n, 1/f) g_i$. Multiplying both sides of the equation by a sufficiently large power of f yields

$$f^m = \sum_{i=1}^{s} A_i g_i \in I \text{ for some } A_i \in R.$$

Thus, $f \in \sqrt{I}$. □

An important consequence of the Nullstellensatz is the following correspondence between affine varieties and radical ideals.

Theorem 4.1.15 (Ideal - Variety Correspondence, [29], Corollary 1.4)**.** *Restricted to radical ideals, the maps*

$$\{ \text{ affine varieties } \} \underset{\mathcal{V}}{\overset{\mathcal{I}}{\rightleftarrows}} \{ \text{ radical ideals } \}$$

are inclusion-reversing. If k is algebraically closed, then the maps are bijections, which are inverses of each other.

Proof. The inclusion-reversing property follows from Propositions 4.1.6 and 4.1.10. Also, for affine varieties V we have $V = \mathcal{V}(\mathcal{I}(V))$ by Proposition 4.1.10.
Note that until now, the properties also hold if we are not restricted to an algebraically closed field and radical ideals.
Since $\mathcal{I}(V)$ is always radical, $\mathcal{I}$ can be seen as a map from affine varieties to radical ideals. Also, we have $\mathcal{I}(\mathcal{V}(I)) = I$ for radical ideals I by Theorem 4.1.14, since $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I} = I$. Thus, the maps are inverses of each other and define bijections. □

This correspondence can be adjusted for irreducible varieties, which gives an interesting result. First, we can give a characterization of irreducible varieties.

Lemma 4.1.16 ([29], Corollary 1.4)**.** *Let $V \subseteq k^n$ be an affine variety. Then V is irreducible if and only if $\mathcal{I}(V)$ is a prime ideal.*

Proof. ($\Rightarrow$) Let V be an irreducible variety and consider $I = \mathcal{I}(V)$. Suppose by contradiction that $\mathcal{I}(V)$ is not prime and let $f, g \in R$ s.t. $fg \in \mathcal{I}(V)$ but $f, g \notin \mathcal{I}(V)$. Then set $V_1 = V \cap \mathcal{V}(f)$ and $V_2 = V \cap \mathcal{V}(g)$. These are affine varieties properly contained in $\mathcal{V}(I)$. If $p \in V$, then $fg(p) = 0$, so either $f(p) = 0$ or $g(p) = 0$, i.e. either $p \in V_1$ or $p \in V_2$. This implies that $V = V_1 \cup V_2$, which is the desired contradiction.

($\Leftarrow$) Let I be prime and consider $V = \mathcal{V}(I)$. Suppose by contradiction that $\mathcal{V}(I)$ is reducible and let V_1, V_2 be affine varieties s.t. $V = V_1 \cup V_2$ with $V_1, V_2 \subsetneq V$. Let $f \in \mathcal{I}(V_1) \setminus \mathcal{I}(V_2)$ and $g \in \mathcal{I}(V_2) \setminus \mathcal{I}(V_1)$. Then $fg \in I$ but $f, g \notin I$, which is a contradiction. Thus, $\mathcal{V}(I)$ is irreducible. □

Since prime ideals are radical, combining the correspondence of Theorem 4.1.15 with Lemma 4.1.16 yields the following result.

Corollary 4.1.17 ([15], Corollary 4, Chapter 4.5)**.** *When k is algebraically closed, $\mathcal{I}$ and $\mathcal{V}$ induce a bijective correspondence between irreducible varieties in k^n and prime ideals in $k[x_1, \ldots, x_n]$.*

4.2 Projective Space

It turns out that working over the affine space is sometimes insufficient and that working over the *projective space* may make things easier. Therefore, it is useful to introduce the notion of projective space, where we refer to [15, Chapter 8] and [43, Chapter 5] for a more detailed discussion.

Definition 4.2.1. Let k be a field and $n \in \mathbb{Z}_{\geq 0}$. Then $\sim$ defines an equivalence relation on $k^{n+1} \setminus \{0\}$ by letting $(a_0, \ldots, a_n) \sim (a_0', \ldots, a_n')$ if and only if there exists $\lambda \in k \setminus \{0\}$ s.t. $(a_0', \ldots, a_n') = (\lambda a_0, \ldots, \lambda a_n)$. The *$n$-dimensional projective space* over k is the set of equivalence classes

$$\mathbb{P}_k^n = (k^{n+1} \setminus \{0\}) / \sim.$$

The equivalence class of a $(n+1)$-tuple $(a_0, \ldots, a_n) \in k^{n+1} \setminus \{0\}$ is called a *(projective) point* P in $\mathbb{P}_k^n$. It is denoted by $(a_0 : a_1 : \cdots : a_n)$. Any $(n+1)$-tuple $(a_0', \ldots, a_n')$ in the equivalence class of P is called a set of *homogeneous coordinates*. If the field k is clear from context the subscript k may be omitted.

Given a polynomial $f \in k[x_0, \ldots, x_n]$ in $n+1$ variables and a point $P \in \mathbb{P}^n$ represented by an $(n+1)$-tuple $(a_0 : \cdots : a_n)$, then evaluating f at P does not make sense because $f(a_0, \ldots, a_n)$ depends on the representative chosen for the equivalence class. Thus, f is not a function on $\mathbb{P}^n$. To resolve this issue, the polynomial ring $S = k[x_0, x_1, \ldots, x_n]$ can be regarded as a standard graded ring $S = \bigoplus_{d \geq 0} S_d$, where the component S_d consists of homogeneous polynomials $f \in S$ of degree d of the form

$$f = \textstyle\sum_\alpha c_\alpha x^\alpha, \text{ with } c_\alpha \neq 0 \text{ only if } |\alpha| = d.$$

Any $f \in S$ has a unique decomposition $f = f_0 + f_1 + \cdots + f_N$ in which f_d is a homogeneous polynomial of degree d.

A homogeneous polynomial $f \in S_d$ has the useful property that

$$f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n)$$

for all $\lambda \in k$.

Like this, the property of f being zero at a point $P \in \mathbb{P}^n$ does only depend on the equivalence class of P and not on the representative, i.e. the condition $f(P) = 0$ is well-defined for homogeneous polynomials. As in the affine case, it now makes sense to look at the roots of polynomials.

Definition 4.2.2. If $T \subseteq S$ is a set of homogeneous polynomials, then the set of points

$$\mathcal{V}_p(T) = \{P \in \mathbb{P}^n \mid f(P) = 0 \ \forall \ f \in T\}$$

is called the *projective variety* of the set T. To extend this notion to homogeneous ideals, $f = f_0 + f_1 + \cdots + f_N \in S$ is said to be zero at a point $P \in \mathbb{P}^n$ if and only if every homogeneous component f_d vanishes at P. Therefore, for a homogeneous ideal $I \subseteq S$, the projective variety $\mathcal{V}_p(I)$ is defined to be $\mathcal{V}_p(T)$, where T is the set of all homogeneous components in I.

Remark 4.2.3. The projective variety of the irrelevant ideal $S_+ = \langle x_0, \ldots, x_n \rangle$ is the empty set, hence the name *irrelevant*.

Example 4.2.4. Consider the polynomials $g_1 = x^2 - z^2, g_2 = xy + xz \in \mathbb{R}[x, y, z]$ as in Example 4.1.11. Then it easy to see that

$$\mathcal{V}_p(g_1, g_2) = \{(0 : 1 : 0), (1 : -1 : 1), (1 : 1 : -1)\}.$$

As before, it is interesting to study, which polynomials vanish on the points of a projective variety.

Definition 4.2.5. Let $Y \subseteq \mathbb{P}^n_k$ be a set of projective points, then

$$\mathcal{I}_p(Y) = \{f \in S \mid f(P) = 0 \ \forall \ P \in Y\}$$

is called the *homogeneous vanishing ideal of* Y. This is equivalent to the ideal generated by $\{f \in S \mid f \text{ homogeneous and } f(P) = 0 \ \forall \ P \in Y\}$. Therefore, $\mathcal{I}_p(Y)$ is in fact a homogeneous ideal.

The properties of Propositions 4.1.6 and 4.1.10 also hold for projective varieties and vanishing ideals.

Proposition 4.2.6. *Let $T_1, T_2 \subseteq S$ be sets of homogeneous polynomials. The following properties hold for projective varieties and homogeneous ideals:*

(a) *If $f, g \in S$, then $\mathcal{V}_p(f, g) = \mathcal{V}_p(f) \cap \mathcal{V}_p(g)$.*

(b) *If $T_1 \subseteq T_2 \subseteq S$, then $\mathcal{V}_p(T_2) \subseteq \mathcal{V}_p(T_1)$.*

(c) *If $I, J \subseteq S$ are homogeneous ideals, then $\mathcal{V}_p(I + J) = \mathcal{V}_p(I \cup J) = \mathcal{V}_p(I) \cap \mathcal{V}_p(J)$.*

(d) *If $I, J \subseteq S$ are homogeneous ideals, then $\mathcal{V}_p(I \cap J) = \mathcal{V}_p(IJ) = \mathcal{V}_p(I) \cup \mathcal{V}_p(J)$.*

(e) *If $X \subseteq Y \subseteq \mathbb{P}^n$, then $\mathcal{I}_p(Y) \subseteq \mathcal{I}_p(X)$.*

(f) *If $X, Y \subseteq \mathbb{P}^n$, then $\mathcal{I}_p(X) \cap \mathcal{I}_p(Y) = \mathcal{I}_p(X \cup Y)$.*

(g) *If $X \subseteq \mathbb{P}^n$, then $X \subseteq \mathcal{V}_p(\mathcal{I}_p(X))$.*

(h) *If $T \subseteq S$, then $T \subseteq \mathcal{I}_p(\mathcal{V}_p(T))$.*

(i) *If $T \subseteq S$, then $\mathcal{V}_p(T) = \mathcal{V}_p(\mathcal{I}_p(\mathcal{V}_p(T)))$.*

(j) *If $X \subseteq \mathbb{P}^n$, then $\mathcal{I}_p(X) \subseteq \mathcal{I}(\mathcal{V}_p(\mathcal{I}_p(X)))$.*

(k) *If I is a homogeneous ideal, then $\mathcal{V}_p(I) = \mathcal{V}_p(\sqrt{I})$.*

The proof is analogous to the affine case and will be omitted.

As mentioned before, the projective variety of the irrelevant ideal is the empty set. Therefore, to restate a projective version of the Nullstellensatz, this has to be taken into consideration.

Theorem 4.2.7 (Projective Nullstellensatz, [43], Theorem 1, Chapter 5.3)**.** *Let k be algebraically closed and $I \subseteq S$ be a homogeneous ideal. Then:*

(a) $\mathcal{V}_p(I) = \emptyset$ *if and only if* $\langle x_0, \dots, x_n \rangle \subseteq \sqrt{I}$,

(b) *if* $\mathcal{V}_p(I) \neq \emptyset$ *then* $\mathcal{I}_p(\mathcal{V}_p(I)) = \sqrt{I}$.

Proof. (a) Let $\pi : k^{n+1} \setminus \{0\} \to \mathbb{P}^n, (a_0, \dots, a_n) \mapsto (a_0 : \cdots : a_n)$ be the map that defines $\mathbb{P}^n$. Then consider the affine variety $\mathcal{V}(I) \subseteq k^{n+1}$ defined by I. Since I is homogeneous, for $\mathcal{V}(I)$ we have

$$(a_0, \dots, a_n) \in \mathcal{V}(I) \iff (\lambda a_0, \dots, \lambda a_n) \in \mathcal{V}(I),$$

and $\mathcal{V}_p(I) = \pi(\mathcal{V}(I) \setminus \{0\}) \subseteq \mathbb{P}^n$. Hence

$$\mathcal{V}_p(I) = \emptyset \iff \mathcal{V}(I) \subseteq \{0\} \iff \sqrt{I} \supseteq \langle x_0, \dots, x_n \rangle,$$

where the second equivalence comes from the affine Nullstellensatz.

(b) We first claim that

$$\mathcal{I}(\mathcal{V}(I)) = \mathcal{I}_p(\mathcal{V}_p(I)) \text{ when } \mathcal{V}_p(I) \neq \emptyset.$$

($\subseteq$) $f \in \mathcal{I}(\mathcal{V}(I))$ implies that any representation of $p \in \mathcal{V}_p(I)$ is a point in $\mathcal{V}(I)$. Thus, f vanishes on $\mathcal{V}_p(I)$.

($\supseteq$) $f \in \mathcal{I}_p(\mathcal{V}_p(I))$ implies that f vanishes on all representations of a point $p \in \mathcal{V}_p(I)$, i.e. it vanishes on $\mathcal{V}(I) \setminus \{0\}$. As f is in a proper homogeneous ideal, the degree zero part f_0 of f must be zero. Thus, f vanishes also on 0.

Now we can conclude since

$$f \in \mathcal{I}_p(\mathcal{V}_p(I)) \iff f \in \mathcal{I}(\mathcal{V}(I)) \iff f \in \sqrt{I},$$

where the last equivalence is again from the corresponding affine version of the statement. □

With the projective version of the Nullstellensatz it is possible, as in the affine case, to establish a one-to-one correspondence between irreducible projective varieties and radical homogeneous ideals. As mentioned before, the only case, where some additional care is needed, is the irrelevant ideal.

Theorem 4.2.8 (Ideal - Variety Correspondence (projective), [43], Corollary 1, Chapter 5.3)**.** *If restricted to homogeneous radical ideals not containing the irrelevant ideal, the maps*

$$\left\{ \begin{array}{l} \textit{Nonempty projective} \\ \textit{varieties} \end{array} \right\} \underset{\mathcal{V}_p}{\overset{\mathcal{I}_p}{\rightleftarrows}} \left\{ \begin{array}{l} \textit{Homogeneous radical} \\ \textit{ideals } J \subseteq k[x_0, \dots, x_n] \\ \textit{with } J \not\supseteq \langle x_0, \dots, x_n \rangle \end{array} \right\}$$

are inclusion-reversing. If k is algebraically closed, the maps are bijections.

Lemma 4.2.9 ([15], Proposition 3, Chapter 4.5)**.** *Let k be algebraically closed. Then I is a graded prime ideal not equal to $\langle x_0, \dots, x_n \rangle$ if and only if $\mathcal{V}_p(I) \subseteq \mathbb{P}^n$ is an nonempty irreducible projective variety and I is radical.*

Proof. ($\Leftarrow$) Let $V = \mathcal{V}_p(I)$ be an irreducible nonempty projective variety and consider its vanishing ideal $\mathcal{I}_p(V) = \sqrt{I} = I$. Let $f, g \in R$ be polynomials s.t. $fg \in \mathcal{I}_p(V)$. Set $V_1 = V \cap \mathcal{V}_p(f), V_2 = V \cap \mathcal{V}_p(g) \subsetneq \mathcal{V}_p(I)$. Then, if $p \in \mathcal{V}_p(I)$ then $fg(p) = 0$. So either $f(p) = 0$ or $g(p) = 0$. Thus, either $p \in V_1$ or V_2. Thus, $V = V_1 \cup V_2$. But as V is irreducible, $V = V_1$ or $V = V_2$. So either $f \in \mathcal{I}_p(V)$ or $g \in \mathcal{I}_p(V)$.

($\Rightarrow$) Let I be a graded prime ideal and consider $\mathcal{V}_p(I)$. Suppose by contradiction that $\mathcal{V}_p(I)$ is reducible and let V_1, V_2 be projective varieties s.t. $V = V_1 \cup V_2$ with $V_1, V_2 \subsetneq V$. Let $f \in \mathcal{I}_p(V_1) \setminus \mathcal{I}_p(V_2), g \in \mathcal{I}_p(V_2) \setminus \mathcal{I}_p(V_1)$. Then $fg \in I$ but $f, g \notin I$, which is a contradiction. Thus, $\mathcal{V}_p(I)$ is irreducible. □

Since graded prime ideals are radical, combining Theorem 4.2.8 with Lemma 4.2.9 yields the following result, which corresponds to the affine case.

Corollary 4.2.10 ([15], Corollary 4, Chapter 4.5)**.** *When k is algebraically closed, $\mathcal{I}_p$ and $\mathcal{V}_p$ induce a bijective correspondence between nonempty irreducible projective varieties in k^n and prime ideals in $k[x_0, \dots, x_n]$ not containing $\langle x_0, \dots, x_n \rangle$.*

The projective space can be seen as a completion of the affine space by adding *points at infinity*. Notice that if $(a_0 : \cdots : a_n)$ with $a_0 \neq 0$ then

$$(a_0 : \cdots : a_n) = (1 : \tfrac{a_1}{a_0} : \cdots : \tfrac{a_n}{a_0}).$$

For a point $(1 : a_1 : \cdots : a_n)$, the elements $a_1, \dots, a_n \in k$ are uniquely determined by this point, since if $(1 : a_1 : \cdots : a_n) = (1 : b_1 : \cdots : b_n)$, there exists a $\lambda \in k$ s.t. $\lambda a_i = b_i$ for all $i = 1, \dots, n$. As $1 = b_0 = \lambda a_0 = \lambda \cdot 1$, we get $\lambda = 1$ and therefore $a_i = b_i$ for all $i = 1, \dots, n$.
This gives an embedding

$$i : \mathbb{A}^n \hookrightarrow \mathbb{P}^n, \qquad (a_1, \dots, a_n) \mapsto (1 : a_1 : \cdots : a_n),$$

where the injectivity comes from the statement about uniqueness. This makes it possible to identify $\mathbb{A}^n$ with $i(\mathbb{A}^n) \subseteq \mathbb{P}^n$, where $i(\mathbb{A}^n)$ is called the *affine part* of $\mathbb{P}^n$
If $n > 0$, then $\mathbb{P}^n = \mathbb{A}^n \cup H^n_{inf}$, where $H^n_{inf} = \{(a_0 : \cdots : a_n) \in \mathbb{P}^n \mid a_0 = 0\}$. Define another map

$$j : \mathbb{P}^{n-1} \to \mathbb{P}^n, \qquad (a_1 : \cdots : a_n) \mapsto (0 : a_1 : \cdots : a_n).$$

This is well defined, as if $(a_1 : \cdots : a_n) = (b_1 : \cdots : b_n)$, there exists $\lambda \in k$ s.t. $\lambda a_i = b_i$ for all $i = 1, \dots, n$. Since $\lambda \cdot 0 = 0$, $(0 : a_1 : \cdots : a_n) = (0 : b_1 : \cdots : b_n)$. Again j is clearly injective and $j(\mathbb{P}^{n-1}) = H^n_{inf}$. Therefore, $H^n_{inf} \cong \mathbb{P}^{n-1}$ and one can write

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

The points in the set H^n_{inf} are called the *points at infinity* of $\mathbb{P}^n$.
Continuing the decomposition by iterating the argument above for smaller n one can actually write

$$\mathbb{P}^n = \mathbb{A}^n \cup \mathbb{A}^{n-1} \cup \cdots \cup \mathbb{A}^0.$$

Where $\mathbb{A}^0$ denotes a single point.

4.3 Homogenization and Dehomogenization

At the end of the last section, an important relationship between affine space and projective space has been introduced. Since many algorithms are improved if the input polynomials are homogeneous, it is of interest to study this and the question of how to make arbitrary polynomials into homogeneous polynomials, further. This section is based on [34, Chapter 4.3].

Definition 4.3.1. Let $R = k[x_1, \dots, x_n]$ and let $S = k[x_1, \dots, x_n, t] = R[t]$.

(a) Let $f \in \sum_\alpha c_\alpha x^\alpha \in R$ be a polynomial in R of total degree d. The *homogenization* of f w.r.t to t is

$$f^h = \sum_\alpha c_\alpha x^\alpha t^{d-|\alpha|}.$$

The variable t is called the *homogenization variable*.

(b) Let $F \in S$ be a homogeneous polynomial. Then $F^{deh} = F(x_1, \ldots, x_n, 1) \in R$ is called the *dehomogenization* of F.

Homogenization can be viewed as the result of multiplying each homogeneous component of f by a power of t to bring it up to degree d. This can be written as

$$f^h = t^d f(\tfrac{x_1}{t}, \ldots, \tfrac{x_n}{t}) \in S.$$

Dehomogenization can be seen as the standard projection map onto the quotient

$$\phi : S \to R \cong S/(t-1).$$

From now on, we will use this homomorphism ϕ to perform dehomogenization.

Example 4.3.2. Consider $f_1 = x^2 - 1, f_2 = xy + x \in \mathbb{R}[x, y]$. After homogenizing w.r.t to the variable t we have

$$f_1^h = t^2 f_1(x/t, y/t) = t^2 x^2/t^2 - t^2 = x^2 - t^2,$$
$$f_2^h = t^2 f_2(x/t, y/t) = t^2 xy/t^2 + t^2 x/t = xy + xt.$$

Dehomogenizing yields

$$\phi(f_1^h) = f_1^h(x, y, 1) = x^2 - 1 = f_1,$$
$$\phi(f_2^h) = f_2^h(x, y, 1) = xy + x = f_2.$$

We just saw that in our examples dehomogenizing the homogenized polynomial yielded the original polynomial. This is actually always the case and these two operations satisfy some more useful properties.

Proposition 4.3.3 (Rules for Homogenization and Dehomogenization, [34], Proposition 4.3.2)**.** *Let $f, g \in R$ and let $F, G \in S$. Then the following hold:*

(a) $\phi(f^h) = f$,

(b) $(fg)^h = (f)^h (g)^h$,

(c) $\phi(FG) = \phi(F)\phi(G)$ *and* $\phi(F + G) = \phi(F) + \phi(G)$,

(d) *Suppose $F \in S \setminus \{0\}$ homogeneous. Let $s = \max\{i \geq 0 \mid t^i$ divides $F\}$. Then $t^s \phi(F)^h = F$.*

Proof. (a) This follows directly from the definition.

(b) Let $\deg(f) = d_1, \deg(g) = d_2$, so $\deg(fg) = d_1 + d_2$. Then

$$(fg)^h = t^{d_1+d_2} fg\left(\frac{x_1}{t}, \ldots, \frac{x_n}{t}\right) = t^{d_1} f\left(\frac{x_1}{t}, \ldots, \frac{x_n}{t}\right)^{d_2} g\left(\frac{x_1}{t}, \ldots, \frac{x_n}{t}\right) = f^h g^h.$$

(c) This follows directly from the fact that dehomogenization ϕ is a ring homomorphism.

(d) Let $F = t^s F'$ s.t. F' is homogeneous and not divisible by t. Suppose $\deg(F') = d$. Then

$$f = F(x_1, \ldots, x_n, 1) = F'(x_1, \ldots, x_n, 1)$$

and f has total degree d. Thus,

$$f^h = t^d f\left(\frac{x_1}{t}, \ldots, \frac{x_n}{t}\right) = t^d F'\left(1, \frac{x_1}{t}, \ldots, \frac{x_n}{t}\right) = F'$$

since F' is homogeneous of degree d. Therefore, we have $F = t^s F' = t^s f^h = t^s \phi(F)^h$. □

The concept of homogenization and dehomogenization can also be defined for ideals.

Definition 4.3.4. Let $I \subseteq R, J \subseteq S$ be ideals.

(a) $I^h = \langle f^h \mid f \in I \rangle \subseteq S$ is called the *homogenization of I.*

(b) $J^{deh} = \phi(J) = \{\phi(F) \mid F \in J\} \subseteq R$ is called the *dehomogenization of J.*

Clearly, J^{deh} is an ideal as it is the image of the ideal J under the surjective dehomogenizing homomorphism ϕ.

Proposition 4.3.5 ([34], Proposition 4.3.5)**.** *Let $I \subseteq R$ be an ideal and let $J \subseteq S$ be a homogeneous ideal. Then the following hold:*

(a) $\phi(I^h) = I$.

(b) *If $F \in S$ homogeneous, then $F \in I^h \Leftrightarrow \phi(F) \in I \Leftrightarrow F = t^s f^h$ for some $f \in I$, $s \in \mathbb{N}$.*

(c) *If $F \in S$ homogeneous, then $\phi(F) \in \phi(J) \Leftrightarrow t^s F \in J$ for some $s \geq 0$.*

(d) $J \subseteq \phi(J)^h = (J : t^\infty)$.

Proof. (a) ($\supseteq$) This follows from Proposition 4.3.3 (a).

($\subseteq$) Let $f \in \phi(I^h)$. Then, $f = \phi(\sum_{i=1}^r G_i g_i^h)$ for some $G_1, \ldots, G_r \in S$ and $g_1, \ldots, g_r \in I$. Since ϕ is a homomorphism, the result follows by Proposition 4.3.3 (c).

(b) Let $F \in S$ homogeneous. Then, by (a) we have $\phi(F) \in \phi(I^h) = I$. Let $F \in S$ s.t. $\phi(F) \in I$, then Proposition 4.3.3 (d) implies that $F = t^s f^h$ for $f = \phi(F)$ and some $s \in \mathbb{N}$. For $F = t^s f^h$ we have $F \in I^h$.

(c) ($\Leftarrow$) This follows, since $t^s F \in J$ implies $\phi(F) = \phi(t^s F) \in \phi(J)$.

($\Rightarrow$) Let $F \in S$ homogeneous s.t. $\phi(F) \in \phi(J)$. $\phi(J)$ being the image of J, there exists $G \in J$ s.t. $\phi(G) = \phi(F)$. Since J is homogeneous, the homogeneous components of G also lie in J. Multiplying each component with an appropriate power of t, we may assume that G is homogeneous. Then Proposition 4.3.3 (d) yields $s_1, s_2 \in \mathbb{N}$ s.t. $F = t^{s_1}\phi(F)^h = t^{s_1}\phi(G)^h$ and $G = t^{s_2}\phi(G)^h$. Thus, $t^s F \in \langle G \rangle \subseteq J$ for $s = \max\{0, s_2 - s_1\}$.

(d) The fact that $J \subseteq \phi(J)^h$ follows from Proposition 4.3.3 (d). Conversely, the inclusion $\phi(J)^h \subseteq (J : t^\infty)$ follows from (c).
Let $F \in (J : t^\infty)$. Then there exists $r \geq 0$ s.t. $t^r F \in J$. Therefore, we have $\phi(F) \in \phi(J)$. Applying Proposition 4.3.3 (d), we get $s \in \mathbb{N}$ s.t. $F = t^s \phi(F)^h \in \phi(J)^h$. □

4.4 Zariski Topology

In Proposition 4.1.6 it was shown that unions and intersections of affine varieties behave well, i.e. the intersection of a collection of affine varieties as well as the union of a finite collection of affine varieties are affine varieties. Also, the empty set and the whole space are affine varieties. Therefore, affine varieties in $\mathbb{A}^n$ satisfy the same properties as closed sets of a topology on $\mathbb{A}^n$.

Definition 4.4.1. The *Zariski Topology* on $\mathbb{A}^n$ is defined by taking the open subsets to be the complement of affine varieties. Let T be a subset of $\mathbb{A}^n$.

(a) T is called *Zariski closed* if $\exists I \subseteq R$ s.t. $T = \mathcal{V}(I)$.

(b) T is called *Zariski open* if $\exists I \subseteq R$ s.t. $T = \mathbb{A}^n \setminus \mathcal{V}(I)$.

(c) The *Zariski closure* of T, denoted, $\overline{T}$ is the smallest affine variety containing T.

Proposition 4.4.2 ([29], Proposition 1.2)**.** *Let $T \subseteq \mathbb{A}^n$. Then $\overline{T} = \mathcal{V}(\mathcal{I}(T))$*

Proof. Set $X = \mathcal{V}(\mathcal{I}(T))$. Then $\mathcal{I}(X) = \mathcal{I}(\mathcal{V}(\mathcal{I}(T))) = \mathcal{I}(T)$. If Y is a variety with $T \subseteq Y \subseteq X$, then $\mathcal{I}(X) \subseteq \mathcal{I}(Y) \subseteq \mathcal{I}(T) = \mathcal{I}(X)$, so $\mathcal{I}(Y) = \mathcal{I}(X)$. But then $Y = X$, since otherwise $\mathcal{I}(X) \subsetneq \mathcal{I}(Y)$, as both X and Y are varieties. □

Proposition 4.4.3 ([34], Proposition 5.5.21)**.** *Let k be an infinite field.*

(a) *Let $I \subseteq R$ be a nonzero ideal. Then $U = \mathbb{A}^n \setminus \mathcal{V}(I)$ has infinitely many elements.*

(b) *Let U_1, U_2 be two nonempty Zariski open subsets of $\mathbb{A}^n$. Then $U_1 \cap U_2$ is nonempty.*

Proof. (a) Let $f \in I \setminus \{0\}$. Since $\mathcal{V}(I) \subseteq \mathcal{V}(f)$, we can just show it for $f \in R$ and $U = k^n \setminus \mathcal{V}(f)$. This is done by induction on the number of variables n. If $n = 1$, then f has at most $\deg(f)$ roots. Thus, there are infinitely many points in $k \setminus \mathcal{V}(f)$.
Let $n > 1$ and suppose the result holds for $n - 1$. Write $f = f_0 + f_1 x_n + \cdots + f_i x_n^i$, for $i \geq 0$ and $f_0, \ldots, f_i \in k[x_1, \ldots, x_{n-1}]$, with $f_i \neq 0$. Then by inductive hypothesis, there exists $(a_1, \ldots, a_{n-1}) \in k^{n-1}$ s.t. $f_i(a_1, \ldots, a_{n-1}) \neq 0$. Thus, $f(a_1, \ldots, a_{n-1}, x_n) \in k[x_n]$ is a nonzero polynomial. Applying the base case $n = 1$ yields infinitely many $a_n \in k$ s.t. $f(a_1, \ldots, a_n) \neq 0$.

(b) Let $U_1 = k^n \setminus V_1, U_2 = k^n \setminus V_2$ and let I_1, I_2 be ideals in R s.t. $V_1 = \mathcal{V}(I_1)$ and $V_2 = \mathcal{V}(I_2)$. Then $V_1 \cup V_2 = \mathcal{V}(I_1 I_2)$. Thus, $U_1 \cap U_2 = k^n \setminus (V_1 \cup V_2) = k^n \setminus \mathcal{V}(I_1 I_2)$ and the result follows from (a) and Proposition 4.1.6. □

Corollary 4.4.4 ([34], Lemma 6.3.20)**.** *Let k be an infinite field. Given $p_1, \ldots, p_s \in k^{n+1}$, there exists a linear polynomial $l \in S_1$ s.t. $l(p_i) \neq 0$ for $i = 1, \ldots, s$.*

Proof. Let $p_i = (c_{i0}, \ldots, c_{in})$ with $c_{ij} \in k$ for $i = 1, \ldots, s$ and consider a linear polynomial $l = a_0 x_0 + \cdots + a_n x_n \in S_1$. l vanishes at p_i if and only if $(a_0, \ldots, a_n)$ is a root of $c_{i0} x_0 + \cdots + c_{in} x_n$. Therefore, we want to find $(a_0, \ldots, a_n) \in k^{n+1}$ that is not a root of $f = \prod_{i=1}^{s} (c_{i0} x_0 + \cdots + c_{in} x_n)$. But by Proposition 4.4.3, such a point and therefore such a linear polynomial l exists. □

The same concepts of Zariski topology can be applied to the projective space.

Definition 4.4.5. The *Zariski Topology* on $\mathbb{P}^n$ is defined by taking the open subsets to be the complement of projective varieties. The rest of the terminology is according to the affine case.

Further topology-theoretic details will not be used in this thesis, but the terminology of the Zariski topology leads to the notion of *genericity* and *generic sets* since many properties hold almost everywhere.

Definition 4.4.6. A property $\mathcal{P}$ of elements holds *generically* or *for a generic element* if there exists a nonempty Zariski open subset U s.t. $\mathcal{P}$ holds for all elements of U. A subset Y of a variety X is called *generic* if it contains a Zariski open subset.

Example 4.4.7. A generic quadratic polynomial $ax^2 + bx + c \in \mathbb{C}[x]$ does not vanish when $x = 0$, since it only vanishes when $c = 0$, i.e. on $\mathcal{V}(c)$.
Also, a generic quadratic polynomial $ax^2 + bx + c \in \mathbb{C}[x]$ has 2 roots, as this is only not true on $\mathcal{V}(b^2 - 4ac)$.
The polynomial $x^2 - 2x + 1$ is generic in the first sense but not in the second. So there is some ambiguity, but in later chapters, the concept of genericity will become useful.

4.5 Dimension of Varieties

We have seen many properties of varieties and how they can be described by finitely many polynomials. An important invariant to describe a variety is the dimension. To discuss dimension we have to introduce some new concepts. To do so, we follow [15, Chapter 9].

Definition 4.5.1. A *coordinate subspace* of k^n is a vector subspace of k^n defined by setting some subset of the variables $x_1, \ldots, x_n$ equal to zero.

It is easy to see that coordinate subspaces are irreducible varieties, since ideals of the form $\langle x_{i_1}, \ldots, x_{i_k} \rangle$ are prime.

Proposition 4.5.2 ([15], Proposition 1, Chapter 9.1)**.** *Let I be a monomial ideal of R. Then $\mathcal{V}(I)$ is a finite union of coordinate subspaces of k^n.*

Proof. By Corollary 2.5.21, every monomial ideal has a primary decomposition into monomial ideals of the form $\mathfrak{q}_i = (x_{i_1}^{a_1}, \ldots, x_{i_k}^{a_k})$. Thus, $\mathcal{V}(I) = \mathcal{V}(\bigcap_i \mathfrak{q}_i) = \bigcup_i \mathcal{V}(\mathfrak{q}_i) = \bigcup_i \mathcal{V}(x_{i_1}, \ldots, x_{i_k})$, which is a finite union of coordinate subspaces. □

Choosing the minimal primary decomposition of $\sqrt{I}$ in the proof of Proposition 4.5.2, yields that there is a unique decomposition of $\mathcal{V}(I) = V_1 \cup \cdots \cup V_s$ into coordinate subspaces, where $V_i \nsubseteq V_j$ for $i \neq j$.

Definition 4.5.3. Let V be a variety, which is the finite union of linear subspaces of k^n. Then the *dimension* of V, denoted $\dim(V)$, is defined to be the largest dimension of the linear subspaces.

To study the dimension of $\mathcal{V}(I)$, it is useful to look at the monomials that are not in I.

Definition 4.5.4. For a monomial ideal I of R, let the *complement of the exponents* of monomials in I be the set of exponents of monomials not in I, denoted

$$C(I) = \{\alpha \in \mathbb{Z}_{\geq 0}^n : x^\alpha \notin I\}.$$

Let e_i be the standard basis vectors of $\mathbb{Z}_{\geq 0}^n$. Then the *coordinate subspace of* $\mathbb{Z}_{\geq 0}^n$ determined by $e_{i_1}, \ldots, e_{i_r}$, where $i_1 < \cdots < i_r$ is defined to be the set

$$[e_{i_1}, \ldots, e_{i_r}] = \{a_i e_{i_1} + \cdots + a_r e_{i_r} : a_j \in \mathbb{Z}_{\geq 0} \text{ for } j = 1, \ldots, r\}.$$

$[e_{i_1}, \ldots, e_{i_r}]$ is also said to be an r-dimensional coordinate subspace.
A *translate* of a coordinate subspace $[e_{i_1}, \ldots, e_{i_r}]$ defined to be a subset of $\mathbb{Z}_{\geq 0}^n$ of the form

$$\alpha + [e_{i_1}, \ldots, e_{i_r}] = \{\alpha + \beta : \beta \in [e_{i_1}, \ldots, e_{i_r}]\},$$

where $\alpha = \sum_{i \notin \{i_1, \ldots, i_r\}} a_i e_i, a_i \geq 0$.

Proposition 4.5.5 ([15], Proposition 2, Chapter 9.2)**.** *Let I be a proper monomial ideal of R.*

(a) $\mathcal{V}(x_i : i \notin \{i_1, \ldots, i_r\}) \subseteq \mathcal{V}(I)$ *if and only if* $[e_{i_1}, \ldots, e_{i_r}] \subseteq C(I)$.

(b) $\dim(\mathcal{V}(I))$ *is the dimension of the largest coordinate subspace in* $C(I)$.

Proof. (a) ($\Rightarrow$) Note that $V = \mathcal{V}(x_i : i \notin \{i_1, \ldots, i_r\})$ contains $p \in k^n$, whose i_j-th component is 1 for $j = 1, \ldots, r$ and 0 otherwise. For $\alpha \in [e_{i_1}, \ldots, e_{i_r}]$, write $x^\alpha = x_{i_1}^{\alpha_{i_1}} \cdots x_{i_r}^{\alpha_{i_r}}$. Then, $x^\alpha = 1$ at p s.t. $x^\alpha \notin I$ since $p \in V \subseteq \mathcal{V}(I)$ by hypothesis. Therefore, $\alpha \in C(I)$.

($\Leftarrow$) Let $[e_{i_1}, \ldots, e_{i_r}] \subseteq C(I)$. Each monomial in I contains one or more variables not contained in $x_{i_1}, \ldots, x_{i_r}$. Therefore, all monomials in I vanish on all points $(a_1, \ldots, a_n) \in k^n$ with $a_i = 0$ for $i \notin \{i_1, \ldots, i_r\}$. Thus, each monomial in I vanishes on $\mathcal{V}(x_i : i \notin \{i_1, \ldots, i_r\})$.

(b) Clearly, $\mathcal{V}(x_i : i \notin \{i_1, \ldots, i_r\})$ is of dimension r. Then (a) implies that the dimension of the coordinate subspaces of k^n in $\mathcal{V}(I)$ and the coordinate subspaces of $\mathbb{Z}^n_{\geq 0}$ in $C(I)$, respectively, coincide. □

Example 4.5.6. Let $I = \langle x^2, xy \rangle \subseteq k[x, y]$. Then

$$C(I) = \{(0,0), (1,0), (0,k) : k \in \mathbb{Z}_{>0}\} = [e_2] \cup \{(1,0)\}.$$

On the other hand we have

$$\mathcal{V}(I) = \mathcal{V}(\langle x \rangle \cap \langle x^2, y \rangle) = \mathcal{V}(x) \cup \mathcal{V}(x, y),$$

which implies that $\dim(\mathcal{V}(I)) = 1$. We also see that

$$\begin{aligned} \mathcal{V}(x,y) \subseteq \mathcal{V}(I) \text{ and } [0] \subseteq C(I), \\ \mathcal{V}(x) \subseteq \mathcal{V}(I) \text{ and } [e_2] \subseteq C(I), \\ \mathcal{V}(y) \nsubseteq \mathcal{V}(I) \text{ and } [e_1] \nsubseteq C(I). \end{aligned}$$

Also, the largest coordinate subspace in $C(I)$ is $[e_2]$ and has dimension 1. This coincides with Proposition 4.5.5.

In the previous example, it was possible to express $C(I)$ as a union of translates of coordinate subspaces. We now show that this always possible for monomial ideals.

Theorem 4.5.7 ([15], Theorem 3, Chapter 9.2)**.** *Let I be a proper monomial ideal of R. Then $C(I)$ is a finite union of translates of coordinate subspaces.*

Proof. If $I = \{0\}$ the result is trivial, so assume that $I = \langle x^\alpha : \alpha \in A \rangle$ for some $A \subseteq \mathbb{Z}^n_{\geq 0}$ s.t. $x^\alpha \in I$ if and only if $\alpha \in A$.

The result is proven by induction on the number of variables n. If $n = 1$ then $I = \langle x^\beta \rangle$ for $\beta = \min\{\alpha \in A\}$. Thus $C(I) = \{0, 1, \ldots, \beta - 1\}$, which is a finite set of translates of $[0]$.

Now, let $n > 1$ and assume that the result holds for $n - 1$ variables. Let $t \geq 0$ and let $A_t = \{\alpha' : (\alpha', t) \in A\} \subseteq \mathbb{Z}^{n-1}_{\geq 0}$. Let $C_t = \{\alpha' \in \mathbb{Z}^{n-1}_{\geq 0} : (\alpha', t) \notin A\}$. Since $A_t \subseteq A_{t+1}$ for all t, there exists s s.t. $A_t = A_s$ for all $t \geq s$. For any integer t, let

$$C_t \times \{t\} = \{(\alpha', t) \in \mathbb{Z}^n_{\geq 0} : \alpha' \in C_t \subseteq \mathbb{Z}^{n-1}_{\geq 0}\}.$$

We claim that

$$C(I) = (C_s \times \mathbb{Z}_{\geq 0}) \cup \bigcup_{t=0}^{s-1} (C_t \times \{t\}).$$

($\supseteq$) Note that $C_t \times \{t\} \subseteq C(I)$ by definition. Also since $A_t = A_s$ for all $t \geq s$, we have $C_s \times \{t\} \subseteq C(I)$. If $t < s$ then $(\alpha', t) \notin A$ whenever $(\alpha', s) \notin A$. Thus, $C_s \times \{t\} \subseteq C(I)$ for $t < s$.

($\subseteq$) When $\alpha = (a_1, \ldots, a_n) \in C(I)$ then $\alpha \in C_{a_n} \times \{a_n\}$.
If $a_n < s$ the conclusion follows.
If $a_n \geq s$ then $A_{a_n} = A_s$. Thus $\alpha \in C_s \times \mathbb{Z}_{\geq 0}$.

$C_0, \ldots, C_s$ are finite unions of translates of coordinate subspaces of $\mathbb{Z}^{n-1}_{\geq 0}$ by induction hypothesis. With our claim, it follows that $C(I)$ satisfies the desired property. □

Lemma 4.5.8 ([15], Lemma 4, Chapter 9.2)**.** *The number of monomials of degree $\leq s$ in $k[x_1, \ldots, x_n]$ is $\binom{n+s}{s}$.*

Proof. The proof is done by induction on s. The case $s = 1$ is clear, as $\binom{n+1}{1} = n + 1$ and the monomials of degree ≤ 1 are $1, x_1, \ldots, x_n$.
Assume that $s > 1$ and that the result holds for $s-1$. Then the monomials of degree $\leq s$ are the monomials of degree $< s$ and those of degree s, which is the set $\{x_1^{\alpha_1} \cdots x_n^{\alpha_n} : \alpha_1 + \cdots + \alpha_n = s\}$. But this is the same as choosing s times from the set $\{x_1, \ldots, x_n\}$ without considering the order. Thus, it has cardinality $\binom{n+s-1}{s}$. By inductive hypothesis, we have that the number of monomial of degree $< s$ is $\binom{n+s-1}{s-1}$. The result now follows from

$$\binom{n+s-1}{s-1} + \binom{n+s-1}{s} = \binom{n+s}{s}. \qquad \square$$

Lemma 4.5.9 ([15], Lemma 5, Chapter 9.2)**.** *Let $\alpha + [e_{i_1}, \ldots, e_{i_r}]$ be a translate of $[e_{i_1}, \ldots, e_{i_r}]$.*

(a) *Let $s > |\alpha|$. Then the number of points in $\alpha + [e_{i_1}, \ldots, e_{i_r}]$ of degree $\leq s$ is $\binom{r+s-|\alpha|}{s-|\alpha|}$.*

(b) *Let $s > |\alpha|$. The number of points of degree $\leq s$ is a polynomial in s of degree r, where the highest degree term has coefficient $\frac{1}{r!}$.*

Proof. (a) Suppose $s > |\alpha|$. Each point $\beta \in \alpha + [e_{i_1}, \ldots, e_{i_r}]$ of degree $\leq s$ can be expressed as $\beta = \alpha + \gamma$, with $\gamma \in [e_{i_1}, \ldots, e_{i_r}]$ and $|\gamma| < s - |\alpha|$. Then Lemma 4.5.8 yields the number of possible γ.

