Gröbner Bases, Elimination, and Generic Initial Ideals

Stephanie Patricia Shand
Falls Church, Virginia

A Thesis presented to the Graduate Faculty
of the University of Virginia in Candidacy for the Degree of
Master of Science

Department of Mathematics

University of Virginia May, 2021

Contents

Acknowledgements

Throughout the writing of this thesis I have received a great deal of support and assistance.

I would first like to thank my thesis advisor, Dr. Craig Huneke. Thank you for your patience and your helpful comments and suggestions throughout this process.

I would like to acknowledge my other committee member, Dr. Mikhail Ershov. Thank you for your comments and feedback on my thesis.

I would also like to thank Sarasij Maitra for his help in my understanding of Macaulay2 and being a contact for me throughout my writing.

In addition, I would like to thank all the friends I have made throughout my studies in Mathematics.

Finally, I could not have completed this thesis without the support of my mother, father, and sister. You all encourage and inspire me to find and do what I love. Thank you so much for helping me get to where I am today and supporting me every step of the way.

Abstract

Gröbner bases are a tool for doing explicit calculations in a polynomial ring over a field. Gröbner bases can be used to calculate two specific computational problems:

1. (Membership Problem) Given an element f in a polynomial ring, do we know whether f is in a particular ideal I of the polynomial ring?

2. (Elimination) Given a finite set of generators for an ideal $I \subset k[x_1, \ldots, x_n]$, can we find a finite set of generators for $I \cap k[x_{r+1}, \ldots, x_n]$, $1 \leq r \leq n-1$?

Even though computational problems are an important application of Gröbner bases, they can also be used to simplify some very well-known theorems such as Hilbert's Basis Theorem and the natural isomorphism between the ring of elementary symmetric functions over a field and the symmetric polynomials. Gröbner bases are also used for theoretical problems, although this thesis will focus on the computational problems.

In this thesis we will define a Gröbner basis and prove several theorems related to the topic such as Dickson's Lemma, the Division Algorithm, Buchberger's Criterion, the Elimination Theorem, and the Existence of Generic Initial Ideals. Examples are also provided throughout the thesis for better understanding of the topic.

Introduction

In this thesis we will define a Gröbner basis and we will prove several of the theorems surrounding the topic.

Starting in Chapter 1 we start with some setup for introducing Gröbner bases such as defining a monomial, a monomial ordering, the initial term, and the initial ideal. In Chapter 2 we introduce the idea of a Gröbner basis starting off with its definition. Then we prove Dickson's Lemma, a theorem related to a non-empty set of monomials having minimal elements, and a theorem stating that the set of monomials not in the initial ideal of an ideal I of a monomial ring $R = k[x_1, \ldots, x_n]$ is a k-basis for R/I. In Chapter 3 we introduce the three basic monomial orderings. We also prove the a general (multi-variable) version of the well-known Division Algorithm, the specific case of the Hilbert Basis Theorem in which our polynomial ring is over a field, and the Criterion for Ideal Membership which proves that a Gröbner basis of an ideal reduces each element of the ideal to zero. In Chapter 4 we state and prove an algorithm to compute a Gröbner basis for an ideal of a polynomial ring ("Buchberger's Algorithm") which comes from Buchberger's Criterion. For this algorithm, we define the S-polynomial which is a method of canceling the leading terms of two polynomials to create a new polynomial. In

Chapter 5 we prove the Elimination theorem which says that a Gröbner basis for the ideal of a polynomial ring that is a particular subset of the original polynomial ring can be calculated using the Gröbner basis in the larger polynomial ring. We use the Elimination Theorem to show how we can find the kernel of a mapping of change of variables. Lastly, in Chapter 6 we state and prove Galligo's theorem about existence of generic initial ideals related to Gröbner bases which says there exists a non-empty open subset of $GL_n(k)$ and a monomial ideal of a polynomial ring such that for each g in this subset, $\text{in}_\tau(gI)$ is equal to the monomial ideal.

Throughout this thesis we used unpublished notes by Craig Huneke [11] in addition to other sources for reference.

Chapter 1

Basic Definitions and Setup

Some of the definitions for the setup of the thesis are from *Gröbner Bases In Commutative Algebra* by Viviana Ene and Jürgen Herzog. [6]

1.1 Introduction to Macaulay2

Throughout this thesis I will provide many examples, both computed by hand and from Macaulay2, a mathematical computer program language created by Daniel Grayson and Michael Stillman for algebraic geometry and commutative algebra. Here is some information about Macaulay2 on their website:
"Macaulay2 is a software system devoted to supporting research in algebraic geometry and commutative algebra, whose creation has been funded by the National Science Foundation since 1992.
Macaulay2 includes core algorithms for computing Gröbner bases and graded or

multi-graded free resolutions of modules over quotient rings of graded or multi-graded polynomial rings with a monomial ordering. The core algorithms are accessible through a versatile high level interpreted user language with a powerful debugger supporting the creation of new classes of mathematical objects and the installation of methods for computing specifically with them. Macaulay2 can compute Betti numbers, Ext, cohomology of coherent sheaves on projective varieties, primary decomposition of ideals, integral closure of rings, and more." [8]
For more information on Macaulay2, how to download it, and some other sample code visit their website at `http://www2.macaulay2.com/Macaulay2/`.
You can also try the web-based version of the program at
`http://habanero.math.cornell.edu:3690/`.

1.2 Setup

Let k be a field. Then $k[x_1, x_2, \ldots, x_n]$ is a *polynomial ring* over k with n variables.

Definition 1.1. *A* ***monomial*** *in the polynomial ring $k[x_1, x_2, \ldots, x_n]$ is an element of the form $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ where $\alpha_1, \alpha_2, \ldots, \alpha_n \geqslant 0$.*

Definition 1.2. *A* ***term*** *in the polynomial ring $k[x_1, x_2, \ldots, x_n]$ is an element of the form $\lambda x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ where $\alpha_1, \alpha_2, \ldots, \alpha_n \geqslant 0$, $\lambda \in k$, and $\lambda \neq 0$.*

Example 1.3.

- A simple example of monomials and terms is in $\mathbb{Q}[x]$. Monomials are of the form x^α where $\alpha \geq 0$ and terms are of the form $\frac{a}{b}x^\alpha$ where $a, b \in \mathbb{Z}$, $b \neq 0$, and $\alpha \geq 0$.

- Consider the polynomial rings $R = k[x, y, z]$ and $S = k[x + y, y + z, z - x]$ and the element $(x + y)(y + z)(z - x)$ in each of the rings. In S this element is a monomial. However, the element in R is equal to $-x^2y + xz^2 - x^2z + y^2z - xy^2 + yz^2$, which is not a monomial in R. From this example we see that monomials depend on the variables defined in the polynomial ring.

Definition 1.4. *[6]*

1. *A **partial order** on a set is a binary ordering (denoted using $\leq$) of some of the elements in that set with respect to each other which satisfies for all m, m_1, m_2, m_3 in the set:*

   - *(Reflexivity) $m \leq m$;*
   - *(Antisymmetry) if $m_1 \leq m_2$ and $m_2 \leq m_1$, then $m_1 = m_2$;*
   - *(Transitivity) if $m_1 \leq m_2$ and $m_2 \leq m_3$, then $m_1 \leq m_3$.*

2. *A partial order on a set is called a **total order**, if for any two elements m, n in the set it is the case that $m \leq n$ or $n \leq m$.*

Definition 1.5.

1. *A* ***term ordering*** τ *(notated* $>_\tau$*) is a partial ordering on the monomials of* $k[x_1, x_2, \ldots, x_n]$ *where:*

   (a) *for any monomial* a *in* $k[x_1, x_2, \ldots, x_n]$ *such that* $a \neq 1$*, then* $a >_\tau 1$*.*

   (b) *if* a*,* b*, and* c *are all monomials where* $a >_\tau b$*, then it follows that* $ac >_\tau bc$*.*

2. *A* ***monomial ordering*** τ *(notated* $>_\tau$*) is a term ordering on the monomials of* $k[x_1, x_2, \ldots, x_n]$ *which is a total ordering instead a partial ordering.*

3. *A* ***degree-wise monomial ordering*** *is a monomial ordering which respects the degrees of a monomial. In other words, it is a degree-wise monomial ordering if a monomial of a higher degree is always greater that a monomial of lower degree under* τ*.*

Example 1.6.

- Consider the monomial ordering τ on the polynomial ring $k[x]$. Since x is a monomial in $k[x]$ then by 1.5.2(a) we have that $x >_\tau 1$. We also then have by 1.5.2(b) that $x^2 = x \cdot x >_\tau 1 \cdot x = x$. Combining the inequalities that we have we get that $x^2 >_\tau x >_\tau 1$. Continuing in this way we get that $x^k >_\tau x^{k-1} >_\tau x^{k-2} >_\tau \cdots >_\tau x^3 >_\tau x^2 >_\tau x >_\tau 1$ for any positive degree k.

- Consider the monomial ordering τ on the polynomial ring $k[x, y]$ where $x >_\tau y$. By 1.5.2(b) we have that $x^2 = x \cdot x >_\tau x \cdot y$ and that $x \cdot y >_\tau y \cdot y = y^2$. Combining these two inequalities we get that $x^2 >_\tau xy >_\tau y^2$. Continuing in the same way we get that
  $x^k >_\tau x^{k-1}y >_\tau x^{k-2}y^2 >_\tau \cdots >_\tau x^2y^{k-2} >_\tau xy^{k-1} >_\tau y^k$ for any positive degree k.

Example 1.7. Consider the monomial ordering τ on the polynomial ring $k[x, y, z]$ where $x >_\tau y >_\tau z$. Then similarly to the previous example we get that $x^2 >_\tau xy >_\tau y^2$, $y^2 >_\tau yz >_\tau z^2$, $x^2 >_\tau xz >_\tau z^2$, $xz >_\tau yz$, $xy >_\tau yz$, and $xy >_\tau xz$ in the degree 2 case. However when trying to "combine" the inequalities into one inequality we run into two different scenarios depending on the ordering of y^2 and xz. Either

1. $x^2 >_\tau xy >_\tau y^2 >_\tau xz >_\tau yz >_\tau z^2$ or
2. $x^2 >_\tau xy >_\tau xz >_\tau y^2 >_\tau yz >_\tau z^2$

Thus, to define τ as a degree-wise monomial ordering in the degree 2 case another choice needs to be made as to whether $y^2 >_\tau xz$ or $xz >_\tau y^2$. However, this does not uniquely define the degree-wise monomial ordering with three variables. Consider the degree 3 case. The monomials of degree 3 are $x^3, x^2y, xy^2, y^3, y^2z, yz^2, z^3, xz^2, x^2z$, and z^3 with either:

1. *when* $y^2 >_\tau xz$:

   (a) $x^3 >_\tau x^2y >_\tau xy^2 >_\tau x^2z >_\tau xyz >_\tau xz^2$ by multiplying the degree 2 ordering by x.

   (b) $x^2y >_\tau xy^2 >_\tau xyz >_\tau y^3 >_\tau y^2z >_\tau yz^2$ by multiplying the degree 2 ordering by y.

   (c) $x^2z >_\tau xyz >_\tau xz^2 >_\tau y^2z >_\tau yz^2 >_\tau z^3$ by multiplying the degree 2 ordering by z.

   When trying to "combine" the inequalities, we can get two different orderings depending on the ordering of y^3 and xz^2:

   (a) $x^3 >_\tau x^2y >_\tau xy^2 >_\tau x^2z >_\tau xyz >_\tau y^3 >_\tau xz^2 >_\tau y^2z >_\tau yz^2 >_\tau z^3$ or

   (b) $x^3 >_\tau x^2y >_\tau xy^2 >_\tau x^2z >_\tau xyz >_\tau xz^2 >_\tau y^3 >_\tau y^2z >_\tau yz^2 >_\tau z^3$

2. *when* $xz >_\tau y^2$:

   (a) $x^3 >_\tau x^2y >_\tau x^2z >_\tau xy^2 >_\tau xyz >_\tau xz^2$ by multiplying the degree 2 ordering by x.

   (b) $x^2y >_\tau xy^2 >_\tau xyz >_\tau y^3 >_\tau y^2z >_\tau yz^2$ by multiplying the degree 2 ordering by y.

   (c) $x^2z >_\tau xyz >_\tau xz^2 >_\tau y^2z >_\tau yz^2 >_\tau z^3$ by multiplying the degree 2 ordering by z.

When trying to "combine" the inequalities, we can get to different orderings depending on the ordering of y^3 and xz^2:

(a) $x^3 >_\tau x^2y >_\tau x^2z >_\tau xy^2 >_\tau xyz >_\tau y^3 >_\tau xz^2 >_\tau y^2z >_\tau yz^2 >_\tau z^3$ or

(b) $x^3 >_\tau x^2y >_\tau x^2z >_\tau xy^2 >_\tau xyz >_\tau xz^2 >_\tau y^3 >_\tau y^2z >_\tau yz^2 >_\tau z^3$

Definition 1.8. *Let τ be a monomial ordering and let $f \in k[x_1, x_2, \ldots, x_n]$.*

1. *The **inital term of f** with respect to τ (notated $\text{in}_\tau(f)$) is the largest monomial in a term of f.*

2. *The **leading term of f** with respect to τ (notated $\text{lt}_\tau(f)$) is the term in f which has $\text{in}_\tau(f)$.*

3. *The **initial ideal of I** with respect to τ (notated $\text{in}_\tau(I)$) is the ideal generated by the initial terms of all elements (not necessarily just generators) in I. Notationally, $\text{in}_\tau(I) := (\text{in}_\tau(f) : f \in I)$.*

Note that the initial ideal of I is not necessarily generated by the initial terms of the generators of I. We will demonstrate this in 1.10.

Example 1.9.

- Let $R = k[x]$. Let f be a polynomial in R such that $f = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + a_nx^n$ where a_n is nonzero. Then $\text{in}_\tau(f) = x^n$ and $\text{lt}_\tau(f) = a_nx^n$.

- Let $R = k[x, y]$ with $x >_\tau y$. Let f, g, and h be polynomials in R where $f = x^3 + 3x^2y + 3xy^2 + y^3$, $g = 4x^2 - y^2$, and $h = 3xy + 6y^2$. Then $\text{in}_\tau(f) = x^3$, $\text{in}_\tau(g) = x^2$, and $\text{in}_\tau(h) = xy$, $\text{lt}_\tau(f) = x^3$, $\text{lt}_\tau(g) = 4x^2$, and $\text{lt}_\tau(h) = 3xy$.

Example 1.10. Let $R = k[x, y, z]$ with $x >_\tau y >_\tau z$ and let I be the ideal of R where $I = (y^2 - xz, xy - z^2)$. Let $f = y^2 - xz$ and $g = xy - z^2$. From 1.7 we know that we have to choose whether $y^2 >_\tau xz$ or $xz >_\tau y^2$ for a complete ordering in degree 2.

1. $y^2 >_\tau xz$:

   $\text{in}_\tau(f) = y^2$ and $\text{in}_\tau(g) = xy$. Now let

   $h_1 = xf - yg = x(y^2 - xz) - y(xy - z^2) = -x^2z + yz^2$. So $\text{in}_\tau(h_1) = x^2z$ which is not in the ideal $(y^2, xy) = (\text{in}_\tau(f), \text{in}_\tau(g))$, even though h_1 is in the ideal generated by f and g.

