COMPUTATION OF THE PRIMARY DECOMPOSITION OF POLYNOMIAL IDEALS USING GRÖBNER BASES

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

BETÜL TOLGAY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
MATHEMATICS

AUGUST 2021

Approval of the thesis:

COMPUTATION OF THE PRIMARY DECOMPOSITION OF POLYNOMIAL IDEALS USING GRÖBNER BASES

submitted by **BETÜL TOLGAY** in partial fulfillment of the requirements for the degree of **Master of Science in Mathematics Department, Middle East Technical University** by,

Prof. Dr. Halil Kalıpçılar
Dean, Graduate School of **Natural and Applied Sciences** _____

Prof. Dr. Yıldıray Ozan
Head of Department, **Mathematics** _____

Assoc. Prof. Dr. Tolga Karayayla
Supervisor, **Mathematics, METU** _____

Examining Committee Members:

Assoc. Prof. Dr. Ali Ulaş Özgür Kişisel
Mathematics, METU _____

Assoc. Prof. Dr. Tolga Karayayla
Mathematics, METU _____

Assoc. Prof. Dr. Mesut Şahin
Mathematics, Hacettepe University _____

Date:6.08.2021

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Surname: Betül Tolgay

Signature :

ABSTRACT

COMPUTATION OF THE PRIMARY DECOMPOSITION OF POLYNOMIAL IDEALS USING GRÖBNER BASES

Tolgay, Betül
M.S., Department of Mathematics
Supervisor: Assoc. Prof. Dr. Tolga Karayayla

August 2021, 88 pages

In this thesis, we investigate algorithms for computing primary decompositions of ideals in polynomial rings. Every ideal in a polynomial ring over a Noetherian commutative ring with identity has a primary decomposition, that is, it can be expressed as the intersection of primary ideals (in a unique way or not). The existence of primary decompositions in such polynomial rings is a result of the ascending chain condition and the existence proof does not suggest any construction method for the primary components of the ideal. In the first part of the thesis, we investigate the algorithms developed by Gianni et al. [13] for the computation of a primary decomposition of a given ideal in a polynomial ring. The main tool used in these algorithms is Gröbner basis techniques for the computation of certain operations on ideals. We give a complete discussion and analysis of the theorems and algorithms developed by Gianni et al. in [13] here. The second part of the thesis presents another approach to the problem of computation of primary decomposition developed by Eisenbud et al. in [4]. This method avoids the projection of an ideal to a polynomial subring with one less variable which was used for reduction in the algorithms developed by Gianni et al. [13]. We give an outline of the algorithms developed by Eisenbud et al. in [4] here.

The algorithms developed by both Gianni et al. [13] and Eisenbud et al. [4] make it possible to compute primary components and associated primes of a given ideal, hence also the radical of the ideal.

Keywords: Primary Decomposition, Polynomial Ideals, Gröbner Bases, Algorithms

ÖZ

POLİNOM İDEALLERİNİN GRÖBNER BAZLARI KULLANILARAK PRİMER BİLEŞENLERİNE AYRILMASI

Tolgay, Betül
Yüksek Lisans, Matematik Bölümü
Tez Yöneticisi: Doç. Dr. Tolga Karayayla

Ağustos 2021 , 88 sayfa

Bu tezde, polinom halkalarındaki idealleri primer bileşenlerine ayırma algoritmalarını inceliyoruz. Birim elemana sahip değişmeli Noteryen halka üzerinde tanımlı bir polinom halkasının her ideali, primer bileşenlerine ayrılabilir. Başka bir deyişle, bu tür idealler, primer ideallerin kesişimi olarak yazılabilir (bir veya birden fazla şekilde). Bu tür polinom halkalarında primer bileşenlerin varlığı, söz konusu halkadaki yükselen zincir şartının sağlanmasının bir sonucudur, ancak bu varlık ispatı, idealin primer çarpanlarının nasıl inşa edileceğine dair bir metot öne sürmez. Tezin ilk kısmında, bir polinom halkasında verilen bir idealin primer bileşenlerini bulmak için Gianni ve diğer yazarlar [13] tarafından geliştirilen algoritmaları inceliyoruz. Bu algoritmalarda kullanılan esas araç, idealler üzerinde tanımlı belirli işlemlerin hesaplanması için kullanılan Gröbner bazı teknikleridir. Bu bölümde, Gianni ve diğer yazarlar [13] tarafından geliştirilen teorem ve algoritmaların tam bir analizini ve mütalaasını yapıyoruz. Tezin ikinci kısmında ise primer bileşenlerin hesabı problemine Eisenbud ve diğer yazarlar [4] tarafından geliştirilen başka bir yaklaşım sunuyoruz. Ancak, bu metot Gianni ve diğer yazarlar [13] tarafından geliştirilen algoritmalarda, indirgeme

yapmak için kullanılan, polinom idealinin, değişkeni bir eksik olan polinom alt halkasına izdüşümünü alma işlemini kullanmamaktadır. Bu bölümde, Eisenbud ve diğer yazarlar [4] tarafından geliştirilen algoritmaların bir taslağını sunuyoruz. Hem Gianni ve diğer yazarlar [13] hem de Eisenbud ve diğer yazarlar [4] tarafından geliştirilen algoritmalar, verilen bir idealin primer ve ortak asal bileşenlerini, böylelikle kökünü de hesaplamayı mümkün kılmaktadır.

Anahtar Kelimeler: Primer Çarpanlar, Polinom İdealleri, Gröbner Bazları, Algoritmalar

To My Family

ACKNOWLEDGMENTS

First and foremost, I thank Allah for granting me the opportunity to write such a thesis in mathematics. Secondly, I thank all my family members and relatives for their mighty support. I would also like to give special thanks to my teachers since my childhood, mentioning first those who are no longer with us. Perihan Kuzlu, may she rest in peace, had taught me how to summarize, among several other skills; Cem Tezer, may he rest in heaven, had tremendous knowledge and an elegant way of teaching, and besides that, he provided invaluable support for me and my friends during our difficult times. As for the others, I am very grateful to my supervisor Tolga Karayayla for accepting me as a master's student. I thank him for his exceptional help in providing feedback, his great patience in tutoring, and his mathematical rigour. I should also thank all my dearest friends for their sincere sharing in my life and studies, especially my Palestinian friend Rana Assaf Öztürk from METU, who passed away years ago. Her education was interrupted because she was practicing her faith. After hearing that her friend's doctoral studies had finished, she once said "Something cracks inside". I hope she is in a place where there is no longing and no regret.

I apologize for those I failed to mention, and I am sorry for the trees whose lives ended to become the papers I use excessively (my sister's idea). My further thanks go to all the scientists and mathematicians for their tireless efforts to make a significant contribution. Lastly, I would like to thank all the internet communities like Stack Exchange, Matematik Kafası, Wolfram MathWorld, ResearchGate, Wikipedia, Overleaf, Grammarly, and Instatext. They helped me a lot in understanding mathematics, improving my grammar, and writing my thesis in LaTeX.

One day, I hope to see Mathematics Villages in Palestine and every corner of the world like the ones in Turkey.

TABLE OF CONTENTS

ABSTRACT v

ÖZ vii

ACKNOWLEDGMENTS x

TABLE OF CONTENTS xi

CHAPTERS

1 INTRODUCTION 1

1.1 Motivation and Problem Definition 1

1.2 Contributions and Novelties 2

1.3 The Outline of the Thesis 3

2 PRIMARY DECOMPOSITION OF IDEALS AND BASIC PROPERTIES . 5

2.1 Introduction 5

3 GRÖBNER BASES 15

3.1 Definitions 15

3.2 Operations on Ideals 20

4 ALGORITHMS FOR COMPUTING PRIMARY DECOMPOSITION USING GRÖBNER BASES 35

4.1 Primality Test 35

4.2 Zero-dimensional Ideals 38

4.3 Zero-dimensional Primary Decomposition 49

4.4 Primary Decomposition in Polynomial Rings over Principal Ideal Domains 55

4.5 Algorithm for Computing the Associated Primes and Radical of an Ideal 66

5 A SECOND APPROACH FOR COMPUTING PRIMARY DECOMPOSITION 69

5.1 Introduction 69

5.2 Finding the Equidimensional Hull of a Submodule 71

5.3 The Radical of an Ideal 74

5.4 Primary Decomposition 82

REFERENCES 87

CHAPTER 1

INTRODUCTION

1.1 Motivation and Problem Definition

In this thesis, we investigate computational methods for obtaining a primary decomposition of a given ideal in a polynomial ring. Primary ideals are in some sense generalizations of prime ideals. A primary ideal is defined by the condition that ab is an element of the ideal implies a is in the ideal or b is in the radical of the ideal. An ideal is said to have a primary decomposition if it can be expressed as the intersection of primary ideals. One of the important results about primary decomposition is that every ideal of a polynomial ring over a Noetherian domain has a primary decomposition. This fact relies on the ascending chain condition on Noetherian rings and its proof is a pure existence proof which does not indicate any method for constructing the primary components in the primary decomposition. Although the problem of computing a primary decomposition of an ideal in a polynomial ring is purely a problem in commutative algebra, it has strong connections with algebraic geometry. For an ideal $I \subset k[x_1, \ldots, x_n]$ where k is a field, if $I = \bigcap_i Q_i$ is a primary decomposition (Q_i are primary ideals), the variety $V(I)$ of the ideal is then equal to $\bigcup_i V(Q_i)$. Here the varieties $V(Q_i)$ are irreducible varieties since $V(Q_i) = V(\sqrt{Q_i})$ and $\sqrt{Q_i}$ is a prime ideal for each i (radicals of primary ideals are prime ideals). This way, $V(I)$ is expressed as a union of irreducible varieties. As a result, having a method for computing a primary decomposition of an ideal gives rise to a method of computing irreducible components of the variety corresponding to this ideal.

1.2 Contributions and Novelties

In this work, we examine two methods for computing a primary decomposition for an ideal I in a polynomial ring. The first method we analyze in depth consists of the algorithms developed by Gianni, Trager and Zacharias in the paper "Gröbner Bases and Primary Decomposition of Polynomial Ideals" [13]. These algorithms are based on Gröbner basis techniques for several operations on ideals. The algorithms are recursively iterated by using a reduction step to a case in a polynomial ring with one less variable. Obtaining the projection of an ideal to a polynomial subring with less number of variables can be easily performed by elimination theory if Gröbner bases with respect to a lexicographic order is used. These algorithms terminate when the problem is reduced to the one variable case. In the paper [13] by Gianni et al., the main result is an algorithm for computing a primary decomposition of a given ideal in a polynomial ring over a PID which uses Gröbner Basis techniques. The algorithm also computes the associated primes of the given ideal. This main algorithm is built by first developing an algorithm for computing a primary decomposition for zero-dimensional ideals and then reducing the general case to the zero-dimensional case within the algorithm. As a biproduct, Gianni et al. provide a test of primality for a given ideal and an algorithm for computing the radical of the given ideal (indeed, the radical is the intersection of the associated primes which are given by the main algorithm). In this thesis, we give a full explanation for the proofs of the theorems which give rise to the algorithms developed by Gianni et al., and we also analyze these algorithms step by step emphasizing their connections to the given theorems. The algorithms usually involve branches and recursive iterations, and in our analysis of these algorithms we clarify how the algorithm proceeds from one step to the other. The second method for computing primary decompositions which we explore in this thesis is developed by Eisenbud, Huneke and Vasconcelos in the paper "Direct Methods for Primary Decomposition" [4]. This method is different from the method developed by Gianni et al. in the sense that it avoids the projection operation used by Gianni et al. to reduce the number of variables. The algorithms developed by Eisenbud et al. use Ext groups and syzygy computations as tools to compute the equidimensional hull, the intersection of associated primes of a given dimension, the radical and a primary decomposition of a given ideal in a polynomial ring over a field. We focus on

explaining the implications of the theorems proved in [4] in the development of the given algorithms rather than the proofs of the theorems, and we examine the structure of the given algorithms and explain how they operate.
The algorithms developed by Gianni et al. in [13] are implemented as a package in REDUCE and AXIOM, and the algorithms developed by Eisenbud et al. in [4] are implemented as a package in Macaulay 2 programs for the computation of primary decomposition of an ideal. This thesis is an extensive examination of these main algorithms.

1.3 The Outline of the Thesis

We begin by reviewing the basic properties of primary decomposition in Chapter 2. We include the proofs of the well-known results about primary decomposition for completeness. In Chapter 3, we introduce Gröbner bases and develop Gröbner basis techniques for performing various operations on ideals. These techniques are the main computational tools in the algorithms we examine in this thesis. In Chapter 4, we discuss the theorems and algorithms by Gianni et al. in [13] in full detail. We begin with a test for checking whether a given ideal is prime or not using Gröbner basis techniques. In §4.2, we investigate properties of zero-dimensional ideals and the use of Gröbner basis in detecting whether a given ideal is zero-dimensional or not. In §4.3, we analyze the algorithm for computing a primary decomposition of a zero-dimensional ideal $I \subset R[x_1, \ldots, x_n]$ such that $I \cap R$ is zero-dimensional for the ring R. In §4.4, we analyze two generalizations of the algorithm in §4.3 to compute a primary decomposition of an ideal in a polynomial ring over a PID. The first of these is for zero-dimensional ideals, and the second one is the general case (for an arbitrary ideal in such a polynomial ring). Mainly, we present three algorithms for the computation of primary decomposition. The conditions on the input of these three algorithms start with the most restrictive ones (zero-dimensional ideal with zero-dimensional contraction to the coefficient ring) and reach the general case in the third algorithm (noting that the coefficient ring is a PID in the last two algorithms). And each of these algorithms uses the previous algorithms in it. Finally, in §4.5 of this chapter, we discuss how the given algorithms also compute the associated primes of

the given ideal besides the primary components. In Chapter 5, we give an outline of the algorithms developed by Eisenbud et al. in [4] together with the analysis of how these algorithms operate explaining the connections to the theorems proved in [4]. In §5.2, we present an algorithm for computing the equidimensional hull of a given ideal. In §5.3, we examine algorithms for computing the equidimensional radical, the intersection of the associated primes of a given dimension, intersection of minimal/embedded primes of a given dimension, and as a consequence an algorithm for computing the radical of an ideal. In §5.4, we explain the procedure for finding associated primes of a given ideal and once all associated primes are known, a primary decomposition of the ideal can be computed.

CHAPTER 2

PRIMARY DECOMPOSITION OF IDEALS AND BASIC PROPERTIES

2.1 Introduction

In this chapter, we will discuss the general properties of primary decomposition of ideals. Mostly, we will benefit from [10] and occasionally from [5] and [6]. For completeness, we include basic theorems related to the thesis. Throughout, R will be a commutative ring with identity.

Definition 2.1.1. *An ideal I in a ring R is called primary if $I \neq R$ and if $ab \in I$, then either $a \in I$ or $b^n \in I$ for some $n > 0$. Equivalently, I is primary if and only if $R/I \neq 0$ and every zero divisor in R/I is nilpotent.*

We can easily deduce that every prime ideal is primary. Moreover, the contraction of a primary ideal is primary, too.

Proposition 2.1.2. *Let I be a primary ideal in a ring R. Then $\sqrt{I}$ is the smallest prime ideal containing I.*

Proof. First, we show that $\sqrt{I}$ is prime whenever I is primary. Let $ab \in \sqrt{I}$. Thus, $(ab)^k \in I$ for some $k > 0$. Since I is primary, we have $a^k \in I$ or $(b^k)^n \in I$ for some $n > 0$. Therefore, $a \in \sqrt{I}$ or $b \in \sqrt{I}$. Secondly, $\sqrt{I} = \bigcap_{I \subset P,\ P\ prime} P$ and $\sqrt{I}$ is prime implies $\sqrt{I}$ is the smallest prime ideal containing I. ($I \subset P$ and P is prime implies $\sqrt{I} \subset P$, since $x^n \in I \subset P$ implies $x \in P$, where $n > 0$). □

Definition 2.1.3. *Let I be a primary ideal of the ring R. If $\sqrt{I} = Q$, then I is said to be a Q-primary ideal where Q is prime.*

Proposition 2.1.4. *If $\sqrt{I} \subset R$ is a maximal ideal, then I is primary. Moreover, the powers of a maximal ideal M are M-primary.*

Proof. Let $\sqrt{I}$ be a maximal ideal of R. Let $xy \in I$ and $x \notin \sqrt{I}$. Since $I \subset \sqrt{I}$, we have $xy \in \sqrt{I}$ and $x \notin \sqrt{I}$. Since $\sqrt{I}$ is maximal, $\sqrt{I}$ and x generate the ring R, i.e., $(\sqrt{I}, x) = (1)$. Therefore, $i + rx = 1$ for some $i \in \sqrt{I}$ and $r \in R$. If $i^k \in I$, then $(i+rx)^k = i^k + r'x = 1^k = 1$ for some $r' \in R$. Hence, $y(i^k + r'x) = yi^k + r'xy = y$, this implies $y \in I$. Therefore, I is primary. (We showed $xy \in I$ and $x \notin \sqrt{I}$ implies $y \in I$). For the second part, let $M \subset R$ be a maximal ideal. Let $M^s = Q$ for some $s > 0$. If $a \in M$, then $a^s \in M^s = Q$ which clearly implies $a \in \sqrt{Q}$, i.e., $M \subset \sqrt{Q}$. Since $Q = M^s \subset M$, we have $1 \notin Q$, hence $1 \notin \sqrt{Q}$ and $\sqrt{Q} \neq R$. $M \subset \sqrt{Q} \neq R$ and M is maximal implies $M = \sqrt{Q}$, hence Q is primary by the first part of the proposition. □

Lemma 2.1.5. *If the ideals $Q_i \subset R$ are P-primary for $1 \leq i \leq n$, then $Q = \bigcap_{i=1}^n Q_i$ is P-primary.*

Proof. Clearly, $\sqrt{Q} = \sqrt{\bigcap_{i=1}^n Q_i} = \bigcap_{i=1}^n \sqrt{Q_i} = P$. Let $ab \in Q$ and $a \notin Q$. Then $a \notin Q_i$ for some i. Since $ab \in Q_i$, and $a \notin Q_i$, and Q_i is primary, we get $b^n \in Q_i$. So, $b \in \sqrt{Q_i} = P = \sqrt{Q}$. Hence, Q is primary. □

Lemma 2.1.6. *Let Q be a P-primary ideal, $r \in R$. Then*

1. *if $r \in Q$, then $(Q : r) = (1)$,*
2. *if $r \notin Q$, then $(Q : r)$ is a P-primary ideal, hence $\sqrt{(Q : r)} = P$,*
3. *if $r \notin P$, then $(Q : r) = Q$.*

Proof. (i) and (iii) are straightforward from definitions. To prove (ii), let $a \in \sqrt{(Q : r)}$, hence $a^k \in (Q : r)$ for some $k > 0$. Thus, $a^k r \in Q$. By assumption, $r \notin Q$, hence $(a^k)^n \in Q$ for some $n > 0$ since Q is primary. Therefore, $a \in \sqrt{Q} = P$. Conversely, if $x \in \sqrt{Q} = P$, then $x^k \in Q$. Hence, for $r \notin Q$, we have $x^k r \in Q$ which implies $x^k \in (Q : r)$, hence $x \in \sqrt{(Q : r)}$. This shows $\sqrt{(Q : r)} = P$. To show that $(Q : r)$ is primary, let $ab \in (Q : r)$ and $a \notin \sqrt{(Q : r)} = P$. Thus, $abr \in Q$ and $a \notin \sqrt{Q}$ implies $a^k \notin Q$ for all $k > 0$.

Hence, $br \in Q$ (since Q is primary). Hence, $b \in (Q : r)$ proving $(Q : r)$ is primary. □

Definition 2.1.7. *Given an ideal $I \subset R$, if it is possible to express I as an intersection of primary ideals such that $I = \bigcap_{j=1}^{n} Q_j$ where Q_j are P_j-primary, then I is said to have a primary decomposition. If in addition, all P_j are distinct and $Q_j \not\supset \bigcap_{i \neq j} Q_i$ for $1 \leq i \leq n$, then this decomposition is called irredundant (or minimal).*

Note that, not every ideal has such a decomposition. If it does, then it is called a *decomposable* ideal. In this thesis, we consider ideals in Noetherian rings, thus they have a primary decomposition by Theorem 7.13 on pg. 83 of [10]. Furthermore, we can reduce any decomposition to an irredundant one by using Lemma 2.1.5 and by excluding Q_j from the decomposition if $Q_j \supset \bigcap_{i \neq j} Q_i$.

Theorem 2.1.8. *(First uniqueness theorem). Let I be a decomposable ideal, let $I = \bigcap_{i=1}^{n} I_i$ be an irredundant primary decomposition of I. Let $Q_i = \sqrt{I_i}$ for $1 \leq i \leq n$. Then Q_i are exactly the prime ideals which appear in the set of ideals $\sqrt{(I : r)}$ for some $r \in R$, hence are independent of the particular decomposition of I.*

Proof. Let $a \in R$, then $(I : a) = (\bigcap_{i=1}^{n} I_i : a) = \bigcap_{i=1}^{n} (I_i : a)$. This implies $\sqrt{(I : a)} = \bigcap_{i=1}^{n} \sqrt{(I_i : a)} = \bigcap_{a \notin I_i} \sqrt{I_i}$ by Lemma 2.1.6. We have $\sqrt{I_i}$ prime, however $\bigcap_{i=1}^{n} \sqrt{I_i}$ need not be prime. If it is prime, then by Proposition 1.11 on pg.8 of [10], we have $\sqrt{(I : a)} = \sqrt{I_t} = Q_t$ for some $1 \leq t \leq n$. On the other hand, since the decomposition is irredundant, for any i we have at least one element $q_i \notin I_i$ whereas $q_i \in \bigcap_{i \neq j} I_j$. Therefore, $\sqrt{(I : q_i)} = \bigcap_{j=1}^{n} \sqrt{(I_j : q_i)} = \sqrt{I_i}$ by Lemma 2.1.6. □

Together with Lemma 2.1.6, the proof of Theorem 2.1.8 indicates that for any i, there is an element $r_i \in R$ such that $(I : r_i)$ is Q_i-primary. Furthermore, if we regard R/I as an R-module, Theorem 2.1.8 amounts to stating that these Q_i are exactly the prime ideals which are the radicals of the annihilators of the elements of R/I.

Definition 2.1.9. *For a decomposable ideal $I \subset R$, if $I = \bigcap_{i=1}^{n} I_i$ is an irredundant primary decomposition and $\sqrt{I_i} = Q_i$, then Q_i are called associated primes of I (or belong to I). The minimal elements of the set $\{Q_1, \ldots, Q_k\}$ are called the minimal*

(or isolated) prime ideals that are associated with I, the other associated prime ideals are called the embedded prime ideals.

Remarks: The terms *isolated* and *embedded* have origins in geometry. If k is a field and $R = k[x_1, \ldots, x_n]$, then the ideal $I \subset R$ induces a variety $V(I) \subset k^n$. Moreover, there is a correspondence between the minimal primes Q_i of I and the irreducible components of $V(I)$. Also, the embedded primes of I correspond to some subvarieties of the irreducible components of $V(I)$.
For an irredundant primary decomposition of $I = \bigcap_{i=1}^{n} I_i$, we have

$$V(I) = V(\bigcap_{i=1}^{n} I_i) = \bigcup_{i=1}^{n} V(I_i) = \bigcup_{i=1}^{n} V(\sqrt{I_i}).$$

Here, $\sqrt{I_i}$ is prime for all i, hence $V(\sqrt{I_i})$ is an irreducible variety. Let $Q_1, \ldots, Q_t$, $(t \leq n)$ where $Q_i = \sqrt{I_i}$ be the minimal primes (isolated primes) of I. For $j > t$, we have $Q_j \supset Q_{i_j}$ for some $i_j \leq t$ by the minimality of $Q_1, \ldots, Q_t$, hence $V(Q_j) \subset V(Q_{i_j})$. Therefore, $V(I) = \bigcup_{i=1}^{n} V(Q_i) = \bigcup_{i=1}^{t} V(Q_i)$ where $V(Q_1), \ldots, V(Q_t)$ are the irreducible components of $V(I)$. In addition, the primary components I_i might not be independent of the decomposition. However, the primary components whose radicals are the minimal primes (isolated primes) of I are unique as we will state below.

Proposition 2.1.10. *The ideal I is primary if and only if it has only one associated prime ideal.*

Proof. Consider the primary decomposition $I = I$, and use the uniqueness of the list of associated primes. For the converse, if there is a single associated prime, then there is a primary decomposition with a single primary component, hence the ideal is primary. □

Proposition 2.1.11. *Let I be a decomposable ideal. Then any prime ideal $P \supset I$ contains a minimal prime ideal associated with I, thus the minimal prime ideals of I are exactly the minimal elements of the set of all prime ideals containing I.*

Proof. Let $I = \bigcap_{i=1}^{n} I_i$ be a primary decomposition of I. Hence, if P is a prime ideal such that $P \supset I = \bigcap_{i=1}^{n} I_i$, then $P = \sqrt{P} \supset \bigcap_{i=1}^{n} \sqrt{I_i} = \bigcap_{i=1}^{n} Q_i$. Thus, by

Proposition 1.11 in [10] on pg.8 (or *prime avoidance lemma*), we have $P \supset Q_j$ for some j. Therefore, P contains a minimal prime ideal associated with I. □

Proposition 2.1.12. *Let $I \subset R$ be a decomposable ideal such that $\bigcap_{i=1}^{n} Q_i$ is an irredundant primary decomposition of I, let $\sqrt{Q_i} = P_i$. Then*

$$\bigcup_{i=1}^{n} P_i = \{r \in R \mid (I : r) \neq I\}.$$

In particular, if the zero ideal is decomposable, the set D of zero divisors of R is the union of the prime ideals associated to (0).

Proof. We have $I \subset \bigcap_{i=1}^{n} Q_i \subset \bigcup_{i=1}^{n} P_i$, hence for $r \in I$, $(I : r) = R \neq I$. For the second part, since I is decomposable, $(\bar{0})$ is decomposable in R/I, i.e., $(\bar{0}) = \bigcap_{i=1}^{n} \bar{Q}_i$ where $\bar{Q}_i$ is the image of the ideal Q_i in R/I under projection. Thus, $\bar{Q}_i$ is primary, too. Hence, it suffices to prove the proposition for $I = (0)$. On the other hand, $D = \bigcup_{r \neq 0} \sqrt{(0 : r)}$ by Proposition 1.15 of [10], pg.9. Therefore, for $r \in R \setminus \{0\}$ we have $\sqrt{(0 : r)} = \bigcap_{i=1}^{n} \sqrt{(Q_i : r)} = \bigcap_{r \notin Q_j} P_j \subset P_j$ for some j, by Lemma 2.1.6. Hence, $D \subset \bigcup_{i=1}^{n} P_i$. Moreover, by Theorem 2.1.8, every P_i is of the form $\sqrt{(0 : r)}$ for some $r \in R$. Thus, $\bigcup_{i=1}^{n} P_i \subset D$. □

As a result, if (0) is decomposable, we have

$$D = \{\textit{zero divisors}\} = \bigcup_{i=1}^{n} P_i$$

where P_i are the prime ideals associated with (0).

$$\mathscr{N} = \{\textit{nilpotent elements}\} = \bigcap_{i=1}^{n} \tilde{P}_i$$

where $\tilde{P}_i$ are the minimal primes associated with (0).

We now present some properties of primary decomposition related to localization all of whose proofs can be found in [10], pp.53 - 54.

Proposition 2.1.13. *Let $S \subset R$ be a multiplicatively closed subset, let Q be a P-primary ideal.*

1. *If $S \cap P \neq \varnothing$, then $S^{-1}Q = S^{-1}R$.*

2. *If $S \cap P = \varnothing$, then $S^{-1}Q$ is $S^{-1}P$-primary and its contraction in R is Q.*

Therefore, the primary ideals correspond to primary ideals in the correspondence between ideals in $S^{-1}R$ and contracted ideals in R.

Notation: If $I \subset R$ is any ideal, and S is any multiplicatively closed subset of R, then the contraction of the ideal $S^{-1}I$ in R is represented as $S(I)$.

Proposition 2.1.14. *Let S be a multiplicatively closed subset of R, let I be a decomposable ideal. Let $I = \bigcap_{i=1}^{n} Q_i$ be an irredundant primary decomposition of I. Let $\sqrt{Q_i} = P_i$. Suppose the Q_i are numbered such that S has a nonempty intersection with $P_{m+1}, \ldots, P_n$ but not with $P_1, \ldots, P_m$. Then*

$$S^{-1}I = \bigcap_{i=1}^{m} S^{-1}Q_i \ \ and \ \ S(I) = \bigcap_{i=1}^{m} Q_i$$

where both are irredundant primary decompositions.

Definition 2.1.15. *Let Ω be a set of prime ideals associated with an ideal $I \subset R$. Ω is called isolated in case it satisfies the following. If $\tilde{P}$ is a prime ideal associated with I and $\tilde{P} \subset P$ for some $P \in \Omega$, then $\tilde{P} \in \Omega$.*

Lemma 2.1.16. *Let Ω be an isolated set of prime ideals associated with I, let $S = R - \bigcup_{P \in \Omega} P$. Then S is multiplicatively closed and for any prime ideal $\tilde{P}$ that is associated with I, we have*

$$\tilde{P} \in \Omega \, implies \, \tilde{P} \cap S = \varnothing.$$

Else if $\tilde{P} \notin \Omega$, then $\tilde{P} \not\subset \bigcup_{P \in \Omega} P$ by Proposition 1.11 (see [10], pg. 8), and thus $\tilde{P} \cap S \neq \varnothing$.

Together with this lemma and Proposition 2.1.14, we conclude the following theorem.

Theorem 2.1.17. *(Second uniqueness theorem). Let $I \subset R$ be a decomposable ideal, let $I = \bigcap_{i=1}^{n} Q_i$ be an irredundant primary decomposition of I, let $\{P_{i_1}, \ldots, P_{i_m}\}$ be an isolated set of prime ideals of I. Then, $Q_{i_1} \cap \cdots \cap Q_{i_m}$ is independent of this decomposition.*

Corollary 2.1.18. *The isolated primary components (the primary components Q_i corresponding to minimal prime ideals P_i) are uniquely determined by I.*

Note that in general the *embedded* primary components are not uniquely determined by I.