(b) We have

$$\binom{r+s-|\alpha|}{s-|\alpha|} = \binom{r+s-|\alpha|}{r} = \frac{(r+s-|\alpha|)!}{r!(s-|\alpha|)!} = \frac{1}{r!}(s+r-|\alpha|)(s+r-|\alpha|-1)\cdots(s-|\alpha|+1),$$

which is clearly a polynomial in s of degree r and $1/r!$ as coefficient of s^r. $\square$

Lemma 4.5.10. *The intersection of two translates A and B of different coordinates subspaces is a translate of a lower dimensional coordinate subspace, where* $\dim(A \cap B) < \max\{\dim(A), \dim(B)\}$.

Proof. Let $A = \alpha + [e_{i_1}, \ldots, e_{i_m}]$, where $\alpha = \sum_{i \notin \{i_1, \ldots, i_m\}} a_i e_i$ and $B = \beta + [e_{j_1}, \ldots, e_{j_r}]$, where $\beta = \sum_{i \notin \{j_1, \ldots, j_r\}} b_i e_i$.
First, we claim that if $A \neq B$ and $A \cap B \neq \emptyset$, then $[e_{i_1}, \ldots, e_{i_m}] \neq [e_{j_1}, \ldots, e_{j_r}]$ and $A \cap B$ is a translate of $[e_{i_1}, \ldots, e_{i_m}] \cap [e_{j_1}, \ldots, e_{j_r}]$.
Suppose by contradiction that $[e_{i_1}, \ldots, e_{i_m}] = [e_{j_1}, \ldots, e_{j_r}]$. Then, one has $\alpha \neq \beta$, since $A \neq B$. Thus, A and B are distinct orthogonal translates of the same coordinate subspace. But this implies that $A \cap B = \emptyset$, which is a contradiction.

Suppose now that $[e_{i_1}, \ldots, e_{i_m}] \cap [e_{j_1}, \ldots, e_{j_r}] = \{0\}$. Let $x \in A \cap B$. Then one has

$$x = \alpha + \sum_{i \in \{i_1, \ldots, i_m\}} c_i e_i = \beta + \sum_{j \in \{j_1, \ldots, j_r\}} d_j e_j,$$

where α, β can be written as $\alpha = \gamma + \sum_{j \in \{j_1, \ldots, j_r\}} d_j e_j$ and $\beta = \gamma + \sum_{i \in \{i_1, \ldots, i_m\}} c_i e_i$ for some $\gamma = \sum_{l \notin \{i_1, \ldots, i_m\} \cup \{j_1, \ldots, j_r\}} f_l e_l$. This implies that the d_j, c_i are unique. Therefore $A \cap B$ contains only one point, i.e. a translate of $\{0\}$.

Without loss of generality we may assume that $[e_{i_1}, \ldots, e_{i_m}] \cap [e_{j_1}, \ldots, e_{j_r}] = [e_{i_1}, \ldots, e_{i_s}] = [e_{j_1}, \ldots, e_{j_s}]$, for some $s \leq \min(m, r)$. Let $x \in A \cap B$ and again we can express x as

$$x = \alpha + \sum_{i \in \{i_1, \ldots, i_m\}} c_i e_i = \beta + \sum_{j \in \{j_1, \ldots, j_r\}} d_j e_j.$$

As before, this implies that $\alpha = \gamma + \sum_{j\in\{j_{s+1},\dots,j_r\}} d_j e_j$ and $\beta = \gamma + \sum_{i\in\{i_{s+1},\dots,i_m\}} c_i e_i$ for some $\gamma = \sum_{l\notin\{i_1,\dots,i_m\}\cup\{j_1,\dots,j_r\}} f_l e_l$. However, this time, we can choose the coefficients of $[e_{i_1},\dots,e_{i_s}]$ freely. Therefore, $A\cap B$ is a translate of $[e_{i_1},\dots,e_{i_s}]$.
This clearly shows that

$$\dim(A\cap B) \leq \min(m,r).$$

If $m\neq r$, then $\dim(A\cap B)\leq \min(m,r) < \max(m,r)$. Otherwise, $s<m=\max(m,r)$ as equality would imply that $[e_{i_1},\dots,e_{i_m}] = [e_{j_1},\dots,e_{r_s}]$, which we showed to be false. □

With these results established, it is now possible to describe the number of polynomials of degree $\leq s$ that do not lie in I with a single polynomial.

Theorem 4.5.11 ([15], Theorem 6, Chapter 9.2)**.** *Let I be a monomial ideal with $\dim(\mathcal{V}(I)) = d$. Then, for all s sufficiently large, the number of monomials not in I of total degree $\leq s$ is a polynomial in s of degree d .*

Proof. By Theorem 4.5.7, we can express $C(I)$ as

$$C(I) = A_1\cup\cdots\cup A_t,$$

where the A_j's denote translates of coordinate subspaces in $\mathbb{Z}^n_{\geq 0}$ s.t. $A_i\neq A_j$ for $i\neq j$.
Since I is an ideal, a coordinate subspace $[e_{i_1},\dots,e_{i_r}]$ lies in $C(I)$ if and only if some translate of $[e_{i_1},\dots,e_{i_r}]$ lies in $C(I)$. Since $\dim(\mathcal{V}(I)) = d$, we have $\dim(A_i)\leq d$ for all i, where equality occurs at least once.
It follows that

$$(C(I))_{\leq s} = (A_1)_{\leq s}\cup\cdots\cup(A_t)_{\leq s},$$

where $|(C(I))_{\leq s}|$ denotes the number of elements in $(C(I))_{\leq s}$. Applying the *inclusion-exclusion principle* A.2.1 for counting elements in a union of sets, to $(C(I))_{\leq s}$, we get

$$|(C(I))_{\leq s}| = \sum_i |(A_i)_{\leq s}| - \sum_{i<j} |(A_i)_{\leq s}\cap(A_j)_{\leq s}| + \sum_{i<j<k} |(A_i)_{\leq s}\cap(A_j)_{\leq s}\cap(A_k)_{\leq s}| - \cdots.$$

Lemma 4.5.9 implies that for s sufficiently large, the number of points in $(A_i)_{\leq s}$ is a polynomial of degree $m_i = \dim(A_i)\leq d$ in s and s^{m_i} has coefficient $1/m_i!$.
The first sum above is a polynomial in s of degree d, when s is sufficiently large. The degree is d as at least one A_i has dimension d and the coefficients of the terms of highest degree are all positive, which implies that they cannot cancel each other.
Furthermore, as the intersection of translates of coordinate subspaces of dimension m and r respectively is either empty or of dimension $< \min(m,r)$, applying Lemma 4.5.10 to the nonzero terms $|(A_i)_{\leq s}\cap(A_j)_{\leq s}|$ in the second sum implies that the $A_i\cap A_j$ is the translate of a coordinate subspace of dimension $< d$. Thus, $|(A_i)_{\leq s}\cap(A_j)_{\leq s}|$ is a polynomial in s of degree $< d$. Summing these terms up for all $i<j$, it follows that it is a polynomial of degree $< d$. Treating the remaining sums in a similar way, it follows that $|(C(I))_{\leq s}|$ is a polynomial of the desired form for s sufficiently large. □

It makes sense to look at these notions also in the projective case, since monomial ideals are homogeneous. Therefore, a monomial ideal I of R yields a projective variety $\mathcal{V}_p(I)\subseteq\mathbb{P}^{n-1}$. In k^n, let $\mathcal{V}(x_{i_1},\dots,x_{i_r})$ be a coordinate subspace of dimension $n-r$ contained in $\mathcal{V}(I)$. Without loss of generality we may assume that $i_1=1$ and $i_r=r$ and let $a\in\mathcal{V}_p(x_1,\dots,x_r)$. The point a can be written as $a=(0:\cdots:0:a_{r+1}:\cdots:a_n)$, where $a_{r+1},\dots,a_n$ are not all zero. Since $\mathcal{V}(x_1,\dots,x_r)\subseteq\mathcal{V}(I)$ contains $(0,\dots,0,a_{r+1},\dots,a_n)$, the monomial generators of I vanish at a. Thus, $a\in\mathcal{V}_p(I)$. This shows that $\mathcal{V}_p(x_1,\dots,x_r)\subseteq\mathcal{V}_p(I)$.
There is also a bijection between $\mathcal{V}_p(x_1,\dots,x_r)$ and $\mathbb{P}^{n-r-1}$ by the map

$$(0:\cdots:0:a_{r+1}:\cdots:a_n)\mapsto(a_{r+1}:\cdots:a_n).$$

Thus, $\mathcal{V}_p(x_1, \ldots, x_r)$ looks like a copy of $\mathbb{P}^{n-r-1}$ inside $\mathbb{P}^{n-1}$, which can be seen as a *projective linear subspace* of dimension $n - r - 1$.

Lemma 4.5.12. *Let I be a monomial ideal of R. Then $\mathcal{V}_p(I)$ is a finite union of projective linear subspaces of dimension one less than the affine counterpart.*

Proof. $\mathcal{V}(I) = V_1 \cup \cdots \cup V_s$ for some coordinate subspaces V_i. By the comments above we have that $(V_1)_p \cup \cdots \cup (V_s)_p \subseteq \mathcal{V}_p(I)$. Conversely, let $a \in \mathcal{V}_p(I)$. Then all representations of a are in $\mathcal{V}(I)$, so in one of the V_i's. Thus, $\mathcal{V}_p(I) \subseteq (V_1)_p \cup \cdots \cup (V_s)_p$, where each $(V_i)_p$ is a projective linear subspace of dimension one less than the affine counterpart. □

Similar to the affine case, this allows us to define the dimension of a finite union of projective linear subspaces as the maximal dimension of these subspaces. Then, Theorem 4.5.11 shows that the dimension of the projective variety $\mathcal{V}_p(I)$ of a monomial ideal I is one less than the degree of the polynomial in s, which counts the number of monomials not in I of degree $\leq s$.

In the homogeneous case, the monomials of degree s form a vector space. Thus, it makes more sense to look at monomials with degree equal to s.

Corollary 4.5.13 ([15], Proposition 8, Chapter 9.2)**.** *Let I be a monomial ideal of R and let $\mathcal{V}_p(I) \subseteq \mathbb{P}^{n-1}$. If $\dim(\mathcal{V}_p(I)) = d - 1$, then for s sufficiently large, the number of monomials not in I of degree s is a polynomial of degree $d - 1$.*

Proof. Since $\dim^p(\mathcal{V}_p(I)) = d - 1$, viewing it as an affine variety yields $\dim(\mathcal{V}(I)) = d$ by Lemma 4.5.12. Then, the number of monomials not in I of degree $\leq s$ is a polynomial $p(s)$ of degree d with a positive coefficient of the highest degree term by Theorem 4.5.11. Removing the monomials of degree $\leq s$, the number of monomials not in I of degree s equals

$$p(s) - p(s-1)$$

for s sufficiently large.
Write the polynomial p as $p(s) = a_d s^d + a_{d-1} s^{d-1} + \cdots + a_0$, with $a_d > 0$. Then we have

$$\begin{aligned} p(s-1) &= a_d(s-1)^d + a_{d-1}(s-1)^{d-1} + \cdots + a_0 \\ &= a_d(s^d - ds^{d-1} + \binom{d}{2} s^{d-2} + \cdots) \\ &\quad + a_{d-1}(s^{d-1} - (d-1)s^{d-2} + \binom{d-1}{2} s^{d-3} + \cdots) \\ &\quad + \cdots + a_0 \\ &= a_d s^d + (a_{d-1} - da_d)s^{d-1} + \text{ terms of lower degree.} \end{aligned}$$

This implies that,

$$\begin{aligned} p(s) - p(s-1) &= (a_{d-1} + da_d - a_{d-1})s^{d-1} + \text{ terms of lower degree} \\ &= da_d s^{d-1} + \text{ terms of lower degree,} \end{aligned}$$

which is a polynomial of degree $d - 1$, where s^{d-1} has a positive coefficient. □

Chapter 5

Gröbner Bases

This chapter contains essential theory about Gröbner bases introduced by B. Buchberger [9]. These bases have many theoretical and practical purposes and will help us to solve polynomial systems algorithmically. We define monomial orders and present a division algorithm for multivariate polynomials. Then, we introduce Gröbner bases and with Buchberger's algorithm, a way to obtain them is given. Next, we explain the relationship between monomial orders and homogenization and how it affects Gröbner bases. After discussing elimination theory and how to solve polynomial systems by the means of Gröbner bases, we present a different Gröbner basis algorithm based on Gaussian elimination. The chapter closes with a generalization of Gröbner bases to the setting of modules.

The main references for this chapter are [15], [16],[30], and [33]. The terminology mostly comes from the from [15]. Unless mentioned otherwise, we use the standard graded polynomial rings $R = k[x_1, \dots, x_n]$ and $S = k[x_1, \dots, x_n, t]$.

5.1 Monomial Orders

For a univariate polynomial $f \in k[x]$, there is an obvious way to order the monomials in $\text{Supp}(f)$, by ordering them w.r.t degree, i.e. $1 < x < x^2 < \cdots$. In the multivariate case, this is not always possible, as several distinct monomials in $\text{Supp}(f)$ can have the same degree. In many algorithms, however, it is important to establish an unambiguous way to represent polynomials. To overcome this obstacle, it is necessary to introduce a new way to order monomials in multiple variables. Recall that a total order on a set $\mathcal{S}$ is a relation σ s.t. for all $x, y, z \in \mathcal{S}$ the following hold:

(a) $x \leq_\sigma x$ (reflexivity).

(b) If $x \leq_\sigma y$ and $y \leq_\sigma x$ then $x = y$ (antisymmetry).

(c) If $x \leq_\sigma y$ and $y \leq_\sigma z$ then $x \leq_\sigma z$ (transitivity).

(d) Either $x \leq_\sigma y$ or $y \leq_\sigma x$ for all $x, y \in \mathcal{S}$ (connexity).

Definition 5.1.1. A monomial order σ on R is a total order on $\text{Mon}(R)$ s.t. the following hold:

(a) If $u, v, w \in \text{Mon}(R)$ and $u \geq_\sigma v$, then $uw \geq_\sigma vw$ (respects multiplication).

(b) Every nonempty subset of $\text{Mon}(R)$ has a smallest element w.r.t σ (well-order).

Notice that σ corresponds to an order on the exponents $\alpha \in \mathbb{Z}^n_{\geq 0}$, where $\alpha >_\sigma \beta$ if and only if $x^\alpha >_\sigma x^\beta$. If the monomial order is clear from the context, we may omit the subscript σ.
The well-order property of a monomial order can be formulated in different ways.

Proposition 5.1.2 ([15], Lemma 2, Chapter 2.2)**.** *Let σ be a total order on* $\text{Mon}(R)$ *satisfying (a) of Definition 5.1.1. Then the following are equivalent:*

(a) *σ is a well-order, i.e. every nonempty subset has a smallest element w.r.t σ.*

(b) *Every strictly decreasing sequence* $u_1 >_\sigma u_2 >_\sigma \cdots$ *in* $\mathrm{Mon}(R)$ *eventually terminates.*

(c) $u \geq 1$ *for all* $u \in \mathrm{Mon}(R) \setminus \{1\}$.

Proof. (b ⇒ a) Suppose there exists a nonempty set $\mathcal{S} \subseteq \mathrm{Mon}(R)$ with no smallest element. Pick $u_1 \in S$, then there must exist u_2 s.t. $u_1 >_\sigma u_2$. Repeating this procedure, we find a decreasing sequence that does not terminate.

(a ⇒ b) Suppose $u_1 >_\sigma u_2 >_\sigma \cdots$ is a decreasing sequence that does not terminate. Then the set of all u_i clearly has no smallest element.

(a ⇒ c) Let u_0 be the smallest element of $\mathrm{Mon}(R)$ and assume $1 >_\sigma u_0$. Then by (b) of Definition 5.1.1 we multiply both sides by u_0 to obtain $u_0 >_\sigma u_0^2$, a contradiction.

(c ⇒ a) Let $\mathcal{S} \subseteq \mathrm{Mon}(R)$ be nonempty. Since $I = \langle u : u \in \mathcal{S} \rangle$ is a monomial ideal, by Dickson's lemma, we may assume that $I = \langle u_1, \ldots, u_s \rangle$. By reordering, we may assume that $u_s >_\sigma \ldots >_\sigma u_1$. Now, take $w \in \mathcal{S}$. Then $w \in I$ is divisible by some u_i by Proposition 2.5.13. Thus, $w = u_i v$ for some $v \in \mathrm{Mon}(R)$. This implies that

$$w = u_i v \geq_\sigma u_1 \cdot 1 = u_i \geq_\sigma u_1.$$

Thus, $\mathcal{S}$ contains a minimal element. □

Two very common monomial orders are the following.

Definition 5.1.3.

(a) *Lexicographic Order (lex)* Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, then $x^\alpha >_{lex} x^\beta$ if the leftmost nonzero entry of $\alpha - \beta \in \mathbb{Z}^n_{\geq 0}$ is positive.

(b) *Degree Reverse Lexicographic Order (DRL)* Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, then $x^\alpha >_{DRL} x^\beta$ if $|\alpha| > |\beta|$ or if $|\alpha| = |\beta|$ and the rightmost nonzero entry of $\alpha - \beta \in \mathbb{Z}^n_{\geq 0}$ is negative.

A monomial order σ is called *degree compatible* if $|\alpha| > |\beta|$ implies $x^\alpha >_\sigma x^\beta$.

Note that in $k[x_1, \ldots, x_n]$, there are $n!$ possible ways to order the individual variables. Unless mentioned otherwise, we always assume that the variables are ordered by $x_1 > x_2 > \cdots > x_n$. Given a monomial order, it is now possible to establish a hierarchy among the monomials in $\mathrm{Supp}(f)$ and represent f in a unique way.

Example 5.1.4. It is easy to see that DRL is degree compatible, while lex is not. Consider $f = x^3 - 2x^2y^2 - 2x^2y + xy \in k[x, y]$ with $\mathrm{Supp}(f) = \{x^3, x^2y^2, x^2y, xy\}$. Ordering this set w.r.t the lex- resp. DRL-order we get

$$x^3 >_{lex} x^2y^2 >_{lex} x^2y >_{lex} xy$$
$$x^2y^2 >_{DRL} x^3 >_{DRL} x^2y >_{DRL} xy.$$

Definition 5.1.5. Let $f = \sum_\alpha c_\alpha x^\alpha \in k[x_1, \ldots, x_n]$ and fix a monomial order σ.

(a) The *multidegree* of f is $\mathrm{multideg}_\sigma(f) = \max_{>_\sigma}\{\alpha \in \mathbb{Z}^n_{\geq 0} \mid c_\alpha \neq 0\}$.

(b) The *leading coefficient* of f is $\mathrm{lc}_\sigma(f) = c_{\mathrm{multideg}(f)} \in k$.

(c) The *initial* or *leading monomial* of f is $\mathrm{in}_\sigma(f) = x^{\mathrm{multideg}(f)} \in \mathrm{Mon}(R)$.

(d) The *leading term* of f is $\mathrm{lt}_\sigma(f) = \mathrm{lc}_\sigma(f)\,\mathrm{in}_\sigma(f) = c_{\mathrm{multideg}(f)} x^{\mathrm{multideg}(f)} \in R$.

Example 5.1.6. As before let $f = x^3 - 2x^2y^2 - 2x^2y + xy \in k[x, y]$. Then:

(a) $\text{multideg}_{DRL}(f) = (2, 2), \quad \text{multideg}_{lex}(f) = (3, 0)$,

(b) $\text{lc}_{DRL}(f) = -2, \quad \text{lc}_{lex}(f) = 1$,

(c) $\text{in}_{DRL}(f) = x^2y^2, \quad \text{in}_{lex}(f) = x^3$,

(d) $\text{lt}_{DRL}(f) = -2x^2y^2, \quad \text{lt}_{lex}(f) = x^3$.

As we are working over fields, we can always multiply a polynomial f by a nonzero constant to achieve that $\text{lc}(f) = 1$. Thus, $\text{in}(f)$ and $\text{lt}(f)$ can usually be used interchangeably.

Lemma 5.1.7 ([30], Lemma 2.1.4)**.** *Let $f, g \in R$ be nonzero polynomials and let $u \in \text{Mon}(R)$. Then the following hold:*

(a) $\text{in}(uf) = u\,\text{in}(f)$,

(b) $\text{in}(fg) = \text{in}(f)\,\text{in}(g)$,

(c) *if $f + g \neq 0$, then $\text{in}(f + g) \leq \max\{\text{in}(f), \text{in}(g)\}$, where equality holds if additionally $\text{in}(f) \neq \text{in}(g)$.*

Proof. (a) Let $v \in \text{Supp}(f)$ s.t. $v < \text{in}(f)$. Since $v < \text{in}(f)$, we have $uv < u\,\text{in}(f)$. Thus, $u\,\text{in}(f) = \text{in}(uf)$.

(b) Note that $\text{Supp}(fg) = \{uv : u \in \text{Supp}(f), v \in \text{Supp}(g)\}$. Then for all $uv \in \text{Supp}(fg)$ we have $uv \leq u\,\text{in}(g) \leq \text{in}(f)\,\text{in}(g)$. Thus, $\text{in}(fg) = \text{in}(f)\,\text{in}(g)$.

(c) When adding $f + g$ we have $\text{Supp}(f + g) \subseteq \{u : u \in \text{Supp}(f) \cup \text{Supp}(g)\}$. Therefore, $\text{in}(f + g) \leq \max\{\text{in}(f), \text{in}(g)\}$. When $\text{in}(f) \neq \text{in}(g)$, then $\max(\text{in}(f), \text{in}(g)) \in \text{Supp}(f + g)$. Thus, equality holds. □

Definition 5.1.8. Let $f \in R$ and let $G \subseteq R$ be an ordered set of polynomials. Fix a monomial order.

(a) f is *reducible by G* if there is a monomial $m \in \text{Supp}(f)$ and $g \in G$ s.t. $\text{in}(g) \mid m$.

(b) f is *irreducible by G* if for all monomials $m \in \text{Supp}(f)$ there is no $g \in G$ s.t. $\text{in}(g) \mid m$.

We can now introduce an algorithm to divide a multivariate polynomial by a set of multivariate polynomials. The idea is the same as for the division by polynomials in one variable.

Theorem 5.1.9 (Division Algorithm, [15], Theorem 3, Chapter 2.3)**.** *Let $F = \{f_1, \ldots, f_s\} \subseteq R$ be an ordered set of polynomials and fix a monomial order. Then every $f \in R$ can be expressed as*

$$f = q_1 f_1 + \cdots + q_s f_s + r,$$

where $q_i, r \in R$ and either $r = 0$ or r is irreducible by F. Furthermore, if $q_i f_i \neq 0$, then $\text{in}(f) \geq \text{in}(q_i f_i)$ for all $i = 1, \ldots, s$.

Proof. The proof is given by stating an explicit algorithm.

Algorithm 1: Multivariate division algorithm

Input : $f_1, \dots, f_s, f$
Output: $q_1, \dots, q_s, r$
$q_1 = \cdots = q_s = r = 0$
$p = f$.
while $p \neq 0$ **do**
  $i = 1$
  $divisionoccured = false$
  while $i \leq s$ *and* $divisionoccured = false$ **do**
    if $\mathrm{lt}(f_i) | \mathrm{lt}(p)$ **then**
      $q_i = q_i + \mathrm{lt}(p)/\mathrm{lt}(f_i)$
      $p = p - (\mathrm{lt}(p)/\mathrm{lt}(f_i))f_i$
      $divisionoccured = true$
    else
      $i = i + 1$
    end
  end
  if $divisionoccured = false$ **then**
    $r = r + \mathrm{lt}(p)$
    $p = p - \mathrm{lt}(p)$
  end
end
return $q_1, \dots, q_s, r$

(Termination) As long as $p \neq 0$, $\mathrm{in}(p)$ gets strictly smaller each time the algorithm changes either r or the q_i. By Proposition 5.1.2, this can only happen finitely many times and p eventually must be zero.

(Correctness) First we have to check that f is always of the form

$$f = q_1 f_1 + \cdots + q_s f_1 + p + r.$$

It clearly holds at the start. Suppose it holds at an intermediate step of the algorithm, where possible changes occur. If a q_i gets changed then also p changes and we get

$$(q_i + \frac{\mathrm{lt}(p)}{\mathrm{lt}(f_i)})f_i + (p - \frac{\mathrm{lt}(p)}{\mathrm{lt}(f_i)}f_i) = q_i f_i + p.$$

Thus, f is still of the desired form. If none of the q_i changes, then r and p change and we get

$$(p - \mathrm{lt}(p)) + (r + \mathrm{lt}(p)) = p + r,$$

which shows that f has the desired form at every step of the algorithm. When the algorithm terminates we additionally have $p = 0$.

It is easy to see that either $r = 0$ or r is irreducible by F, since every time a change of r occurs, the algorithm adds a term to r that is not divisible by any of the $\mathrm{lt}(f_i)$.

Finally, we check that $\mathrm{in}(f) \geq \mathrm{in}(q_i f_i)$ if $q_i f_i \neq 0$. This is clearly true at the initial stage. Suppose it holds at an intermediate stage, where $q_i f_i \neq 0$. If the q_i get changed we have

$$\mathrm{in}((q_i + \frac{\mathrm{lt}(p)}{\mathrm{lt}(f_i)})f_i) \leq \max\{\mathrm{in}(q_i f_i), \mathrm{in}(p)\} \leq \mathrm{in}(f)$$

by Lemma 5.1.7. If $q_i f_i = 0$ at the intermediate step, the same conclusion clearly holds. □

Definition 5.1.10. The irreducible polynomial r from the division algorithm is called a *remainder of f on division by F* denoted $r = \overline{f}^F$.

Example 5.1.11. Continuing the previous example, let $f = -2x^2y^2 + x^3 - 2x^2y + xy \in k[x, y]$ and fix the DRL-order. Consider the polynomials $f_1 = x^2 - 1, f_2 = xy + x \in k[x, y]$ and let $F_1 = \{f_1, f_2\}, F_2 = \{f_2, f_1\}$ be ordered sets polynomials. Applying Algorithm 1 yields

$$\begin{aligned} f &= -2x^2y^2 + x^3 - 2x^2y + xy \\ &= -2y^2 f_1 + x^3 - 2x^2y + xy - 2y^2 \\ &= (-2y^2 + x)f_1 - 2x^2y + xy - 2y^2 + x \\ &= (-2y^2 + x - 2y)f_1 + xy - 2y^2 - 2y + x \\ &= (-2y^2 + x - 2y)f_1 + f_2 - (2y^2 + 2y) \end{aligned}$$

and

$$\begin{aligned} f &= -2x^2y^2 + x^3 - 2x^2y + xy \\ &= (-2xy)f_2 + x^3 + xy \\ &= (-2xy)f_2 + xf_1 + xy + x \\ &= (-2xy + 1)f_2 + xf_1, \end{aligned}$$

which shows that the remainder depends on the ordering of the polynomials and is not unique. Also the number of steps required may vary depending on the order.

Remark 5.1.12. If $r = 0$, then $f = q_1f_1 + \cdots + q_sf_s$, which implies that $f \in \langle f_1, \ldots, f_s\rangle$. Therefore, $r = 0$ is a sufficient condition to show ideal membership. However, since r is not uniquely determined it may happen that $r \neq 0$ but $f \in \langle f_1, \ldots, f_s\rangle$ is still satisfied.

Definition 5.1.13. Let $G = \{g_1, \ldots, g_s\} \subseteq R$ and fix a monomial order. A polynomial f is said to *reduce to zero mod G* if f has a *standard representation*, i.e. $f = q_1g_1 + \cdots + q_sg_s, q_i \in R$ and $\mathrm{in}(f) \geq \mathrm{in}(q_ig_i)$, whenever $q_ig_i \neq 0$.

The concept of initial monomials motivates the concept of ideals generated by initial monomials.

Definition 5.1.14. Let $I \subseteq R$ be a nonzero ideal, fix a monomial σ order. The *initial ideal* of I w.r.t σ denoted $\mathrm{in}_\sigma(I)$, is the ideal generated by $\{\mathrm{in}_\sigma(f) : f \in I\, f \neq 0\}$.
If $T = \{t_1, \ldots, t_r\} \subseteq R$ is a finite set and not an ideal, we mean $\mathrm{in}_\sigma(T) = \{\mathrm{in}_\sigma(t_1), \ldots, \mathrm{in}_\sigma(t_r)\}$.

Example 5.1.15. Let $I = \langle f_1, f_2\rangle \subseteq k[x, y]$, where $f_1 = x^2 - 1, f_2 = xy + x$. We have $y + 1 = x(xy + y) - (y + 1)(x^2 + 1) \in I$. Thus

$$\langle \mathrm{in}_{DRL}(f_1), \mathrm{in}_{DRL}(f_2)\rangle = \langle x^2, xy\rangle \subsetneq \langle x^2, y\rangle \subseteq \mathrm{in}_{DRL}(I).$$

Initial ideals w.r.t the DRL-order have some nice properties, which will come in handy in later chapters.

Lemma 5.1.16 ([4], Lemma 2.2)**.** *Let I be a homogeneous ideal of R. Fix the DRL-order and choose $i \in \{1, \ldots, n\}$. Then:*

(a) $\mathrm{in}(\langle I, x_n, \ldots, x_i\rangle) = \langle \mathrm{in}(I), x_n, \ldots, x_i\rangle$.

(b) *Let $x_n, \ldots, x_{i+1} \in I$ and let $m \geq 0$. Then*

$$(I : x_i)_m = I_m \iff (\mathrm{in}(I) : x_i)_m = \mathrm{in}(I)_m.$$

(c) *Let* $x_n, \dots, x_{i+1} \in I$ *and let* $m \geq 0$. *Suppose that* $(I : x_i)_d = I_d$ *for all* $d \geq m$ *and that* $\operatorname{in}(I, x_i)$ *is generated by elements of degree* $\leq m$. *Then* $\operatorname{in}(I)$ *is generated by elements of degree* $\leq m$.

Proof. (a) ($\supseteq$) This is true for any monomial order, as all the generators of the RHS are contained in the LHS.

($\subseteq$) Suppose $f \in \langle I, x_n, \dots, x_i \rangle$ is homogeneous. If x_j divides $\operatorname{in}(f)$ for some $j \geq i$, then $\operatorname{in}(f) \in \langle \operatorname{in}(I), x_n, \dots, x_i \rangle$. If not, we can write $f = g + h_n x_n + \cdots + h_i x_i$ for some $g \in I$ and $h_n, \dots, h_i \in R$ s.t. $x_j \nmid g$ for all $j \geq i$. Then we have that $\operatorname{in}(f) = \operatorname{in}(g)$, which implies that $\operatorname{in}(g) \in \operatorname{in}(I)$.

(b) ($\Rightarrow$) Let $u \in \operatorname{Mon}_m(R)$. If $u \in (\operatorname{in}(I) : x_i)_m$, then $x_i u = \operatorname{in}(f)$ for some $f \in I_{m+1}$ homogeneous. If $x_j | u$ for some $j \in \{i+1, \dots, n\}$, then $u \in \operatorname{in}(I)_m$. If not, we can subtract multiples of $x_n, \dots, x_{i+1}$ to achieve that $f \in k[x_1, \dots, x_i]$. Then, since we work with the *DRL*-order and $x_i | \operatorname{in}(f)$, there exists $g \in R_m$ with $\operatorname{in}(g) = u$ s.t. $f = g x_i$. Our hypothesis implies that $g \in I_m$, thus $u \in \operatorname{in}(I)_m$.

($\Leftarrow$) We show this by an inductive argument. Let $x_i f \in I_{m+1}$ and assume that for each $g \in R_m$ with $\operatorname{in}(f) > \operatorname{in}(g)$ and $x_i g \in I_{m+1}$ one has $g \in I_m$. Since $x_i \operatorname{in}(f) = \operatorname{in}(x_i f) \in \operatorname{in}(I)_{m+1}$ then $\operatorname{in}(f) \in \operatorname{in}(I)_m$ by our assumption. Let $\operatorname{in}(f) = \operatorname{in}(g)$ for some $g \in I_m$. Then $x_i(f - g) \in I_{m+1}$ and $\operatorname{in}(f) > \operatorname{in}(f - g)$. So by inductive hypothesis, we conclude $f - g \in I_m$ and therefore $f \in I_m$.

(c) Let $G(\operatorname{in}(I))$ be the minimal set of monomial generators of $\operatorname{in}(I)$. Let $f \in I$ homogeneous with $\deg(f) > m$. If $x_j | \operatorname{in}(f)$ for some $j \in \{i+1, \dots, n\}$ then $\operatorname{in}(f) \notin G(\operatorname{in}(I))$, since $x_j \in I$. If not, we may again subtract multiples of $x_{i+1}, \dots, x_n$ to achieve that $f \in k[x_1, \dots, x_i]$. Suppose $x_i | \operatorname{in}(f)$. Then there is $g \in R$ homogeneous s.t. $f = x_i g$, since we are working with the *DRL*-order. Then for $d = \deg(f) - 1 \geq m$ we have $g \in (I : x_i)_d$. Thus, $g \in I_d$ by hypothesis. This implies again that $\operatorname{in}(f) \notin G(I)$.

If $x_j \nmid \operatorname{in}(f)$ for $j = i, \dots, n$, we may write $\operatorname{in}(f) = u \operatorname{in}(g)$ for some polynomial $g \in \langle I, x_i \rangle$ with $1 \neq u \in \operatorname{Mon}(R)$, since $\operatorname{in}(\langle I, x_i \rangle)$ is generated by elements of degree $\leq m$ but $\deg(f) > m$. Now we can write $g = g_1 + x_i g_2$ for some $g_1 \in I$. Since g is homogeneous we have $\operatorname{in}(g) >_{DRL} \operatorname{in}(x_i g_2)$, so $\operatorname{in}(g) = \operatorname{in}(g_1)$. Thus, $\operatorname{in}(f) = u \operatorname{in}(g_1) \notin G(\operatorname{in}(I))$. □

Corollary 5.1.17 ([4], Lemma 2.3)**.** *Let* I *be a homogeneous ideal of* R *and fix the DRL-order. Let* $r \geq 0$ *and* $m \geq 0$. *Then the following are equivalent:*

(a) $(\langle I, x_n, \dots, x_{i+1} \rangle : x_i)_m = \langle I, x_n, \dots, x_{i+1} \rangle$ *for* $i = n, \dots, n - r + 1$ *and* $\langle I, x_n, \dots, x_{n-r+1} \rangle = R_m$,

(b) $(\langle \operatorname{in}(I), x_n, \dots, x_{i+1} \rangle : x_i)_m = \langle \operatorname{in}(I), x_n, \dots, x_{i+1} \rangle_m$ *for* $i = n, \dots, n - r + 1$ *and* $\langle \operatorname{in}(I), x_n, \dots, x_{n-r+1} \rangle = R_m$.

Proof. The equivalences follow immediately from (a) and (b) of the previous lemma. □

5.2 Gröbner Bases

As we have seen in Example 5.1.15, for an ideal $I = \langle f_1, \dots, f_r \rangle$ it is not always the case that $\operatorname{in}(I) = \langle \operatorname{in}(f_1), \dots, \operatorname{in}(f_r) \rangle$. This motivates the following definition.

Definition 5.2.1. Let $I \subseteq R$ be an ideal and fix a monomial order. A finite subset of polynomials $\{g_1, \dots, g_s\} \subseteq I$ s.t. $\langle \operatorname{in}(g_1), \dots, \operatorname{in}(g_s) \rangle = \operatorname{in}(I)$ is called a *Gröbner Basis* of I.

While not every generating system is a Gröbner basis, the converse is true.

Proposition 5.2.2 ([30], Theorem 2.1.8)**.** *Fix a monomial order σ on R.*

(a) *Every ideal $I \subseteq R$ has a finite σ-Gröbner basis.*

(b) *A Gröbner basis of an ideal I is a basis of I.*

Proof. (a) $\operatorname{in}(I)$ is a monomial ideal. Therefore, by Dickson's Lemma, there exist monomials $m_1, \dots, m_s$ s.t. $\operatorname{in}(I) = \langle m_1, \dots, m_s \rangle$. Since $m_i \in \operatorname{in}(I)$, there exist $g_i \in I$ s.t. $\operatorname{in}(g_i) = m_i$. Therefore, $\operatorname{in}(I) = \langle \operatorname{in}(g_1), \dots, \operatorname{in}(g_s) \rangle$.

(b) Let $G = \{g_1, \dots, g_s\}$ be a Gröbner basis of I. Let $f \in I$ be nonzero. Clearly $\operatorname{in}(f) \in \operatorname{in}(I)$, which implies that $\operatorname{in}(g_{i_0}) | \operatorname{in}(f)$ for some $i_0 \in \{1, \dots, s\}$. Thus, $\operatorname{in}(f) = w_0 \operatorname{in}(g_{i_0})$ for some $w_0 \in \operatorname{Mon}(R)$. Let

$$h_0 = f - \operatorname{lc}(g_{i_0})^{-1} \operatorname{lc}(f) w_0 g_{i_0}.$$

Since $\operatorname{in}(w_0 g_{i_0}) = w_0 \operatorname{in}(g_{i_0})$, we get that $\operatorname{in}(f) > \operatorname{in}(h_0)$.
If $h_0 = 0$ then $f \in \langle g_1, \dots, g_s \rangle$. Otherwise, similarly to f, consider

$$h_1 = h_0 - \operatorname{lc}(g_{i_1})^{-1} \operatorname{lc}(h_0) w_1 g_{i_1}.$$

Then $h_1 \in I$ and $\operatorname{in}(h_0) > \operatorname{in}(h_1)$.
If $h_1 = 0$ then $f \in \langle g_1, \dots, g_s \rangle$. Otherwise, proceed in the same way. This process terminates, since otherwise we would get a contradiction to the well-order property of the monomial order, since $\operatorname{in}(h_0) > \operatorname{in}(h_1) > \cdots$ would be an infinite decreasing sequence. Thus, there exists $N \geq 0$ s.t. $h_{N+1} = 0$ and therefore

$$f = \sum_{j=0}^{N} \operatorname{lc}(g_{i_j})^{-1} \operatorname{lc}(h_{j-1}) w_j g_{i_j} \in \langle g_1, \dots, g_s \rangle. \qquad \square$$

By the definition of a Gröbner basis, it is easy to see that a generating set $G \subseteq R$ for an ideal $I \subseteq R$ is a Gröbner Basis if and only if for every $p \in I \setminus \{0\}$ there is $g \in G \setminus \{0\}$ s.t. $\operatorname{in}(g) \mid \operatorname{in}(p)$.

Another interesting property is that when using the division algorithm w.r.t a Gröbner basis, the remainder is unique, which resolves the ambiguity in Example 5.1.11.

Proposition 5.2.3 ([30], Lemma 2.2.3)**.** *Let $G = \{g_1, \dots, g_s\}$ be a Gröbner Basis for a nonzero ideal $I \subseteq R$. Let $f \in R$. Then there exists a unique $r \in R$ s.t.*

(a) *r is irreducible by G,*

(b) *there exists $g \in I$ s.t. $f = g + r$.*

In particular, r is the remainder on division of f by G regardless of how G is ordered.

Proof. (a) Existence of r follows immediately from the division algorithm 5.1.9.

(b) Existence follows again immediately from the division algorithm by setting

$$g = q_1 g_1 + \cdots + q_s g_s.$$

Suppose that $f = g + r = g' + r'$. Then $r - r' = g - g' \in I$. So, if $r \neq r'$, then we have $\operatorname{in}(r - r') \in \langle \operatorname{in}(g_1), \dots, \operatorname{in}(g_s) \rangle$. Hence $\operatorname{in}(r - r')$ is divisible by $\operatorname{in}(g_i)$ for some i. But since no term of r nor r' is divisible by any $\operatorname{in}(g_i)$, this yields a contradiction. Thus, $r = r'$ is the unique remainder. $\square$

Corollary 5.2.4 ([30], Corollary 2.2.4)**.** *Let $I \subseteq R$ be a nonzero ideal and let G be a Gröbner basis for I. Let $f \in R$, then $f \in I$ if and only if $\overline{f}^G = 0$.*

Proof. ($\Leftarrow$) If the remainder of f is zero w.r.t $G = \{g_1, \dots, g_s\}$, then $f \in I$.

($\Rightarrow$) Let $0 \neq f \in I$, and suppose $r = \overline{f}^G \neq 0$. We know that $\mathrm{in}(r)$ is not divisible by any of the terms $\mathrm{in}(g_1), \dots, \mathrm{in}(g_s)$. But on the other hand, $f \in I$ implies that $r \in I$, i.e we have $\mathrm{in}(r) \in \mathrm{in}(I) = \langle \mathrm{in}(g_1), \dots, \mathrm{in}(g_s) \rangle$, which is a contradiction since none of the terms $\mathrm{in}(g_i)$ divide $\mathrm{in}(r)$. Thus, $r = 0$. □

A first application of Gröbner bases occurs w.r.t the k-space R/I.

Proposition 5.2.5 ([30], Proposition 2.2.5)**.** *Let I be a nonzero ideal of R and fix a monomial order.*

(a) *The set of monomials not in* $\mathrm{in}(I)$ *form a k-basis of R/I.*

(b) *If I is graded, then* $\dim_k(I_j) = \dim_k(\mathrm{in}(I)_j)$ *for all j.*

Proof. (a) Let G be a Gröbner basis of I. Let $f \in R$ and $r = \overline{f}^G$. Then $\mathrm{Supp}(r) \cap \mathrm{in}(I) = \emptyset$ and $\bar{f} = \bar{r} \in R/I$. Thus, R/I is generated by the monomials not in $\mathrm{in}(I)$.

Suppose there are monomials $u_1 > u_2 > \cdots > u_r \in R \setminus \mathrm{in}(I)$ s.t. they are linearly dependent in R/I. Let $f = \sum_{i=1}^r a_i u_i \in I$ for some $a_i \in k$ with not all a_i's zero. Then $\mathrm{in}(f) \in I$, which is a contradiction.

(b) The monomials of degree j in $\mathrm{Mon}(R) \setminus \mathrm{in}(I)$ form a k-basis of $(R/I)_j$ by (a). But by Corollary 2.5.12 they also form a k-basis of $(R/\mathrm{in}(I))_j$. Therefore, we see that for each j we have $\dim_k(R_j) - \dim_k(I_j) = \dim_k(R_j) - \dim_k(\mathrm{in}(I)_j)$. Thus, we have $\dim_k(I_j) = \dim_k(\mathrm{in}(I)_j)$. □

An ideal can have many different Gröbner bases. But when we require some additional properties, there is a certain type of Gröbner basis that turns out to be unique for every ideal.

Definition 5.2.6. A Gröbner basis $G = \{g_1, \dots, g_s\}$ for an ideal $I \subseteq R$ is called *reduced* if the following conditions are satisfied:

(a) $\mathrm{lc}(g_i) = 1$ for all $i = 1, \dots, s$,

(b) if $i \neq j$, then none of the monomials in $\mathrm{Supp}(g_j)$ is divisible by $\mathrm{in}(g_i)$.