2. $xz >_\tau y^2$:

   $\text{in}_\tau(f) = xz$ and $\text{in}_\tau(g) = xy$. Now let

   $h_2 = yf - zg = y(y^2 - xz) - z(xy - z^2) = y^3 + z^3$. So $\text{in}_\tau(h_2) = y^3$ which is not in the ideal $(xz, xy) = (\text{in}_\tau(f), \text{in}_\tau(g))$, even though h_2 is in the ideal generated by f and g.

Thus, as we can see from both of these cases, it is not necessarily the case that if $I = (f_1, f_2, f_3, \ldots, f_m)$ then $\text{in}_\tau(I) = (\text{in}_\tau(f_1), \text{in}_\tau(f_2), \text{in}_\tau(f_3), \ldots, \text{in}_\tau(f_m))$.

Chapter 2

Gröbner Bases

In this chapter we introduce the idea of a Gröbner basis starting off with its definition. We will prove Dickson's Lemma which states that a non-empty set of monomials has a finite number of minimal elements which depends on its monomial ordering. Using Dickson's Lemma we will prove an important theorem. This theorem states that the set of monomials not in the initial ideal of an ideal I of a monomial ring $R = k[x_1, \ldots, x_n]$ is a k-basis for R/I.

Definition 2.1. *A* ***Gröbner basis of an ideal I*** *in the polynomial ring* $k[x_1, x_2, \ldots, x_n]$ *with respect to the monomial ordering* τ *is a set* $\{f_i\} \subseteq I$ *such that* $\text{in}_\tau(I) =< \text{in}_\tau(f_i) >$.

Example 2.2.

- Let $R = k[x, y, z]$ and $I = (x + y, x + z, y + z)$ be an ideal of R. Let τ be a

monomial ordering on R such that $x >_\tau y >_\tau z$. Let $f_1 = x + y$, $f_2 = x + z$, and $f_3 = y + z$. Then $\text{in}_\tau(f_1) = x = \text{in}_\tau(f_2)$ and we can subtract f_2 from f_1 to get $f_1 - f_2 = y - z$ where $\text{in}_\tau(f_1 - f_2) = y = \text{in}_\tau(f_3)$. So now we can subtract $f_1 - f_2$ from f_3 to get $f_3 - (f_1 - f_2) = 2z$ where $\text{in}_\tau(f_3 - (f_1 - f_2) = z$. Therefore $\text{in}_\tau(I) = (x, y, z)$ and a Gröbner basis of I is $\{f_1, f_1 - f_2, f_3 - (f_1 - f_2)\}$.

- Let $R = k[x, y, z]$ such that $\text{char}(k) \neq 2$ and let $I = (x + y - z, x - y + z)$ be an ideal of R. Let τ be a monomial ordering on R such that $x >_\tau y >_\tau z$. Let $f_1 = x + y - z$ and $f_2 = x - y + z$. Then $\text{in}_\tau(f_1) = x = \text{in}_\tau(f_2)$ and we can subtract f_2 from f_1 to get $f_1 - f_2 = 2y - 2z$ where $\text{in}_\tau(f_1 - f_2) = y$. We claim that $\text{in}_\tau(I) = (x, y)$. To prove this, suppose that a power of z is in $\text{in}_\tau(I)$. Since $x >_\tau y >_\tau z$, then that same power of z is in I since it cannot be canceled out by any other $\text{in}_\tau(m)$ where m is a monomial in $k[x, y, z]$. Thus, z is in $rad(I)$ since a power of z is in I. We also have $y - z$ and x are in I so it must also be the case that $y - z$ and x are in $rad(I)$ and since $rad(I)$ is closed under addition, we must have that $(y - z) + z = y$ is in $rad(I)$. Therefore $rad(I) = (x, y, z)$. This implies that $ht(I) = 3$ which contradicts the fact that I is an ideal generated by just two elements, $x + y - z$ and $x - y + z$ (using Krull's Height Theorem which states that if R is a Noetherian ring, I is a proper ideal of R which is generated by n elements, and P is a minimal prime ideal containing I among all of the prime ideals containing I, then the height

of I, denoted $ht(I)$, is at most n). Thus we have that $\text{in}_\tau(I) = (x, y)$ and a Gröbner Basis of I is $\{f_1, f_1 - f_2\} = \{x + y - z, 2y - 2z\}$.

Lemma 2.3 (Dickson's Lemma)**.** *Let τ be a term ordering on $R = k[x_1, x_2, \ldots, x_n]$ and let M be a non-empty set of monomials in R. Then M has a non-zero finite number of minimal elements.*

Proof. [6] We will prove Dickson's Lemma by an induction on n (the number of variables in R).

If $\underline{n = 1}$, then M consists of certain powers of x_1, and the set of minimal elements of M is the set $\{x_1^\alpha\}$ where α is the smallest such that x_1^α is in M.

Next we let $\underline{n > 1}$, and let N be the set of monomials $\boldsymbol{x^a} \in k[x_1, x_2, \ldots, x_{n-1}]$ such that $\boldsymbol{x^a} x_n^b \in M$ for some $b \geq 0$. By the induction hypothesis, let N^{min} be the set of minimal elements of N, which is finite. Let $N^{min} = \{\boldsymbol{x^{a_1}}, \boldsymbol{x^{a_2}}, \ldots, \boldsymbol{x^{a_k}}\}$ where $\boldsymbol{a_i} = (\boldsymbol{a_{i_1}}, \boldsymbol{a_{i_2}}, \ldots, \boldsymbol{a_{i_{n-1}}})$. For each $\boldsymbol{x^{a_i}}$ there is $c_i \geq 0$ such that $\boldsymbol{x^{a_i}} x_n^{c_i} \in M$ by definition of the set of elements in N. Let $c = \max\{c_1, c_2, \ldots, c_k\}$. For each d such that $0 \leq d < c$, let $N_d = \{\boldsymbol{x^a} \in k[x_1, x_2, \ldots, x_{n-1}] : \boldsymbol{x^a} x_n^d \in M\}$. Again, by the induction hypothesis, N_d^{min} is a finite set. Denote the set of monomials $\boldsymbol{x^a} x_n^d$ with $\boldsymbol{x^a} \in N_d^{min}$ by $N_d^{min} x_n^d$.

Claim. $M^{min} \subseteq \{\boldsymbol{x^{a_1}} x_n^{c_1}, \boldsymbol{x^{a_2}} x_n^{c_2}, \ldots, \boldsymbol{x^{a_k}} x_n^{c_k}\} \cup \bigcup_{d=1}^{n-1} N_d^{min} x_n^d$

Let $u = \boldsymbol{x^a} x_n^b$ be a monomial in M. If $b \geq c$, then some monomial in $\{\boldsymbol{x^{a_1}} x_n^{c_1}, \boldsymbol{x^{a_2}} x_n^{c_2}, \ldots, \boldsymbol{x^{a_k}} x_n^{c_k}\}$ divides u since $\{\boldsymbol{x^{a_1}}, \boldsymbol{x^{a_2}}, \ldots, \boldsymbol{x^{a_k}}\}$ is the set of minimal elements of N so an element of $\{\boldsymbol{x^{a_1}}, \boldsymbol{x^{a_2}}, \ldots, \boldsymbol{x^{a_k}}\}$ will divide $\boldsymbol{x^a}$ and since

$b \geq c = \max\{c_1, c_2, \ldots, c_k\}$ then one of the x^{c_i} will also divide x_n^b. If $0 \leq b < c$, then u is divisible by a monomial in $N_b^{min} x_n^b$ since N_b^{min} is the set of minimal monomials $\{\boldsymbol{x}^{\boldsymbol{a}}\}$ where $\boldsymbol{x}^{\boldsymbol{a}} x_n^b$ is in M, as desired.

Since the right-hand-side of the claim is a finite set, this proves that M will also be finite. □

Corollary 2.4. *Let τ be a* monomial *ordering on $R = k[x_1, x_2, \ldots, x_n]$ and let M be a non-empty set of monomials in R. Then M has a minimal element.*

Theorem 2.5. *Let τ be a monomial ordering on $R = k[x_1, x_2, \ldots, x_n]$ and let I be an ideal of R. Let B be the set of all monomials not in $\text{in}_\tau(I)$. Then B is a k-basis of R/I.*

Proof. To prove B to be a k-basis, we must show that (1) B is linearly independent and (2) B spans R/I.

1. *Linear independence:* Let $m_1, m_2, \ldots, m_r$ be distinct elements in B such that $\lambda_1 m_1 + \lambda_2 m_2 + \cdots + \lambda_r m_r = 0$ in R/I where $\lambda_i \in$ k. Since $\lambda_1 m_1 + \lambda_2 m_2 + \cdots + \lambda_r m_r = 0$ in R/I, then $\lambda_1 m_1 + \lambda_2 m_2 + \cdots + \lambda_r m_r \in I$. Suppose that $\lambda_i \neq 0$ for some i. This would imply that $\text{in}_\tau(\lambda_1 m_1 + \lambda_2 m_2 + \cdots + \lambda_r m_r) = m_j$ for some j with $1 \leq j \leq r$ since there is at least one λ_i which is not 0 so the entire summation will not be zero so there exists an initial term. That then implies that $m_j = \text{in}_\tau(\lambda_1 m_1 + \lambda_2 m_2 + \cdots + \lambda_r m_r) \in \text{in}_\tau(I)$ which is a contradiction since

by *initial* assumption $m_j \in B$ and B is defined to be all monomials not in $\text{in}_\tau(I)$. Thus $\lambda_i = 0$ for all $1 \leq i \leq r$ and so B is linearly independent.

2. *B spans R/I:* To show that B spans R/I we will show that $I+ \text{k}< B >= R$ where k$< B >$ is the k-span of B. Suppose that $I+ \text{k}< B > \neq R$. Then let $M = \{\text{in}_\tau(g) : g \in R \setminus (I + k < B >)\}$. Since M is non-empty by assumption we can use Dickson's Lemma to say that M has a least element. Let that element be $m = \text{in}_\tau(g)$ for some g in $R\backslash(I+ \text{k}< B >)$.

   (a) Suppose $m \notin B$. Then $m \in \text{in}_\tau(I)$ since B by definition is the set of monomials not in $\text{in}_\tau(I)$. This means that $m = \text{in}_\tau(f)$ for some f in I by definition of $\text{in}_\tau(I)$. Since $\text{in}_\tau(g) = m = \text{in}_\tau(f)$ then we can find a $\lambda \in k$ such that $m >_\tau \text{in}_\tau(g - \lambda f)$. This is because $g = am+$ {lower degree terms} and $f = bm+$ {lower degree terms} where $m = \text{in}_\tau(g) = \text{in}_\tau(f)$, so if we let $\lambda = ab^{-1}$, then $g - \lambda f$ will have a lesser initial term than m since we are subtracting the leading terms from both f and g. Since m is the minimal element of M, then $g - \lambda f \in I+ \text{k}< B >$ and so $g \in I+ \text{k}< B >$ since $\lambda f \in I$, which is a contradiction.

   (b) Now suppose $m \in B$. Then there is a $\lambda \in$ k such that $m >_\tau \text{in}_\tau(g - \lambda m)$ since $g = \lambda m+$ {lower degree terms} where $m = \text{in}_\tau(g)$, so $g - \lambda m$ will have a lesser initial term than m since we are subtracting the leading term. Since m is the minimal element of M, then $g - \lambda m \in I+ \text{k}< B >$

and so $g \in I+$ k$< B >$ since $\lambda m \in$ k$< B >$ by definition, which is a contradiction.

So in either case we face a contradiction. Thus we must have that $I+$ k$< B >= R$. Thus B is a k-basis of R/I.

□

Chapter 3

The Division Algorithm, the Hilbert Basis Theorem, and Symmetric Polynomials

In this chapter we introduce the three basic monomial orderings. We will prove the a general version of the well-known Division Algorithm, but in this thesis we will prove a more general version of it using more than one variable and which uses initial terms. Next we will prove a specific case of the Hilbert Basis Theorem which states that for $k[x_1, \ldots, x_n]$ a polynomial ring over a field k, then any non-zero ideal is finitely generated. The usual Hilbert Basis Theorem is for any commutative, not specifically for fields. We also prove the Criterion for Ideal Membership which proves that a Gröbner basis of an ideal reduces each element of the ideal to zero. We also provide a proof of the natural isomorphism from the field of elementary

symmetric functions to the field of symmetric polynomials, which is referenced from Mark Green's *Generic initial ideals. Six lectures on commutative algebra* [9]. The examples in this chapter are both written examples and Macaulay2 examples.

Notation 3.1. Let $R = k[x_1, x_2, \ldots, x_n]$, $A = (a_1, a_2, \ldots, a_n)$ with each $a_i \geq 0, a_i \in \mathbb{Z}$. We denote $\boldsymbol{x}^A$ to be the monomial $\boldsymbol{x}^A := x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$. With this, we define the **total degree** of $\boldsymbol{x}^A$ by $|A| := \sum_{i=1}^{n} a_i$.

Example 3.2. Let $\boldsymbol{x}^A \in R$ with $A = (1, 3, 5, 0, 4)$ then we have that the total degree of $\boldsymbol{x}^A$ is $|A| = 1 + 3 + 5 + 0 + 4 = 13$.

Definition 3.3. *There are three different types of basic monomial orderings:*

1. ***Lex**: $\boldsymbol{x}^A >_{lex} \boldsymbol{x}^B$ if and only if the first nonzero entry of $A - B$ is positive. In this definition we can also say that $\boldsymbol{x}^A$ has "more in the front" than $\boldsymbol{x}^B$.*

2. ***Deglex**: $\boldsymbol{x}^A >_{deglex} \boldsymbol{x}^B$ if and only if either:*

   (a) $|A| > |B|$ *or*

   (b) $|A| = |B|$ *and* $\boldsymbol{x}^A >_{lex} \boldsymbol{x}^B$.

3. ***Revlex**: $\boldsymbol{x}^A >_{revlex} \boldsymbol{x}^B$ if and only if either:*

   (a) $|A| > |B|$ *or*

   (b) $|A| = |B|$ *and the* last *nonzero entry of $A - B$ is negative.*

   In this definition we can also say that $\boldsymbol{x}^A$ has "less in the back" than $\boldsymbol{x}^B$.

Example 3.4.

- Let $R = k[x_1, x_2, x_3]$, $A = (4, 2, 6)$, and $B = (2, 3, 4)$ then we have that $A - B = (2, -1, 2)$ and so $\boldsymbol{x}^A >_{lex} \boldsymbol{x}^B$ since the first entry is positive.

- Let $R = k[x_1, x_2, x_3]$, $A = (4, 2, 6)$, and $B = (4, 3, 4)$ then we have that $A - B = (0, -1, 2)$ and so $\boldsymbol{x}^B >_{lex} \boldsymbol{x}^A$ since the *first nonzero* entry is negative.

- Let $R = k[x_1, x_2, x_3, x_4]$, $A = (1, 3, 6, 7)$, and $B = (2, 1, 4, 5)$. Then $|A| = 1 + 3 + 6 + 7 = 17$ and $|B| = 2 + 1 + 4 + 5 = 12$. So $\boldsymbol{x}^A >_{deglex} \boldsymbol{x}^B$ and $\boldsymbol{x}^A >_{revlex} \boldsymbol{x}^B$ since $|A| = 17 > 12 = |B|$.