Next, we investigate the properties of the primary decomposition in Noetherian rings.

Definition 2.1.19. *An ideal $I \subset R$ is called irreducible if $I = J \cap K$ then either $I = J$ or $I = K$ where J, K are ideals of R.*

Lemma 2.1.20. *If R is a Noetherian ring, then every ideal of R is a finite intersection of irreducible ideals.*

Proof. Assume not. Let Σ be the set of ideals which are not finite intersection of irreducible ideals. Hence, Σ is nonempty. Since R is Noetherian, Σ has a maximal element, say Q. We complete the proof by obtaining a contradiction by showing $Q \notin \Sigma$. First, Q is not irreducible, otherwise Q is an intersection of one irreducible ideal $(Q = Q)$. Hence, $Q = J \cap K$ for ideals $Q \subsetneq J$, $Q \subsetneq K$. By maximality of Q, we get $J \notin \Sigma$, $K \notin \Sigma$. Then J and K are intersections of finitely many irreducible ideals, and hence so is $Q = J \cap K$ contradicting $Q \in \Sigma$. □

Lemma 2.1.21. *If R is a Noetherian ring, then every irreducible ideal is primary.*

Proof. Let I be an irreducible ideal in R. There is no difference between studying on the actual ring R or the quotient ring R/I. Hence, we can assume $I = (0)$. Let $ab \in (0)$. Thus, $ab = 0$. Suppose $b \neq 0$. To show $a^n = 0$ for some $n > 0$, let $(0 : a) = Ann(a) \subset Ann(a^2) \subset \cdots \subset Ann(a^k) \subset \cdots$ be a chain of ideals. Since R is Noetherian, this chain stabilizes after some $n > 0$. Hence, $Ann(a^n) = Ann(a^{n+1}) = \cdots$. Now, we need to show $(a^n) \cap (b) = (0)$. Let $xa^n = yb$, hence $xa^{n+1} = yab = 0$. Thus, $x \in Ann(a^{n+1}) = Ann(a^n)$. Therefore, $xa^n = 0$ which proves $(a^n) \cap (b) = (0)$. We assumed (0) was irreducible, thus either $(a^n) = (0)$ or $(b) = (0)$. Since $b \neq 0$, we get $(a^n) = (0)$, therefore $a^n = 0$ which implies (0) is primary. □

Last two lemmas imply the following result.

Theorem 2.1.22. *If R is a Noetherian ring, then every ideal has a primary decomposition.*

As a result, the properties we proved above about decomposable ideals are valid for all ideals in Noetherian rings.

Proposition 2.1.23. *Let R be a Noetherian ring. Then every ideal I contains a power of its radical.*

Proof. Let $\sqrt{I} = \langle a_1, \ldots, a_s \rangle$. Let $a_i^{k_i} \in I$ for $1 \leq i \leq s$. If we let $q = \Sigma_{i=1}^{s}(k_i - 1) + 1$, then $(\sqrt{I})^q$ is generated by monomials of the form $a_1^{m_1} \cdots a_s^{m_s}$ where $\Sigma_{i=1}^{s} m_i = q$. Therefore, $m_j \geq k_j$ for at least one j which implies that the above monomials are in I. Hence, $(\sqrt{I})^q \subset I$ for some $q > 1$. □

Corollary 2.1.24. *Let R be a Noetherian ring. Then the nilradical (the intersection of its prime ideals) is nilpotent.*

Proof. Let $I = (0)$ in Proposition 2.1.23. □

Corollary 2.1.25. *Let R be a Noetherian ring, M be a maximal ideal in R. Let Q be any ideal in R. Then the following are equivalent.*

1. *Q is M-primary.*
2. *$\sqrt{Q} = M$.*
3. *$M^k \subset Q \subset M$ for some $k > 0$.*

Proof. (i) implies (ii) by definition. (ii) implies (iii) by Proposition 2.1.23. (iii) implies (i) by taking the radicals of (ii) and having $\sqrt{M^k} = M = \sqrt{M}$. □

Proposition 2.1.26. *Let $I \neq (1)$ be an ideal in a Noetherian ring R. Then the prime ideals associated with I are exactly the prime ideals which appear in the set of ideals $(I : r)$ for some $r \in R$.*

Proof. If $(I : r)$ is prime, then it is radical, hence $(I : r) = \sqrt{(I : r)}$. Thus $(I : r)$ is an associated prime by Theorem 2.1.8. Conversely, assume that $I = \bigcap Q_i$ where

Q_i are P_i-primary (an irredundant primary decomposition). Let $I_i = \bigcap_{i \neq j} Q_j$. Let $a \in I_i$ and let $a \notin I$ (such an a exists by the irredundancy of the decomposition). Thus, $I \subset (I : a) = \bigcap (Q_j : a) \subset (Q_i : a) \subset P_i$ since $a \notin Q_i$ and Q_i is P_i-primary . Hence, $\sqrt{(I : a)} = P_i$. Therefore, $P_i^k \subset (I : a)$ for some $k \geq 1$. Let k be the minimal such number. Thus, $P_i^{k-1} \not\subset (I : a)$. Therefore, $aP_i^{k-1} \not\subset I$. Hence, there exists an element r such that $r \in aP_i^{k-1} \subset I_i$ and $r \notin I$. This implies $P_i \subset (I : r) = (Q_i : r) \subset P_i$ which yields $P_i = (I : r)$. $\square$

CHAPTER 3

GRÖBNER BASES

3.1 Definitions

We set our basic assumptions and notation as follows.

R is a Noetherian commutative ring with identity.

$S^{-1}R = \{r/s \mid s \in S, r \in R\}$ is the ring of fractions of R with respect to S where S is a multiplicatively closed subset of R.

$R_f = S^{-1}R$ is the localization of R at f where $f \in R$ and $S = \{\ f^n \mid n \in \mathbb{Z}, n \geq 0\}$.

$R_P = S^{-1}R$ is the localization of R at P where $S = R - P$ and $P \subset R$ is a prime ideal of R.

$I : J = \{a \in R \mid aJ \subset I\}$ is the ideal quotient of I by J where I and J are ideals in R.

$\sqrt{I} = \{a \in R \mid a^m \in I$ for some positive integer $m\}$ is the radical of the ideal $I \subset R$.

When we say that an ideal I is *given*, we mean that we are explicitly given a finite set of generators for this ideal.

For the polynomial ring $R[x_1, \ldots, x_n]$, we can abbreviate the notation as $R[x] := R[x_1, \ldots, x_n]$ and we denote the monomial $x_1^{\alpha(1)} x_2^{\alpha(2)} \cdots x_n^{\alpha(n)}$ by x^α where $\alpha = (\alpha(1), \ldots, \alpha(n)) \in \mathbb{N}^n$ is the multi-degree of the monomial. We will use the terms multi-degree and degree interchangeably.

Definition 3.1.1. *If the following holds, we say that linear equations are solvable in* R.

- *For any given $r,\ r_1, \ldots, r_k \in R$, it is possible to decide if $r \in (r_1, \ldots, r_k)R$ or not where $(r_1, \ldots, r_k)R$ is the ideal generated by $\{r_1, \ldots, r_k\}$ in R and if $r \in (r_1, \ldots, r_k)R$, it is possible to find $s_1, \ldots, s_k \in R$ such that $r = \sum s_i r_i$. (i.e. ideal membership problem is solvable in R).*

- *For any given $r_1, \ldots, r_k \in R$, it is possible to find a finite set of generators for the R-module $\{(s_1, \ldots, s_k) \in R^k \mid \sum s_i r_i = 0\}$.(i.e. syzygies are computable over R).*

Throughout, we assume that linear equations are solvable in the ring R.

Definition 3.1.2. *A total order $>$ on $\mathbb{N}^k$ is compatible with the semigroup structure if the following holds:*

- *$A \geq 0$ for all $A \in \mathbb{N}^k$ where 0 denotes the tuple $(0, \ldots, 0) \in \mathbb{N}^k$.*

- *$A > B$ implies $A + C > B + C$ for all $A,\ B,\ C \in \mathbb{N}^k$.*

Definition 3.1.3. *For a compatible total order $>$ on $\mathbb{N}^k$ we define the monomial order $>$ on $R[x] = R[x_1, \ldots, x_k]$ by $x^\alpha > x^\beta$ if $\alpha > \beta$ in $\mathbb{N}^k$.*

We fix a compatible order $>$ on $\mathbb{N}^k$ which induces a monomial order on $R[x] = R[x_1, \ldots, x_k]$. Such an order is necessarily a well-ordering [18], i.e., every nonempty subset of monomials has a least element. Equivalently, every descending sequence of monomials stabilizes after finitely many steps.

Definition 3.1.4. *We can write any non-zero $f \in R[x] = R[x_1, \ldots, x_n]$ as*

$$f = cx^A + \bar{f}$$

where $c \in R$, $c \neq 0$, and $A > A'$ for every nonzero term $c'x^{A'}$ of $\bar{f}$. According to this, we set

$$lt(f) = cx^A, \ \textit{the leading term of } f.$$
$$lc(f) = c, \ \textit{the leading coefficient of } f.$$
$$\deg(f) = A, \ \textit{the degree (multidegree) of } f.$$

If $G \subset R[x]$ is any subset, then we define $Lt(G) =$ the ideal generated by the set $lt(G) := \{lt(g) \mid g \in G\}$, i.e. the leading term ideal of G.

Moreover, $lt(0) = lc(0) = 0$ and $deg(0) = -\infty$ by convention.

Definition 3.1.5. *$f \in R[x]$ is called reducible modulo $G \subset R[x]$ if f is nonzero and $lt(f) \in Lt(G)$. Otherwise, f is called reduced modulo G.*

Note that this definition is rather different from the ones about polynomial reducibility.

Proposition 3.1.6 (Reduction Algorithm)**.** *Let $f \in R[x] = R[x_1, \ldots, x_n]$ and $G = \{g_1, \ldots, g_m\} \subset R[x]$. It is possible to construct f' as $f \equiv f'$ mod$(g_1, \ldots, g_m)R[x]$ where f' is reduced modulo G.*

Proof. By Definition 3.1.1, given $G = \{g_1, \ldots, g_m\} \subset R[x]$, we can decide whether $f \in R[x]$ is reducible modulo G or not as follows.

Let $lt(f) = cx^\alpha$ and $lt(g_i) = c_i x^{\alpha_i}$. Without loss of generality, we may assume $\alpha \geq \alpha_i$ for $1 \leq i \leq r$ and $\alpha < \alpha_i$ for $r < i \leq m$ for some r.

f is reducible modulo G if and only if there are $a_1, a_2, \ldots, a_r$ such that

$$lt(f) = cx^\alpha = \sum_{i=1}^{r} a_i x^{\alpha-\alpha_i} lt(g_i) = \sum_{i=1}^{r} a_i x^{\alpha-\alpha_i} c_i x^{\alpha_i}.$$

That is, f is reducible modulo G if and only if $lc(f) = c \in (c_1, \ldots, c_r)R$ which is decidable by Definition 3.1.1 (note that by assumption, linear equations are solvable in R), and we can compute $a_1, \ldots, a_r$ if they exist. In this case, we have $lt(f) = \sum_{i=1}^{r} a_i x^{\alpha-\alpha_i} lt(g_i)$.

Suppose f is not reducible, i.e., f is reduced. Then, we can take $f' = f$ and the proposition holds in this case.

Suppose f is reducible. Then as above, we can find $a_1, a_2, \ldots, a_r$ such that $lt(f) = \sum_{i=1}^{r} a_i x^{\alpha-\alpha_i} lt(g_i)$. Let $f_1 = f - \sum_{i=1}^{r} a_i x^{\alpha-\alpha_i} g_i$. Note that, the leading term of $\sum_{i=1}^{r} a_i x^{\alpha-\alpha_i} g_i$ cancels the leading term of f. Therefore, $\deg(f) > \deg(f_1)$ and we have $f \equiv f_1$ modulo$(g_1, \ldots, g_m)R[x]$. By induction on the degree of polynomials in

the monomial order $>$, we can find a reduced f' where $f' \equiv f_1 \; mod(g_1, \ldots, g_m)R[x]$. However, $f \equiv f_1$, therefore $f \equiv f' \; mod(g_1, \ldots, g_m)R[x]$. □

Definition 3.1.7 (Gröbner basis)**.** *A subset G of an ideal I where $I \subset R[x] = R[x_1, \ldots, x_n]$ is a Gröbner basis for I if $Lt(G) = Lt(I)$. Namely, if every nonzero element of I is reducible modulo G. G is called a minimal Gröbner basis if every $g \in G$ is nonzero and reduced modulo $G - \{g\}$.*

If $lt(g) \in Lt(G - \{g\})$, that is, if g is reducible modulo $G - \{g\}$, then $Lt(G - \{g\}) = Lt(G)$. Thus, if G is a Gröbner basis for I, then $G - \{g\}$ is a Gröbner basis for I, too. In fact, we can convert any Gröbner basis to a minimal one by eliminating the elements which are reducible modulo others.

The next proposition is about the crucial property of Gröbner bases.

Proposition 3.1.8 (Proposition 2.7. in [13])**.** *Let G be a Gröbner basis for $I \subset R[x]$. Then, $f \in I$ if and only if applying the reduction algorithm in Proposition 3.1.6 to f returns 0.*

Proof. Let $f \in I$ and let $f \equiv f' \; mod(g_1, \ldots, g_m)R[x]$ where $G = \{g_1, \ldots, g_m\}$ and f' is reduced modulo G. (Note that such an f' can be computed by Proposition 3.1.6). Since G is a Gröbner basis for I, $G \subset I$. Hence, $f' - f \in (g_1, \ldots, g_m)R[x] \subset I$ and $f \in I$ imply that $f' \in I$. If $f' \neq 0$, then $Lt(G) = Lt(I)$ and $f' \in I$ imply that f' is reducible modulo G which contradicts f' is reduced modulo G. Therefore $f' = 0$. Conversely, let $f \equiv 0 \; mod(g_1, \ldots, g_m)R[x]$, so $f = \sum_{i=1}^{m} \alpha_i g_i$ for some $\alpha_i \in R[x]$ which implies $f \in I$. □

Corollary 3.1.9 (Corollary 2.8. in [13])**.** *If G is a Gröbner basis for I, then ideal membership in I is decidable. That is, using G we can determine whether a given f in $R[x]$ is in I or not.*

Proof. Let $f \in R[x]$ and $G = \{g_1, \ldots, g_m\}$ be a Gröbner basis for I. By Proposition 3.1.6 we can compute $f' \in R[x]$ such that $f \equiv f' \mod(g_1, \ldots, g_m)R[x]$ and f' is reduced modulo G. By Proposition 3.1.8, $f \in I$ if and only if $f' = 0$. □

Corollary 3.1.10 (Corollary 2.9. in [13])**.** *If G is a Gröbner basis for I, then G generates I.*

Proof. Let $G = \{g_1, \ldots, g_m\}$ be a Gröbner basis for the ideal $I \subset R[x]$ where $R[x] = R[x_1, \ldots, x_n]$. By Definition 3.1.7, $G \subset I$, hence $(g_1, \ldots, g_m)R[x] \subset I$. Let $f \in I$. Then, by Proposition 3.1.8, $f \equiv 0 \bmod (g_1, \ldots, g_m)R[x]$, which means $f \in (g_1, \ldots, g_m)R[x]$. Therefore, $I \subset (g_1, \ldots, g_m)R[x]$ which proves the corollary. □

Proposition 3.1.11. *Every ideal I in $R[x_1, \ldots, x_n]$ has a finite Gröbner basis.*

Proof. Let I be an ideal in $R[x_1, \ldots, x_n]$, then $Lt(I)$ is also an ideal in $R[x_1, \ldots, x_n]$. By Hilbert Basis Theorem, $Lt(I)$ has a finite basis $\{h_1, \ldots, h_s\} \subset R[x_1, \ldots, x_n]$. Since $h_i \in Lt(I)$ for all i, we can write $h_i = \sum_{j=1}^{N_i} a_{ij} lt(f_{ij})$ for some $a_{ij} \in R[x_1, \ldots, x_n]$ and $f_{ij} \in I$. Let $G = \{g_1, \ldots, g_t\} = \{f_{ij} \mid 1 \leq i \leq s, 1 \leq j \leq N_i\}$. Since each $h_i \in Lt(G)$, we get $Lt(I) = (h_1, \ldots, h_s)R[x] \subset Lt(G)$. Also, $G \subset I$ implies $Lt(G) \subset Lt(I)$. This proves $Lt(G) = Lt(I)$. Since $G \subset I$, G is a Gröbner basis for I. □

Corollary 3.1.12 (Corollary 2.10. in [13])**.** *If $I \subset J$ are ideals in $R[x]$ and $Lt(I) = Lt(J)$, then $I = J$.*

Proof. Let G be a Gröbner basis for I, then $G \subset I$ and $Lt(G) = Lt(I) = Lt(J)$. $I \subset J$ implies $G \subset J$. Since $Lt(J) = Lt(G)$, G is also a Gröbner basis for J. Since G is Gröbner basis of both I and J, this implies G generates I, and G generates J by Corollary 3.1.10. Thus $I = J$. □

Proposition 3.1.13 (Proposition 2.11. in [13])**.** *One can compute a Gröbner basis for an ideal I in $R[x]$ from any given set of generators of I.*

Proof. We can find proof in [15] and [18].

Due to Hilbert Basis Theorem (see [3], pg.75-80), we proved the existence of a Gröbner basis in Proposition 3.1.11 above. For $k[x_1, \ldots, x_n]$ where k is a field, we can compute a Gröbner basis for I from a given set of generators using Buchberger's Algorithm (see [3] pg.88-95, [1]). In the more general case where R is a Noetherian ring in which linear equations are solvable, there is an algorithm to compute a Gröbner basis of I given in [15, 18]. □

3.2 Operations on Ideals

We can use Gröbner bases to do basic operations on ideals in $R[x]$. We build following structures which rely on an investigation by [14] that if Gröbner bases are computed according to the lexicographical order on monomials, then they have the effect of eliminating the more "basic" variables. Below is the proposition that defines this property in a detailed fashion.

Proposition 3.2.1 (Proposition 3.1. in [13])**.** *Let I be an ideal in $R[y,x]$ such that $R[y,x] = R[y_1,\ldots,y_n,x_1,\ldots,x_m]$. Let $>_1$ and $>_2$ be two orders on monomials in x and y respectively. Define an order $>$ by $x^A y^B > x^{A'} y^{B'}$ if $x^A >_1 x^{A'}$, or if $x^A = x^{A'}$ and $y^B >_2 y^{B'}$. Let $G \subset R[y,x]$ be a Gröbner basis for I with respect to $>$. Then we have,*

1. *G is a Gröbner basis for I with respect to the order $>_1$ on $(R[y])[x]$, i.e, on the polynomial ring in $x_1,\ldots,x_m$ with coefficients in $R[y]$.*
2. *$G \cap R[y]$ is a Gröbner basis for $I \cap R[y]$ with respect to the order $>_2$ (Gröbner basis of the elimination ideal).*

Proof. (i) We begin with the following claim.

Claim 1: $lt_>(lt_{>_1}(f)) = lt_>(f)$ *for any* $f \in R[x,y]$.

Proof of Claim 1: To find $lt_{>_1}(f)$, we order the terms of f comparing the components containing x. Afterwards, the biggest component has a coefficient that is a polynomial in y. Thus, if we order that polynomial with respect to $>_2$, then we get the leading term of f with respect to $>$ which proves the claim.

Let $G = \{g_1,\ldots,g_t\}$ be a Gröbner basis for I with respect to the order $>$. For each $g_i \in G$, by the above claim, we have $lt_>(g_i) = lt_>(lt_{>_1}(g_i))$. Thus, $lt_>(g_i) \in Lt_>(Lt_{>_1}(G))$, which implies $Lt_>(G) \subset Lt_>(Lt_{>_1}(G))$. Hence,

$$Lt_>(I) = Lt_>(G) \subset Lt_>(Lt_{>_1}(G)) \subset Lt_>(Lt_{>_1}(I)) \tag{3.1}$$

since $G \subset I$. We continue with the following claim.

Claim 2: $Lt_>(Lt_{>_1}(I)) \subset Lt_>(I)$.

Proof of Claim 2: Let $G_1 = \{k_1, \ldots, k_s\}$ be a Gröbner basis for I with respect to the order $>_1$. So, $I = \langle k_1, \ldots, k_s \rangle$ where $k_i \in I$ for all i and $Lt_{>_1}(I) = \langle lt_{>_1}(k_1), \ldots, lt_{>_1}(k_s) \rangle$. Let $f \in Lt_{>_1}(I)$, then $f = \sum_i h_i(x,y) lt_{>_1}(k_i)$ where $h_i(x,y) \in R[x,y]$ for all i (since G_1 is a Gröbner basis of I with respect to $>_1$, i.e., $Lt_{>_1}(I) = Lt_{>_1}(G_1)$). Let $lt_{>_1}(k_i) = p_i(y)x^{\alpha_i}$. Thus, $f = \sum_i h_i(x,y)p_i(y)x^{\alpha_i}$. Let $lt_{>_1}(f)$ have degree A. So,

$lt_{>_1}(f) = \sum_i q_i(y)x^{A-\alpha_i}p_i(y)x^{\alpha_i}$ where $q_i(y)x^{A-\alpha_i}$ is the term of h_i with degree $(A-\alpha_i)$ in x. Hence,

$$lt_{>_1}(f) = lt_{>_1}(\sum_i q_i(y)x^{A-\alpha_i}k_i) = lt_{>_1}(F)$$

where $F = \sum_i q_i(y)x^{A-\alpha_i}k_i \in I$ since $I = \langle k_1, \ldots, k_s \rangle$. Therefore, $lt_>(f) = lt_>(lt_{>_1}(f)) = lt_>(lt_{>_1}(F)) = lt_>(F) \in Lt_>(I)$ which proves the claim.

As a result of Claim 2 and Eq.(3.1), we get

$$Lt_>(I) = Lt_>(G) = Lt_>(Lt_{>_1}(G)) = Lt_>(Lt_{>_1}(I)).$$

By Corollary 3.1.12, $Lt_>(Lt_{>_1}(I)) = Lt_>(Lt_{>_1}(G))$ implies $Lt_{>_1}(I) = Lt_{>_1}(G)$ which proves (i).

(ii) By definition of $>$ in the ring $R[y,x]$, terms involving only y_i variables are smaller than the ones involving any x_i variable. Hence, if a polynomial has a leading term in y, then none of its terms can involve any x_i variable, i.e., $lt_>(g) \in R[y]$ if and only if $g \in R[y]$.

Let $G = \{g_1, \ldots, g_u, g_{u+1}, \ldots, g_t\}$ be a Gröbner basis of I such that $G \cap R[y] = \{g_1, \ldots, g_u\}$. $I \cap R[y]$ is an ideal of $R[y]$ and we have $G \cap R[y] \subset I \cap R[y]$. To prove that $G \cap R[y]$ is a Gröbner basis of $I \cap R[y]$ with respect to $>_2$, we must show $lt_{>_2}(f) \in Lt_{>_2}(G \cap R[y])$ for all $f \in I \cap R[y]$. If $f \in I \cap R[y]$, then $lt_{>_2}(f) = lt_>(f) = \sum_{i=1}^{t} p_i(x,y) lt_>(g_i)$ since G is a Gröbner basis of I and $f \in I$. (Note that $>$ and $>_2$ coincide on $R[y]$. Hence, $lt_>(g_i) = lt_{>_2}(g_i)$ for $i = 1, \ldots, u$). If we write $p_i(x,y) = q_i(x,y) + a_i(y)$ where $q_i(x,y)$ consists of terms of $p_i(x,y)$ involving at

least one x_j variable, then we get

$$\begin{aligned} lt_{>_2}(f) &= \sum_{i=1}^{t}(q_i(x,y)+a_i(y))lt_{>}(g_i) \\ &= \sum_{i=1}^{u} a_i(y)lt_{>_2}(g_i) + \sum_{i=1}^{u} q_i(x,y)lt_{>_2}(g_i) + \sum_{i=u+1}^{t} p_i(x,y)lt_{>}(g_i) \\ &= \sum_{i=1}^{u} a_i(y)lt_{>_2}(g_i) \in Lt_{>_2}(G \cap R[y]) \end{aligned}$$

since the terms involving at least one x_j variable are collected in the last two sigma summations and they add up to zero (as the left hand side is in $R[y]$). Therefore, $Lt_{>_2}(f) \in Lt_{>_2}(G \cap R[y])$ which proves (ii). □

We review applications of Gröbner bases in computations regarding basic ideal operations.

Proposition 3.2.2 (Computing intersection of ideals)**.** *Let I and J be given ideals in $R[x] = R[x_1, \ldots, x_n]$. Then $I \cap J$ can be computed. In other words, we can determine a finite basis of $I \cap J$ when finite bases of I and J are given.*

Proof. Let I and J be ideals in $R[x]$. We start with a claim.

Claim: $I \cap J = (tI + (1-t)J) \cap R[x]$ *where t is a new variable.*

Proof of Claim: $tI + (1-t)J$ is the ideal of $R[x,t] = R[x_1, \ldots, x_n, t]$ generated by all tf and $(1-t)g$ where $f \in I$ and $g \in J$.

Let $f \in I \cap J$. So, $f \in I$ implies $tf \in tI$. Also, $f \in J$ implies $(1-t)f \in (1-t)J$. Therefore, $f = tf + (1-t)f \in tI + (1-t)J$. Hence, we have $f \in (tI + (1-t)J) \cap R[x]$.

Now, let $f \in (tI + (1-t)J) \cap R[x]$. Then, we can write f as

$$f = \sum_{i=1}^{N} k_i(x,t)tl_i(x) + \sum_{j=1}^{M} \bar{k_j}(x,t)(1-t)\bar{l_j}(x)$$

for some $l_i \in I$ and $\bar{l_j} \in J$. Note that, $f \in R[x,t]$ and f has no terms involving t. Substituting $t = 0$ we get $f(x) = 0 + \sum_{j=1}^{M} \bar{k_j}(x,0)\bar{l_j}(x) \in J$. Similarly, substituting $t = 1$ we get $f = \sum_{i=1}^{N} k_i(x,1)l_i(x) + 0$ from above, hence, $f \in I$. Therefore, $f \in I \cap J$ which proves the claim.

By this claim and the elimination theorem (see, Proposition 3.2.1(ii)), we get an algorithm for computing intersection of ideals.

If we let $I = \langle f_1, \ldots, f_k \rangle$, and $J = \langle g_1, \ldots, g_m \rangle$ be ideals in $R[x_1, \ldots, x_n]$, then we can compute a Gröbner basis G for the ideal $tI + (1-t)J = \langle tf_1, \ldots, tf_k, (1-t)g_1, \ldots, (1-t)g_m \rangle \subset R[x_1, \ldots, x_n, t]$ with respect to the lexicographical order where $t > x_i$ for all i. The elements of this Gröbner basis G that do not contain the variable t form a Gröbner basis of the ideal $(tI + (1-t)J) \cap R[x] = I \cap J$ (that is, $G \cap R[x]$ is a Gröbner basis of $I \cap J$). □

Proposition 3.2.3 (Computing ideal quotients)**.** *Let I and J be given ideals in $R[x] = R[x_1, \ldots, x_n]$. Then $I : J$ can be computed provided the generators of J are not zero divisors.*

Proof. Let $I = \langle f_1, \ldots, f_s \rangle$ and $J = \langle g_1, \ldots, g_k \rangle$ be ideals in $R[x]$. We first prove a claim.

Claim 1: $I : J = I : \langle g_1, \ldots, g_k \rangle = \bigcap_{i=1}^{k} I : \langle g_i \rangle$.

Proof of Claim 1: $I : \langle g_1, \ldots, g_k \rangle = \{f \in R[x] \mid fg \in I \text{ for all } g \in \langle g_1, \ldots, g_k \rangle\}$. If $f \in I : \langle g_1, \ldots, g_k \rangle$, then for each $g = h_i g_i$ where $h_i \in R[x]$, we get $f h_i g_i \in I$ since $h_i g_i \in \langle g_1, \ldots, g_k \rangle$. Thus, $f \in I : \langle g_i \rangle$ for all $i \in \{1, \ldots, k\}$ which implies $f \in \bigcap_{i=1}^{k} I : \langle g_i \rangle$. Conversely, if $f \in \bigcap_{i=1}^{k} I : \langle g_i \rangle$, then $f h_i g_i \in I$ for all i and $h_i \in R[x]$. Hence, if $g \in \langle g_1, \ldots, g_k \rangle$, then $g = h_1 g_1 + \cdots + h_k g_k$ where $h_i \in R[x]$. Therefore, $fg = f h_1 g_1 + \cdots + f h_k g_k \in I$ which shows $f \in I : \langle g_1, \ldots, g_k \rangle$ and this proves the claim.

As a result, if we can compute each $I : \langle g_i \rangle$ then we can compute $I : J$.

Claim 2: Let $\{h_1, \ldots, h_s\}$ be a a basis of $I \cap \langle g_i \rangle$. Then a basis of $I : \langle g_i \rangle$ is given by $\{h_1/g_i, \ldots, h_s/g_i\}$ provided that g_i is not a zero divisor.

Proof of Claim 2: Note that, we can compute $\{h_1, \ldots, h_s\}$ by Proposition 3.2.2. Since $g_i(h_j/g_i) = h_j \in I$, we have $\langle h_1/g_i, \ldots, h_s/g_i \rangle \subset I : \langle g_i \rangle$. Now, let $f \in I : \langle g_i \rangle$. Then, $f g_i \in I$ and $f g_i \in \langle g_i \rangle$ which means $f g_i \in I \cap \langle g_i \rangle$. We can write $f g_i = a_1 h_1 + \cdots + a_s h_s$ for some $a_j \in R[x]$ which gives $f = a_1(h_1/g_i) + \cdots + a_s(h_s/g_i)$ since each h_j is divisible by g_i (as $h_j \in \langle g_i \rangle$) and g_i is not a zero divisor. This shows

$I : \langle g_i \rangle \subset \langle h_1/g_i, \ldots, h_s/g_i \rangle$ which gives the equality and proves the claim.