Proposition 5.2.7 ([30], Theorem 2.2.7)**.** *Let I be an ideal of R and fix a monomial order. Then there exists a unique reduced Gröbner basis of I.*

Proof. (Existence) Let I be a nonzero ideal of R and let $G(\mathrm{in}(I)) = \{u_1, \dots, u_s\}$ be the minimal system of monomial generators of $\mathrm{in}(I)$. By choosing a polynomial $g_i \in I$ s.t. $\mathrm{in}(g_i) = u_i$ for all i, we get that $G = \{g_1, \dots, g_s\}$ is a Gröbner basis of I.
Condition (a) can be satisfied by simply dividing each g_i by $\mathrm{lc}(g_i)$.
Next, let $h_i = \overline{g_i}^{G \setminus \{g_i\}}$. Then we have $\mathrm{in}(h_i) = \mathrm{in}(g_i)$, since $\mathrm{in}(g_i)$ is not divisible by $\mathrm{in}(g_j)$ for all $i \neq j$. So $G = \{h_1, \dots, h_s\}$ is still a Gröbner basis. Also, each h_i is irreducible by $G \setminus \{h_i\}$ by construction. Thus, G is reduced.

(Uniqueness) Suppose $\{g_1, \dots, g_s\}$ and $\{h_1, \dots, h_t\}$ are reduced Gröbner bases of I. Then $\{\mathrm{in}(g_1), \dots, \mathrm{in}(g_s)\} = \{\mathrm{in}(h_1), \dots, \mathrm{in}(h_t)\}$ as these are minimal sets of monomial generators. Hence $s = t$ and by arranging $g_1, \dots, g_s$ appropriately, we see that $\mathrm{in}(h_i) = \mathrm{in}(g_i)$ for each i. Now, if $g_i \neq h_i$, then $0 \neq h_i - g_i \in I$ with $\mathrm{in}(g_i) > \mathrm{in}(h_i - g_i) \in \mathrm{in}(I)$. That is, $\mathrm{in}(g_i) \nmid \mathrm{in}(h_i - g_i)$. Also, $\mathrm{in}(h_i - g_i) \in \mathrm{Supp}(g_i) \cup \mathrm{Supp}(h_i)$. Therefore, no $\mathrm{in}(g_j)$ divides $\mathrm{in}(h_i - g_i)$ for any $j \neq i$. Thus, $\mathrm{in}(h_i - g_i) \notin \mathrm{in}(I)$, which is a contradiction. □

Reduced Gröbner bases therefore only depend on the ideal I and the chosen monomial order. Clearly, ideals are equal if and only if they have the same reduced Gröbner basis. Since reduced Gröbner bases are unique, we can define the following notion, which is important in Chapter 8.

Definition 5.2.8. Let I be an ideal of R and fix a monomial order σ. By $\text{max. GB. deg}_\sigma(I)$, we denote the maximum degree of a polynomial appearing in the reduced σ-Gröbner basis of I. If $I = \langle F \rangle$, for a set $F \subseteq R$, we may write $\text{max. GB. deg}_\sigma(F)$ instead of $\text{max. GB. deg}_\sigma(I)$.

5.3 Buchberger's Algorithm

While we know that every ideal has a Gröbner basis, we still need a way to obtain them. To do so, we present Buchberger's algorithm to construct Gröbner bases.
First, we need to introduce some notations.

Definition 5.3.1. Let $f, g \in R$ be nonzero polynomials and fix a monomial order on R. The *S-polynomial* of f and g is defined to be

$$S(f,g) = \frac{x^\gamma}{\text{lt}(f)} f - \frac{x^\gamma}{\text{lt}(g)} g,$$

where $x^\gamma = \text{lcm}\{\text{in}(f), \text{in}(g)\}$.

Example 5.3.2. With reference to the previous example, let $f_1 = x^2 - 1, f_2 = xy + x$ and fix the DRL-order. Then $\text{lcm}\{\text{in}(f_1), \text{in}(f_2)\} = \text{lcm}\{x^2, xy\} = x^2y$. The S-polynomial is given by

$$S(f_1, f_2) = \frac{x^2y}{x^2}(x^2 - 1) - \frac{x^2y}{xy}(xy + x) = (x^2y - y) - (x^2y + x^2) = -x^2 - y.$$

Observe that S-polynomials cancel initial monomials, i.e. $\text{lcm}\{\text{in}(f), \text{in}(g)\} > \text{in}(S(f,g))$ for a fixed monomial order.
The next result shows that all cancellations among monomials are generated by a certain type of syzygies.

Lemma 5.3.3 ([27], Proposition 18, Chapter 3.11)**.** *Let $\{m_1, \ldots, m_t\} \subseteq \text{Mon}(R)$ be a set of monomials. Then $\text{Syz}(m_1, \ldots, m_t)$ is generated by syzygies of the form*

$$s_{i,j} = \frac{\text{lcm}\{m_i, m_j\}}{m_i} e_i - \frac{\text{lcm}\{m_i, m_j\}}{m_j} e_j,$$

where $1 \leq i < j \leq t$.

Proof. Let $s = (s_1, \ldots, s_t) \in \text{Syz}(m_1, \ldots, m_t)$, i.e. $s_1m_1 + \cdots + s_tm_t = 0$. Each sum of terms in the same multidegree must be zero, so we may assume that $s_i = c_in_i$ with $c_i \in k, n_i \in \text{Mon}(R)$ s.t. $\text{multideg}(n_im_i) = \text{multideg}(n_jm_j)$ for all i, j. This implies that $\sum_{i=1}^t c_i = 0$. Such a syzygy is called *homogeneous* and we have just shown that each syzygy can be written as a sum of homogeneous syzygies.

Let $s = (c_1n_1, \ldots, c_tn_t) \in \text{Syz}(m_1, \ldots, m_t)$ homogeneous. Define

$$b_i = \sum_{j=1}^{i} c_j \left(n_ie_i - n_{i+1}e_{i+1}\right).$$

Since $\operatorname{lcm}\{m_i, m_{i+1}\}$ divides $n_i m_i = n_{i+1} m_{i+1}$, we see that b_i is a multiple of $s_{i,i+1}$. Now, consider

$$\begin{aligned}
\sum_{i=1}^{s-1} b_i &= \sum_{i=1}^{s-1} \left(\left(\sum_{j=1}^{i} c_j \right) n_i e_i - \left(\sum_{j=1}^{i} c_j \right) n_{i+1} e_{i+1} \right) \\
&= \sum_{i=1}^{s-1} \sum_{j=1}^{i} c_j n_i e_i - \sum_{i=2}^{s} \sum_{j=1}^{i-1} c_j n_i e_i \\
&= c_1 n_1 e_1 + \sum_{i=2}^{s-1} c_i n_i e_i - \left(\sum_{j=1}^{s-1} c_j \right) n_s e_s \\
&= \sum_{i=1}^{s} c_i n_i e_i = s.
\end{aligned}$$

Thus, s is a linear combination of b_i, which implies that $\operatorname{Syz}(m_1, \ldots, m_t)$ is generated by the syzygies $s_{i,j}$. □

We can now give a criterion to check if a set of polynomials is a Gröbner basis.

Theorem 5.3.4 (Buchberger's Criterion, [30], Theorem 2.3.2)**.** *Let $I \subseteq R$ be a nonzero ideal and fix a monomial order. A basis $G = \{g_1, \ldots, g_s\}$ for I is a Gröbner basis if and only if $\overline{S(g_i, g_j)}^{G} = 0$ for all $i \neq j$.*

Proof. ($\Rightarrow$) Since for each $i \neq j$, it is true that $S(g_i, g_j) \in I$, it follows by Corollary 5.2.4 that $\overline{S(g_i, g_j)}^{G} = 0$.

($\Leftarrow$) Let $f \in \langle g_1, \ldots, g_t \rangle$, where we may assume that $\operatorname{lc}(g_i) = 1$ for all $i = 1, \ldots, t$. We can write $f = q_1 g_1 + \cdots + q_t g_t$ with $m = \max_i\{\operatorname{in}(q_i g_i)\} \geq \operatorname{in}(f)$. If $\operatorname{in}(f) = m$, then we have $\operatorname{in}(f) \in \langle \operatorname{in}(g_1), \ldots, \operatorname{in}(g_t) \rangle$ and we are done.

So assume that $m > \operatorname{in}(f)$ and let $A = \{i : m = \operatorname{in}(q_i g_i)\}$. Set $Q = (q_1, \ldots, q_t)$. If $m > \operatorname{in}(f)$, we must have a cancellation in $\sum_{i=1}^{t} q_i g_i$ among the maximal initial terms. Let $S_Q = (s_1, \ldots, s_t)$, where $s_i = \operatorname{in}(q_i)$ for $i \in A$ and $s_i = 0$ otherwise. Then $S_Q \in \operatorname{Syz}(\operatorname{in}(g_1), \ldots, \operatorname{in}(g_t))$. So by Lemma 5.3.3, we can write

$$S_Q = \sum_{i,j} n_{i,j} s_{i,j} \text{ for some } n_{i,j} \in \operatorname{Mon}(R) \text{ and } s_{i,j} = \frac{\operatorname{lcm}\{\operatorname{in}(g_i), \operatorname{in}(g_j)\}}{\operatorname{in}(g_i)} e_i - \frac{\operatorname{lcm}\{\operatorname{in}(g_i), \operatorname{in}(g_j)\}}{\operatorname{in}(g_j)} e_j.$$

By the definition of S-polynomials, we see that $s_1 g_1 + \cdots + s_t g_t = \sum_{i,j} n_{i,j} S(g_i, g_j)$. Since $\overline{S(g_i, g_j)}^{G} = 0$, $S(g_i, g_j)$ has a standard representation $S(g_i, g_j) = \sum_{k=1}^{t} h_k^{(i,j)} g_k$. Therefore, $s_{i,j} - (h_1^{(i,j)}, \ldots, h_t^{(i,j)}) \in \operatorname{Syz}(g_1, \ldots, g_t)$, which implies that

$$Z = \sum_{i,j} n_{i,j} (s_{i,j} - (h_1^{(i,j)}, \ldots, h_t^{(i,j)})) \in \operatorname{Syz}(g_1, \ldots, g_t).$$

Consider $Q' = Q - Z = (q_1', \ldots, q_t')$. Since Z is a syzygy, Q' yields a representation $f = \sum_{i=1}^{t} q_i' g_i$, where $\max_i\{\operatorname{in}(q_i' g_i)\} < \max_i\{\operatorname{in}(q_i g_i)\}$ by construction. Iteratively applying the same procedure, yields after finitely many steps $(q_1', \ldots, q_t')$ s.t. $f = \sum_{i=1}^{t} q_i' g_i$ and $\max_i\{\operatorname{in}(q_i' g_i)\} = \operatorname{in}(f)$, which implies that $\operatorname{in}(f) \in \langle \operatorname{in}(g_1), \ldots, \operatorname{in}(g_t) \rangle$. □

Corollary 5.3.5 ([15], Theorem 3, Chapter 2.9)**.** *A basis $G = \{g_1, \ldots, g_s\}$ for I is a Gröbner basis if and only if $S(g_i, g_j)$ has a standard representation w.r.t G.*

Proof. Examining the proof of Buchberger's criterion, we see that we only used the fact that $S(g_j, g_k)$ has a standard representation. So the result follows immediately. □

This criterion leads to an algorithm constructing Gröbner bases by extending the original generating set to a Gröbner basis by adding more polynomials from the ideal $I = \langle f_1, \dots, f_s \rangle$ to the set $\{f_1, \dots, f_s\}$.

Theorem 5.3.6 (Buchberger's Algorithm, [15] Theorem 2, Chapter 2.7)**.** *Let $I \subseteq R$ be a nonzero ideal. Then it is possible to compute a Gröbner basis for I in finitely many steps by the following algorithm.*

Algorithm 2: Buchberger's Algorithm

Input : $F = \{f_1, \dots, f_s\}$
Output: *A Gröbner Basis* $G = \{g_1, \dots, g_m\}$ *with* $F \subseteq G$.
$G = F$.
$P = \{(p, q) \mid p \neq q \in G\}$.
while $P \neq \emptyset$ **do**
  for $(p, q),\ p \neq q$ *in* P **do**
    $f = \overline{S(p,q)}^{G}$
    $P = P \setminus (p, q)$
    if $f \neq 0$ **then**
      $P = P \cup \{(f, g) \mid g \in G\}$
      $G = G \cup \{f\}$
    end
  end
end
return G

Proof. (Correctness) Clearly, G is still a generating set of I at each step of the algorithm. Suppose the algorithm terminates and let G be the output. By construction, we have that $S(p, q)$ reduces to zero w.r.t G for all $p \neq q \in G$, which by Corollary 5.3.5 implies that G is indeed a Gröbner basis for I.

(Termination) Suppose by contradiction that the algorithm does not terminate after a finite number of steps. This means that the if-condition is satisfied infinitely many times and each time we add a polynomial f to G. Call G_i the set after adding an irreducible polynomial f to G for the i-th time. This gives a strictly increasing chain of sets $G_1 \subsetneq G_2 \subsetneq \cdots$. Since $\mathrm{in}(f) \in \mathrm{in}(G_{i+1}) \setminus \mathrm{in}(G_i)$, we have a proper containment $\mathrm{in}(G_i) \subsetneq \mathrm{in}(G_{i+1})$. Since by assumption the chain does not terminate, we get a strictly increasing chain of ideals $\mathrm{in}(G_1) \subsetneq \mathrm{in}(G_2) \subsetneq \cdots$, which does not terminate. But this is a contradiction to the fact that R is Noetherian. Thus, after finitely many steps we have $G_{i+k} = G_i$ for all $k \geq 0$, i.e. no polynomials get added to G anymore. From this step onwards, the set P in the algorithm gets smaller at each step and the algorithm terminates after finitely many steps. □

Example 5.3.7. Consider the two polynomials $f_1 = x^2 - 1$, $f_2 = xy + x \in k[x, y]$ and fix the DRL-order. We apply Buchberger's algorithm to find a DRL-Gröbner basis of the ideal $\langle f_1, f_2 \rangle = \langle x^2 - 1, xy + x \rangle$.

(1) $G = \{x^2 - 1, xy + x\}, P = \{(x^2 - 1, xy + x)\}$

- $S(x^2 - 1, xy + x) = -x^2 - y$
- $\overline{-x^2 - y}^{G} = -y - 1 \Rightarrow G = G \cup \{-y - 1\}$.

(2) $G = \{x^2 - 1, xy + x, -y - 1\}, P = \{(x^2 - 1, -y - 1), (xy + x, -y - 1\}$

- $S(x^2 - 1, -y - 1) = -x^2 - y$
- $\overline{-x^2 - y}^{G} = 0 \Rightarrow G$ remains the same.
- $S(xy + x, -y - 1) = 0 \Rightarrow G$ remains the same and $P = \emptyset$.

The algorithm returns the Gröbner basis $G = \{x^2-1, xy+x, -y-1\}$ of the ideal $\langle x^2-1, xy+x\rangle$.

Remark 5.3.8. Since this algorithm extends the given set until it is a Gröbner basis, it often constructs Gröbner bases too large for practical purposes. Also, the efficiency of the algorithm depends on the strategy by which the algorithm chooses the pairs (p, q) from the set P. Since we are interested in another class of Gröbner basis algorithms, we will not dive further into this.

Another useful property of Gröbner bases concerns graded ideals.

Proposition 5.3.9 ([27], Lemma 29, Chapter 8.3)**.** *An ideal I of R is graded if and only if the reduced Gröbner basis of I consists of homogeneous polynomials.*

Proof. ($\Leftarrow$) This follows directly since I is generated by homogeneous elements.

($\Rightarrow$) First, we show that dividing a homogeneous polynomial f by homogeneous polynomials $f_1, \ldots, f_s$, the division algorithm gives an expression

$$f = q_1 f_1 + \cdots + q_s f_s + r,$$

where q_i, r are homogeneous. We may assume that $\mathrm{lc}(f_i) = 1$.
Let $\deg(f) = d$. Let $p, r, q_1, \ldots, q_s$ be as in the division algorithm. We claim that p, r are always zero or homogeneous of degree d and that the q_i are either zero or homogeneous of degree $d - \deg(f_i)$.

This is clearly true at the start of the algorithm, when $q_1 = \cdots = q_a = r = 0$ and $p = f$.
Now, assume it holds at some intermediate stage. If $\mathrm{in}(f_i) | \mathrm{in}(p)$ for some i, then the algorithm adds $\mathrm{in}(p)/\mathrm{in}(f_i)$ to q_i. Since $\mathrm{in}(p)/\mathrm{in}(f_i)$ is a monomial of degree $d - \deg(f_i)$, the new q_i is of degree $d - \deg(f_i)$.
Subtracting $\mathrm{in}(p)/\mathrm{in}(f_i) f_i$ from p does not change the degree of p as $\mathrm{in}(p)/\mathrm{in}(f_i) f_i$ is homogeneous of degree $d = \deg(p)$. Also, r does not change in this case.

If $\mathrm{in}(f_i) \nmid \mathrm{in}(p)$ for all i, then the algorithm subtracts $\mathrm{in}(p)$ from p and adds it to r. Since both are homogeneous of degree d the same holds for the new values of r and p. The q_i do not change in this case. This proves the claim.

Next, we show that $S(f, g)$ is homogeneous if f, g are homogeneous. Let $m = \mathrm{lcm}(\mathrm{in}(f), \mathrm{in}(g))$. Then

$$S(f, g) = \frac{m}{\mathrm{in}(f)} f - \frac{m}{\mathrm{in}(g)} g,$$

where $\frac{m}{\mathrm{in}(f)} f$ is homogeneous of degree $\deg(m) - \deg(f) + \deg(f) = \deg(m)$. Similarly for $\frac{m}{\mathrm{in}(g)} g$. Therefore, $S(f, g)$ is either homogeneous of degree $\deg(m)$ or zero.

Now, Buchberger's algorithm starts with a set G of homogeneous polynomials and only adds polynomials to the intermediate set G' of the form $r = \overline{S(p, q)}^{G'}$. But by an inductive argument, G' only consists of homogeneous polynomials, so r is homogeneous and the new set still only contains homogeneous polynomials. Therefore, the output of the algorithm consists of homogeneous polynomials.

A reduced Gröbner basis can then be obtained by dividing basis elements by constants and removing terms. None of these operations change the fact that the basis elements are homogeneous. Therefore, the reduced Gröbner basis contains only homogeneous polynomials. □

5.4 Extending Monomial Orders and Homogeneous Gröbner Bases

In this section we present a way to extend monomial orders and the relationship between Gröbner bases and homogenization. This is based on [11, Section 3.2].
Recall the notion of dehomogenization, where $\phi : S \to S/(t-1) \cong R$ denotes the dehomogenization and f^h denotes the homogenization map w.r.t.the homogenization-variable t.
Let $I = \langle f_1, \ldots, f_s \rangle \subseteq R$ be an ideal. We recall, respectively define the following homogeneous ideals associated to I:

(a) $I^h = \langle \{ f^h \mid f \in I \} \rangle \subseteq S$,

(b) $\tilde{I} = \langle f_1^h, \ldots, f_s^h \rangle \subseteq S$.

Remark 5.4.1. The following properties are easy to see.

(a) I^h is a homogeneous ideal in S that contains $\tilde{I}$.

(b) $\phi(I^h) = \phi(\tilde{I}) = I$ for any ideal $I \subseteq R$.

We are interested in monomial orders on R and S that are related to each other in a particular way. The following notion of extending monomial orders follows [11, Section 3.2].

Definition 5.4.2. Let σ be a monomial order on R and τ be a monomial order on S. τ is said to be a *ϕ-extension* of σ, if $\phi(\mathrm{in}_\tau(f)) = \mathrm{in}_\sigma(\phi(f))$ for all $f \in S$ homogeneous.

Theorem 5.4.3 (Dehomogenizing Gröbner Bases, [11], Theorem 3.7)**.** *Fix a monomial order σ on R and let τ be a ϕ-extension of σ. Let $I \subseteq R$ be an ideal and let $J \subseteq S$ a homogeneous ideal s.t. $\phi(J) = I$. Then the following hold:*

(a) $\mathrm{in}_\sigma(I) = \phi(\mathrm{in}_\tau(J))$,

(b) *if $G = \{g_1, \ldots, g_s\}$ is a homogeneous τ-Gröbner basis of J, then $\{\phi(g_1), \ldots, \phi(g_s)\}$ is a σ-Gröbner basis of I.*

Proof. (a) Since J is homogeneous we have $\mathrm{in}_\tau(J) = \langle \mathrm{in}_\tau(f) : f \in J, f \text{ homogeneous} \rangle$. Thus, $\phi(\mathrm{in}_\tau(J)) = \langle \phi(\mathrm{in}_\tau(f)) : f \in J, f \text{ homogeneous} \rangle = \langle \mathrm{in}_\sigma(\phi(f)) : f \in J, f \text{ homogeneous} \rangle$. Next, we claim that $I = \{\phi(f) : f \in J, f \text{ homogeneous}\}$.

($\supseteq$) This is immediate as $\phi(J) = I$ by assumption.

($\subseteq$) Suppose I is generated by $f_1, \ldots, f_r$. Let $f = \sum_{i=1}^r a_i f_i \in I$, $a_i \in R$. Choose $h_i \in J$ homogeneous s.t. $\phi(h_i) = f_i$ for each i and let $\tilde{f} = \sum_{i=1}^r t^{\alpha_i} a_i^h h_i$. Clearly, $\tilde{f} \in J$ and it is homogeneous for an appropriate choice of the α_i's. But then $\phi(\tilde{f}) = \sum_{i=1}^r a_i f_i = f$ and the inclusion follows.

Thus, $\phi(\mathrm{in}_\tau(J)) = \langle \mathrm{in}_\sigma(\phi(f)) : f \in J, f \text{ homogeneous} \rangle = \mathrm{in}_\sigma(I)$.

(b) Since ϕ is a homomorphism and τ is a σ-extension of ϕ, we get

$$\phi(\mathrm{in}_\tau(J)) = \langle \phi(\mathrm{in}_\tau(g_i)) : i = 1 \ldots, s \rangle = \langle \mathrm{in}_\sigma(\phi(g_i)) : i = 1, \ldots, s \rangle.$$

Thus, $\{\phi(g_1), \ldots, \phi(g_s)\}$ is a σ-Gröbner basis of $\phi(\mathrm{in}_\tau(J)) = \mathrm{in}_\sigma(I)$ by (a). □

There is a simple ϕ-extension of the DRL-order on R.

Definition 5.4.4. Fix a DRL-order on R. The DRL-order on S by letting t be the smallest variable is denoted DRL^+.

Lemma 5.4.5 ([11] Lemma 3.11)**.** *The DRL^+-order on S ϕ-extends the DRL-order on R.*

Proof. Consider a homogeneous polynomial $f = \sum_{i=1}^{d} a_i t^{\alpha_i} u_i \in S$, where the $u_i \in \mathrm{Mon}(R)$ are distinct and $\alpha_i \in \mathbb{N}, a_i \in k \setminus \{0\}$. Then dehomogenizing f yields $\phi(f) = \sum_{i=1}^{d} a_i u_i$ and $\deg(u_i) = \deg(f) - \alpha_1$. If there was any cancellation in the terms of $\phi(f)$, the monomials involved are of the same degree. Thus, this cancellation also occurs in f, so there is no such cancellation. Now, without loss of generality assume that $\mathrm{in}_{DRL}(\phi(f)) = u_1$. Then for each $i = 2, \ldots, n$ we distinguish two cases:

(case 1) $\deg(u_1) > \deg(u_i)$. Then $\alpha_1 < \alpha_i$, since $\deg(u_j) + \alpha_j = \deg(f)$ for all j. Therefore, $t^{\alpha_1} u_1 >_{DRL^+} t^{\alpha_i} u_i$.

(case 2) $\deg(u_1) = \deg(u_i)$. Then $\alpha_1 = \alpha_i$, so since $u_1 >_{DRL} u_i$ it follows that $t^{\alpha_1} u_1 >_{DRL^+} t^{\alpha_i} u_i$.

Therefore, we have $\mathrm{in}_{DRL^+}(f) = t^{\alpha_1} u_1$ and $\phi(\mathrm{in}_{DRL^+}(f)) = u_1 = \mathrm{in}_{DRL}(\phi(f))$. □

Using this particular ϕ-extension of the DRL-order allows us to homogenize a Gröbner basis of an ideal to obtain a Gröbner basis of the homogenized ideal.

Proposition 5.4.6 ([11], Proposition 3.13)**.** *Fix the monomial orders DRL on R and DRL^+ on S. Let $I \subseteq R$ be an ideal with a Gröbner basis $G = \{g_1, \ldots, g_s\}$, then $G^h = \{g_1^h, \ldots, g_s^h\}$ is a Gröbner basis of $I^h \subseteq S$.*

Proof. First we have to check that $\langle g_1^h, \ldots, g_s^h \rangle = I^h$.

($\subseteq$) This is immediate as $g_1^h, \ldots, g_s^h \in I^h$.

($\supseteq$) Consider $f \in I$ s.t. $\deg(\mathrm{in}(f)) = d$ with a standard representation $f = \sum_{i=1}^{s} q_i g_i$ for some $q_i \in R$.
Since DRL is degree-compatible, we have that $d \geq \deg(q_i) + \deg(g_i)$. Thus, we can express f^h as

$$f^h = \sum_{i=1}^{s} t^{d - \deg(q_i) - \deg(g_i)} q_i^h g_i^h,$$

which implies that $f^h \in \langle g_1^h, \ldots, g_s^h \rangle$.

Next, we need to show that it is a Gröbner basis. To do so, we just have to check that the above representation of f^h is a standard representation. Note that $\mathrm{in}_{DRL^+}(f^h) = \mathrm{in}_{DRL}(f)$ is not divisible by t. We distinguish two cases:

(case 1) $d - \deg(q_i) - \deg(g_i) > 0$. Then t divides $t^{d - \deg(q_i) - \deg(g_i)} q_i^h g_i^h$ and also its initial monomial. It follows that $\mathrm{in}_{DRL^+}(f^h) \geq \mathrm{in}_{DRL^+}(t^{d - \deg(q_i) - \deg(g_i)} q_i^h g_i^h)$.

(case 2) $d - \deg(q_i) - \deg(g_i) = 0$. Then t does not divide $\mathrm{in}_{DRL^+}(q_i^h g_i^h)$. Thus, we have $\mathrm{in}_{DRL^+}(q_i^h g_i^h) = \mathrm{in}_{DRL}(q_i g_i) \leq_{DRL} \mathrm{in}_{DRL}(f) = \mathrm{in}_{DRL^+}(f^h)$. □

Example 5.4.7. As in previous examples consider $f_1 = x^2 - 1, f_2 = xy + x \in k[x, y]$ and let $f_1^h, f_2^h \in k[x, y, t]$ be their homogenizations w.r.t t. Consider the ideals

$$\begin{aligned} I &= \langle f_1, f_2 \rangle = \langle x^2 - 1, xy + x \rangle, \\ \tilde{I} &= \langle f_1^h, f_2^h \rangle = \langle x^2 - t^2, xy + xt \rangle, \\ I^h &= \langle x^2 - t^2, y + t \rangle. \end{aligned}$$

A Gröbner basis of $\tilde{I}$ is given by $\tilde{G} = \{x^2 - t^2, xy + yt, yt^2 + t^3\}$. By Proposition 5.4.6, a Gröbner basis of I^h is given by $G^h = \{x^2 - t^2, y + t\}$.
We see that $G^h \neq \tilde{G}$ but on the other hand $\phi(G^h) = \phi(\tilde{G}) = \{x^2 - 1, y + 1\} = G$ which is the Gröbner basis of I, which coincides with Theorem 5.4.3

5.5 Solving Systems with Finitely Many Solutions

In this section, we use concepts from elimination theory and Gröbner bases to provide a systematic way of eliminating variables in a system of polynomial equations. This then results in an algorithm to find the solutions of certain polynomial systems. The main focus lies on systems of polynomials with finitely many solutions. We mainly follow [15, Chapter 3].

Definition 5.5.1. An ideal I of R is called *zero-dimensional* if the affine variety over the algebraic closure $\bar{k}$ of k, i.e

$$\{p \in \bar{k}^n : f(p) = 0 \text{ for all } f \in I\}$$

is finite.

An important type of ideal in elimination theory is the following.

Definition 5.5.2. Let $I \subseteq k[x_1, \dots, x_n]$ be an ideal. Then the ideal

$$I_l = I \cap k[x_{l+1}, \dots, x_n]$$

is called the *l-th eliminiation ideal* of I.

Lemma 5.5.3. *Let I be an ideal of $k[x_1, \dots, x_n]$. Then:*

(a) *$I_l \subseteq k[x_{l+1}, \dots, x_n]$ is an ideal.*

(b) *I_{l+1} is the first elimination ideal of I_l.*

Proof. (a) I_l is clearly closed under addition as the intersection of two additively closed subsets of $k[x_1, \dots, x_n]$. Let $f \in I_l$ and $h \in k[x_{l+1}, \dots, x_n]$. Since I is an ideal, we have $hf \in I$. Moreover, we have $h, f \in k[x_{l+1}, \dots, x_n]$. Thus, $hf \in k[x_{l+1}, \dots, x_n]$, which implies that $hf \in I_l$ so I_l is an ideal of $k[x_{l+1}, \dots, x_n]$.

(b) The first elimination ideal of $I_l \subseteq k[x_{l+1}, \dots, x_n]$ is

$$\begin{aligned}(I_l)_1 &= I_l \cap k[x_{l+2}, \dots, x_n] = (I \cap k[x_{l+1}, \dots, x_n]) \cap k[x_{l+2}, \dots, x_n] \\ &= I \cap k[x_{l+2}, \dots, x_n] = I_{l+1}.\end{aligned}$$

□

Until now we mainly used the DRL-order. Regarding elimination theory the lex-order turns out to have favourable properties. Recall that unless otherwise mentioned, we assume that $x_1 > x_2 > \cdots > x_n$.

Theorem 5.5.4 (Elimination Theorem, [15], Theorem 2, Chapter 3.1)**.** *Let $I \subseteq k[x_1, \dots, x_n]$ be an ideal and let G be a lex-Gröbner basis of I. Then $G_l = G \cap k[x_{l+1}, \dots, x_n]$ is a Gröbner basis of I_l for any $l = 0, \dots, n-1$.*

Proof. Let $l \in \{0, \dots, n-1\}$. Clearly, $G_l \subseteq I_l$, so it is enough to show that $\mathrm{in}(I_l) = \langle \mathrm{in}(G_l) \rangle$.

($\supseteq$) This is obvious.

($\subseteq$) Let $f \in I_l$, so $f \in I$. Since G is a Gröbner basis, we know that $\mathrm{in}(g) \,|\, \mathrm{in}(f)$ for some $g \in G$. As $f \in I_l$, this implies that $\mathrm{in}(g)$ can only contain the variables $x_{l+1}, \dots, x_n$. But since we are working with the lex-order with $x_1 > \cdots > x_n$, this implies that $g \in k[x_{i+1}, \dots, x_n]$, as any monomial containing other variables would be greater than the initial monomial. Thus, $g \in G_l$ and every leading term of an element $f \in I_l$ is divisible by some $\mathrm{in}(g), g \in G_l$. Hence, G_l is a lex-Gröbner Basis of I_l. □

Definition 5.5.5. Let $I \subseteq k[x_1, \dots, x_n]$ be an ideal. A point $(a_{l+1}, \dots, a_n) \in \mathcal{V}(I_l) \subseteq k^{n-l}$ is called a *partial solution* of $\mathcal{V}(I)$.

The goal is to extend partial solutions to complete solutions $(a_1, \ldots, a_n) \in \mathcal{V}(I)$. This is done iteratively by adding one more coordinate to the partial solution $(a_{l+1}, \ldots, a_n) \in \mathcal{V}(I_l)$, i.e. finding $a_l \in k$ s.t. $(a_l, a_{l+1}, \ldots, a_n) \in \mathcal{V}(I_{l-1})$. However, it is not guaranteed that this is always possible. To see, when it is possible, we look at elimination as projecting a variety onto a lower-dimensional subspace.
To eliminate the variables $x_1, \ldots, x_l$ consider the projection map

$$\pi_l : k^n \to k^{n-l},$$

which maps $(a_1, \ldots, a_n)$ to $(a_{l+1}, \ldots, a_n)$. Applying π_l to an affine variety $V \subseteq k^n$ we get a set $\pi_l(V) \subseteq k^{n-l}$.

Lemma 5.5.6 ([15], Lemma 1, Chapter 3.2)**.** *Let I be an ideal of R and let I_l its l-th elimination ideal. Let $V = \mathcal{V}(I) \subseteq k^n$. Then*

$$\pi_l(V) \subseteq \mathcal{V}(I_l) \subseteq k^{n-l}.$$

Proof. Let $f \in I_l$ and $a = (a_1, \ldots, a_n) \in V$. Then $f(a) = 0$ as $f \in I$. But f only contains the variables $x_{l+1}, \ldots, x_n$, which allows us to write

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

Thus, f vanishes on $\pi_l(V)$, i.e. $\pi_l(V) \subseteq \mathcal{V}(I_l)$. □

We therefore see that all $\pi_l(V)$ are partial solutions. In fact, $\pi_l(V)$ are exactly these partial solutions that can be extended to complete solutions.

Theorem 5.5.7 (Closure Theorem, [15], Theorem 3, Chapter 3.2)**.** *Let k be algebraically closed. Let I be an ideal of R and let $V = \mathcal{V}(I)$. Then $\mathcal{V}(I_l)$ is the smallest affine variety containing $\pi_l(V) \subseteq k^{n-l}$.*

Proof. The smallest affine variety containing $\pi_l(V)$ is $\mathcal{V}(\mathcal{I}(\pi_l(V)))$ by Proposition 4.4.2. Thus, we show that $\mathcal{V}(I_l) = \mathcal{V}(\mathcal{I}(\pi_l(V)))$.

($\supseteq$) From Lemma 5.5.6 we know that $\pi_l(V) \subseteq \mathcal{V}(I_l)$. Since $\mathcal{V}(\mathcal{I}(\pi_l(V)))$ is the smallest variety containing $\pi_l(V)$, the inclusion follows.

($\subseteq$) Let $f \in \mathcal{I}(\pi_l(V))$, i.e. $f(a_{l+1}, \ldots, a_n) = 0$ for all $(a_{l+1}, \ldots, a_n) \in \pi_l(V)$. Regarding f as polynomial in $k[x_1, \ldots, x_n]$ we clearly also have $f(a_1, \ldots, a_n) = 0$ for all $(a_1, \ldots, a_n) \in V$. Then the Nullstellensatz implies that $f^m \in I$ for some m. Since f does not contain any variables $x_1, \ldots, x_l$, neither does f^m. Therefore $f^m \in I_l$, i.e. $f \in \sqrt{I_l}$. Finally, this yields the inclusion $\mathcal{V}(I_l) = \mathcal{V}(\sqrt{I_l}) \subseteq \mathcal{V}(\mathcal{I}(\pi_l(V)))$. □

The next result shows us that the reduced lexicographic Gröbner basis of a zero-dimensional ideal always has a certain structure. This structure will allow us to reduce the problem of computing the solutions to the univariate case and extend partial solutions to complete solutions.

Theorem 5.5.8 ([11], Theorem 2.6)**.** *Let $I \subseteq k[x_1, \ldots, x_n]$ be a zero-dimensional ideal and let G be the reduced lex-Gröbner basis of I. Then G consists of polynomials of the form*

$$\begin{aligned}
p_{n,1}(x_n) &\in G_{n-1},\\
p_{n-1,1}(x_{n-1}, x_n), \ldots, p_{n-1,t_{n-1}}(x_{n-1}, x_n) &\in G_{n-2},\\
p_{n-2,1}(x_{n-2}, x_{n-1}, x_n), \ldots, p_{n-2,t_{n-2}}(x_{n-2}, x_{n-1}, x_n) &\in G_{n-3},\\
&\vdots\\
p_{1,1}(x_1, \ldots, x_n), \ldots, p_{n_1,t_1}(x_1, \ldots, x_n) &\in G_0,
\end{aligned}$$

where $p_{i,j} \in k[x_i, \dots, x_n]$ *for every* $i \in \{1, \dots, n\}$, $j \in \{1, \dots, t_i\}$ *and* $t_1, \dots, t_{n-1} \geq 1$. *Moreover, for any* $l \in \{1, \dots, n\}$, *let* $a = (a_{l+1}, \dots, a_n) \in k^{n-l}$ *be a root of the polynomials*

$$\begin{aligned} p_{n,1}(x_n) &\in G_{n-1}, \\ p_{n-1,1}(x_{n-1}, x_n), \dots, p_{n-1,t_{n-1}}(x_{n-1}, x_n) &\in G_{n-2}, \\ &\vdots \\ p_{l+1,1}(x_{l+1}, \dots, x_n), \dots, p_{l+1,t_{l+1}}(x_{l+1}, \dots, x_n) &\in G_l, \end{aligned}$$

and let

$$p_l(x_l) = \gcd(p_{l,1}(x_l, a_{l+1}, \dots a_n), \dots, p_{l,t_l}(x_l, a_{l+1}, \dots, a_n)).$$

Then $p_l(x_l) \notin k$.

Proof. Consider all affine varieties over the algebraic closure $\overline{k}$. Since I is zero-dimensional, we have that $\mathcal{V}(I) = \{p \in \overline{k}^n : f(p) = 0 \text{ for all } f \in I\}$ is finite. Let G be the reduced *lex*-Gröbner basis of I. Then, by Theorem 5.5.4, the set $G_{l-1} = G \cap k[x_l, \dots, x_n]$ is a *lex*-Gröbner basis of the elimination ideal I_{l-1} and is of the form

$$G_{l-1} = \{p_{i,j}(x_i, \dots, x_n) : l \leq i \leq n, 1 \leq j \leq t_i\},$$

for some $t_1, \dots, t_n \geq 0$. Furthermore, If $p_l(x_l) \neq 0$ for some $l = 1, \dots, n$, we have $t_l \geq 1$. Thus, it remains to show that $p_l(x_l) \notin k$ for $l = 1, \dots, n$.

This is shown by descending induction on $l \geq n$. Let $l = n$. Then, since G_{l-1} is the reduced *lex*-Gröbner basis of I_{l-1}, we get a monic generator $p_{n,1}(x_n)$ of I_{n-1}. Then $G_{n-1} = \{p_{n,1}(x_n)\}$ and $t_n = 1$. Since $|\mathcal{V}(I)| < \infty$, it follows that $p_{n,1}(x_n) \neq 0$ and $p_n(x_n) = p_{n,1}(x_n) \notin k \setminus \{0\}$, since $\emptyset \neq \mathcal{V}(I) \subseteq \mathcal{V}(p_n)$.

Let $l < n$ and assume by induction that the result holds for $l+1$. G_{l-1} is the reduced *lex*-Gröbner basis of I_{l-1}, so we have

$$I_{l-1} = \langle p_{i,j} : l \leq i \leq n, 1 \leq j \leq t_i \rangle.$$

Let $a \in \mathcal{V}(I_l) \cap \overline{k}^{n-l}$ and let

$$I(l, a) = \langle p_{l,1}(x_l, a_{l+1}, \dots, a_n), \dots, p_{l,t_l}(x_l, a_{l+1}, \dots, a_n) \rangle = \langle p_l(x_l) \rangle.$$

Since $|\mathcal{V}(I)| < \infty$, Theorem 5.5.7 implies that one has $\mathcal{V}(I_{l-1}) = \pi_{l-1}(\mathcal{V}(I))$. So clearly, $|\mathcal{V}(I_{l-1})| < \infty$. If $p_l(x_l) = 0$, then $\mathcal{V}(I(l, a)) = \bar{k}$ and $\{(a_l, \dots, a_n) : a_l \in \bar{k}\} \subseteq \mathcal{V}(I_{l-1})$, which contradicts the finiteness of $\mathcal{V}(I_{l-1})$.

On the other hand, if $p_l(x_l) \in k \setminus \{0\}$, then $\mathcal{V}(I(l, a)) = \emptyset$. But we have chosen the point $a = (a_{l+1}, \dots, a_n) \in \mathcal{V}(I_l) = \pi_l(\mathcal{V}(I))$, where the equality comes from Theorem 5.5.7. Thus, there are $a_1, \dots, a_l \in \bar{k}$ s.t. $(a_1, \dots, a_n) \in \mathcal{V}(I)$. This implies $\pi_{l-1}(a_1, \dots, a_n) = (a_l, \dots, a_n) \in \mathcal{V}(I_{l-1})$, i.e. $a_l \in \mathcal{V}(I(l, a)) = \emptyset$, which is a contradiction. □

This ensures that the reduced lexicographic Gröbner basis contains a univariate polynomial in the smallest variable. Therefore, as in the case of linear equations, it is possible to solve this univariate equation first and then substitute the values into the remaining polynomials contained in the Gröbner basis to simplify them and get another set of univariate polynomials. Iteratively applying this to a set of polynomial equations with finitely many solutions yields an algorithmic

way to compute all its solutions.

Algorithm 3: Algorithm to solve systems with finitely many solutions

Input : I zero-dimensional
Output: $\mathcal{V}(I)$
$\mathcal{V}(I) = \{\}$
G_{lex} := reduced lex-Gröbner basis of I
$p_n(x_n) := G_{lex} \cap k[x_n]$
if $p_n(x_n) = 1$ **then**
  return $\mathcal{V}(I)$
else
  $A^{(n)} := \{\text{roots of } p_n(x_n)\}$
  for $a^{(n)} \in A^{(n)}$ **do**
    $p_{n-1}(x_{n-1}) = \gcd(p_{n-1,1}(x_{n-1}, a^{(n)}), \ldots, p_{n-1,t_{n-1}}(x_{n-1}, a^{(n)}))$
    $A^{(n-1)} := \{\text{roots of } p_{n-1}(x_{n-1})\}$
    for $a^{(n-1)} \in A^{(n-1)}$ **do**
      $p_{n-2}(x_{n-2}) = \gcd(p_{n-2,1}(x_{n-2}, a^{(n-1)}, a^{(n)}), \ldots, p_{n-2,t_{n-2}}(x_{n-2}, a^{(n-1)}, a^{(n)}))$
      $\vdots$
      for $a^{(1)} \in A^{(1)}$ **do**
        $\mathcal{V}(I) := \mathcal{V}(I) \cup \{(a^{(1)}, a^{(2)}, \ldots, a^{(n)})\}$
      end
      $\vdots$
    end
  end
  return $\mathcal{V}(I)$
end

Example 5.5.9. Consider $I = \langle x^2 - z^2, xy + xz, x^2 - 1\rangle \subseteq k[x, y, z]$. We compute $\mathcal{V}(I)$ using Algorithm 3.
The reduced lex-Gröbner basis is $\{x^2 - 1, y + z, z^2 - 1\}$.
$p_3(z) = (z + 1)(z - 1)$, thus $A^{(3)} = \{1, -1\}$.

(1) Let $1 \in A^{(3)}$. Then $p_2(y) = y + 1$. Thus $A^{(2)} = \{-1\}$

- Let $-1 \in A^{(2)}$. Then $p_1(x) = (x - 1)(x + 1)$. Thus $A^{(1)} = \{1, -1\}$
  $\mathcal{V}(I) = \{(1, -1, 1), (-1, -1, 1)\}$.

(2) Let $-1 \in A^{(3)}$. Then $p_2(y) = y - 1$. Thus $A^{(2)} = \{1\}$

- Let $1 \in A^{(2)}$. Then $p_1(x) = (x - 1)(x + 1)$. Thus $A^{(1)} = \{1, -1\}$
  $\mathcal{V}(I) = \{(1, -1, 1), (-1, -1, 1), (1, 1, -1), (-1, 1, -1)\}$.

The algorithm returns all four solutions $\mathcal{V}(I)$ of the system.