- Let $R = k[x_1, x_2, x_3, x_4, x_5, x_6]$, $A = (4, 2, 6, 3, 1, 5)$, and $B = (4, 4, 0, 4, 4, 5)$. Then $|A| = 4 + 2 + 6 + 3 + 1 + 5 = 21$ and $|B| = 4 + 4 + 4 + 0 + 4 + 5 = 21$, so $|A| = |B|$. We also have that $A - B = (0, -2, 2, 3, -3, 0)$ and so $\boldsymbol{x}^B >_{deglex} \boldsymbol{x}^A$ since $\boldsymbol{x}^B >_{lex} \boldsymbol{x}^A$. We also have that $\boldsymbol{x}^A >_{revlex} \boldsymbol{x}^B$ since the *last nonzero* entry is negative.

Example 3.5. (Macaulay2) This example illustrates differences in lex and revlex, but computed in Macaulay2. The command 'MonomialOrder' in the initialization of the ring sets the monomial ordering in the ring for our computations, where 'Lex' is the lex ordering and 'GRevLex' is the revlex ordering. The command 'monomialIdeal I,' where I is an ideal of the ring, outputs the initial ideal generated by the lead monomials of a Gröbner basis of I. First, we set up our polymonial ring R with $x >_\tau y >_\tau >_\tau z >_\tau w$ where τ is the lex monomial ordering:

```
i1 : R = QQ[x, y, z, w, MonomialOrder => Lex, Global => false];

i2 : I = ideal(w*y-x^2, x*z-y^2, w*z-x*y)

                2               2
o2 = ideal (- x  + y*w, x*z - y , - x*y + z*w)

o2 : Ideal of R

i3 : monomialIdeal I

                      2        3
o3 = monomialIdeal (x , x*y, y , x*z)

o3 : MonomialIdeal of R
```

But if the monomial ordering is revlex instead of lex we get:

```
i1 : R = QQ[x, y, z, w, MonomialOrder => GRevLex, Global => false];

i2 : I = ideal(w*y-x^2, x*z-y^2, w*z-x*y)

                2           2
o2 = ideal (- x  + y*w, - y  + x*z, - x*y + z*w)

o2 : Ideal of R

i3 : monomialIdeal I

                      2        2
o3 = monomialIdeal (x , x*y, y )

o3 : MonomialIdeal of R
```

So in lex we get that the initial ideal is (x^2, xy, y^3, xz), whereas with revlex we get that the initial ideal is (x^2, xy, y^2). These two initial ideals are obviously not equal since with lex there is a term in the initial ideal with z and there is not on in the initial ideal using revlex.

As stated in the last example, changing monomial orderings can change answers to various problems. For some computations and theorems it is important to use a specific type of monomial ordering. We will demonstrate in the next theorem why specifying a specific type of monomial ordering is important to the proof. But first we have a couple of definitions for the setup of the theorem:

Definition 3.6. *[9] Let S_n be the symmetric group on $\{1, 2, \ldots, n\}$, which acts on $k[x_1, x_2, \ldots, x_n]$ by permuting the variables. The* ***symmetric polynomials*** *are the polynomials left invariant by this action. The set of symmetic polynomials in n variables is denoted by $k[x_1, x_2, \ldots, x_n]^{S_n}$. In other words, the symmetric polynomials are those which do not change after the "swap" of two or more variables in the polynomial.*

Definition 3.7. *[9] The* ***elementary symmetric functions*** *σ_k are defined by $\prod_{i=1}^{n}(x + x_i) = x^n + \sum_{k=1}^{n} \sigma_k x^{n-k}$. So $\sigma_1 = x_1 + x_2 + \cdots + x_n$, $\sigma_2 = \sum_{i \neq j} x_i x_j$, $\sigma_3 = \sum_{i \neq j \neq k} x_i x_j x_k, \ldots, \sigma_n = x_1 x_2 \cdots x_n$. These are symmetric polynomials since they are invariant under the under the action of permuting the variables, as stated in the definition above.*

Remark 3.8. For the elementary symmetric polynomials in n variables, the σ_is are:

$$\sigma_1 = x_1 + x_2 + \cdots + x_n,$$

$$\sigma_2 = x_1x_2 + x_1x_3 + \cdots + x_2x_3 + x_3x_4 + \cdots + x_{n-1}x_n,$$

$$\vdots$$

$$\sigma_n = x_1x_2 \cdots x_n.$$

Remark 3.9. Since the symmetric polynomials are preserved under addition and multiplication (of the polynomials), the symmetric polynomials form a subring of $k[x_1, \ldots, x_n]$, denoted $k[x_1, \ldots, x_n]^{S_n}$. This also implies that every polynomial expression $p(\sigma_1, \ldots, \sigma_n)$ in the elementary symmetric polynomials is symmetric in $k[x_1, \ldots, x_n]$ and hence we can look at the subring $k[\sigma_1, \ldots, \sigma_n] \subseteq k[x_1, \ldots, x_n]^{S_n}$. For instance, the monomial $\sigma_1^{i_1} \cdots \sigma_n^{i_n}$ in the elementary symmetric polynomials is symmetric and homogeneous of degree $i_1 + 2i_2 + \cdots + ni_n$ (Since we "choose" a term of degree i_1 from $\sigma_1^{i_1}$, a term of degree $2i_2$ from σ_2, and so on to create a term in the product) in the original variables $x_1, x_2, \ldots, x_n$.

Theorem 3.10. *[9] The natural map $k[\sigma_1, \sigma_2, \ldots, \sigma_n] \to k[x_1, x_2, \ldots, x_n]^{S_n}$ is an isomorphism.*

Proof. [9] As discussed in 3.9, the natural map $k[\sigma_1, \sigma_2, \ldots, \sigma_n] \to k[x_1, x_2, \ldots, x_n]^{S_n}$ is the inclusion map where we replace σ_i by its explicit value in the variables $x_1, x_2, \ldots, x_n$ as in 3.8. We just need to show that any $p \in k[x_1, \ldots, x_n]^{S_n}$ can be

generated by a (necessarily nonzero) polynomial expression in the σ_i's. In other words, we need to prove surjectivity of this map.

Now let p be a symmetric polynomial. Let τ be the lex monomial ordering. Then $\text{in}_\tau(p) = x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$. Suppose that we do not have $i_1 \geq i_2 \geq \cdots \geq i_n$. Then, for example, we have a pair i_j and i_k with $j < k$ but $i_j < i_k$. Since p is a symmetric polynomial then $x_1^{i_1}x_2^{i_2}\cdots x_j^{i_k}\cdots x_k^{i_j}\cdots x_n^{i_n}$ is also a term in p. But since τ is the lex monomial ordering then it must be the case that

$$x_1^{i_1}x_2^{i_2}\cdots x_j^{i_k}\cdots x_k^{i_j}\cdots x_n^{i_n} >_\tau x_1^{i_1}x_2^{i_2}\cdots x_j^{i_j}\cdots x_k^{i_k}\cdots x_n^{i_n}$$

since $j < k$ and $i_k > i_j$, which is a contradiction to our choice of initial term. Thus the i_k's are weakly decreasing.

We observe that $\text{in}_\tau(\sigma_1^{j_1}\sigma_2^{j_2}\cdots\sigma_n^{j_n}) = x_1^{j_1+j_2+\cdots+j_n}x_2^{j_2+\cdots+j_n}\cdots x_n^{j_n}$ and also notice that the initial terms are all different. If not, consider $\sigma_1^{j_1}\cdots, \sigma_n^{j_n}$ and $\sigma_1^{k_1}\cdots\sigma_n^{k_n}$ and suppose that the initial terms are the same. Then, working backwards, we have that

$$\begin{gathered}
j_n = k_n, \\
j_n + j_{n-1} = k_n + k_{n-1} \Rightarrow j_{n-1} = k_{n-1}, \\
\vdots \\
j_2 + j_3 + \cdots + j_n = k_2 + k_3 + \cdots + k_n \Rightarrow j_2 = k_2, \\
j_1 + j_2 + \cdots + j_n = k_1 + k_2 + \cdots + k_n \Rightarrow j_1 = k_1
\end{gathered}$$

so they are equal.

So now recall $\text{in}_\tau(p) = x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$ where $i_1 \geq i_2 \geq \cdots \geq i_n$. Now consider $\sigma_1^{a_1}\sigma_2^{a_2}\sigma_3^{a_3}\cdots\sigma_n^{a_n}$ where

$$a_1 = i_1 - i_2, a_2 = i_2 - i_3, a_3 = i_3 - i_4, \ldots, a_{n-1} = i_{n-1} - i_n, a_n = i_n.$$

Since the i_k's are weakly decreasing, the $a_m \geq 0$ for all m. Then, this term under the natural map, has initial term

$$\begin{aligned}
&x_1^{a_1+a_2+\cdots+a_n} x_2^{a_2+a_3+\cdots+a_n} x_3^{a_3+a_4+\cdots+a_n} \cdots x_{n-1}^{a_{n-1}+a_n} x_n^{a_n} \\
=&x_1^{(i_1-i_2)+(i_2-i_3)+\cdots(i_{n-1}-i_n)+i_n} x_2^{(i_2-i_3)+(i_3-i_4)+\cdots(i_{n-1}-i_n)+i_n} \cdots x_{n-1}^{(i_{n-1}-i_n)+i_n} x_n^{i_n} \\
=&x_1^{i_1} x_2^{i_2} x_3^{i_3} \cdots x_{n-1}^{i_{n-1}} x_n^{i_n}
\end{aligned}$$

which is equal to $\mathrm{in}_\tau(p)$ and with all of the terms that are generated by switching around the n variables. Consider

$$p_1 = p - \frac{\mathrm{lt}_\tau(p)}{\mathrm{in}_\tau(p)} \sigma_1^{a_1} \sigma_2^{a_2} \sigma_3^{a_3} \cdots \sigma_n^{a_n}$$

with the same above choices of a_m. Note that by the discussion above,

$$\mathrm{in}_\tau(p_1) <_\tau \mathrm{in}_\tau(p).$$

Let $f_1 = \frac{\mathrm{lt}_\tau(p)}{\mathrm{in}_\tau(p)} \sigma_1^{a_1} \sigma_2^{a_2} \sigma_3^{a_3} \cdots \sigma_n^{a_n}$. If $p_1 = 0$, then we are done. Otherwise, apply the same above procedure to p_1 to further reduce the initial term and we keep adding the term to create $f_{i+1} = f_i + \frac{\mathrm{lt}_\tau(p_i)}{\mathrm{in}_\tau(p_i)} \sigma_1^{a_{i,1}} \sigma_2^{a_{i,2}} \sigma_3^{a_{i,3}} \cdots \sigma_n^{a_{i,n}}$.

Notice that this process terminates as there are only finitely many monomials m with $m <_\tau \mathrm{in}_\tau(p)$ because their degree is bounded. Suppose that this process terminates at step k (i.e. $p_k = 0$) then $p = f_k$ by construction. Thus, we have expressed p in terms of a polynomial in $k[\sigma_1, \ldots, \sigma_n]$ thereby finishing the proof. $\square$

Proposition 3.11. *Any such expression, f_k, as obtained in the proof above is unique.*

Proof. For this, we only need to show that no nonzero polynomial expression evaluated on σ_i's can give rise to 0 (because if $p = q_1$ and $p = q_2$ then $q_1 - q_2 = 0$). Let $q \in k[y_1, \ldots, y_n] \setminus \{0\}$, such that $q(\sigma_1, \ldots, \sigma_n) = 0$ (this would be $q = q_1 - q_2 = 0$ if $p = q_1$ and $p = q_2$). Consider $\text{in}_\tau(q) = y_1^{j_1} y_2^{j_2} \cdots y_n^{j_n}$. Then when we substitute σ_i for y_i and look at the initial term, then this is

$$\text{in}_\tau(\sigma_1^{j_1} \sigma_2^{j_2} \cdots \sigma_n^{j_n}) = x_1^{j_1 + j_2 + \cdots + j_n} x_2^{j_2 + \cdots + j_n} \cdots x_n^{j_n}$$

which is lexicographically the largest, and cannot be cancelled by other monomials in σ_i. Thus this is a contradiction to our assumption that $q(\sigma_1, \ldots, \sigma_n) = 0$ and $q \neq 0$. □

Example 3.12. We illustrate the process above via the following example in two variables x_1, x_2. Let τ be the lex monomial ordering. Consider the polynomial in $k[x_1, x_2]^{S_2}$:

$$p = x_1^3 + x_2^3$$

Then $\text{in}_\tau(p) = x_1^3$. And so choose

$$\sigma_1^{3-0} \sigma_2^0 = \sigma_1^3 = (x_1 + x_2)^3 = x_1^3 + 3x_1^2 x_2 + 3x_1 x_2^2 + x_2^3$$

Now let

$$p_1 = p - \frac{\mathrm{lt}_\tau(p)}{\mathrm{in}_\tau(p)}\sigma_1^3 = x_1^3 + x_2^3 - (x_1^3 + 3x_1^2x_2 + 3x_1x_2^2 + x_2^3) = -3x_1^2x_2 - 3x_1x_2^2$$

and

$$f_1 = \frac{\mathrm{lt}_\tau(p)}{\mathrm{in}_\tau(p)}\sigma_1^3 = {\sigma_1}^3$$

We have that $p_1 \neq 0$ so we continue the process.

Now we have $\mathrm{in}_\tau(p_1) = x_1^2x_2$. And so choose

$$\sigma_1^{2-1}\sigma_2^1 = \sigma_1\sigma_2 = (x_1 + x_2)(x_1x_2) = x_1^2x_2 + x_1x_2^2$$

Now let

$$p_2 = p_1 - \frac{\mathrm{lt}_\tau(p_1)}{\mathrm{in}_\tau(p_2)}\sigma_1\sigma_2 = -3x_1^2 - 3x_1x_2^2 - (-3)(x_1^2x_2 + x_1x_2^2) = 0$$

and

$$f_2 = f_1 + \frac{\mathrm{lt}_\tau(p_1)}{\mathrm{in}_\tau(p_1)}\sigma_1\sigma_2 = {\sigma_1}^3 - 3\sigma_1\sigma_2$$

Since $p_2 = 0$ then we are done and hence

$$x_1^3 + x_2^3 = {\sigma_1}^3 - 3\sigma_1\sigma_2$$

The importance of lex monomial ordering in the proof is by the way we are able to set up the one-to-one correspondence between $\mathrm{in}_\tau(\sigma_1^{j_1}\sigma_2^{j_2}\cdots\sigma_n^{j_n})$ and $x_1^{j_1+j_2+\cdots+j_n}x_2^{j_2+\cdots+j_n}\cdots x_n^{j_n}$ since

$j_1 + j_2 + \cdots + j_n \geq j_2 + j_3 + \cdots + j_n \geq \cdots \geq j_{n-1} + j_n \geq j_n$.