After computing a basis for each $I : \langle g_i \rangle$ as in Claim 2, we can compute $I : J$ as the intersection of these ideals using Proposition 3.2.2. □

Proposition 3.2.4 (Computing the kernel of a homomorphism)**.** *Let I be an ideal in $R[x_1, \ldots, x_n]$. Then the kernel of a given homomorphism $\phi : R[y_1, \ldots, y_m] \to R[x_1, \ldots, x_n]/I$ can be computed.*

Proof. Let $\phi : R[y] \to R[x]/I$ be a homomorphism given by $\phi(y_i) = f_i + I$ where $f_i \in R[x]$ for $i \in \{1, \ldots, m\}$.

Claim: $J = (y_1 - f_1, \ldots, y_m - f_m, I)R[x, y] \cap R[y]$ is the kernel of the above homomorphism ϕ.

Proof of Claim: Suppose $I = \langle G_1, \ldots, G_k \rangle$ and $F \in J$ where $F = F(y_1, \ldots, y_m)$. Then,

$$F = H_1(x, y)(y_1 - f_1) + \cdots + H_m(x, y)(y_m - f_m) + \sum_{j=1}^{k} L_j(x, y)G_j$$

for some $H_i(x, y) \in R[x, y]$ and $L_j(x, y) \in R[x, y]$. Note that, since F is a polynomial and $\phi(y_i) = f_i + I$ for the homomorphism ϕ, we have $\phi(F) = F(f_1, \ldots, f_m) + I$. Thus,

$$\begin{aligned}\phi(F) = (\sum_{i=1}^{m} H_i(x_1, \ldots, x_n, f_1, \ldots, f_m)(f_i - f_i) + \\ \sum_{j=1}^{k} L_j(x_1, \ldots, x_n, f_1, \ldots, f_m)G_j) + I \\ = 0 + (\sum_{j=1}^{k} L_j(x_1, \ldots, x_n, f_1, \ldots, f_m)G_j) + I = 0 + I.\end{aligned}$$

Since $\sum_{j=1}^{k} L_j(x_1, \ldots, x_n, f_1, \ldots, f_m)G_j \in I$. Therefore, $F \in Ker(\phi)$.

Conversely, let $F \in Ker(\phi)$. So, $\phi(F) \equiv 0$ in $R[x]/I$. Here, $F = F(y_1, \ldots, y_m) \in R[y]$. Hence, $\phi(F) = F(f_1, \ldots, f_m) \in I$.

We can write, $F(y_1, \ldots, y_m) = F((y_1 - f_1) + f_1, \ldots, (y_m - f_m) + f_m)$. If we take a term of F, we have

$$c_i y_1^{\alpha_1} \cdots y_m^{\alpha_m} = c_i (y_1 - f_1 + f_1)^{\alpha_1} \cdots (y_m - f_m + f_m)^{\alpha_m}$$

where $c_i \in R$. After binomial expansion, this term becomes $(\sum_{i=1}^{N} H_i(x)(y_1 - f_1)^{\beta_{i1}} \cdots (y_m - f_m)^{\beta im}) + c_i f_1^{\alpha_1} \cdots f_m^{\alpha_m}$ where $(\beta_{i1}, \ldots, \beta_{im}) \neq (0, \ldots, 0)$.

As a result, $F(y_1, \ldots, y_m) = G(x, y) + F(f_1, \ldots, f_m)$ where, $G(x, y) \in \langle y_1 - f_1, \ldots, y_m - f_m \rangle$. Since $F(f_1, \ldots, f_m) \in I$, we obtain $F \in (y_1 - f_1, \ldots, y_m - f_m, I)R[x, y] \cap R[y] = J$, hence $Ker(\phi) \subset J$ which proves the claim and the proposition.

Note that, J is computable since by using a *lex* order where $x_i > y_j$ for all i and j, we can compute the elimination ideal $(y_1 - f_1, \ldots, y_m - f_m, I)R[x, y] \cap R[y]$ using Proposition 3.2.1. □

Corollary 3.2.5 (Computing the ideal of polynomial relations among polynomials)**.** *For a given set of polynomials $\{f_1, \ldots, f_m\} \subset R[x]$, the ideal of polynomial relations satisfied by $f_1, \ldots, f_m$ can be computed.*

Proof. In Proposition 3.2.4, if we take $I = \langle 0 \rangle$ and $\phi : R(y_1, \ldots, y_m) \to R[x] = R[x]/I$ where $\phi(y_i) = f_i$ for all i, then we get $h(f_1, \ldots, f_m) = 0$ if and only if $h(y_1, \ldots, y_m) \in Ker(\phi)$. Therefore, the ideal of polynomial relations among $f_1, \ldots, f_m$ is exactly $Ker(\phi)$ which can be computed by Proposition 3.2.4. □

Proposition 3.2.6 (Computing the saturation of an ideal at an element)**.** *For a given ideal I in $R[x]$, $IR[x]_f \cap R[x]$ can be computed for any nonzero divisor $f \in R[x]$.*

Proof. Here, $R[x]_f = S^{-1}R[x]$ where $S = \{f^n \mid n \geq 0\}$ and $IR[x]_f$ is the ideal generated by I in $R[x]_f$.

Claim: $R[x]_f \cong R[x, t]/\langle tf - 1 \rangle$ where $f \in R[x]$, t is a new variable.

Proof of Claim: Let $\varphi : R[x, t] \to R[x]_f$ be a homomorphism given by $g(x, t) \mapsto g(x, 1/f)$. φ is an epimorphism since we can replace every $(1/f)^s$ in $h \in R[x]_f$ by t^s and get a polynomial in $R[x, t]$.

First, we show $Ker(\varphi) = \langle tf - 1 \rangle$.

Let $h(x,t) \in \langle tf-1 \rangle$, then we have $h(x,t) = g(x,t)(tf-1)$ where $g(x,t) \in R[x,t]$. Hence, $\varphi(h(x,t)) = h(x,1/f) = g(x,1/f)((1/f)f-1) = 0$ which implies $h(x,t) \in Ker(\varphi)$.

Conversely, let $h(x,t) \in Ker(\varphi)$. Let $(tf-1) \nmid h(x,t)$. So, by reduction algorithm in $(R[x])[t]$ (see Proposition 3.1.6), we get $h(x,t) = (tf-1)g(x,t) + r(x,t)$ where $r(x,t) \neq 0$ such that $r(x,t)$ is reduced modulo $\langle tf-1 \rangle$. Then $lt(tf-1) \nmid lt(r(x,t))$, i.e., $f(x)t \nmid lt(r(x,t))$. If we let $r(x,t) = a_0(x)t^m + a_1(x)t^{m-1} + \cdots + a_{m-1}(x)t + a_m(x)$, then $f(x)t \nmid a_0(x)t^m$ implies $f(x) \nmid a_0(x)$ if $m \geq 1$.

On the other hand, $h(x,1/f) = (0)g(x,1/f) + r(x,1/f) = 0$ implies

$r(x,1/f) = a_0(x)(1/f^m) + \cdots + a_{m-1}(1/f) + a_m(x) = 0$. In the case $m \geq 1$, after equating the denominators, $f(x)$ divides $a_0(x)$ which contradicts the above implication. If $m = 0$ then $r(x,1/f) = 0$ implies $a_0(x) = 0$. Hence $(tf-1) \mid h(x,t)$ which is again a contradiction. Thus, the claim is proven by the first isomorphism theorem.

Define $\psi : R[x] \to R[x,t]/\langle tf-1 \rangle$ by $\psi(g) = g + \langle tf-1 \rangle$. ψ is a monomorphism ($g_1, g_2 \in R[x]$ and $(tf-1) \mid (g_1 - g_2)$ implies $g_1 = g_2$) and $\psi(R[x])$ is the isomorphic copy of $R[x]$ in $R[x,t]/\langle tf-1 \rangle$. If we identify $R[x]_f$ and $R[x,t]/\langle tf-1 \rangle$ by the isomorphism in the above claim, then $IR[x]_f$ is generated by all $g + \langle tf-1 \rangle$ in $R[x,t]/\langle tf-1 \rangle$ where $g \in I$ (i.e., generated by $\psi(I)$). Hence, $IR[x]_f$ is given by $J/\langle tf-1 \rangle$ in $R[x,t]/\langle tf-1 \rangle$ where $J = (I, tf-1)R[x,t]$. Since ψ is a monomorphism, every coset in $\psi(R[x])$ is represented as $g(x) + \langle tf-1 \rangle$ by a unique $g(x) \in R[x]$. Therefore, $IR[x]_f \cap R[x]$ is given by $J/\langle tf-1 \rangle \cap \psi(R[x])$ in $R[x,t]/\langle tf-1 \rangle$. Let $h(x,t) + \langle tf-1 \rangle \in (J/\langle tf-1 \rangle) \cap \psi(R[x])$, then $h(x,t) \in J$ and $h(x,t) = \bar{h}(x) + (tf-1)k(x,t)$ for some $k(x,t)$. Thus, $h(x,t) + \langle tf-1 \rangle = \bar{h}(x) + \langle tf-1 \rangle$. Since $h \in J$ and $tf - 1 \in J$ we get $\bar{h}(x) \in J$. Hence, $\bar{h}(x) \in J \cap R[x]$. This shows $\psi(J \cap R[x]) = (J/\langle tf-1 \rangle) \cap \psi(R[x])$. Therefore, since ψ is a monomorphism, $IR[x]_f \cap R[x]$ which is given by $\psi(J \cap R[x])$ in $R[x,t]/\langle tf-1 \rangle$ is isomorphic to $J \cap R[x]$ in $R[x]$. Therefore, by the above identification, we get $IR[x]_f \cap R[x] = J \cap R[x] = (tf-1, I)R[x,t] \cap R[x]$.

We can compute $J \cap R[x]$ by using a Gröbner basis of J with respect to a *lex* order

where $t > x_i$ for all i as in Proposition 3.2.1 (ii). $\square$

In Proposition 3.2.1(ii), we saw that if G is a Gröbner basis of the ideal $I \subset R[x, y]$ with respect to the order $>$, then $G \cap R[y]$ is a Gröbner basis for $I \cap R[y]$ (with respect to the order $>_2$). In particular $G \cap R$ is a basis for $I \cap R$. This can be described in a complete manner as follows.

Proposition 3.2.7 (Proposition 3.3.i in [13])**.** *Let I be an ideal in $R[x]$ and let $\rho : R[x] \to (R/(I \cap R))[x]$ be the quotient map. If $G \subset I$ is a Gröbner basis for I, then*

1. *$G \cap R$ generates $I \cap R$ and $\rho(G)$ is a Gröbner basis for $\rho(I)$.*
2. *G is a minimal Gröbner basis for I if and only if $G \cap R$ is a minimal basis for $I \cap R$, $\rho(G - G \cap R)$ is a minimal Gröbner basis for $\rho(I)$ and $\rho(lt(g)) \neq 0$ for all $g \in (G - G \cap R)$.*

Proof. (i) We begin with a claim.

Claim: $\rho(Lt(I)) = Lt(\rho(I))$.

Proof of Claim: If $f = \sum_{i=1}^{N} a_i x^{\alpha_i}$ where $a_i \in R$ and $\alpha_i \in \mathbb{N}$, then $\rho(f) = \sum_{i=1}^{N} \bar{a}_i x^{\alpha_i}$ where $\bar{a}_i \in R/(I \cap R)$. Hence, either $\rho(lt(f)) = \bar{0}$ or $\rho(lt(f)) = lt(\rho(f))$. Therefore, $\rho(Lt(I)) \subset Lt(\rho(I))$. Conversely, if $f \in I$, let $f = f_0 + f_1$ where $\rho(f_0) = \bar{0}$ and $\rho(lt(f_1)) \neq \bar{0}$. In particular, $f_0 \in I$ since all coefficients of f_0 are in $I \cap R$, hence $f_1 = f - f_0 \in I$ and $lt(\rho(f)) = lt(\rho(f_1)) = \rho(lt(f_1)) \in \rho(Lt(I))$. Thus, $Lt(\rho(I)) \subset \rho(Lt(I))$. Therefore, $\rho(Lt(I)) = Lt(\rho(I))$ which proves the claim.

Now, if G is a Gröbner basis for I, then by Proposition 3.2.1(ii), $G \cap R$ generates $I \cap R$. Since $Lt(G) = Lt(I)$ and $\rho(Lt(I)) = Lt(\rho(I))$, we have $Lt(\rho(I)) = \rho(Lt(I)) = \rho(Lt(G)) \subset Lt(\rho(G)) \subset Lt(\rho(I))$ implying $Lt(\rho(I)) = Lt(\rho(G))$. Hence, $\rho(G)$ is a Gröbner basis for $\rho(I)$. Note that, if $G = \{g_1, \ldots, g_s\}$, then $\rho(Lt(G)) = \rho(\langle lt(g_1), \ldots, lt(g_s)\rangle) = \langle \rho(lt(g_1)), \ldots, \rho(lt(g_s))\rangle$
$= \langle lt(\rho(g_1)), \ldots, lt(\rho(g_r))\rangle \subset \langle lt(\rho(g_1)), \ldots, lt(\rho(g_s))\rangle = Lt(\rho(G))$ where without loss of generality, $\rho(lt(g_i)) = \bar{0}$ for $r < i \leq s$ and $\rho(lt(g_j)) \neq \bar{0}$, hence $\rho(lt(g_j)) = lt(\rho(g_j))$ for $1 \leq j \leq r$. Since $G \subset I$ we have $\rho(G) \subset \rho(I)$ which implies $Lt(\rho(G)) \subset Lt(\rho(I))$.

We can prove (ii) by using definitions and (i). $\square$

We can obtain ring of fractions of $R[x]$ by using multiplicative subsets of R. Gröbner basis has a useful property regarding this process which is as follows.

Proposition 3.2.8 (Gröbner basis of ideals in ring of fractions)**.** *Let S be a multiplicatively closed subset of R. If G is a Gröbner basis for an ideal $I \subset R[x]$, then G is a Gröbner basis for the ideal $S^{-1}I \subset (S^{-1}R)[x]$.*

Proof. We begin by proving the following.

Claim: $Lt(S^{-1}I) = S^{-1}Lt(I)$.

Proof of Claim: Let $G = \{f_1, \ldots, f_k\}$ be a Gröbner basis for I. We have $S^{-1}I = \{f/\alpha \mid \alpha \in S,\ f \in I\}$ where $f/\alpha = \sum_{i=1}^{k}(h_i f_i/\alpha)$ such that $\alpha \in S$, $f_i \in G$, $h_i \in R[x]$. Thus, $Lt(S^{-1}I) = \langle lt(f/\alpha) \mid f \in I,\ \alpha \in S\rangle$. We know that $lt(f/\alpha) = lt(f)/\alpha$ by basic ring axioms. Hence, $\langle lt(f/\alpha) \mid f \in I,\ \alpha \in S\rangle = \langle lt(f)/\alpha \mid f \in I,\ \alpha \in S\rangle$ and since $\alpha \in S$ are units in $S^{-1}R$, we have $\langle lt(f)/\alpha \mid f \in I,\ \alpha \in S\rangle = \langle lt(f) \mid f \in I\rangle$ where $\langle lt(f)\rangle$ as ideals of $S^{-1}R[x]$. Thus, $Lt(S^{-1}I) = \langle lt(f) \mid f \in I\rangle$ in $S^{-1}R[x]$. Now, $S^{-1}Lt(I) = S^{-1}\langle lt(f) \mid f \in I\rangle = \langle lt(f) \mid f \in I\rangle = Lt(S^{-1}I)$. This proves the claim.

By definition of Gröbner basis, $Lt(I) = Lt(G)$, hence $Lt(S^{-1}I) = S^{-1}Lt(I) = S^{-1}Lt(G) = \langle lt(g) \mid g \in G\rangle$ in $S^{-1}R[x]$ by above claim. This implies $Lt(S^{-1}I) = Lt(G)$ in $S^{-1}R[x]$ which proves the result. $\square$

Now we look at an important property about the saturation ideal which relates it to the leading term ideal.

Lemma 3.2.9 (Lemma 3.5 in [13])**.** *Let $T \subset S$ be multiplicatively closed subsets of R, let I be an ideal in $R[x]$. If*

$$S^{-1}Lt(I) \cap R[x] = T^{-1}Lt(I) \cap R[x]$$

then

$$S^{-1}I \cap R[x] = T^{-1}I \cap R[x].$$

Proof. Since $T \subset S$ are multiplicative subsets of R, we have $R[x] \subset T^{-1}R[x] \subset S^{-1}R[x]$ as ring extensions. Moreover, $T \subset S$ implies $T^{-1}(S^{-1}R) = S^{-1}R$. Now, we need some claims.

Claim 1: $Lt(S^{-1}I \cap T^{-1}R[x]) \subset Lt(S^{-1}I) \cap T^{-1}R[x]$.

Proof of Claim 1: Note that $Lt(S^{-1}I \cap T^{-1}R[x])$ is the leading term ideal in $T^{-1}R[x]$ and we have $Lt(S^{-1}I \cap T^{-1}R[x]) \subset T^{-1}R[x]$. Also, $S^{-1}I \cap T^{-1}R[x] \subset S^{-1}I$ which implies $Lt(S^{-1}I \cap T^{-1}R[x]) \subset Lt(S^{-1}I)$ as ideals in $S^{-1}R[x]$. This proves the claim.

Moreover, we have $Lt(S^{-1}I) \cap T^{-1}R[x] = S^{-1}Lt(I) \cap T^{-1}R[x]$ by the claim in Proposition 3.2.8.

Claim 2: $S^{-1}Lt(I) \cap T^{-1}R[x] = T^{-1}(S^{-1}Lt(I) \cap R[x])$.

Proof of Claim 2: First of all, since $T \subset S$, $T^{-1}(S^{-1}Lt(I)) = S^{-1}Lt(I)$. Hence, $T^{-1}(S^{-1}Lt(I) \cap R[x]) \subset S^{-1}Lt(I)$, and clearly $T^{-1}(S^{-1}Lt(I) \cap R[x]) \subset T^{-1}R[x]$ which implies $RHS \subset LHS$. To prove $LHS \subset RHS$, let $F = \sum_i \frac{h_i}{s_i} lt(f_i) \in S^{-1}Lt(I) \cap T^{-1}R[x]$ where $h_i \in R[x]$, $s_i \in S$ and $f_i \in I$. Since $F \in T^{-1}R[x]$, $F = G/t$ for some $G \in R[x]$, $t \in T$ which gives $G = tF = \sum_i \frac{th_i}{s_i} lt(f_i) \in S^{-1}Lt(I)$. Thus, $G \in S^{-1}Lt(I) \cap R[x]$. Therefore, $F = G/t \in T^{-1}(S^{-1}Lt(I) \cap R[x])$. This proves the equality of both sides.

Now, by the assumption of the lemma, $T^{-1}(S^{-1}Lt(I) \cap R[x]) = T^{-1}(T^{-1}Lt(I) \cap R[x])$.

Claim 3: $T^{-1}(T^{-1}Lt(I) \cap R[x]) = T^{-1}Lt(I)$.

Proof of Claim 3: Since $Lt(I) \subset T^{-1}Lt(I) \cap R[x]$, we get $RHS \subset LHS$. And since $T^{-1}Lt(I) \cap R[x] \subset T^{-1}Lt(I)$, the ideal generated by $T^{-1}Lt(I) \cap R[x]$ in $T^{-1}R[x]$ which equals LHS is a subset of $T^{-1}Lt(I)$. (The ideal generated by a subset of an ideal is a subset of that ideal). Hence, we get $LHS \subset RHS$ which proves the claim.

We have $T^{-1}Lt(I) = Lt(T^{-1}I)$ by the claim in proof of Proposition 3.2.8.

Claim 4: $T^{-1}I \subset S^{-1}I \cap T^{-1}R[x]$.

Proof of Claim 4: We have $T^{-1}I \subset S^{-1}I$ since $T \subset S$. Moreover, $T^{-1}I \subset T^{-1}R[x]$, too. Hence the result follows.

As a summary of all these claims and arguments, we have shown that $Lt(S^{-1}I \cap T^{-1}R[x]) \subset Lt(S^{-1}I) \cap T^{-1}R[x] = S^{-1}Lt(I) \cap T^{-1}R[x] = T^{-1}(S^{-1}Lt(I) \cap R[x]) = T^{-1}(T^{-1}Lt(I) \cap R[x]) = T^{-1}Lt(I) = Lt(T^{-1}I) \subset Lt(S^{-1}I \cap T^{-1}R[x])$. This proves $Lt(S^{-1}I \cap T^{-1}R[x]) = Lt(T^{-1}I)$. Using Corollary 3.1.12, we get $S^{-1}I \cap T^{-1}R[x] = T^{-1}I$. If we intersect both sides with $R[x]$, then we prove the lemma. □

Remark: If we take $T = \{1\}$ in the Lemma 3.2.9, then $S^{-1}I \cap R[x] = I$ provided that $S^{-1}Lt(I) \cap R[x] = Lt(I)$, i.e., if $Lt(I)$ is saturated with respect to S, then so is I. In fact, according to this lemma, we can compute the saturation of I with respect to S using a "smaller" multiplicative set T, in case this change of sets does not have an effect on the leading term ideal.

Corollary 3.2.10 (Proposition 3.6 in [13])**.** *Let S be a multiplicatively closed subset of R, let I be an ideal in $R[x]$. If for some $s \in S$,*

$$S^{-1}Lt(I) \cap R[x] = (LT(I)R_s[x]) \cap R[x]$$

then

$$S^{-1}I \cap R[x] = IR_s[x] \cap R[x].$$

Proof. In Lemma 3.2.9, if we let $T = \{s^n \mid n \geq 0\}$, then the result follows since $T^{-1}R[x] = R_s[x]$ and $T^{-1}Lt(I) = Lt(I)R_s[x]$ and $T^{-1}I = IR_s[x]$. □

By Corollary 3.2.6, we can compute $IR_s[x] \cap R[x]$, thus we can compute $S^{-1}I \cap R[x]$ if we can find an $s \in S$ satisfying the assumption of Corollary 3.2.10. Therefore, Corollary 3.2.10 evolves the problem of computing the saturation $S^{-1}I \cap R[x]$ of an ideal I in $R[x]$ to an equivalent problem for ideals generated by leading terms. The computability of solution depends on R and S.

The localization R_P at a prime ideal $P \subset R$ is another issue if we let $S = R - P$ in aforementioned results. In the special case that the prime ideal P is principal, the saturation of I with respect to P can be computed using the following proposition.

Proposition 3.2.11 (Proposition 3.7 in [13]). *Let R be an integral domain, $(p) \subset R$ be a principal prime ideal. For any given ideal $I \subset R[x]$, it is possible to find $s \in R - (p)$ such that*

$$IR_{(p)}[x] \cap R[x] = IR_s[x] \cap R[x].$$

In particular, $IR_{(p)}[x] \cap R[x]$ can be computed.

Proof. We need to prove a claim beforehand.

Claim 1: If R is a Noetherian domain, then $\bigcap_{k=1}^{\infty}(p^k) = (0)$, where (p) is a prime ideal in R as above.

Proof of Claim 1: Assume $\bigcap_{k=1}^{\infty}(p^k) \neq (0)$. Then there exists an element a such that $a \in (p^k)$ for all k. Hence, $a/p\ , a/p^2,\ \ldots$ are elements of R. Thus, we can form an ascending chain of ideals $(a/p) \subset (a/p^2) \subset \cdots \subset (a/p^n) \subset \ldots$ because inductively, we have $a/p^n = p(a/p^{n+1})$ for all positive integer n. However, R is Noetherian and this chain must stabilize for some m. Therefore, $(a/p^m) = (a/p^{m+1}) = \ldots$ which implies p is a unit contradicting (p) being a prime ideal. This proves the claim.

Therefore, for any $r \neq 0$ in R, there exists an integer $k \geq 0$ such that $r \in (p^k)$ but $r \notin (p^{k+1})$. Hence, $r = sp^k$ for some $s \notin (p)$. This s and k can be computed by ideal membership algorithm. Let $G = \{g_1, \ldots, g_r\}$ be a Gröbner basis for I. So, $lt(g_i) = s_i p^{k_i} x^{A_i}$ where $s_i \notin (p)$ as mentioned before. Thus, $Lt(I) = \langle s_i p^{k_i} x^{A_i} \mid 1 \leq i \leq r \rangle$.

Claim 2: $Lt(I)R_{(p)}[x] = \langle p^{k_i} x^{A_i} \mid 1 \leq i \leq r \rangle$ for the prime ideal (p) in R.

Proof of Claim 2: We have $R_{(p)} = S^{-1}R$ where $S = R - (p)$ and (p) is a prime ideal. If $s_i \notin (p)$ for all i, then $s_i \in S$ for all i where s_i is a factor in the leading coefficient of the above mentioned g_i. Since $Lt(I)$ is generated by $s_i p^{k_i} x^{A_i}$ in $R[x]$, so is its extension to $R_{(p)}[x]$. Thus, $Lt(I)R_{(p)}[x] = \langle s_i p^{k_i} x^{A_i} \mid 1 \leq i \leq r \rangle = \langle p^{k_i} x^{A_i} \mid 1 \leq i \leq r \rangle$ since s_i are units in $R_{(p)}$, this proves Claim 2.

Claim 3: $Lt(I)R_{(p)}[x] \cap R[x] = \langle p^{k_i} x^{A_i} \mid 1 \leq i \leq r \rangle$ in $R[x]$ for the prime ideal (p) in R.

Proof of Claim 3: Let $f \in \langle p^{k_i} x^{A_i} \mid 1 \leq i \leq r \rangle$, then $f = \sum_{i=1}^{r} h_i(x) p^{k_i} x^{A_i}$ where $h_i(x) \in R[x]$, hence $f \in R[x]$. Since $p^{k_i} x^{A_i} \in Lt(I)R_{(p)}[x]$, $f \in Lt(I)R_{(p)}[x] \cap R[x]$.

Conversely, if $f \in Lt(I)R_{(p)}[x] \cap R[x]$, then $f = \sum_{i=1}^{r}(f_i(x)/c_i)p^{k_i}x^{A_i}$ where $f_i(x) \in R[x]$ and $c_i \in R-(p)$. For $B \geq min\{A_i\}$, the term in x^B in the sum is $\sum_{i=1}^{s}(d_i/c_i)x^{B-A_i}p^{k_i}x^{A_i}$ where $(d_i/c_i)x^{B-A_i}$ is the term of f_i with degree $B-A_i$. Here, $d_i = 0$ if no such term exists. After equating the denominators, the coefficient of x^B is $\sum_{i=1}^{s}(D_i/C)p^{k_i} \in R_{(p)}$ where $C \in R-(p)$, $D_i \in R$. We have $\sum_{i=1}^{s}(D_i/C)p^{k_i} = \sum_{i=1}^{s}(D_ip^{k_i})/C$. Let $k = min_{D_i\neq 0}\{k_i\}$, then $\sum_{i=1}^{s} D_ip^{k_i} = rp^M$ where $r \notin (p)$ and $M \geq k$. Thus, $\sum_{i=1}^{s}(D_ip^{k_i})/C = (rp^M)/C \in R$ since $f \in Lt(I)R_{(p)}[x] \cap R[x]$. Let $(rp^M)/C = t \in R$, so $tC = rp^M$ where $C \notin (p)$ and (p) is prime. Thus, $p^M \mid t$, hence, $t \in (p)$. This implies $t = p^M\tilde{t}$ where $\tilde{t} = r/C \in R$. Therefore, $\sum_{i=1}^{s}(D_i/C)p^{k_i} = (rp^M)/C = \tilde{t}p^M$. Thus, the term in x^B is $\frac{rp^M}{C}x^B = \tilde{t}p^Mx^B = \tilde{t}p^{M-k_j}p^{k_j}x^{B-A_j}x^{A_j}$ where $k_j = min_{D_i\neq 0}\{k_i\}$ as above. If we arrange this term, we get $\tilde{t}p^{M-k_j}x^{B-A_j}p^{k_j}x^{A_j}$ where $\tilde{t} \in R$, $p^{M-k_j} \in R$ and $\tilde{t}p^{M-k_j}x^{B-A_j} \in R[x]$. Thus, the term in x^B is in the ideal $\langle p^{k_i}x^{A_i} \mid 1 \leq i \leq r\rangle$ in $R[x]$. Hence, adding up all these terms in x^B we get $f \in \langle p^{k_i}x^{A_i} \mid 1 \leq i \leq r\rangle$. This proves the claim.