5.6 Macaulay Matrices

Buchberger's algorithm is a very basic algorithm to compute Gröbner bases and can be improved by several additional criteria. However, in this thesis, the focus lies on a second family of algorithms that base the computation of Gröbner bases on Gaussian elimination of matrices. These algorithms are usually faster than the different versions of Buchberger's algorithm. This family of algorithms include F_4 [25], *MatrixF*$_5$ [21], *XL* [14] and *mutantXL* [10]. In this section

we present a very basic algorithm that computes a Gröbner basis by Gaussian elimination on matrices.

Recall that the set of all monomials on R form a k-vector space. Let $\mathrm{Mon}_d(R)$ and $\mathrm{Mon}_{\leq d}(R)$ denote the sets of monomials of R of degree d resp. degree $\leq d$. As a *shift* of a polynomial f, we will mean a product tf for some $t \in \mathrm{Mon}(R)$.
First, we have to define a map that maps a set of polynomials to a matrix.

Definition 5.6.1. Fix a monomial order σ and let $F = \{f_1, \ldots, f_m\} \subseteq R$ be a list of polynomials with $|F| = m$. Let $T_\sigma = \{u_1 >_\sigma u_2 >_\sigma \cdots\}$ be an ordered set of monomials with $|T_\sigma| = l$, s.t. $\mathrm{Supp}(F) = \bigcup_{f_i \in F} \mathrm{Supp}(f_i) \subseteq T_\sigma$.
Define $\mathrm{Coef} : F \times T_\sigma \to k^{m \times l}$ to be the map s.t. $\mathrm{Coef}(F, T_\sigma)$ is the matrix satisfying the following properties.

(a) The columns are indexed in σ-decreasing order from left to right by the monomials in T_σ.

(b) The rows are indexed by the polynomials of F, where the row corresponding to $f_i \in F$ is the coefficient vector $(c_i^{(1)}, c_i^{(2)}, \ldots, c_i^{(l)}) \in k^l$ s.t. $f_i = \sum_{j=1}^{l} c_i^{(j)} u_j, c_i^{(j)} \in k, u_j \in T_\sigma$.

Let $A \in k^{m \times l}$ be an arbitrary matrix and let T_σ be an ordered l-element set of monomials. The right inverse function of Coef, denoted $\mathrm{Coef}^{-1} : k^{m \times l} \times T_\sigma \to R$ is defined to give the unique list $F' \subseteq R$ of m polynomials s.t. $\mathrm{Coef}(F', T_\sigma) = A$ and $\mathrm{Supp}(F') \subseteq T_\sigma$.

We may omit the subscript σ of the set T if there is no ambiguity. Thus, it is always true that $\mathrm{Coef}(\mathrm{Coef}^{-1}(A, T), T) = A$. And since we always choose T in such a way that $\mathrm{Supp}(F) \subseteq T$, it is also true that $\mathrm{Coef}^{-1}(\mathrm{Coef}(F, T), T) = F$. These maps now allow us to introduce the notion of *Macaulay matrices* of a set of polynomials.

Definition 5.6.2. Fix $d \in \mathbb{Z}_{\geq 0}$ and a monomial order σ on R.

(a) Let $F = \{f_1, \ldots, f_s\} \subseteq R$ be a finite set of homogeneous polynomials and define the set $\overline{F}_d = (\mathrm{Mon}(R)F)_d = \{t_{ij} f_j : t_{ij} \in \mathrm{Mon}_{\leq d}(R), f_j \in F \text{ s.t. } \deg(t_{ij} f_j) = d\}$ to be the set of all shifts of polynomials in F with degree equal to d. Then the *homogeneous Macaulay matrix* of degree d of F is defined to be

$$M_d(F) = \mathrm{Coef}(\overline{F}_d, \mathrm{Mon}_d(R)).$$

(b) Let $F = \{f_1, \ldots, f_s\}$ be a finite set of (not necessarily homogeneous) polynomials and define the set $\overline{F}_{\leq d} = (\mathrm{Mon}(R)F)_{\leq d} = \{t_{ij} f_j : t_{ij} \in \mathrm{Mon}_{\leq d}(R), f_j \in F \text{ s.t. } \deg(t_{ij} f_j) \leq d\}$ to be the set of all shifts of F with total degree less or equal to d. Then the *inhomogeneous Macaulay matrix* of degree d of F is defined to be

$$M_{\leq d}(F) = \mathrm{Coef}(\overline{F}_{\leq d}, \mathrm{Mon}_{\leq d}(R)).$$

Example 5.6.3. Fix the DRL-order on $R = k[x, y, z]$. Let $f_1 = x^2 - z^2, f_2 = xy + xz \in R$. We construct $M_3(F)$ for $F = \{f_1, f_2\} \subseteq R$. The DRL-ordered set of monomials of degree 3 is

$$\mathrm{Mon}_3(R) = \{x^3, x^2y, xy^2, y^3, x^2z, xyz, y^2z, xz^2, yz^2, z^3\}.$$

The set of all shifts of F of degree 3 is

$$\overline{F}_3 = \{x(x^2 - z^2), y(x^2 - z^2), z(x^2 - z^2), x(xy + xz), y(xy + xz), z(xy + xz)\}.$$

Then $\mathrm{Coef}(\overline{F}_3, \mathrm{Mon}_3(R))$ yields

$$M_3(F) = \begin{array}{c} \\ xf_1 \\ yf_1 \\ zf_1 \\ xf_2 \\ yf_2 \\ zf_2 \end{array} \begin{array}{c} \begin{array}{cccccccccc} x^3 & x^2y & xy^2 & y^3 & x^2z & xyz & y^2z & xz^2 & yz^2 & z^3 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \end{pmatrix} \end{array}$$

Note that if F consists of homogeneous polynomials, then the inhomogeneous Macaulay matrix $M_{\leq d}(F)$ is a block matrix, where the blocks are the homogeneous Macaulay matrices $M_0(F), \ldots, M_d(F)$.

Before we can state the algorithm, we recall the notion of the reduced row echelon form of a matrix.

Definition 5.6.4. Let $A \in k^{m \times l}$ be a matrix, where A_i denotes the i-th row of A for $i = 1, \ldots, m$.

(a) If $A_i \neq 0$, then $\mathrm{pivot}(A, i)$ is defined to be the smallest index $j \in \{1, \ldots, l\}$ s.t. $A_{i,j} \neq 0$.

(b) A is said to be in *reduced row echelon form* denoted $\mathrm{rref}(A)$ if all nonzero rows A_i satisfy $A_{i,\mathrm{pivot}(A,i)} = 1$ and $A_{i',\mathrm{pivot}(A,i)} = 0$ for all $i \neq i'$.

Usually, there are some more conditions for a matrix to be in reduced row echelon form, but they will not be needed in this thesis.
Every matrix can be transformed into reduced row echelon form by elementary row operations, i.e. swapping rows, adding one row to another and multiplying rows by nonzero scalars.

It will be shown that the following algorithm computes a Gröbner basis by transforming Macaulay matrices into reduced row echelon form if the degree d is chosen large enough. The algorithm is due to A. Maletzky [36] and M. Wiesinger-Widi [49].

Algorithm 4: Computing Gröbner basis by row reducing Macaulay matrices

Input : $F = \{f_1, \ldots, f_s\}$, $d \in \mathbb{Z}_{\geq 0}$
Output: Gröbner basis $G = \{g_1, \ldots, g_m\}$ of $\langle F \rangle$.
Compute: $M_{\leq d}(F)$
Compute: $A := \mathrm{rref}(M_{\leq d}(F))$
Compute: $G := \mathrm{Coef}^{-1}(A, \overline{F}_{\leq d})$
return G

Theorem 5.6.5 ([36], Theorem 2.3)**.** *Fix a monomial order. Let $F = \{f_1, \ldots, f_s\} \subseteq R$ be a set of polynomials and let H be a Gröbner basis of $\langle F \rangle$. Fix $d \in \mathbb{Z}_{\geq 0}$ s.t. for all $h \in H$ there exist $q_1, \ldots, q_s \in R$ with $h = \sum_{i=1}^{s} q_i f_i$ and $\deg(q_i f_i) \leq d$. Then Algorithm 4 computes a Gröbner basis of $\langle F \rangle$.*

Proof. Let $M_{\leq d}(F), A$ and G be as in the algorithm, where

$$M_{\leq d}(F) = \mathrm{Coef}(\overline{F}_{\leq d}, \mathrm{Mon}_{\leq d}(R)).$$

As we have chosen d in such a way that $h = \sum_{i=1}^{s} q_i f_i$ and $\deg(q_i f_i) \leq d$, we clearly have $\mathrm{Supp}(q_i)\{f_i\} \subseteq \overline{F}_{\leq d}$ for all $i = 1, \ldots, s$ and for all $h \in H$. Thus, for all $h \in H$ we have

$$\begin{aligned} \mathrm{Coef}(\{h\}, \mathrm{Mon}_{\leq d}(R)) \in\ & \mathrm{rowspace}(\mathrm{Coef}(\overline{F}_{\leq d}, \mathrm{Mon}_{\leq d}(R))) \\ =\ & \mathrm{rowspace}(M_{\leq d}(F)) \\ =\ & \mathrm{rowspace}(A), \end{aligned}$$

where $\mathrm{Coef}(\{h\}, \mathrm{Mon}_{\leq d}(R))$ is the $1 \times |\mathrm{Mon}_{\leq d}(R)|$-matrix corresponding to the row-vector in $k^{|\mathrm{Mon}_{\leq d}(R)|}$.
Hence every $h \in H$ can be written as a linear combination of elements in G. Also, since A is in reduced row echelon form, it is true that for $g_i, g_j \in G$ and $i \neq j$ we also have $\mathrm{in}(g_i) \neq \mathrm{in}(g_j)$. This implies that additionally $\mathrm{in}(h) \in \mathrm{in}(G)$ for all $h \in H$, i.e. $\mathrm{in}(H) \subseteq \mathrm{in}(G)$. Furthermore, $G \subseteq \langle \overline{F}_{\leq d} \rangle = \langle F \rangle = \langle H \rangle$, which implies that $\langle \mathrm{in}(G) \rangle \subseteq \mathrm{in}(\langle F \rangle) = \mathrm{in}(\langle H \rangle)$. Therefore, we have $\langle \mathrm{in}(G) \rangle = \mathrm{in}(\langle F \rangle)$. So G is indeed a Gröbner basis of $\langle F \rangle$. □

Example 5.6.6. Fix the *DRL*-order on $R = k[x, y, z]$. With reference to the previous example let $F = \{x^2 - z^2, xy + xz\} \subseteq R$. Since we apply the algorithm to a set of homogeneous polynomials, we can consider the homogeneous Macaulay matrices $M_d(F)$ to perform Gaussian elimination, as $M_{\leq d}(F)$ would be a block matrix containing $M_0(F), \ldots, M_d(F)$. It is easy to see that $\overline{F}_2 = \{x^2, xy, y^2, xz, yz, z^2\}$ and

$$M_2(F) = \begin{array}{c} \\ f_1 \\ f_2 \end{array} \begin{array}{c} \begin{array}{cccccc} x^2 & xy & y^2 & xz & yz & z^2 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix} \end{array}$$

which is already in reduced row echelon form. Thus, the algorithm returns F, which is clearly not a Gröbner basis. This means we have to increase d. Let $d = 3$. Bringing $M_3(F)$ into reduced row echelon form yields

$$\mathrm{rref}(M_3(F)) = \begin{array}{c} \begin{array}{cccccccccc} x^3 & x^2y & xy^2 & y^3 & x^2z & xyz & y^2z & xz^2 & yz^2 & z^3 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \end{pmatrix} \end{array}$$

The algorithm returns

$$G = \{x^3 - xz^2, x^2y + z^3, x^2z - z^3, yz^2 + z^3, xy^2 - xz^2, xyz + xz^2\} \cup F,$$

where F comes from $M_2(F)$. After removing multiplies of each other we get the set

$$\{yz^2 + z^3, x^2 - z^2, xy + xz\},$$

which is a Gröbner basis of I as we have already mentioned in Example 5.4.7.

Since we do not know how large to choose d in advance, this algorithm itself is not very useful. But in Chapter 8 we introduce the concept of solving degree to find some bounds.

While in Theorem 5.5.8 we need the reduced *lex*-Gröbner basis to find the solutions of systems of polynomials, it is often easier to compute Gröbner bases w.r.t to other monomial orders. As it turns out, the *DRL*-Gröbner basis is usually the computationally easiest to obtain. Therefore, it makes sense to first compute a Gröbner basis w.r.t to a different monomial order and then to convert it to a *lex*-Gröbner basis. One way to do so is by the FGLM algorithm [24] that performs the conversion of Gröbner bases of zero-dimensional ideals efficiently and is largely considered to be the most practical for this purpose. Thus, the standard procedure to solve a zero-dimensional system of polynomials $\mathcal{F}$ is the following:

(a) Compute *DRL*-Gröbner basis of $\langle \mathcal{F} \rangle$.

(b) Convert the *DRL*-Gröbner basis to *lex*-Gröbner basis with FGLM algorithm.

(c) Apply Algorithm 3, to compute $\mathcal{V}(\langle \mathcal{F} \rangle)$.

5.7 Gröbner Bases for Modules

For some purposes, it is useful to extend the notions of Gröbner bases to modules. We will use these generalizations to present a proof of the Hilbert syzygy theorem due to F.-O. Schreyer. This will confirm that modules over polynomial rings have a finite free resolution. Several results are restatements of the ideal case with very similar proofs. Thus, we focus on the proofs that contain new and essential concepts needed to derive the Hilbert syzygy theorem. For a more detailed description of this subject, see [16, Chapters 5 and 6], [33, Chapter 2] and [45].

First, we have to extend the notion of monomials to modules. Let $(e_i)_{i=1}^m$ be the standard basis of R^m.

Definition 5.7.1. A (*module-*) *monomial* $\mathbf{m} \in R^m$ is an element of the form $x^\alpha e_i$ for some $i \in \{1, \dots, m\}, x^\alpha \in \mathrm{Mon}(R)$. The monomial $\mathbf{m}$ is said to *contain* the basis vector e_i. The set of all such monomials will be denoted $\mathrm{Mon}(R^m)$.

Every element $\mathbf{f} \in R^m$ can be written as a unique k-linear combination

$$\mathbf{f} = \sum_{i=1}^{s} c_i \mathbf{m}_i,$$

of monomials $\mathbf{m}_i$, where $c_i \in k \setminus \{0\}$.

Definition 5.7.2. A product $c\mathbf{m}$ of a monomial $\mathbf{m}$ with a scalar $c \in k$ is called a *term* and c is the *coefficient* of $\mathbf{m}$.
The terms $c_i\mathbf{m}_i$ s.t. $c_i \neq 0$ in the expansion of $\mathbf{f} \in R^m$ are said to *belong* to $\mathbf{f}$.

If $\mathbf{m}, \mathbf{n} \in \mathrm{Mon}(R^m)$, $\mathbf{m} = x^\alpha e_i, \mathbf{n} = x^\beta e_j$, then $\mathbf{n}$ *divides* $\mathbf{m}$ if and only if $i = j$ and $x^\alpha | x^\beta$. If $\mathbf{n}$ divides $\mathbf{m}$, then the quotient $\mathbf{m}/\mathbf{n}$ is defined to be $x^\alpha / x^\beta = x^{\alpha-\beta} \in \mathrm{Mon}(R)$.

If $\mathbf{m}, \mathbf{n}$ contain the same basis vector e_i, the *greatest common divisor* $\gcd(\mathbf{m}, \mathbf{n})$ and the *least common multiple* $\mathrm{lcm}(\mathbf{m}, \mathbf{n})$ are defined to be $\gcd(x^\alpha, x^\beta)e_i$ and $\mathrm{lcm}(x^\alpha, x^\beta)e_i$, respectively. If they do not contain the same basis vector, then the convention is $\mathrm{lcm}(\mathbf{m}, \mathbf{n}) = 0$.

As in the ideal case, what we are first interested in are those modules generated by monomials.

Definition 5.7.3. $M \subseteq R^m$ is called a *monomial* submodule if M can be generated by a set of monomials.

By the following generalization of Dickson's lemma, we get that monomial submodules can be generated by finitely many monomials.

Theorem 5.7.4 (Structure Theorem for Monomial Modules, [33], Theorem 1.3.9)**.** *Let M be a monomial submodule.*

(a) *There are finitely many monomials $m_1, \dots, m_s \in \mathrm{Mon}(R)$, $i_1, \dots, i_s \in \{1, \dots, m\}$ s.t. $M = \langle m_1 e_{i_1}, \dots, m_s e_{i_s} \rangle$.*

(b) *There are monomial ideals $I_1, \dots, I_m$ of R s.t. $M \cong \bigoplus_{i=1}^m I_i e_i$.*

Proof. (a) Consider a system of generators $B \subseteq \mathrm{Mon}(R^m)$ of M. For $i = 1, \dots, m$, consider $B_i = \{m \in \mathrm{Mon}(R) : me_i \in B\} \subseteq \mathrm{Mon}(R)$. Dickson's lemma implies that the monomial ideal $I_i = \langle B_i \rangle$ is generated by a set $G_i \subseteq B_i$ of finitely many monomials. Clearly, the finite set $G_1 e_1 \cup \dots \cup G_m e_m \subseteq \mathrm{Mon}(R^m)$ generates M.

(b) By (a) we have $M = \sum_{i=1}^m I_i e_i$. Since $M \subseteq \bigoplus_{i=1}^m R e_i$ it follows that $M = \bigoplus_{i=1}^m I_i e_i$. □

Monomial modules can be characterized in the same way as monomial ideals.

Corollary 5.7.5. *Let M be a monomial module. Then $\mathbf{f} \in M$ if and only if every term belonging to $\mathbf{f}$ is in M.*

Proof. Let $\mathbf{f} \in M = \bigoplus_{i=1}^{m} I_i e_i$. Thus, $\mathbf{f} \in M$ if and only if $\mathbf{f} = (f_1, \ldots, f_m)$ and $f_i \in I_i$ for all $i = 1, \ldots, m$ if and only if every term of f_i is in I_i for all $i = 1, \ldots, m$ which is the case if and only if every term belonging to $\mathbf{f}$ is in M. □

Corollary 5.7.6 ([33], Corollary 1.3.10)**.** *Every ascending chain of monomial submodules of R^m eventually stabilizes.*

Proof. Suppose by contradiction that there exists such an infinite chain $M_1 \subseteq M_2 \subseteq \cdots$ of monomial submodules of R^m. Every M_i is generated by monomials. Thus, there exist monomials $\mathbf{m}_i \in M_i \setminus M_{i-1}$ for each $i \geq 2$. Clearly, $\langle \mathbf{m}_1, \ldots, \mathbf{m}_i \rangle \subseteq M_i$ for all $i \geq 1$, which implies that $\mathbf{m}_{i+1} \notin \langle \mathbf{m}_1, \ldots, \mathbf{m}_i \rangle \subseteq M_i$. Thus, $\langle \mathbf{m}_1, \mathbf{m}_2, \ldots \rangle \subseteq R^m$ cannot be generated by finitely many monomials, a contradiction. □

For the next result, recall the definition of *syzygy*-module. We confirm that also for modules, all syzygies are generated by a certain type of syzygies.

Proposition 5.7.7 ([16], Proposition 2.3, Chapter 5)**.** *Let $\{\mathbf{m}_1, \ldots, \mathbf{m}_t\}$ be a set of monomial generators of a monomial submodule of R^m. Let $\epsilon_1, \ldots, \epsilon_t$ be the standard basis vectors of R^t. Let $\mathbf{m}_{i,j} = \operatorname{lcm}(\mathbf{m}_i, \mathbf{m}_j)$. Then $\operatorname{Syz}(\mathbf{m}_1, \ldots, \mathbf{m}_t)$ is generated by the syzygies*

$$\mathbf{s}_{i,j} = \left(\frac{\mathbf{m}_{i,j}}{\mathbf{m}_i}\right)\epsilon_i - \left(\frac{\mathbf{m}_{i,j}}{\mathbf{m}_j}\right)\epsilon_j,$$

for all $i, j = 1, \ldots, t$.

Proof. By the definition of lcm, clearly, $\boldsymbol{s}_{i,j} = 0$ unless $\mathbf{m}_i$ and $\mathbf{m}_j$ contain the same standard basis vector of R^m. It is easy to see that $\mathbf{s}_{i,j}$ is a syzygy.
Let $(a_1, \ldots, a_t) \in R^t$ be a syzygy on $\{\mathbf{m}_1, \ldots, \mathbf{m}_t\}$. Expanding it w.r.t the basis vectors e_i yields

$$0 = a_1\mathbf{m}_1 + \cdots + a_t\mathbf{m}_t = f_1 e_1 + \cdots + f_m e_m$$

and therefore $f_1 = \cdots = f_m = 0$. Thus, $(a_1, \ldots, a_t)$ is a sum of syzygies on subsets of $\{\mathbf{m}_1, \ldots, \mathbf{m}_t\}$ containing the same basis vector. Hence, it is enough to show the claim for sets of monomials containing the same e_i,

$$\mathbf{m}_1 = m_i e_i, \ldots, \mathbf{m}_s = m_s e_i.$$

But in this case, the result follows from Lemma 5.3.3. □

Next, we can extend the notions of monomial order on R to R^m, which stays basically the same.

Definition 5.7.8. A *monomial order* on R^m is a total order σ on $\operatorname{Mon}(R^m)$ s.t.

(a) σ respects multiplication: for all $\mathbf{m}, \mathbf{n} \in R^m$ with $\mathbf{m} >_\sigma \mathbf{n}$ one has $x^\alpha \mathbf{m} >_\sigma x^\alpha \mathbf{n}$ for every $x^\alpha \in \operatorname{Mon}(R)$,

(b) σ is a well-order.

Once a monomial order σ on R^m is established, we can write $\mathbf{f} \in R^m$ as

$$\mathbf{f} = \sum_{i=1}^{t} c_i \mathbf{m}_t,$$

where $c_i \neq 0$ and $\mathbf{m}_1 >_\sigma \cdots >_\sigma \mathbf{m}_t$.

Thus, as in the ideal case we define the *leading/ initial monomial, leading coefficient* and *leading term*:

(a) $\text{in}(\mathbf{f}) = \mathbf{m}_1$,

(b) $\text{lc}(\mathbf{f}) = c_1$,

(c) $\text{lt}(\mathbf{f}) = c_1\mathbf{m}_1$.

With a monomial order on R^m, it is possible to divide by a set $F \subseteq R^m$ exactly the same way as in R. The division algorithm can be restated, where the proof is the same as in Theorem 5.1.9.

Theorem 5.7.9 (Division Algorithm in R^m, [16], Theorem 2.5, Chapter 5)**.** *Fix a monomial order on R^m and let $F = \{\mathbf{f}_1, \ldots, \mathbf{f}_s\} \subseteq R^m$ be an ordered set of polynomials. Then every $\mathbf{f} \in R^m$ can expressed as*

$$\mathbf{f} = q_1\mathbf{f}_1 + \cdots + q_s\mathbf{f}_s + \mathbf{r},$$

where $q_i \in R, \mathbf{r} \in R^m, \text{in}(q_i\mathbf{f}_i) \leq \text{in}(\mathbf{f})$ for all i and either $\mathbf{r} = 0$ or $\mathbf{r}$ is a k-linear combination of monomials none of which is divisible by any $\text{in}(\mathbf{f}_1), \ldots, \text{in}(\mathbf{f}_s)$. $\mathbf{r}$ is called the remainder on division by F.

As before, the division algorithm behaves the best, when F is a Gröbner basis.

Definition 5.7.10. Let M be a submodule of R^m and fix be a monomial order σ.

(a) The monomial submodule generated by the initial monomials of all $\mathbf{f} \in M$ w.r.t σ is called the *initial module* denoted $\text{in}_\sigma(M)$.

(b) A set $\{\mathbf{g}_1, \ldots, \mathbf{g}_s\} \subseteq M$ is called a *σ-Gröbner basis* of M if $\text{in}_\sigma(M) = \langle \text{in}_\sigma(\mathbf{g}_1), \ldots, \text{in}_\sigma(\mathbf{g}_s)\rangle$.

If the monomial order is clear from context, we may omit the subscript σ.

Most of the properties of a Gröbner basis extend to the module case, with essentially the same proofs. A Gröbner basis G of M is a generating set (not necessarily a basis) of M and does exist for all submodules M of R^m. Also $\mathbf{f} \in M$ if and only if the remainder on division by G is zero. Also, the notion of reduced Gröbner basis can be defined as for ideals. Again, every module has a unique reduced Gröbner basis.

To restate a version of Buchberger's algorithm in the module case, we first have to adjust the notion of S-polynomials.

Definition 5.7.11. Fix a monomial order on R^m and let $\mathbf{f}, \mathbf{g} \in R^m$. The *S-vector* of $\mathbf{f}$ and $\mathbf{g}$, denoted $S(\mathbf{f}, \mathbf{g})$ is defined as follows. Let $\mathbf{m} = \text{lcm}(\text{in}(\mathbf{f}), \text{in}(\mathbf{g}))$. Then

$$S(\mathbf{f}, \mathbf{g}) = \frac{\mathbf{m}}{\text{lt}(\mathbf{f})}\mathbf{f} - \frac{\mathbf{m}}{\text{lt}(\mathbf{g})}\mathbf{g}.$$

The foundation for Buchberger's algorithm in the module case is the generalized version of Buchberger's criterion, which can be proved the same way as in the ideal case. For a proof see [33, Section 2.5].

Theorem 5.7.12 (Buchberger's Criterion for Modules, [16], Theorem 2.9, Chapter 5)**.** *A set $G = \{\mathbf{g}_1, \ldots, \mathbf{g}_s\} \subseteq R^m$ is a Gröbner basis for $\langle G\rangle$ if and only if the remainder on division by G of $S(\mathbf{g}_i, \mathbf{g}_j)$ is zero for all i, j.*

Theorem 5.7.13 (Buchberger's Algorithm for Modules, [16], Theorem 2.11, Chapter 5)**.** *Fix a monomial order on R^m and let $F = \{\mathbf{f}_1, \ldots, \mathbf{f}_s\} \subseteq R^m$ be an ordered set of polynomials. Then F can be extended into a Gröbner basis in finitely many steps.*

The algorithm can be stated as in the ideal case. The proof of termination is based on the fact from Corollary 5.7.6 that the ascending chain condition also holds for submodules.

Now, we use these generalized notions to show some results that will be necessary for the proof of the Hilbert syzygy theorem. Let $G = \{\mathbf{g}_1, \dots, \mathbf{g}_s\}$ be a Gröbner basis of a submodule $M \subseteq R^m$ w.r.t some fixed monomial order. Choose a free R-module F with standard basis $e_1, \dots, e_s$ and let $\varphi : F \to M$ be the usual surjective homomorphism defined by $\varphi : e_i \mapsto \mathbf{g}_i$ for $i = 1, \dots, s$. As before $\mathrm{Syz}(\mathbf{g}_1, \dots, \mathbf{g}_s)$ denotes the kernel of φ.
In the following construction, we resume the idea from the proof of Buchberger's criterion in the ideal case. Since G is a Gröbner basis, the remainder of the S-vectors $S(\mathbf{g}_i, \mathbf{g}_j)$ on division by G is zero and the division algorithm give us an expression

$$S(\mathbf{g}_i, \mathbf{g}_j) = h_1^{(i,j)}\mathbf{g}_1 + \cdots + h_s^{(i,j)}\mathbf{g}_s, \text{ with } \mathrm{in}(h_k^{(i,j)}\mathbf{g}_k) \leq \mathrm{in}(S(\mathbf{g}_i, \mathbf{g}_j)) \tag{5.1}$$

for all i, j, k and each pair $\mathbf{g}_i, \mathbf{g}_j$ containing the same basis element of R^m.
Let $\mathbf{m}_{i,j} = \mathrm{lcm}(\mathrm{in}(\mathbf{g}_i), \mathrm{in}(\mathbf{g}_j))$, then

$$\varphi(\mathbf{s}_{i,j}) = S(\mathbf{g}_i, \mathbf{g}_j) = \frac{\mathbf{m}_{i,j}}{\mathrm{lt}(\mathbf{g}_i)}\mathbf{g}_i - \frac{\mathbf{m}_{i,j}}{\mathrm{lt}(\mathbf{g}_j)}\mathbf{g}_j. \tag{5.2}$$

Equations (5.1) and (5.2) give rise to the following relation:

$$\mathbf{r}_{i,j} = \mathbf{s}_{i,j} - (h_1^{(i,j)}, \dots, h_s^{(i,j)}) \in \mathrm{Syz}(\mathbf{g}_1, \dots, \mathbf{g}_s) \subseteq R^s, \tag{5.3}$$

where $\mathbf{r}_{i,j} = 0$ if $\mathbf{g}_i, \mathbf{g}_j$ do not contain the same basis vector of R^m.

Next, we define a monomial order on R^m, which we use later.

Definition 5.7.14. Fix a monomial order σ on R^m. Let $M \subseteq R^m$ be a submodule generated by the Gröbner basis $G = \{\mathbf{g}_1, \dots, \mathbf{g}_s\}$. Let $F = R^s$ be the free R-module with standard basis $e_1, \dots, e_s$ and define $\varphi : F \to M$ as the usual surjective homomorphism with $\varphi : e_i \mapsto \mathbf{g}_i$ for $i = 1, \dots, s$. We define the monomial order $>_G$ called *induced by* G on R^s as follows: Let $ue_i, ve_j \in \mathrm{Mon}(R^s)$. Then let

$$ue_i >_G ve_j \iff \mathrm{in}(u\mathbf{g}_i) >_\sigma \mathrm{in}(v\mathbf{g}_j) \text{ or } \mathrm{in}(u\mathbf{g}_i) = \mathrm{in}(v\mathbf{g}_j) \text{ and } i < j.$$

Lemma 5.7.15. *Let G be a Gröbner basis of $M \subseteq R^m$ and $>_G$ defined as in Definition 5.7.14. Then $>_G$ is a monomial order on R^s.*

Proof. (total order) Assume that $ue_i \not>_G ve_j$. Then we have $\mathrm{in}(u\mathbf{g}_i) \not> \mathrm{in}(v\mathbf{g}_j)$ and either $\mathrm{in}(u\mathbf{g}_i) \neq \mathrm{in}(v\mathbf{g}_j)$ or $i \geq j$.

(case 1) Then $\mathrm{in}(u\mathbf{g}_i) < \mathrm{in}(v\mathbf{g}_j)$ since σ is a total order. But then $ve_j >_G ue_i$.

(case 2) In this case we have $ve_j \geq_G ue_i$ by definition of $>_G$.

(respects multiplication) Let $w \in \mathrm{Mon}(R)$ and $ue_i, ve_j \in \mathrm{Mon}(R^s)$ s.t. $ue_i >_G ve_j$.

(case 1) $\mathrm{in}(u\mathbf{g}_i) > \mathrm{in}(v\mathbf{g}_j)$. Therefore $\mathrm{in}(wu\mathbf{g}_i) = w\,\mathrm{in}(u\mathbf{g}_i) > w\,\mathrm{in}(v\mathbf{g}_j) = \mathrm{in}(wv\mathbf{g}_j)$, which implies that $wue_i >_G wve_j$.

(case 2) $\mathrm{in}(u\mathbf{g}_i) = \mathrm{in}(v\mathbf{g}_j)$ and $i < j$. But then $\mathrm{in}(wue_i) = \mathrm{in}(wue_j)$ and $i < j$. Thus, we get $wue_i >_G wve_j$.

(well-order) Suppose we have a decreasing sequence of monomials $\mathbf{m}_1 >_G \mathbf{m}_2 >_G \cdots$ in R^s, where $\mathbf{m}_j = u_j e_{i_j}$ for some $u_j \in \mathrm{Mon}(R)$.
Then, for each j we either have $\mathrm{in}(u_j\mathbf{g}_{i_j}) > \mathrm{in}(u_{j+1}\mathbf{g}_{i_{j+1}})$ or $\mathrm{in}(u_j\mathbf{g}_{i_j}) = \mathrm{in}(u_{j+1}\mathbf{g}_{i_{j+1}})$ and $i_j < i_{j+1}$. But the second case can only occur s-times in R^s. Thus, there is an infinite decreasing sequence of monomials in R^m, which is a contradiction.
Thus, $>_G$ is indeed a monomial order. □

This monomial order can be used to show an interesting property about the relations $\mathbf{r}_{i,j}$ as described in (5.3).

Theorem 5.7.16 (Schreyer's Theorem, [16], Theorem 3.3, Chapter 5)**.** *Let $M \subseteq R^m$ be a submodule generated by the Gröbner basis $G = \{\mathbf{g}_1, \dots, \mathbf{g}_s\}$ and fix a monomial order on R^m. Let $>_G$ defined as in Definition 5.7.14. Then, the relations $\mathbf{r}_{i,j}$ as described in (5.3) form a Gröbner basis for $\mathrm{Syz}(\mathbf{g}_1, \dots, \mathbf{g}_s) \subseteq R^s$.*
Also, for $i < j$ let $\mathbf{m}_{i,j} = \mathrm{lcm}(\mathrm{in}(\mathbf{g}_i), \mathrm{in}(\mathbf{g}_j))$. Then we have that

$$\mathrm{lt}(\mathbf{r}_{i,j}) = \frac{\mathbf{m}_{i,j}}{\mathrm{lt}(\mathbf{g}_i)} e_i.$$

Proof. We only consider $\mathbf{r}_{i,j}$ for $i < j$, since $S(\mathbf{g}_i, \mathbf{g}_j)$ and $S(\mathbf{g}_j, \mathbf{g}_i)$ only differ by sign. First, we show the second claim of the statement. Since $i < j$ we have

$$\frac{\mathbf{m}_{i,j}}{\mathrm{lt}(\mathbf{g}_i)} e_i >_G \frac{\mathbf{m}_{i,j}}{\mathrm{lt}(\mathbf{g}_j)} e_j.$$

The $h_k^{(i,j)}$ come from the division algorithm s.t. $\mathrm{in}(S(\mathbf{g}_i, \mathbf{g}_j)) \geq \mathrm{in}(h_k^{(i,j)} \mathbf{g}_k)$ for all $k = 1, \dots, s$. Also, for S-vectors one has

$$\mathrm{lt}\left(\frac{\mathbf{m}_{i,j}}{\mathrm{lt}(\mathbf{g}_i)} \mathbf{g}_i\right) > \mathrm{lt}(S(\mathbf{g}_i, \mathbf{g}_j)),$$

which implies that

$$\frac{\mathbf{m}_{i,j}}{\mathrm{lt}(\mathbf{g}_i)} e_i >_G h_k^{(i,j)} e_k,$$

for all $k = 1, \dots, s$. Thus, the claim follows.

Next, consider $\mathbf{f} = \sum_{i=1}^s f_i e_i \in \mathrm{Syz}(\mathbf{g}_1, \dots, \mathbf{g}_s)$ and let $\mathrm{in}_{>_G}(f_i e_i) = m_i e_i$ for some monomial $m_i \in \mathrm{Supp}(f_i)$. Further, let $\mathrm{in}_{>_G}(\mathbf{f}) = m_v e_v$ for some v and fix this v.
Set

$$\mathbf{s} = \sum_{u \in S} m_u e_u,$$

with $S = \{u : m_u \,\mathrm{in}(g_u) = m_v \,\mathrm{in}(g_v)\}$.
Since $\mathbf{f} \in \mathrm{Syz}(\mathbf{g}_1, \dots, \mathbf{g}_s)$ and $m_u \,\mathrm{in}(\mathbf{g}_u) \geq m_i \,\mathrm{in}(\mathbf{g}_i)$ for all $i = 1, \dots, s$, it follows that the monomials $m_u \,\mathrm{in}\,(\mathbf{g}_u)$ with $u \in S$ must cancel, i.e. $\mathbf{s} \in \mathrm{Syz}(\{\mathrm{in}(\mathbf{g}_u) : u \in S\})$.

But by Proposition 5.7.7, it follows that this set is generated by syzygies of the form

$$\mathbf{s}_{u,w} = \frac{\mathbf{m}_{u,w}}{\mathrm{lt}(\mathbf{g}_u)} e_u - \frac{\mathbf{m}_{u,w}}{\mathrm{lt}(\mathbf{g}_w)} e_w,$$

where $u < w \in S$.
This implies that $\mathrm{lt}(\mathbf{f}) = \mathrm{lt}(\mathbf{s})$ is divisible by some $\mathrm{lt}(\mathbf{r}_{i,j})$ for some $i < j$. Thus, the $\mathbf{r}_{i,j}$ form a Gröbner basis of M w.r.t $>_G$. □

The next result shows that by arranging the elements of a Gröbner basis in a certain way, it is possible to eliminate variables from the leading terms of the syzygy module.

Corollary 5.7.17 ([16], Lemma 2.2, Chapter 6)**.** *Let $M \subseteq R^m$ be a submodule generated by the Gröbner basis $G = \{\mathbf{g}_1, \dots, \mathbf{g}_s\}$ and fix a monomial order σ on R^m. Let $>_G$ defined as in Definition 5.7.14.*
Arrange the elements of G in such a way, that whenever $\mathrm{in}(\mathbf{g}_i)$ and $\mathrm{in}(\mathbf{g}_j)$ for some $i < j$ contain the same standard basis vector e_k, say $\mathrm{in}(\mathbf{g}_i) = u e_k$ and $\mathrm{in}(\mathbf{g}_j) = v e_k$, then

$$\frac{\mathrm{in}(\mathbf{g}_i)}{e_k} = u >_{lex} v = \frac{\mathrm{in}(\mathbf{g}_j)}{e_k}.$$

Then, if for some $t < n$, the variables $x_1, \dots, x_t$ do not divide any of the leading terms of G, then the variables $x_1, \dots, x_{t+1}$ do not divide any of the leading terms of $\mathbf{r}_{i,j} \in \mathrm{Syz}(G)$ w.r.t $>_G$.

Proof. By the second statement of Theorem 5.7.16, we have

$$\text{in}_{>_G}(\mathbf{r}_{i,j}) = \frac{\mathbf{m}_{i,j}}{\text{in}(\mathbf{g}_i)} e_k.$$

As in the proof of Theorem 5.7.16, it suffices to consider only the relations $\mathbf{r}_{i,j}$ with $i < j$ s.t. $\text{in}(\mathbf{g}_i)$ and $\text{in}(\mathbf{g}_j)$ contain the same e_k. As the variables $x_1, \dots, x_t$ do not divide the initial monomials of $\text{in}(\mathbf{g}_i), \text{in}(\mathbf{g}_j)$, we may write

$$\frac{\text{in}(\mathbf{g}_i)}{e_k} = x_{t+1}^a n_i$$
$$\frac{\text{in}(\mathbf{g}_j)}{e_k} = x_{t+1}^b n_j,$$

where $a \geq b$, by the choice of ordering of the elements of G and the monomials n_i, n_j only contain the variables $x_{t+2}, \dots, x_n$. Then $\mathbf{m}_{i,j}$ contains x_{t+1}^a but no higher power of x_{t+1}. Thus,

$$\text{in}(\mathbf{r}_{i,j}) = \frac{\mathbf{m}_{i,j}}{\text{in}(\mathbf{g}_i)} e_i$$

does not contain $x_{t+1}, \dots, x_n$. □

If there are no more variables among the leading terms of a reduced Gröbner basis, we can show that the module this basis generates is free.

Lemma 5.7.18. *Let $G = \{\mathbf{g}_1, \dots, \mathbf{g}_s\}$ be a reduced Gröbner basis of a submodule $M \subseteq R^t$ w.r.t to a monomial order σ. Assume the leading terms are all constant multiples of the standard basis vectors $e_i \in R^t$ for some i. Then M is a free R-module.*

Proof. Since G is reduced and therefore monic, we have that $\text{in}(\mathbf{g}_i) \neq \text{in}(\mathbf{g}_j)$ for all $i \neq j$. Thus, if e_i is a leading term of some element of G, it is the leading term of exactly one element of G. Let $\text{Syz}(G) \subseteq R^s$ and let $a = (a_1, \dots, a_s) = a_1\epsilon_1 + \cdots + a_s\epsilon_s \in \text{Syz}(G)$, where ϵ_i are the standard basis vectors of R^s. Then $a_1\mathbf{g}_1 + \cdots + a_s\mathbf{g}_s = (0, \dots, 0) \in R^t$. Choose $k \in \{1, \dots, s\}$ s.t. $\text{in}(a_k)\epsilon_k >_G \text{in}(a_i)\epsilon_i$ for all $i = 1, \dots, s$, then $\text{in}(a_k\mathbf{g}_k) > \text{in}(a_i\mathbf{g}_i)$ or $\text{in}(a_k\mathbf{g}_k) = \text{in}(a_i\mathbf{g}_i)$ and $k < i$. But in the second case, we have $a_k e_{j_k} = \text{in}(a_k\mathbf{g}_k) = \text{in}(a_i\mathbf{g}_i) = a_i e_{j_i}$, which is a contradiction, since $j_k \neq j_i$ for all $i \neq k$. Thus, we have that $\text{in}(a_k\mathbf{g}_k) > \text{in}(a_i\mathbf{g}_i)$ for all $i \neq k$, which implies that $\text{in}(a_k\mathbf{g}_k) = \text{in}(a_1\mathbf{g}_1 + \cdots + a_s\mathbf{g}_s) = \text{in}(0) = 0$. Thus $a_k = 0$, which implies that $a = 0$, i.e. $\text{Syz}(G) = 0$. But since $\text{Syz}(G) = \ker(\varphi)$ for $\varphi : R^s \to M$, it follows that M is a free module. □

These results lead to the desired result that states, that an R-module M has a free resolution of finite length. Recall that we work over the standard graded polynomial ring $R = k[x_1, \dots, x_n]$.

Theorem 5.7.19 (Hilbert Syzygy Theorem, [16], Theorem 2.1, Chapter 6)**.** *Let M be a finitely generated R-module. Then M has a free resolution of finite length.*

Proof. Since M is a finitely generated module, there exists the usual surjective homomorphism $\varphi_0 : F_0 \to M$ from a free module $F_0 = R^{r_0}$ of finite rank. Let $\text{Syz}(M) = \ker(\varphi_0) \subseteq F_0$ and let $G_0 = \{\mathbf{g}_1, \dots, \mathbf{g}_{r_1}\}$ be a Gröbner basis for $\text{Syz}(M)$, w.r.t to a monomial order on F_0.
Let $F_1 = R^{r_1}$ be the free module with the surjective homomorphism $\varphi_1 : F_1 \to F_0$ s.t. $e_i \mapsto \mathbf{g}_i$. After ordering the elements of G_0 according to the hypothesis of Lemma 5.7.17, we can apply Schreyer's theorem to get a Gröbner basis G_1 for the submodule $\text{Syz}(G_0) = \ker(\varphi_1) \subseteq F_1$, w.r.t to the induced monomial order $>_{G_0}$. We may assume that G_1 is a reduced Gröbner basis. By Lemma 5.7.17, at least x_1 is not contained in the initial monomials of G_1.