Definition 3.13. *Let f, g, h be polynomials in $R = k[x_1, \ldots, x_n]$, $g \neq 0$. Fix a monomial ordering τ on R. We say that f* ***directly reduces*** *to h with respect to g (notationally $f \longrightarrow_g h$) if $\mu \boldsymbol{x}^{\boldsymbol{A}} = \mathrm{lt}_\tau(g)$ divides a nonzero term $\lambda \boldsymbol{x}^{\boldsymbol{B}}$ of f and $h = f - (\frac{\lambda}{\mu})\boldsymbol{x}^{\boldsymbol{B}-\boldsymbol{A}} g$.*

More generally, if $f, h \in R$ and G is a collection of nonzero polynomials in R, we say f ***reduces*** *to h with respect to G if there is a chain $f \longrightarrow_{g_1} h_1 \longrightarrow_{g_2} h_2 \cdots \longrightarrow_{g_k} h$ where each $g_i \in G$ (notationally $f \longrightarrow_G h$).*

We say that $h \in R$ is ***reduced*** *with respect to $G \subseteq R \backslash \{0\}$ if h has no reductions with respect to G, i.e. no term in h is divisible by $\mathrm{in}_\tau(g_i)$ for any $g_i \in G$.*

Theorem 3.14 (The Division Algorithm)**.** *Let $R = k[x_1, \ldots, x_n]$ be a polynomial ring over a field. Let $G = \{g_1, \ldots, g_k\}$ be a collection of nonzero polynomials in R and f be any polynomial in R. There are polynomials $u_1, \ldots, u_k, r \in R$ such that we can write $f = \sum_{i=1}^{k} u_i g_i + r$ (*), where r is reduced with respect to G and $\mathrm{in}_\tau(f) \geq \max\{\mathrm{in}_\tau(u_1 g_1), \ldots, \mathrm{in}_\tau(u_k g_k))\}$.*

Proof. Suppose there is an f such that (*) doesn't hold. By Dickson's Lemma, we can choose an f with least $\mathrm{in}_\tau(f)$.

Case 1: ($\mathrm{in}_\tau(f) \in < \mathrm{in}_\tau(g_i) : 1 \leq i \leq k >$, say $\mathrm{in}_\tau(f) = m\mathrm{in}_\tau(g_i)$) Since $\mathrm{in}_\tau(f) = m\mathrm{in}_\tau(g)$, we can find $\lambda \in$ k such that $\mathrm{in}_\tau(f - \lambda m g_i) < \mathrm{in}_\tau(f)$ by canceling the leading term (term with respect to $\mathrm{in}_\tau(f)$). Thus, since $\mathrm{in}_\tau(f)$ is minimal such that (*) doesn't hold, then we can find $u_1, \ldots, u_k, r \in R$ such that $f - \lambda m g_i = \sum_{i=1}^{k} u_i g_i + r$, where r is reduced with respect to G and

$\text{in}_\tau(f - \lambda m g_i) \geq \max\{\text{in}_\tau(u_1 g_1, \ldots, \text{in}_\tau(u_k g_k)\}$. Rewriting, we get

$f = \sum_{j \neq i}^{k} u_j g_j + (u_i + \lambda m) g_i + r$, where r is reduced with respect to G. Moreover,

for $j \neq i$, $\text{in}_\tau(f) > \text{in}_\tau(f - \lambda m g_i) \geq \text{in}_\tau(u_j g_j)$ since

$\text{in}_\tau(f - \lambda m g_i) \geq \max\{\text{in}_\tau(u_1 g_1, \ldots, \text{in}_\tau(u_k g_k)\}$. For $j = i$,

$\text{in}_\tau(f) = \text{in}_\tau(\sum_{j \neq i}^{k} u_j g_j + (u_i + \lambda m) g_i + r)$ but

$\text{in}_\tau(f - \lambda m g_i) \geq \max\{\text{in}_\tau(u_1 g_1, \ldots, \text{in}_\tau(u_k g_k)\}$ so $\text{in}_\tau(f) = \text{in}_\tau((u_i + \lambda m) g_i + r)$. But

r is reduced with respect to G and $\text{in}_\tau(f) = m\text{in}_\tau(g_i)$ so if $\text{in}_\tau(f) = \text{in}_\tau(r)$ then

$\text{in}_\tau(r) = m\text{in}_\tau(g_i)$, then r would not be reduced with respect to G which is a

contradiction. Hence $\text{in}_\tau(f) > \text{in}_\tau(r)$ and $\text{in}_\tau(f) = \text{in}_\tau((u_i + \lambda m) g_i)$. Thus f satisfies

(*) which is a contradiction.

Case 2: $(\text{in}_\tau(f) \notin < \text{in}_\tau(g_i) : 1 \leq i \leq k >)$ Since $\text{in}_\tau(f)$ is minimal such that f

doesn't satisfy (*) then $f - \text{lt}_\tau(f)$ satisfies (*) (since subtracting $\text{lt}_\tau(f)$ leads to

$\text{in}_\tau(f - \text{lt}_\tau(f)) < \text{in}_\tau(f))$. Therefore we can find $u_1, \ldots, u_k, r' \in R$ such that

$f - \text{lt}_\tau(f) = \sum_{i=1}^{k} u_i g_i + r'$, where r' is reduced with respect to G and

$\text{in}_\tau(f - \text{lt}_\tau(f)) \geq \max\{\text{in}_\tau(u_1 g_1, \ldots, \text{in}_\tau(u_k g_k)\}$. Thus we can write

$f = \sum_{i=1}^{k} u_i g_i + r$, where $r = r' + \text{lt}_\tau(f)$ is reduced with respect to G (since

$\text{in}_\tau(f) = \text{in}_\tau(\text{lt}_\tau(f)) so \text{in}_\tau(\text{lt}_\tau(f)) \notin < \text{in}_\tau(g_i) : 1 \leq i \leq k >)$ and

$\text{in}_\tau(f) > \text{in}_\tau(f - \text{lt}_\tau(f) \max\{\text{in}_\tau(u_1 g_1, \ldots, \text{in}_\tau(u_k g_k)\}$, i.e. f satisfies (*), which is a

contradiction.

Thus, since both cases lead to a contradiction, then it must be the case that

$f = \sum_{i=1}^{k} u_i g_i + r$ (*), where r is reduced with respect to G and

$\text{in}_\tau(f) \geq \max\{\text{in}_\tau(u_1 g_1), \ldots, \text{in}_\tau(u_k g_k))\}$. □

In the equation of the Division Algorithm, any r appearing is called a **remainder** of f with respect to G. This remainder is not necessarily unique (see next example). It turns out that to be unique in the case G is a Gröbner basis of the ideal it generates.

Example 3.15. Let $R = k[x, y]$ and let τ be a monomial ordering on R such that $x >_\tau y$. Let $f = x^2y$, $G = \{xy, x^2 + y^2\}$ and $G' = \{x^2 + y^2, xy\}$. Note that $\text{in}_\tau(xy)|\text{in}_\tau(f)$, so we have that $f = x(xy) + 0$, using G as our set for reduction. On the other hand, using G' as our set for reduction, we have $f = y(x^2 + y^2) - y^3$. So the remainder is not unique since $G = G'$ except for the ordering in the set. Note also that G is not a Gröbner basis of $(xy, x^2 + y^2)$ since $y^3 \in (xy, x^2 + y^2)$ but $y^3 \notin (\text{in}_\tau(xy), \text{in}_\tau(x^2 + y^2))$.

Definition 3.16. *A commutative ring R is called **Noetherian** if it satisfies the equivalent conditions:*

1. *Every ideal of R is finitely generated (as an ideal)*
2. *Every ascending sequence of ideals stabilizes after finitely many steps, that is, if $I_1 \subseteq I_2 \subseteq \cdots$ is an ascending sequence of ideals, $\exists N \in \mathbb{N}$ such that $I_n = I_N$ for all $n \geq N$.*

Lemma 3.17. *Let R be a polynomial ring. Let J, I be ideals of R such that $J \subset I$. Let τ be a monomial ordering on R. If $\text{in}_\tau(I) = \text{in}_\tau(J)$, then $I = J$.*

Proof. Suppose that $I \neq J$. Since $J \subset I$, then all elements in J are automatically in I. So since $I \neq J$ we have that nonempty set $M \subset I$ $M = \{h \in I | h \notin J\}$. Let $N = \{\text{in}_\tau(g) | g \in M\}$. Then, by Dickson's Lemma, N has a minimal element. Choose $f \in M$ so that $\text{in}_\tau(f)$ corresponds to the minimal element in N. Since $\text{in}_\tau(I) = \text{in}_\tau(J)$, then there exists $g \in J$ with $\text{in}_\tau(g) = \text{in}_\tau(f)$. Then $(\frac{\text{lt}_\tau(g)}{\text{in}_\tau(g)})f - (\frac{\text{lt}_\tau(f)}{\text{in}_\tau(f)})g$ is in I (since f, g are in I), not in J (since f is not in J), and has lower leading term than f (since we canceled the leading term with the leading term from g), which is a contradiction since we assumed that f has the minimal initial term of I. □

Theorem 3.18. *Let k be a field. Then for any non-zero ideal $I \subseteq k[x_1, x_2, \ldots, x_n]$, I is finitely generated.*

Proof. Let τ be a monomial order and let I be a non-zero ideal of $k[x_1, \ldots, x_n]$. By 3.21, there are $f_1, \ldots, f_t \in I$ such that $(\text{in}_\tau(I)) = (\text{in}_\tau(f_1), ..., \text{in}_\tau(f_t))$. Clearly $(f_1, \ldots, f_t) \subseteq I$ (by choice of the f_i above). Conversely, let $f \in I$ and use 3.14 to reduce f by $(f_1, \ldots, f_t)$ to get $f = \sum_{i=1}^{t} a_i f_i + r$ where no term of the remainder is divisible by any of $\text{in}_\tau(f_i)$. If $r \neq 0$, then $\text{in}_\tau(r) \in (\text{in}_\tau(I)) = (\text{in}_\tau(f_i))$, which is impossible (or else $\text{in}_\tau(f_i) | \text{in}_\tau(r)$ for some i). Hence $I = (f_1, \ldots, f_t)$. □

Remark 3.19. (*The Hilbert Basis Theorem*): Let R be a commutative Noetherian Ring with 1. Then $R[x]$ is also Noetherian.

The Hilbert Basis Theorem is similar to the previous theorem, specifically when R is a field.

Proposition 3.20 (Criterion for Ideal Membership)**.** *Let $R = k[x_1, x_2, \ldots, x_n]$ be a polynomial ring over a field k and let $I \subseteq R$ be an ideal of R. Let $G = \{g_1, \ldots, g_k\} \subseteq I, g_i \neq 0$ for all i. Then the following are equivalent:*

1. *G is a Gröbner basis for I.*
2. *$f \in I$ if and only if $f \longrightarrow_G 0$.*

Proof.

(1) $\Rightarrow$ (2): Let G be a Gröbner basis for I.

($\Leftarrow$): Suppose that $f \longrightarrow_G 0$. Then there is a chain $f \longrightarrow_{g_{j_1}} h_1 \longrightarrow_{g_{j_2}} \cdots \longrightarrow_{g_{j_{l-1}}} h_{l-1} \longrightarrow_{g_{j_l}} 0$ (by definition of reduction by G). So, by 3.14, $f = \sum_{i=1}^{k} u_i g_i$ for some $u_i \in R$. Thus $f \in (g_1, \ldots, g_k) \subseteq I$.

($\Rightarrow$): Suppose that $f \in I$. By 3.14, we can write $f = \sum_{i=1}^{k} u_i g_i + r$ where $u_i, r \in R$ and r is *reduced with respect to G*. We can rewrite the equation so that $r = f - \sum_{i=1}^{k} u_i g_i$ and since $f, g_i \in I$ then, by ideal membership, $r \in I$. And since G is a Gröbner basis for I, then $\text{in}_\tau(r) \in (\text{in}_\tau(g_1), \ldots, \text{in}_\tau(g_k))$. But r is reduced with respect to G by the division algorithm sum above, i.e. $\text{in}_\tau(r)$ is not divisible by any of the $\text{in}_\tau(g_i)$. So it must be the case that $\text{in}_\tau(r) = 0$ which means that $r = 0$ since the leading monomial of r in 0. Thus $f = \sum_{i=1}^{k} u_i g_i$ where $u_i \in R$ so $f \longrightarrow_G 0$.

(2) $\Rightarrow$ (1): Let $f \in I$ if and only if $f \longrightarrow_G 0$. This implies that every f in I can be written as $f = \sum_{i=1}^{k} u_i g_i$ for some $u_i \in R$. In other words, G generates I. Let $f \in I$. To show the G is a Gröbner basis of I we need show that $\text{in}_\tau(f) \in (\text{in}_\tau(g_1, \ldots, \text{in}_\tau(g_k)$. By the division algorithm, we can write $f = \sum_{i=1}^{k} u_i g_i + r$ where $\text{in}_\tau(f) \geq \max\{\text{in}_\tau(u_1 g_1), \ldots, \text{in}_\tau(u_k g_k)\}$ and r is reduced with respect to G. We can rewrite the equation so that $r = f - \sum_{i=1}^{k} u_i g_i$ and since $f, g_i \in I$ then, by ideal membership, $r \in I$, and so, by hypothesis, $r \longrightarrow_G 0$. But r is reduced with respect to G by the division algorithm sum above, i.e. $\text{in}_\tau(r)$ is not divisible by any of the $\text{in}_\tau(g_i)$. So it must be the case that $\text{in}_\tau(r) = 0$ which means that $r = 0$ since the leading monomial of r in 0. Suppose the $\text{in}_\tau(f) \notin (\text{in}_\tau(g_1), \ldots, \text{in}_\tau(g_k))$, then $\text{in}_\tau(f) > \max\{\text{in}_\tau(u_1 g_1), \ldots, \text{in}_\tau(u_k g_k)\}$ so $\text{in}_\tau(f) = \text{in}_\tau(r) = 0$, which implies that $f = 0$ which is a contradiction since we assumed that f is nonzero. Thus $\text{in}_\tau(f) \in (\text{in}_\tau(g_1), \ldots, \text{in}_\tau(g_k))$. Therefore G is a Gröbner basis of I. □

Corollary 3.21. *If G is a Gröbner basis for I, then G generates I.*

Proof. By the previous theorem, if G is a Gröbner basis for I, then $f \in I$ if and only if $f \longrightarrow_G 0$, so for each $f \in I$, $f = \sum_{i=1}^{k} u_i g_i$, i.e. G generates I. □

Proposition 3.22. *If $G = \{g_1, \ldots, g_k\}$ is a Gröbner basis of $I = (g_1, \ldots, g_k)$ and $f \in R = k[x_1, \ldots, x_n]$, then the remainder of f with respect to G is* unique.

Proof. Suppose $f = \sum_{i=1}^{k} u_i g_i + r$ and $f = \sum_{i=1}^{k} v_i g_i + r'$ where $u_i, v_i, r, r' \in R$, r, r'

are reduced with respect to G and $\text{in}_\tau(f) \geq \max\{\text{in}_\tau(u_1g_1, \ldots, \text{in}_\tau(u_kg_k))\}$ and $\text{in}_\tau(f) \geq \max\{\text{in}_\tau(v_1g_1, \ldots, \text{in}_\tau(u_kv_k))\}$ (by 3.14). Then

$$r - r' = f - \sum_{i=1}^{k} u_ig_i - (f - \sum_{i=1}^{k} v_ig_i) = \sum_{i=1}^{k} v_ig_i - \sum_{i=1}^{k} u_ig_i$$

Hence, by ideal membership, $r - r' \in I$ and, since G is a Gröbner basis of I, then $\text{in}_\tau(r - r') \in (\text{in}_\tau(g_1), \ldots, \text{in}_\tau(g_k))$. Suppose that $r \neq r'$. Then $r - r'$ is nonzero and so $\text{in}_\tau(r - r')$ is nonzero. Then $\text{in}_\tau(r - r')$ is a monomial in either r or r' since we can look at the terms of r and r' individually and then compare to see which is greater, which will be divisible by $\text{in}_\tau(g_i)$ for some i since $\text{in}_\tau(r - r') \in (\text{in}_\tau(g_1), \ldots, \text{in}_\tau(g_k))$. This contradicts the fact that r and r' are reduced with respect to G, i.e. $\text{in}_\tau(g_i) \nmid \text{in}_\tau(r)$ for all i and $\text{in}_\tau(g_i) \nmid \text{in}_\tau(r')$ for all i. Therefore $r = r'$. □

Remark 3.23. We can create an explicit algorithm for using the Division Algorithm (3.14). If we want to find the expression for f with respect to G , we write $\overline{f}^G$ for some choice of the remainder of f with respect to G, determined by the following:

- If $\text{in}_\tau(f) \in (\text{in}_\tau(g_1), \ldots, \text{in}_\tau(g_k))$, then choose the least i such that $\text{in}_\tau(g_i)|\text{in}_\tau(f)$ and set $\overline{f}^G = \overline{f - \frac{\text{lt}_\tau(f)}{\text{lt}_\tau(g_i}(g_i)}^G$.
  - Suppose that $\text{in}_\tau(f) = m{\cdot}\text{in}_\tau(g_i)$ then there exists a $\lambda \in$ k such that $\text{lt}_\tau(f) = \lambda(m{\cdot}\text{lt}_\tau(g_i))$. So then $f - \frac{\text{lt}_\tau(f)}{\text{lt}_\tau(g_i}(g_i) = f - \lambda m g_i$ which will cancel the leading terms of f and g_i. Then you repeat from the beginning with $f - \frac{\text{lt}_\tau(f)}{\text{lt}_\tau(g_i}(g_i)$ instead of f.