For a similar result in $R_s[x]$, we need to find an $s \in R-(p)$ such that every s_i is invertible in $R_s[x]$. If we let $s = \prod s_i$ then s_i are invertible in R_s since $1/s_i = (s_1\cdots s_{i-1}s_{i+1}\cdots s_n)/s$. Hence, $Lt(I)R_s[x] = \langle s_ip^{k_i}x^{A_i} \mid 1 \leq i \leq r\rangle R_s[x] = \langle p^{k_i}x^{A_i} \mid 1 \leq i \leq r\rangle R_s[x]$. As in the proof of Claim 3, $\langle p^{k_i}x^{A_i} \mid 1 \leq i \leq r\rangle R_{(p)}[x] \cap R[x] = \langle p^{k_i}x^{A_i} \mid 1 \leq i \leq r\rangle$ which means $\langle p^{k_i}x^{A_i} \mid 1 \leq i \leq r\rangle$ is saturated in the ring extension $R_{(p)}[x]$. Since $s \in R-(p)$, we have the extensions $R[x] \subset R_s[x] \subset R_{(p)}[x]$ and $\langle p^{k_i}x^{A_i} \mid 1 \leq i \leq r\rangle$ is also saturated in the intermediate extension $R_s[x]$ (i.e. $\langle p^{k_i}x^{A_i} \mid 1 \leq i \leq r\rangle R_s[x] \cap R[x] = \langle p^{k_i}x^{A_i} \mid 1 \leq i \leq r\rangle$). This gives $Lt(I)R_s[x] \cap R[x] = \langle p^{k_i}x^{A_i} \mid 1 \leq i \leq r\rangle R_s[x] \cap R[x] = \langle p^{k_i}x^{A_i} \mid 1 \leq i \leq r\rangle$. Thus, we obtain

$$Lt(I)R_{(p)}[x] \cap R[x] = Lt(I)R_s[x] \cap R[x] = \langle p^{k_i}x^{A_i} \mid 1 \leq i \leq r\rangle.$$

Since $Lt(I)R_{(p)}[x] = S^{-1}Lt(I)$ where $S = R-(p)$, and $Lt(I)R_s[x] = T^{-1}Lt(I)$ for $T = \{s^k \mid k \geq 0\}$, we can use Corollary 3.2.10 to conclude that $IR_{(p)}[x] \cap R[x] = IR_s[x] \cap R[x]$ and $IR_{(p)}[x] \cap R[x]$ is computable by using Gröbner basis since $IR_s[x] \cap R[x]$ can be computed by Proposition 3.2.6. □

Corollary 3.2.12 (Corollary 3.8 in [13]). *Let R be an integral domain, K be the*

quotient field of R. Then for any given ideal $I \subset R[x]$, $IK[x] \cap R[x]$ can be computed.

Proof. If $p = 0$ in Proposition 3.2.11, then $R_{(0)}$ becomes the quotient field of R, hence the result follows. □

CHAPTER 4

ALGORITHMS FOR COMPUTING PRIMARY DECOMPOSITION USING GRÖBNER BASES

4.1 Primality Test

The Gröbner basis techniques for operations on ideals described in the previous chapter have an application to test whether an ideal $I \subset R[x]$ is prime or not. The algorithm relies on the following observations.

Lemma 4.1.1. *Let $I \subset R[x]$ be an ideal. I is prime if and only if $I \cap R$ is prime and the image of I in the canonical homomorphism from $R[x]$ to $(R/(I \cap R))[x]$ is prime.*

Proof. See [12], Ch.3, Theorem 11. □

Lemma 4.1.2. *Let R be an integral domain, K be the quotient field of R. If I is an ideal of $R[x]$ such that $I \cap R = (0)$, then I is prime if and only if $IK[x]$ is prime and $I = IK[x] \cap R[x]$.*

Proof. See [12], Ch. 4, Corollary 1 of Theorem 16. □

Before stating the crucial tool for primality test, we make some assumptions. We suppose we can decide whether an ideal is prime in the ring R. We also suppose we can test whether polynomials in one variable over fields of fractions of residue rings of $R[x]$ are irreducible (for example, if R is a prime field or $R = \mathbb{Z}$, then this condition holds).

Proposition 4.1.3 (Proposition 4.3 in [13])**.** *It is possible to decide whether an ideal in $R[x] = R[x_1, \ldots, x_n]$ is prime.*

Proof. We will use induction on the number of variables. For the base step, if the number of variables is zero, then we know that we can check if an ideal $I \subset R$ is prime in R by the assumptions on the ring R. Assume when the number of variables is less then n, we can test the primality of an ideal I. Suppose I is an ideal in $\tilde{R}[x_1] = R[x_2, \ldots, x_n][x_1]$ where $\tilde{R} = R[x_2, \ldots, x_n]$. I is prime in $R[x]$ if and only if I is prime in $\tilde{R}[x_1]$. Now, we need to check whether I is prime in $\tilde{R}[x_1]$. For this purpose, we apply Lemma 4.1.1 to $I \subset \tilde{R}[x_1]$ and first check the primality of $I \cap \tilde{R}$. We find a Gröbner basis G of I. Hence, by Proposition 3.2.1(ii), a Gröbner basis of $I \cap \tilde{R}$ can be found as $G \cap \tilde{R}$, where G is a Gröbner basis for I (using a *lex* order with x_1 as the largest variable). Now, $I \cap \tilde{R}$ is an ideal in $\tilde{R} = R[x_2, \ldots, x_n]$. Number of variables drops by one. By inductive hypothesis, we can decide if $I \cap \tilde{R}$ is prime or not in $\tilde{R}$. Hence, we recursively start the algorithm from the beginning for $I \cap \tilde{R}$ in $\tilde{R}$:

If $I \cap \tilde{R}$ is not prime in $\tilde{R}$, then I is not prime in $\tilde{R}[x_1]$ due to Lemma 4.1.1. If $I \cap \tilde{R}$ is prime in $\tilde{R}$, then we continue. We check if the image of I in $(\tilde{R}/(I \cap \tilde{R}))[x_1]$ is prime by Lemma 4.1.1. We introduce a new notation for practical purposes: $I' :=$ image of I in $(\tilde{R}/(I \cap \tilde{R}))[x_1]$ and $I^c := I \cap \tilde{R}$, hence $(\tilde{R}/(I \cap \tilde{R}))[x_1] = (\tilde{R}/I^c)[x_1]$ and $R' := \tilde{R}/I^c$.

With this notation, I' is an ideal in $R'[x_1]$. By the reason of our continuation, $I^c = I \cap \tilde{R}$ is prime in $\tilde{R}$. Thus, $R' = \tilde{R}/I^c$ is an integral domain. For future usage of Lemma 4.1.2, we need a claim.

Claim: $I' \cap R' = (0)$ in R'.

Proof of Claim: Let $\phi : \tilde{R}[x_1] \to (\tilde{R}/(I \cap \tilde{R}))[x_1]$ be the canonical homomorphism such that $\tilde{R} = R[x_2, \ldots, x_n]$. Hence, $y \in \phi(I) = I'$ if and only if $y = \phi(f) = \sum \tilde{a}_i x_1^i$ for some $f = \sum a_i x_1^i \in I$ where $a_i \in \tilde{R}$. So, $y \in I' \cap R' = \phi(I) \cap (\tilde{R}/(I \cap \tilde{R}))$ if and only if $\sum \tilde{a}_i x_1^i = \tilde{a}_0$ in $R' = \tilde{R}/(I \cap \tilde{R})$. Hence, $\tilde{a}_i = \tilde{0} \in \tilde{R}/(I \cap \tilde{R})$ for all $i \in \{1, \ldots, d\}$ where $d = deg(f)$. Thus, $a_1, \ldots, a_d \in I \cap \tilde{R} \subset I$. Therefore, $a_0 = f - a_1 x_1 - \cdots - a_d x_1^d \in I$. Since $a_0 \in \tilde{R}$, $a_0 \in I \cap \tilde{R}$. Thus, $y \equiv \tilde{0} \bmod (I \cap \tilde{R})$ which proves the claim.

Let $\phi : \tilde{R}[x_1] \to R'[x_1] = (\tilde{R}/(I \cap \tilde{R}))[x_1]$ be the canonical homomorphism. So, if $f = a_d x_1^d + a_{d-1} x_1^{d-1} + \cdots + a_1 x_1 + a_0$ then $\phi(f) = \tilde{a}_d x_1^d + \tilde{a}_{d-1} x_1^{d-1} + \cdots +$

$\tilde{a}_1 x_1 + \tilde{a}_0$ where $\phi(a_i) \equiv \tilde{a}_i$ in $\tilde{R}/(I \cap \tilde{R})$. (i.e. $\tilde{a}_i = a_i + (I \cap \tilde{R})$). Since we know the generators of I' in $R'[x_1]$ ($\phi(G)$ generates $\phi(I)$ for a Gröbner basis G of I by Proposition 3.2.7(i)), we can compute I'. Now, we can use Lemma 4.1.2 since R' is an integral domain, $I' \cap R' = (0)$ and I' is an ideal of $R'[x_1]$. We let K' be the quotient field of R'. So, I' is prime in $R'[x_1]$ if and only if the following two conditions are satisfied:

1. $I'K'[x_1]$ is a prime ideal in $K'[x_1]$.

2. $I'K'[x_1] \cap R'[x_1] = I'$.

For 1., we have $I' \subset R'[x_1]$ an ideal, so, let $I' = \langle \tilde{f}_1, \ldots, \tilde{f}_r \rangle$ in $R'[x_1]$, where $\tilde{f}_i = \phi(f_i)$ for ϕ given above where $\{f_i\}_{i=1}^r$ generates I in $\tilde{R}[x_1]$. $I'K'[x_1]$ is an extension ideal of I' in $K'[x_1]$, so it is generated by $\{\tilde{f}_i\}_{i=1}^r$, too. Since K' is a field, $K'[x_1]$ is a PID. Thus, $I'K'[x_1]$ is a principal ideal in $K'[x_1]$. Hence, $I'K'[x_1] = \langle F \rangle$ for some $F \in K'[x_1]$. So, $\langle \tilde{f}_1, \ldots, \tilde{f}_r \rangle = \langle F \rangle$. To find F in $K'[x_1]$, we either find GCD of $\tilde{f}_1, \ldots, \tilde{f}_r$ using Euclidean Algorithm or find a reduced Gröbner basis of $\langle \tilde{f}_1, \ldots, \tilde{f}_r \rangle$ in $K'[x_1]$. Therefore, this reduced Gröbner basis must consist of one element cF where c is a unit in K', $c \neq 0$. Now, $I'K'[x_1] = \langle F \rangle$ is a prime ideal in $K'[x_1]$ if and only if F is an irreducible polynomial in $K'[x_1]$. This is computable by our aforementioned assumption.

For 2., we check if $I'K'[x_1] \cap R'[x_1] = I' = \langle \tilde{f}_1, \ldots, \tilde{f}_r \rangle$. We use Corollary 3.2.12 to compute the generators of $I'K'[x_1] \cap R'[x_1]$ and we check if two ideals I' and $I'K'[x_1] \cap R'[x_1]$ are the same by Gröbner basis techniques (ideal membership algorithm). □

As a result of the previous proposition and its proof, we obtain the following algorithm for testing the primality of ideals.

Algorithm 4.1.4. PT(R; x; I). Primality Test

Input: Ring R; variables $x = x_1, \ldots, x_n$; ideal $I \subset R[x]$ (here, I is given means we know the generators of I).

Assumptions: We can test primality of ideals in R. We can test irreducibility of univariate polynomials over quotient fields of residue rings of $R[x]$.

Output: TRUE if I is prime, otherwise FALSE.

Step 1: If $n = 0$, then if $I \subset R$ is prime, then return TRUE, otherwise return FALSE (by using our assumptions on R, we know how to test the primality of $I \subset R$).

Step 2: Compute $J = I \cap R[x_2, \ldots, x_n]$ (by Proposition 3.2.1(ii)). Note that $J = I \cap \tilde{R}$ in the proof of Proposition 4.1.3.

Step 3: If $PT(R; x_2, \ldots, x_n; J) =$ FALSE then return FALSE. (By the inductive hypothesis, we can check whether J is prime. The number of variables is reduced by one, and the algorithm will stop when the number of variables drops to zero (Step 1)).

Step 4: Let $R' = R[x_2, \ldots, x_n]/J$ and $I' = IR'[x_1]$, $K' =$ the quotient field of R'.

Step 5: Compute $I'K'[x_1] = \langle f \rangle$ (since we are in a Euclidean domain, we apply Euclidean Algorithm to the generators of I' to find their GCD or we find a reduced Gröbner basis for I', since generators of I' also generate $I'K'[x_1]$ and $K'[x_1]$ is a PID).

Step 6: If f is not irreducible over K' (implying $I'K'[x_1]$ is not prime) then return FALSE (this irreducibility can be tested by assumptions). Else if f is irreducible, then go to Step 7.

Step 7: Compute $(I')^{ec} = I'K'[x_1] \cap R'[x_1]$ (by Corollary 3.2.12 and by using Gröbner bases).

Step 8: If $(I')^{ec} \subset I'$ then return TRUE, otherwise return FALSE. (By Proposition 3.2.12 we can find generators of $(I')^{ec}$ and we can test whether each generator is in I' or not by ideal membership algorithm and Gröbner basis. Since obviously $I' \subset (I')^{ec}$, $(I')^{ec} \subset I'$ implies $(I')^{ec} = I'$ and if this is true, I' is prime by Lemma 4.1.2 which implies primality of I.

4.2 Zero-dimensional Ideals

In this section, we investigate the properties of ideals that have Krull dimension zero. We introduce Gröbner basis techniques to characterize zero-dimensional ideals.

Definition 4.2.1. *Let R be a commutative ring which is not trivial ($0_R \neq 1_R$). Krull dimension of R is the maximal length l of a chain of prime ideals of R such as $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_l$ (see [2] p.827).*

Definition 4.2.2. *Krull dimension of an ideal I of a nontrivial commutative ring R is the Krull dimension of R/I, that is, maximum length of ideal chains $I \subset P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_l$ where P_i are prime ideals of R for all i.*

Definition 4.2.3. *If R is as above and I is an ideal of R, then I is zero-dimensional if there exists no prime ideal P such that $I \subset P \subsetneq M$ where M is any maximal ideal containing I.*

Zero-dimensional ideals have very interesting properties. Computing their primary decomposition is possible under a few extra conditions. Here we show that if specific conditions are satisfied, then we can determine whether an ideal is zero-dimensional by examining its Gröbner basis.

Lemma 4.2.4 (Lemma 5.1 in [13])**.** *Let $I \subset R[x]$ be an ideal such that $I \cap R$ is zero-dimensional. Then I is zero-dimensional if and only if $R[x]/I$ is integral over R.*

Proof. Let $R[x]/I$ be integral over R. So, it is integral over the subring $R/(I \cap R) \subset R[x]/I$ since if $f(a + I) = 0$ in $R[x]/I$ for $a \in R[x]$ and a monic polynomial $f(x_1) \in R[x_1]$, then $f(a) \in I$ and if we let $\bar{f}(x_1) = \sum \bar{c}_i x_1^i$ where $\bar{c}_i = c_i + (I \cap R)$ and $f(x_1) = \sum c_i x_1^i$, we get $\bar{f}(a + I) = f(a) + I = 0 + I$ in $R[x]/I$. Note that $\bar{f}(x_1) \in R/(I \cap R)[x_1]$ is also monic. By Corollary A.4.2 in [17], pg. 291, $R/(I \cap R)$ and $R[x]/I$ have the same dimension since this is an integral extension. By assumption, $I \cap R$ is zero-dimensional in R, hence this implies I is zero-dimensional in $R[x]$.

For the converse, assume that I is zero-dimensional in $R[x]$. Let $I = \bigcap_{k=1}^{m} Q_k$ be a primary decomposition of I. Let $M_k = \sqrt{Q_k}$. Since I is zero-dimensional and $I \subset \sqrt{I} = \bigcap M_k \subset M_k$ where each M_k is prime (an associated prime of I), we obtain M_k is maximal in $R[x]$ (the only prime ideals which can contain a zero-dimensional ideal are maximal ideals). Therefore, $M_k \cap R$ is prime in R (note that $M_k \cap R \neq R$, otherwise $1 \in M_k$ contradicting M_k being maximal). We have, $I \cap R \subset M_k \cap R$ where

$I \cap R$ is zero-dimensional and $M_k \cap R$ is prime, which again implies that $M_k \cap R$ is maximal in R. Now, the field $R[x]/M_k$ is a finite algebraic extension of the field $R/(M_k \cap R)$ by Hilbert's Nullstellensatz. (See Corollary 7.10 in [10], pg.82). Hence, for any $h \in R[x]$, we have $h + M_k \in R[x]/M_k$ is algebraic over $R/(M_k \cap R)$. The minimal polynomial of $h + M_k$ is $\bar{f}_k(x_1) = \sum \bar{c}_i x_1^i$ where $f_k(x_1) = \sum c_i x_1^i \in R[x_1]$ and $\bar{c}_i = c_i + (M_k \cap R)$. Here, f_k is monic and $\bar{f}_k(h + M_k) = 0 + M_k = f_k(h) + M_k$ implies $f_k(h) \in M_k$. Since $M_k = \sqrt{Q_k}$, we have $(f_k(h))^N \in Q_k$ for some $N > 0$ for all k. Thus, $F(h) = \prod_k (f_k(h))^N \in \bigcap Q_k = I$ which implies $R[x]/I$ is integral over R. (i.e. this product being in I is an expression of integral dependence for h mod I. $F(h + I) = F(h) + I = 0 + I$ in $R[x)/I$ and F is monic). □

Proposition 4.2.5 (Proposition 5.2 in [13]). *$R[x]/I$ is integral over R if and only if $(x_1, \ldots, x_n) \subset \sqrt{Lt(I)}$.*

Proof. Let $R[x]/I$ be integral over R. Hence, for each i, there exists a monic polynomial $f(y_1) \in R[y_1]$ such that $f(x_i + I) = f(x_i) + I = 0 + I$ in $R[x]/I$ which means $f(x_i) \in I$. Thus, $lt(f(x_i)) \in Lt(I)$, but $lt(f(x_i))$ is a power of x_i, hence $x_i \in \sqrt{Lt(I)}$. For the converse statement, by Proposition 5.1 in [10], pg.59, if we can show $R[x]/I$ is finitely generated as an R-module, then we can conclude that it is integral over R. Assuming $(x_1, \ldots, x_n) \subset \sqrt{Lt(I)}$, let $x_i^{m_i} \in Lt(I)$. Consider the finitely generated R-module $K = \sum_{a_i < m_i} R x_1^{a_1} \cdots x_n^{a_n}$. If we show that the R-module homomorphism $\phi : K \to R[x]/I$ is surjective, then since K is a finitely generated R-module, $R[x]/I$ is a finitely generated R-module, too. Note that, here $\phi(h) = h + I$ for $h \in K$. Let $f \in R[x]$, consider $f + I \in R[x]/I$. We will prove that ϕ is surjective by induction on the degree of f. If $deg(f) = 0$ then $f = c \in R$ and $f + I = \phi(c)$ since $c \in K$. Assume $g + I$ is in the image of ϕ for all g such that $deg(g) < deg(f)$. We can assume $f \notin I$ (if $f \in I$, then $f + I = 0 + I = \phi(0)$ and $f + I$ is in the image). By reduction algorithm (Proposition 3.1.6), there exists $f' \in R[x]$ such that $f' \equiv f$ mod I and $lt(f') \notin Lt(I)$. Thus, $lt(f') \notin (x_1^{m_1}, \ldots, x_n^{m_n}) \subset Lt(I)$. Therefore, $lt(f') \in K$. Moreover, since $f - f' \in I$ and $lt(f') \notin Lt(I)$, we have $lt(f - f') \neq lt(f')$. Hence, $deg(f') \leq deg(f)$. This implies, $deg(f' - lt(f')) < deg(f') \leq deg(f)$. By the inductive hypothesis, $(f' - lt(f')) + I = \phi(h)$ for some $h \in K$. Therefore, $\phi(lt(f') + h) = \phi(lt(f')) + \phi(h) = lt(f') + I + (f' - lt(f')) + I = f' + I = f + I$.

Hence, $f + I$ is in the image of ϕ. $\square$

Corollary 4.2.6 (Corollary 5.3 in [13])**.** *By using Gröbner basis, it is possible to decide whether $R[x]/I$ is integral over R or not. If $R[x]/I$ is not integral over R, then it is possible to find an i such that $x_i + I$ is not integral over R.*

Proof. Let G be a Gröbner basis for the ideal I and let $G_i = \{g \in G \mid lt(g) = cx_i^m \text{ for some } c \in R,\ m \geq 0\}$. Let $L_i \subset R$ be the ideal generated by the leading coefficients of elements of G_i.

Claim 1: $Lt(G_i) = Lt(G) \cap R[x_i]$ where G and G_i are as above and $Lt(G_i)$ is considered as an ideal in $R[x_i]$.

Proof of Claim 1:($\subset$) : If $a \in Lt(G_i)$, then $a = \sum_j h_j lt(g_j)$ where $h_j \in R[x_i]$, and $g_j \in G_i$, so $g_j \in G$. Hence, $a \in Lt(G)$, also $a \in R[x_i]$, too.

($\supset$) : If $b \in Lt(G) \cap R[x_i]$, then $b = \sum_j h_j lt(g_j)$ where $g_j \in G$, $h_j \in R[x]$. For $g_j \in G_i$ let $h_j = \bar{h}_j + \tilde{h}_j$ where $\tilde{h}_j \in R[x_i]$ is the sum of the terms of h_j involving only the variable x_i. Then

$$b = \sum_{g_j \notin G_i} h_j lt(g_j) + \sum_{g_j \in G_i} \bar{h}_j lt(g_j) + \sum_{g_j \in G_i} \tilde{h}_j lt(g_j).$$

Since each term in the first two sums contains variables other than x_i and $b \in R[x_i]$, the first two sums add up to zero. Hence $b = \sum_{g_j \in G_i} \tilde{h}_j lt(g_j) \in Lt(G_i)$. This proves Claim 1.

Claim 2: $x_i \in \sqrt{Lt(I)}$ if and only if $L_i = (1)$ where L_i is as given above.

Proof of Claim 2: If $x_i \in \sqrt{Lt(I)}$, then $x_i^M \in Lt(I) \cap R[x_i]$ for some $M > 0$.Hence, $x_i^M \in Lt(G_i)$ by Claim 1. Thus, $x_i^M = \sum_j h_j lt(g_j)$ where $h_j \in R[x_i]$ and $g_j \in G_i$. Let $lt(g_j) = c_j x_i^{m_j}$, so $L_i = \langle c_1, \ldots, c_k \rangle$. Thus, $1 = \sum_j r_j c_j$ where $r_j =$ *coefficient of* $x_i^{M-m_j}$ in h_j. Hence, $1 \in \langle c_j \rangle$ which implies $L_i = (1)$. Conversely, if $L_i = (1)$, then $\sum_j c_j r_j = 1$ where $r_j \in R$. Let $N = max\{m_i\}$, then $x_i^N \sum_j c_j r_j = x_i^N = \sum_j c_j x_i^{m_j} r_j x_i^{N-m_j} = \sum_j lt(g_j) r_j x_i^{N-m_j} \in Lt(G_i) \subset Lt(I)$ which implies $x_i \in \sqrt{Lt(I)}$. This proves the claim.

By Proposition 4.2.5 $R[x]/I$ is integral over R if and only if each x_i is in $\sqrt{Lt(I)}$ which is equivalent to $L_i = (1)$ in R. If I is given, we can compute a Gröbner basis

G of I. Thus, we can compute G_i and L_i for each i. Then we can check whether $L_i = (1)$ or not. Hence, this way, we can decide whether $R[x]/I$ is integral over R or not.

Now, if $x_i \notin \sqrt{Lt(I)} = \sqrt{Lt(G)}$ (i.e. if $L_i \neq (1)$), then $x_i + I$ is not integral over R. Hence, the result follows. □

Corollary 4.2.7 (Corollary 5.4 in [13]). *If $I \cap R$ is zero-dimensional, then it is possible to determine whether I is zero-dimensional or not. If I is not zero-dimensional, then it is possible to find an i such that $I \cap R[x_i]$ is not zero-dimensional.*

Proof. By Lemma 4.2.4 if $I \cap R$ is zero-dimensional, then I is zero-dimensional if and only if $R[x]/I$ is integral over R. By Proposition 4.2.5, $R[x]/I$ is integral over R if and only if $(x_1, \ldots, x_n) \in \sqrt{Lt(I)}$. Hence, if $x_i \notin \sqrt{Lt(I)}$, then $x_i + I \in R[x]/I$ is not integral over R, and thus I is not zero-dimensional. Here, we can determine whether x_i is in $\sqrt{Lt(I)}$ or not by using Gröbner bases due to the Corollary 4.2.6. Hence, we can decide the zero-dimensionality of I. Now, if I is not zero-dimensional, then by Corollary 4.2.6, we can find an i such that $x_i + I$ is not integral over R. Thus, $x_i + (I \cap R[x_i]) \in R[x_i]/(I \cap R[x_i])$ is not integral over R and hence $I \cap R[x_i]$ is not zero-dimensional by Lemma 4.2.4. (If there exists a monic $f(y_1) \in R[y_1]$ such that $f(x_i + (I \cap R[x_i])) = 0 + I \cap R[x_i]$, then $f(x_i) \in R[x_i]$, hence $f(x_i + I) = f(x_i) + I = 0 + I$ in $R[x]/I$, contradicting $x_i + I$ is not integral over R). □

Proposition 4.2.8 (Proposition 5.5 in [13]). *Let $I \subset R[x]$ be an ideal, let $I \cap R$ be primary and zero-dimensional. Let G be a Gröbner basis for I. Then I is zero-dimensional if and only if for each i, there exists a $g_i \in G$ such that $lt(g_i) = c_i x_i^{m_i}$ where $c_i \in R$ is a unit modulo $I \cap R$.*

Proof. For a given Gröbner basis G of I, let us define $G_i = \{g \in G \mid lt(g) = cx_i^m \text{ for some } c \in R,\ m \geq 0\}$. Let $L_i \subset R$ be the ideal generated by the leading coefficients of elements of G_i. Since the polynomial ring $R[x]$ is over a commutative ring R here, G can contain some constants. Thus, $G \cap R \subset G_i$. Also, definition of L_i implies $I \cap R \subset L_i$. Since $G \cap R$ generates $I \cap R$ and $G \cap R \subset L_i$. If $I \cap R$ is zero-dimensional and primary, then there exists a unique maximal ideal containing $I \cap R$. This is so, because if we let $I \cap R \subset M$ (every proper ideal is contained in a

maximal ideal), then $\sqrt{I \cap R} \subset \sqrt{M} = M$ (since maximal ideals are radical). Also, since $I \cap R$ is zero-dimensional, $I \cap R \subset \sqrt{I \cap R} \subset M$ implies $M = \sqrt{I \cap R}$ (since $I \cap R$ is primary, $\sqrt{I \cap R}$ is prime). Therefore, $M = \sqrt{I \cap R}$ is unique.

Claim: $L_i \neq (1)$ *if and only if* $L_i \subset \sqrt{I \cap R}$ *where* L_i *is as above.*

Proof of Claim: If $L_i \subset \sqrt{I \cap R}$ and $L_i = (1)$, then $L_i = R$ which contradicts $L_i \subset \sqrt{I \cap R}$, since $\sqrt{I \cap R}$ is a maximal ideal, hence a proper ideal. Conversely, if we assume $L_i \neq (1)$, then there exists a maximal ideal, say M, such that $I \cap R \subset L_i \subset M$. By the part before this claim, we have $M = \sqrt{I \cap R}$; hence, this proves the claim.

Therefore, I is zero-dimensional if and only if $L_i = (1)$ for all i, if and only if $L_i \not\subset \sqrt{I \cap R}$ if and only if there exists a $g_i \in G_i$ such that $lc(g_i) = c_i \notin \sqrt{I \cap R}$ where $(c_i, \sqrt{I \cap R}) = (1)$ since $\sqrt{I \cap R}$ is a maximal ideal. To prove that c_i is a unit modulo $I \cap R$, we have $1 = c_i r + a$ where $a \in \sqrt{I \cap R}$, $r \in R$. Thus, $a^M \in I \cap R$. Also, we have $(c_i r + a)^M = 1$, too. Hence $c_i K + a^M = 1$ after binomial expansion. Since $a^M \in I \cap R$, $a^M \equiv 0$ modulo $I \cap R$, thus we get c_i is a unit modulo $I \cap R$. This gives $(1) = (c_i, I \cap R)$. □

Remark: Using the notation and assumptions as in Proposition 4.2.8, the elements of I whose leading terms are divisible by $x_i^{m_i}$ are reducible modulo $\{g_i\} \cup (G \cap R)$ where $lt(g_i) = c_i x_i^{m_i}$. This is so, because $(1) = (lc(g_i), I \cap R)$ implies $1 = r \cdot lc(g_i) + h$ where $h \in I \cap R$. Hence $x_i^{m_i} = r \cdot lc(g_i) x_i^{m_i} + h x_i^{m_i}$. If G is a minimal Gröbner basis, then by definition of minimal Gröbner basis, all elements of G_i except for g_i have degree in x_i that is less than m_i (otherwise, if there is a $g \neq g_i$ in G_i such that $deg(g) \geq m_i$, then by the above argument, g is reducible modulo $\{g_i\} \cup (G \cap R) \subset G - \{g\}$ which contradicts minimality of G). Therefore, using a minimal Gröbner basis to determine whether I is zero-dimensional, it suffices to check that there exists only one element of maximal degree in G_i and this element's leading coefficient generates R together with $G \cap R$. On the other hand, if I is zero-dimensional and G is a minimal Gröbner basis of I, then g_i can be identified as the unique element of G_i with the maximum degree and necessarily $lc(g_i)$ is a unit modulo $I \cap R$.

In what follows, we try to understand the nature of zero-dimensional primary ideals.

Here, a polynomial satisfies a property modulo an ideal I in R means, that polynomial's image as a polynomial over R/I satisfies that property. We begin with the following lemmas about polynomials in one variable.

Lemma 4.2.9 (Lemma 5.6 in [13]). *Let $I \subset R[x_1]$ be an ideal such that $I \cap R$ is zero-dimensional. Assume $x_1^m \in Lt(I)$ and $x_1^{m-1} \notin Lt(I)$. Then every $f \in I$ with $deg(f) < m$ is a zero divisor or zero modulo $I \cap R$.*

Proof. If $L \subset R$ is the ideal generated by the leading coefficients of elements of I whose degrees are less than m, then we have the following claim.

Claim: If $f \in I$ has degree less than m, then $f \equiv 0$ modulo L, where L is as above.