Again, when G_1 contains r_2 elements, we can obtain the exact sequence

$$F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \to M \to 0,$$

where $F_2 = R^{r_2}$ and s.t. $\mathrm{Im}(\varphi_2) = \mathrm{Syz}(G_0) \subseteq F_1$. Iterating this process, we obtain maps $\varphi_i : F_i \to F_{i-1}$, with $\mathrm{Im}(\varphi_i) = \ker(\varphi_{i-1}) = \mathrm{Syz}(G_{i-2})$ and $G_{i-1} \subseteq R^{r_{i-1}} = F_{i-1}$ is a Gröbner basis of $\mathrm{Syz}(G_{i-2})$. At each step, the Gröbner basis G_{i-1} gets ordered in such a way that it satisfies the hypothesis of Lemma 5.7.17. The number of variables appearing in the initial monomials of the Gröbner basis decreases at each step by at least one. By an inductive argument, we see that after $l \leq n$ steps, the initial monomials of the reduced Gröbner basis G_l is not divisible by any variable. Our exact sequence has the form

$$F_l \xrightarrow{\varphi_l} F_{l-1} \to \cdots \to F_1 \to F_0 \to M \to 0$$

and the initial monomials of the Gröbner basis of $\ker(\varphi_l)$ are nonzero constant multiples of standard basis vectors of F_l. But then Lemmas 3.2.3 and 5.7.18 imply that the free resolution has length at most $l + 1$. □

To be able to introduce Castelnuovo–Mumford regularity in Chapter 7, we need a graded module M to have a finite graded free resolution. Luckily, as in the ungraded case, the process of building a graded free resolution of modules over the polynomial ring $k[x_1, \ldots, x_n]$ stops eventually.

Theorem 5.7.20 (Graded Hilbert Syzygy Theorem, [16], Theorem 3.8, Chapter 6)**.** *Let M be a finitely generated graded R-module. Then M has a graded free resolution of finite length.*

Proof. By a similar argument as in the proof of Proposition 5.3.9, the reduced Gröbner basis G of a graded submodule $M \subseteq \bigoplus_{i=1}^{m} R(-d_i)$ consists of homogeneous elements. If we apply Schreyer's theorem to this Gröbner basis, similarly to Proposition 5.3.9, we see that the resulting relations $\mathbf{r}_{i,j}$ that form a Gröbner basis of $\mathrm{Syz}(G)$ are also homogeneous. The rest of the proof then follows the ungraded case. □

Corollary 5.7.21. *Let $R = k[x_1, \ldots, x_n]$ be standard graded. Let M be a finitely generated graded R-module. Then M has a finite minimal graded free resolution that is unique up to isomorphism.*

Proof. The result follows immediately from the graded Hilbert syzygy theorem and Propositions 3.2.9 and 3.2.10. □

Chapter 6

Hilbert Function

This chapter deals with Hilbert functions and Hilbert polynomials. They are important invariants of graded modules over graded polynomial rings and contain a lot of information. We start by studying these concepts for ideals, where we consider the affine and projective case and explain the relationship to the concept of dimension. Then, we generalize it to graded modules and introduce the Hilbert series. If not mentioned otherwise we assume that $R = k[x_1, \ldots, x_n]$.

6.1 Hilbert Function for Ideals

Before we introduce the Hilbert function and Hilbert polynomial in the general case of modules, we look at it for ideals, where we follow [15, Chapters 9.3 and 9.4].

6.1.1 The Affine Hilbert Function

First, we look at ideals that are not necessarily homogeneous.

Definition 6.1.1. Let I be an ideal of R. The *affine Hilbert function* of I is the function on nonnegative integers $s \in \mathbb{Z}$ defined by

$$ {}^aHF_{R/I}(s) = \dim_k(R_{\leq s}/I_{\leq s}) = \dim_k(R_{\leq s}) - \dim_k(I_{\leq s}). $$

When I is a monomial ideal, then clearly for $s \geq 0$, ${}^aHF_{R/I}(s)$ is the number of monomials not in I of degree $\leq s$.

Proposition 6.1.2 ([15], Proposition 3, Chapter 9.3)**.** *Let I be a monomial ideal of R. For s sufficiently large, ${}^aHF_{R/I}(s)$ is a polynomial in s, where the degree is the maximal dimension of coordinate subspaces in $\mathcal{V}(I)$.*

Proof. This follows directly from the definition of ${}^aHF_{R/I}$ and Theorem 4.5.11. □

Proposition 6.1.3 ([15], Proposition 4, Chapter 9.3)**.** *Let I be an ideal of R and fix a monomial order on R. Then the ideal $\operatorname{in}(I)$ has the same affine Hilbert function as I.*

Proof. We know by Proposition 5.2.5 that the set of monomials that do not belong to $\operatorname{in}(I)$ form a k-basis of R/I. Thus, those in $R_{\leq s}$ not belonging to $\operatorname{in}(I)_{\leq s}$ form a k-basis of $R_{\leq s}/I_{\leq s}$. By Lemma 2.5.12, they also form a k-basis of $R_{\leq s}/\operatorname{in}(I)_{\leq s}$. Therefore, we have

$$ {}^aHF_{R/I}(s) = \dim_k(R_{\leq s}/I_{\leq s}) = \dim_k(R_{\leq s}/\operatorname{in}(I)_{\leq s}) = {}^aHF_{R/\operatorname{in}(I)}(s). $$ □

Thus, for any ideal I and s sufficiently large, ${}^aHF_{R/I}(s)$ will become a polynomial.

Definition 6.1.4. The polynomial which equals ${}^aHF_{R/I}(s)$ for all s sufficiently large, is called the *affine Hilbert polynomial* of I and is denoted by ${}^aHP_{R/I}(s) \in \mathbb{Q}[s]$.

Example 6.1.5. Fix the *DRL*-order on $R = k[x, y, z]$ and let $I = \langle x^2 - z^2, xy + xz \rangle$. To compute $HP_{R/I}$ we look at $\text{in}_{DRL}(I) = \langle x^2, xy, yz^2 \rangle$. Counting the monomials of degree $\leq s$ not in $\text{in}_{DRL}(I)$, we get

$$\begin{aligned} {}^aHF_{R/\text{in}(I)}(0) &= 1 \\ {}^aHF_{R/\text{in}(I)}(1) &= 3 \\ {}^aHF_{R/\text{in}(I)}(2) &= 8 \\ {}^aHF_{R/\text{in}(I)}(3) &= 12 \\ &\vdots \\ {}^aHF_{R/\text{in}(I)}(s) &= 4s. \end{aligned}$$

Thus, ${}^aHP_{R/I}(s) = 4s$, which is a polynomial of degree 1.

Lemma 6.1.6. *Let $I \subseteq J \subseteq R$ be ideals. Then* $\deg({}^aHP_{R/I}) \geq \deg({}^aHP_{R/J})$.

Proof. Suppose that the opposite is the case. Then we have that ${}^aHF_{R/J}(s) = {}^aHF_{R/\text{in}(J)}(s)$ is the number of monomials not in $\text{in}(J)$ of total degree $\leq s$. But the monomials not in $\text{in}(J)$ are also not in $\text{in}(I)$. Thus, ${}^aHF_{R/J}(s) \leq {}^aHF_{R/I}(s)$ for all $s \geq 0$. Now, since the term of highest degree has a positive coefficient, our assumption implies that for $s \to \infty$ we have ${}^aHP_{R/I} < {}^aHP_{R/J}$, which is a contradiction, as ${}^aHF_{R/J}(s) \leq {}^aHF_{R/I}(s)$ for all s and this coincides with the Hilbert polynomial for s sufficiently large. □

Lemma 6.1.7 ([15], Proposition 6, Chapter 9.3)**.** *Let I be an ideal of R. Then the affine Hilbert polynomial of I and $\sqrt{I}$ have the same degree.*

Proof. Let I be a monomial ideal. Then $\deg({}^aHP_{R/I})$ corresponds to the dimension of the largest coordinate subspace of k^n inside $\mathcal{V}(I)$. Since $\mathcal{V}(\sqrt{I}) = \mathcal{V}(I)$ and $\sqrt{I}$ is monomial, the claim follows in the monomial case.

Now, consider an ideal I which is not necessarily monomial, and fix a degree-compatible monomial order. We will show that $\text{in}(I) \subseteq \text{in}(\sqrt{I}) \subseteq \sqrt{\text{in}(I)}$.

The inclusion $\text{in}(I) \subseteq \text{in}(\sqrt{I})$ is obvious, as $I \subseteq \sqrt{I}$. Now, let $u \in \text{in}(\sqrt{I})$ be a monomial. There exists a polynomial $f \in \sqrt{I}$ s.t. $\text{in}(f) = u$. Since $f^r \in I$ for some $r \geq 0$, it follows that $u^r = \text{in}(f)^r = \text{in}(f^r) \in \text{in}(I)$. Thus, $u \in \sqrt{\text{in}(I)}$ and the claim follows.

Set $J = \text{in}(I)$ to obtain $J \subseteq \text{in}(\sqrt{I}) \subseteq \sqrt{J}$. Applying Lemma 6.1.6, we get

$$\deg({}^aHP_{R/J}) \geq \deg({}^aHP_{R/\text{in}(\sqrt{I})}) \geq \deg({}^aHP_{R/\sqrt{J}}),$$

where the outer terms are equal, since we have already shown the result for monomial ideals. Thus, we have shown that the Hilbert polynomial of $\text{in}(I)$ and $\text{in}(\sqrt{I})$ have the same degree. By Proposition 6.1.3, the same holds for I and $\sqrt{I}$. □

We now can define the dimension of affine varieties for all ideals.

Definition 6.1.8. The dimension of an affine variety $V \subseteq k^n$, denoted $\dim^a(V)$, is defined to be the degree of the affine Hilbert polynomial of the ideal $\mathcal{I}(V)$.

Theorem 6.1.9 (Dimension Theorem, [15], Theorem 8, Chapter 9.3)**.** *Let $V = \mathcal{V}(I)$ for an ideal I of R. If k is algebraically closed, then* $\dim^a(V) = \deg({}^aHP_{R/I})$. *Fix a degree compatible monomial order. Then* $\dim^a(V) = \deg({}^aHP_{R/\text{in}(I)})$, *which equals the maximal dimension of a coordinate subspace in $\mathcal{V}(\text{in}(I))$.*

Proof. By the Nullstellensatz we have that $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$ as k is algebraically closed. Then by Lemma 6.1.7 we have

$$\dim^a(V) = \deg({}^aHP_{R/\mathcal{I}(V)}) = \deg({}^aHP_{R/\sqrt{I}}) = \deg({}^aHP_{R/I}).$$

The second statement follows from Proposition 6.1.3 and Lemma 4.5.3. □

The next result characterizes affine varieties of dimension zero as those consisting of finitely many points.

Proposition 6.1.10 ([15], Proposition 6, Chapter 9.4)**.** *Let V be a nonempty affine variety. Then V contains finitely many points if and only if* $\dim^a(V) = 0$.

Proof. Fix a degree-compatible monomial order on R.

($\Rightarrow$) Fix $i \in \{1, \dots, n\}$. Since V contains only finitely many points, there are only finitely many distinct i-th coordinates for points in V, say a_j, $j = 1, \dots, m_i$. Consider the polynomial

$$f = \prod_{j=1}^{m_i}(x_i - a_j) \in \mathcal{I}(V) = I.$$

Since we chose a degree-compatible order, we can conclude that $\text{in}(f) = x_i^{m_i} \in \text{in}(\mathcal{V}(I))$. This works for all $i = 1, \dots, n$. It follows that $\mathcal{V}(\text{in}(\mathcal{I}(V)) = \{0\}$. Then the second part of Theorem 6.1.9 implies that $\dim^a(V) = 0$.

($\Leftarrow$) If $\dim^a(V) = 0$, then ${}^aHF_{R/\mathcal{I}(V)} = C$ for some $C \in \mathbb{N}$, i.e.

$$\dim_k(R_{\leq s}/\mathcal{I}(V)_{\leq s}) = C$$

for s sufficiently large. If also $s \geq C$, then the residue classes $[1], [x_i], \dots, [x_i^s] \in R_{\leq s}/\mathcal{I}(V)_{\leq s}$ are $s+1$ elements in a C-dimensional vector space with $C \leq s$. This forces them to be linearly dependent, i.e. there is a nontrivial linear combination

$$[0] = \sum_{j=0}^{s} a_j[x_i^j] = \left[\sum_{j=0}^{s} a_j x_i^j\right].$$

This implies that $f = \sum_{j=0}^{s} a_j x_i^j \in \mathcal{I}(V)_{\leq s}$. Therefore, f vanishes on V, which implies that for points in V, there can only be finitely many different i-th coordinates.
Since the argument works for all $i = 1, \dots, n$, V can only contain finitely many points. □

6.1.2 The Projective Hilbert Function

Similar to the affine case we can establish some results for projective varieties. In this case, we work with homogeneous polynomials in $S = k[x_0, \dots, x_n]$ of degree s instead of degree $\leq s$. All ideals in S are assumed to be homogeneous.

Definition 6.1.11. Let I be a graded ideal of S. The *Hilbert function* of I is defined to be

$$HF_{S/I}(s) = \dim_k(S_s/I_s).$$

Remark 6.1.12. $HF_{S/I}(s)$ is the number of monomials not in I of degree s.

It follows from Corollary 4.5.13 that for a monomial ideal I and s sufficiently large, $HF_{S/I}$ can be expressed as a polynomial of degree d, where d is the largest dimension of a projective coordinate subspace of $\mathcal{V}_p(I) \subseteq \mathbb{P}^n(k)$.

Proposition 6.1.13 ([30], Corollary 6.1.5)**.** *Let I be a graded ideal of S and fix a monomial order. Then the Hilbert functions of I and $\operatorname{in}(I)$ are the same.*

Proof. This follows directly from Proposition 5.2.5. □

Lemma 6.1.14 ([15], Theorem 12, Chapter 9.3)**.** *Let I be a graded ideal of S. For $s \geq 1$ we have*

$$HF_{S/I}(s) = {}^aHF_{S/I}(s) - {}^aHF_{S/I}(s-1).$$

Proof. This is clear, by reducing it to the monomial case of $\operatorname{in}(I)$. As the monomials not in $\operatorname{in}(I)$ of degree are those of degree $\leq s$ without those of degree $\leq s-1$, the result follows. □

Definition 6.1.15. The polynomial which equals $HF_{S/I}(s)$ for s sufficiently large is called the *Hilbert polynomial* of I denoted $HP_{S/I}$, with the convention that if $HP_{S/I} = 0$, then $\deg(HP_{S/I}) = -1$.

Example 6.1.16. Continuing the previous example we let $I = \langle x^2 - z^2, xy + xz \rangle \subseteq R = k[x, y, z]$ with $\operatorname{in}_{DRL}(I) = \langle x^2, xy, yz^2 \rangle$. Counting monomials of degree s not in $\operatorname{in}_{DRL}(I)$, we get

$$\begin{aligned} HF_{R/\operatorname{in}(I)}(0) &= 1 \\ HF_{R/\operatorname{in}(I)}(1) &= 3 \\ HF_{R/\operatorname{in}(I)}(2) &= 4 \\ HF_{R/\operatorname{in}(I)}(3) &= 4 \\ &\vdots \\ HF_{R/\operatorname{in}(I)}(s) &= 4. \end{aligned}$$

Thus,

$$HP_{R/I}(s) = {}^aHP_{R/I}(s) - {}^aHP_{R/I}(s) = 4s - 4(s-1) = 4,$$

which is a constant polynomial of degree 0.

Next we show some properties of the degree of the Hilbert polynomial.

Lemma 6.1.17. *Let $I \subseteq J \subseteq S$ be graded ideals. Then $\deg(HP_{S/I}) \geq \deg(HP_{S/J})$.*

Proof. Any monomial not in $\operatorname{in}(J)$ is also not contained in $\operatorname{in}(I)$. Then $HF_{S/J}(s) \leq HF_{S/I}(s)$ for all $s \geq 0$. Then the result follows by the same argument as in the proof of Lemma 6.1.6. □

Proposition 6.1.18. *Let I be a graded ideal of S. Then $\deg(HP_{S/I}) = \deg(HP_{S/\sqrt{I}})$.*

Proof. By Lemma 6.1.14 we have $HF_{S/I}(s) = {}^aHF_{S/I}(s) - {}^aHF_{S/I}(s-1)$. Combining Lemma 6.1.7 with the proof of Corollary 4.5.13 yields

$$\deg(HP_{S/I}) = \deg({}^aHP_{S/I}) - 1 = \deg({}^aHP_{S/\sqrt{I}}) - 1 = \deg(HP_{S/\sqrt{I}}).$$ □

Similar to the affine case we can define the dimension of projective varieties.

Definition 6.1.19. The dimension of a nonempty projective variety $V \subseteq \mathbb{P}^n$, denoted $\dim^p(V)$ is defined to be the degree of the Hilbert polynomial of the corresponding homogeneous ideal $\mathcal{I}_p(V) \subseteq S$. By convention we set $\dim^p(\emptyset) = -1$.

Theorem 6.1.20 (Dimension Theorem, [15], Theorem 11, Chapter 9.3)**.** *Let I be a graded ideal of S and consider the projective variety $V = \mathcal{V}_p(I) \subseteq \mathbb{P}^n$. If k is algebraically closed, then $\dim^p(V) = \deg(HP_{S/I})$.*
Furthermore, for a monomial order on S, one has $\dim^p(V) = \deg(HP_{S/\operatorname{in}(I)})$, which equals the maximal dimension of a projective coordinate subspace in $\mathcal{V}_p(\operatorname{in}(I))$.

Proof. If $V = \emptyset$, then the result is clear. So suppose that V is nonempty. By the projective Nullstellensatz, we have that $\sqrt{I} = \mathcal{I}_p(V)$. By Proposition 6.1.18, the Hilbert polynomials of I and $\sqrt{I}$ have the same degree. Thus, we have that

$$\dim^p(V) = \deg(HP_{S/\mathcal{I}(V)}) = \deg(HP_{S/\sqrt{I}}) = \deg(HP_{S/I}).$$

The rest follows, as I and $\text{in}(I)$ have the same Hilbert function. □

Example 6.1.21. As in the previous example let $I = \langle x^2 - z^2, xy + xz\rangle \subseteq R = k[x, y, z]$. We have seen in Example 4.2.4 that $\mathcal{V}_p(I) = \{(0 : 1 : 0), (1 : -1 : 1), (1 : 1 : -1)\}$. Now, by Theorem 6.1.20 we see that $\dim^p(\mathcal{V}_p(I)) = \deg(HP_{R/I}) = 0$.

We have just seen a finite projective variety of dimension zero. We now show that, as in the affine case, this is actually an equivalent definition.

Proposition 6.1.22 ([15], Proposition 6, Chapter 9.4)**.** *Let V be a nonempty projective variety. Then V contains finitely many points if and only if* $\dim^p(V) = 0$.

Proof. Fix a monomial order with $x_1 > x_2 > \cdots > x_n > x_0$.

($\Rightarrow$) Let $V = \{p_1, \ldots, p_s\}$ for $p_i = (c'_{i0} : c'_{i1} : \cdots : c'_{in}) \in \mathbb{P}^n$. Then, by Corollary 4.4.4, there exists a linear form $l \in S_1$ s.t. $l(p_i) \neq 0$ for all $p_i \in V$. After performing a linear change of coordinates, we may assume that $l = x_0$. So $V \cap H^n_{inf} = \emptyset$, i.e. V contains no points at infinity. Thus, all $p_i \in V$ can be uniquely written in the form $p_i = (1 : c_{i1} : \cdots : c_{in}) \in \mathbb{P}^n$ for $c_{ij} = c'_{ij}/c'_{i0} \in k$.
Let $a_j, j = 1, \ldots, m_i$ be the distinct elements of k that appear as i-th coordinates of points in V, for $i = 1 \ldots, n$. Then

$$f = \prod_{j=1}^{m_i}(x_i - a_j x_0) \in \mathcal{I}_p(V) \text{ for all } i = 1, \ldots, n.$$

Thus we can conclude that $\text{in}(f) = x_i^{m_i} \in \text{in}(\mathcal{I}_p(V))$ for all $i = 1, \ldots, n$ and $x_0 \notin \text{in}(\mathcal{I}_p(V))$. This implies that $\mathcal{V}_p(\text{in}(\mathcal{I}_p(V)) = \mathcal{V}_p(x_1, \ldots, x_n)$, which is a zero-dimensional projective coordinate subspace of $\mathbb{P}^n$.

($\Leftarrow$) Suppose $\dim^p(V) = 0$. Then the $HP_{R/\mathcal{I}_p(V)} = C$ for some constant $C \in \mathbb{N}$ s.t. $\dim_k(R_s/I_s) = C$ for s sufficiently large. If we additionally have that $s \geq C$, then the residue classes $[x_0^s], [x_0^{s-1}x_i], \ldots, [x_i^s] \in R_s/\mathcal{I}_p(V)_s$ are $s + 1$ elements in a C-dimensional vector space with $C \leq s$. This forces them to be linearly dependent, i.e. there is a nontrivial linear combination

$$[0] = \sum_{j=0}^{s} a_j[x_0^j x_i^{s-j}] = \left[\sum_{j=0}^{s} a_j x_0^j x_i^{s-j}\right].$$

But this implies that $f = \sum_{j=0}^{s} a_j x_0^j x_i^{s-j}$ is a nonconstant homogeneous polynomials in $\mathcal{I}_p(V)_s$. Let $p = (c_0 : c_1 : \cdots : c_n) \in V$. Since $(0 : 0 : \cdots : 0) \notin \mathbb{P}^n$ we may assume that $c_0 \neq 0$, i.e. we may assume that $c_0 = 1$. Then $f(p) = \sum_{j=0}^{s} a_j c_i^{s-j} = 0$, which yields finitely many possibilities for c_i. Since this is true for all $i = 1, \ldots, n$ it is clear that $\{p \in V : c_0 = 1\}$ is finite. If $c_0 = 0$, then $c_i \neq 0$ for some $i = 1, \ldots, n$ and we may apply the same concept. Therefore, all the sets $V^{(i)} = \{p \in V : p = (x_0 : x_1 : \cdots : x_n), x_i = 1\}$ are finite, so V is finite. □

6.1.3 Hilbert Polynomial and Krull Dimension

We have characterized varieties of dimension zero. To study the properties of varieties of higher dimension, we first take a look at projective varieties defined by a single polynomial.

Lemma 6.1.23 ([15], Proposition 2, Chapter 9.4)**.** *Let k be algebraically closed and let $f \in S$ be a nonconstant homogeneous polynomial. Then* $\dim^p(\mathcal{V}_p(f)) = n-1$.

Proof. Fix some monomial order on S. The dimension theorem implies that $\dim^p(V)$ is the maximal dimension of a projective coordinate subspace in $\mathcal{V}_p(\text{in}(I))$, where $I = \langle f \rangle$. Since $\text{in}(I) = \langle \text{in}(f) \rangle$ and $\text{in}(f) \in \text{Mon}(S)$ is nonconstant, $\mathcal{V}_p(\text{in}(f))$ can be expressed as a finite union of projective coordinate subspaces of $\mathbb{P}^n(k)$ of dimension $n-1$. Thus, $\dim^p(V) = n-1$. □

Proposition 6.1.24 ([15], Corollary 4, Chapter 9.4)**.** *Let k be algebraically closed and let I be a graded ideal of S. Let $f \in S$ be a nonconstant homogeneous polynomial, s.t. $\overline{f} = f + I$ is S/I-regular. Then*

$$\dim^p(\mathcal{V}_p(\langle I, f \rangle)) = \dim^p(\mathcal{V}_p(I)) - 1,$$

when $\dim^p(\mathcal{V}_p(I)) > 0$.
Furthermore, If $\dim^p(\mathcal{V}_p(I)) = 0$*, then* $\mathcal{V}_p(\langle I, f \rangle) = \emptyset$.

Proof. We get the short exact sequence $0 \to S/I \xrightarrow{f} S/I \to (S/I)/f(S/I) \cong S/\langle I, f \rangle \to 0$, since $\overline{f}$ is S/I-regular. Corollary 6.2.12, which we will show in a more general case, implies that $\deg(HP_{S/\langle I,f \rangle}) = \deg(HP_{S/I}) - 1$. Thus, $\dim^p(\mathcal{V}_p(\langle I, f \rangle)) = \deg(HP_{S/I}) - 1 = \dim^p(\mathcal{V}_p(I)) - 1$. If $\dim^p(\mathcal{V}_p(I)) = 0$, this implies that $\deg(HP_{S/\langle I,f \rangle}) = -1$, i.e by convention $HP_{S/\langle I,f \rangle} = 0$. Thus, $HF_{S/\langle I,f \rangle}(s) = 0$, i.e. $S_s = \langle I, f \rangle_s$ for all s sufficiently large. Thus, $\mathfrak{m} \subseteq \sqrt{\langle I, f \rangle}$, which implies that $\mathcal{V}_p(\sqrt{\langle I, f \rangle}) = \mathcal{V}_p(\langle I, f \rangle) = \mathcal{V}_p(\mathfrak{m}) = \emptyset$. □

Proposition 6.1.25 ([15], Proposition 8, Chapter 9.4)**.** *Let $V, W \subseteq \mathbb{P}^n$ be nonempty varieties. Then*

$$\dim^p(V \cup W) = \max\{\dim^p(V), \dim^p(W)\}.$$

Proof. ($\leq$) Let $I = \mathcal{I}_p(V), J = \mathcal{I}_p(W)$ s.t. $\dim^p(V) = \deg(HP_{S/I})$, $\dim^p(W) = \deg(HP_{S/I})$. We know that $\mathcal{I}_p(V \cup W) = \mathcal{I}_p(V) \cap \mathcal{I}_p(W) = I \cap J$ and that $IJ \subseteq I \cap J \subseteq \sqrt{IJ}$. Also, by Lemma 2.1.8, we have $\sqrt{IJ} = \sqrt{I \cap J}$. Therefore, we see that

$$\deg(HP_{S/IJ}) \geq \deg(HP_{S/(I \cap J)}) \geq \deg(HP_{S/\sqrt{IJ}}),$$

where the two outer terms are equal by Proposition 6.1.18. Thus, $\dim^p(V \cup W) = \deg(HP_{S/IJ})$.

Fix a monomial order on S. It follows by Theorem 6.1.20 that $\dim^p(V), \dim^p(W)$, and $\dim^p(V \cup W)$ are equal to the maximal dimension of a projective coordinate subspace in $\mathcal{V}_p(\text{in}(I))$, $\mathcal{V}_p(\text{in}(J))$ and $\mathcal{V}_p(\text{in}(IJ))$, respectively. Since we have $\text{in}(I)\,\text{in}(J) \subseteq \text{in}(IJ)$, we get the following inclusion: $\mathcal{V}_p(\text{in}(IJ)) \subseteq \mathcal{V}_p(\text{in}(I)) \cup \mathcal{V}_p(\text{in}(J))$. Each coordinate subspace is irreducible, which implies that each coordinate subspace in $\mathcal{V}_p(\text{in}(IJ))$ lies in $\mathcal{V}_p(\text{in}(I))$ or $\mathcal{V}_p(\text{in}(J))$. This implies that $\dim^p(V \cup W) \leq \max\{\dim^p(V), \dim^p(W)\}$.

($\geq$) The inclusion $V, W \subseteq V \cup W$ implies that $\mathcal{I}_p(V) \supseteq \mathcal{I}_p(V \cup W)$, i.e. it yields the inequality $\dim^p(V) = \deg(HP_{S/I}) \leq \deg(HP_{S/IJ}) = \dim^p(V \cup W)$. Similar for $\dim^p(W)$. □

Corollary 6.1.26 ([15], Corollary 9, Chapter 9.4)**.** *The dimension of a projective variety is the largest dimension of its irreducible components.*

Proof. Let $V = V_1 \cup \cdots \cup V_r$ be the decomposition of V into irreducible components. Iteratively applying Proposition 6.1.25 implies that that

$$\dim^p(V) = \max\{\dim^p(V_1), \ldots, \dim^p(V_r)\}.$$ □

Proposition 6.1.27 ([15], Proposition 10, Chapter 9.4)**.** *Let k be algebraically closed and let $V \subseteq \mathbb{P}^n$ be an irreducible variety.*

(a) *If $f \in S$ is a homogeneous polynomial and does not vanish on all of V, then we get* $\dim^p(V \cap \mathcal{V}_p(f)) = \dim^p(V) - 1$, *when* $\dim^p(V) > 0$. *If* $\dim^p(V) = 0$, *then* $V \cap \mathcal{V}_p(f) = \emptyset$.

(b) *If W is a projective variety s.t. $W \subsetneq V$, then* $\dim^p(W) < \dim^p(V)$.

Proof. (a) Since V is irreducible, $\mathcal{I}_p(V)$ is a prime ideal and thus, $S/\mathcal{I}_p(V)$ is an integral domain. Since $f \notin \mathcal{I}_p(V)$, the residue class of f is a nonzerodivisor. The result then follows by Proposition 6.1.24.

(b) If $W \subsetneq V$, then there is $f \in \mathcal{I}_p(W) \setminus \mathcal{I}_p(V)$. Therefore, $W \subseteq V \cap \mathcal{V}_p(f)$. It follows that $\dim^p(W) \leq \dim^p(V \cap \mathcal{V}_p(f)) = \dim^p(V) - 1 < \dim^p(V)$. □

With the previous result, we can now define the dimension of a projective variety in a way that resembles the definition of Krull dimension.

Theorem 6.1.28. *If k is algebraically closed and $V \subseteq \mathbb{P}^n$ is irreducible then* $\dim^p(V)$ *is the number of proper inclusions in the longest chain of irreducible varieties contained in V.*

Proof. We first claim that if $\dim^p(V) > 0$, then there exists an irreducible variety $W \subsetneq V$ s.t. $\dim^p(W) = \dim^p(V) - 1$.

To show this, let f be a homogeneous polynomial not vanishing on all points of V. Then, Proposition 6.1.27 implies that $\dim^p(V \cap \mathcal{V}_p(f)) = \dim^p(V) - 1$. Let

$$V \cap \mathcal{V}_p(f) = W_1 \cup \cdots \cup W_r$$

be its decomposition into irreducible components. Then, by Lemma 6.1.26, we have that $\dim^p(V \cap \mathcal{V}_p(I))$ is the largest dimension of its irreducible components. Thus, one of the $W_i \subsetneq V$ satisfies $\dim^p(W_i) = \dim^p(V) - 1$, which concludes the claim.

Next, we show that there is such a chain of length at least equal to $\dim^p(V)$.
Let $\dim^p(V) = m$. If $m = 0$, take $V_0 = V$ and the claim follows. So let $m > 0$. By the claim before, there exists an irreducible variety $V_{m-1} \subsetneq V_m = V$ s.t. $\dim^p(V_{m-1}) = m - 1$. Applying this argument again to V_{m-1} and continuing iteratively, we find a chain of irreducible varieties $V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_{m-1} \subsetneq V_m = V$ s.t. $\dim^p(V_i) = i$. This chain consists of m proper inclusions, so the claim follows.

Now, we show that there is no such chain with more than m proper inclusions. Suppose by contradiction, there is such a chain $V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_{m+1} = V$ of irreducible varieties. Then $0 \leq \dim^p(V_0) \leq \dim^p(V_1) \leq \cdots \leq \dim^p(V_{m+1}) = \dim^p(V) = m$. Thus, for some $i \leq m$ we have $\dim^p(V_i) = \dim^p(V_{i+1})$ with $V_i \subsetneq V_{i+1}$. But this is a contradiction to Proposition 6.1.27. Thus, the result follows. □

Corollary 6.1.29. *Let I be a graded ideal of S. Then*

$$\operatorname{kdim}(S/I) = \deg(HP_{S/I}) + 1.$$

Proof. We have $HP_{S/I} = 0$, i.e. $\deg(HP_{S/I}) = -1$ if and only if there is no irreducible variety contained in $\mathcal{V}(I)$, i.e. there is no graded prime ideal apart from $\mathfrak{m}$ in S containing I. But this is the case if and only if $\operatorname{kdim}(S/I) = 0$ by Proposition 2.4.7.

Let $\deg(HP_{S/I}) = m \geq 0$. Thus, Theorem 6.1.28 implies that there exists a chain of varieties $V_0 \subsetneq \cdots \subsetneq V_m \subseteq \mathcal{V}_p(I) = V$, where V_m is the irreducible component of highest dimension in V. This chain of irreducible varieties cannot be elongated and by Corollary 4.2.10 corresponds to a chain of graded prime ideals $\mathcal{I}_p(V_0) \supsetneq \cdots \supsetneq \mathcal{I}_p(V_m) \supseteq \mathcal{I}_p(\mathcal{V}_p(I)) \supseteq I$ containing I that cannot be elongated. By adding the irrelevant ideal $\mathfrak{m}$ to this chain of homogeneous prime ideals, we get $\operatorname{kdim}(S/I) \geq \deg(HP_{S/I}) + 1$.

Conversely, let $\operatorname{kdim}(S/I) = m > 0$. Then there exists a chain of prime ideals $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_m$, where $\mathfrak{p}_m$ is maximal. By Proposition 2.4.7 we can chose $\mathfrak{p}_0, \ldots, \mathfrak{p}_{m-1}$ as graded primes. By Proposition 4.2.10, these primes ideals correspond to irreducible varieties $\mathcal{V}_p(\mathfrak{p}_{m-1}) \subsetneq \cdots \subsetneq \mathcal{V}_p(\mathfrak{p}_0) \subseteq \mathcal{V}_p(I)$. So, $\dim^p(\mathcal{V}_p(I)) \geq \operatorname{kdim}(S/I) - 1$. □

Example 6.1.30. To compute $\operatorname{kdim}(S)$ we look at the degree of the Hilbert polynomial HP_S. As mentioned in the proof of Lemma 4.5.8, the number of polynomials of degree s in S is $\binom{n+s}{s} = \binom{n+s}{n}$, which is a polynomial of degree n in s. Thus $\operatorname{kdim}(S) = n + 1$.

6.2 Hilbert Function for Modules

The concept of Hilbert function and Hilbert polynomials are useful for several additional purposes. For this, it makes sense to generalize these notions to modules. For reference, we refer to [34, Chapter 5].

Definition 6.2.1. Let M be a graded module. The *Hilbert function* of M is defined to be

$$HF_M(d) = \dim_k(M_d) \text{ for } d \in \mathbb{Z}.$$

Proposition 6.2.2 ([34], Proposition 5.1.14)**.** *Let A, B, C be finitely generated graded R-modules.*

(a) $HF_{A(j)}(d) = HF_A(d + j)$ *for all* $d \in \mathbb{Z}$.

(b) *Let* $0 \to A \to B \to C$ *be an exact sequence. Then*

$$HF_B(d) = HF_A(d) + HF_C(d)$$

for all $d \in \mathbb{Z}$.

(c) *Let* $A^{(1)}, \ldots, A^{(r)}$ *be finitely generated graded R-modules. Then*

$$HF_{A^{(1)} \oplus \cdots \oplus A^{(r)}}(d) = HF_{A^{(1)}}(d) + \cdots + HF_{A^{(r)}}(d), \text{ for all } d \in \mathbb{Z}.$$

Proof. (a) This is immediate, as $\dim_k(A(j)_d) = \dim_k(A_{d+j})$.

(b) Since the maps in the exact sequence are homogeneous homomorphisms, we have an exact sequence $0 \to A_d \to B_d \to C_d \to 0$ for every $d \in \mathbb{Z}$. As $\dim_k(B_d) = \dim_k(\ker(B_d \to C_d)) + \dim_k((\operatorname{Im}(A_d \to B_d))$, the claim follows.

(c) We show this for the case of two module $A^{(1)}, A^{(2)}$. Then the result follows iteratively. The exact sequence $0 \to A^{(1)} \to A^{(1)} \oplus A^{(2)} \to A^{(2)} \to 0$ combined with (b) yields the result for this case. □

Corollary 6.2.3 ([2], Proposition 2.11)**.** *Let* $0 \to A^{(0)} \xrightarrow{f_0} A^{(1)} \xrightarrow{f_1} \cdots \xrightarrow{f_{r-1}} A^{(r)} \to 0$ *be an exact sequence of graded R-modules. Then we have*

$$\sum_{i=0}^{r} (-1)^i HF_{A^{(i)}}(d) = 0 \text{ for all } d \in \mathbb{Z}.$$

Proof. Fix $d \in \mathbb{Z}$ and split up the exact sequence in short exact sequences of the form

$$0 \to \ker(f_i)_d \to A_d^{(i)} \to \operatorname{Im}(f_i)_d \to 0,$$

where $\ker(f_0) = \operatorname{Im}(f_n) = 0$. Then by Proposition 6.2.2, we have

$$HF_{A^{(i)}}(d) = HF_{\ker(f_i)}(d) + HF_{\operatorname{Im}(f_i)}(d).$$

Taking the alternating sum, with the fact that $\operatorname{Im}(f_i) = \ker(f_{i+1})$, the result follows. □

The Hilbert function provides information about the homogeneous components of a graded module. Some of this information can be stored in the generating series of the Hilbert function.

Definition 6.2.4. Let M be a graded R-module. The *Hilbert series* of M is defined to be the generating function of $HF_M(d)$, denoted

$$HS_M(t) = \sum_{d\in\mathbb{Z}} HF_M(d)t^d.$$

Theorem 6.2.5 (Hilbert–Serre, [2], Theorem 11.1)**.** *Let M be a finitely generated graded R-module. $HS_M(t)$ is a rational function in t of the form*

$$HS_M(t) = \frac{h(t)}{\prod_{i=1}^{n}(1-t)^d}, \text{ where } h(t) \in \mathbb{Z}[t, t^{-1}].$$

Proof. This is shown by induction on the number of variables n. Let $n = 0$. Then $R_d = 0$ for all $d > 0$ s.t. $R = R_0$ and M is a finitely generated R_0-module. This implies that $\dim_k(M_d) = 0$ for all d large enough, s.t. $HS_M(t)$ is in $\mathbb{Z}[t, t^{-1}]$.

Let that $n > 0$ and assume that the result is true for $n - 1$. Multiplication by x_n yields an R-module endomorphism $f : M \to M$. Let $K = \ker(f)$, $C = \operatorname{coker}(f)$. Then K, M and C are graded R-modules and yield the exact sequence

$$0 \to K \to M \xrightarrow{f} M \to C \to 0,$$

which implies that

$$0 \to K_d \to M_d \xrightarrow{x_n} M_{d+1} \to C_{d+1} \to 0 \tag{6.1}$$

is exact for all $d \in \mathbb{Z}$. Applying Corollary 6.2.3 to (6.1) yields

$$HF_K(d) - HF_M(d) + HF_M(d+1) - HF_C(d+1) = 0 \text{ for all } d \in \mathbb{Z}.$$

Multiplying by t^{d+1} and adding up w.r.t d we get

$$\begin{aligned}
(1-t)HS_M(t) &= \sum_{d\in\mathbb{Z}} HF_M(d)t^d - \sum_{d\in\mathbb{Z}} HF_M(d)t^{d+1} \\
&= \sum_{d\in\mathbb{Z}} \left(HF_M(d+1) - HF_M(d)\right) t^{d+1} \\
&= \sum_{d\in\mathbb{Z}} \left(HF_C(d+1) - HF_K(d)\right) t^{d+1} \\
&= \sum_{d\in\mathbb{Z}} HF_C(d)t^d - t\sum_{d\in\mathbb{Z}} HF_K(d)t^d \\
&= HS_C(t) - tHS_K(t)
\end{aligned}$$

Since K and C are annihilated by x_n, x_n acts as multiplication by 0 on K, C. Thus, K, C can be seen as an $R/\langle x_n\rangle \cong k[x_1, \ldots, x_{n-1}]$-module. So, we can apply the induction hypothesis to $HS_C(t)$ and $HS_K(t)$, which yields the result. □

Remark 6.2.6. Suppose M is a finitely generated R-module s.t. $M_d = 0$ for all $d < 0$. Note that in the proof of Theorem 6.2.5, we have $C_d = M_d/x_nM_{d-1}$. Thus, $C_0 = M_0$, i.e. $HF_M(0) = HF_C(0)$ and $HF_M(d) = 0$ for all $d < 0$. This implies that $h(t) \in \mathbb{Z}[t]$ in Theorem 6.2.5.

Cancelling powers of $(1 - t)$ in $HS_M(t)$, there is $d \in \mathbb{Z}_{\geq 0}$, s.t. we may write

$$HS_M(t) = \frac{h_M(t)}{(1-t)^d},$$

where $h_M(1) \neq 0$. We may denote the order of the pole at $t = 1$ as $d(M)$.

We now can recover the result that the Hilbert function turns into a polynomial for the case of modules.

Lemma 6.2.7. *Let d be a positive integer. Then*

$$(1-t)^{-d} = \sum_{k\geq 0} \binom{d+k-1}{d-1} t^k.$$

Proof. This is shown by induction on d. If $d = 1$ we have that $\frac{1}{1-t} = 1 + t + \cdots + t^s + \cdots$. Suppose $d + 1 > 1$ and that the result holds for d. Then derivation w.r.t t yields

$$\frac{d}{(1-t)^{d+1}} = \sum_{k\geq 1} k\binom{d+k-1}{d-1} t^{k-1} = \sum_{k\geq 0} (k+1)\binom{d+k}{d-1} t^k.$$

Since

$$\frac{k+1}{d}\binom{d+k}{d-1} = \frac{(d+k)!}{d!k!} = \binom{d+k}{d},$$

the result follows. □

Corollary 6.2.8 ([2], Corollary 11.2)**.** *Let M be a graded module. For $s \geq 0$ sufficiently large, $HF_M(s)$ is a polynomial of degree $d(M) - 1$.*

Proof. Let $d = d(M)$. By definition, we have that $HF_M(s)$ is the coefficient of t^s in $HS_M(t)$. Suppose that $h_M(t) = \sum_{k=l}^{N} a_k t^k$. Using Lemma 6.2.7 yields

$$\sum_{s\in\mathbb{Z}} HF_M(s)t^s = HS_M(t) = \sum_{k\geq 0} \binom{d+k-1}{d-1} t^k \left(\sum_{i=l}^{N} a_i t^i\right).$$

By comparing coefficients we obtain

$$HF_M(s) = \sum_{k=l}^{N} a_k \binom{d+s-k-1}{d-1} \text{ for all } s \geq N.$$

The RHS is a polynomial in s of degree $d-1$, and has leading term $\sum_{k=0}^{N} a_k s^{d-1}/(d-1)! \neq 0$. □

Definition 6.2.9. Let M be a graded R-module. The polynomial that $HF_M(s)$ turns into for sufficiently large s is called the *Hilbert polynomial* of M, denoted $HP_M(s)$.

The next result is an immediate consequence of the previous one.

Corollary 6.2.10. *Let M be a graded R-module. Then* $\deg(HP_M) = d(M) - 1$.

Example 6.2.11. As in Example 6.1.21 consider $I = \langle x^2 - z^2, xy + xz\rangle \subseteq R = k[x, y, z]$ with $\text{in}_{DRL}(I) = \langle x^2, xy, yz^2\rangle$. We have seen that $HF_{R/I}(0) = 1, HF_{R/I}(1) = 3$ and $HF_{R/I}(s) = 4$ for $s \geq 2$. Calculating the Hilbert series we get

$$\begin{aligned} HS_{R/I}(t) &= 1 + 3t + 4t^2 + 4t^3 + \cdots \\ &= 1 + 3t + 4t^2(1 + t + t^2 + \cdots) \\ &= 1 + 3t + 4t^2(1-t)^{-1} \\ &= \frac{1 + 2t + t^2}{1-t}. \end{aligned}$$

So, $d(R/I) = 1 = \deg(HP_{R/I}) + 1$

To conclude this chapter, we prove an interesting property about nonzerodivisors.