- If $\mathrm{in}_\tau(f) \notin (\mathrm{in}_\tau(g_1), \ldots, \mathrm{in}_\tau(g_k))$, then set $\overline{f}^G = \mathrm{lt}_\tau(f) + \overline{f - \mathrm{lt}_\tau(f)}^G$ (and then repeat the process from the beginning with $f - \mathrm{lt}_\tau(f)$ instead of f).

Chapter 4

Buchberger's Algorithm

In this chapter, we state and prove an algorithm to compute a Gröbner basis for an ideal of a polynomial ring. This algorithm is called "Buchberger's Algorithm." In order to state this algorithm, we also define the S-polynomial which is a method of canceling the lead terms of two polynomials to create a new polynomial (if the original polynomials were in the same ideal then the new polynomial will also be in the ideal). The examples in this chapter are both written examples and Macaulay2 examples.

Definition 4.1. *Let τ be a monomial ordering on $R = k[x_1, x_2, \ldots, x_n]$. Let $I \subseteq R$ be an ideal of R and let $G = \{g_1, \ldots, g_s\}$ be a Gröbner basis of I. We say that G is:*

1. ***minimal*** *if $\frac{\mathrm{lt}_\tau(g_i)}{\mathrm{in}_\tau(g_i)} = 1$ for every i (i.e. every leading term is a monomial) and $\{\mathrm{in}_\tau(g_1), \ldots, \mathrm{in}_\tau(g_s)\}$ is a minimal generating set of $\mathrm{in}_\tau(I)$.*

2. ***reduced*** *if G is minimal and each g_i is reduced with respect to $G_i = G\backslash\{g_i\}$ (i.e. $\text{in}_\tau(g_j)$ does not divide any term of g_i for all $j \neq i$).*

Proposition 4.2. *Let τ be a monomial ordering on $R = k[x_1, x_2, \ldots, x_n]$. Let I be an ideal of R. Then I has a unique reduced Gröbner basis.*

Proof.

Existence: Let $G = \{g_1, \ldots, g_s\}$ be any Gröbner basis of I. We can first make G *minimal* by first choosing a subset that minimally generates $\text{in}_\tau(I)$ and then multiplying each g_i by the unit $\frac{\text{in}_\tau(g_i)}{\text{lt}_\tau(g_i)}$. Now let $\overline{g_i}$ denote the remainder of g_i with respect to G_i. Then $\{\overline{g_i} : 1 \leq i \leq s\}$ is a reduced Gröbner basis of I since (1) $\text{in}_\tau(\overline{g_i}) = \text{in}_\tau(g_i)$ and (2) and $\overline{g_i}$ is reduced with respect to G_i. The first statement is because, by the 3.14, we can write $g_i = \sum_{j\neq i} u_j g_j + \overline{g_i}$ where $\text{in}_\tau(g_i) \geq \max\{\text{in}_\tau(u_j g_j), \text{in}_\tau(\overline{g_i})\}$, but g_i and g_j are minimal, so $u_j = 1$ for all j and so $\text{in}_\tau(g_i) \geq \max\{\text{in}_\tau(g_j), \text{in}_\tau(\overline{g_i})\}$ and, again by minimality, $\text{in}_\tau(g_i) \neq \text{in}_\tau(g_j)$ (minimally generating) so it must be the case that $\text{in}_\tau(g_i) = \text{in}_\tau(\overline{g_i})$.

Uniqueness: Suppose that $G = \{g_1, \ldots, g_s\}$ and $H = \{h_1, \ldots, h_t\}$ are both reduced Gröbner bases for I. First $s = t$ and, after renumbering $\text{in}_\tau(g_i) = \text{in}_\tau(h_i)$ for all i. So now assume that $g_i \neq h_i$ for some i. Then $\text{in}_\tau(g_i - h_i) < \text{in}_\tau(g_i)$ since g_i and h_i are both minimal so $\frac{\text{lt}_\tau(g_i)}{\text{in}_\tau(g_i)} = frac\text{lt}_\tau(h_i)\text{in}_\tau(h_i) = 1$ and $\text{in}_\tau(g_i) = \text{in}_\tau(h_i)$ so $g_i - h_i$ cancels the lead term of g_i and h_i. We also have that $\text{in}_\tau(g_i - h_i) \in \text{in}_\tau(I)$ since both g_i and h_i are in I. Hence there is a $j(\neq i)$ such that $\text{in}_\tau(g_j) = \text{in}_\tau(h_j)|\text{in}_\tau(g_i - h_i)$. This means that either g_i or h_i is not reduced with respect to G_i or H_i, respectively.

But this contradicts that G and H are reduced. $\square$

Definition 4.3. *Let τ be a monomial ordering on $R = k[x_1, \ldots, x_n]$. Let f and g be polynomials in R. Then we define the* ***S-polynomial*** *by*

$$S(f,g) = \frac{\text{lcm}(\text{in}_\tau(f), \text{in}_\tau(g))}{\text{lt}_\tau(f)} f - \frac{\text{lcm}(\text{in}_\tau(f), \text{in}_\tau(g))}{\text{lt}_\tau(g)} g$$

Example 4.4. Let $R = k[x,y,z]$. Let τ be the *deglex* monomial ordering with $x >_\tau y >_\tau z$. Let $I = (g_1, g_2)$ be an ideal of R with $g_1 = xy - z^2$ and $g_2 = y^2 - xz$. $\text{in}_\tau(g_1) = xy$ and $\text{in}_\tau(g_2) = xz$ and so

$S(g_1,g_2) = \frac{\text{lcm}(\text{in}_\tau(g_1),\text{in}_\tau(g_2))}{\text{lt}_\tau(g_1)} g_1 - \frac{\text{lcm}(\text{in}_\tau(g_1),\text{in}_\tau(g_2))}{\text{lt}_\tau(g_2)} g_2 =$

$\frac{\text{lcm}(xy,xz)}{xy}(xy - z^2) - \frac{\text{lcm}(xy,xz)}{-xz}(y^2 - xz) = \frac{xyz}{xy}(xy - z^2) - \frac{xyz}{-xz}(y^2 - xz) =$

$z(xy - z^2) + y(y^2 - xz) = xyz - z^3 + (y^3 - xyz) = y^3 - z^3.$

Example 4.5. Let $R = k[a,b,c,d,e,f]$, let τ be a relex monomial ordering on R with $a >_\tau b >_\tau c >_\tau d >_\tau e >_\tau f$, and let $I = (b^3c, d^2f^3, abe, a^9df - c^{11}, a^2c^2d^2 - e^6)$ be an ideal of R. Let $g_1 = b^3c, g_2 = d^2f^3, g_3 = abe, g_4 = a^9df - c^{11}, g_5 = a^2c^2d^2 - e^6$.

1. $S(g_1,g_2) = \frac{b^3cd^2f^3}{b^3c}(b^3c) - \frac{b^3cd^2f^3}{d^2f^3}(d^2f^3) = 0$

2. $S(g_1,g_3) = \frac{ab^3ce}{b^3c}(b^3c) - \frac{ab^3ce}{abe}(abe) = 0$

3. $S(g_1,g_4) = \frac{b^3c^{11}}{b^3c}(b^3c) - \frac{b^3c^{11}}{-c^{11}}(a^9df - c^{11}) = b^3c^{11} + a^9b^3df - b^3c^{11} = a^9b^3df$

4. $S(g_1,g_5) = \frac{a^2b^3c^2d^2}{b^3c}(b^3c) - \frac{a^2b^3c^2d^2}{a^2c^2d^2}(a^2c^2d^2 - e^6) = a^2b^3c^2d^2 - a^2b^3c^2d^2 + b^3e^6 = b^3e^6$

5. $S(g_2, g_3) = \frac{abd^2ef^3}{d^2f^3}(d^2f^3) - \frac{abd^2ef^3}{abe}(abe) = 0$

6. $S(g_2, g_4) = \frac{c^{11}d^2f^3}{d^2f^3}(d^2f^3) - \frac{c^{11}d^2f^3}{-c^{11}}(a^9df - c^{11}) = c^{11}d^2f^3 + a^9d^3f^4 - c^{11}d^2f^3 = a^9d^3f^4$

7. $S(g_2, g_5) = \frac{a^2c^2d^2f^3}{d^2f^3}(d^2f^3) - \frac{a^2c^2d^2f^3}{a^2c^2d^2}(a^2c^2d^2 - e^6) = a^2c^2d^2f^3 - a^2c^2d^2f^3 + e^6f^3 = e^6f^3$

8. $S(g_3, g_4) = \frac{abc^{11}e}{abe}(abe) - \frac{abc^{11}e}{-c^{11}}(a^9df - c^{11}) = abc^{11}e + a^{10}bdef - abc^{11}e = a^{10}bdef$

9. $S(g_3, g_5) = \frac{a^2bc^2d^2e}{abe}(abe) - \frac{a^2bc^2d^2e}{a^2c^2d^2}(a^2c^2d^2 - e^6) = a^2bc^2d^2e - a^2bc^2d^2e + be^7 = be^7$

10. $S(g_4, g_5) = \frac{a^2c^{11}d^2}{-c^{11}}(a^9df - c^{11}) - \frac{a^2c^{11}d^2}{a^2c^2d^2}(a^2c^2d^2 - e^6) = -a^{11}d^3f + a^2c^{11}d^2 - a^2c^{11}d^2 + c^7e^6 = c^7e^6 - a^{11}d^3f$

Remark 4.6.

- The S-polynomial generates a new polynomial in the ideal generated by f and g. Specifically, the S-polynomial cancels the leading terms of f and g.
- It is clear that $S(f, g) = -S(g, f)$ by switching the roles of f and g in the defined equation.

Theorem 4.7 (Buchberger's Criterion)**.** *Let τ be a monomial ordering on $R = k[x_1, x_2, \ldots, x_n]$. Let $I = (g_1, \ldots, g_s)$ be an ideal of R. Let $G = \{g_1, \ldots, g_s\}$. Fix remainders of $S(g_i, g_j)$ with respect to G, say $\overline{S(g_i, g_j)}^G$. Then $G = \{g_1, \ldots, g_s\}$ is a Gröbner basis for I if and only if $\overline{S(g_i, g_j)}^G = 0$ for all i, j where $1 \leq i < j \leq s$.*

Proof.

$\underline{(\Leftarrow)}$: Assume that G is a Gröbner basis for I. Since g_i, $g_j \in I$ then $S(g_i, g_j) = \frac{\text{lcm}(\text{in}_\tau(g_i), \text{in}_\tau(g_j))}{\text{lt}_\tau(g_i)} g_i - \frac{\text{lcm}(\text{in}_\tau(g_i), \text{in}_\tau(g_j))}{\text{lt}_\tau(g_j)} g_j \in I$ by ideal membership. Then $\overline{S(g_i, g_j)}^G = 0$ (by 3.20).

$\underline{(\Rightarrow)}$: Now suppose that $\overline{S(g_i, g_j)}^G = 0$ for all $i, j, 1 \leq i < j \leq s$. Suppose that G *is not a Gröbner basis for* I (for proof by contradiction). Choose $f \in I$ such that:

1. $\text{in}_\tau(f) \in (\text{in}_\tau(g_1, \ldots, \text{in}_\tau(g_s))$ (which exists since G is not a Gröbner basis),

2. among all expressions $f = \sum f_i g_i$ (we can write it in this form since $f \in I = (g_1, \ldots, g_s)$) and $\max\{\text{in}_\tau(f_i g_i) : i = 1, \ldots, s\} =: m$ is minimal (i.e. the maximum is minimal among all others in the set), and

3. among all other expressions as in (2) where m is maximum, m occurs a minimal number of times in the list of the initial monomials $\text{in}_\tau(f_i g_i)$.

Suppose that m only occurs once. Then $m = \text{in}_\tau(f)$. Then $\text{in}_\tau(f_i g_i) = \text{in}_\tau(f_i)\text{in}_\tau(g_i)$ so $m = \text{in}_\tau(f_i)\text{in}_\tau(g_i)$ and since m is the maximum among the $\text{in}_\tau(f_i g_i)$ then $\text{in}_\tau(f) = m = \text{in}_\tau(f_i)\text{in}_\tau(g_i)$ which then implies that $\text{in}_\tau(f) \in (\text{in}_\tau(g_i))$ which contradicts (1). Thus m occurs at least twice. So, without loss of generality, $\text{in}_\tau(f_1 g_1) = \text{in}_\tau(f_2 g_2) = m$.

We will use the S-polynomial $S(g_1, g_2)$ to cancel the two m's and reduce. Note that $\text{in}_\tau(S(g_1, g_2)) < \text{lcm}(\text{in}_\tau(g_1), \text{in}_\tau(g_2))$ (since the S-polynomial cancels the leading terms of g_1 and g_2). Also $\text{in}_\tau(g_i) | m$ for $i = 1, 2$ since $m = \text{in}_\tau(f_i g_i) = \text{in}_\tau(f_i)\text{in}_\tau(g_i)$.

Thus there is a monomial n such that $\text{lcm}(\text{in}_\tau(g_1), \text{in}_\tau(g_2))n = m$.

Let $L_i = \frac{\text{lcm}(\text{in}_\tau(g_1),\text{in}_\tau(g_2))}{\text{lt}_\tau(g_i)}$ for $i = 1, 2$ so that $S(g_1, g_2) = L_1 g_1 - L_2 g_2$. By 3.14 and our assumption that $\overline{S(g_i, g_j)}^G = 0$, we can write $S(g_1, g_2) = \sum_{i=1}^s h_i g_i$, where $\text{in}_\tau(S(g_1, g_2)) \geq \max\{\text{in}_\tau(h_1 g_1), \ldots, \text{in}_\tau(h_s g_s)\}$.