Proof of Claim: Let $f = c_1x_1^{m-1} + c_2x_1^{m-2} + \cdots + c_m$. Hence, either $c_1 = 0$ or $c_1 \in L$. By the assumption of the lemma, there exists a $g \in I$ such that $lt(g) = x_1^m$, so let $g = x_1^m + d_1x_1^{m-1} + \cdots + d_m$. If we also let $f' = x_1f - c_1g$, then we get the following equalities.

$$\begin{aligned}
f' &= x_1f - c_1g \\
&= x_1(c_1x_1^{m-1} + c_2x_1^{m-2} + \cdots + c_m) - c_1g \\
&= c_1x_1^m + c_2x_1^{m-1} + \cdots + c_mx_1 - c_1(x_1^m + d_1x_1^{m-1} + \cdots + d_m) \\
&= c_1x_1^m + c_2x_1^{m-1} + \cdots + c_mx_1 - c_1x_1^m - c_1d_1x_1^{m-1} - \cdots - c_1d_m \\
&= (c_2 - c_1d_1)x_1^{m-1} + (c_3 - c_1d_2)x_1^{m-2} + \cdots + (c_m - c_1d_{m-1})x_1 - c_1d_m
\end{aligned}$$

Therefore, $f' \in I$ and if we let $f' = c_1'x_1^{m-1} + c_2'x_2^{m-2} + \cdots + c_m'$, then $c_1' = (c_2 - c_1d_1)$. Since $c_1d_1 \in L$, we get $c_1' \equiv c_2 \; modL$. We have $c_1' \in L$, because $f' \in I$ and $deg(f') < m$. Thus, $c_2 \in L$. By the same argument, we get $c_2' \in L$, too. Hence, this implies $c_3 \in L$ since $c_2' \equiv c_3 \; modL$. Continuing this way results in $c_i \in L$ for all i. Therefore, $f \equiv 0 \; modL$ which proves the claim.

Now, if $L = (1)$, then I contains a monic polynomial of degree less than m, since if $1 = \sum r_jc_j$ where $c_j = lc(h_j)$ and $d_j = deg(h_j) < m$, then for $d = max\{d_j\}$ we get $h = \sum r_jx_1^{d-d_j}h_j$ which has leading term x_1^d, so $deg(h) = d < m$. This contradicts the assumption that $x_1^m \in Lt(I)$ and $x_1^{m-1} \notin Lt(I)$. Hence, L is a proper ideal of R. Let $L \subset M$ where M is a maximal ideal of R. We also have $I \cap R \subset L$ by definition of L. We have $I \cap R \subset L \subseteq M$. Since $I \cap R$ is zero-dimensional,

$I \cap R = \bigcap Q_i$ (primary decomposition of $I \cap R$) and $\sqrt{Q_i} = M_i$ where M_i are maximal ideals. $I \cap R \subset M$ implies $\sqrt{I \cap R} = \bigcap M_i \subset \sqrt{M} = M$, and $\bigcap M_i \subset M$ implies $M_i \subset M$ for some i since M_i are maximal, hence prime (if intersection of prime ideals is a subset of another prime ideal P, then one of these prime ideals is a subset of P). Since M_i and M are both maximal ideals, $M_i \subset M$ gives $M_i = M$. Thus, we have $I \cap R \subset L \subset M_i$. Since M_i is an associated prime of $I \cap R$, we have $M_i = (I \cap R : a)$ for some $a \notin I \cap R$ (see Proposition 7.17 in [10], pg.83) , then $aM \subset I \cap R$ which implies $aL \subset I \cap R$, since $L \subset M$. Hence, there exists an $a \notin I \cap R$ so that $aL \subset I \cap R$. Therefore, $af \equiv 0 \; mod(I \cap R)$ if $deg(f) < m$ by the help of the above claim. This shows f is a zero divisor or zero $mod(I \cap R)$. □

Lemma 4.2.10 (Lemma 5.7 in [13])**.** *Let $I \subset R[x_1]$ be a zero-dimensional ideal and $I \cap R$ be zero-dimensional, primary. Let G be a minimal Gröbner basis for I and let $g_1 \in G$ be such that $lt(g_1) = c_1 x_1^{m_1}$ where $c_1 \in R$ is a unit $mod(I \cap R)$ as in Proposition 4.2.8. In this case, $\sqrt{I} = \sqrt{(g_1, I \cap R)}$.*

Proof. For $g_1 \in G$, if $lt(g_1) = c_1 x_1^{m_1}$ and $c_1 \in R$ is a unit $mod(I \cap R)$, then we have $x_1^{m_1} \in Lt(g_1, I \cap R) \subset Lt(I)$ since $(1) = (g_1, I \cap R)$. Here, $Lt(I)$ contains no smaller power of x_1, since G is a minimal Gröbner basis (otherwise if for $m < m_1$, we have x_1^m is reducible modulo $G - \{g_1\}$, then this implies g_1 is reducible modulo $G - \{g_1\}$, contradicting the minimality of G). Therefore, by Lemma 4.2.9, every $f \in I$ whose degree is less than m_1 is a zero divisor or zero modulo $I \cap R$.

Claim 1: If $I \cap R$ is primary, then the set of zero divisors and zero $mod(I \cap R)$ in R is $\sqrt{I \cap R}$.

Proof of Claim 1: Let a be a zero divisor modulo $I \cap R$ in R, then $ab \equiv 0 \; mod(I \cap R)$ for some $b \not\equiv 0 \; mod(I \cap R)$ in R. That is, $ab \in I \cap R$ and $b \notin I \cap R$. Since $I \cap R$ is primary, by definition of primary ideals, we get $a \in \sqrt{I \cap R}$. Conversely, if $a^k \in I \cap R$, but $a^{k-1} \notin I \cap R$, then $aa^{k-1} \equiv 0 \; mod(I \cap R)$ implies a is a zero divisor or zero modulo $I \cap R$. This proves the claim.

If $f \in I$ and $deg(f) < m_1$, then the proof of Lemma 4.2.9 implies $af \equiv 0 \; mod(I \cap R)$ for some $a \in R$, i.e. all coefficients of f are zero divisors or zero modulo $I \cap R$. Hence, they are in $\sqrt{I \cap R}$. Now, let $F \in I$. So, by Proposition 3.1.6, we have $F \equiv$

$F'\ mod(g_1, \sqrt{I \cap R})$ where F' is reduced $mod(g_1, \sqrt{I \cap R})$. Moreover, $deg(F') < m_1$, because $x_1^{m_1} \in Lt(g_1, I \cap R)$. Therefore, $F' \equiv 0\ mod(\sqrt{I \cap R})$. Hence, $F \in ((g_1, I \cap R) + (\sqrt{I \cap R})R[x_1]) = (g_1, \sqrt{I \cap R})$. Therefore, $I \subset (g_1, \sqrt{I \cap R}) \subset \sqrt{I}$. If we take the radicals, $\sqrt{I} \subset \sqrt{(g_1, \sqrt{I \cap R})} \subset \sqrt{\sqrt{I}}$. Since $\sqrt{\sqrt{I}} = \sqrt{I}$, we have $\sqrt{I} = \sqrt{(g_1, \sqrt{I \cap R})}$.

Claim 2: $\sqrt{(g_1, \sqrt{I \cap R})} = \sqrt{(g_1, I \cap R)}$.

Proof of Claim 2: Since $\sqrt{I \cap R} \supset I \cap R$, we have $LHS \supseteq RHS$. Conversely, if $f \in \sqrt{(g_1, \sqrt{I \cap R})}$, then $f^k \in (g_1, \sqrt{I \cap R})$. Hence, $f^k = g_1 f_1 + h$ where $f_1 \in R[x_1]$, $h \in \sqrt{I \cap R}$. Thus, $h^s \in I \cap R$ for some $s > 0$. Taking s-th power of both sides, we have $(f^k)^s = (g_1 f_1 + h)^s$. Using binomial formula, we get $(f^k)^s = (g_1 f_1)^s + s(g_1 f_1)^{s-1} h + \cdots + h^s = g_1 F + h^s$ where $g_1 F + h^s \in (g_1, I \cap R)$. Hence, $f^{ks} \in (g_1, I \cap R)$ which implies $f \in \sqrt{(g_1, I \cap R)}$ and that proves the claim.

As a result, we get $\sqrt{I} = \sqrt{(g_1, \sqrt{I \cap R})} = \sqrt{(g_1, I \cap R)}$. □

Now, it is possible for us to describe the zero-dimensional primary ideals by using computable conditions on their Gröbner bases.

Proposition 4.2.11 (Proposition 5.8 in [13])**.** *Let $I \subset R[x]$ be a zero-dimensional ideal, $I \cap R$ be zero-dimensional and primary. Let G be a minimal Gröbner basis for I with respect to the lexicographical order such that $x_1 > x_2 > \cdots > x_n$ and let $g_1, \ldots, g_n \in G$ so that $lt(g_i) = c_i x_i^{m_i}$ where $c_i \in R$ is a unit $mod(I \cap R)$ for all $i \in \{1, \ldots, n\}$ (note that such g_i exists by Proposition 4.2.8). In this case, I is primary if and only if for all i, g_i is a power of an irreducible polynomial modulo $\sqrt{I \cap R[x_{i+1}, \ldots, x_n]}$. If this is the case, then for every $h \in G \cap R[x_i, \ldots, x_n] - \{g_i\}$, $h \equiv 0\ mod(\sqrt{I \cap R[x_{i+1}, \ldots, x_n]})$.*

Proof. We use induction on the number of variables n. Let $n = 0$, then $I \cap R = I$ is zero-dimensional and primary by assumption. Now, assume that the statement holds for $n-1$ variables. For the ideal $I \subset R[x_1, x_2, \ldots, x_n]$ satisfying the conditions of the statement, let $R' = R[x_2, \ldots, x_n]$, $I' = I \cap R'$. Then we can show that the conditions of the statement hold for the ideal $I' \subset R[x_2, \ldots, x_n]$ and $g_2, \ldots, g_n \in G' = G \cap R'$ (which is a minimal Gröbner basis of I') as follows. We have $I' \cap R = I \cap R' \cap R =$

$I \cap R$ is zero-dimensional and primary. Also, we need to show I' is zero-dimensional.

Claim 1: I is zero-dimensional implies $I \cap R' = I'$ is zero-dimensional.

Proof of Claim 1: Let I be zero-dimensional. Let G be a Gröbner basis for I in the lexicographical order $x_1 > \cdots > x_n$. So, by Proposition 4.2.8, for each i, there exists a $g_i \in G$ such that $lt(g_i) = c_i x_i^{m_i}$ where c_i is a unit $mod(I \cap R)$. Since $G' = G \cap R'$ is a minimal Gröbner basis of $I' = I \cap R'$, for each $i \in \{2, \ldots, n\}$, $g_i \in G \cap R'$, $lt(g_i) = c_i x_i^{m_i}$ where c_i is a unit $mod(I' \cap R)$ (since $I' \cap R = I \cap R$) implies $I \cap R' = I'$ is zero-dimensional by Proposition 4.2.8 and this proves the claim.

As a result, the statement holds for the ideal I' in the polynomial ring R' with $n-1$ variables. Therefore, it suffices to prove that I is primary if and only if I' is primary and g_1 is a power of an irreducible polynomial modulo $\sqrt{I'}$. To complete the proof, we also need to show that, in this case, for every $h \in G - \{g_1\}$, $h \equiv 0 \ mod(\sqrt{I'})$. (If I is primary then I' is primary by Claim 2 below and since the statement holds for I', g_i is a power of an irreducible polynomial $mod(\sqrt{I \cap R[x_{i+1}, \ldots, x_n]})$ for $i \in \{2, \ldots, n\}$. Hence, it remains to show that this holds for $i = 1$. For the converse, if I' is primary, and g_1 is a power of an irreducible modulo $\sqrt{I'}$, then each g_i is a power of an irreducible modulo $\sqrt{I \cap R[x_{i+1}, \ldots, x_n]}$ for $i \in \{1, \ldots, n\}$.)

Claim 2: I is primary implies I' is primary.

Proof of Claim 2: Let I be primary, and assume $ab \in I' = I \cap R'$ for some $a, b \in R'$, then $ab \in I$, thus $a \in I$ or $b^k \in I$ for some $k > 0$ (since I is primary). Also, we have $a, b \in R'$ which implies $a \in I \cap R'$ or $b^k \in I \cap R'$. Hence, $I' = I \cap R'$ is primary proving the claim.

Now, assume $I' = I \cap R'$ is primary. Let $lt(g_1) = c_1 x_1^{m_1}$. If $h \in G \cap R[x_1] - \{g_1\}$, then $deg(h) < m_1$ in x_1. Otherwise, h would be reducible $mod(g_1, G \cap R)$ by the remark after Proposition 4.2.8 and this contradicts the minimality of G. Thus, by proof of Lemma 4.2.9 and its notation, there exists an $a \notin I \cap R'$ such that $aL \subset I \cap R'$. Hence, $ah \equiv 0 \ mod(I')$, i.e. $ac_j \in I'$ where c_j's are coefficients of h. Since I' is primary and $a \notin I'$, then $c_j^k \in I'$. Thus, $c_j \in \sqrt{I'}$, i.e. $h \equiv 0 \ mod(\sqrt{I'})$. This proves the second part of the proposition.(The condition holds for g_i where $i \in \{2, \ldots, n\}$, since by induction the statement holds for I' and I' is primary.)

Claim 3: Let I be zero-dimensional. Then I is primary if and only if $\sqrt{I}$ is prime.

Proof of Claim 3: Let I be primary, and let $ab \in \sqrt{I}$ for $a, b \in R[x_1, \ldots, x_n]$. Thus, $(ab)^k \in I$ for some $k > 0$. Hence, $(ab)^k = a^k b^k \in I$. Since I is primary, $a^k \in I$ or $(b^k)^t \in I$ for some $t > 0$. This implies $a \in \sqrt{I}$ or $b \in \sqrt{I}$. Conversely, let $\sqrt{I}$ be prime, let I be zero-dimensional. So, let $I = \bigcap_{i=1}^{s} Q_i$ be an irredundant primary decomposition of I. Hence, $\sqrt{I} = \bigcap_{i=1}^{s} \sqrt{Q_i}$ where $\sqrt{I}$ is prime. Since I is zero-dimensional, $\sqrt{Q_i}$ is maximal. Now, if $P = \bigcap_{i=1}^{k} P_i$ where P and P_i are prime ideals, then $P = P_i$ for some i. (See, Proposition 1.11 in [10], pg.8). Since maximal ideals are prime, we have $\sqrt{I} = \sqrt{Q_j}$ for some j. Let $\sqrt{Q_i} = M_i$ where M_i is maximal. Thus, $\sqrt{I} = M_j$ for some j. Therefore, $M_j \subset M_i$ for $i \neq j$. However, since M_i's are maximal, this implies $M_i = M_j$ for all i, j. Hence, there is only one maximal ideal which implies there is only one associated prime. Therefore, $I = Q_j$ where Q_j is primary. This proves the claim.

By Lemma 4.2.10 and its proof, we have $\sqrt{I} = \sqrt{(g_1, I')} = \sqrt{(g_1, \sqrt{I'})}$. Thus, we can use Claim 3, since I is given to be zero-dimensional. We have I is primary if and only if $\sqrt{I}$ is prime if and only if $\sqrt{(g_1, \sqrt{I'})}$ is prime if and only if $(g_1, \sqrt{I'})$ is primary (since $\sqrt{I} = \sqrt{(g_1, \sqrt{I'})}$ and I is zero-dimensional, we get $J = (g_1, \sqrt{I'})$ is also zero-dimensional and we apply Claim 3 for the ideal J).

Claim 4: $(g_1, \sqrt{I'})$ is primary if and only if the ideal generated by g_1 in $(R'/\sqrt{I'})[x_1]$ is primary.

Proof of Claim 4: Let $\phi : R'[x_1] \to (R'/\sqrt{I'})[x_1]$ be the canonical homomorphism. Since ϕ is an epimorphism and $\ker \phi = (\sqrt{I'})R'[x_1] \subset (g_1, \sqrt{I'})$, by using the definition of being primary, we can easily show that $\phi((g_1, \sqrt{I'})) = (\phi(g_1))$ is primary if and only if $(g_1, \sqrt{I'})$ is primary. This proves the claim.

Using the above claims, we complete the proof as follows. What remains to be shown is that I is primary if and only if I' is primary and g_1 is a power of an irreducible polynomial modulo $\sqrt{I'}$. Assume first that I is primary. Then by Claim 2, I' is primary. Since I' is zero-dimensional (by Claim 1) and primary, $\sqrt{I'}$ is prime by Claim 3. Indeed, $\sqrt{I'}$ is maximal since I' is zero-dimensional. Hence, $R'/\sqrt{I'}$ is a field. Therefore, $(R'/\sqrt{I'})[x_1]$ is a PID. By Claim 4 and its preceding paragraph, we

have I is primary if and only if $(g_1, \sqrt{I'})$ is primary if and only if the ideal generated by g_1 in $(R'/\sqrt{I'})[x_1]$ is primary. Since $(R'/\sqrt{I'})[x_1]$ is a PID, the ideal generated by g_1 in $(R'/\sqrt{I'})[x_1]$ is primary if and only if it is a power of an irreducible polynomial in $(R'/\sqrt{I'})[x_1]$.

Conversely, assume that I' is primary and g_1 is a power of an irreducible polynomial modulo $\sqrt{I'}$, i.e., g_1 is a power of an irreducible polynomial in $(R'/\sqrt{I'})[x_1]$. Since $\sqrt{I'}$ is maximal (I' is one dimensional by Claim 1 and primary by assumption), $R'/\sqrt{I'}$ is a field, hence $(R'/\sqrt{I'})[x_1]$ is a PID. Following the equivalent statements in the above paragraph, we can conclude that I is primary. □

4.3 Zero-dimensional Primary Decomposition

Throughout this section, we assume that we can factor polynomials in one variable over finitely generated algebraic extensions of R/M where $M \subset R$ is any maximal ideal. We will give an algorithm to compute the irredundant primary decomposition of zero-dimensional ideals in $R[x]$. First, we write I as $\bigcap I_i$ where $I_i \cap R[x_n]$ is M_i-primary while $I \cap R$ is M-primary. We then iterate the algorithm for each I_i and by induction on the number of variables, in the end, we reach a primary decomposition of I.

The following proposition yields the induction step.

Proposition 4.3.1 (Proposition 6.1 in [13])**.** *Let $I \subset R[x]$ be a zero-dimensional ideal and let $I \cap R$ be an M-primary ideal where $M \subset R$ is a maximal ideal. Then one can construct zero-dimensional ideals $I_1, \ldots, I_m \subset R[x]$ and distinct maximal ideals $M_1, \ldots, M_m \subset R[x_n]$ such that $I = \bigcap_i I_i$ and $I_i \cap R[x_n]$ is M_i-primary.*

Proof. If we let $I^c = I \cap R[x_n]$, then to apply Lemma 4.2.10, we need a claim.

Claim 1: $I^c \cap R = I \cap R$ is zero-dimensional and primary.

Proof of Claim 1: First of all, $I^c \cap R = I \cap R[x_n] \cap R = I \cap R$ and we are given $I \cap R$ as M-primary, hence $\sqrt{I \cap R} = M$ where M is a maximal ideal. Every prime ideal containing $I \cap R$ is maximal. This is because if we let $I \cap R \subset P$ where $I \cap R$

is primary and P is prime, then $\sqrt{I \cap R} \subset \sqrt{P} = P$. However, $\sqrt{I \cap R}$ is maximal, so $M = \sqrt{I \cap R} = P$. This implies $I \cap R$ is zero-dimensional and proves the claim.

Since I is zero-dimensional and $I \cap R$ is zero-dimensional and primary, by Proposition 4.2.8 there exists a $g_n \in I$ such that, $lt(g_n) = c_n x_n^{k_n}$ where c_n is a unit modulo $I \cap R$. Since x_n is the smallest variable in the *lex* order we use, we get $g_n \in I \cap R[x_n]$, hence by Proposition 4.2.8 again, $I^c = I \cap R[x_n]$ is zero-dimensional. Then by Lemma 4.2.10 and its proof, for $g = g_n$, we have $\sqrt{I^c} = \sqrt{(g, I^c \cap R)} = \sqrt{(g, \sqrt{I^c \cap R})} = \sqrt{(g, M)}$.

At the beginning of this section, we assumed that we can factorize univariate polynomials, so we let $g(x_n) = \prod_i (p_i(x_n))^{s_i}$ be the irreducible factorization of $g(x_n)$ $mod(M)$, i.e. factorization in $(R/M)[x_n]$, hence the coefficients of $p_i(x_n)$'s are in R/M. Although these coefficients are in R/M, we can see $p_i(x_n)$ in $R[x_n]$ by choosing a representative for each coefficient. The images of $p_i(x_n)$ in $(R/M)[x_n]$ are irreducible polynomials in a PID (since R/M is a field), hence they are pairwise comaximal non-units.

Claim 2: $\prod_i (p_i(x_n))^{s_i} \in (g, M) \subset \sqrt{I^c}$.

Proof of Claim 2: In $(R/M)[x_n]$, we have $\prod_i (p_i(x_n))^{s_i} = g(x_n)$. This implies, $\prod_i (p_i(x_n))^{s_i} - g(x_n) \in MR[x_n]$. Therefore, $\prod_i (p_i(x_n))^{s_i} \in (g, M)$ where $(g, M) \subset \sqrt{(g, M)}$, and since $\sqrt{(g, M)} = \sqrt{I^c}$, we prove the claim.

Hence, $(\prod_i (p_i(x_n))^{s_i})^s \in I^c$ for some $s > 0$.

Claim 3: I contains a power of M.

Proof of Claim 3: Since R is Noetherian, $M = \sqrt{I \cap R}$ has a finite basis. Let $M = \langle h_1, \ldots, h_s \rangle$. So, $h_i^{k_i} \in I \cap R$ for all $i \in \{1, \ldots, s\}$. Each element of M is expressed as $\sum_{i=1}^{s} \alpha_i h_i$, hence $(\sum_{i=1}^{s} \alpha_i h_i)^{k_1 + \cdots + k_s} \in I \cap R$. Let $K = max\{k_i\}$. Thus, $M^{Ks} \subset I \cap R \subset I$. If we let $Ks = t$, then $M^t \subset I$ which proves the claim.

Claim 4: If $p_i(x_n)$ and $p_j(x_n)$ are comaximal mod(M) for $i \neq j$, and I contains a power of M, then $p_i(x_n)$ and $p_j(x_n)$ are comaximal mod(I).

Proof of Claim 4: If $p_i(x_n), p_j(x_n) \in R[x_n]$ are comaximal $mod(M)$, then one of

their linear combinations in $(R/M)[x_n]$ is $\bar{1}$, i.e. $(\bar{p_i}) + (\bar{p_j}) = (R/M)[x_n]$. Thus, $\bar{a}\bar{p_i} + \bar{b}\bar{p_j} = \bar{1}$ in $(R/M)[x_n]$ where $a, b \in R[x_n]$. So, $ap_i + bp_j - 1 \in MR[x_n]$. Let $ap_i + bp_j - 1 = F \in MR[x_n]$. We have $M^k \subset I \cap R$ for some $k > 0$ by Claim 3. Therefore, F^N has coefficients in $I \cap R$ for some $N > 0$. Hence, $F^N \in I$. Thus, $(ap_i + bp_j - 1)^N \in I$ which implies $(ap_i + bp_j - 1)^N \equiv 0$ in $R[x_n]/I$. If we write this binomial expansion explicitly, we get $cp_i + dp_j + (-1)^N \equiv 0$ in $R[x]/I$ for some $c, d \in R[x_n]$. This implies p_i and p_j are comaximal in $R[x]/I$, hence proves the claim.

Claim 5: $\bigcap_i (p_i^{s_i s}, I) = (\prod_i p_i^{s_i s}, I) = I$.

Proof of Claim 5: Since $p_i^{s_i}$ are pairwise comaximal in $R[x]/I$ by Claim 4, we can conclude $p_i^{s_i s}$ are also pairwise comaximal in $R[x]/I$. Hence, by Chinese Remainder Theorem, $\bigcap(p_i^{s_i s}) = (\prod p_i^{s_i s})$ in $R[x]/I$ (see [5], pg.131). Thus, $\bigcap(p_i^{s_i s}, I) = (\prod p_i^{s_i s}, I) = I$ in $R[x]$ since $(\prod p_i^{s_i})^s \in I^c \subset I$. This proves the claim.

Let $I_i = (p_i^{s_i s}, I)$ and $M_i = (p_i, M)R[x_n]$. Therefore, by Claim 5 we get $\bigcap I_i = I$.

Claim 6: $M_i = (p_i, M)R[x_n]$ *is maximal in* $R[x_n]$.

Proof of Claim 6: We have the isomorphism:

$$\frac{R[x_n]}{M_i} \cong \frac{R[x_n]/(MR[x_n])}{M_i/(MR[x_n])}.$$

Also, $\dfrac{R[x_n]}{MR[x_n]} \cong \dfrac{R}{M}[x_n]$ and $\dfrac{(p_i, M)R[x_n]}{MR[x_n]} \cong (\bar{p_i}) \subset (R/M)[x_n]$. Moreover, since M is maximal , R/M is a field, and since $\bar{p_i}$ is irreducible in $(R/M)[x_n]$, $\dfrac{(R/M)[x_n]}{(\bar{p_i})}$ is a field. Thus, M_i is a maximal ideal in $R[x_n]$. This finishes the proof of the claim.

Claim 7: $I_i \cap R[x_n] = (p_i^{s_i s}, I) \cap R[x_n]$ *contains a power of* $M_i = (p_i, M)R[x_n]$.

Proof of Claim 7: We have $p_i^{s_i s} \in I_i$, $p_i \in R[x_n]$, $M_i \subset R[x_n]$ and since $M = \sqrt{I \cap R}$, we get $M^t \subset I \cap R \subset I_i \cap R[x_n]$, for some $t > 0$ (by Claim 3). Hence, a suitable power of M_i, say $M_i^{s_i s + t}$ is in $I_i \cap R[x_n]$ which completes the proof of the claim.

Claim 8: If $I_i \cap R[x_n]$ *contains a power of* M_i*, then* $I_i \cap R[x_n]$ *is either* M_i*-primary or the unit ideal in* $R[x_n]$.

Proof of Claim 8: If $M_i^t \subset I_i \cap R[x_n]$ for some $t > 0$, then $\sqrt{M_i^t} \subset \sqrt{I_i \cap R[x_n]}$. Since M_i is maximal, we can show that $\sqrt{M_i^t} = M_i$. Hence, $M_i \subset \sqrt{I_i \cap R[x_n]}$. Since M_i is maximal, either $M_i = \sqrt{I_i \cap R[x_n]}$ or $\sqrt{I_i \cap R[x_n]} = R[x_n]$. In the latter case $I_i \cap R[x_n] = R[x_n]$. In the former case, we can conclude that $I_i \cap R[x_n]$ is M_i-primary. (Since $I \cap R[x_n]$ is zero-dimensional and $I \cap R[x_n] \subset I_i \cap R[x_n]$, we get $I_i \cap R[x_n]$ is either zero-dimensional or the unit ideal in $R[x_n]$. If $I_i \cap R[x_n]$ is zero-dimensional, then $\sqrt{I_i \cap R[x_n]} = \bigcap K_j$ where K_j are the associated primes which are all maximal. Then, $\sqrt{I_i \cap R[x_n]} = M_i = \bigcap K_j$ implies there exists only one K_j and $M_i = K_1$, hence $I_i \cap R[x_n]$ is M_i-primary since there is one associated prime, hence one primary component.) This proves the claim.

Claim 9: $I_i \cap R[x_n] \neq R[x_n]$.

Proof of Claim 9: Since $I_i = (p_i^{s_i s}, I)$, if $c \in I_i$, then $c = a p_i^{s_i s} + b$ where $a \in R[x]$, $b \in I$. Thus, $(\prod_{i \neq j} p_j^{s_j s}) I_i \subset I$ since $(\prod_{i \neq j} p_j^{s_j s})(a p_i^{s_i s} + b) \in I$ as $\prod_i p_i^{s_i s} \in I$. Assume $I_i \cap R[x_n] = (1)$, then $(\prod_{i \neq j} p_j^{s_j s}) \cdot 1 = \prod_{i \neq j} p_j^{s_j s} \in I$. Since $p_j \in R[x_n]$ for all j, $\prod_{i \neq j} p_j^{s_j s} \in I \cap R[x_n] = I^c \subset \sqrt{I^c} = \sqrt{(g, M)}$ which implies $\prod_{i \neq j} p_j \in (g, M)$. Hence, $\prod_{i \neq j} p_j = gh + m$ for some $h \in R[x_n]$, $m \in MR[x_n]$. Modulo M (in $(R/M)[x_n]$), we get $\prod_{i \neq j} p_j \equiv (\prod p_i^{s_i}) \cdot h$ which contradicts that p_i is an irreducible, non-unit in the PID $(R/M)[x_n]$ (considering unique factorization in $(R/M)[x_n]$). Therefore, $I_i \neq (1)$ which proves the claim.

As a result of Claim 8 and 9, $I_i \cap R[x_n]$ is M_i-primary. We have already shown that $I = \bigcap I_i$ which completes the proof. □

If we use the above proposition recursively for M_i and I_i over $R[x_n]$, then we can obtain the complete primary decomposition of the ideal I and its associated primes.

Algorithm 4.3.2. ZPD (R; x; M). Zero-dimensional ideals' primary decomposition

Input: Ring R; variables $x = x_1, \ldots, x_n$; ideal $I \subset R[x]$; ideal $M \subset R$.

Assumptions: M is maximal, I is zero-dimensional, $I \cap R$ is M-primary.

Output: $\{(Q_1, M_1), \ldots, (Q_m, M_m)\}$ where Q_i and M_i are ideals in $R[x]$ such that M_i is maximal, $M_i \neq M_j$ for $i \neq j$, Q_i is M_i-primary, and $I = \bigcap_i Q_i$ (irredundant primary decomposition of I).

Step 1: If $n = 0$ then return $\{(I, M)\}$. (Here, if $n = 0$, then $I \cap R = I$. I is zero-dimensional and $\sqrt{I} = M$ by assumption. So, I is M-primary and its decomposition is itself.)

Step 2: Compute a minimal Gröbner basis G for $I \cap R[x_n]$ (by using Proposition 3.2.1 (ii).) (For an ideal I, we can compute a Gröbner basis $\tilde{G}$ and make it minimal. Then by Proposition 3.2.1 (ii), $\tilde{G} \cap R[x_n]$ is a minimal Gröbner basis, say G, for $I \cap R[x_n]$.)