Proposition 6.2.12 ([2], Proposition 11.3)**.** *Let M be a graded R-module and let $x \in R_k$ be a nonzerodivisor on M. Then $d(M/xM) = d(M) - 1$.*

Proof. Since x is a nonzerodivisor, we get the short exact sequence

$$0 \to M_s \xrightarrow{x} M_{s+k} \to C_{s+k} \to 0,$$

with $C_{s+k} = \operatorname{coker}(M_s \xrightarrow{x} M_{s+k})$. Corollary 6.2.3 yields $HF_M(s+k) - HF_M(s) - HF_C(s+k) = 0$. Multiplying by t^{s+k} and summing up w.r.t s, as we did in the proof of Theorem 6.2.5, we get

$$(1 - t^k) HS_M(t) = HS_{M/xM}(t).$$

But $(1 - t^k) = (1 - t)(1 + t + t^2 + \cdots + t^{k-1})$. Thus,

$$HS_{M/xM}(t) = (1 + t + t^2 + \cdots + t^{k-1}) \frac{h_M(t)}{(1 - t)^{d-1}}.$$

Therefore, we can conclude that $d(M/xM) = d(M) - 1$. □

Chapter 7

Castelnuovo–Mumford Regularity

In this chapter, we use the results and tools we acquired in the previous chapters to define the notion of Castelnuovo–Mumford regularity. We define it in terms of minimal graded free resolutions and show equivalence with a definition coming from local cohomology based on [23, Chapter 4]. After studying the most important properties of regularity, the chapter closes with the presentation of a criterion for m-regularity due to D. Bayer and M. Stillman [4].

7.1 Definition and Properties of Regularity

Our first definition of Castelnuovo–Mumford regularity is based on minimal graded free resolution and Betti-numbers. The construction follows [42, Chapter 11]. Let $R = k[x_1, \dots, x_n]$ standard graded and let M be a graded R-module. As minimal graded free resolutions are unique up to isomorphism, this property also holds for the kernels of the boundary maps in this resolution. This allows us to define the following.

Definition 7.1.1. For a minimal graded free resolution $(\mathcal{F}, \partial) \to M$, let $\Omega_k(M) = \ker(\partial_{k-1})$ denote the *k-th syzygy module* of M

Let $\{m_1, \dots, m_{\beta_0}\}$ be a minimal system of homogeneous generators of the graded module M and let $d_i = \deg(m_i)$. Fix the epimorphism $\varphi_0 : R^{\beta_0} \to M, e_i \mapsto m_i$ and twist the free module R^{β_0} in a way s.t. $\varphi_0 : F_0 = \bigoplus_{j=1}^{\beta_0} R(-d_{0j}) \to M$ is homogeneous.
Consider the $\Omega_1(M) \subseteq F_0$, which is again a finitely generated graded R-module. Choosing a minimal system of homogeneous generators of $\Omega_1(M)$ and continuing as before, it is clear, by Proposition 3.2.8, that this results in the unique minimal graded free resolution of M. By Theorem 5.7.20, this process stops after a finite number of steps and the minimal graded free resolution has the form

$$0 \to F_p \to F_{p-1} \to \cdots \to F_1 \to F_0 \xrightarrow{\varphi} M \to 0, \tag{7.1}$$

where the free graded modules are of the form

$$F_i = \bigoplus_{j=1}^{\beta_i} R(-d_{ij}),$$

for appropriate twists d_{ij}. The number p in Resolution (7.1) is called the *projective dimension* of M, denoted $\operatorname{pdim}(M)$.

Definition 7.1.2. Let $\mathcal{F}$ be as in (7.1). The *global Betti-numbers* of M are defined to be the ranks of the free modules F_i in $\mathcal{F}$, denoted

$$\beta_i(M) = \operatorname{rk}(F_i) = \operatorname{rk}\left(\bigoplus_{j=1}^{\beta_i} R(-d_{ij})\right).$$

By regrouping the twists d_{ij} it is possible to rewrite the twisted free R-modules F_i as follows:

$$F_i = \bigoplus_{j\in\mathbb{Z}} R(-j)^{\beta_{ij}}, \tag{7.2}$$

where β_{ij} denotes the number of generators of degree j in F_i.

Definition 7.1.3. The numbers $\beta_{ij} \in \mathbb{Z}_{\geq 0}$ in (7.2) are called the *graded Betti-numbers* of M denoted $\beta_{ij}(M)$.

Remark 7.1.4. It is easy to see that $\beta_i(M) = \sum_{j\in\mathbb{Z}} \beta_{ij}(M)$. Also, it is immediate that one has $\beta_{ij}(M) = \beta_{i-k,j}(\Omega_k(M))$.

The notion of graded Betti-numbers leads to the definition of an invariant of M that measures how complicated a graded module M is in terms of its graded free resolution.

Definition 7.1.5. Let M be a graded R-module. The *Castelnuovo–Mumford regularity* (or just *regularity*) of M is defined to be

$$\operatorname{reg}_R(M) = \max\{j - i : \beta_{ij}(M) \neq 0\}.$$

If T is a set of homogeneous elements, $\operatorname{reg}_R(T)$ is defined to be the regularity of the graded R-module they generate. When the ring R is clear from context, we may omit the subscript R.

Remark 7.1.6. The construction of the minimal graded free resolution of M can be carried out over finite fields, as well as field extensions. Thus, the Castelnuovo–Mumford regularity is preserved under field extensions.

Example 7.1.7. Continuing Example 3.2.6 with the ideal $I = \langle x^2 - z^2, xy + xz\rangle$ and its free resolution

$$0 \to R(-4) \to R(-2)^2 \to I \to 0,$$

notice that this is in fact the minimal graded resolution of I. The Betti-numbers of I are $\beta_0(I) = 2, \beta_1(I) = 1$.
The graded Betti-numbers are $\beta_{0,2}(I) = 2, \beta_{1,4}(I) = 1$. Thus,

$$\operatorname{reg}(I) = \max\{2 - 0, 4 - 1\} = 3.$$

While the definition of Castelnuovo–Mumford regularity above is rather intuitive, there is another, more technical equivalent definition in terms of local cohomology that is useful for proving several results.

Theorem 7.1.8 (Equivalence of Definitions, [23], Theorem 4.3)**.** *Let M be a finitely generated graded R-module and let $d \in \mathbb{Z}$. The following are equivalent:*

(a) $d \geq \operatorname{reg}(M)$,

(b) $d \geq \max\{e \in \mathbb{N} : H^0_{\mathfrak{m}}(M)_e \neq 0\}$ *and* $H^i_{\mathfrak{m}}(M)_{d-i+1} = 0$ *for all* $i > 0$.

To prove this result, we first need to introduce some terminology.

Definition 7.1.9. A finitely generated graded R-module M is called

(a) *weakly d-regular* if $H^i_{\mathfrak{m}}(M)_{d-i+1} = 0$ for all $i > 0$,

(b) *d-regular* if in addition $d \geq \max\{e \in \mathbb{N} : H^0_{\mathfrak{m}}(M)_e \neq 0\}$.

Lemma 7.1.10 ([23], Proposition 4.10)**.** *Let M be a finitely generated graded R-module and let x be a linear M-regular element. Then:*

(a) *If M is weakly d-regular, then M/xM is weakly d-regular.*

(b) *If M is (weakly) d-regular, then M is (weakly) $(d+1)$-regular.*

(c) *M is d-regular if and only if M/xM is d-regular and $H^0_{\mathfrak{m}}(M)_e = 0$ for all $e > d$.*

Proof. (a) Consider the exact sequence

$$0 \to M(-1) \xrightarrow{x} M \to M/xM \to 0. \tag{7.3}$$

Lemma 3.4.16 yields

$$H^i_{\mathfrak{m}}(M)_{d+1-i} \to H^i_{\mathfrak{m}}(M/xM)_{d+1-i} \to H^{i+1}_{\mathfrak{m}}(M(-1))_{d+1-i},$$

where $H^{i+1}_{\mathfrak{m}}(M(-1))_{d+1-i} \cong H^{i+1}_{\mathfrak{m}}(M)_{d-i}$. The module on the left vanishes for all $i > 0$ since M is weakly d-regular. Thus, the modules on the right vanish as well. Therefore, we have $H^i_{\mathfrak{m}}(M/xM)_{d+1-i} = 0$ for all $i > 0$ and M/xM is weakly d-regular.

(b) The proof is done by induction on $\operatorname{kdim}(M)$.

If $\operatorname{kdim}(M) = 0$, then $M = \Gamma_{\mathfrak{m}}(M)$, so by Theorem 3.4.20 $H^i_{\mathfrak{m}}(M) = 0$ for all $i > 0$. Then M is clearly weakly e-regular for all e.

Let $\operatorname{kdim}(M) > 0$ and assume that the result holds for modules of lower dimension. Since x is a nonzerodivisor on M, Proposition 6.2.12 implies that $\operatorname{kdim}(M/xM) = \operatorname{kdim}(M)-1$. From (a) we know that M/xM is weakly d-regular, so by inductive hypothesis it is also weakly $(d+1)$-regular. Again using the long exact sequence of local cohomology associated to (7.3) yields

$$H^i_{\mathfrak{m}}(M(-1))_{(d+1)+1-i} \to H^i_{\mathfrak{m}}(M)_{(d+1)+1-i} \to H^i_{\mathfrak{m}}(M/xM)_{(d+1)+1-i}.$$

Since $H^i_{\mathfrak{m}}(M(-1))_{(d+1)+1-i} \cong H^i_{\mathfrak{m}}(M)_{d+1-i}$ and M is weakly d-regular, this vanishes for $i > 0$. The term on the right of the sequence vanishes since M/xM is weakly $(d+1)-$regular. Thus, the middle term vanishes as well, which shows that M is weakly $(d+1)$-regular.
Now, suppose that in addition, M is d-regular, i.e. $d \geq \max\{e \in \mathbb{N} : H^0_{\mathfrak{m}}(M)_e \neq 0\}$. This clearly holds for $d+1$ as well, so M is $(d+1)$-regular.

(c) ($\Rightarrow$) Suppose M is d-regular. Since $H^0_{\mathfrak{m}}(M)_e = 0$ for all $e > d$ is necessary for M being d-regular, this trivially holds. So we only have to show that M/xM is d-regular. By (a) it follows that M/xM is weakly d-regular, so it remains to prove that $H^0_{\mathfrak{m}}(M/xM)_e = 0$ for $e > d$ Using the long exact sequence associated to (7.3) again, we get

$$H^0_{\mathfrak{m}}(M)_e \to H^0_{\mathfrak{m}}(M/xM)_e \to H^1_{\mathfrak{m}}(M(-1))_e,$$

where the module on the left vanishes by our assumption. Also $H^1_{\mathfrak{m}}(M(-1))_e \cong H^1_{\mathfrak{m}}(M)_{e-1}$. But by (b), we know that since $e \geq d+1$, M is weakly e-regular, so the module on the right vanishes as well. Thus, $H^0_{\mathfrak{m}}(M/xM)_e = 0$ for all $e > d$ and M/xM is d-regular.

($\Leftarrow$) Suppose M/xM is d-regular and $H^0_{\mathfrak{m}}(M)_e = 0$ for all $e > d$. It is enough to prove that M is weakly d-regular, as the additional part of the definition is given by hypothesis. Using (7.3) again, we get for each $e > d$ and $i > 0$ the exact sequence

$$H^{i-1}_{\mathfrak{m}}(M/xM)_{e+1} \to H^i_{\mathfrak{m}}(M)_e \xrightarrow{\alpha_x} H^i_{\mathfrak{m}}(M)_{e+1}.$$

By (b), M/xM is e-regular for all $e \geq d$ since it is d-regular. Thus, the module on the left is zero for $e \geq d - i + 1$, s.t. α_x is injective. Since this holds for all $e > d$, we get an infinite sequence of monomorphisms

$$H^i_{\mathfrak{m}}(M)_{d-i+1} \xrightarrow{\alpha_x} H^i_{\mathfrak{m}}(M)_{d-i+2} \xrightarrow{\alpha_x} \cdots,$$

where each α_x is induced by multiplication by x. But every element of $H^i_{\mathfrak{m}}(M)$ is annihilated by a power of $x \in \mathfrak{m}$, thus $H^i_{\mathfrak{m}}(M)_{d-i+k} = 0$ for some $k \geq 1$ and therefore $H^i_{\mathfrak{m}}(M)_{d-i+1} = 0$, since the α_x's are injective. Thus, M is d-regular. □

We now have the tools to prove Theorem 7.1.8.

proof of Theorem 7.1.8. $(a \Rightarrow b)$ This is done by induction on $\operatorname{pdim}(M)$. If $\operatorname{pdim}(M) = 0$, then M is a free graded module of the form $M = \bigoplus_j R(-d_j)$ and by definition of regularity it is clear that $\operatorname{reg}(M) = \max_j\{d_j\}$. It then can be shown that M is d-regular if and only if $d_j \leq d$ for all i, which concludes this case. This is done by computing the local cohomology of M and uses the theory of *simplicial complexes* and *Cech-complexes*, which are beyond the scope of this thesis. However, it can be looked up in [23, Section A.1].

Let $\operatorname{pdim}(M) > 0$ and assume that the result holds for modules of lower projective dimension. Let $d \geq \operatorname{reg}(M)$ and consider the minimal graded free resolution of M

$$\cdots \to F_1 \xrightarrow{\varphi_1} F_0 \to M \to 0.$$

Let $M' = \Omega_1(M) \subseteq F_0$ be the first syzygy-module. Looking at the minimal resolution of $\Omega_1(M)$ it is clear by definition of regularity that $\operatorname{reg}(M') \leq 1 + \operatorname{reg}(M) \leq 1 + d$. Thus, by induction hypothesis, M' is $(d+1)$-regular. Further, since $e \geq \operatorname{reg}(M)$ for all $e \geq d$, we can assume that M' is $(e+1)$-regular for all $e \geq d$.

Let $0 \to M' \to F_0 \to M \to 0$ be a short exact sequence. Then Lemma 3.4.16 yields

$$\cdots \to H^i_{\mathfrak{m}}(F_0) \to H^i_{\mathfrak{m}}(M) \to H^{i+1}_{\mathfrak{m}}(M') \to \cdots.$$

Since $e \geq d \geq \operatorname{reg}(M) \geq \max_j\{d_j\}$, where $F_0 = \bigoplus_j R(-d_j)$, and M' is $(e+1)$-regular for every $e \geq d$, it follows that $H^i_{\mathfrak{m}}(F_0)_{e-i+1} = 0$ and $H^{i+1}_{\mathfrak{m}}(M')_{(e+1)-(i+1)+1} = 0$. Therefore, $H^i_{\mathfrak{m}}(M)_{e-i+1} = 0$ for all $e \geq d, i \geq 0$, which shows that M is e-regular for all $e \geq d$.

$(b \Rightarrow a)$ We may assume that the base field k is infinite as the construction of local cohomology commutes with field extensions. Let

$$\cdots \to F_1 \xrightarrow{\varphi_1} F_0 \to M \to 0 \tag{7.4}$$

be the minimal graded free resolution of M. First, we show that F_0 is generated by elements of degree $\leq d$. This is done by showing that M is generated by elements of degree $\leq d$.

We prove this claim by induction on $\operatorname{kdim}(M)$. If $\operatorname{kdim}(M) = 0$, then $M_e = H^0_{\mathfrak{m}}(M)_e = 0$ for all $e > d$, since M is d-regular. Thus, M is generated by elements of degree $\leq d$.

Now suppose, $\operatorname{kdim}(M) > 0$ and assume that the claim is true for modules of lower dimension. Let $\overline{M} = M/H^0_{\mathfrak{m}}(M)$ and form the exact sequence

$$0 \to H^0_{\mathfrak{m}}(M) \to M \to \overline{M} \to 0. \tag{7.5}$$

We know that $H^0_{\mathfrak{m}}(M)_e = 0$ for all $e > d$. We also know by Lemma 3.4.10 that $\overline{M}$ is either zero, from which the claim follows, or is $\mathfrak{m}$-torsion free. Thus, by Lemma 3.4.9, there is a nonzerodivisor x on $\overline{M}$, which may be chosen linear by Lemma 3.4.18. Then, by Lemma 3.4.17, we have that $H^i_{\mathfrak{m}}(M) = H^i_{\mathfrak{m}}(\overline{M})$ for all $i > 0$ and thus, by Lemma 7.1.10, we see that $\overline{M}/x\overline{M}$

is d-regular. Since $\operatorname{kdim}(\overline{M}/x\overline{M}) < \operatorname{kdim}(\overline{M})$, by inductive hypothesis we have that $\overline{M}/x\overline{M}$ is generated by elements of degree $\leq d$. In this case, clearly $\overline{M}/\mathfrak{m}\overline{M}$ is generated by elements of degree $\leq d$. Nakayama's lemma implies that $\overline{M}$ is generated by degree $\leq d$. Thus, looking at (7.5), we can conclude that M is generated by elements of degree $\leq d$.

If M is free, it follows that $d \geq \operatorname{reg}(M)$ and the result follows.
Otherwise, suppose that $\operatorname{pdim}(M) > 0$ and we do an inductive argument on $\operatorname{pdim}(M)$. Let $M' = \Omega_1(M) \subseteq F_0$. Using (7.4) the long exact sequence in local cohomology yields

$$H^i_{\mathfrak{m}}(M)_e \to H^{i+1}_{\mathfrak{m}}(M')_e \to H^{i+1}_{\mathfrak{m}}(F_0)_e, \tag{7.6}$$

where the left and right terms vanish if $e \geq d - i + 1$. Thus, M' is $(d+1)$-regular and then, the induction hypothesis implies that $\operatorname{reg}(M') \leq d + 1$. That means that the part of the minimal graded free resolution of M starting from F_1 satisfies the conditions for $\operatorname{reg}(M) \leq d$. Since additionally M is generated by degree $\leq d$, it follows that $\operatorname{reg}(M) \leq d$. □

The above proof shows that M is d-regular if and only if $\operatorname{reg}(M) \leq d$ and allows us to reformulate the definition of Castelnuovo–Mumford regularity.

Corollary 7.1.11. *Let M be a finitely generated graded R-module. Then*

$$\operatorname{reg}(M) = \min\{m \in \mathbb{N} : H^i_{\mathfrak{m}}(M)_d = 0 \text{ for all } i \geq 0 \text{ and } d \geq m - i + 1\}.$$

Next, we state some important properties of regularity.

Lemma 7.1.12 ([50], Lemma 2.1.4)**.** *Let $0 \to A \to B \to C \to 0$ be a short exact sequence of finitely generated graded R-modules. Then:*

(a) $\operatorname{reg}(A) \leq \max\{\operatorname{reg}(B), \operatorname{reg}(C) + 1\}$,

(b) $\operatorname{reg}(B) \leq \max\{\operatorname{reg}(A), \operatorname{reg}(C)\}$,

(c) $\operatorname{reg}(C) \leq \max\{\operatorname{reg}(B), \operatorname{reg}(A) - 1\}$.

Proof. (a) Let $m = \max\{\operatorname{reg}(B), \operatorname{reg}(C) + 1\}$ and $d \geq m - i + 1$. Then, the long exact sequence of local cohomology yields

$$H^{i-1}_{\mathfrak{m}}(C)_d \to H^i_{\mathfrak{m}}(A)_d \to H^i_{\mathfrak{m}}(B)_d.$$

But $H^{i-1}_{\mathfrak{m}}(C)_d = 0$ for all $d \geq m - i + 1 \geq \operatorname{reg}(C) - (i-1) + 1$. Also $H^i_{\mathfrak{m}}(B)_d = 0$ for all $d \geq m - i + 1 \geq \operatorname{reg}(B) - i + 1$. Thus, $\operatorname{reg}(A) \leq m$.

(b) Let $m = \max\{\operatorname{reg}(A), \operatorname{reg}(C)\}$ and $d \geq m - i + 1$. Then, the long exact sequence of local cohomology yields

$$H^i_{\mathfrak{m}}(A)_d \to H^i_{\mathfrak{m}}(B)_d \to H^i_{\mathfrak{m}}(C)_d.$$

But $H^i_{\mathfrak{m}}(A)_d = H^i_{\mathfrak{m}}(C)_d = 0$ for all $d \geq m - i + 1$. Thus, $\operatorname{reg}(B) \leq m$.

(c) Let $m = \max\{\operatorname{reg}(B), \operatorname{reg}(A) - 1\}$ and $d \geq m - i + 1$. Then, the long exact sequence of local cohomology yields

$$H^i_{\mathfrak{m}}(B)_d \to H^i_{\mathfrak{m}}(C)_d \to H^{i+1}_{\mathfrak{m}}(A)_d.$$

But $H^i_{\mathfrak{m}}(B)_d = 0$ for all $d \geq m - i + 1 \geq \operatorname{reg}(B) - i + 1$. Also, we have $H^{i+1}_{\mathfrak{m}}(A)_d = 0$ for all $d \geq m - (i+1) + 1 \geq \operatorname{reg}(A) - (i+1) + 1$. Thus, $\operatorname{reg}(C) \leq m$. □

Lemma 7.1.13 ([50], Lemma 2.1.5)**.** *Let M be a finitely generated graded R-module.*

(a) $\operatorname{reg}(M(-d)) = \operatorname{reg}(M) + d$.

(b) *If $y \in R_d$ is an M-regular element, then* $\operatorname{reg}(M/yM) = \operatorname{reg}(M) + d - 1$.

(c) *If $\boldsymbol{y} = y_1, \ldots, y_r$ is an M-regular sequence with $y_i \in R_{d_i}$, for $i = 1, \ldots, r$, then* $\operatorname{reg}(M/\boldsymbol{y}M) = \operatorname{reg}(M) + (d_1 + \cdots + d_r) - r$.

Proof. (a) $\beta_{i,j}(M) = \beta_{i,j+d}(M(-d))$ so the result follows from the definition of $\operatorname{reg}(M)$.

(b) Since y is an M-regular element, we get the short exact sequence

$$0 \to M(-d) \xrightarrow{y} M \to M/yM \to 0.$$

So by Lemma 7.1.12, we get that

$$\begin{aligned} \operatorname{reg}(M/yM) &\leq \max\{\operatorname{reg}(M(-d)) - 1, \operatorname{reg}(M)\} \\ &= \max\{\operatorname{reg}(M) + d - 1, \operatorname{reg}(M)\} \\ &= \operatorname{reg}(M) + d - 1. \end{aligned}$$

Again using Lemma 7.1.12 and (a), we get

$$\operatorname{reg}(M) + d - 1 = \operatorname{reg}(M(-d)) - 1 \leq \max\{\operatorname{reg}(M) - 1, \operatorname{reg}(M/yM)\}.$$

Since $d \geq 1$, this implies that $\max\{\operatorname{reg}(M) - 1, \operatorname{reg}(M/yM)\} = \operatorname{reg}(M/yM)$. Thus, we get $\operatorname{reg}(M) + d - 1 \leq \operatorname{reg}(M/yM)$.

(c) This is done by induction on r, where the case $r = 1$ follows from (b).
Let $r > 1$ and assume the result holds for $r - 1$. For the M-regular sequence $y_1, \ldots, y_r$, let $M' = M/(y_1, \ldots, y_{r-1})M$ s.t. $M/\mathbf{y}M = M'/y_rM'$. By induction hypothesis, we have

$$\operatorname{reg}(M') = \operatorname{reg}(M) + (d_1 + \cdots + d_{r-1}) - (r - 1).$$

Applying (b) we get

$$\operatorname{reg}(M/\mathbf{y}M) = \operatorname{reg}(M'/y_rM') = \operatorname{reg}(M') + d_r - 1 = \operatorname{reg}(M) + (d_1 + \cdots + d_r) - r. \qquad \square$$

Lemma 7.1.14 ([50], Theorem 2.1.6)**.** *Let I be a proper graded ideal of R. Then*

$$\operatorname{reg}(I) = \operatorname{reg}(R/I) + 1.$$

Proof. From the short exact sequence $0 \to I \to R \to R/I \to 0$ and Lemma 7.1.12, it follows that

$$\operatorname{reg}(I) \leq \max\{\operatorname{reg}(R), \operatorname{reg}(R/I) + 1\} = \operatorname{reg}(R/I) + 1 \text{ as } \operatorname{reg}(R) = 0$$

and

$$\operatorname{reg}(R/I) \leq \max\{\operatorname{reg}(R), \operatorname{reg}(I) - 1\} = \operatorname{reg}(I) - 1 \text{ as } \operatorname{reg}(I) \geq 1 \text{ and } \operatorname{reg}(R) = 0.$$

Thus, $\operatorname{reg}(R/I) + 1 \leq \operatorname{reg}(I) \leq \operatorname{reg}(R/I) + 1$, which yields the conclusion. $\square$

When $\operatorname{kdim}(R/I) \leq 1$, there is a nice bound of the regularity that is linear in the number and the degrees of generators of I. The result is due to M. Chardin [13, Theorem 12.4].

Theorem 7.1.15. *Let I be a graded ideal of R generated by homogeneous elements of degrees $d_1 \geq d_2 \geq \cdots \geq d_r$ and let $l = \min(n, r)$. If* $\operatorname{kdim}(R/I) \leq 1$*, then*

$$\operatorname{reg}(R/I) \leq d_1 + d_2 + \cdots + d_l - l.$$

7.2 Criterion for m-regularity

In this section we show a technical result due to D. Bayer and M. Stillman [4] that will be important in Chapter 8. All ideals are assumed to be graded in $R = k[x_1, \dots, x_n]$. The base field k is assumed to be infinite.

Let $I^{sat} = I^{sat}_{\mathfrak{m}}$ denote the saturation of I w.r.t. the irrelevant ideal $\mathfrak{m}$.

Definition 7.2.1. An ideal I of R is *m-saturated* if $I_d = I^{sat}_d$ for all $d \geq m$.

Remark 7.2.2. For the exact sequence $0 \to I \to R \to R/I \to 0$, the long exact sequence in local cohomology yields $H^1_{\mathfrak{m}}(I) \cong H^0_{\mathfrak{m}}(R/I) = \Gamma_{\mathfrak{m}}(R/I) = I^{sat}/I$. Therefore, I is m-saturated if and only if $H^1_{\mathfrak{m}}(I)_d = 0$ for all $d \geq m$. Thus, if $\operatorname{reg}(I) \leq m$ then I is m-saturated.

Lemma 7.2.3 ([4], Lemma 1.4)**.** *Let I be an ideal of R, $\operatorname{kdim}(R/I) \neq 0$ and $h \in R$.*

(a) *If h is a nonzerodivisor on R/I, then $(I : h) = I$.*

(b) *If h is a zerodivisor on R/I, then $(I : h)_d \neq I_d$ for all d sufficiently large.*

Proof. (a) This is immediate by the definition of $(I : h)$.

(b) Choose a homogeneous polynomial $f \in (I : h)$ s.t. $f \notin I$. $\mathfrak{m}$ contains a nonzerodivisor $g \in R$ on R/I that can be chosen linear by Lemma 3.4.18. Clearly, $gf \notin I$, but $gf \in (I : h)$. Continuing the same way, we can find elements of $(I : h)_d \setminus I_d$ of all degrees $d \geq \deg(f)$. □

Definition 7.2.4. Let I be an ideal of R. An element $h \in R$ is called *generic for I* if h is not a zerodivisor on R/I^{sat}. If $\operatorname{kdim}(R/I) = 0$, we mean that every $h \in R$ is generic for I.
For $j > 0$, define

$$U_j(I) = \{(h_1, \dots, h_j) \in R_1^j : h_i \text{ is generic for } (I, h_1, \dots, h_{i-1}) \text{ for } i = 1, \dots, j\} \subseteq R_1^j.$$

The terminology *generic for I* makes sense w.r.t to the comments in Section 2.4, as the set $U_j(I)$ happens to be a Zariski open subset of R_1^j.

Lemma 7.2.5 ([4], Lemma 1.6)**.** *Let I be an ideal of R and let $h \in R$. Then $(I : h)_d = I_d$ for all $d \geq m$ if and only if I is m-saturated and h is generic for I.*

Proof. ($\Rightarrow$) Let f be homogeneous of maximal degree s.t. $f \in I^{sat} \setminus I$. Then $hf \in I$, i.e. $f \in (I : h)$. This implies that $\deg(f) < m$ and I is m-saturated. If $\operatorname{kdim}(R/I) = 0$, we are done, as all $h \in R$ are generic for I.
If $\operatorname{kdim}(R/I) \neq 0$, we have $(I^{sat} : h)_d = (I : h)_d = I_d = I^{sat}_d$ for all $d \geq m$. Thus, by Lemma 7.2.3, h is not a zerodivsior on R/I^{sat}, i.e. h is generic for I.

($\Leftarrow$) If $\operatorname{kdim}(R/I) = 0$, then $I^{sat}/I = H^0_{\mathfrak{m}}(R/I) = R/I$, from which the result follows immediately. Otherwise, $\operatorname{kdim}(R/I) > 0$ and Lemma 7.2.3 implies $(I : h)_d = (I^{sat} : h)_d = (I^{sat})_d = I_d$ for all $d \geq m$. □

The next two results relate regularity with m-saturated ideals.

Lemma 7.2.6 ([4], Lemma 1.7)**.** *Let I be an ideal of R. Suppose that* $\operatorname{kdim}(R/I) = 0$. *Then the following are equivalent:*

(a) *I is m-saturated.*

(b) *I is m-regular.*

(c) $I_m = R_m$

Proof. $(a \Leftrightarrow c)$ Since $\operatorname{kdim}(R/I) = 0$ and I is homogeneous, by Lemmas 2.1.20 and 2.3.18 we have that $\sqrt{I} = \mathfrak{m}$. Thus, there exists $n \in \mathbb{N}$ s.t. $\mathfrak{m}^n \subseteq I \subseteq \mathfrak{m}$, which implies that $R = I^{sat}$. From there the equivalence is immediate.

$(b \Rightarrow a)$ This follows directly from Remark 7.2.2.

$(a \Rightarrow b)$ We have $H^0_{\mathfrak{m}}(I) = 0$ and $H^i_{\mathfrak{m}}(I) = 0$ for all $i > 1$, since $\operatorname{kdim}(R/I) = 0$ implies that $H^{i+1}_{\mathfrak{m}}(I) \cong H^i_{\mathfrak{m}}(R/I) = 0$ for all $i > 0$ by Theorem 3.4.20.
$H^1_{\mathfrak{m}}(I) = H^0_{\mathfrak{m}}(R/I) = R/I$. Since $H^1_{\mathfrak{m}}(I)_d = 0$ for all $d \geq m$ by hypothesis, it follows that $\operatorname{reg}(I) \leq m$, i.e I is m-regular. □

Lemma 7.2.7 ([4], Lemma 1.8)**.** *Let I be an ideal of R and suppose $h \in R_1$ is generic for I. Then I is m-regular if and only if I is m-saturated and $\langle I, h\rangle$ is m-regular.*

Proof. First, suppose I is m-saturated and define $Q = (I : h)/I$. We get a short exact sequence $0 \to I \to (I : h) \to Q \to 0$. By Lemma 7.2.5, $I_d = (I : h)_d$ for all $d \geq m$. But this implies that $\operatorname{kdim}(Q) = 0$. Thus, $H^i_{\mathfrak{m}}(Q) = 0$ for all $i \neq 0$. Also, $H^0_{\mathfrak{m}}(Q) = \Gamma_{\mathfrak{m}}(Q) = Q$, so $H^0_{\mathfrak{m}}(Q)_d = 0$ for all $d \geq m$. Thus, the long exact sequence of local cohomology implies

$$H^i_{\mathfrak{m}}(I)_d \cong H^i_{\mathfrak{m}}((I : h))_d \text{ for } d \geq m - i + 1, i > 0. \tag{7.7}$$

$(\Rightarrow)$ Remark 7.2.2 implies that I is m-saturated. It remains to show that $\operatorname{reg}(\langle I, h\rangle) \leq m$. Consider $0 \to I \cap \langle h\rangle \to I \oplus \langle h\rangle \to \langle I, h\rangle \to 0$, which is an exact sequence. The equality $I \cap \langle h\rangle = (I : h)h$ yields the exact sequence

$$0 \to (I : h)(-1) \xrightarrow{h} I \oplus \langle h\rangle \to (I, h) \to 0.$$

The long exact sequence of local cohomology yields

$$H^i_{\mathfrak{m}}(I \oplus \langle h\rangle)_d \to H^i_{\mathfrak{m}}(\langle I, h\rangle)_d \to H^{i+1}_{\mathfrak{m}}((I : h))_{d-1}.$$

Then the isomorphism (7.7) and the exact sequence (7.2) give us the exact sequence

$$H^i_{\mathfrak{m}}(I \oplus \langle h\rangle)_d \to H^i_{\mathfrak{m}}(\langle I, h\rangle)_d \to H^{i+1}_{\mathfrak{m}}(I)_{d-1} \text{ for all } d \geq m - i + 1.$$

Since $\operatorname{reg}(I) \leq m$, the module on the right vanishes for $d \geq m - i + 1$. Also, we have that $\langle h\rangle \cong R(-1)$. Thus, by Lemma 7.1.12, we can see that $\operatorname{reg}(I \oplus \langle h\rangle) \leq \operatorname{reg}(I) \leq m$, i.e. the module on the left vanishes as well. It follows that $H^i_{\mathfrak{m}}(\langle I, h\rangle)_d = 0$ for all $d \geq m - i + 1$, i.e. $\langle I, h\rangle$ is m-regular.

$(\Leftarrow)$ The long exact sequence associated to $0 \to (I : h)(-1) \xrightarrow{h} I \oplus \langle h\rangle \to (I, h) \to 0$ yields

$$H^i_{\mathfrak{m}}((I : h))_{d-1} \to H^i_{\mathfrak{m}}(I \oplus \langle h\rangle)_d \to H^i_{\mathfrak{m}}(\langle I, h\rangle)_d.$$

Since $\operatorname{reg}(\langle I, h\rangle) \leq m$, we get that $H^i_{\mathfrak{m}}((I : h))_{d-1} \cong H^i_{\mathfrak{m}}(I \oplus \langle h\rangle)_d$ for all i and $d \geq m - i + 2$. Applying the isomorphism (7.7) for all i and $d \geq m - i + 1$, we see that

$$H^i_{\mathfrak{m}}(I)_d \cong H^i_{\mathfrak{m}}(I \oplus \langle h\rangle)_{d+1} = H^i_{\mathfrak{m}}(I)_{d+1} \oplus H^i_{\mathfrak{m}}(\langle h\rangle)_{d+1},$$

where local cohomology commutes with the direct sum, since $\Gamma_{\mathfrak{m}}(\cdot)$ is additive and (co)homology commutes with direct sums. Since the local cohomology vanishes for d sufficiently large, we can conclude that $H^i_{\mathfrak{m}}(I)_d = 0$ for all $d \geq m - i + 1$, so $\operatorname{reg}(I) \leq m$. □

Lemma 7.2.8 ([4], Lemma 1.9)**.** *Let I be an ideal of R that is generated by elements of degree $\leq m$ and let $h \in R_1$. If $\operatorname{reg}(\langle I, h\rangle) \leq m$, then $(I : h)$ is generated in degree $\leq m$.*

Proof. Let $f_1, \dots, f_s \in R$ s.t. $\{f_1, \dots, f_r, hf_{r+1}, \dots, hf_s\}$ is a minimal set of homogeneous generators of I and $\{f_1, \dots, f_r, h\}$ is a minimal set of generators for $\langle I, h\rangle$.
Let $f \in (I : h)$, then there exist $g_1, \dots, g_s \in R$ s.t.

$$hf = g_1 f_1 + \cdots + g_r f_r + h(g_{r+1} f_{r+1} + \cdots + g_s f_s) \in I.$$

Reordering the terms we get

$$(f - g_{r+1} f_{r+1} - \cdots - g_s f_s)h - g_1 f_1 - \cdots - g_r f_r = 0, \tag{7.8}$$

which corresponds to a syzygy in $\mathrm{Syz}(f_1, \dots, f_r, h)$.

Since $\mathrm{reg}(\langle I, h\rangle) \leq m$, every syzygy in $\mathrm{Syz}(f_1, \dots, f_r, h)$ can be written as a combination of syzygies of degree $\leq m + 1$. Applying this to (7.8) and noticing that $h \in R_1$, we see that $(f - g_{r+1} f_{r+1} - \cdots - g_s f_s) \in (I : h)$ can be written as a combination of elements in $(I : h)$ of degree $\leq m$. Since $f_{r+1}, \dots, f_s \in (I : h)$ are of degree $\leq m$ by hypothesis, we see that f and thus all of $(I : h)$ is generated by elements of degree $\leq m$. □

Finally, we can present a way to check if an ideal is m-regular.

Theorem 7.2.9 (Criterion for m-regularity, [4], Theorem 1.10)**.** *Let I be an ideal of R generated in degree $\leq m$. Then the following are equivalent:*

(a) $\mathrm{reg}(I) \leq m$.

(b) *There are $h_1, \dots, h_j \in R_1$ for some $j \geq 0$ s.t.*

$$(\langle I, h_1, \dots, h_{i-1}\rangle : h_i)_m = \langle I, h_1, \dots, h_{i-1}\rangle_m, \text{ for } i = 1, \dots, j$$

and $\langle I, h_1, \dots, h_j\rangle_m = R_m$.

(c) *Let $r = \mathrm{kdim}(R/I)$. For all $(h_1, \dots, h_r) \in U_r(I)$ and $p \geq m$, one has*

$$(\langle I, h_1, \dots, h_{i-1}\rangle : h_i)_p = \langle I, h_1, \dots, h_{i-1}\rangle_p \text{ for } i = 1, \dots, r$$

and $\langle I, h_1, \dots, h_r\rangle_p = R_p$.

Furthermore, if $h_1, \dots, h_j$ satisfy (b), then $(h_1, \dots, h_j) \in U_j(I)$.

Proof. $(a \Rightarrow c)$ This is shown by induction on $r = \mathrm{kdim}(R/I)$. If $r = 0$, then by Lemma 7.2.6, we have that $I_p = R_p$ for all $p \geq m$. Thus, (c) holds.
Let $r > 0$ and assume the result holds for $r - 1$. Let $(h_1, \dots, h_r) \in U_r(I)$. Lemma 7.2.7 implies that I is m-saturated and $\mathrm{reg}(\langle I, h_1\rangle) \leq m$. By Lemma 7.2.5 we have also that $(I : h_1)_p = I_p$ for all $p \geq m$. Clearly $(h_2, \dots, h_r) \in U_{r-1}(\langle I, h_1\rangle)$ by construction. The fact that $\mathrm{reg}(\langle I, h_1\rangle) \leq m$ and our induction hypothesis for $\langle I, h_1\rangle$ imply that (c) is satisfied.

$(c \Rightarrow b)$ This is immediate.

$(b \Rightarrow a)$ This is shown by induction on j. If $j = 0$, then $I_m = R_m$. So I is m-saturated by Remark 7.2.2 and $\mathrm{kdim}(R/I) = 0$. Thus, by Lemma 7.2.6, $\mathrm{reg}(I) \leq m$.
Suppose $j > 0$ and assume that the result holds for $j - 1$. $I_m = (I : h_1)_m$ by hypothesis and by induction, we can assume that $\mathrm{reg}(\langle I, h_1\rangle) \leq m$. Also $(h_2, \dots, h_j) \in U_j(\langle I, h_1\rangle)$ for $j \geq 2$. Now, by Lemma 7.2.8, it follows that $(I : h_1)$ is generated in degree $\leq m$. This implies that $(I : h_1)_d = I_d$ for all $d \geq m$. Thus, by Lemma 7.2.5, I is m-saturated and $h_1 \in U_1(I)$, which by Lemma 7.2.7 implies that $\mathrm{reg}(I) \leq m$. Also $(h_1, \dots, h_j) \in U_j(I)$, which proves the additional statement. □

Chapter 8

Complexity of Gröbner Basis Algorithms

This chapter is concerned with the complexity of Gröbner basis algorithms. We present the generic initial ideal, which is invariant under the action of generic linear change of coordinates and show how it behaves w.r.t to regularity. Then the notion of solving degree is introduced to explain the relationship between regularity and the complexity of Gröbner basis algorithms. Finally, we close with two other notions, the degree of regularity and the first fall-degree, that are often used in literature to estimate the complexity of Gröbner basis algorithms, and show their relation to the solving degree.

8.1 Generic Initial Ideals

Many results depend on the choice of variables and basis. With the notion of generic initial ideals, we get ideals that depend only on the monomial order. This discussion about generic initial ideals is based on [30, Chapter 4].

Definition 8.1.1. Consider the following groups of matrices

$$\begin{array}{ll} M_n(k) & = \{n \times n \text{ matrices}\} \\ \cup & \\ GL_n(k) & = \{\text{invertible } n \times n \text{ matrices}\} = \text{ General Linear group} \\ \cup & \\ B_n(k) & = \{\text{upper trinagular } n \times n \text{ matrices}\} = \text{ Borel Group} \\ \cup & \\ D_n(k) & = \{\text{diagonal } n \times n \text{ matrices}\} = \text{Algebraic Torus Group.} \end{array}$$

Remark 8.1.2. By identifying the set $M_n(k)$ with points in k^{n^2}, the coordinates of the points are the entries of the corresponding matrix. It is clear that $GL_n(k)$ is a Zariski open subset of $M_n(k)$ because $\boldsymbol{g} \in GL_n(k)$ if and only if $\det(\boldsymbol{g}) \neq 0$, i.e. if $\boldsymbol{g} \notin \mathcal{V}(\det(x_{ij}) \in k[x_{ij}, i, j = 1, \ldots, n])$. Since $GL_n(k)$ itself is open, a subset of $GL_n(k)$ is open if and only if it is open in k^{n^2}.

Elements of $GL_n(k)$ act on elements of R as linear automorphisms.

Definition 8.1.3. Let $\boldsymbol{g} \in GL_n(k)$, $\boldsymbol{g} = (g_{ij})$. Then $\boldsymbol{g}$ acts as an automorphism

$$\boldsymbol{g} : R \to R, \quad x_j \mapsto \boldsymbol{g}x_j = \sum_{i=1}^{n} g_{ij}x_i$$

$$f(x_1, \ldots, x_n) \mapsto \boldsymbol{g}f = f(\boldsymbol{g}x_1, \ldots, \boldsymbol{g}x_n).$$

These linear automorphisms are called *linear changes of coordinates.*
Given an ideal I, this leads to a new ideal, by applying $\boldsymbol{g}$ to all elements of I:

$$\boldsymbol{g}I = \langle \{\boldsymbol{g}f : f \in I\} \rangle.$$

The ideals $\boldsymbol{g}I$ are usually much more complicated than I itself. But we are interested in ideals, that are fixed (i.e. $\boldsymbol{g}I = I$) under actions from certain matrices from the groups introduced at the beginning of the section.

Proposition 8.1.4 ([38], Proposition 2.1)**.** *Let I be an ideal of R. Then I is fixed under $D_n(k)$ if and only if I is monomial.*

Proof. ($\Leftarrow$) Diagonal matrices send each variable to a multiple of itself. Thus, the same holds for monomials. This means that monomial ideals are fixed by $D_n(k)$.