From our construction of f, by (2) we have that $f = \sum_{i=1}^s f_i g_i$. This gives $f = \sum_{i=1}^s f_i g_i + nS(g_1, g_2) - \sum_{i=1}^s nh_i g_i$ (since $S(g_1, g_2) = \sum_{i=1}^s h_i g_i$ so $S(g_1, g_2) - \sum_{i=1}^s h_i g_i = 0$. Then $n(S(g_1, g_2) - \sum_{i=1}^s h_i g_i) = 0)$. Notice that $\text{in}_\tau(nh_i g_i) \leq \text{in}_\tau(nS(g_1, g_2))$ since $\text{in}_\tau(h_i g_i) \leq \text{in}_\tau(S(g_1, g_2))$ by our Division Algorithm sum. Also $\text{in}_\tau(nS(g_1, g_2)) < m$ since $\text{in}_\tau(S(g_1, g_2)) < \text{lcm}(\text{in}_\tau(g_1), \text{in}_\tau(g_2))$ and $\text{lcm}(\text{in}_\tau(g_1), \text{in}_\tau(g_2))n = m$ so $\text{in}_\tau(nS(g_1, g_2)) = \text{in}_\tau(n)\text{in}_\tau(S(g_1, g_2)) < n(\text{lcm}(\text{in}_\tau(g_1), \text{in}_\tau(g_2))) = m$ ($\text{in}_\tau(n) = n$ since n is a monomial). Combining these two inequalities we get $\text{in}_\tau(nh_i g_i) \leq \text{in}_\tau(nS(g_1, g_2)) < m$. So none of the $h_i g_i$ affect the number of m's or the fact that m is maximal.

We can rewrite the equality to

$f = g_1(f_1 + nL_1 - nh_1) + g_2(f_2 - nL_2 - nh_2) + \sum_{i=3}^s (f_i - nh_i)g_i$.

Consider $\text{in}_\tau(g_2(f_2 - nL_2 - nh_2))$. We have that $\text{in}_\tau(g_2 f_2) = m$, $\text{in}_\tau(nh_2 g_2) < m$, and $\text{in}_\tau(ng_2 L_2) = n(\text{in}_\tau(g_2))(\frac{\text{lcm}(\text{in}_\tau(g_1),\text{in}_\tau(g_2))}{\text{in}_\tau(g_2)}) = m$ (where $\text{in}_\tau(L_2) = \text{in}_\tau(\frac{\text{lcm}(\text{in}_\tau(g_1),\text{in}_\tau(g_2))}{\text{lt}_\tau(g_i)}) = \frac{\text{lcm}(\text{in}_\tau(g_1),\text{in}_\tau(g_2))}{\text{in}_\tau(g_i)}$). So, since $\text{in}_\tau(f_2 g_2) = m = \text{in}_\tau(ng_2 L_2)$ and $\text{in}_\tau(nh_2 g_2) < m$, then $\text{in}_\tau(g_2(f_2 - nL_2 - nh_2)) < m$ which decreases the number of times m occurs, which contradicts (3) for our

construction of f.

Therefore, by contradiction, G is a Gröbner basis for I. □

Remark 4.8. Buchberger's Criterion can be turned into an algorithm:

Given $g_1, \ldots, g_s \in I$

1. Compute $\overline{S(g_i, g_j)}^G = h_{ij}$. If $h_{ij} = 0$, then we are done.

2. If $h_{ij} \neq 0$, replace $\{g_1, \ldots, g_s\}$ by $\{g_1, \ldots, g_s, h_{ij}\}$ and repeat (that way the nonzero $\overline{S(g_i, g_j)}^G = h_{ij}$ will now reduce to 0).

Example 4.9. [11] Let $R = k[x, y, z]$. Let τ be the *deglex* monomial ordering with $x >_\tau y >_\tau z$. Let $I = (g_1, g_2)$ be an ideal of R with $g_1 = xy - z^2$ and $g_2 = y^2 - xz$. We want to find a reduced Gröbner basis for I with respect to τ.

1. Let $G = \{g_1, g_2\}$. $\text{in}_\tau(g_1) = xy$ and $\text{in}_\tau(g_2 = xz$ and so $S(g_1, g_2) = y^3 - z^3$ (which was calculated in 4.4). Note that $\text{in}_\tau(y^3 - z^3) = y^3$. Since $\text{in}_\tau(g_1) \nmid \text{in}_\tau(y^3 - z^3)$ and $\text{in}_\tau(g_2) \nmid \text{in}_\tau(y^3 - z^3)$ then $y^3 - z^3$ is reduced with respect to G, hence $\overline{S(g_1, g_2)}^G \neq 0$.

2. Now let $g_3 = y^3 - z^3$ and $G = \{g_1, g_2, g_3\}$. Note that $\text{in}_\tau(y^3 - z^3) = y^3$. Then the S-polynomials are:

   - $S(g_1, g_2) = y^3 - z^3 \Rightarrow \overline{S(g_1, g_2)}^G = 0$
   - $S(g_1, g_3) = y^2(xy - z^2) - x(y^3 - z^3) = xy^3 - y^2z^2 - xy^3 + xz^3 = xz^3 - y^2z^2 = z^2(xz - y^2) = z^2 g_2 \Rightarrow \overline{S(g_1, g_3)}^G = 0$

- $S(g_2, g_3) = -y^3(y^2 - xz) - xz(y^3 - z^3) = -y^5 + xy^3z - xy^3z + xz^4 = -y^5 + xz^4$
  And so $\overline{S(g_2, g_3)}^G = \overline{xz^4 - y^5 + z^3(y^2 - xz)}^G = \overline{y^2z^3 - y^5}^G =$
  $\overline{y^2z^3 - y^5 + y^2(y^3 - z^3)}^G = 0$

So by 4.7, $\{g_1, g_2, g_3\}$ is a Gröbner basis for I.

Example 4.10. Sometimes computing the Gröbner basis can be long and tedious. In this example, we will start by computing by hand. Let $R = k[a, b, c, d, e, f]$, let τ be a relex monomial ordering on R with $a >_\tau b >_\tau c >_\tau d >_\tau e >_\tau f$, and let $I = (b^3c, d^2f^3, abe, a^9df - c^{11}, a^2c^2d^2 - e^6)$ be an ideal of R. Let $g_1 = b^3c, g_2 = d^2f^3, g_3 = abe, g_4 = a^9df - c^{11}, g_5 = a^2c^2d^2 - e^6$. (These preliminary S-polynomials were already calculated in 4.5).

1. $S(g_1, g_2) = 0$
2. $S(g_1, g_3) = 0$
3. $S(g_1, g_4) = a^9b^3df \notin (\text{in}_\tau(g_1), \text{in}_\tau(g_2), \text{in}_\tau(g_3), \text{in}_\tau(g_4), \text{in}_\tau(g_5))$
4. $S(g_1, g_5) = b^3e^6 \notin (\text{in}_\tau(g_1), \text{in}_\tau(g_2), \text{in}_\tau(g_3), \text{in}_\tau(g_4), \text{in}_\tau(g_5))$
5. $S(g_2, g_3) = 0$
6. $S(g_2, g_4) = a^9d^3f^4 \in (\text{in}_\tau(g_1), \text{in}_\tau(g_2), \text{in}_\tau(g_3), \text{in}_\tau(g_4), \text{in}_\tau(g_5))$ since
   $a^9d^3f^4 = a^9df(d^2f^3)$
7. $S(g_2, g_5) = e^6f^3 \notin (\text{in}_\tau(g_1), \text{in}_\tau(g_2), \text{in}_\tau(g_3), \text{in}_\tau(g_4), \text{in}_\tau(g_5))$

8. $S(g_3, g_4) = a^{10}bdef \in (\text{in}_\tau), \text{in}_\tau(g_2), \text{in}_\tau(g_3), \text{in}_\tau(g_4), \text{in}_\tau(g_5))$ since

   $a^{10}bdef = a^9df(abe)$

9. $S(g_3, g_5) = be^7 \notin (\text{in}_\tau(g_1), \text{in}_\tau(g_2), \text{in}_\tau(g_3), \text{in}_\tau(g_4), \text{in}_\tau(g_5))$

10. $S(g_4, g_5) = c^7e^6 - a^{11}d^3f$ so

    $\text{in}_\tau(S(g_4, g_5)) = c^7e^6 \notin (\text{in}_\tau(g_1), \text{in}_\tau(g_2), \text{in}_\tau(g_3), \text{in}_\tau(g_4), \text{in}_\tau(g_5))$.

So to continue calculating the Gröbner basis for I we need to add the polynomials $g_6 = a^9b^3df, g_7 = b^3e^6, g_8 = e^6f^3, g_9 = be^7$, and $g_{10} = c^7 - a^{11}d^3f$ to G and compute all of the S-polynomials of G (with the new variables) to check that the S-polynomials reduce to 0 for each one.

This computation will take several pages to compute by hand. But if we instead put this problem into Macaulay2 it will take a couple of seconds to compute:

```
i1 : R = RR[a,b,c,d,e,f, MonomialOrder => GRevLex, Global => false];

i2 : I = ideal(b^3*c, d^2*f^3, a*b*e, a^9*d*f-c^11, a^2*c^2*d^2-e^6)

              3    2 3            11    9      2 2 2    6
o2 = ideal (b c, d f , a*b*e, - c   + a d*f, a c d  - e )

o2 : Ideal of R

i3 : gens gb(I)
-- warning: experimental computation over inexact field begun
--          results not reliable (one warning given per session)

o3 = | abe b3c d2f3 a2c2d2-e6 be7 e6f3 b3e6 c11-a9df a9b3df c9e6-a11d3f a12bd3f
     ------------------------------------------------------------------------
     c7e12-a13d5f c5e18-a15d7f c3e24-a17d9f ce30-a19d11f e36-a21cd13f |

              1       16
o3 : Matrix R  <--- R
```

So, as can be seen with Macaulay2, the reduced Gröbner basis of I is 16 elements with the largest element being $e^{36} - a^{21}cd^{13}f$ which has degree 36.

Example 4.11. If we setup the example the same as the previous example except now τ is a lex monomial ordering on R then we can compute the Gröbner basis in Macaulay2:

```
i1 : R = RR[a,b,c,d,e,f, MonomialOrder => Lex, Global => false];

i2 : I = ideal(b^3*c, d^2*f^3, a*b*e, a^9*d*f-c^11, a^2*c^2*d^2-e^6)

             3    2 3          9       11   2 2 2    6
o2 = ideal (b c, d f , a*b*e, a d*f - c  , a c d  - e )

o2 : Ideal of R

i3 : gens gb(I)
-- warning: experimental computation over inexact field begun
--          results not reliable (one warning given per session)

o3 = | e6f3 e36f2 e66f e102 d2f3 ce30f2 ce96 c2e60f c3e24f2 c3e90 c4e54f c5e18f2
     ------------------------------------------------------------------------------
     c5e84 c6e48f c7e12f2 c7e78 c8e42f c9e6f2 c9e72 c10e36f c11e66 c11df2 c12e30f
     ------------------------------------------------------------------------------
     c13e60 c14e24f c15e54 c16e18f c17e48 c18e12f c19e42 c20e6f c21e36 c22f c23e30
     ------------------------------------------------------------------------------
     c25e24 c27e18 c29e12 c31e6 c33 be7 bc11e bc13d bc24 b3e6 b3c ae24f-c19d7
     ------------------------------------------------------------------------------
     ac21d9-e30f abe a2c2d2-e6 a3e18f-c17d5 a5e12f-c15d3 a7e6f-c13d a9df-c11 |

             1       53
o3 : Matrix R  <--- R
```

So, as can be seen with Macaulay2, the reduced Gröbner basis of I is 53 elements with the largest element being e^{102} which has degree 102.

So the monomial ordering on R is important when computing the Gröbner bais of an ideal because different monomial orderings can output different Gröbner bases.

Corollary 4.12. *Let τ be a monomial ordering on $R = k[x_1, \ldots, x_n]$. Then*

1. *Any set of monomials is a Gröbner basis for the ideals they generate.*

2. *If I is generated by binomials (i.e. elements of the form $\lambda_A \boldsymbol{x}^A + \lambda_B \boldsymbol{x}^B$), then I has a Gröbner basis of binomials.*

3. *If I is homogeneous, I has a homogeneous Gröbner basis.*

4. *If $(g_1, \ldots, g_s) = I$ and $(\mathrm{in}_\tau(g_i), \mathrm{in}_\tau(g_j)) = 1$ whenever $i \neq j$, then $\{g_1, \ldots, g_s\}$ is a Gröbner basis for I.*

5. *If $\{g_1, \ldots, g_s\}$ is a Gröbner basis for $I = (g_1, \ldots, g_s)$ and $k \subseteq L$ is a field extension, then $\{g_1, \ldots, g_s\}$ is a Gröbner basis for $IL[x_1, \ldots, x_n]$.*

Proof.

1. For any two monomials $a = \boldsymbol{x}^A$, $b = \boldsymbol{x}^B$, $S(\boldsymbol{x}^A, \boldsymbol{x}^B) = 0$.

2. *I need to go back and review this proof becuase I'm not entirely sure about the S-polynomial here* Let $b_1 = \lambda_A \boldsymbol{x}^A + \lambda_B \boldsymbol{x}^B$ and $b_2 = \lambda_C \boldsymbol{x}^C + \lambda_D \boldsymbol{x}^D$ be two binomials where $\boldsymbol{x}^A > \boldsymbol{x}^B$ and $\boldsymbol{x}^C > \boldsymbol{x}^D$ and $\lambda_A \lambda_C \neq 0$. Then $S(b_1, b_2) = \frac{\lambda_A \lambda_C \mathbf{x}^A \mathbf{x}^C}{\lambda_A \mathbf{x}^A}(\lambda_A \mathbf{x}^A + \lambda_B \mathbf{x}^B) - \frac{\lambda_A \lambda_C \mathbf{x}^A \mathbf{x}^C}{\lambda_A \mathbf{x}^A}(\lambda_C \mathbf{x}^C + \lambda_D \mathbf{x}^D) = \lambda_C \lambda_B \mathbf{x}^C \mathbf{x}^B - \lambda_A \lambda_D \mathbf{x}^A \mathbf{x}^D$, which is a binomial.

3. If g_1 and g_2 are *homogeneous* (a *homogeneous polynomial* is a polynomial whose nonzero terms have the same degree), then so is $S(g_1, g_2)$.