Step 3: Select $g \in G$ of largest degree. (Since G is minimal, I is zero-dimensional and $I \cap R$ is zero-dimensional primary, there exists a unique such g by the remark after Proposition 4.2.8).

Step 4: Compute the irreducible factorization of $g \ mod(M)$ where $g = \prod_i p_i^{s_i}$ in $(R/M)[x_n]$, and $p_i \in R[x_n]$. (We can compute this factorization by the assumption preceding Proposition 4.3.1. Afterwards, we can choose one representative from each coset of R/M, thus we can write $p_i \in R[x_n]$).

Step 5: Find an integer $s > 0$ such that $(\prod_i p_i^{s_i})^s \in I \cap R[x_n]$. (If we let $f = \prod_i p_i^{s_i}$, then for consecutive values of s, we can compute f^s and we can determine whether $f^s \in I \cap R[x_n]$ by ideal membership algorithm. Note that such an s exists by the proof of Proposition 4.3.1).

Step 6: Let $I_i = (p_i^{s_i s}, I)$, $M_i = (p_i, M)R[x_n]$ (by Proposition 4.3.1 $I = \bigcap I_i$ and $I_i \cap R[x_n]$ is M_i-primary).

Step 7: Return $\bigcup_i \text{ZPD}(R[x_n];\ x_1, \ldots, x_{n-1};\ I_i,\ M_i)$

The algorithm is recursively defined. At *Step 6* we get $I = \bigcap I_i$ and $I_i \cap R[x_n]$ is M_i-primary by Proposition 4.3.1. Each I_i is zero-dimensional since I is zero-dimensional, $I \subset I_i$ and $I_i \neq R[x]$ ($1 \notin I_i$ since $I_i \cap R[x_n] \neq R[x_n]$ as $I_i \cap R[x_n]$ is primary in $R[x_n]$). I_i is zero-dimensional, $I_i \cap R[x_n]$ is M_i-primary and M_i is maximal in $R[x_n]$, hence the assumptions of the algorithm hold for $I_i \subset (R[x_n])[x_1, \ldots, x_{n-1}]$ considering $R[x_n]$ as the coefficient ring and $x_1, \ldots, x_{n-1}$ as variables. Therefore, in *Step 7*, we can apply the algorithm to I_i and M_i where this time, the number of variables is $n - 1$. At each stage of the algorithm (at each iteration) the number of variables drops by 1, and the algorithm terminates when the number of variables is 0.

By induction on n (number of variables) we can prove that this algorithm gives an irredundant primary decomposition of I as follows. If $n = 0$, then $I = I \cap R$ is M-primary, thus $I = I$ is an irredundant primary decomposition of I. We can also see that if $n = 1$, at *Step 6*, $I = \bigcap I_i$ is a primary decomposition of I (here, $I \subset R[x_1]$ and $I_i \cap R[x_1] = I_i$ is M_i-primary in $R[x_1]$), and it is irredundant since M_i are distinct by proof of Proposition 4.3.1. This argument shows that the algorithm works for $n = 0$ and $n = 1$. Assume now, the algorithm works for $n - 1$ variables.

For $I \subset R[x_1, \ldots, x_n]$ satisfying the assumptions of the algorithm, at *Step 6*, we get $I = \bigcap I_i$, $I \subset (R[x_n])[x_1, \ldots, x_{n-1}]$ considering $R[x_n]$ as the coefficient ring, and $x_1, \ldots, x_{n-1}$ as variables, as explained above, we can apply the algorithm to I_i and M_i. Since there are $n - 1$ variables, by inductive hypothesis, the algorithm returns $I_i = \bigcap_j Q_{ij}$ (an irredundant primary decomposition of I_i) and $M_{ij} = \sqrt{Q_{ij}}$ where Q_{ij} is M_{ij}-primary. Then we get, $I = \bigcap_i I_i = \bigcap_i (\bigcap_j Q_{ij}) = \bigcap_{i,j} Q_{ij}$ which gives primary decomposition of I.

To show irredundancy, we need to prove $M_{i_1 j_1} \neq M_{i_2 j_2}$ whenever $(i_1, j_1) \neq (i_2, j_2)$. By the induction hypothesis on $n-1$ variables, we have $M_{ij_1} \neq M_{ij_2}$ if $j_1 \neq j_2$ since $I_i = \bigcap_j Q_{ij}$ is an irredundant primary decomposition of I_i by assumption. Since $I_i \cap R[x_n]$ is M_i-primary, $\sqrt{I_i \cap R[x_n]} = M_i \subset R[x_n]$. Thus, M_i is equal to the following:

$$\sqrt{I_i \cap R[x_n]} = \sqrt{(\bigcap_j Q_{ij}) \cap R[x_n]} = \sqrt{\bigcap_j (Q_{ij} \cap R[x_n])} = \bigcap_j \sqrt{Q_{ij} \cap R[x_n]}.$$

Therefore, $M_i \subset \sqrt{Q_{ij} \cap R[x_n]}$ and since $Q_{ij} \cap R[x_n] \neq R[x_n]$ ($1 \notin Q_{ij}$ as Q_{ij} is primary) we can conclude $M_i = \sqrt{Q_{ij} \cap R[x_n]}$ using M_i is maximal in $R[x_n]$. We have $M_i = \sqrt{Q_{ij} \cap R[x_n]} = \sqrt{Q_{ij}} \cap R[x_n] = M_{ij} \cap R[x_n]$. Assume $M_{i_1 j_1} = M_{i_2 j_2}$ for $i_1 \neq i_2$, then $M_{i_1} = M_{i_1 j_1} \cap R[x_n] = M_{i_2 j_2} \cap R[x_n] = M_{i_2}$ which contradicts $M_{i_1} \neq M_{i_2}$ (M_i are distinct by proof of Proposition 4.3.1). Therefore, $M_{i_1 j_1} \neq M_{i_2 j_2}$ whenever $i_1 \neq i_2$. This completes the proof of irredundancy for the primary decomposition $I = \bigcap_{i,j} Q_{ij}$. Hence, the algorithm works for n variables completing the proof by induction.

To clarify the procedure in this algorithm, we look at a few initial stages more explicitly. At the first stage, $I \subset R[x_1, \ldots, x_n]$, $I \cap R$ is M-primary, I is zero-

dimensional. At the end of this stage, we get $I = \bigcap I_i$, $I_i \cap R[x_n]$ is M_i-primary where $M_i \subset R[x_n]$ is maximal. In stage two, we apply the algorithm to each pair (I_i, M_i) where $I_i \subset (R[x_n])[x_1, \ldots, x_{n-1}]$ (the coefficient ring is $R[x_n]$ and there are $n-1$ variables $x_1, \ldots, x_{n-1}$). At the end of stage two, we get $I_i = \bigcap_j I_{ij}$ and $I_{ij} \cap R[x_{n-1}, x_n]$ is M_{ij}-primary where $M_{ij} \subset R[x_{n-1}, x_n]$ is maximal. So, $I = \bigcap_i I_i = \bigcap_{i,j} I_{ij}$. Similarly, at stage three, we apply the algorithm to each pair (I_{ij}, M_{ij}) where $I_{ij} \subset (R[x_{n-1}, x_n])[x_1, \ldots, x_{n-2}]$ (the coefficient ring is $R[x_{n-1}, x_n]$ and there are $n-2$ variables $x_1, \ldots, x_{n-2}$. At the end of stage three, we get $I_{ij} = \bigcap_k I_{ijk}$ and $I_{ijk} \cap R[x_{n-2}, x_{n-1}, x_n]$ is M_{ijk}- primary where M_{ijk} is a maximal ideal in $R[x_{n-2}, x_{n-1}, x_n]$. We obtain $I = \bigcap_{i,j} I_{ij} = \bigcap_{i,j,k} I_{ijk}$.

Continuing this way, at the end of $k-th$ stage, we get $I = \bigcap_{i_1, i_2, \ldots, i_k} I_{i_1 i_2 \ldots i_k}$ where $I_{i_1 \ldots i_k} \cap R[x_{n-k+1}, \ldots, x_n]$ is $M_{i_1 \ldots i_k}$-primary where $M_{i_1 i_2 \ldots i_k}$ is a maximal ideal in $R[x_{n-k+1}, \ldots, x_n]$.

The algorithm stops at the end of the $n-th$ stage where we obtain $I = \bigcap_{i_1, \ldots, i_n} I_{i_1 i_2 \ldots i_n}$ where $I_{i_1 \ldots i_n} \cap R[x_1, \ldots, x_n] = I_{i_1 \ldots i_n}$ is $M_{i_1 \ldots i_n}$ primary where $M_{i_1 \ldots i_n}$ is a maximal ideal in $R[x_1, \ldots, x_n] = R[x]$, therefore we reach an irredundant primary decomposition of I.

Remark: At the end of the algorithm, we obtain the irredundant primary decomposition, hence $I = \bigcap \tilde{I}_i$ where $\tilde{I}_i$ is $\tilde{M}_i$ primary and $\tilde{M}_i$ is maximal in $R[x]$. We can compute $\sqrt{I}$ as $\sqrt{I} = \sqrt{\bigcap \tilde{I}_i} = \bigcap \sqrt{\tilde{I}_i} = \bigcap \tilde{M}_i$ since $\sqrt{\tilde{I}_i} = \tilde{M}_i$. The algorithm explicitly computes the maximal ideals $\tilde{M}_i$, hence we can explicitly compute $\sqrt{I}$ as $\bigcap \tilde{M}_i$.

4.4 Primary Decomposition in Polynomial Rings over Principal Ideal Domains

In this section, we investigate the problem of primary decomposition where the coefficient ring is a PID.

Lemma 4.4.1 (Lemma 8.1 in [13]). *Let S be a multiplicatively closed subset of R and let $s \in S$.*

$$\textit{If } (S^{-1}I) \cap R \subset (I : s) \textit{ then } I = (I : s) \cap (I, s).$$

Proof. $I \subset (I : s)$ since if $i \in I$ then $is \in I$, by definition of an ideal. Also, $I \subset (I, s)$ since I is in the generator set of (I, s). Conversely, let $a \in (I : s) \cap (I, s)$. So, since $a \in (I, s)$, $a = i + ks$ where $k \in R$, $i \in I$. Also, we have $a \in (I : s)$, thus $as = is + ks^2 \in I$. Here, $is \in I$, $as \in I$ implies $ks^2 \in I$. Thus, $k = \dfrac{ks^2}{s^2} \in S^{-1}I$. Together with $k \in R$, this implies $k \in (S^{-1}I) \cap R \subset (I : s)$ by assumption of the lemma. Then, $ks \in I$ which implies $a = i + ks \in I$. □

If we use this lemma and Proposition 3.2.11, then we reach the next proposition which serves as the key of the decomposition process.

Proposition 4.4.2 (Proposition 8.2 in [13])**.** *Let R be an integral domain, $(p) \subset R$ be a principal prime ideal. For any given ideal $I \subset R[x]$, it is possible to find an element $r \in R - (p)$ such that*

$$I = (I, r) \cap I^{ec}$$

where $I^{ec} = IR_{(p)}[x] \cap R[x]$.

Proof. We can find an element $s \in R - (p)$ so that $I^{ec} = IR_s[x] \cap R[x] = IR_{(p)}[x] \cap R[x]$ by using Proposition 3.2.11. Also, we can find a generating set (a Gröbner basis) of I^{ec}, i.e., we can compute I^{ec} by Corollary 3.2.6. Let $G = \{g_1, \ldots, g_t\}$ be a Gröbner basis for $I^{ec} = IR_s[x] \cap R[x]$. So, $g_i = h_{i1}f_1 + \cdots + h_{ik}f_k$ where $I = \langle f_1, \ldots, f_k \rangle$ and $h_{ij} \in R_s[x]$ for all $i \in \{1, \ldots, t\}$, $j \in \{1, \ldots, k\}$ and for some $k \in \mathbb{N}$. Here, each h_{ij} has a denominator $s^{\alpha_{ij}}$. Let $m_i = max_j\{\alpha_{ij}\}$. Then, $s^{m_i}h_{ij} \in R[x]$ and hence, $s^{m_i}g_i \in I$. If we let $m = max\{m_i\}$, then we have $s^m g_i \in I$, for all $i \in \{1, \ldots, t\}$. Since g_i's are the basis elements for I^{ec}, we have $s^m I^{ec} \subset I$, i.e., $I^{ec} \subset (I : s^m)$. Here, we can compute m_i for each g_i by checking whether $s^{m_i}g_i \in I$ or not by using ideal membership algorithm and substituting $m_i = 1, 2, \ldots$. Surely, we can compute $m = max\{m_i\}$ then. Since for $S = R - (p)$, we have $S^{-1}I \cap R[x] = IR_{(p)}[x] \cap R[x] = I^{ec}$ and $I^{ec} \subset (I : s^m)$ from above, we obtain $S^{-1}I \cap R[x] \subset (I : s^m)$ where $s^m \in S$ since $s \in S$. Therefore, by Lemma 4.4.1, we have $I = (I : s^m) \cap (I, s^m)$. Thus, since $I^{ec} \subset (I : s^m)$ and $I \subset I^{ec}$,

$$I \subset I^{ec} \cap (I, s^m) \subset (I : s^m) \cap (I, s^m) = I.$$

Therefore, $I^{ec} \cap (I, s^m) = (I : s^m) \cap (I, s^m) = I$. Taking $s^m = r$ finishes the proof. □

Following is the central proposition of this section.

Proposition 4.4.3 (Proposition 8.3 in [13])**.** *Let R be a PID, I be an ideal in $R[x]$, $(p) \subset R$ be a maximal ideal. If $I \cap R$ is (p)-primary, then it is possible to compute a primary decomposition for I.*

Proof. Let us note that if $I \cap R$ is (p)-primary and (p) is a maximal ideal, then $I \cap R$ is zero-dimensional.

Suppose I is zero-dimensional, then we can find a decomposition by zero-dimensional primary decomposition algorithm, i.e., ZPD which was introduced after Proposition 4.3.1. Now, suppose I is not zero-dimensional, then by Corollary 4.2.7 we can find an i such that $I \cap R[x_i] = I \cap R'$ is not zero-dimensional where $R' = R[x_i]$. Let $x' = x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$ (x' is equal to the whole sequence of variables $x_1, x_2, x_3, \ldots$). Thus, $R'[x'] = R[x]$ and $I \cap R'$ is not zero-dimensional.

By Proposition 4.4.2, we can find an element $r' \in R' - (p)R'$ such that $I = (I, r') \cap I^{ec}$ where $I^{ec} = IR'_{(p)}[x'] \cap R'[x']$. Therefore, it is enough to decompose (I, r') and I^{ec} separately.

Claim 1: Since $(I, r') \cap R'$ contains both the (p)-primary ideal $I \cap R$ and the element $r' \notin (p)R'$, we can conclude $(I, r') \cap R'$ is either zero-dimensional or the unit ideal R'.

Proof of Claim 1: We need to clarify a possible misconception here: Since $(I, r') \cap R'$ is an ideal in R' and $I \cap R$ is an ideal in R, we can not conclude directly that "If $(I \cap R) \subseteq (I, r') \cap R'$ and $I \cap R$ is (p)-primary then $(I, r') \cap R'$ is zero-dimensional."

Now, let $J = (I, r') \cap R'$. Assume that J is not the unit ideal. So, J is contained in at least one maximal (hence prime) ideal. Let there be a chain of prime ideals containing J as follows: $(I \cap R) \subseteq J \subseteq Q_1 \subseteq \cdots \subseteq Q_t \subseteq R'$ where J contains $I \cap R$ as a set. We are given that $(I \cap R)$ is (p)-primary. Thus, $\sqrt{I \cap R} = (p)$ implying $p^k \in I \cap R$ for some $k > 0$. Thus, $p^k \in J$ and $p^k \in Q_1$, hence $p \in Q_1$ since Q_1 is prime.

Therefore, $(p)R^{'} \subseteq Q_1$. If we look at the quotient ideals, then we have:

$$\frac{Q_1}{(p)R^{'}} \subseteq \frac{Q_2}{(p)R^{'}} \subseteq \cdots \subseteq \frac{Q_t}{(p)R^{'}} \subseteq \frac{R^{'}}{(p)R^{'}}.$$

Note that if Q_i is prime in R', then $\frac{Q_i}{(p)R^{'}}$ is prime in $\frac{R^{'}}{(p)R^{'}}$. Now, since $p \in R$,

$$\frac{R^{'}}{(p)R^{'}} = \frac{R[x_i]}{(p)R[x_i]} \cong \frac{R}{(p)}[x_i].$$

Moreover, since (p) is maximal in R, $R/(p)$ is a field. Then, $\frac{R^{'}}{(p)R^{'}}$ is a PID. Prime ideals in a PID are either (0) which is one dimensional, or (α) which is zero-dimensional, where α is an irreducible element. So, if $\frac{Q_1}{(p)R^{'}} = (0)$ then $Q_1 = (p)R^{'}$. However, $r^{'} \notin (p)R^{'}$ and $r^{'} \in Q_1$ since $r' \in J \subseteq Q_1$. Therefore, $\frac{Q_1}{(p)R^{'}} \neq (0)$. Hence, $\frac{Q_1}{(p)R^{'}}$ is zero-dimensional. Thus, the chain of prime ideals containing $J = (I, r^{'}) \cap R^{'}$ in $R^{'}$ can have at most one prime ideal Q_1. Therefore, J is zero-dimensional. (If $Q_1 \subsetneq Q_2$ then $\frac{Q_1}{(p)R^{'}} \subsetneq \frac{Q_2}{(p)R^{'}}$). This proves the claim.

Here, we can check whether $1 \in J$ by using Gröbner Basis and ideal membership algorithm. If $1 \notin J$, i.e. $J \neq R^{'}$, then J is zero-dimensional.

If $(I, r^{'}) \cap R[x_i]$ is zero-dimensional for $(I, r^{'})$, then the number of x_k's where $(I, r^{'}) \cap R[x_k]$ is not zero-dimensional is at least one less than the number of variables where $I \cap R[x_k]$ is not zero-dimensional. Then we start the Algorithm 4.4.5 from $(I, r^{'})$ instead of I and obtain a primary decomposition of (I, r') by induction on the number of variables such that $I \cap R[x_k]$ is not zero-dimensional. For this purpose, we need to check whether $(I, r^{'}) \cap R$ is (p)-primary: Since $I \cap R \subset (I, r') \cap R$, $I \cap R$ is zero-dimensional and $(I, r') \cap R \neq (1)$ (because $(I, r') \cap R'$ is zero-dimensional which means $1 \notin (I, r')$). We can conclude $(I, r') \cap R$ is zero-dimensional. Since $I \cap R$ is (p)-primary and (p) is maximal, $(p) = \sqrt{I \cap R} \subset \sqrt{(I, r') \cap R} \neq (1)$ gives $(p) = \sqrt{(I, r') \cap R}$. Therefore, $(I, r') \cap R$ is (p)-primary since it is zero-dimensional.

If on the other hand, $(I, r^{'}) \cap R^{'} = R^{'}$, then $(I, r^{'}) = R[x]$ since $1 \in (I, r^{'})$. Therefore, $I = (I, r^{'}) \cap I^{ec} = I^{ec}$. In this case, we need to decompose I^{ec}.

Decomposing I^{ec} is equivalent to decomposing $I^e = IR'_{(p)}[x']$ and finding its contrac-

tion to $R^{'}[x^{'}]$ by Proposition 3.2.11. We have $I^{ec} = I^e \cap R^{'}[x^{'}]$, let $I^e = \bigcap_{i=1}^{m} Q_i$ be a primary decomposition of I^e. Thus, $I^{ec} = (\bigcap_{i=1}^{m} Q_i) \cap R^{'}[x^{'}] = \bigcap_{i=1}^{m}(Q_i \cap R^{'}[x^{'}])$. Let $(Q_i \cap R^{'}[x^{'}]) = \widetilde{Q_i}$. Let us check whether $\widetilde{Q_i}$ is primary. Let $ab \in \widetilde{Q_i}$ for $a, b \in R^{'}[x^{'}]$. Hence, $ab \in Q_i$ which implies $a \in Q_i$ or $b^k \in Q_i$ for some $k > 0$ since Q_i is primary. We also have $a, b \in R^{'}[x^{'}]$. So $a \in \widetilde{Q_i}$ or $b^k \in \widetilde{Q_i}$ which implies $\widetilde{Q_i}$ is primary.

Claim 2: $R^{'}_{(p)}$ *is a PID.*

Proof of Claim 2: If $S = R[x_i] - (p)R[x_i]$ then $R^{'}_{(p)} = (R[x_i])_{(p)} = S^{-1}R^{'}$. There is a one-to-one correspondence between the proper ideals of $R[x_i]$ which do not intersect with S and the proper ideals of $S^{-1}R[x_i]$ which can be depicted as $I \longleftrightarrow S^{-1}I$ where $S \cap I = \varnothing$. We know that if R is a PID then R is Noetherian, thus $R[x_i]$ is Noetherian by Hilbert's Basis theorem. Let us take an ideal J in $S^{-1}R[x_i] = R^{'}_{(p)}$. Hence, $J = S^{-1}I$ for some ideal $I \subseteq R[x_i]$ where $I \cap S = \varnothing$. Since $R[x_i]$ is Noetherian, $I = \langle f_1, \ldots, f_s \rangle$ in $R[x_i]$. $J = S^{-1}I = \langle f_1, \ldots, f_s \rangle R^{'}_{(p)}$. Elements of S are units in $S^{-1}R^{'} = R^{'}_{(p)}$. We have S as the set of polynomials in $R[x_i]$ which are not divisible by p since $S = R[x_i] - (p)R[x_i]$.

Now, since R is a PID, R is a UFD and hence $R[x_i]$ is a UFD. Therefore, if p is irreducible in R, then p is irreducible in $R[x_i]$. Since $R[x_i]$ is a UFD, $f_i = p^{\alpha_i}.\tilde{f}_i$ where $\alpha_i > 0$, $\tilde{f}_i$ are units in $S^{-1}R[x_i]$, and $p \nmid \tilde{f}_i$. In fact, $\alpha_i \geq 1$ since $I \cap S = \varnothing$. Hence, all elements of I are divisible by p: $J = S^{-1}I = \langle f_1, \ldots, f_s \rangle R^{'}_{(p)} = \langle p^{\alpha_1}\tilde{f}_1, p^{\alpha_2}\tilde{f}_2, \ldots, p^{\alpha_s}\tilde{f}_s \rangle R^{'}_{(p)} = \langle p^{\alpha_1}, \ldots, p^{\alpha_s} \rangle R^{'}_{(p)}$ since $\tilde{f}_i$ is unit in $R^{'}_{(p)}$. Thus, $J = S^{-1}I = \langle p^{\alpha} \rangle R^{'}_{(p)}$ where $\alpha = min_i\{\alpha_i\}$. Therefore, J is a principal ideal which implies that $R^{'}_{(p)}$ is a PID. This completes the proof of the claim.

Note that for any ideal $\widetilde{I} = \langle q_1, \ldots, q_s \rangle \subseteq \widetilde{R}$ and units $u_1, \ldots, u_s \in \widetilde{R}$ we have $\widetilde{I} = \langle q_1, \ldots, q_s \rangle = \langle q_1 u_1, \ldots, q_s u_s \rangle$ in $\widetilde{R}$.

Claim 3: $(p)R^{'}_{(p)}$ *is the unique maximal ideal of* $R^{'}_{(p)}$.

Proof of Claim 3: By the proof of Claim 2, all proper ideals of $R'_{(p)}$ are given by $(p^{\alpha})R'_{(p)}$ for $\alpha \geq 1$. Then, $\alpha = 1$ gives the unique maximal ideal.

Claim 4: $I^e \cap R^{'}_{(p)}$ *is* $(p)R^{'}_{(p)}$*-primary.*

Proof of Claim 4: We are given that $I \cap R$ is (p)-primary. Hence, $(p) = \sqrt{I \cap R}$ which implies $p^k \in I \cap R$. Thus, $p^k \in I$, so $p^k \in IR'_{(p)}[x']$. We have $IR'_{(p)}[x'] = I^e$, thus $p^k \in I^e$. Hence, $p^k \in I^e \cap R'_{(p)}$. Therefore, $p \in \sqrt{I^e \cap R'_{(p)}}$ implying $(p)R'_{(p)} \subseteq \sqrt{I^e \cap R'_{(p)}}$. Now, we need to show $IR'[x'] \cap R' \subseteq (p)R'$ since this will imply $IR'_{(p)}[x'] \cap R'_{(p)} \subseteq (p)R'_{(p)}$.

Let P be a non zero-dimensional associated prime of $I \cap R'$. (Note that $I \cap R'$ is not zero-dimensional, thus such a P exists). Hence, $I \cap R' = \bigcap_{i=1}^{r} Q_i$ where Q_i are primary, which implies $\sqrt{I \cap R'} = \bigcap_{i=1}^{r} \sqrt{Q_i}$. Let, without loss of generality, $\sqrt{Q_1} = P$ where P is not zero-dimensional. Thus, $(p)R' \subseteq P$ since (as we have shown above) $(p)R' \subseteq \sqrt{I \cap R'} \subset P$ (as $\bigcap_{i=1}^{r} \sqrt{Q_i} \subseteq P$).

$(p)R'$ is one dimensional in R' since $R'/((p)R')$ is a PID which is not a field as shown above, hence has Krull dimension 1. We have $dimP \geq 1$ and $dim(p)R' = 1$. Also, $P \supseteq (p)R'$ implies $dimP \leq dim(p)R' = 1$. Therefore, $dimP = 1$. We have $(p)R' \subseteq P$ and both are one dimensional and prime, hence $P = (p)R'$. Furthermore, $I \cap R' \subseteq (p)R'$ since $I \cap R' \subseteq \sqrt{I \cap R'} \subseteq P = (p)R'$.

This shows $I \cap R' = IR'[x'] \cap R' \subseteq (p)R'$ which implies $IR'_{(p)}[x'] \cap R'_{(p)} \subseteq (p)R'_{(p)}$ which then implies $\sqrt{IR'_{(p)}[x'] \cap R'_{(p)}} \subseteq \sqrt{(p)R'_{(p)}} = (p)R'_{(p)}$ since $(p)R'_{(p)}$ is maximal. Thus, $\sqrt{I^e \cap R'_{(p)}} = (p)R'_{(p)}$ since we have shown $(p)R'_{(p)} \subseteq \sqrt{I^e \cap R'_{(p)}}$ before. Therefore, $I^e \cap R'_{(p)}$ is $(p)R'_{(p)}$-primary (since $(p)R'_{(p)}$ is maximal). This completes the proof of the claim.

Let us collect all these four claims towards a proof. If I is zero-dimensional, we apply the ZPD algorithm introduced before. Otherwise, we find $r' \in R' - (p)R'$ such that $I = (I, r') \cap I^{ec}$ and we need to decompose (I, r') and I^{ec} separately. By Claim 1, $(I, r') \cap R'$ is zero-dimensional or the unit ideal in R'. If $(I, r') \cap R'$ is zero-dimensional, then we can compute the primary decomposition of (I, r') by induction on the number of x_k's where the contraction of the ideal to $R[x_k]$ is not zero-dimensional. Else if $(I, r') \cap R'$ is the unit ideal, then $I = I^{ec}$ and we decompose I^{ec} only.

To decompose I^{ec}, we need to decompose $I^e = IR'_{(p)}[x']$ and then contract the decomposition back to $R'[x']$ by Proposition 3.2.11. By Claim 2, $R'_{(p)}$ is a PID and

by Claim 3, $(p)R'_{(p)}$ is the unique maximal ideal of $R'_{(p)}$. By Claim 4, $I^e \cap R'_{(p)}$ is $(p)R'_{(p)}$-primary. Thus, $I^e \subseteq R'_{(p)}[x']$ satisfies the conditions of Proposition 4.4.3. Then, we can apply the algorithm to I^e in $R'_{(p)}[x']$ which has $n-1$ variables and we can obtain the primary decomposition of I^e by induction on n, where n is the number of variables in the polynomial ring. Note that for the base step of induction, if $n = 0$ then $I \subseteq R$ is an ideal in PID R such that $I \cap R = I$ is (p)-primary in R, so I is already primary.

Note that, in the proof we used two induction arguments. In each recursive iteration of the algorithm, either the number of the variables in the polynomial ring drops by 1 or the number of variables x_k such that the contraction of the ideal to $R[x_k]$ is not zero-dimensional drops by 1. If the number of variables becomes zero, the algorithm terminates as explained in the above paragraph and if there is no variable x_k such that the contraction of the ideal to $R[x_k]$ is not zero-dimensional, then the ideal is itself zero-dimensional, hence we terminate the algorithm by applying the ZPD algorithm. □

Corollary 4.4.4 (Corollary 8.4 in [13])**.** *If K is a field, then it is possible to compute the primary decomposition of any proper ideal in $K[x]$.*

Proof. First of all, if K is a field, then K is a PID. $I \cap K \neq (1)$ since I is a proper ideal of $K[x]$. Hence, $I \cap K = (0)$ since the only proper ideal of a field is (0). Then by taking $p = 0$ and $R = K$ in Proposition 4.4.3 we can obtain a primary decomposition of I. (Note that (0) is a maximal ideal in K and $I \cap K = \sqrt{I \cap K} = (0)$ implies $I \cap K$ is (0)-primary). □

Following the arguments in the proof of Proposition 4.4.3, we obtain the following algorithm for computing the primary decomposition of ideals satisfying the conditions of Proposition 4.4.3.

Algorithm 4.4.5. PPD-0 $(R; x; I; p)$: Primary Decomposition Over a PID - Primary Contraction Case

Input: Ring R; variables $x = x_1, \ldots, x_n$; ideal $I \subset R[x]$; $p \in R$

Assumptions: R is a PID, $(p)R$ is maximal, $I \cap R$ is (p)-primary.

Output: $\{Q_1, \ldots, Q_m\}$ such that $Q_i \subset R[x]$ is primary and $I = \bigcap Q_i$.

Step 1: If I is zero-dimensional (which can be checked by Proposition 4.2.8) return its decomposition using ZPD (which was developed in Proposition 4.3.1).