($\Rightarrow$) Consider a polynomial $p = \sum_{i=1}^{s} c_i x^{\alpha_i}$, $\alpha_i = (\alpha_{i1}, \ldots, \alpha_{in}) \in \mathbb{Z}_{\geq 0}^n$ that lies in I. Let $\boldsymbol{t} = \operatorname{diag}(t_1, \ldots, t_n) \in D_n(k)$ be a diagonal matrix. Let $\boldsymbol{t}^\alpha$ denote the evaluation of x^α at the point $(t_1, \ldots, t_n)$, i.e. $\boldsymbol{t}^\alpha = t_1^{\alpha_1} \cdots t_n^{\alpha_n}$. Then

$$\boldsymbol{t}p = \sum_{i=1}^{s} c_i \boldsymbol{t}^{\alpha_i} x^{\alpha_i} \in I,$$

since I is fixed by $p \in D_n(k)$.
Define $\mathcal{T} = \{\boldsymbol{t}^{(1)}, \ldots, \boldsymbol{t}^{(s)}\} \subseteq D_n(k)$ as a generic set of diagonal matrices $\boldsymbol{t}^{(i)} = \operatorname{diag}(t_1^{(i)}, \ldots, t_n^{(i)})$, where $|\mathcal{T}| = |\operatorname{Supp}(p)| = s$.
For each $x^\alpha \in \operatorname{Supp}(p)$ and $\boldsymbol{t} \in \mathcal{T}$, the evaluation $\boldsymbol{t}^\alpha$ is a monomial in $k[t_1, \ldots, t_n]$. Form the $s \times s$ matrix $(\boldsymbol{t}^\alpha)$, whose columns are indexed by the s monomials in $\operatorname{Supp}(p)$ and whose rows are indexed by the elements of $\mathcal{T}$. The ij-th entry of $(\boldsymbol{t}^\alpha)$ is the evaluation of $\boldsymbol{t}^{(i)}$ at x^{α_j}.
The determinant of $(\boldsymbol{t}^\alpha)$ is a polynomial $k[t_1^{(i)}, \ldots, t_n^{(i)} : i = 1, \ldots, s]$ and as such is a nonzero polynomial, because the terms in the expansion are distinct. Since $\mathcal{T}$ was chosen generic, we may assume that $\det(\boldsymbol{t}^\alpha) \neq 0$, i.e. an inverse $(\boldsymbol{t}^\alpha)^{-1}$ exists. Multiplying $(\boldsymbol{t}^\alpha)^{-1}$ with the column vector, whose entries are the polynomials $\boldsymbol{t}^{(i)}p$ for $\boldsymbol{t}^{(i)} \in \mathcal{T}$, results in a column vector, whose entries are the terms $c_i x^{\alpha_i}$ of p. Thus, each $c_i x^{\alpha_i}$ appearing in p is a linear combination of the polynomials $\boldsymbol{t}^{(i)}p \in I$ and therefore lies in I as well.
This implies that I is indeed a monomial ideal. □

Another class of ideals, in which we are interested, are those that are fixed by$B_n(k)$.

Definition 8.1.5. An ideal I of R is called *Borel-fixed* if it is fixed under the action of $B_n(k)$, i.e. $\boldsymbol{g}I = I$ for all $\mathbf{g} \in B_n(k)$.

Since $B_n(k)$ contains $D_n(k)$ and $D_n(k)$-fixed ideals are monomial, it is immediate that Borel-fixed ideals also must be monomial.

Definition 8.1.6. For $1 \leq i \leq j \leq n$ and $c \in k$, let $\boldsymbol{g}_{ij}(c) \in GL_n(k)$ be an upper triangular matrix given by

$$\boldsymbol{g}_{ij}(c)x_i = x_i + cx_j$$
$$\boldsymbol{g}_{ij}(c)x_p = x_p \text{ for } p \neq i.$$

These matrices are also called *elementary upper triangular matrices.*

It is well known that $D_n(k)$ and the set of all such elementary upper triangular matrices $\boldsymbol{g}_{ij}(c)$ generate the group $B_n(k)$.
Borel-fixed ideals possess the additional property that in characteristic zero, larger indexed variable can be swapped for smaller indexed variables within the ideal.

Proposition 8.1.7 ([4], Proposition 2.7)**.** *Let I be a monomial ideal and suppose* $\operatorname{char}(k) = 0$. *Then the following are equivalent:*

(a) *I is Borel-fixed.*

(b) *If $x_1^{p_1} \cdots x_n^{p_n} \in I$ then $x_1^{p_1} \cdots x_j^{p_j+q} \cdots x_i^{p_i-q} \cdots x_n^{p_n} \in I$ for each $1 \leq j < i \leq n$.*

Proof. Fix $1 \leq j < i \leq n$. If $u = x_1^{p_1} \cdots x_n^{p_n} \in I$, then

$$\begin{aligned} \boldsymbol{g}_{ij}(c)u \in I &\iff x_1^{p_1} \cdots x_j^{p_j} \cdots (x_i + cx_j)^{p_i} \cdots x_n^{p_n} \in I \\ &\iff x_1^{p_1} \cdots x_j^{p_j+q} \cdots x_i^{p_i-q} \cdots x_n^{p_n} \in I \text{ for all } q = 0, \ldots, p_i. \end{aligned}$$

As a monomial ideal I is Borel-fixed if and only if $\boldsymbol{g}_{ij}(c)u \in I$ for all $u \in \mathrm{Mon}(R)$, $1 \leq j \leq i \leq n$ and $c \in k$, the result follows. □

The next result shows that for a graded ideal I, there exists a Zariski open set $U \subseteq GL_n(K)$ s.t. $\mathrm{in}(\boldsymbol{g}I)$ is independent of the choice of $\boldsymbol{g} \in U$.

Theorem 8.1.8 (Existence of Generic Initial Ideal, [30], Theorem 4.1.2)**.** *Let k be an infinite field and let I be a graded ideal of R. Fix a monomial order on R. Then there exists a nonempty Zariski open subset $U \subseteq GL_n(K)$ s.t. $\mathrm{in}(\boldsymbol{g}I) = \mathrm{in}(\boldsymbol{g}'I)$ for all $\boldsymbol{g}, \boldsymbol{g}' \in U$.*

Proof. The proof is given in Appendix A.3. □

Definition 8.1.9. The ideal $\mathrm{in}_\sigma(\boldsymbol{g}I)$ with $\boldsymbol{g} \in U$ and $U \subseteq GL_n(k)$ as given in Theorem 8.1.8 is called the *generic initial ideal* of I w.r.t a monomial order σ and is denoted $\mathrm{Gin}_\sigma(I)$.

As usual, we may omit the subscript σ if the monomial order is clear from the context. The generic initial ideal has the useful property of being Borel-fixed.

Theorem 8.1.10 (Galligo, [30], Theorem 4.2.1)**.** *Let k be an infinite field and let I be a graded ideal of R. Fix a monomial order σ on R. Then $\mathrm{Gin}_\sigma(I)$ is Borel-fixed.*

Proof. The proof is given in Appendix A.3. □

The idea of generic initial ideals motivates the following definition.

Definition 8.1.11. Let k be an infinite field. A graded ideal I of R is said to be *in generic coordinates* if $\mathbf{1} \in U$, i.e. if $\mathrm{in}(\boldsymbol{g}I) = \mathrm{in}(I)$ for all $\boldsymbol{g} \in U$, where $U \subseteq GL_n(k)$ is the Zariski open subset from Theorem 8.1.8.
Let k be any field and let K be a field extension of k s.t. K is infinite. Then I is in *generic coordinates over K* if $IK[x_1, \ldots, x_n] \subseteq K[x_1, \ldots, x_n]$ is in generic coordinates.

Let k be an infinite field and $\boldsymbol{g} \in U$ be a generic linear change of coordinates. Then $\boldsymbol{g}I$ is in generic coordinates. Informally, this means that every homogeneous ideal I can be put into generic coordinates by simply applying a random linear change of coordinates to it. If k is finite, the change of coordinates $\boldsymbol{g}$ has to be chosen over a sufficiently large field extension.

Let I be a graded ideal of R and recall the definition of the set $U_r(I) \subseteq R_1^r$. By convention we set $x_i = 0$ if $i > n$ and $U_0 = 0$.

Theorem 8.1.12 ([4], Theorem 2.4)**.** *Let I be a graded ideal of R and fix the DRL-order on R. Let $r = \mathrm{kdim}(R/I)$.*

(a) *$(x_n, \ldots, x_{n-r+1}) \in U_r(I)$ if and only if $(x_n, \ldots, x_{n-r+1}) \in U_r(\mathrm{in}(I))$.*

(b) *If $(x_n, \ldots, x_{n-r+1}) \in U_r(I)$, then $\mathrm{reg}(I) = \mathrm{reg}(\mathrm{in}(I))$.*

Proof. (a) $r = \mathrm{kdim}(R/\mathrm{in}(I))$, as the Hilbert function and therefore the Hilbert polynomial of I and $\mathrm{in}(I)$ are equal. If $r = 0$, then Lemma 7.2.6 implies the result. So suppose that $r > 0$.

($\Rightarrow$) Let $m = \operatorname{reg}(I)$, so I is generated in degree $\leq m$. Then $(x_n, \ldots, x_{n-r+1})$ satisfies condition (c) of Theorem 7.2.9 for I. Thus $\langle I, x_n, \ldots, x_{n-r+1}\rangle_m = R_m$ and $\operatorname{in}(\langle I, x_n, \ldots, x_{n-r+1}\rangle)$ is generated in degree $\leq m$.
By induction on i, suppose that $\operatorname{in}(\langle I, x_n, \ldots, x_i\rangle)$ is generated in degree $\leq m$. Then, by Lemma 5.1.16 $\operatorname{in}(I, x_n, \ldots, x_{i+1})$ is generated in degree $\leq m$. So iteratively, we can conclude that $\operatorname{in}(I)$ is generated in degree $\leq m$. Also, Corollary 5.1.17 implies that $\langle \operatorname{in}(I), x_n, \ldots, x_{n-r+1}\rangle_m = R_m$ and $(\langle \operatorname{in}(I), x_n, \ldots, x_{i+1}\rangle : x_i)_m = \langle \operatorname{in}(I), x_n, \ldots, x_{i+1}\rangle_m$. Then, Theorem 7.2.9 implies that $(x_n, \ldots x_{n-r+1}) \in U_r(\operatorname{in}(I))$ and $\operatorname{in}(I)$ is m-regular, i.e. $\operatorname{reg}(\operatorname{in}(I)) \leq \operatorname{reg}(I)$.

($\Leftarrow$) Let $m = \operatorname{reg}(\operatorname{in}(I))$. Choose a minimal homogeneous generator f of I. If there exists $g \in I$ and $1 \neq u \in \operatorname{Mon}(R)$ s.t. $\operatorname{in}(f) = u \operatorname{in}(g)$, we may replace f by $f - ug$, with $\operatorname{in}(f - ug) < \operatorname{in}(f)$. Iterating this procedure, we may assume that $\operatorname{in}(f)$ is a minimal generator of $\operatorname{in}(I)$ w.r.t the DRL-order, i.e. $\operatorname{in}(f) \in G(\operatorname{in}(I))$. This implies that $\deg(f) \leq m$, as $\operatorname{in}(I)$ is generated in degree $\leq m$, so I can be generated by elements of degree $\leq m$ as well. Thus, by Theorem 7.2.9 and Corollary 5.1.17 we have $(\langle I, x_n, \ldots, x_{i+1}\rangle : x_i)_m = \langle I, x_n, \ldots, x_{i+1}\rangle_m$ for $i = n, \ldots, n-r+1$ and $\langle I, x_n, \ldots, x_{n-r+1}\rangle_m = R_m$. Therefore, Theorem 7.2.9 implies that $(x_n, \ldots x_{n-r+1}) \in U_r(I)$ and I is m-regular, i.e $\operatorname{reg}(I) \leq \operatorname{reg}(\operatorname{in}(I))$.

(b) This follows immediately from parts of the proof of (a). □

Corollary 8.1.13 ([4], Corollary 2.5)**.** *Let I be a graded ideal of R and fix the DRL-order. If $(x_n, \ldots, x_{n-r+1}) \in U_r(I)$, then* $\operatorname{in}(I)$ *is generated in degree $\leq m$.*

Proof. This was shown in the ($\Rightarrow$)-direction of Theorem 8.1.12 □

Proposition 8.1.14 ([4], Proposition 2.9)**.** *Let I be a Borel-fixed monomial ideal generated by monomials of degree $\leq m$ with a minimal generator of degree m. If* $\operatorname{char}(k) = 0$*, then* $\operatorname{reg}(I) = m$*.*

Proof. It is clear that $\operatorname{reg}(I) \geq m$ as I has a minimal generator of degree m.

Since I contains a monomial $u \in \operatorname{Mon}(R)$ of degree m and I is Borel-fixed, by repeatedly applying Proposition 8.1.7 to u, we get that $x_1^m \in I$. Now, choose $r \geq 0$ s.t. $x_{n-r}^q \in I$ for some q but $x_{n-r+1}^p \notin I$ for all p.
Since I is generated by monomials of degree $\leq m$, we know that $x_{n-r}^m \in I$. Thus, applying Proposition 8.1.7 several times to x_{n-r}^m, we see that any monomial of degree m that only contains the variables $x_1, \ldots, x_{n-r}$ is also contained in I. Thus, $\langle I, x_n, \ldots, x_{n-r+1}\rangle_m = R_m$.

Next, let $J = \langle I, x_n, \ldots, x_{i+1}\rangle$ for some $i \in \{n-r+1, \ldots, n\}$. Suppose $x_i u \in J$, i.e. $u \in (J : x_i)$ for some $u \in \operatorname{Mon}_m(R)$. If $x_j | u$ for any $j \geq i+1$, then $u \in J$. If not, then $x_i u \in I$. Since $\deg(x_i u) = m+1$, it can not be a minimal generator of I and we may write $x_i u = x_j v$ for some $j \leq i$, with $v \in \operatorname{Mon}(I)$. If $j = i$ then $u = v \in J$. If $j < i$, then we can write $v = x_i w$ for some $w \in \operatorname{Mon}(R)$ and $u = x_j w$. Since $v \in I$, applying Proposition 8.1.7 to $v = x_i w$ yields $u = x_j w \in I$. This implies that $(J : x_i)_m = J_m$, i.e.$(\langle I, x_n, \ldots, x_{i+1}\rangle : x_i)_m = \langle I, x_n, \ldots, x_{i+1}\rangle_m$. So by Theorem 7.2.9 we can conclude that I is m-regular, i.e. $\operatorname{reg}(I) \leq m$. □

Lemma 8.1.15 ([4], Lemma 2.10)**.** *Let U be the generic open subset of $GL_n(k)$ as defined in Theorem 8.1.8 and let $U_2 \subseteq GL_n(k)$ given by*

$$U_2 = \{\boldsymbol{g} \in GL_n(k) : (x_n, \ldots x_{n-r+1}) \in U_r(\boldsymbol{g}I)\}.$$

Then $U \subseteq U_2$.

Proof. Let $\boldsymbol{g} \in U$. Since $\operatorname{in}(\boldsymbol{g}I)$ is Borel-fixed, so are its associated primes. But the only monomial prime ideals that are Borel-fixed can be those of the form $(x_1, \ldots, x_j)$ for $j = 1, \ldots, n-r$, where $r = \operatorname{kdim}(R/I)$. Thus, $(x_n, \ldots, x_{n-r+1}) \in U_r(\operatorname{in}_{DRL}(\boldsymbol{g}I))$. Finally, $(x_n, \ldots, x_{n-r+1}) \in U_r(\boldsymbol{g}I)$ by Theorem 8.1.12, which implies that $\boldsymbol{g} \in U_2$. □

Corollary 8.1.16 ([4], Proposition 2.11)**.** *Let I be a graded ideal of R with* $\operatorname{reg}(I) = m$ *and fix the DRL-order. Let* $\operatorname{char}(k) = 0$ *and let U be as in Theorem 8.1.8. Then* $\operatorname{in}(\boldsymbol{g}I)$ *has a minimal generator of degree m for all $\boldsymbol{g} \in U$.*

Proof. The monomial ideal $\operatorname{in}(\boldsymbol{g}I)$ is Borel-fixed by Theorem 8.1.10 for all $\boldsymbol{g} \in U$. The inclusion $U \subseteq U_2$, where U_2 is defined as in Lemma 8.1.15, implies that $(x_n, \dots, x_{n-r+1}) \in U_r(\boldsymbol{g}I)$ and by Theorem 8.1.12 it follows that $\operatorname{reg}(\operatorname{in}(\boldsymbol{g}I)) = m$. Thus, $\operatorname{in}(\boldsymbol{g}I)$ has a generator of degree m, as otherwise $\operatorname{reg}(\operatorname{in}(\boldsymbol{g}I)) < m$. □

These results allow us to show that, for an ideal in generic coordinates, the regularity does not change by taking the initial ideal w.r.t. the DRL-order.

Theorem 8.1.17 ([11], Theorem 3.20)**.** *Let I be a graded ideal of R that is in generic coordinates over $\overline{k}$. Then* $\operatorname{reg}(I) = \operatorname{reg}(\operatorname{in}_{DRL}(I))$.

Proof. Since I is in generic coordinates, we see that $\mathbf{1} \in U$, where $U \subseteq GL_n(k)$ is the Zariski open set as described in Theorem 8.1.8. Let $r = \operatorname{kdim}(R/I)$. Then, Lemma 8.1.15 implies that $\mathbf{1} \in \{\boldsymbol{g} \in GL_n(k) : (x_n, \dots, x_{n-r+1}) \in U_r(\boldsymbol{g}I)\}$. Thus, $(x_n, \dots, x_{n-r+1}) \in U_r(I)$. So by Theorem 8.1.12, it follows that $\operatorname{reg}(I) = \operatorname{reg}(\operatorname{in}_{DRL}(I))$. □

Remark 8.1.18. If $\operatorname{char}(k) = 0$, then $\operatorname{reg}(\operatorname{in}_{DRL}(I))$ is the maximal degree of a minimal system of generators of $\operatorname{in}_{DRL}(I)$. But since we work with the DRL-order, this implies that $\operatorname{reg}(\operatorname{in}_{DRL}(I)) = \operatorname{max.GB.deg}_{DRL}(I)$. If the characteristic is positive, one still has the inequality $\operatorname{max.GB.deg}_{DRL}(I) \leq \operatorname{reg}(\operatorname{in}_{DRL}(I))$. This is very often an equality. But there exist examples, where the inequality is strict [11].

8.2 Solving Degree

The computational complexity of computing a Gröbner basis in Algorithm 4 is dominated by the Gaussian elimination of Macaulay matrices for increasing values of d. Then, the size of the matrix and therefore the complexity is determined by d. Our goal in this section is to study the behaviour of this degree d and how to bound it. The concept of solving degree was originally introduced in [18] and was further studied in [11].

Definition 8.2.1. Let F be a set of polynomials of R and fix a monomial order σ. The *solving degree* of F w.r.t σ denoted $\operatorname{solv.deg}_\sigma(F)$ is the least degree $d \in \mathbb{Z}_{\geq 0}$ s.t. Gaussian elimination on the Macaulay matrix $M_{\leq d}(F)$ yields a σ-Gröbner basis of $I = \langle F \rangle$.
If F consists of homogeneous polynomials, then $\operatorname{solv.deg}_\sigma(F)$ is the least degree d s.t. Gaussian elimination on $M_0(F), \dots, M_d(F)$ produces a σ-Gröbner basis of I.

Lemma 8.2.2 ([11], Remark 3.4)**.** *Let $F \subseteq R$ be a set of polynomials and let σ be a monomial order. Then* $\operatorname{max.GB.deg}_\sigma(F) \leq \operatorname{solv.deg}_\sigma(F)$, *where equality holds if F consists of homogeneous polynomials.*

Proof. This is clear, as the polynomials appearing in the d-th step of Algorithm 4 have at most degree d and reducing the Gröbner basis does not increase the degree. If all $f \in F$ are homogeneous, then Gaussian elimination on $M_d(F)$ only produced rows corresponding to polynomials of degree d. So the resulting Gröbner basis does contain elements of degree d. □

The next result allows us to compare the solving degrees of different sets of polynomials and relate them to the maximal degree of an element in the reduced Gröbner basis of the ideal they generate.

Theorem 8.2.3 ([11], Theorem 3.14)**.** *Let $F = \{f_1, \dots, f_r\}$ be a set of polynomials in R. Let $\tilde{F} = \{f_1^h, \dots, f_r^h\} \subseteq I^h \subseteq S = R[t]$, where I^h denotes the homogenization of $I = \langle f_1, \dots, f_r \rangle$. Fix the DRL-order on R and DRL^+ on S. Then*

$$\begin{aligned}\text{max. GB. deg}_{DRL^+}(I^h) &= \text{max. GB. deg}_{DRL}(F) \leq \text{solv. deg}_{DRL}(F)\\ &= \text{solv. deg}_{DRL^+}(\tilde{F}) = \text{max. GB. deg}_{DRL^+}(\tilde{F}).\end{aligned}$$

Proof. The equality $\text{solv. deg}_{DRL^+}(\tilde{F}) = \text{max. GB. deg}_{DRL^+}(\tilde{F})$ is immediate by Lemma 8.2.2 as $\tilde{F}$ is homogeneous.

$\text{max. GB. deg}_{DRL}(F) \leq \text{solv. deg}_{DRL}(F)$ was shown in Lemma 8.2.2.

By Theorem 5.4.3, the dehomogenization of DRL^+-Gröbner basis of I^h yields a DRL-Gröbner basis of $\langle F \rangle$. Since dehomogenization does not increase the degree, it follows that we have $\text{max. GB. deg}_{DRL}(F) \leq \text{max. GB. deg}_{DRL^+}(I^h)$.
Also, by Proposition 5.4.6, the homogenization of a DRL-Gröbner basis of $\langle F \rangle$ produces a DRL^+-Gröbner basis of I^h. Since homogenization does not increase the degree of the terms of highest degrees, we have $\text{max. GB. deg}_{DRL^+}(I^h) \leq \text{max. GB. deg}_{DRL}(F)$.

To show that $\text{solv. deg}_{DRL}(F) = \text{solv. deg}_{DRL^+}(\tilde{F})$ we claim that the Macaulay matrix $M_{\leq d}(F)$ w.r.t DRL is equal to $M_d(\tilde{F})$ w.r.t DRL^+ for every $d \geq 1$.

Clearly, there is a bijection between $\text{Mon}_d(S)$ and $\text{Mon}_{\leq d}(R)$, i.e. between the column-indices of $M_d(\tilde{F})$ and $M_{\leq d}(F)$, given by dehomogenization as every $m \in \text{Mon}_{\leq d}(R)$ can be written as $m = \phi(n)$ for $n = mt^{d-deg(m)} \in \text{Mon}_d(S)$ and for every $n \in \text{Mon}_d(S)$ there is $m \in \text{Mon}_{\leq d}(R)$ s.t. $n = mt^{d-deg(m)}$.
This bijection is order-preserving: If we have $m_1 >_{DRL^+} m_2$ for $m_1, m_2 \in \text{Mon}_d(S)$, then by rewriting $m_1 = n_1 t^{d_1}, m_2 = n_2 t^{d_2}$ for some $n_1, n_2 \in \text{Mon}_{\leq d}(R)$, we either have $d_1 < d_2$ or $n_1 >_{DRL} n_2$. Both of these cases imply that $\phi(m_1) >_{DRL} \phi(m_2)$.

Also, if $m_{ij} f_j^h$ is the index of a row of $M_d(\tilde{F})$, i.e. $\deg(m_{ij} f_j^h) = d$, then $\phi(m_{ij} f_j^h) = \phi(m_{ij}) f_j$ has degree $\leq d$ and is an index of a row in $M_{\leq d}(F)$.

Conversely, every index $m_{ij} f_j^h$ of a row of $M_d(\tilde{F})$ can be obtained from an index of a row of $M_{\leq d}(F)$ by homogenizing and multiplying by an appropriate power of t. Thus, there is also a bijection between the set of shifts defining the matrix, i.e. the indices of the rows.

Considering a homogeneous polynomial $m_{ij} f_j^h = \sum_{j=1}^{l} c_i^{(j)} u_j$, $c_i^{(j)} \in k, u_j \in \text{Mon}_d(S)$ corresponding to a row vector $(c_i^{(1)}, \dots, c_i^{(l)})$ of $M_d(\tilde{F})$, it is easy to see that the polynomial $\phi(m_{ij}) f_j = \sum_{j=1}^{l} c_i^{(j)} \phi(u_j)$, $c_i^{(j)} \in k, u_j \in \text{Mon}_d(S)$ corresponds to the same row vector in $M_{\leq d}(F)$. This yields that $M_d(\tilde{F}) = M_{\leq d}(F)$.

Since by Theorem 5.4.3 the dehomogenization of a Gröbner basis of $\langle \tilde{F} \rangle$ yields a Gröbner basis of $\langle F \rangle$, we get $\text{solv. deg}_{DRL}(F) \leq \text{solv. deg}_{DRL^+}(\tilde{F})$.

To show equality, consider for each minimal generator m of $\text{in}_{DRL}(\langle \tilde{F} \rangle)$ the least degree d, for which a polynomial f with $\text{in}_{DRL}(f) = m$ corresponds to a row of $\text{rref}(M_{\leq d}(F))$. By the equality of the Macaulay matrices, the polynomial $t^{d-\deg(f)} f^h$ corresponds to one of the rows of $\text{rref}(M_d(\tilde{F}))$.

Suppose a polynomial g with $\text{in}_{DRL^+}(g) | t^{d-\deg(f)} m = \text{in}_{DRL^+}(t^{d-\deg(f)} f^h)$ corresponds to a row of $\text{rref}(M_e(\tilde{F}))$ for some degree $e < d$. Then, from Lemma 5.4.5, it follows that we have $\text{in}_{DRL}(\phi(g)) = \phi(\text{in}_{DRL^+}(g)) = m$ and $\phi(g)$ would correspond to a row of $\text{rref}(M_{\leq e}(F))$, which is a contradiction to the choice of d. Thus, no such g exists. Therefore, the least degree d, in which the leading terms of the rows of $\text{rref}(M_{\leq d}(F))$ generate $\text{in}_{DRL}(\langle \tilde{F} \rangle)_d$ is the same as the least degree d', in which the rows of $\text{rref}(M_{d'}(\tilde{F}))$ generate $\text{in}_{DRL^+}(\langle \tilde{F} \rangle)_{d'}$. Thus, we have

$$\text{solv. deg}_{DRL}(F) = \text{solv. deg}_{DRL^+}(\tilde{F}). \qquad \square$$

Combining the results regarding regularity and solving degree finally allows us to bound the solving degree.

Theorem 8.2.4 ([11], Theorem 3.22)**.** *Let $F = \{f_1, \dots, f_r\} \subseteq R$ be a system of homogeneous polynomials and suppose that $\langle F \rangle$ is in generic coordinates over $\overline{k}$. Then*

$$\text{solv.}\deg_{DRL}(F) \leq \text{reg}(F).$$

Proof. We may extend all ideals to $\overline{k}$, as $\text{max.}\,\text{GB.}\deg(F)$ and $\text{reg}(F)$ are invariant under this process. Lemma 8.2.2, Proposition 8.1.14 and Theorem 8.1.17 yield

$$\text{solv.}\deg_{DRL}(F) = \text{max.}\,\text{GB.}\deg_{DRL}(F) \leq \text{reg}(\text{in}_{DRL}(F)) = \text{reg}(F). \qquad \square$$

A similar result holds for non-homogeneous polynomials.

Theorem 8.2.5 ([11], Theorem 3.23)**.** *Let $F = \{f_1, \dots, f_r\} \subseteq R$ be a system of non-homogeneous polynomials and let $\tilde{F} = \{f_1^h, \dots, f_r^h\} \subseteq S$. Suppose $\langle \tilde{F} \rangle$ is in generic coordinates over $\overline{k}$. Then*

$$\text{solv.}\deg_{DRL}(F) \leq \text{reg}_S(\tilde{F}).$$

Proof. Again, we may extend all ideals to $\overline{k}$. Then, Theorem 8.2.3, Proposition 8.1.14 and Theorem 8.1.17 yield

$$\text{solv.}\deg_{DRL}(F) = \text{solv.}\deg_{DRL^+}(\tilde{F}) = \text{max.}\,\text{GB.}\deg_{DRL^+}(\tilde{F}) \leq \text{reg}_S(\text{in}_{DRL^+}(\tilde{F})) = \text{reg}_S(\tilde{F}).$$
$\square$

Remark 8.2.6. When, $\text{char}(k) = 0$ (and also very often in positive characteristic as mentioned in Remark 8.1.18), the upper bound is an equality by Corollary 8.1.15.

Combining these results with upper bounds on regularity we get

Theorem 8.2.7 (Macaulay bound, [11], Corollary 3.25)**.** *Let $F = \{f_1, \dots, f_r\} \subseteq R$ by a system of r polynomials with $d_i = \deg(f_i)$ and $d_1 \geq d_2 \geq \cdots \geq d_r$. Let $l = \min(n+1, r)$. Let $\tilde{F} = \{f_1^h, \dots, f_r^h\}$ and assume that $|\mathcal{V}_p(\tilde{F})| < \infty$ and that $\langle \tilde{F} \rangle$ is in generic coordinates over $\overline{k}$. Then*

$$\text{solv.}\deg_{DRL}(F) \leq d_1 + \cdots + d_l - l + 1.$$

If $r > n$ and $d = d_1$, then

$$\text{solv.}\deg_{DRL}(F) \leq (n+1)(d-1) + 1.$$

Proof. Since $\langle \tilde{F} \rangle$ is in generic coordinates, Theorem 8.2.5 implies $\text{solv.}\deg_{DRL}(F) \leq \text{reg}_S(\tilde{F})$. $|\mathcal{V}_p(\tilde{F})| < \infty$ implies that $\dim^p(\mathcal{V}_p(\tilde{F})) = 0$, or $\mathcal{V}_p(\tilde{F}) = \emptyset$. Thus, by Corollary 6.1.29 this means that $\text{kdim}(S/\langle \tilde{F} \rangle) \leq 1$. Applying Lemma 7.1.14 and Theorem 7.1.15, we get the desired inequality $\text{solv.}\deg_{DRL}(F) \leq \text{reg}_S(\tilde{F}) \leq d_1 + \cdots + d_l - l + 1$.
The second part of the statement is immediate, as $\text{reg}_S(\tilde{F}) \leq l(d-1)+1 \leq (n+1)(d-1)+1$. $\square$

Example 8.2.8. Let $F = \{x^2 - 1, xy + x\} \subseteq k[x, y]$ and $\tilde{F} = \{x^2 - z^2, xy + xz\} \subseteq k[x, y, z]$. We have seen in Example 4.2.4 that $|\mathcal{V}_p(\tilde{F})| < \infty$. Therefore, Theorem 8.2.7 implies that $\text{solv.}\deg_{DRL}(F) \leq 2 + 2 - 2 + 1 = 3$.
This coincides with Examples 5.6.6 and 7.1.7, where we had $\text{solv.}\deg_{DRL}(\tilde{F}) = 3 = \text{reg}_S(\tilde{F})$.

This recovers a result shown by D. Lazard [35], who proved this bound for $\text{max.}\,\text{GB.}\deg_{DRL}(F)$. Notice that if additionally $f_1^h, \dots, f_r^h$ form a regular sequence, then by Lemma 7.1.13 we have that $\text{reg}_S(\tilde{F}) = d_1 + \cdots + d_l - l + 1$ and since $\text{max.}\,\text{GB.}\deg_{DRL}(\tilde{F}) = \text{reg}_S(\text{in}_{DRL^+}(\tilde{F}))$ holds most of the time, then $\text{solv.}\deg_{DRL}(F) = d_1 + \cdots + d_l - l + 1$ holds most of the time.

That $\langle \tilde{F} \rangle$ is in generic coordinates, is usually not easy to verify, but if we work over a finite field and add some equations to F, it is possible to show that the result of Theorem 8.2.7 still holds.

Definition 8.2.9. Let $\mathbb{F}_q$ be a finite field, where $q = p^e$ for some p prime. Then the polynomials $Q = \{x_1^q - x_1, \dots, x_n^q - x_n\} \subseteq \mathbb{F}_q[x_1, \dots, x_n]$ are called the *field equations* of $\mathbb{F}_q$.

For an arbitrary system of finitely many polynomials $F = \{f_1, \dots, f_r\} \subseteq \mathbb{F}_q[x_1, \dots, x_n]$, we have $\mathcal{V}(F \cup Q) = \mathcal{V}(F) \cap \mathbb{F}_q$. Thus, adding the field equations ensures that a system of polynomials has finitely many solutions that also lie in $\mathbb{F}_q$.

Theorem 8.2.10 ([11], Theorem 3.26)**.** *Let $\mathbb{F}_q$ be a field with $\mathrm{char}(\mathbb{F}_q) = p > 0$ prime and let $q = p^e$. Let $F = \{f_1, \dots, f_r\} \subseteq k[x_1, \dots, x_n]$ be a system of polynomials. Set $d_i = \deg(f_i)$ with $d_1 \geq d_2 \geq \cdots \geq d_r$ and $l = \min(n+1, r)$. Suppose F contains the field-equations Q of $\mathbb{F}_q$. Then*

$$\text{solv.deg}_{DRL}(F) \leq d_1 + \cdots + d_l - l + 1.$$

If $r > n$ and $d = d_1$, then

$$\text{solv.deg}_{DRL}(F) \leq (n+1)(d-1) + 1.$$

Proof. Let $\tilde{F} = \{f_1^h, \dots, f_r^h\} \subseteq S$. Since F contains the field equations, evaluating the equations of $\tilde{F}$ at $t = 0$ yields $x_1 = \cdots = x_n = 0$, so $\mathcal{V}_p(\tilde{F})$ does not contain points at infinity. $\mathcal{V}_p(\tilde{F})$ contains also only finitely many points with $t = 1$, as F contains the field equations of the finite field $\mathbb{F}_q$. Thus, we have $|\mathcal{V}_p(\tilde{F})| < \infty$.
This also means that t is a nonzerodivisor on $S/\langle \tilde{F} \rangle^{sat}$, i.e. t is generic for $\langle \tilde{F} \rangle$, i.e. $t \in U_1(\langle \tilde{F} \rangle)$, as defined in Definition 7.2.4. Thus, by Theorem 8.1.12, we have $\mathrm{reg}_S(\mathrm{in}_{DRL^+}(\langle \tilde{F} \rangle)) = \mathrm{reg}_S(\langle \tilde{F} \rangle)$ as well as $\text{max. GB.deg}_{DRL^+}(\tilde{F}) \leq \mathrm{reg}_S(\mathrm{in}_{DRL^+}(\tilde{F}))$. So, the result follows.
The second part of the statement follows the same way as in Theorem 8.2.7. □

8.3 Degree of Regularity

The degree of regularity was introduced in [3] and is often used to estimate the complexity of Gröbner basis algorithms. Let $R = k[x_1, \dots, x_n]$ be standard graded and let I be a graded ideal of R. Let $M = R/I$. Recall the notion of the Hilbert series and the fact that it can be expressed as

$$HS_M(t) = \frac{h_M(t)}{(1-t)^d},$$

where $h_M \in \mathbb{Z}[t]$ s.t. $h_M(1) \neq 0$. As the Hilbert function coincides with the Hilbert polynomial for large enough values, it is of interest to study, from which integer onwards this is the case.

Definition 8.3.1. The *index of regularity* of I is the smallest positive integer s.t. the Hilbert function and the Hilbert polynomial start to coincide, i.e.

$$i_{reg}(I) = \min\{m \in \mathbb{N} : HP_{R/I}(s) = HF_{R/I}(s)\ \forall s \geq m\}.$$

If the Hilbert series is known, the index of regularity can be deduced from it.

Theorem 8.3.2 ([8], Proposition 4.1.12)**.** *Let I be a graded ideal of R and let $b = \deg(h_{R/I})$ and $d = d(R/I)$. Then*

$$i_{reg}(I) = b - d + 1.$$

Proof. Since $h_{R/I}(t)$ is a polynomial of degree b we can write it as $h_{R/I}(t) = \sum_{i=a}^{b} h_i t^i$, with $h_b \neq 0$. Define

$$H_i(t) = \frac{h_i t^i}{(1-t)^d} \text{ and } P_i(s) = h_i \binom{s-i+d-1}{d-1}.$$

First, we see that

$$\begin{aligned}\sum_{s=i}^{\infty} P_i(s)t^s &= \sum_{s=i}^{\infty} h_i \binom{s-i+d-1}{d-1} t^s \\ &= h_i t^i \sum_{s=0}^{\infty} \binom{s+d-1}{d-1} t^s \\ &= \frac{h_i t^i}{(1-t)^d} = H_i(t).\end{aligned}$$

But since by convention we have that $\binom{s-i+d-1}{d-1} = 0$ for $s = i-(d-1), \ldots, i-1$, we even have

$$H_i(t) = \sum_{s=i-(d-1)}^{\infty} P_i(s)t^s.$$

Next, we have

$$\begin{aligned}\sum_{s=0}^{\infty} HF_{R/I}(s)t^s = HS_{R/I}(t) = \sum_{i=a}^{b} H_i(t) &= \sum_{i=a}^{b} \left(\sum_{s=i-(d-1)}^{\infty} P_i(s)t^s \right) \\ &= \sum_{s=a-d+1}^{b-d} \left(\sum_{i=a}^{s+d-1} P_i(s)t^s \right) + \sum_{s=b-d+1}^{\infty} \left(\sum_{i=a}^{b} P_i(s)t^s \right).\end{aligned}$$

Thus, by comparing coefficients of t^s we get

$$\begin{aligned}HF_{R/I}(b-d) &= \sum_{i=1}^{b-1} P_i(b-d) \\ HF_{R/I}(b-d+i) &= \sum_{i=1}^{b} P_i(b-d+i) \ \forall i > 0\end{aligned}$$

On the other hand $\sum_{i=a}^{b} P_i(s) = \sum_{i=a}^{b} h_i \binom{s-i+d-1}{d-1}$ is a polynomial of degree $d-1$ that coincides with $HF_{R/I}(s)t^s$ for $s \geq b-d+1$. Thus, $HP_{R/I}(s) = \sum_{i=1}^{b} P_i(s)$ for all $s \in \mathbb{Z}$.
So by comparing $HP_{R/I}$ with $HF_{R/I}$ we see that

$$HP_{R/I}(s) = \sum_{i=a}^{b} P_i(s) = HF_{R/I}(s) \text{ for } s \geq b-d+1.$$

But we also have

$$HP_{R/I}(b-d) = \sum_{i=a}^{b} P_i(b-d) \neq \sum_{i=a}^{b-1} P_i(b-d) = HF_{R/I}(b-d),$$

since $P_b(b-d) = h_b \binom{b-d-b+d-1}{d-1} \neq 0$.
Thus, we can conclude that $i_{reg}(I) = b-d+1$. □

The next result is due to J.-P. Serre and allows us to compare the Hilbert function and Hilbert polynomial to local cohomology.

Theorem 8.3.3 ([8], Theorem 4.4.3)**.** *Let I be a graded ideal with $d = d(R/I)$. Then*

$$HF_{R/I}(s) - HP_{R/I}(s) = \sum_{i=0}^{d} (-1)^i \dim_k(H^i_{\mathfrak{m}}(R/I)_s) \text{ for all } s \in \mathbb{Z}_{\geq 0}.$$

Proof. Let $M = R/I$. By Corollary 6.1.29, we have that $\operatorname{kdim}(M) = d(M)$. The proof is done by induction on d.

If $d = 0$, then $HP_M = 0$ and $H^0_{\mathfrak{m}}(M) = M$, where $H^i_{\mathfrak{m}}(M) = 0$ for all $i > 0$. Then both sides equal $\dim_k(M_s)$ and the result follows.

Now, suppose $d > 0$ and the result holds for $d-1$. We replace M with $M/H^0_{\mathfrak{m}}(M)$. Then the RHS of the equation gets smaller by $\dim_k(H^0_{\mathfrak{m}}(M))$, as $H^i_{\mathfrak{m}}(M/H^0_{\mathfrak{m}}(M)) \cong H^i_{\mathfrak{m}}(M)$ for all $i > 0$ by Theorem 3.4.20.
On the LHS, the Hilbert function gets smaller by $\dim_k(H^0_{\mathfrak{m}}(M))$ by definition. Meanwhile, since $H^0_{\mathfrak{m}}(M) = \Gamma_{\mathfrak{m}}(M)$ is $\mathfrak{m}$-torsion we have that $\dim_k(H^0_{\mathfrak{m}}(M)) < \infty$, which implies that $HP_M = HP_{M/H^0_{\mathfrak{m}}(M)}$. So the LHS also gets smaller by $H^0_{\mathfrak{m}}(M)$ in total. Thus, we may assume that $H^0_{\mathfrak{m}} = 0$. Then, by Lemma 3.4.9, $\mathfrak{m}$ contains a homogeneous M-regular element of say degree e. This allows us to construct the short exact sequence

$$0 \to M(-e) \xrightarrow{x} M \to M/xM \to 0. \tag{8.1}$$

Define the two functions

$$H'_M(t) = \sum_{s\geq 0} (HF_M(s) - HP_M(s))\, t^s,$$
$$H''_M(t) = \sum_{s\geq 0} \left(\sum_{i=0}^{d} (-1)^i \dim_k(H^i_{\mathfrak{m}}(M)_s) \right) t^s$$

As in the proof of Proposition 6.2.12, we see that $HS_{M/xM}(t) = (1-t^e)HS_M(t)$, so by comparing coefficients we get $HF_{M/xM}(s) = HF_M(s) - HF_M(s-e)$, which then consequently implies that $HP_{M/xM}(s) = HP_M(s) - HP_M(s-e)$ for all s sufficiently large. Therefore, we have $HP_{M/xM}(s) = HP_M(s) - HP_M(s-e)$ for all $s \geq 0$. Thus, we have

$$\begin{aligned} H'_{M/xM}(t) &= \sum_{s\geq 0} (HF_M(s) - HF_M(s-e) + HP_M(s) - HP_M(s-e))\, t^s \\ &= (1-t^e) \left(\sum_{s\geq 0} HF_M(s) - HP_M(s) \right) = (1-t^e) H'_M(t). \end{aligned}$$

On the other hand, (8.1) and the long exact sequence of graded local cohomology yields

$$\begin{aligned} 0 \to H^0_{\mathfrak{m}}(M)_{s-e} \to H^0_{\mathfrak{m}}(M)_s \to H^0_{\mathfrak{m}}(M/xM)_s \to \cdots \\ \cdots \to H^d_{\mathfrak{m}}(M)_{s-e} \to H^d_{\mathfrak{m}}(M)_s \to H^d_{\mathfrak{m}}(M/xM)_{s-e} = 0 \to 0. \end{aligned}$$

Then, Corollary 6.2.3 yields

$$\sum_{i=0}^{d-1} \dim_k(H^i_{\mathfrak{m}}(M/xM)_s) = \sum_{i=0}^{d} \dim_k(H^i_{\mathfrak{m}}(M)_s) - \sum_{i=0}^{d} \dim_k(H^i_{\mathfrak{m}}(M)_{s-e}).$$

Thus,

$$\begin{aligned} H''_{M/xM}(t) &= \sum_{s\geq 0} \left(\sum_{i=0}^{d-1} \dim_k(H^i_{\mathfrak{m}}(M/xM)_s) \right) t^s \\ &= (1-t^e) \sum_{s\geq 0}^{d} (-1)^i \dim_k(H^i_{\mathfrak{m}}(M)_s) t^s \\ &= (1-t^e) H''_M(t). \end{aligned}$$

Applying the inductive hypothesis, we obtain $H''_{M/xM}(t) = H'_{M/xM}(t)$, so we can conclude $H''_M(t) = H'_M(t)$. Then, by comparing coefficients of t^s in $H''_M(t)$ and $H'_M(t)$, the result follows. □

Being able to relate the difference between the Hilbert function and the Hilbert polynomial with local cohomology suggests that there is, additionally to a similar name, some relation between the index of regularity and Castelnuovo–Mumford regularity. As it turns out, the index of regularity is bounded by Castelnuovo–Mumford regularity, i.e. for values larger than $\operatorname{reg}(I)$, the Hilbert function coincides with the Hilbert polynomial.