4. We will show that if $(\mathrm{in}_\tau(g_1, \mathrm{in}_\tau(g_2)) = 1$, then $\overline{S(g_1, g_2)}^G = 0$ (so then by 4.7, $\{g_1, g_2\}$ is a Gröbner basis. If g_1, g_2 is arbitrary, then true for $\{g_1, \ldots, g_s\}$) for any $G \supseteq \{g_1, g_2\}$. If $(\mathrm{in}_\tau(g_1, \mathrm{in}_\tau(g_2)) = 1$, then $\mathrm{lcm}(\mathrm{in}_\tau(g_1), \mathrm{in}_\tau(g_2)) = \mathrm{in}_\tau(g_1)\mathrm{in}_\tau(g_2)$. Hence there is a nonzero $\lambda \in$ k ($\lambda = \lambda_1\lambda_2$ where $\mathrm{lt}_\tau(g_1) = \lambda_1 \mathrm{in}_\tau(g_1)$ and $\mathrm{lt}_\tau(g_2) = \lambda_2 \mathrm{in}_\tau(g_2)$) such that $\lambda S(g_1, g_2) = \mathrm{lt}_\tau(g_2)g_1 - \mathrm{lt}_\tau(g_1)g_2$ (since $S(g_1, g_2) = \frac{\mathrm{lcm}(\mathrm{in}_\tau(g_1), \mathrm{in}_\tau(g_2))}{\mathrm{lt}_\tau(g_1)} g_1 - \frac{\mathrm{lcm}(\mathrm{in}_\tau(g_1), \mathrm{in}_\tau(g_2))}{\mathrm{lt}_\tau(g_2)} g_2 =$ $\frac{\mathrm{in}_\tau(g_1)\mathrm{in}_\tau(g_2)}{\lambda_1 \mathrm{in}_\tau(g_1)} g_1 - \frac{\mathrm{in}_\tau(g_1)\mathrm{in}_\tau(g_2)}{\lambda_2 \mathrm{in}_\tau(g_2)} g_2 = \frac{\mathrm{in}_\tau(g_2)}{\lambda_1} g_1 - \frac{\mathrm{in}_\tau(g_1)}{\lambda_2} g_2$). For $i = 1, 2$, write $g_i = \mathrm{lt}_\tau(g_i) + h_i$, where $\mathrm{in}_\tau(h_i) < \mathrm{in}_\tau(g_i)$. Then $\lambda S(g_1, g_2) = \mathrm{lt}_\tau(g_2)(\mathrm{lt}_\tau(g_1) + h_1) - \mathrm{lt}_\tau(g_1)(\mathrm{lt}_\tau(g_2) + h_2) =$ $\mathrm{lt}_\tau(g_2)h_1 - \mathrm{lt}_\tau(g_1)h_2 = \mathrm{lt}_\tau(g_2)h_1 + h_2h_1 - h_2h_1 - \mathrm{lt}_\tau(g_1)h_2 =$ $(\mathrm{lt}_\tau(g_2) + h_2)h_1 - (\mathrm{lt}_\tau(g_1) + h_1)h_2 = g_2h_1 - g_1h_2$. If $\mathrm{in}_\tau(g_1)\mathrm{in}_\tau(h_2) = \mathrm{in}_\tau(g_2)\mathrm{in}_\tau(h_1)$ then $(\mathrm{in}_\tau(g_1), \mathrm{in}_\tau(g_2)) = 1$ forces $\mathrm{in}_\tau(g_1) | \mathrm{in}_\tau(h_1)$ and $\mathrm{in}_\tau(g_2) | \mathrm{in}_\tau(h_2)$ which is a contradiction since $\mathrm{in}_\tau(h_i) < \mathrm{in}_\tau(g_i)$. Hence $\mathrm{in}_\tau(g_1)\mathrm{in}_\tau(h_2) \neq \mathrm{in}_\tau(g_2)\mathrm{in}_\tau(h_1)$. Thus $\mathrm{in}_\tau(\lambda S(g_1, g_2)) \geq \max\{\mathrm{in}_\tau(g_1h_2), \mathrm{in}_\tau(g_2h_1)\}$ since it is equal to one of them. Therefore $\overline{S(g_1, g_2)}^G = 0$ by 3.14 and definition of $\overline{S(g_1, g_2)}^G = 0$.

5. This is clear since the S-polynomial calculations and the steps in the division algorithm are all performed over the ground field.

□

Example 4.13. Let $R = k[a, b, c, d, e, f]$, let τ be a revlex monomial ordering on R and let $I = (ab - cf^6, c^2d^2 + abe^2, e^3 - f^3, f)$. Let $g_1 = ab - cf^6, g^2 = c^2d^2 + abe^2, g_3 = e^3 - f_3$, and $g_4 = f$. We could calculate the Gröbner basis for I by computing the S-polynomials for each pair (g_i, g_j), but instead if we notice that $(\text{in}_\tau(g_1), \text{in}_\tau(g_2) = (\text{in}_\tau(g_1), \text{in}_\tau(g_3) = (\text{in}_\tau(g_1), \text{in}_\tau(g_4) = (\text{in}_\tau(g_2), \text{in}_\tau(g_3) = (\text{in}_\tau(g_2), \text{in}_\tau(g_4) = (\text{in}_\tau(g_3), \text{in}_\tau(g_4) = 1$ then, by 4.12 part (4), $G = \{g_1, g_2, g_3, g_4\}$ is a Gröbner basis for I. We can verify this with Macaulay2:

```
i1 : R = RR[a,b,c,d,e,f, MonomialOrder => GRevLex, Global => false];

i2 : I = ideal(a*b - c*f^6, c^2*d^2 + a*b*e^2, e^3-f^3, f)

                  6         2 2        2   3    3
o2 = ideal (- c*f  + a*b, c d  + a*b*e , e  - f , f)

o2 : Ideal of R

i3 : gens gb(I)
-- warning: experimental computation over inexact field begun
--          results not reliable (one warning given per session)

o3 = | f ab e3 c2d2 |

              1       4
o3 : Matrix R  <--- R
```

The Gröbner basis that Macaulay2 calculated just included in initial terms of each of our g_i's, but the Gröbner basis is still involves just our preliminary polynomials.

Chapter 5

Elimination

In this chapter we state and prove the Elimination theorem related to Gröbner bases which says that a Gröbner basis for the ideal of a polynomial ring that is a particular subset of the original polynomial ring can be calculated using the Gröbner basis in the larger polynomial ring. A corollary of this theorem states how we can find the kernel of a mapping of change of variables. The examples in this chapter are both written examples and Macaulay2 examples. Some familiar theorems are referenced from *Abstract Algebra*. 3rd ed. by David Steven Dummit and Richard M. Foote. [4]

Theorem 5.1 (Elimination)**.** *Let $R = k[x_1, x_2, \ldots, x_n]$ and let I be an ideal of R. Let τ be a lex order on R. Then:*

1. $\text{in}_\tau(I) \cap k[x_i, x_{i+1}, \ldots, x_n] = \text{in}_\tau(I \cap k[x_i, x_{i+1}, \ldots, x_n])$.

2. *Let* $\{f_1, \ldots, f_s\}$ *be a Gröbner basis of* I. *Then* $\{f_1, \ldots, f_s\} \cap k[x_i, x_{i+1}, \ldots, x_n]$ *is a Gröbner basis of* $I \cap k[x_i, x_{i+1}, \ldots, x_n]$.

Proof.

1. Let $m \in \text{in}_\tau(I) \cap k[x_i, x_{i+1}, \ldots, x_n]$. Since m is in $\text{in}_\tau(I)$, then, by definition of $\text{in}_\tau(I)$, there is an element $f \in I$ such that $\text{in}_\tau(f) = m$. Since τ is a lex ordering, it follows that f cannot have any nonzero terms with $x_1, x_2, \ldots$ or x_{i-1}. If f did have a term containing some $x_k \in \{x_1, x_2, \ldots, x_{i-1}\}$ then, because of the lex ordering, $\text{in}_\tau(f)$ would be a monomial involving x_k and so $\text{in}_\tau(f) \notin \text{in}_\tau(I) \cap k[x_i, x_{i+1}, \ldots, x_n]$, a contradiction. Thus f is in $k[x_i, x_{i+1}, \ldots, x_n]$ and so $f \in I \cap k[x_i, x_{i+1}, \ldots, x_n]$ and $m = \text{in}_\tau(f) \in \text{in}_\tau(I \cap k[x_i, x_{i+1}, \ldots, x_n])$. Therefore $\text{in}_\tau(I) \cap k[x_i, x_{i+1}, \ldots, x_n] \subseteq \text{in}_\tau(I \cap k[x_i, x_{i+1}, \ldots, x_n])$. Also it is clear that for $g \in I \cap k[x_i, x_{i+1}, \ldots, x_n]$, then since $g \in I$ then $\text{in}_\tau(g) \in \text{in}_\tau(I)$ and since $g \in k[x_i, x_{i+1}, \ldots, x_n]$ then $\text{in}_\tau(g) \in k[x_i, x_{i+1}, \ldots, x_n]$. Hence $\text{in}_\tau(g) \in \text{in}_\tau(I) \cap k[x_i, x_{i+1}, \ldots, x_n]$ and $\text{in}_\tau(I) \cap k[x_i, x_{i+1}, \ldots, x_n] \subseteq \text{in}_\tau(I \cap k[x_i, x_{i+1}, \ldots, x_n])$. Therefore, $\text{in}_\tau(I) \cap k[x_i, x_{i+1}, \ldots, x_n] = \text{in}_\tau(I \cap k[x_i, x_{i+1}, \ldots, x_n])$.

2. Since $\{f_1, \ldots, f_s\}$ is a Gröbner basis of I, then $\text{in}_\tau(I) = (m_1, \ldots, m_s)$ where $m_i = \text{in}_\tau(f_i)$. Suppose that $m_1, \ldots, m_j \in k[x_i, x_{i+1}, \ldots, x_n]$, but $m_{j+1}, \ldots, m_s \notin k[x_i, x_{i+1}, \ldots, x_n]$. Then, by part (1) above, we have that

$m_1, \ldots, m_j \in \text{in}_\tau(I) \cap k[x_i, x_{i+1}, \ldots, x_n] = \text{in}_\tau(I \cap k[x_i, x_{i+1}, \ldots, x_n])$, so $f_1, \ldots, f_j \in I \cap k[x_i, x_{i+1}, \ldots, x_n]$. Importantly, $f_1, \ldots, f_j \in k[x_i, x_{i+1}, \ldots, x_n]$. So clearly $\{f_1, \ldots, f_s\} \cap k[x_i, x_{i+1}, \ldots, x_n] = \{f_1, \ldots, f_j\}$. If we have that $g \in I \cap k[x_i, x_{i+1}, \ldots, x_n]$ then $\text{in}_\tau(g) \in \text{in}_\tau(I \cap k[x_i, x_{i+1}, \ldots, x_n]) = \text{in}_\tau(I) \cap k[x_i, x_{i+1}, \ldots, x_n]$ by part (1) above and so, since $\text{in}_\tau(I) = (m_1, m_2, \ldots, m_s)$, $\text{in}_\tau(g) \in (m_1, m_2, \ldots, m_s) \cap k[x_i, x_{i+1}, \ldots, x_n] = (m_1, m_2, \ldots, m_j)$ (in $k[x_i, x_{i+1}, \ldots, x_n]$). Therefore $\{f_1, f_2, \ldots, f_j\}$ is a Gröbner basis for $k[x_i, x_{i+1}, \ldots, x_n]$.

□

Example 5.2. (A good application of 5.1) Let $I = (xy - t^2, y^2)$. We want to figure out if $t \in \sqrt{I}$. Suppose $t^n \in I$ for some n. Then $t^n \in I \cap k[t]$. Let τ be a lex ordering with $x >_\tau y >_\tau t$. Set $f_1 = xy - t^2$ and $f_2 = y^2$ Then $\text{in}_\tau(f_1) = xy$ and $\text{in}_\tau(f_2) = y^2$. Set $f_3 = y(xy - t^2) - x(y^2) = xy^2 - yt^2 - xy^2 = -yt^2$ and so $\text{in}_\tau(f_3) = yt^2$. Set $f_4 = t^2(xy - t^2) + x(-yt^2) = xyt^2 - t^4 - xyt^2 = -t^4$ and $\text{in}_\tau(f_4) = t^4$. Thus, with lex ordering, $\text{in}_\tau(I) = (xy, y^2, yt^2, t^4)$. Thus $\{f_1, f_2, f_3, f_4\}$ is a Gröbner basis for I. By 5.1 part (2) we have that $\{f_1, f_2, f_3, f_4\} \cap k[t] = \{xy - t^2, y^2, -yt^2, -t^4\} \cap k[t] = \{-t^4\}$ is a Gröbner basis for $I \cap k[t]$. Importantly $t^4 \in I$ and so $t \in \sqrt{I}$.

Example 5.3. (Macaulay2) This is the same as 5.2 but written in Macaulay2 code.

```
i1 : --This line sets up the polynomial ring with lex order x>y>t
     --The "Eliminate 2" means we are going to use Elimination
     --to get rid of the first two variables
     R = QQ[x, y, t, MonomialOrder => Eliminate 2]

o1 = R

o1 : PolynomialRing

i2 : --This line sets up our ideal
     I = ideal(x*y - t^2, y^2)

                    2   2
o2 = ideal (x*y - t , y )

o2 : Ideal of R

i3 : --This is our Grobner basis for I
     gens gb(I)

o3 = | t4 yt2 y2 xy-t2 |

              1       4
o3 : Matrix R  <--- R

i4 : --This is the Elimination step, eliminating x and y
     selectInSubring(1, gens gb(I))

o4 = | t4 |

              1       1
o4 : Matrix R  <--- R
```

Lemma 5.4. *(First Isomorphism Theorem for Rings) If ϕ: $R \to S$ is a homomorphism of rings, then the kernel of ϕ is an ideal of R, the image of ϕ is a subring of S, and $R/ker(\phi)$ is isomorphic as a ring to $\phi(R)$.*

Proof. [4] the kernel of ϕ is a subring of R: If $\alpha, \beta \in \ker(\phi)$ then $\phi(\alpha) = \phi(\beta) = 0$. Hence $\phi(\alpha - \beta) = 0$ and $\phi(\alpha\beta) = 0$, so $\ker(\phi)$ is closed under subtraction and under multiplication, so is a subring of R. Smilarly, for any $r \in R$ we have $\phi(r\alpha) = \phi(r)\phi(\alpha) = \phi(r)0 = 0$, and also $\phi(\alpha r) = \phi(\alpha)\phi(r) = 0\phi(r) = 0$, so $r\alpha, \alpha r \in \ker(\phi)$.

the kernel of ϕ is an ideal of R: If I is the kernel of ϕ, then the cosets (under addition) of I are precisely the fibers of ϕ. In particular, the cosets $r + I$, $s + I$, and $rs + I$ are the fibers of ϕ over $\phi(r)$, $\phi(s)$, and $\phi(rs)$, respectively. Since ϕ is a ring homomorphism $\phi(r)\phi(s) = \phi(rs)$, hence $(r + I)(s + I) = rs + I$. Multiplication of cosets is well-defined and so I is an ideal and R/I is a ring.

the image of ϕ is a subring of S: If $s_1, s_2 \in \mathrm{Im}(\phi)$ then $s_1 = \phi(r_1)$ and $s_2 = \phi(r_2)$ for some $r_1, r_2 \in R$. Then $\phi(r_1 - r_2) = s_1 - s_2$ and $\phi(r_1 r_2) = s_1 s_2$. This shows $s_1 - s_2, s_1 s_2 \in \mathrm{Im}(\phi)$, so the image of ϕ is closed under subtraction and multiplication, hence is a subring of S.

$R/ker(\phi)$ is isomorphic as a ring to $\phi(R)$:The correspondence $r + I \mapsto \phi(r)$ is a bijection between the rings R/I and $\phi(R)$ which respects addition and multiplication, hence is a ring isomorphism. □

Theorem 5.5. *Let k be a field . The polynomial ring $k[x]$ is a Euclidean Domain. Specifically, if $f(x)$ and $g(x)$ are two polynomials in $k[x]$ with $f(x)$ nonzero, then there are* unique *$q(x)$ and $r(x)$ in $k[x]$ such that $g(x) = q(x)f(x) + r(x)$ where $deg(r(x)) = 0$ or $deg(r(x)) < deg(f(x))$.*

Proof. [4] Existence: If $g(x) = 0 \Rightarrow q(x) = r(x) = 0$ so assume $g(x) \neq 0$. We will prove existence by induction on $n = \deg(g(x))$. Let $\deg(f(x)) = m$. If $n < m \Rightarrow q(x) = 0$ and $r(x) = g(x)$. Otherwise $n \geq m$. Let $g(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ and $f(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$. Then $g_1(x) = g(x) - \frac{a_n}{b_m}x^{n-m}f(x)$ is of degree less than n (since the leading term for x^n is $a_n x^n - \frac{a_n}{b_m}b_m x^{n-m}(x^m) = a_n x^n - a_n x^n = 0$). Since k is a field and $b_m \neq 0$ then this is well-defined. Then by induction $\exists q_1(x), r(x)$ such that $g_1(x) = q_1(x)f(x) + r(x)$ with $r(x) = 0$ or $\deg(r(x)) < \deg(f(x))$. Let $q(x) = q_1(x) + \frac{a_n}{b_m}x^{n-m}$. Then $g(x) - \frac{a_n}{b_m}x^{n-m}f(x) = (q(x) - \frac{a_n}{b_m}x^{n-m})f(x) + r(x)$. Thus $g(x) = q(x)f(x) + r(x)$ where $\deg(r(x)) = 0$ or $\deg(r(x)) < \deg(f(x))$.