Step 2: Else if I is not zero-dimensional, find i such that $I \cap R[x_i]$ is not zero-dimensional (such an i can be found by Corollary 4.2.7).

Step 3: Let $R' = R[x_i]$, $x' = x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$, $I^e = IR'_{(p)}[x']$.

Step 4: Find $r' \in R' - (p)R'$ such that $I = (I, r') \cap (I^e \cap R'[x'])$ (such an r' exists by Proposition 4.4.2).

Step 5: Let $\{Q_1, \ldots, Q_m\} =$ PPD-0 $(R'_{(p)}; x'; I^e; p)$. (As in the proof of Proposition 4.4.3, I^e and $(p)R'_{(p)}$ satisfy the assumptions of the algorithm. This step is a recursive iteration of the algorithm where the number of variables is reduced by 1).

Step 6: Let $Q_i^c = Q_i \cap R'[x']$. (If $Q_i = (h_1, h_2, \ldots, h_s)R'_{(p)}[x']$ where $h_j \in R'_{(p)}[x']$, then after equating the denominators of the coefficients of h_j we can write $h_j = f_j/t_j$ where $f_j \in R'[x']$ and $t_j \in R' - (p)R'$. Since t_j is a unit in $R'_{(p)}$ we have $Q_i = (f_1, f_2, \ldots, f_s)R'_{(p)}[x'] = I_iR'_{(p)}[x']$ where $I_i = (f_1, f_2, \ldots, f_s)$ as an ideal in $R'[x']$. Hence, $Q_i^c = I_iR'_{(p)}[x'] \cap R'[x']$ which can be computed by Proposition 3.2.11. Then as in proof of Proposition 4.4.3, $\{Q_1^c, Q_2^c, \ldots, Q_m^c\}$ is a primary decomposition of I^{ec}).

Step 7: If $(I, r') = (1)$ then return $\{Q_1^c, \ldots, Q_m^c\}$. (By ideal membership algorithm we can check whether $(I, r') = (1)$ or not. In this case, $I = I^{ec}$, hence a primary decomposition of I^{ec} gives a primary decomposition of I).

Step 8: If $(I, r') \neq (1)$, then let $\{Q'_1, \ldots, Q'_m\} =$ PPD-0 $(R; x; (I, r'); p)$. (Note that as in the proof of Proposition 4.4.3, if $(I, r') \neq (1)$, the conditions of the algorithm hold for the ideal (I, r') in $R[x]$. While $I \cap R[x_i]$ is not zero-dimensional, $(I, r') \cap R[x_i]$ is zero-dimensional as in the proof of Proposition 4.4.3. In the recursive iteration of the algorithm in this step, the number of variables x_j such that the contraction of the ideal to $R[x_j]$ is not zero-dimensional is reduced at least by 1).

Step 9: Return $\{Q_1^c, \ldots, Q_m^c, Q_1^{'}, \ldots, Q_k^{'}\}$ where $\{Q_1^c, \ldots, Q_m^c\}$ is the decomposition

of I^{ec} and $\{Q_1', \ldots, Q_k'\}$ is the decomposition of (I, r') in the case $(I, r') \neq (1)$.

Proposition 4.4.6 (Proposition 8.5 in [13]). *Let R be a PID and I be an ideal in $R[x]$. Then it is possible to compute a primary decomposition for I.*

Proof. We have two cases.

Case 1: $I \cap R$ is not zero-dimensional, i.e., $I \cap R = (0)$ and R is not a field (since in a PID which is not a field, the dimension of an ideal can only be 0 or 1. (0) is the only ideal of dimension 1 and zero-dimensional prime ideals are given by (p) where p is a prime in the PID). Then by Proposition 4.4.2, for the prime ideal $(0) \subset R$ we can find $r \neq 0$, $r \in R$ such that $I = (I, r) \cap (IR_{(0)}[x] \cap R[x])$ where $IR_{(0)}[x] \cap R[x] = I^{ec}$. Since $R_{(0)}$ is the quotient field of R, $IR_{(0)}[x]$ can be decomposed by Corollary 4.4.4 by the algorithm PPD-0 developed in Proposition 4.4.3. Then we can contract the decomposition to $R[x]$ by Proposition 3.2.11. Afterwards, we need to decompose (I, r). We have $(I, r) \cap R = (r')$ for some $r' \in R$ such that $r' \mid r$ (since $r \in (I, r) \cap R$). Here, $r' \neq 0$ since $r \neq 0$. If r' is a unit in R, then $(I, r) = R[x]$, thus we do not need to decompose it. If r' is not a unit, then $(I, r) \cap R$ is zero-dimensional and how to decompose (I, r) is explained in *Case 2*.

Case 2: $I \cap R$ is zero-dimensional. Let $I \cap R = (r') = (\prod p_i^{\alpha_i})$ where $r' = \prod p_i^{\alpha_i}$ is the factorization of r' into irreducibles in R and each $(p_i)R$ is a maximal ideal in R. We need a claim.

Claim 1: $(p_i^{\alpha_i}, I) \cap R$ *is* (p_i)*-primary in* R.

Proof of Claim 1: We need to show that $\sqrt{(p_i^{\alpha_i}, I) \cap R} = (p_i)$ (since (p_i) is maximal, this will imply $(p_i^{\alpha_i}, I) \cap R$ is (p_i)-primary). We have $p_i^{\alpha_i} \in (p_i^{\alpha_i}, I)$, therefore $(p_i) \subseteq \sqrt{(p_i^{\alpha_i}, I) \cap R}$. To show that $(p_i) \supseteq \sqrt{(p_i^{\alpha_i}, I) \cap R}$, it suffices to show $(p_i) \supseteq (p_i^{\alpha_i}, I) \cap R$ since $\sqrt{(p_i)} = (p_i)$ (because (p_i) is a prime ideal). Let $m = p_i^{\alpha_i} h(x_1, \ldots, x_n) + k(x_1, \ldots, x_n) \in (p_i^{\alpha_i}, I) \cap R$. Here, $h(x_1, \ldots, x_n) \in R[x]$ and $k(x_1, \ldots, x_n) \in I$. Thus, $k(x_1, \ldots, x_n) = p_i^{\alpha_i} q(x_1, \ldots, x_n) + k_0$ where $k_0 \in R$, $p_i^{\alpha_i} q(x_1, \ldots, x_n)$ consists of the non-constant terms of $k(x_1, \ldots, x_n)$, and k_0 is the constant term of $k(x_1, \ldots, x_n)$. If we multiply both sides of the above equation by

$p_1^{\alpha_1} \cdots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \cdots p_s^{\alpha_s}$, then we get

$$p_1^{\alpha_1} \cdots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \cdots p_s^{\alpha_s} k = (\prod_{i=1}^{s} p_i^{\alpha_i}) q + p_1^{\alpha_1} \cdots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \cdots p_s^{\alpha_s} k_0$$

which is an element of I since $k \in I$. Thus, we can conclude $p_1^{\alpha_1} \cdots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \cdots p_s^{\alpha_s} k_0 \in I \cap R$ since $\prod_{i=1}^{s} p_i^{\alpha_i} \in I$. Therefore, $p_i^{\alpha_i} \mid k_0$ since $I \cap R = (\prod_{i=1}^{s} p_i^{\alpha_i})$. Hence, $p_i \mid k_0$. Thus, $m = p_i^{\alpha_i} h(x_1, \ldots, x_n) + k(x_1, \ldots, x_n) \in (p_i)$ which shows $(p_i^{\alpha_i}, I) \cap R \subset (p_i)$. Therefore, $(p_i^{\alpha_i}, I) \cap R$ is (p_i)-primary in R which proves the claim.

Now, $(p_i^{\alpha_i}, I)$ can be decomposed by the algorithm PPD-0 developed in Proposition 4.4.3 (Note that the conditions of Proposition 4.4.3 hold since $(p_i^{\alpha_i}, I) \cap R$ is (p_i) -primary and (p_i) is maximal in R). Here, we need another claim:

Claim 2: $I = \bigcap_{i=1}^{s} (p_i^{\alpha_i}, I)$.

Proof of Claim 2: Let $p = \prod p_i^{\alpha_i}$ and $q_i = p/p_i^{\alpha_i}$. Then we get $(q_1, q_2, \ldots, q_s)R = R$ since in the PID R, we have $gcd(q_1, \ldots, q_s) = 1$. Then $r_1 q_1 + r_2 q_2 + \cdots + r_s q_s = 1$ for some $r_i \in R$. Let $y \in \bigcap (p_i^{\alpha_i}, I)$, then for each i, we can write $y = p_i^{\alpha_i} h_i + k_i$ where $h_i \in R[x]$ and $k_i \in I$. Since $q_i p_i^{\alpha_i} = \prod p_i^{\alpha_i} \in I$ we get $q_i y \in I$ for all i. Thus, $y = 1 \cdot y = (r_1 q_1 + r_2 q_2 + \cdots + r_s q_s) \cdot y = \sum r_i (q_i y) \in I$. This shows $\bigcap_{i=1}^{s} (p_i^{\alpha_i}, I) \subset I$. The reverse inclusion is obvious, hence we get the equality which proves the claim.

Now, since $I = \bigcap_{i=1}^{s} (p_i^{\alpha_i}, I)$ and we can find primary decompositions of $(p_i^{\alpha_i}, I)$ as stated above, we can obtain a primary decomposition of I. Note that the above decomposition is not necessarily irredundant. □

Algorithm 4.4.7. PPD (R; x; I) : Primary Decomposition Over a PID

Input: Ring R; variables $x = x_1, \ldots, x_n$; ideal $I \subset R[x]$.

Assumptions: R is a PID.

Output: $\{Q_1, \ldots, Q_m\}$ such that $Q_i \subset R[x]$ is primary and $I = \bigcap_i Q_i$.

Step 0: If $I \cap R$ is zero-dimensional (i.e., if $I \cap R \neq (0)$, skip to *Step 4* replacing (I, r) in *Step 4* by I and $\{Q_1^c, \ldots, Q_k^c\}$ by $\varnothing$.)

Step 1: If $I \cap R$ is not zero-dimensional (i.e., if $I \cap R = (0)$), then find an $r \neq 0, r \in R$ such that $I = (I, r) \cap (IR_{(0)}[x] \cap R[x])$ (we can find such an $r \in R$ by Proposition 4.4.2).

Step 2: Let $\{Q_1, \ldots, Q_k\}$ = PPD-0 $(R_{(0)}; x; IR_{(0)}[x]; 0)$. (Here, we find the decomposition of $I^e = IR_{(0)}[x]$ as in the proof of Proposition 4.4.6).

Step 3: Let $Q_i^c = Q_i \cap R[x]$. (Each Q_i^c can be computed using Proposition 3.2.11 as explained in *Step 6* of Algorithm 4.4.5 above. Then $\{Q_1^c, \ldots, Q_k^c\}$ gives a primary decomposition of I^{ec}).

Step 4: Compute $(I, r) \cap R = (r')$. (We can use Elimination Theory to compute a basis of $(I, r) \cap R$ and since $(I, r) \cap R$ is a PID, we can reduce this basis to a single element. Note that we should compute $I \cap R = (r')$ if $I \cap R \neq (0)$ in *Step 0*).

Step 5: If r' is a unit, then return $\{Q_1^c, \ldots, Q_m^c\}$. (Since then $I = I^{ec}$).

Step 6: Else if r' is not a unit in R, then factorize $r' = \prod p_i^{m_i}$ where p_i are irreducible in R (note that by assumption, we can factorize elements of R).

Step 7: For all i, let $\{Q_1^i, \ldots, Q_{k_i}^i\}$ =PPD-0 $(R; x; (I, p_i^{m_i}); p_i)$. (Here, this gives the decomposition of $((I, r), p_i^{m_i}) = (I, p_i^{m_i})$ (the equality holds since $p_i^{m_i} \mid r$). Note that in the case that $I \cap R \neq (0)$ in *Step 0*, we already need to compute the decomposition of $(I, p_i^{m_i})$).

Step 8: Return $\{Q_1^c, \ldots, Q_k^c\} \cup (\bigcup_i \{Q_1^i, \ldots, Q_{k_i}^i\})$. (As in the proof of Proposition 4.4.6, if $I \cap R = (0)$, which corresponds to *Case 1* in the proof, we have $I = (I, r) \cap I^{ec}$. $\{Q_1^c, \ldots, Q_k^c\}$ is the list of primary components of I^{ec}, $\{Q_1^i, \ldots, Q_{k_i}^i\}$ is the list of the primary components for $((I, r), p_i^{m_i}) = (I, p_i^{m_i})$ as explained above, and $(I, r) = \bigcap_i ((I, r), p_i^{m_i})$. Therefore, the union of these lists is a list of the primary components of I. We get $I = I^{ec} \cap (I, r) = I^{ec} \cap (\bigcap_i ((I, r), p_i^{m_i})) = (\bigcap_i Q_i^c) \cap (\bigcap_{i,j} Q_j^i)$.
In the case where $I \cap R \neq (0)$, which corresponds to *Case 2* in the proof of Proposition 4.4.6, we go from *Step 0* to *Step 4* and replace (I, r) by I. In this case, we have $I = \bigcap_i (I, p_i^{m_i}) = \bigcap_{i,j} Q_j^i$. Here, $\{Q_1^i, \ldots, Q_{k_i}^i\}$ is the list of the primary components

of $(I, p_i^{m_i})$ and we take $\{Q_1^c, \ldots, Q_k^c\} = \varnothing$ as noted in Step 0).

4.5 Algorithm for Computing the Associated Primes and Radical of an Ideal

In this section, we show that the algorithms introduced above also give the associated primes, hence, the radical of the ideal I to which the algorithms can be applied. If $I = \bigcap Q_i$ is an irredundant primary decomposition of I and $\sqrt{Q_i} = P_i$, then $\sqrt{I} = \bigcap P_i$, where P_i are the associated primes of I. Note that, the ZPD (Algorithm 4.3.2) returns an irredundant primary decomposition. The other algorithms PPD-0 (Algorithm 4.4.5) and PPD (Algorithm 4.4.7) return primary decompositions which may or may not be irredundant. For any primary decomposition $I = \bigcap Q_i$ we can obtain an irredundant primary decomposition of I by checking $Q_i \supset \bigcap_{j \neq i} Q_j$ using Gröbner basis techniques and removing the redundant component. Therefore, to obtain the associated primes and the radical of I, it suffices to know each $\sqrt{Q_i}$ for the decompositions of $I = \bigcap Q_i$ returned by the algorithms we introduced.

Proposition 4.5.1. *For each ideal $I \subset R[x]$ where one of Algorithm 4.4.5 or Algorithm 4.4.7 is applicable, it is possible to compute the associated primes and the radical of I.*

Proof. We need to show that we can compute $\sqrt{Q_i}$ for the decomposition $I = \bigcap Q_i$ returned by any of the algorithms mentioned above. As stated in the remark after Algorithm 4.3.2, this algorithm returns an irredundant decomposition $I = \bigcap Q_i$ and explicitly computes $\sqrt{Q_i}$. For Algorithm 4.4.7, as in the proof of Proposition 4.4.6, the algorithm expresses I as $I = \bigcap I_i$ such that Algorithm 4.4.5 can be applied to decompose each I_i, thus it suffices to show that the radicals of the primary components are computable for the output of Algorithm 4.4.5.

In the Algorithm 4.4.5 let $I \subset R[x_1, \ldots, x_n]$ be such that there are k variables x_i, where $I \cap R[x_i]$ is not zero-dimensional. If $k = 0$, then I is zero-dimensional and we can apply Algorithm 4.3.2 to compute primary decomposition and the associated primes. Also, if $n = 0$, then by assumption $I = I \cap R$ is (p)-primary, hence $(p) \subset R$ is the unique associated prime of I. Thus, if $k = 0$ or $n = 0$ the associated primes are computable by Algorithm 4.4.5. Proceeding by induction, assume that the

associated primes of I are computable by Algorithm 4.4.5 when $I \subset R[x_1, \ldots, x_n]$ and number of x_i such that $I \cap R[x_i]$ is not zero-dimensional is less than k, or when $I \subset R[x_1, \ldots, x_{n-1}]$ (note that $k = 0$ or $n = 0$ is the base step of induction). For the ideal $I \cap R[x_1, \ldots, x_n]$ ($n \geq 1$) with $k > 1$ variables x_i such that $I \cap R[x_i]$ is not zero-dimensional, following the arguments in the proof of Proposition 4.4.3, the algorithm first expresses I as $I = (I, r') \cap I^{ec}$. Here, $(I, r') \subset R[x_1, \ldots, x_n]$ is either the unit ideal or the algorithm can be applied to (I, r') in which case there are less than k variables x_i such that $(I, r') \cap R[x_i]$ is not zero-dimensional. In the former case, $I = I^{ec}$, hence the decomposition of I is the decomposition of I^{ec} which is explained below. In the latter case, by the inductive hypothesis, the associated primes of (I, r') are computable (the number of variables did not change but k is dropped).

The algorithm decomposes I^{ec} by decomposing $I^e = IR'_{(p)}[x']$ and then contracting it to $R'[x'] = (R[x_i])[x'] = R[x_1, \ldots, x_n]$. The algorithm can be applied to I^e which is in a polynomial ring with $n - 1$ variables. Hence, by the inductive hypothesis, the algorithm returns a primary decomposition $I^e = \bigcap \tilde{Q}_i$, where $\sqrt{\tilde{Q}_i} = \tilde{P}_i$ are explicitly computed. Then the primary decomposition of I^{ec} is $I^{ec} = \bigcap \tilde{Q}_i^c = \bigcap (\tilde{Q}_i \cap R'[x'])$. Using the general property $\sqrt{J^c} = (\sqrt{J})^c$ for the contracted ideals, we obtain $\sqrt{\tilde{Q}_i^c} = (\sqrt{\tilde{Q}_i})^c = \tilde{P}_i^c = \tilde{P}_i \cap R'[x']$. This is so, because $\tilde{P}_i$ are explicitly computed and we can compute the contractions $\tilde{P}_i \cap R'[x']$ by Proposition 3.2.11 as explained in *Step 6* of Algorithm 4.4.5. Therefore, the associated primes of I^{ec} can be explicitly computed. As a result, for $I = (I, r') \cap I^{ec}$, the algorithm returns primary decompositions of (I, r') and I^{ec} separately where the radical of each primary component is explicitly computable. This completes the proof of Algorithm 4.4.5 by induction. $\square$

CHAPTER 5

A SECOND APPROACH FOR COMPUTING PRIMARY DECOMPOSITION

5.1 Introduction

In this chapter, we give a summary of the methods and algorithms developed by Eisenbud, Huneke, and Vasconcelos in the paper entitled as "Direct Methods for Primary Decomposition" [4] for the computation of the equidimensional hull, the radical, the associated primes, and the primary decomposition of an ideal I in a polynomial ring $S = k[x_1, \ldots, x_n]$, where k is a field.

The algorithms by Gianni et al. in [13] for primary decomposition which we examined in the previous chapters include a PROJECTION process of intersecting an ideal I in $R[x_1, \ldots, x_n]$ with $R[x_1, \ldots, x_{n-1}]$ (using elimination theory and Gröbner basis). This PROJECTION process decreases the number of variables and inductively reduces the problem to one variable case eventually.

However, the methods developed by Eisenbud et al. [4] do not use such a PROJECTION process and are called direct methods. These methods only use the FACTOR and SYZYGY processes which are intrinsic in the problems related to primary decomposition.

As stated by Eisenbul et al. in [4], avoiding the PROJECTION process is desirable since the choice of the subring $R[x_1, \ldots, x_{n-1}]$ to which the ideal I is projected (contracted) is generic and it does not take into consideration the symmetry or special properties the generators of the ideal I may have, hence the use of PROJECTION results in less efficient algorithms.

Besides, the use of FACTOR process (factorizing a polynomial into irreducible fac-

tors) in the case of one variable polynomials in the problem of finding associated primes of an ideal (the last section in this chapter), the algorithms we will examine use computational techniques derived from computation of syzygies. Basically, for a submodule of a free module over the polynomial ring $S = k[x_1, \ldots, x_n]$, Gröbner basis of the submodule (with respect to a multiplicative order) can be computed using standard algorithms, and the corresponding syzygy for the generators of the given submodule is obtained as a result of these algorithms. (For $r_1, \ldots, r_m$ in the module M over $S = k[x_1, \ldots, x_n]$, the syzygy submodule is $\{(a_1, \ldots, a_m) \in S^m \mid a_1 r_1 + \cdots + a_m r_m = 0\}$).

Given that Gröbner bases and syzygies can be computed, the following can also be computed, and the algorithms we will examine make use of these computations:

1) For a given module M over S ("M is given " means, finitely many generators of M as an S-module are specified with finitely many relations among them which generate all S-linear dependence relations), a free resolution of M can be computed.

2) The codimension of an S-module M can be computed.

3) If I and J are ideals of S and $M \subset N$ are submodules, then $I \cap J$, $(M : J) = \{r \in N \mid jr \in M \text{ for all } j \in J\}$, $(M : N) = \{j \in S \mid jN \subset M\}$, $annM = (0 : M)$, $(M : J^\infty) = \bigcup_{n \geq 1} (M : J^n)$ can be computed.

4) Given an S-module M and $i \geq 0$, $Ext^i(M, S)$ can be computed first by constructing a free resolution of M, and then dualizing this sequence and computing $Kernel/Image$.

Using the algorithms of the above computations as tools, we now present the outline of the algorithms for computing the equidimensional hull, the radical, the associated primes and the primary decomposition of an ideal I of $S = k[x_1, \ldots, x_n]$. Note that the primary decomposition of an ideal is generalized to the primary decomposition of a submodule in a module (see [5] pp.383), and some results and algorithms we examine in this chapter are stated in this more general setting, although the aim is the primary decomposition of ideals in $S = k[x_1, \ldots, x_n]$.

We will omit the proofs of the theorems (which are often technical results involving

higher level homological algebra) and we focus on explaining the algorithms which are consequences of these theorems.

5.2 Finding the Equidimensional Hull of a Submodule

Throughout, we assume that all modules are finitely generated. We define *equidimensional hull of* 0 in a module M as the submodule N that consists of all elements whose annihilators have dimension less than the dimension of M. Alternatively, N is the intersection of all the primary components of 0 in M having maximal dimension. As to the modules, if $M' \subset M$ is a submodule, *equidimensional hull of* M' is defined as the preimage in M of equidimensional hull of 0 in M/M'.

If I is an ideal in ring S, then the equidimensional hull of I means the equidimensional hull of I in S as a submodule of S. We write $hull(N, M)$ or, if it is obvious from the context, $hull\ N$ for equidimensional hull.

The following theorem establishes a connection between hull and some other properties of primary decomposition and Ext.

Theorem 5.2.1 (Theorem 1.1. in [4])**.** *Let M be a module over a regular domain S, set I_e = ann $Ext^e_S(M, S)$:*

1) I_e has codimension $\geq e$ and $M/(0 :_M I_e)$ has no associated primes of codimension e. In particular, a prime ideal $P \subset S$ of codimension e is associated to M if and only if P contains I_e.

2) The equidimensional hull of 0 in M is the kernel of the natural map

$$\pi : M \longrightarrow Ext^c_S(Ext^c_S(M, S), S)$$

where c is the codimension of M.

3) If $I = ann_S M$, then hull(I) $= I_c$.

In particular, for any ideal I, hull(I) $= ann_S Ext^c_S(S/I, S)$.

We omit the proof of this theorem and concentrate on the applications of it. The proof is given in [4].

We can use Theorem 5.2.1 to compute equidimensional hull of an ideal, or to remove the components of dimension less than a given number. We can state the result in case of modules.

Algorithm 5.2.2 (Algorithm 1.2. in [4]). (Removing components of dimension less than e) Let M be a module over $S = k[x_1, \ldots, x_n]$, let e be an integer (in general bigger than or equal to $dimM$). We find a submodule N_e which is the intersection of the primary components of M that have dimension bigger than or equal to e.

$Set\ f := dimS,\ set\ N := 0 \subset M.$
while $f > e$ **do**
  $Compute\ Ext^f(M, S);$
  if $codim(Ext^f(M, S)) = f$ **then**
    $I_f := annihilator(Ext^f(M, S));$
    $N := (N :_M I_f);$
  end if
  $Decrement\ f;$
  $(Optional :\ Set\ M := M/N);$
end while
return $N.$

The following is a direct application of Theorem 5.2.1 to find the equidimensional hull of an ideal.

Algorithm 5.2.3 (Algorithm 1.3. in [4]). (Equidimensional hull of an ideal) Given an ideal $I \subset S = k[x_1, \ldots, x_n]$, we need to find the equidimensional hull of I which is the intersection of the primary components of I having maximal dimension.

c:= codim$I$;
return
ann $Ext^c_S(S/I, S)$.

If we replace S/I by M in the algorithm, then we can compute the equidimensional hull of the support of any module M. In fact, this algorithm is an application of third part of the Theorem 5.2.1 above. Following is another application that is used to find the equidimensional hull of 0 in a module.

Algorithm 5.2.4 (Algorithm 1.4. in [4]). (Equidimensional hull of 0 in a module)

Let M be a finitely generated module over $S = k[x_1, \ldots, x_n]$. We need to find the equidimensional kernel $N \subset M$.

c := codim M ;

π: $M \to Ext^c_S(Ext^c_S(M, S), S)$;

return N = kernelπ.

Here, π is the canonical map which can be computed in several different ways. One way is to form the comparison map between the dual of a free resolution of M and a free resolution of $Ext^c_S(S/I, S)$. Another way is to construct a polynomial subring of S, say T, where dim$T$ = dim N such that N is finitely generated over T and T can be constructed as a Noether normalization for $S/annN$. Afterwards, the kernel of the natural map of N into its double dual over T can be taken.

We can find an ideal whose associated primes are equal to the associated primes of a module which has a given codimension:

Algorithm 5.2.5 (Algorithm 1.5. in [4]). (Associated primes of given codimension) Given a finitely generated module M over $S = k[x_1, \ldots, x_n]$, we want to find an ideal whose associated primes are exactly the associated primes of M having codimension e.

$I_e :=$ ann $Ext^e_S(M, S)$;

if codim $I_e > e$ **then**

  return S ;

else

  return the equidimensional hull of I_e .

end if

Analysis of the Algorithm: This algorithm uses the second part of the first statement of Theorem 5.2.1, that is, for a prime ideal P of codimension e in S, P is associated to the module M if and only if P contains I_e.

Let P be an associated prime of M having codimension e. Then, since $codim(I_e) \geq e$ by Theorem 1.1., we analyze two cases: $codim(I_e) > e$ and $codim(I_e) = e$.

For the case $codim(I_e) > e$ (the first part of the algorithm), if $I_e \subseteq P$, where P is a prime of codimension e, then by definition of codimension of ideals, $codim I_e \leq$

$codimP$. Therefore, $e < codimI_e \leq codimP$ implying $e < codimP$ which is a contradiction. Therefore, there is no such prime ideal P in this case. Hence, M has no associated primes of codimension e. To express this result, the algorithm returns S (as an ideal of S, S has no primary decomposition, hence no associated primes. The set of associated primes of S and the set of associated primes of M which have codimension e are both empty).

For the case where $codim(I_e) = e$ (the second part of the algorithm), let $I_e \subset P$ where P is a prime ideal of codimension e. Since $codimI_e = codimP = e$ by our uppermost assumption on P and $I_e \subset P$, we can conclude P is a minimal prime containing I_e. Since any prime ideal containing I_e contains a minimal prime ideal associate to I_e (see [10] pg. 52), we obtain that P is an associated prime of I_e. Therefore, the equidimensional hull of I_e is the desired ideal, since the associated primes are the minimal primes containing I_e, and have the same codimension as I_e. Equivalently, (as shown above), it consists of the primes P containing I_e which have codimension e, hence the associated primes of M which have codimension e by part 1 of Theorem 5.2.1.

Note that we compute the equidimensional hull of I_e by Algorithm 5.2.3

5.3 The Radical of an Ideal

To find the radical of an ideal I in a polynomial ring S, we state two methods here.

Algorithm 5.3.1 (Algorithm 2.2. in [4]). (Radical of a generically complete intersection) Let J be an unmixed ideal of pure dimension c which is a generically complete intersection where $J = (f_1, \ldots, f_m) \subset k[x_1, \ldots, x_n]$.

$Set\ J_{n-c}$:= the ideal of $c \times c$ minors of the Jacobian matrix
$\partial(z_1, \ldots, z_d, f_1, \ldots, f_m)/\partial(x_1, \ldots, x_n)$ where $z_1, \ \ldots \ z_d$ are general linear forms.
return $radJ := (J : J_{n-c})$.