Corollary 8.3.4 ([23], Corollary 4.8)**.** *Let I be a graded ideal of R. Then*

$$i_{reg}(I) \leq \operatorname{reg}(I).$$

Moreover, if $R_s = I_s$ for s sufficiently large, equality holds.

Proof. Let $m = \operatorname{reg}(I) = \operatorname{reg}(R/I) + 1$. Then $H^i_{\mathfrak{m}}(R/I)_s = 0$ for all $s \geq m - i$ and $i \geq 0$. By Theorem 8.3.3 we have

$$HF_{R/I}(m) - HP_{R/I}(m) = \sum_{i=0}^{d} (-1)^d \dim_k(H^i_{\mathfrak{m}}(R/I)_m).$$

But since $m \geq m-i$ for all $i \geq 0$, the RHS vanishes s.t. $HF_{R/I}(s) = HP_{R/I}(s)$ for all $s \geq \operatorname{reg}(I)$, i.e $i_{reg}(I) \leq \operatorname{reg}(I)$.

Now, if $R_s = I_s$ for s sufficiently large, then $HP_{R/I} = 0$, i.e. $\operatorname{kdim}(R/I) = 0$ s.t. $H^i_{\mathfrak{m}}(R/I) = 0$ for all $i > 0$. Thus, $HF_{R/I}(s) - HP_{R/I}(s) = \dim_k(H^0_{\mathfrak{m}}(R/I))_s$. Thus, if $m + 1 = i_{reg}(I)$, then $\dim_k(H^0_{\mathfrak{m}}(R/I)_s) = 0$ for all $s \geq m + 1$ and $H^i_{\mathfrak{m}}(R/I)_s = 0$ for all $s \geq m - i + 1$. This means that $\operatorname{reg}(R/I) \leq i_{reg}(I) - 1$ or equivalently $\operatorname{reg}(I) \leq i_{reg}(I)$, which concludes the second part of the statement. □

Example 8.3.5. As usual let $I = \langle x^2 - z^2, xy + xz\rangle \subseteq R = k[x, y, z]$. We know from Example 6.1.16 that $HF_{R/I}(1) = 3$ and $HF_{R/I}(s) = 4 = HP_{R/I}(s)$ for all $s \geq 2$. Thus, $i_{reg}(I) = 2$. But $\operatorname{reg}(I) = 3$, so equality in Corollary 8.3.4 does not always hold.

Definition 8.3.6. Let $F = \{f_1, \ldots, f_r\} \subseteq R$ be a finite set of polynomials and define the set $F^{top} = \{f_1^{top}, \ldots . f_r^{top}\}$ as the set of the homogeneous parts of highest degree of the polynomials in F. Assume that $\langle F^{top}\rangle_s = R_s$ for s sufficiently large. Then the *degree of regularity* of F is defined to be $d_{reg}(F) = i_{reg}(\langle F^{top}\rangle)$.

Note that the assumption $\langle F^{top}\rangle_s = R_s$ for s sufficiently large implies that $|\mathcal{V}(F)| < \infty$, but the other way around does not have to be true.

Lemma 8.3.7 ([11], Proposition 4.5)**.** *Let $F = \{f_1, \ldots, f_r\} \subseteq R$ be a set of polynomials and suppose $\langle F^{top}\rangle_s = R_s$ for s sufficiently large. Then*

$$d_{reg}(F) = \operatorname{reg}(F^{top}).$$

Moreover, if F is homogeneous, then $d_{reg}(F) = \operatorname{reg}(F)$.

Proof. By Corollary 8.3.4 and the definition of d_{reg}, we have $d_{reg}(F) = i_{reg}(\langle F^{top}\rangle) = \operatorname{reg}(F^{top})$. The second part follows directly, since in this case we have $F = F^{top}$. □

The assumption $\langle F^{top}\rangle_s = R_s$ for s sufficiently large, yields that the degree of regularity can be seen as an upper bound on $\max.\,\mathrm{GB}.\deg(F)$.

Lemma 8.3.8 ([11], Remark 4.6)**.** *Let F be a system of polynomials and fix a degree compatible monomial order σ on R. Assume that $\langle F^{top}\rangle_s = R_s$ for s sufficiently large. Then*

$$\max.\,\mathrm{GB}.\deg_\sigma(F) \leq d_{reg}(F).$$

Proof. Let $I = \langle F\rangle, J = \langle F^{top}\rangle$. Then $HP_{R/\operatorname{in}(J)} = HP_{R/J} = 0$. Thus, $J_s = \operatorname{in}_\sigma(J)_s = R_s$ for $s \geq d_{reg}(F)$. $\operatorname{in}_\sigma(J)_s \subseteq \operatorname{in}_\sigma(I)_s$ is true for all s, because σ is degree compatible. Thus, $\operatorname{in}(I)_s = R_s$ for all $s \geq d_{reg}(F)$. Thus, every element of the reduced σ-Gröbner basis of I is of degree $\leq d_{reg}(F)$, which proves the statement. □

Given a system of polynomials $F = \{f_1, \ldots, f_r\}$, there is a simple relation between the homogeneous ideals $\langle F^{top}\rangle \subseteq R$ and $\tilde{F} = \{f_1^h, \ldots, f_r^h\} \subseteq S$, namely

$$\langle F^{top}\rangle S + \langle t\rangle = \langle \tilde{F}\rangle + \langle t\rangle. \tag{8.2}$$

Since $F^{top} \subseteq R$ it is clear that t is a nonzerodivisor on $S/\langle F^{top}\rangle S$.
If additionally, the element t is a nonzerodivisor on $S/\langle \tilde{F}\rangle$, we get another interesting property. Let $\varphi : S \to S$, $t \mapsto 0$. Clearly, $S/\langle t\rangle \cong R$. Theorem 3.4.21 and the relation (8.2) lead to the following result.

Lemma 8.3.9. *Let $\tilde{F} = \langle f_1^h, \ldots, f_r^h\rangle \subseteq S$ s.t $|\mathcal{V}_p(\tilde{F})| < \infty$. If t is $S/\langle \tilde{F}\rangle$-regular, then*

$$\operatorname{reg}_S(\tilde{F}) = \operatorname{reg}_{S/\langle t\rangle}(\langle \tilde{F}, t\rangle/\langle t\rangle).$$

Proof. Since $|\mathcal{V}_p(\tilde{F})| < \infty$, we have that $\dim^p(\mathcal{V}_p(\tilde{F})) = 0$ i.e. $\operatorname{kdim}(S/\langle \tilde{F}\rangle) = 1$. Thus, $\operatorname{kdim}(S/\langle \tilde{F}, t\rangle) = 0$, since t is $S/\langle \tilde{F}\rangle$-regular. The element t is $S/\langle \tilde{F}\rangle$-regular, thus

$$0 \to S/\langle \tilde{F}\rangle(-1) \xrightarrow{t} S/\langle \tilde{F}\rangle \to S/\langle \tilde{F}, t\rangle \to 0 \tag{8.3}$$

is exact.

($\geq$) Let $\operatorname{reg}_S(\tilde{F}) = m+1$, i.e. $\operatorname{reg}_S(S/\langle \tilde{F}\rangle) = m$. Since $\operatorname{reg}_S(\tilde{F}) \leq m+1$ and t is $S/\langle \tilde{F}\rangle$-regular, by Lemma 7.2.7 it follows that $\operatorname{reg}_S(\langle \tilde{F}, t\rangle) \leq m+1$. Thus, $\operatorname{reg}_S(S/\langle \tilde{F}, t\rangle) \leq m$. Since $S/\langle \tilde{F}, t\rangle$ can be seen as an $S/\langle t\rangle$-module, the independence theorem implies that we have $\operatorname{reg}_{S/\langle t\rangle}((S/\langle t\rangle)/(\langle \tilde{F}, t\rangle/\langle t\rangle)) = \operatorname{reg}_{S/\langle t\rangle}(S/(\tilde{F}, t)) \leq m$. Thus, $\operatorname{reg}_{S/\langle t\rangle}(\langle \tilde{F}, t\rangle/\langle t\rangle) \leq m+1$.

($\leq$) Let $\operatorname{reg}_{S/\langle t\rangle}(\langle \tilde{F}, t\rangle/\langle t\rangle) = m+1$, i.e. $\operatorname{reg}_{S/\langle t\rangle}(S/\langle \tilde{F}, t\rangle) = \operatorname{reg}_{S/\langle t\rangle}((S/\langle t\rangle)/(\langle \tilde{F}, t\rangle/\langle t\rangle)) = m$. Then $\operatorname{reg}_S(S/\langle \tilde{F}, t\rangle) = m$ by the independence theorem.
Consider (8.3) and the resulting long exact sequence of cohomology:

$$\begin{aligned} 0 \to H^0_{\mathfrak{m}}(S/\langle \tilde{F}\rangle(-1))_d \to H^0_{\mathfrak{m}}(S/\langle \tilde{F}\rangle)_d \to H^0_{\mathfrak{m}}(S/\langle \tilde{F}, t\rangle)_d \to \\ \to H^1_{\mathfrak{m}}(S/\langle \tilde{F}\rangle(-1))_d \to H^1_{\mathfrak{m}}(S/\langle \tilde{F}\rangle)_d \to 0. \end{aligned}$$

Since $\operatorname{reg}_S(S/\langle \tilde{F}, t\rangle) = m$ we have $H^0_{\mathfrak{m}}(S/\langle \tilde{F}, t\rangle)_d = 0$ for all $d \geq m - i + 1$. Thus, we have

$$H^0_{\mathfrak{m}}(S/\langle \tilde{F}\rangle)_{d-1} = H^0_{\mathfrak{m}}(S/\langle \tilde{F}\rangle)_d = H^0_{\mathfrak{m}}(S/\langle \tilde{F}, t\rangle)_{d+1} = \cdots = 0$$

and

$$H^1_{\mathfrak{m}}(S/\langle \tilde{F}\rangle)_{d-1} = H^1_{\mathfrak{m}}(S/\langle \tilde{F}\rangle)_d = H^1_{\mathfrak{m}}(S/\langle \tilde{F}, t\rangle)_{d+1} = \cdots = 0.$$

Thus, $H^1_{\mathfrak{m}}(S/\langle \tilde{F}\rangle)_d = 0$ for all $d \geq m - i + 1$, so $\operatorname{reg}_S(S/\langle \tilde{F}\rangle) \leq m$, i.e. $\operatorname{reg}_S(\tilde{F}) \leq m+1$. □

Viewing F^{top} as the homomorphic image of $\langle \tilde{F}, t\rangle/\langle t\rangle$ under the natural isomorphism $S/\langle t\rangle \cong R$ yields the following relationship between the degree of regularity and the Castelnuovo–Mumford regularity.

Theorem 8.3.10 ([5], Corollary 2.6)**.** *Let $F = \{f_1, \dots, f_r\}$ s.t. $\langle F^{top}\rangle_s = R_s$ for s sufficiently large. Assume t is $S/\langle \tilde{F}\rangle$-regular. Then $d_{reg}(F) = \mathrm{reg}_S(\tilde{F})$.*

Proof. By (8.2) we have that $\langle F^{top}\rangle S + \langle t\rangle = \langle \tilde{F}\rangle + \langle t\rangle$ and $S/\langle t\rangle \cong R$. This gives us

$$\mathrm{reg}_R(F^{top}) = \mathrm{reg}_{S/\langle t\rangle}(\langle F^{top}\rangle S + \langle t\rangle)/\langle t\rangle) = \mathrm{reg}_{S/\langle t\rangle}(\langle \tilde{F}, t\rangle/\langle t\rangle) = \mathrm{reg}_S(\tilde{F}),$$

where the last equality follows from Lemma 8.3.9. Then we get the equality we wanted to show: $d_{reg}(F) = i_{reg}(F^{top}) = \mathrm{reg}_R(F^{top}) = \mathrm{reg}_S(\tilde{F})$. □

The result above shows that under the assumption that t is $S/\langle \tilde{F}\rangle$-regular we can bound $\mathrm{solv.deg}_{DRL}(F)$ by $d_{\mathrm{reg}}(F)$. However, this assumption is pretty restrictive since it implies that $\langle \tilde{F}\rangle = \langle F\rangle^h$, which is generally not the case.

Lemma 8.3.11 ([5], Theorem 4.12)**.** *If t is nonzerodivisor on $S/\langle \tilde{F}\rangle$, then $\langle F\rangle^h = \langle \tilde{F}\rangle$.*

Proof. Let $\tilde{I} = \langle \tilde{F}\rangle$ and $I^h = \langle F\rangle^h$. Consider the saturation of $\tilde{I}$ w.r.t. t, that is

$$(\tilde{I} : t^\infty) = \{f \in S : \ \exists d \geq 0 \text{ s.t. } ft^d \in \tilde{I}\}.$$

($\subseteq$) We have $\tilde{I} \subseteq (\tilde{I} : t^\infty) = I^h$ by Proposition 4.3.5.

($\supseteq$) We have to show that $(\tilde{I} : t^\infty) \subseteq \tilde{I}$. Let $f \in (\tilde{I} : t^\infty)$. Suppose d is the least nonnegative integer s.t. $ft^d \in \tilde{I}$. Then since t is a nonzerodivisor on $S/\tilde{I}$ we see that $ft^{d-1} \in \tilde{I}$, which contradicts the minimality of d. Therefore, d must be zero, i.e $f \in \tilde{I}$. □

8.4 First Fall Degree

The notion of first fall degree was introduced by V. Dubois and N. Gama in [20] to study the complexity of HFE-systems and further studied in [18]. Our description is based on the latter and [11].

Let $\mathbb{F}_q$ be a finite field, where $q = p^l$ for p prime, $l \in \mathbb{N}$. Let $R = \mathbb{F}_q[x_1, \dots, x_n]/\langle x_1^q, \dots, x_n^q\rangle$ be the graded quotient ring and let $F = \{f_1, \dots, f_r\} \subseteq R$ be a set of homogeneous quadratic polynomials. Let $\varphi : R^r \to R$, $e_i \mapsto f_i$ be the usual epimorphism.

Definition 8.4.1. The module of *trivial syzygies* denoted $\mathrm{Triv}(f_1, \dots, f_r)$ is the submodule of $\mathrm{Syz}(f_1, \dots, f_r) = \ker(\varphi)$ generated by the *Koszul syzygies* $\{f_i e_j - f_j e_i : 1 \leq i < j \leq n\}$ and the syzygies $\{f_i^{q-1} e_i : i = 1, \dots, r\}$ coming from the structure of R.
For $d \in \mathbb{N}$, let $\mathrm{Syz}(F)_d = \mathrm{Syz}(F) \cap R_d^r$ denote the syzygies of degree d. Analogously, define $\mathrm{Triv}(F)_d = \mathrm{Triv}(F) \cap R_d^r$ to be the trivial syzygies of degree d.

Clearly, $\mathrm{Triv}(F)_d \subseteq \mathrm{Syz}(F)_d$ is always true. The first fall degree is intuitively similar to the degree of regularity as it measures, at which degree the system starts to behave differently when solving it.

Definition 8.4.2. The *first fall degree* of an ideal I generated by homogeneous quadratic polynomials is

$$d_{fall}(F) = \min\{d \in \mathbb{N} : \mathrm{Syz}(F)_{d-2} / \mathrm{Triv}(F)_{d-2} \neq 0\}.$$

If F contains nonhomogeneous quadratic polynomials, then

$$d_{fall}(F) = d_{fall}(F^{top}).$$

The first fall degree is the first degree, where linear combinations of multiples of $f_1, \ldots, f_r$ produce a nontrivial cancellation of all highest degree components. It is sometimes also called *degree of regularity*. However, while it is largely accepted that the first fall degree can be used to estimate the complexity of Gröbner basis algorithms, there is no obvious connection with the degree of regularity defined in Definition 8.3.6 apart from the name. Also, the first fall degree does not have to be close to the solving degree either. While experimental results in [18] suggest that the first fall degree is usually close to the solving degree, when working with a small number of variables, there exist systems where these two degrees are far apart.

Bibliography

[1] Allen Altman and Steven Kleiman. *A term of Commutative Algebra*. Worldwide Center of Mathematics, May 2013. ISBN: 978-0-9885572-1-5.

[2] Michael Atiyah and Ian G. Macdonald. *Introduction to Commutative Algebra*. Londond Mathematical Society Student Texts. Addison Wesley Publishing Company, 1969.

[3] Magali Bardet. "Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie". PhD thesis. University of Paris 6, Dec. 2004.

[4] David Bayer and Michael Stillman. "A criterion for detecting m-regularity." In: *Inventiones mathematicae* 87 (1987), pp. 1–12.

[5] Mina Bigdeli, Emanuela De Negri, Manuela M. Dizdarevic, Elisa Gorla, Sulamithe Tsakou, and Romy Minko. *Semi-regular sequences and other random systems of equations*. preprint (2020) available at https://arxiv.org/abs/2011.01032.

[6] Mark Blumstein. "Dimension and Multiplicity of Graded Rings and Modules". MA thesis. Colorado State University, Sept. 2017.

[7] Markus Brodmann and Rodney Y. Sharp. *Local cohomology: an algebraic introduction with geometric applications*. Vol. 60. Cambridge Studies in Advanced Mathematics. Cambridge: Cambridge University Press, 1998. ISBN: 0-521-37286-0. DOI: 10.2277/0521372860.

[8] Winfried Bruns and H. Jürgen Herzog. *Cohen-Macaulay Rings*. 2nd ed. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1998. DOI: 10.1017/CBO9780511608681.

[9] Bruno Buchberger. "Bruno Buchberger's PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal". In: *Journal of Symbolic Computation* 41.3 (2006), pp. 475 –511. DOI: 10.1016/j.jsc.2005.09.007.

[10] Johannes Buchmann, Jintai Ding, Mohamed Mohamed, and Wael Mohamed. "MutantXL: Solving Multivariate Polynomial Equations for Cryptanalysis". In: *Symmetric Cryptography*. Jan. 2009.

[11] Alessio Caminata and Elisa Gorla. *Solving Multivariate Polynomial Systems and an Invariant from Commutative Algebra*. preprint (2017) available at http://arxiv.org/abs/1706.06319.

[12] Guido Castelnuovo. *Sui multipli di una serie lineare di gruppi di punti appartenente ad una curva algebrica*. Dec. 1893. DOI: 10.1007/bf03012436.

[13] Marc Chardin. "Some results an questions on Castelnuovo-Mumford regularity". In: *Lecture Notes in Pure and Applied Mathematics* 254 (2007), pp. 1–40.

[14] Nicolas Courtois, Alexander Klimov, Jacques Patarin, and Adi Shamir. "Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations". In: *Advances in Cryptology — EUROCRYPT 2000*. Ed. by Bart Preneel. Springer Berlin Heidelberg, 2000, pp. 392–407.

[15] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms*. Undergraduate Texts in Mathematics. Springer, Jan. 2015. ISBN: 978-3-319-16720-6. DOI: 10.1007/978-3-319-16721-3.

[16] David Cox, John Little, and Donal O'Shea. *Using Algebraic Geometry*. Graduate Texts in Mathematics. Springer, Jan. 2005. ISBN: 978-0-387-98492-6. DOI: 10.1007/978-1-4757-6911-1.

[17] Jintai Ding and Dieter Schmidt. "Rainbow, a New Multivariable Polynomial Signature Scheme". In: *Applied Cryptography and Network Security*. Ed. by John Ioannidis, Angelos Keromytis, and Moti Yung. Springer Berlin Heidelberg, 2005, pp. 164–175. ISBN: 978-3-540-31542-1.

[18] Jintai Ding and Dieter Schmidt. "Solving Degree and Degree of Regularity for Polynomial Systems over a Finite Fields". In: (Jan. 2013), pp. 34–49. DOI: 10.1007/978-3-642-42001-6_4.

[19] Jintai Ding and Bo-Yin Yang. "Multivariate Public Key Cryptography". In: *Post-Quantum Cryptography*. Ed. by Daniel J. Bernsein, Johannes Buchmann, and Erik Dahmen. Springer Berlin Heidelberg, Jan. 2009, pp. 193–241. ISBN: 978-3-540-88701-0. DOI: 10.1007/978-3-540-88702-7_6.

[20] Vivien Dubois and Nicolas Gama. "The Degree of Regularity of HFE Systems". In: *Advances in Cryptology - ASIACRYPT 2010*. Ed. by Masayuki Abe. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 557–576. ISBN: 978-3-642-17373-8.

[21] Christian Eder and Jean-Charles Faugère. "A survey on signature-based algorithms for computing Gröbner bases". In: *Journal of Symbolic Computation* 80 (2017), pp. 719 –784. ISSN: 0747-7171. DOI: 10.1016/j.jsc.2016.07.031.

[22] David Eisenbud. *Commutative Algebra: With a View Toward Algebraic Geometry*. Graduate Texts in Mathematics. Springer, 1995. ISBN: 978-0-387-94269-8. DOI: 10.1007/978-1-4612-5350-1.

[23] David Eisenbud. *The Geometry of Syzygies: A Second Course in Algebraic Geometry and Commutative Algebra*. Graduate Texts in Mathematics. Springer, 2005. ISBN: 978-0-387-22215-8. DOI: 10.1007/b137572.

[24] Jean Charles Faugère, Patrizia Gianni, Daniel Lazard, and Teo Mora. "Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering". In: *Journal of Symbolic Computation* 16.4 (1993), pp. 329 –344. ISSN: 0747-7171. DOI: 10.1006/jsco.1993.1051.

[25] Jean-Charles Faugére. "A new efficient algorithm for computing Gröbner bases (F4)". In: *Journal of Pure and Applied Algebra* 139.1 (1999), pp. 61 –88. ISSN: 0022-4049. DOI: 10.1016/S0022-4049(99)00005-5.

[26] Gerd Fischer. *Lehrbuch der Algebra*. 3rd ed. Springer Spektrum, 2013. ISBN: 978-3-658-02221-1.

[27] Ralf Fröberg. "An introduction to Gröbner bases". In: *Pure and applied mathematics*. 1998.

[28] Michael R. Garey and David S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness*. 1st ed. Series of Books in the Mathematical Sciences. W. H. Freeman, 1979. ISBN: 978-0-716-71045-5.

[29] Robin Hartshorne. *Algebraic Geometry*. Graduate Texts in Mathematics. Springer, Jan. 1977. ISBN: 978-1-4419-2807-8. DOI: 10.1007/978-1-4757-3849-0.

[30] Jürgen Herzog and Takayuki Hibi. *Monomial Ideals*. Graduate Texts in Mathematics. Springer, Jan. 2011. ISBN: 978-0-85729-105-9. DOI: 10.1007/978-0-85729-106-6.

[31] Rotman Joseph. *An Introduction to Homological Algebra*. 1st ed. Universitext. Springer, 2009. ISBN: 978-0-387-24527-0. DOI: 10.1007/b98977.

[32] Mitchel T. Keller and William T. Trotter. *Applied Combinatorics*. CreateSpace, 2017. ISBN: 978-1-973-70271-9.

[33] Martin Kreuzer and Lorenzo Robbiano. *Computational Commutative Algebra 1*. Springer, Jan. 2000. ISBN: 978-3-540-67733-8. DOI: 10.1007/978-3-540-70628-1.

[34] Martin Kreuzer and Lorenzo Robbiano. *Computational Commutative Algebra 2*. Springer, Jan. 2005. ISBN: 978-3-540-25527-7. DOI: 10.1007/3-540-28296-3.

[35] Daniel Lazard. "Gröbner-Bases, Gaussian elimination and resolution of systems of algebraic equations". In: *Computer Algebra, EUROCAL '83, European Computer Algebra Conference, London, England, March 28-30, 1983, Proceedings*. Ed. by J. A. van Hulzen. Vol. 162. Lecture Notes in Computer Science. Springer, 1983, pp. 146–156. DOI: 10.1007/3-540-12868-9_99. URL: https://doi.org/10.1007/3-540-12868-9_99.

[36] Alexander Maletzky. *Gröbner bases and Macaulay matrices in Isabelle/HOL*. Tech. rep. Research Institute for Symbolic Computation, Johannes Kepler University Linz, Austria, 2018.

[37] Hideyuki Matsumura. *Commutative Ring Theory*. Ed. by Miles Reid. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1987. DOI: 10.1017/CBO9781139171762.

[38] Ezra Miller and Bernd Sturmfels. *Combinatorial Commutative Algebra*. 1st ed. Vol. 227. Graduate Texts in Mathematics. Springer, 2005. DOI: 10.1007/b138602.

[39] Victor S. Miller. "Use of Elliptic Curves in Cryptography". In: *Advances in Cryptology — CRYPTO '85 Proceedings*. Ed. by Hugh C. Williams. Berlin, Heidelberg: Springer Berlin Heidelberg, 1986, pp. 417–426. ISBN: 978-3-540-39799-1.

[40] David Mumford. *Lectures on Curves on an Algebraic Surface. (AM-59)*. Princeton University Press, 1966. ISBN: 9780691079936.

[41] Daniel Murfet. *Derived Functors*. University of Melbourne. Oct. 2006.

[42] Irena Peeva. *Graded Syzygies*. Springer, London, Jan. 2011. DOI: 10.1007/978-0-85729-177-6.

[43] Miles Reid. *Undergraduate Algebraic Geometry*. London Mathematical Society Student Texts. Cambridge University Press, 1988. DOI: 10.1017/CBO9781139163699.

[44] Ronald L. Rivest, Adi Shamir, and Loenard M. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". In: *Commun. ACM* 21.2 (Feb. 1978), 120–126. ISSN: 0001-0782. DOI: 10.1145/359340.359342.

[45] Aritra Sen and Ambedkar Dukkipati. *Gröbner Basis Theory for Modules over Polynomial Rings over Fields with Valuation*. Apr. 2014.

[46] Rodney Y. Sharp. *Cohen-Macaulay Rings*. 2nd ed. Vol. 51. London Mathematical Society Student Texts. Cambridge University Press, 2000.

[47] Alexei Skorobogatov. *Algebra IV*. Imperial College London. Apr. 2020.

[48] Charles A. Weibel. *An introduction to homological algebra*. 1st ed. Cambridge studies in advanced mathematics 38. Cambridge University Press, 1994. ISBN: 9780521435000.

[49] Manuela Wiesinger-Widi. "Gröbner Bases and Generalized Sylvester Matrices". PhD thesis. Research Institute for Symbolic Computation, Johannes Kepler University Linz, Austria, July 2015.

[50] Ali Akbar Yazdan Pour. "Resolutions and Castelnuovo-Mumford Regularity". PhD thesis. University of Grenoble, Oct. 2012.

Appendix A

Appendix

A.1 Zorn's Lemma

Theorem A.1.1 (Zorn's Lemma, [46], Theorem 3.8)**.** *Let $(V, \geq)$ be a nonempty partially ordered set which has the property that every nonempty totally ordered subset of V has an upper bound in V. Then V has at least one maximal element.*

A.2 Inclusion-Exclusion Principle

The inclusion-exclusion principle is a standard result from combinatorics and can be applied in many areas.

Theorem A.2.1 (Inclusion - Exclusion Principle, [32], Theorem 7.6)**.** *For finite sets $A_1, \ldots, A_n$ on has*

$$|\bigcup_{i=1}^{n} A_i| = \sum_{i=1}^{n} |A_i| - \sum_{1\leq i<j\leq n} |A_i \cap A_j| + \sum_{1\leq i<j<k\leq n} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n-1}|A_1 \cap \cdots \cap A_n|.$$

A.3 Proof of Generic Initial Ideals

To prove Theorem 8.1.8, we have to introduce some notations and notions. We closely follow [30, Chapter 4.1]

Definition A.3.1. Fix $d, t \in \mathbb{N}$ with $t \leq \dim_k(R_d)$ and consider the t-th exterior power $\bigwedge^t R_d$ of the k-space R_d. Fix a monomial order on R. An element $u_1 \wedge u_2 \wedge \cdots \wedge u_t \in \bigwedge^t R_d$, where $u_i \in \mathrm{Mon}_d(R)$ for all i and $u_1 > \cdots > u_t$, is said to be a *standard exterior monomial* of $\bigwedge^t R_d$.

Clearly, standard exterior monomials form a k-basis of the k-space $\bigwedge^t R_d$. Thus, any element $f \in \bigwedge^t R_d$ is a unique linear combination of standard exterior monomials.

Definition A.3.2. Let $f \in \bigwedge^t R_d$. The set of all standard exterior monomials appearing in f with a nonzero coefficient is called the *support* of f, denoted $\mathrm{Supp}(f)$.

The standard exterior monomials can be ordered similar to the lexicographic monomial order by setting

$$u_1 \wedge u_2 \wedge \cdots \wedge u_t > v_1 \wedge v_2 \wedge \cdots \wedge v_t,$$

if $u_i > v_i$ for the smallest index i with $u_i \neq v_i$.

Definition A.3.3. The *initial monomial* $\mathrm{in}(f)$ of a nonzero element $f \in \bigwedge^t R_d$ is defined to be the largest standard exterior monomial in $\mathrm{Supp}(f)$.

Let $V \subseteq R_d$ be a t-dimensional subspace and let $f_1, \ldots, f_t$ be a k-basis of V. Then $\bigwedge^t V$ is a one-dimensional k-space that is generated by the element $f_1 \wedge f_2 \wedge \cdots \wedge f_t$. $\mathrm{in}(V)$ denotes the k-space generated by all initial monomial $\mathrm{in}(f)$ with $0 \neq f \in V$.

Lemma A.3.4 ([30], Lemma 4.1.4)**.** *Let $w_1, \dots, w_t \in \mathrm{Mon}_d(R)$ with $w_1 > w_2 > \cdots > w_t$. Then the following are equivalent:*

(a) *$w_1, \dots, w_t$ form a k-basis of $\mathrm{in}(V)$.*

(b) *If $w_i = \mathrm{in}(g_i)$ with $g_i \in V$, then $g_1, \dots, g_t$ is a k-basis of V and*

$$\mathrm{in}(g_1 \wedge \cdots \wedge g_t) = \mathrm{in}(g_1) \wedge \cdots \wedge \mathrm{in}(g_t).$$

(c) *If $f_1, \dots, f_t$ forms a k-basis of V, then $\mathrm{in}(f_1 \wedge \cdots \wedge f_t) = w_1 \wedge \cdots \wedge w_t$.*

Proof. $(a \Rightarrow b)$ Suppose $0 \neq f \in V$. Then $\mathrm{in}(f) = w_i$ for some i. Now, there exists $a \in k$ s.t. $f - ag_i = 0$ or $\mathrm{in}(f - ag_i) < w_i$. By an inductive argument we see that $f - ag_i$ can be expressed as a k-linear combination of $g_{i+1}, \dots, g_t$, i.e. $g_1, \dots, g_t$ are a system of generators.

Suppose the g_i are not linearly independent, i.e. there are some $a_i \in k$ not all being zero s.t. $\sum_{i=1}^t a_i g_i = 0$. Let j be the smallest index s.t. $a_j \neq 0$. Then, by the way we ordered the w_i, we get $\mathrm{in}(\sum_{i=1}^t a_i g_i) = w_j \neq 0$, a contradiction.

As $w_1 > \cdots > w_t$, we see that $\mathrm{in}(g_1) \wedge \cdots \wedge \mathrm{in}(g_t)$ is a standard exterior monomial. Now let $g = g_1 \wedge \cdots \wedge g_t$. Then every standard exterior monomial $u \in \mathrm{Supp}(g)$ is, up to sign, equal to $u_1 \wedge \cdots \wedge u_t$ for some $u_i \in \mathrm{Supp}(g_i)$. Since $w_i \geq u_i$ for all i, the biggest standard exterior monomial in $\mathrm{Supp}(g)$ is $w_1 \wedge \cdots \wedge w_t$.

$(b \Rightarrow c)$ When $f_1, \dots, f_t$ is a basis of V, then $f_1 \wedge \cdots \wedge f_t$ is, up multiplication by a scalar, equal to $g_1 \wedge \cdots \wedge g_t$.

$(c \Rightarrow a)$ Every basis $f_1, \dots, f_t$ of V satisfies $\mathrm{in}(f_1 \wedge \cdots \wedge f_t) = w_1 \wedge \cdots \wedge w_t$. Thus, we may assume that $\mathrm{in}(f_1) > \cdots > \mathrm{in}(f_t)$. Then $\mathrm{in}(f_i) = w_i$, which implies that $w_i \in \mathrm{in}(V)$. Since $\dim_k(V) = \dim_k(\mathrm{in}(V))$, it follows that $w_1, \dots, w_t$ is a k-basis. □

Let $\boldsymbol{g} \in GL_n(k)$ be a linear change of coordinates on R. If $f_1, \dots, f_t$ is a k-basis of $V \subseteq R_d$, then $\boldsymbol{g}(f_1), \dots, \boldsymbol{g}(f_t)$ is k-basis of $\boldsymbol{g}V \subseteq R_d$. If $\mathrm{in}(\boldsymbol{g}(f_1) \wedge \cdots \wedge \boldsymbol{g}(f_t)) = w_1 \wedge \cdots \wedge w_t$, then by Lemma A.3.4, $w_1, \dots, w_t$ form a k-basis of $\mathrm{in}(\boldsymbol{g}V)$.

Lemma A.3.5 ([30], Lemma 4.1.5)**.** *Let $w_1 \wedge \cdots \wedge w_t$ be the largest exterior monomial of $\bigwedge^t R_d$ s.t. there is $\boldsymbol{g} \in GL_n(k)$ s.t.*

$$\mathrm{in}(\boldsymbol{g}(f_1) \wedge \cdots \wedge \boldsymbol{g}(f_t)) = w_1 \wedge \cdots \wedge w_t.$$

Then $U = \{\boldsymbol{g} \in GL_n(k) : \mathrm{in}(\boldsymbol{g}(f_1) \wedge \cdots \wedge \boldsymbol{g}(f_t)) = w_1 \wedge \cdots \wedge w_t\} \subseteq GL_n(k)$ is a nonemtpy Zariski open set.

Proof. Clearly, $U \neq 0$. Now express $\boldsymbol{g}(f_1) \wedge \cdots \wedge \boldsymbol{g}(f_t)$ as a linear combination of standard exterior monomials and let $p(\boldsymbol{g})$ be the coefficient of $w_1 \wedge \cdots \wedge w_t$. Then $p(\boldsymbol{g}) \neq 0$ if and only if $\boldsymbol{g} \in U$. But $p(\boldsymbol{g})$ is a polynomial in the entries of $\boldsymbol{g}$, which depend on $f_1, \dots, f_t$. Thus U is a Zariski open set. □

With these preliminary results, it is now possible to show the existence of the generic initial ideal.

proof of Theorem 8.1.8. Fix an integer $d \in \mathbb{Z}_{\geq 0}$ with $I_d \neq 0$. Let $f_1, \dots, f_t$ be a k-basis of I_d s.t. $\boldsymbol{g}(f_1), \dots, \boldsymbol{g}(f_t)$ is a k-basis of $\boldsymbol{g}I_d \subseteq R_d$. Then, define the standard exterior monomial $w_1 \wedge \cdots \wedge w_t$ as in Lemma A.3.5 and let

$$U_d = \{\boldsymbol{g} \in GL_n(k) : \mathrm{in}(\boldsymbol{g}(f_1) \wedge \cdots \wedge \boldsymbol{g}(f_t)) = w_1 \wedge \cdots \wedge w_t\} \subseteq GL_n(k).$$

We know by Lemma A.3.5 that U_d is Zariski open. For $d \in \mathbb{Z}_{\geq 0}$ s.t. $I_d = 0$, let $U_d = GL_n(k)$.

Let $\boldsymbol{g} \in U_d$ and $J_d = \operatorname{in}(\boldsymbol{g}I_d)$. Then by construction of U_d, J_d is independent of the choice of $\boldsymbol{g} \in U_d$.

Next, we claim that $J = \bigoplus_d J_d$ is an ideal of R. Since the sets U_d are Zariski open, by Proposition 4.4.3, we have $U_d \cap U_{d+1} \neq 0$. Let $\boldsymbol{g} \in U_d \cap U_{d+1}$. Then it follows that

$$R_1 J_d = R_1 \operatorname{in}(\boldsymbol{g}I_d) \subseteq \operatorname{in}(\boldsymbol{g}I_{d+1}) = J_{d+1}.$$

Thus, J is an ideal.

Let c be the maximal degree of a generator of J. We show that $U = U_1 \cap \cdots \cap U_c$ is the Zariski open set we look for. For this, we prove that $J_d = \operatorname{in}(\boldsymbol{g}I_d)$ for all d and for any $\boldsymbol{g} \in U$. We have $\boldsymbol{g} \in U_d$ for all $d \leq c$, so the claim is clearly true in this case. Thus, assume that $d \geq c$. We do induction on d, where the case $d = c$ is immediate. So, let $d > c$ and assume it is true for $d-1$. By the inductive hypothesis, we get

$$J_d = R_1 J_{d-1} = R_1 \operatorname{in}(\boldsymbol{g}I_{d-1}) \subseteq \operatorname{in}(\boldsymbol{g}I_d).$$

Since additionally we have $\dim_k(J_d) = \dim_k(\operatorname{in}(\boldsymbol{g}I_d))$ we can conclude that $J_d = \operatorname{in}(\boldsymbol{g}I_d)$. Thus, $J = \operatorname{in}(\boldsymbol{g}I)$ for all $\boldsymbol{g} \in U$, i.e. $J = \operatorname{Gin}(I)$ exists. □

Fix $d \in \mathbb{Z}_{\geq 0}$ and let $t = \dim_k(I_d)$. By the choice of $w_1 \wedge \cdots \wedge w_t$ in Lemma A.3.5 for the construction of U_d in the proof of Theorem 8.1.8, it follows that $w_1 \wedge \cdots \wedge w_t$ generates $\bigwedge^t \operatorname{in}(\boldsymbol{g}I)_d$ for all $\boldsymbol{g} \in U_d$. Thus, we get the following result.

Corollary A.3.6 ([30], Proposition 4.1.7)**.** *Let $t = \dim_k(I_d)$ and let $w_1 \wedge \cdots \wedge w_t$ be the standard exterior monomial generating $\bigwedge^t \operatorname{Gin}(I)_d$. Then*

$$w_1 \wedge \cdots \wedge w_t = \max\{\operatorname{in}(f) : 0 \neq f \in \bigwedge^t (\boldsymbol{g}I)_d,\ \boldsymbol{g} \in GL_n(k)\}.$$

Next, we give the proof of Theorem 8.1.10, i.e. we show that the generic initial ideal is indeed Borel-fixed.

proof of Theorem 8.1.10. Suppose by contradiction that $\operatorname{Gin}(I)$ is not Borel-fixed, i.e. there exists $\boldsymbol{g} \in B_n(k)$ s.t. $\boldsymbol{g}(\operatorname{Gin}(I)) \neq \operatorname{Gin}(I)$. Since $B_n(k)$ is generated by invertible diagonal matrices, which fix $\operatorname{Gin}(I)$ and elementary upper triangular matrices, we may assume that $\boldsymbol{g}$ is such an elementary upper triangular matrix.

Since $\boldsymbol{g}(\operatorname{Gin}(I)) \neq \operatorname{Gin}(I)$, there exists an integer $d \in \mathbb{Z}_{\geq 0}$ with $\boldsymbol{g}(\operatorname{Gin}(I))_d \neq \operatorname{Gin}(I)_d$. Let $t = \dim_k(I_d) = \dim_k(\operatorname{Gin}(I)_d)$ and set

$$\boldsymbol{g}(w_1 \wedge \cdots \wedge w_t) = \boldsymbol{g}(w_1) \wedge \cdots \wedge \boldsymbol{g}(w_t)$$

for all standard exterior monomials $w_1 \wedge \cdots \wedge w_t \in \bigwedge^t R_d$ s.t. $\boldsymbol{g}$ acts as a k-linear map on $\bigwedge^t R_d$. Let $w = w_1 \wedge \cdots \wedge w_t$ be a standard exterior monomial that generates $\bigwedge^t \operatorname{Gin}(I)_d$. Because $\boldsymbol{g}$ is an upper triangular matrix, and $\boldsymbol{g}(\operatorname{Gin}(I)) \neq \operatorname{Gin}(I)$, there must be a standard exterior monomial $u \in \operatorname{Supp}(\boldsymbol{g}w)$ s.t. $u > w$.

Now, let $\boldsymbol{h} \in GL_n(k)$ with $\operatorname{Gin}(I) = \operatorname{in}(\boldsymbol{h}I)$ and let $f_1, \ldots, f_t$ be a k-basis of $\boldsymbol{h}I_d$ s.t. $\operatorname{in}(f_i) = w_i$. Let $f = f_1 \wedge \cdots \wedge f_t$. Let $\boldsymbol{d} = \operatorname{diag}(d_1, \ldots, d_n) \in D_n(k)$ be a diagonal matrix. Consider all standard exterior monomials $v = v_1 \wedge \cdots \wedge v_t \in \operatorname{Supp}(f)$ s.t. $v_1 \cdots v_t$ is the same monomial $x^\alpha \in R_{td}$. Applying $\boldsymbol{d}$ to those v yields each time the same scalar multiple $\boldsymbol{d}^\alpha v$ of themselves. By defining f_α as the sum of all terms $a_v v_1 \wedge \cdots \wedge v_t \in \operatorname{Supp}(f)$ s.t. $v_1 \cdots v_t = x^\alpha$ we can write

$$f = f_{\alpha_0} + \sum_{\alpha \neq \alpha_0} f_\alpha,$$

where $f_{\alpha_0} = aw_1 \wedge w_2 \wedge \cdots \wedge w_t = a\,\mathrm{in}(f)$ and $a \in k \setminus \{0\}$.
Applying $\boldsymbol{d}$ to f then yields

$$\boldsymbol{d}(f) = a\boldsymbol{d}^{\alpha_0}\,\mathrm{in}(f) + \sum_{\alpha \neq \alpha_0} \boldsymbol{d}^{\alpha} f_{\alpha}.$$

Applying $\boldsymbol{g}$ then yields

$$(\boldsymbol{gd})(f) = a\boldsymbol{d}^{\alpha_0}\boldsymbol{g}(\mathrm{in}(f)) + \sum_{\alpha \neq \alpha_0} \boldsymbol{d}^{\alpha}\boldsymbol{g}(f_{\alpha}).$$

Since $u \in \mathrm{Supp}(\boldsymbol{g}(\mathrm{in}(f))$, i.e. u appears in $\boldsymbol{g}\,\mathrm{in}(f))$ with a nonzero coefficient $c \in k$, one can see that the coefficient of u in $(\boldsymbol{gd})(f)$ equals $ac\boldsymbol{d}^{\alpha_0} + \sum_{x^{\alpha} \in W} c_{\alpha}\boldsymbol{d}^{\alpha}$, with $c_{\alpha} \in k$ and where W is the set of all monomials x^{α} s.t. $u \in \mathrm{Supp}(\boldsymbol{g}(f_{\alpha}))$.
Since $p = ac_{\alpha_0}x^{\alpha_0} + \sum_{x^{\alpha} \in W} c_{\alpha}x^{\alpha}$ is a polynomial in R, and k is infinite, there exists $d_1, \ldots, d_n$ s.t. $p(d_1, \ldots, d_n) \neq 0$.

By choosing $\boldsymbol{d} = \mathrm{diag}(d_1, \ldots, d_n)$ and letting $\boldsymbol{q} = \boldsymbol{gd}$, we see that $w < u \in \mathrm{Supp}(\boldsymbol{q}(f))$ for $\boldsymbol{q} \in B_n(k)$. But this is a contradiction to Corollary A.3.6, so $\mathrm{Gin}(I)$ must be Borel-fixed. □