Proposition 5.3.2 (Proposition 2.3. in [4]). *Let $J \subset I \subset S = k[x_1, \ldots, x_n]$ be ideals of the same dimension, let J be equidimensional with radical J'.*

In this case, equidimensional hull of the radical of I is given by the following formula:

$$\textit{equidimensional rad(I)} = (J' : (J' : I)).$$

Proof. For this proof, we use the last statement of Lemma 5.3.3 below. Let $J' = \bigcap P_i$ where P_i are all prime ideals containing J, by definition of radical ideal. In fact, this is equal to the intersection of minimal prime ideals of J. So, let $J' = P_1 \cap \cdots \cap P_t$ where P_i are minimal primes of J, $1 \leq i \leq t$. Since J is equidimensional, $dimP_i = dimJ$, for all i, where $1 \leq i \leq t$. By assumption, $dimJ = dimI$, so let $dimP_i = dimJ = dimI = d$. By Lemma 5.3.3.c, $(J' : I) = \bigcap Q_i$, where Q_i are prime ideals such that $J' \subset Q_i$, and $I \not\subset Q_i$. Let $P_1, \ldots, P_s$, $s \leq t$ be the prime ideals among $P_1, \ldots, P_t$ such that $J' \subset P_i$ and $I \not\subset P_i$ and let $P_{s+1}, \ldots, P_t$ be the ones such that $I \subset P_j$ for $(s+1) \leq j \leq t$. $P_1, \ldots, P_s$ are among the above mentioned ideals Q_j's. Since Q_j is a prime ideal containing J', there exists prime ideals P_{i_j} such that $P_{i_j} \subset Q_j$ for some i_j, where $1 \leq i_j \leq t$. This is because P_i's are minimal primes of J (or J'). In fact, $1 \leq i_j \leq s$, since these P_{i_j} cannot contain I. Otherwise, $I \subset P_{i_j} \subset Q_j$ implies $I \subset Q_j$ which contradicts the result obtained above by using Lemma 5.3.3.c. Thus, $(J' : I) = \bigcap Q_j = P_1 \cap \cdots \cap P_s$ since each Q_j contains a minimal prime P_i (see [10], pg.52) . Let $K = (J' : I)$. Hence, $K = P_1 \cap \cdots \cap P_s$ by above. Then, $(J' : K) = \bigcap \widetilde{Q_j}$ where $\widetilde{Q_j}$ are prime ideals such that $J' \subset \widetilde{Q_j}$ and $K \not\subset \widetilde{Q_j}$ by Lemma 5.3.3.c. So, there exists prime ideals P_{i_j} such that $P_{i_j} \subset \widetilde{Q_j}$ for some i_j, where $(s+1) \leq i_j \leq t$. Here, $K \not\subset P_{i_j}$; otherwise, $K \subset P_{i_j} \subset \widetilde{Q_j}$ but this contradicts the above result obtained by Lemma 5.3.3.c. We obtain, $(J' : K) = \bigcap \widetilde{Q_i} = \bigcap P_i$ such that $K \not\subset P_i$. We know that $P_1, \ldots, P_s$ all contain K. If $(P_1 \cap \cdots \cap P_s) \subset P_i$ for some $1 \leq i \leq t$, then $P_j \subset P_i$ for some $1 \leq j \leq s$. This is because if a prime ideal contains an intersection of prime ideals, then one of the primes in the intersection is contained in the prime ideal that contains the intersection. Since J is equidimensional, $dimP_i = dimP_j$, therefore, $P_i = P_j$. Thus, $(J' : (J' : I)) = \bigcap \widetilde{Q_j} = P_{s+1} \cap \cdots \cap P_t$, where $P_{s+1}, \ldots, P_t$ are the minimal primes of J containing I and they all have dimension d. In fact, it is the intersection of the minimal primes of I having dimension d. We have $dimP_{s+1} = \cdots = dimP_t = d = dimI = dimJ$.

Now, *(equidimensional radical of I)* = $\bigcap \widetilde{P_i}$, where $\widetilde{P_i}$ is a minimal prime of I such that $dim\widetilde{P_i} = d$. Since $J \subset I$ and $dimI = dimJ$, each $\widetilde{P_i}$ is also a minimal prime of

J. Therefore, $\{P_{s+1}, \ldots, P_t\} = \{\widetilde{P}_i\}$ which means that *(equidimensional radical of* I*)* $= (J' : (J' : I))$. □

For completeness, we include the following technical lemma which plays an important role in the proof of the above proposition.

Lemma 5.3.3 (Lemma 2.4.c in [4])**.** *For ideals* I *and* J *in a Noetherian ring* R*, if* I *is radical, then* $(I : J)$ *is radical and*

$$(I : J) = \bigcap P_i$$

where P_i *ranges over all prime ideals containing* I*, but not containing* J*.*

Algorithm 5.3.4 (Algorithm 2.5. in [4]). (Reduction of equidimensional radical to complete intersection case) Given ideals $J \subset I \subset k[x_1, \ldots, x_n]$, where J is a complete intersection, and I and J have the same codimension, we compute the equidimensional hull of the radical of I as follows:

Compute

$J' := radJ$ by Algorithm 5.3.1;

return

equidimensional radical $I := (J' : (J' : I))$.

This is an implementation of Proposition 5.3.2 above.

The following theorem, which is proved in [4], plays the central role in the second method for computing the radical of an ideal that we will present in this section.

Theorem 5.3.5 (Theorem 2.7. in [4])**.** *Let* S *be a polynomial ring over a perfect field* k*, let* $I \subset S$ *be an ideal whose dimension is* d*. If the characteristic of* k *is nonzero, suppose that the nilradical of* S/I *is generated by elements whose index of nilpotency is less than the characteristic of* k*. If for some integer* $a \geq d$ *we have*

$$dim\, \mathscr{J}_{a+1}(I) < d$$

then

$$I_1 := (I : \mathscr{J}_a(I))$$

has the same equidimensional radical as I*. Moreover, if* $a = d$ *then* I_1 *is radical in dimension* d*, i.e. the primary components of* I_1 *having dimension* d *are prime.*

Remark: Here, if I is generated by the sequence of relations $f = f_1, \ldots, f_r$ then $\mathscr{J}(f)$ stands for the *Jacobian matrix* of this sequence, i.e. it is the $n \times r$ matrix having the partial derivative $\frac{\partial f_j}{\partial x_i}$ as the term in the ith row and jth column. On the other hand, $\mathscr{J}_a(f)$ is the ideal generated by $(n-a) \times (n-a)$ minors of $\mathscr{J}(f)$ and we have $\mathscr{J}_a(I) = \mathscr{J}_a(f) + I$.

The following algorithm is an application of this theorem for finding the radical of an equidimensional ideal.

Algorithm 5.3.6 (Algorithm 2.9 in [4]). (Equidimensional Radical) Let $I \subset S = k[x_1, \ldots, x_n]$ be an equidimensional ideal. We find the equidimensional radical U of I which is equal to the intersection of all primes containing I whose dimensions are the same as the dimension of I.

$a := n - 1$
$d := dim I$
while $a > d$ **do**
  while $dim\, \mathscr{J}_a(I) = d$ **do**
    $I := (I : \mathscr{J}_a(I))$;
  end while
  $decrement\ a$;
end while
$I := (I : \mathscr{J}_d(I))$;
return I.

Analysis of the Algorithm: First of all, $I \subset \mathscr{J}_0(I) \subset \mathscr{J}_1(I) \subset \cdots \subset \mathscr{J}_{n-1}(I) \subset \mathscr{J}_n(I) = S$ and $d = dim(I) \geq dim\, \mathscr{J}_0(I) \geq \cdots \geq dim\, \mathscr{J}_{n-1}(I) \geq dim\, \mathscr{J}_n(I) = dim(S) = -1$ (by convention) imply that there exists a largest value of a such that $dim\, \mathscr{J}_{a+1}(I) < d$ (hence $dim\, \mathscr{J}_a(I) = d$). The second $while$ loop in the algorithm starts from this largest value of a ($a \leq n-1$). Since the ring is Noetherian, every ascending ideal chain stabilizes after finitely many steps. Let $I = I_0 \subset I_1 \subset \cdots \subset I_t = I_{t+1}$ be the ideal chain in S, defined by $I = I_0$ and $I_{i+1} = (I_i : \mathscr{J}_a(I_i))$ for $i \geq 0$, $0 \leq i \leq t$. Then we have $I_t = (I_t : \mathscr{J}_a(I_t))$ since the chain is stabilized at I_t ($I_t = I_{t+1}$). $I = I_0 \subset I_1 \subset \cdots \subset I_t$ and $dim\, \mathscr{J}_{a+1}(I) < d$ imply $d > dim\, \mathscr{J}_{a+1}(I) \geq dim\, \mathscr{J}_{a+1}(I_1) \geq \cdots \geq dim\, \mathscr{J}_{a+1}(I_t)$, that is $dim\, \mathscr{J}_{a+1}(I_i) < d$

for all i (Note that, $I_k \subset I_{k+1}$ implies $\mathscr{J}_{a+1}(I_k) \subset \mathscr{J}_{a+1}(I_{k+1})$ since we can extend a set of generators of I_k to a set of generators of I_{k+1}, hence the Jacobian matrix for $\mathscr{J}_{a+1}(I_k)$ is a submatrix of the Jacobian matrix of $\mathscr{J}_{a+1}(I_{k+1})$. Note also that, $\mathscr{J}_{a+1}(I_k)$ is independent of the choice of generators for I_k. $\mathscr{J}_{a+1}(I_k) \subset \mathscr{J}_{a+1}(I_{k+1})$ implies $dim\, \mathscr{J}_{a+1}(I_k) \geq dim\, \mathscr{J}_{a+1}(I_{k+1})$).

Note that, throughout this $while$ loop, the ideal I is modified by assigning the new value of I as $(I : \mathscr{J}_a(I))$ for some value of a where I satisfies the conditions of Theorem 5.3.5 above. Under these conditions, I and $(I : \mathscr{J}_a(I))$ have the same equidimensional radical due to Theorem 5.3.5 above. Hence, $dim(I) = dim(I : \mathscr{J}_a(I))$. As a result, $dim I_i = d$ for all i, where $0 \leq i \leq t$, and the equidimensional radicals of I_i are the same for all i. If we can show that $dim\, \mathscr{J}_a(I_t) < d$ then the $while$ loop terminates at I_t, and we can decrement a.

Since $I_t \subset \mathscr{J}_a(I_t)$ by definition of $\mathscr{J}_a(I_t)$, we have $dim\, \mathscr{J}_a(I_t) \leq dim I_t = d$. To prove $dim\, \mathscr{J}_a(I_t) < d$, assume $dim\, \mathscr{J}_a(I_t) = dim I_t = d$. Thus, there exist prime ideals $P_0, \ldots, P_d$ such that:

$$I_t \subset \mathscr{J}_a(I_t) \subset P_0 \subset \cdots \subset P_d$$

Since the dimension of $\mathscr{J}_a(I_t)$ and I_t are assumed to be equal, P_0 is a minimal prime of I_t. Therefore, P_0 is an associated prime of I_t, too (see [10] pg.52). Hence, $P_0 = (I_t : q)$ for some $q \in S - I_t$. (If q were in I_t then $(I_t : q)$ would be S which is not possible, since P_0 is a prime ideal of S). Therefore, $\mathscr{J}_a(I_t) \subset P_0 = (I_t : q)$. This means, for every $x \in P_0$, $qx \in I_t$. Hence, for every $x \in \mathscr{J}_a(I_t)$, $qx \in I_t$. So, $q \in (I_t : \mathscr{J}_a(I_t)) = I_t$ which is a contradiction since $q \in S - I_t$. Therefore, $dim\, \mathscr{J}_a(I_t) < dim I_t = d$. As a result, in the sequence $I \subset I_1 \subset \cdots \subset I_t = I_{t+1}$ there exists $i \leq t$ such that $dim\, \mathscr{J}_a(I_i) < d$. This proves that the second $while$ loop terminates at I_i for the smallest such i. Indeed, $i = t$ by the defining condition of the $while$ loop (I_{i+1} exists if $dim\, \mathscr{J}_a(I_i) = d$).

If we write $\mathscr{J}_a(I_t) = \mathscr{J}_{a+1-1}(I_t)$, then we can apply Theorem 5.3.5 above by substituting $I = I_t$ and taking $a - 1$ in place of a, indeed we keep decrementing a until we get $dim\, \mathscr{J}_a(I_t) = d$ (here, $dim\, \mathscr{J}_{a+1}(I_t) < d$). For this decremented value of a, we start the second loop again which gives the sequence of ideals $\mathcal{I}_0 = I_t$, $\mathcal{I}_{k+1} = (\mathcal{I}_k : \mathscr{J}_a(\mathcal{I}_k))$ for $k \geq 0$. This $while$ loop terminates as explained above.

By the same argument, we keep decrementing a until a becomes $d+1$. Suppose the ideal that the algorithm gives at the end of the first $while$ loop where $a = d+1$ is J, then we have $dim\, \mathscr{J}_{d+1}(J) < d$, hence by Theorem 5.3.5 above and by taking $a = d$ we obtain the ideal $J_1 = (J : \mathscr{J}_d(J))$ that is, an ideal which is radical in dimension d, and J and J_1 have the same equidimensional radical. Note that throughout the algorithm, the equidimensional radical of the ideals do not change by Theorem 5.3.5 above. Hence, the equidimensional radical of I is equal to the equidimensional radical of J_1 which equals to the equidimensional hull of J_1 since J_1 is radical in dimension d, where $d = dimI = dimJ_1$. Since the ideal I we started with is equidimensional, J_1 is also equidimensional, hence *rad(I) = equidimensional rad(I) = equidimensional hull of* $J_1 = J_1$.

Remark: If we apply the above algorithm to an ideal I which is not necessarily equidimensional, then the equidimensional radical of I is given by the equidimensional hull of J_1, where J_1 is the ideal that the above algorithm returns.

Now it is possible to compute the following invariants of any given module:

Algorithm 5.3.7 (Algorithm 2.10. in [4]). (Finding the intersection of the primes associated to M having codimension e)

$I_e := annExt^e_S(M, S)$.
if $codimI_e = e$, **then**
  return $the\ radical\ of\ the\ equidimensional\ hull\ of\ I_e$;
else
  return S.
end if

Analysis of the Algorithm: By Algorithm 5.2.5, we find the ideal I whose associated primes are the associated primes of M having codimension e.

The aim of Algorithm 5.3.7 is to find the intersection of these ideals. Since I is equidimensional, we can use Algorithm 5.3.6 above. Furthermore, since all associated primes have equal dimension, by Algorithm 5.3.6, we find the equidimensional radical of I . This gives us, by definition, the intersection of the associated primes of M having codimension e, as desired.

Computation of the Radical of an Ideal I: Using Algorithm 5.3.7, we can compute the radical of an ideal I as follows:

For each e, where $0 \leq e \leq dimI = d$, compute the intersection of the associated primes of I having dimension e, say K_e. So, $rad(I) = \bigcap_{e=0}^{d} K_e$.

Algorithm 5.3.8 (Algorithm 2.11. in [4]). (Finding the intersection of the minimal associated primes of M having dimension e)

$Compute\ the\ ideals\ J_e\ and\ J_{e+1},\ where\ J_e\ is\ the\ intersection\ of$
$the\ associated\ primes\ of\ M\ having\ dimension\ \geq e.$
$(That\ is,\ J_e = \bigcap K_i\ , i \geq e,\ where\ K_i\ is\ computed\ by\ Algorithm\ 5.3.7$
$and\ it\ is\ the\ intersection\ of\ the\ primes\ associated\ to\ M\ having\ dimension\ i).$
return $(rad(J_e) : J_{e+1})$.

Analysis of the Algorithm: We first define J_e as above. $J_e = \bigcap_{i \geq e} K_i$. Each K_i can be computed by Algorithm 5.3.7 above. Hence, we can compute J_e and J_{e+1}. Note that, J_e and J_{e+1} are radical, since they are the intersections of prime ideals. Hence, $rad(J_e) = J_e$ and the algorithm returns $(J_e : J_{e+1})$. Now, J_e is the intersection of the associated primes of M which have dimension $\geq e$. Hence, J_e is radical. Similarly, J_{e+1} can be found. Hence, by Lemma 5.3.3 above, $(J_e : J_{e+1}) = \bigcap P_i$ where $J_e \subset P_i$ and $J_{e+1} \not\subset P_i$.

Claim: $(J_e : J_{e+1}) = \bigcap P_i$, where P_i is a minimal prime containing J_e and $J_{e+1} \not\subset P_i$.

Proof of Claim: Let P_i be a prime that is not minimal. Let $J_e = \bigcap Q_k \subset P_i$. P_i contains a minimal prime containing J_e, say $\widetilde{P}_i$. If P_i does not contain J_{e+1} then $\widetilde{P}_i$ does not contain J_{e+1}. This proves the claim.

To prove that $(J_e : J_{e+1})$ equals the intersection of the minimal primes of dimension e, we proceed as follows:
Let $J_e = \bigcap Q_k$. Since $J_e = \bigcap Q_k \subset P_i$ implies $Q_{k_i} \subset P_i$. (Here, Q_k and P_i are prime ideals). We get $Q_{k_i} = P_i$, since P_i is a minimal prime containing J_e. We have, $(J_e : J_{e+1}) = \bigcap P_i$, where P_i is a minimal prime containing J_e and not containing J_{e+1}. For such a P_i, $J_e \subset P_i$. P_i is a minimal prime containing J_e implies that $P_i = Q_{k_i}$ for some k_i, where $J_e = \bigcap Q_k$ (Q_k are associated primes). For such a P_i, we have the following three cases:

Case 1: $dimP_i > e$. This implies $J_{e+1} \subset P_i$ which contradicts $J_{e+1} \not\subset P_i$. $J_{e+1} = \bigcap Q_j$ where Q_j are the associated primes of M having dimension $\geq e$. $dimP_i > e$ also implies $P_i = Q_j$ for some j as shown above. Thus, $J_{e+1} \subset P_i$, where $dim(P_i) \geq e+1$.

Case 2: $dimP_i = e$ and $Q_{k_i} = P_i$ is not a minimal associated prime of M of dimension e. Then Q_{k_i} contains a minimal prime of M, say Q_{t_i}, where Q_{t_i} is a minimal prime of M. Here, $dimQ_{t_i} > e$, thus, $J_{e+1} \subset Q_{t_i}$. Hence, $J_{e+1} \subset Q_{t_i} \subset Q_{k_i} = P_i$. Again, we get a contradiction to $J_{e+1} \not\subset P_i$.

Case 3: $dimP_i = e$ and P_i is a minimal associated prime of M.

Claim:$J_{e+1} \not\subset Q_{k_i} = P_i$.

Proof of Claim: Otherwise, if $J_{e+1} = \bigcap \widetilde{Q_k} \subset Q_{k_i}$, where $dim\widetilde{Q_k} \geq e+1$, and $\widetilde{Q_k}$ are associated primes of M, then there exists $\widetilde{Q_{m_i}}$ such that $\widetilde{Q_{m_i}} \subset Q_{k_i}$ and $dim\widetilde{Q_{m_i}} \geq e+1$ with $\widetilde{Q_{m_i}}$ being an associated prime of M. However, this contradicts Q_{k_i} being a minimal associated prime of M. This proves the claim.

As a result, $(J_e : J_{e+1}) = \bigcap P_i$, where $J_e \subset P_i$ and $J_{e+1} \not\subset P_i$ and these P_i are the minimal associated primes of M having dimension e.

Algorithm 5.3.9 (Algorithm 2.12. in [4]). (Finding the intersection of the embedded primes of M having dimension e)

Let K_1 be the ideal that is the intersection of associated primes of M having dimension e which can be computed by Algorithm 5.3.7;
Let K_2 be the ideal that is the intersection of minimal primes of M having dimension e which can be computed by Algorithm 5.3.8;
return $(K_1 : K_2)$.

Analysis of the Algorithm: Since K_1 is radical, $(K_1 : K_2)$ is equal to the intersection of prime ideals containing K_1 and not containing K_2 by Lemma 5.3.3 above. To compute K_1 we can run the Algorithm 5.3.7 above for codimension $n-e$. Let $K_2 = P_1 \cap \cdots \cap P_s$ and $K_1 = P_1 \cap \cdots \cap P_s \cap \cdots \cap P_t$. Hence, $(K_1 : K_2) = (\bigcap_{i=1}^{t} P_i : K_2) = \bigcap_{i=1}^{t}(P_i : K_2)$. $(P_i : K_2) = S$ if $1 \leq i \leq s$ since $K_2 \subset P_i$. $(P_i : K_2) = P_i$ if $s+1 \leq i \leq t$ since $K_2 \not\subset P_i$. (Otherwise, if $K_2 = P_1 \cap \cdots \cap P_s \subset P_i$ then $P_j \subset P_i$ for some $1 \leq j \leq s$. Hence, $P_j = P_i$ (they are prime ideals with the same dimension)

which yields a contradiction, since $i > s$.) Therefore, $(K_1 : K_2) = (\bigcap_{i=1}^{t} P_i : K_2) = S \cap \cdots \cap S \cap P_{s+1} \cap \cdots \cap P_t$, where $P_{s+1}, \ldots, P_t$ are the embedded primes of M.

5.4 Primary Decomposition

From now on, we will be able to find primary decompositions with the help of aforementioned techniques and a technique for finding a maximal ideal containing a given ideal.

The process of finding a primary decomposition for an ideal I consists of two parts: First, we find the individual associated primes; then we find a primary component for each associated prime found in the first part.

The second part of this process can be done with the above developed techniques and the following claim.

Claim: A primary component for the ideal I with the associated prime P is of the form:

$$Q_m := Equidimensional\ hull(I + P^m)$$

for sufficiently large m.

Proof of Claim: The proof of this claim can be found in [11]. We show below that Q_m is P-primary. Let $E(I)$ stand for the *equidimensional hull* of an ideal I. Let $(I + P^m) = J_m$ and let $J_m = T_1 \cap \cdots \cap T_k$ be an irredundant primary decomposition of J_m. Also, let $Q_m = E(J_m) = T_1 \cap \cdots \cap T_s$, where T_j are the maximum dimensional primary components of J_m for $1 \leq j \leq s$. We have $P^m \subset J_m$ and $rad(P^m) = P$, so $rad(P^m) = P \subset rad(J_m)$. On the other hand, $I \subset P$ (since P is an associated prime of I) and $P^m \subset P$ implies $I + P^m = J_m \subset P$. Hence, $rad(J_m) \subset rad(P) = P$ (since P is prime). Therefore, $rad(J_m) = P$. So, $P = \bigcap rad(T_i)$ implies $rad(T_i) = P$ for some i (see [10], pg.8). Thus, $rad(T_i) = P \subsetneq rad(T_j)$ for all $i \neq j$. Hence, $dim(rad(T_j)) < dim(rad(T_i))$ for all $i \neq j$. Therefore, $rad(T_i)$ is the unique associated prime of J_m which has the maximum dimension. As a result, $E(J_m) = Q_m = T_i$ where T_i is primary and $rad(T_i) = P$. This proves that Q_m is P-primary.

Here, Q_m is uniquely defined if P is a minimal prime for I. Also, Q_m is in any case

a P-primary ideal. Bounds for the required m can be directly given, but for practical purposes it is better to guess it and check the sufficiency by the following criterion:

Let Q be a P-primary ideal containing I. Then Q is a primary component for I if and only if the natural map

$$(I_{[P]} : P^{\infty})/I_{[P]} \longrightarrow S/Q$$

is a monomorphism [11]. An algorithm to compute $I_{[P]}$ is developed in §3 at [4].

As to find the associated primes of I, we can suppose that S is a polynomial ring. Since we can find the intersection of all the associated primes of a given dimension by Algorithm 5.3.7 above, it suffices to find the individual components of an equidimensional radical ideal I. If we know the associated prime ideals of the homogenization of the ideal I, then we can obtain the associated prime ideals of I. Hence, we may assume I is homogeneous. By correspondence, finding the prime components of I is equivalent to finding the minimal primes of the ring $R := S/I$.

First, using the method of [16], (also see [7]), we can compute the integral closure R' of $R := S/I$.

The minimal primes of R are the intersections of R with the minimal primes of R'. Hence, it is enough to find the minimal primes of a reduced integrally closed graded ring which is R' here.

Any integrally closed ring is a finite product of integral domains (see [9], pp.64). Hence, minimal primes of R' are in one-to-one correspondence with the indecomposable idempotents of R'.

To illustrate this, if we let $R' = R_1 \times \cdots \times R_k$, where R_i are integral domains, and let $I \subset R'$ be an ideal, then $I = I_1 \times \cdots \times I_k$, where I_i is an ideal of R_i. Obviously, I is prime if and only if R'/I is an integral domain. Hence, $R'/I = R_1/I_1 \times \cdots \times R_k/I_k$, where $R_i/I_i = (0)_{R_i}$ for all but one i, which means $I_i = R_i$. Therefore, if I is prime, then $I = R_1 \times \cdots \times R_{i-1} \times P_i \times R_{i+1} \times \cdots \times R_k$, where P_i is a prime of R_i. Thus, if I is minimal, then $I = R_1 \times \cdots \times R_{i-1} \times (0)_{R_i} \times R_{i+1} \times \cdots \times R_k$, since integral domains have only one minimal prime which is (0).

Hence, a minimal prime ideal I of R' can be matched to an indecomposable idempo-

tent element of R' which is $\hat{e_i} = (0_{R_1} \times \cdots \times 0_{R_{i-1}} \times e_{R_i} \times 0_{R_{i+1}} \times \cdots \times 0_{R_k})$, where e_{R_i} is the multiplicative identity of R_i. The correspondence is given by $I = (0 : \hat{e_i})$ in R'.

Any idempotent has degree 0, since $e^2 = e$ and the ring R' is graded. Hence, idempotents are elements of the finite dimensional k-algebra $A := R'_0$, where R'_0 is the subgroup of R' that consists of the elements having degree 0.

The minimal ideals of A (which is a product of fields since it is a reduced finite dimensional k-algebra) are generated by indecomposable idempotents, i.e. the ones which can not be written as a sum of any other idempotents. To find these minimal ideals without using the idempotents, we need to find the intersection of all finitely many maximal ideals of A except one. This is because the maximal ideals of A are of the form:

$$F_1 \times \cdots \times F_{i-1} \times (0)_{F_i} \times F_{i+1} \times \cdots \times F_k$$

where F_i are fields.

To compute the minimal primes of R', let $\mathcal{N}$ be a minimal ideal of A, choose a nonzero element $s \in \mathcal{N}$. Thus,

$$P = (0 : s^\infty)$$

gives a minimal prime ideal of A.

Now, we state a method to find the maximal ideals of a finite dimensional k-algebra, $A = k[x_1, \ldots, x_n]/I$. There is a different approach to this problem which is mentioned in [8]. The method we mention here is probabilistic.

We can assume that A is reduced, since we are able to compute radicals by algorithms in the second section. Thus, A is a product of fields.

Let $x \in A$ be any random element and let $x \notin k$. Determine whether x is a zero divisor by computing Gröbner basis for $(I : x)$. Note that x is a zero divisor in $k[x_1, \ldots, x_n]/I$ if and only if $(I : x) \neq I$.

If x is a zero divisor, then let $I := (I, x)$ and consider the following quotient $A = k[x_1, \ldots, x_n]/(I, x)$. Note that, since x is a zero divisor in $A = k[x_1, \ldots, x_n]/I$,

$(I, x) \neq k[x_1, \ldots, x_n]$. Hence, $k[x_1, \ldots, x_n]/(I, x)$ is a finite dimensional k-algebra with a smaller dimension. We proceed by induction on $dim_k A$. $dim_k A = 1$ implies A is a field, hence (0) is a maximal ideal in A (base step).

Else if x is not a zero divisor, then determine $dim_k A$ by computing a Gröbner basis for the ideal defining A. Now, let $r = r(x)$ be the smallest integer such that the powers

$$1, x, x^2, \ldots, x^r$$

are linearly dependent. If $r(x) = dim_k A$, then the linear dependence relation can be stated as $q(x) = 0$, where $q(t)$ is a polynomial in one variable t. Hence, $A \cong k[t]/(q)$. If q is a product of nonconstant polynomials as $q = p_1 p_2$, then $p_1(x)p_2(x) = 0$. Therefore, $p_1(x)$ is a zero divisor, and we return to the first case. However, if q is irreducible, then A is a field and (0) is a maximal ideal.

Hence, provided that x is a zero divisor or $r(x) = dim_k A$, we can proceed the algorithm and reach the result by induction on $dim_k A$. Otherwise, we choose x again and execute the above method.

REFERENCES

[1] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal . (German) [An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal]*. PhD thesis, Universitat Innsbruck, Innsbruck, Austria, 1965.

[2] T. Coquand and H. Lombardi. A short proof for the krull dimension of a polynomial ring. *The American Mathematical Monthly*, 112(9):826–829, 2005.

[3] D. O. David Cox, John Little. *Ideals, Varieties and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer Science+Business Media, LLC, New York, USA, 2007.

[4] W. V. David Eisenbud, Craig Huneke. Direct methods for primary decomposition. *Inventiones Mathematicae*, 110:207–235, 1992.

[5] T. W. Hungerford. *Algebra*. Springer Science & Business Media, 2003.

[6] K. Igusa. Math 205b (commutative algebra), spring 2010, 2010. http://people.brandeis.edu/∼igusa/Math205bS10/Math205b_S10_71.pdf.

[7] W. V. V. Joseph P. Brennan. Effective computation of the integral closure of a morphism. *Journal of Pure and Applied Algebra*, 86:125–134, 1993.

[8] D. Lazard. Solving zero-dimensional algebraic systems. *Journal of Symbolic Computation*, 13(2):117–131, 1992.

[9] H. Matsumura. *Commutative Ring Theory*. The Press Syndicate of The University of Cambridge, 2000.

[10] I. M. M.F. Atiyah. *Introduction to Commutative Algebra*. Addison-Wesley Publishing Company, 1969.

[11] A. T. Nazeran Idrees, Afshan Sadiq. On primary composition of modules. unpublished, 2014.

[12] P. S. Oscar Zariski. *Commutative Algebra, Volume I*. Springer New York, 1975.

[13] G. Z. Patrizia Gianni, Barry Trager. Gröbner bases and primary decomposition of polynomial ideals. *Journal of Symbolic Computation*, 6:149–167, 1988.

[14] D. A. Spear. A constructive approach to commutative ring theory. In *Proceedings of the 1977 MACSYMA Users' Conference*, NASA CP-2012, pages 369–376, Washington, DC, 1977. National Aeronautics and Space Administration.

[15] W. Trinks. Über B. Buchbergers Verfahren, Systeme algebraischer Gleichungen zu lösen. *Journal of Number Theory*, 10:475–488, 1978.

[16] W. Vasconcelos. Computing the integral closure of an affine domain. In *Proceedings of the American Mathematical Society*, volume 113 of *0002-9939/91*, pages 633–638. American Mathematical Society, 1991.

[17] W. V. Vasconcelos, D. R. Grayson, M. Stillman, D. Eisenbud, and J. Herzog. *Computational Methods in Commutative Algebra and Algebraic Geometry*. Springer-Verlag, Berlin, Heidelberg, 1997.

[18] G. Zacharias. Generalized Gröbner bases in Commutative Polynomial Rings. Bachelor's thesis, Massachusetts Institute of Technology, MIT Dept. of Comp. Sci., 1978.