Uniqueness: Suppose $g(x) = q(x)f(x) + r(x) = q'(x)f(x) + r'(x)$ with $\deg(r(x)) = 0$ or $\deg(r(x)) < \deg(f(x))$ and $\deg(r'(x)) = 0$ or $\deg(r'(x)) < \deg(f(x))$. Then $g(x) - q(x)f(x) = r(x)$ and $g(x) - q'(x)f(x) = r'(x)$, which both have degree less than $\deg(f(x)) = m$. So $r(x) - r'(x) = f(x)(q'(x) - q(x))$ also has degree less than m. But $\deg(f(x)(q'(x) - q(x))) = \deg(f(x)) + \deg(q'(x) - q(x)) = m + \deg(q'(x) - q(x)) \leq m$, so $\deg(q'(x) - q(x)) = 0$. Hence $q(x) = u \cdot q'(x)$ and so $q(x) = q'(x)$ since k is a field. This implies that $r(x) = r'(x)$. □

Lemma 5.6. $f(a) = 0 \iff (z - a)|f$.

Proof.

($\Rightarrow$) If you divide $f \in R[z]$ by $(z - a)$ then, by the Division Algorithm, the result is

$f(z) = q(z)(z-a) + r$ where r is a constant since the $\deg(r) < \deg(z-a) = 1$.

Then $f(a) = q(a)(a-a) + r(a) = r(a) = r$ and since $f(a) = 0$, we have that $r = 0$.

($\Leftarrow$) If you divide $f \in R[z]$ by $(z-a)$ then, by the Division Algorithm, the result is

$f(z) = q(z)(z-a) + r$ where r is a constant since the $\deg(r) < \deg(z-a) = 1$.

Since $(z-a)|f$ then $r = 0$. Thus $f(a) = q(a)(a-a) = 0$. □

Lemma 5.7. *Let R be a ring. $R[z]/(z-r) \cong R$ by the evaluation map.*

Proof. Let ϕ be the map $\phi : R[z] \to R$ by $\phi(f) = f(r)$.

ϕ is a ring homomorphism: Let $f, g \in R[z]$.

$\phi(f+g) = (f+g)(r) = f(r) + g(r) = \phi(f) + \phi(g)$.

$\phi(f \cdot g) = (f \cdot g)(r) = f(r) \cdot g(r) = \phi(f) \cdot \phi(g)$.

$\therefore \phi$ is a ring homomorphism.

ϕ is surjective: Let $s \in R$. Then let $f(z) = a_n z^n + \cdots + a_1 z + s \in R[z]$ where $a_i = 0$ for $i \in \{1, \ldots, n\}$. So $\phi(f) = f(r) = s$.

$\therefore \phi$ is a surjective map.

$\ker(\phi) = (z-r)$: $\ker(\phi) = \{f \in R[z] | f(r) = 0\} = (z-r)$ since

$f(r) = 0 \iff (z-r)|f$ by 5.6.

$\therefore R[z]/(z-r) \cong R$ by the First Isomorphism for rings. □

Theorem 5.8. *(Third Isomorphism Theorem for rings) Let I and J be ideals of R with $I \subseteq J$. Then J/I is an ideal of R/I and $(R/I)/(J/I) \cong R/J$.*

Proof.

J/I is an ideal of R/I: Since I and J are ideals, they are nonempty and so $\{j + I : j \in J\}$ are also nonempty. Let $j_1, j_2, j \in J$ and let $r \in R$. Then we have $(j_1 + I) + (j_2 + I) = (j_1 + j_2) + I, (r + I)(j + I) = rj + I$, and $(j + I)(r + I) = jr + I$ by the definition of addition and multiplication on left cosets. Since J is an ideal then $j_1 + j_2, jr, rj \in J$ so J/I is an ideal of R/I.

$(R/I)/(J/I) \cong R/J$: Let $\phi : R/I \to R/J$ be the map that sends $r + I$ to $r + J$. Let $r_1 + I = r_2 + I$. Then $r_1 - r_2 \in I$ and since $I \subseteq J$ then $r_1 - r_2 \in J$ and so $r_1 + J = r_2 + J$. Therefore $\phi(r_1 + I) = \phi(r_2 + I)$ and so the map is well-defined. We also have that ϕ is surjective since if we have an element $r + J$ in R/J where $r \in R$, then, since $I \subseteq J$, $\phi(r + I) = r + J$. Let $r + I \in \ker(\phi)$. Then $\phi(r + I) = r + J = 0 + J$. So $r - 0 = r \in J$. Therefore $\ker(\phi) = \{j + I : j \in J\} = J/I$. Thus, by the First Isomorphism Theorem for rings, $(R/I)/\ker(\phi) = (R/I)/(J/I) \cong R/J$. □

Corollary 5.9. *Let R be a ring. Then $R[z_1, \ldots, z_m]/(z_1 - r_1, \ldots, z_m - r_m) \cong R$ by the evaluation map.*

Proof. This is just by repetition of 5.7 using $R[z_1, \ldots, z_i]/(z_1 - r_1, \ldots, z_i - r_i) \cong R[z_1, \ldots, z_i]/(z_1 - r_1, \ldots, z_{i-1} - r_{i-1})$ and then "combining" all of the isomorphisms using the Third Isomorphism Theorem. □

Theorem 5.10. *Let $S = k[t_1, \ldots, t_n]$ be a polynomial ring and $f_1, \ldots, f_m \in S$. Let ϕ be the map*

$$\phi : k[x_1, \ldots, x_m] \to k[f_1, \ldots, f_m],$$
$$\phi(x_i) = f_i$$

Let $J = (x_1 - f_1, x_2 - f_2, \ldots, x_n - f_n)$ be an ideal in the polynomial ring $k[t_1, \ldots, t_n, x_1, \ldots, x_m]$. Then $K = ker(\phi) = J \cap k[x_1, \ldots, x_m]$.

Proof. Let $J = (x_1 - f_1, \ldots, x_m - f_m)$ in $k[t_1, \ldots, t_n, x_1, \ldots, x_m]$.

($\supseteq$) $g \in J \cap k[x_1, \ldots, x_m]$. Then $g \in (x_1 - f_1, \ldots, x_m - f_m) = J$. By 5.7/5.9 we have that $k[t_1, \ldots, t_n, x_1, \ldots, x_m]/J = k[t_1, \ldots, t_n, x_1, \ldots, x_m]/(x_1 - f_1, \ldots, x_m - f_m) \cong k[t_1, \ldots, t_n]$ by the natural evaluation map. Let ψ be the isomorphism between $k[t_1, \ldots, t_n, x_1, \ldots, x_m]/(x_1 - f_1, \ldots, x_m - f_m)$ and $k[t_1, \ldots, t_n]$ where $\psi(x_i) = f_i$. Since $g \in (x_1 - f_1, \ldots, x_m - f_m) = J$, then $\psi(g) = g(f_1, \ldots, f_m) = 0$. Therefore $J \cap k[x_1, \ldots, x_m] \subseteq K = \ker(\phi)$.

($\subseteq$) Let $h \in K = \ker(\phi)$. Then $h \in k[x_1, \ldots, x_m]$ by the map ϕ. Since $h \in K = \ker(\phi)$, $h(f_1, \ldots, f_m) = 0$. Then, $h \in (x_1 - f_1, \ldots, x_m - f_m) = J$ and so $h \in J \cap k[x_1, \ldots, x_m]$ and so $K = \ker(\phi) \subseteq J \cap k[x_1, \ldots, x_m]$. □

To find the intersection of J and $k[x_1, \ldots, x_n]$, we can use elimination to "get rid of" the last few variables, using the proper lex ordering. So we can combine 5.1 and 5.10 to compute the kernel of a map. The next couple examples demonstrate this in Macaulay2.

Example 5.11. (Macaulay2) If we have a map from $k[x, y]$ to $k[t]$ defined by $x \mapsto t^2$ and $y \mapsto t^3$ and we want to find the kernel of the map (the values in $k[x, y]$ that map to 0 in $k[t]$) then we can also use elimination, as seen in this example following Theorem 4.3:

```
i1 : R = QQ[t,x,y, MonomialOrder => Eliminate 1]

o1 = R

o1 : PolynomialRing

i2 : I = ideal(t^2-x, t^3-y)

              2       3
o2 = ideal (t  - x, t  - y)

o2 : Ideal of R

i3 : gens gb(I)

o3 = | x3-y2 ty-x2 tx-y t2-x |

              1       4
o3 : Matrix R  <--- R

i4 : selectInSubring(1, gens gb(I))

o4 = | x3-y2 |

              1       1
o4 : Matrix R  <--- R
```

So the kernel of the map is $(x^3 - y^2)$.

Example 5.12. (Macaulay2) If we have a map from $k[a, b, c]$ to $k[x, y]$ defined by $a \mapsto x^2$, $b \mapsto xy$, and $c \mapsto y^2$ and we want to find the kernel of the map (the values

in $k[a,b,c]$ that map to 0 in $k[x,y]$) then we can also use elimination, as seen in this example following Theorem 4.3:

```
i1 : R = QQ[x, y, a, b, c, MonomialOrder => Eliminate 2]

o1 = R

o1 : PolynomialRing

i2 : I = ideal(a-x^2, b-x*y, c-y^2)

                2                     2
o2 = ideal (- x  + a, - x*y + b, - y  + c)

o2 : Ideal of R

i3 : gens gb(I)

o3 = | b2-ac yb-xc ya-xb y2-c xy-b x2-a |

             1       6
o3 : Matrix R  <--- R

i4 : selectInSubring(1, gens gb(I))

o4 = | b2-ac |

             1       1
o4 : Matrix R  <--- R
```

So the kernel of the map is $(b^2 - ac)$.

Chapter 6

Generic Initial Ideals

In this chapter we state and prove Galligo's theorem about existence of generic initial ideals related to Gröbner bases which says there exists a subset of $GL_n(k)$ and a monomial ideal of a polynomial ring such that for each g in this subset, $\text{in}_\tau(gI)$ is equal to the monomial ideal. Prior to this theorem, we have some introductory definitions and theorems. The theorems in this section come from David Eisenbud's *Commutative Algebra with a View Toward Algebraic Geometry* [5].

Let k be a field and let $R = k[x_1, x_2, \ldots, x_n]$ be a polynomial ring. There are three groups that will be used throughout this section:

1. the **general linear group**, $GL_n(k)$, which is the group consisting of all $n \times n$ invertible matrices

2. the **Borel subgroup**, $B_n(k)$, which is the subgroup of $GL_n(k)$ consisting of all upper triangular matrices

(a) We can also think of the Borel subgroup instead as being the subgroup of $GL_n(k)$ consisting of all lower triangular matrices. The subgroup of the lower triangular matrices will be denoted $B'_n(k)$.

3. the **n-dimensional Torus**, $T_n(k)$, which is the subgroup of $GL_n(k)$ consisting of all invertible diagonal matrices (and is hence isomorphic to $(k \setminus \{0\})^n$).

With this definition we have that $T_n(k) \subseteq B_n(k) \subseteq GL_n(k)$.

$GL_n(k)$ acts on R, which is determined by its action on $\{x_1, x_2, \ldots, x_n\}$ (and then extending the action to R). Let $A = (a_{ij})$ be an invertible $n \times n$ matrix, then we define $(A{\cdot}x_1, A{\cdot}x_2, \ldots, A{\cdot}x_n) = (x_1, x_2, \ldots, x_n)(a_{ij})$, i.e. $A{\cdot}x_j = \sum_{i=1}^{n} a_{ij}x_i$. We extend this to a polynomial $f(x_1, x_2, \ldots, x_n) \in R$ by $A{\cdot}f = f(A{\cdot}x_1, A{\cdot}x_2, \ldots, A{\cdot}x_n)$.

Definition 6.1. *[11] An ideal $I \subseteq R = k[x_1, x_2, \ldots, x_n]$ is a* ***strongly stable monomial ideal*** *if the following condition holds: Let $m = x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n} \in I$ be a monomial such that $x_j|m$, then for all $i < j$, $x_i\frac{m}{x_j} = x_1^{a_1}x_2^{a_2}\cdots x_i^{a_i+1}\cdots x_j^{a_j-1}\cdots x_n^{a_n} \in I$.*

Theorem 6.2. *Let k be a field and $R = k[x_1, x_2, \ldots, x_n]$. Suppose $char(k) = 0$. Let I be an ideal of R and let $M = (x_1, x_2, \ldots, x_n)$ (the unique homogeneous maximal ideal). Then:*

1. *I is fixed by $T_n(k)$ (i.e. for all $f \in I$, for any $t \in T_n(k)$, $t{\cdot}f \in I$) if and only if it is generated by monomials.*

2. *I is Borel-fixed (i.e. fixed by the Borel subgroup, $B_n(k)$) if and only if I is a strongly stable monomial ideal.*

3. *I is invariant (i.e. does not change) under the $GL_n(k)$-action if and only if $I = M^d$ for some d.*

Proof.

1. ($\Rightarrow$) Suppose that I is generated by monomials. Let $x^a = x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n} \in I$ be a monomial. Let $t = \begin{bmatrix} t_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & t_n \end{bmatrix} \in T_n(k)$,
then $t{\cdot}x^a = (t_1x_1)^{a_1}(t_2x_2)^{a_2}\cdots(t_nx_n)^{a_n}$ by the action of t where $t{\cdot}x_i^{a_i} = (t_ix_i)^{a_i} = t_i^{a_i}x_i^{a_i}$. So $t{\cdot}x^a = t_1^{a_1}t_2^{a_2}\cdots t_n^{a_n}(x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}) \in I$ by ideal membership. Thus I is fixed by $T_n(k)$.

   ($\Leftarrow$) Suppose that I is fixed by $T_n(k)$. Let $f = \sum_{i=1}^{m} \lambda_i x^{A_i}$ be some polynomial in I where $\lambda_i \neq 0$, $\lambda_i \in k$, $A_i = (a_{i_1}, a_{i_2}, \ldots, a_{i_n})$, and $x^{A_i} = x_1^{a_{i_1}}x_2^{a_{i_2}}\cdots x_n^{a_{i_n}}$. By our assumption that I is fixed by $T_n(k)$, then for all $t \in T_n(k)$, $t{\cdot}f \in I$. It is enough to show that $\lambda_i x^{A_i} \in < t{\cdot}f : t \in T_n(k) >$ since each term of f is an output of t acting on f and since I is fixed then it must be the case that $\lambda_i x_i^{A_i} \in I$ and hence, since f is not a specific polynomial in I, I is generated by monomials.
   Let $t = \begin{bmatrix} t_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & t_n \end{bmatrix} \in T_n(k)$.
   We will denote $t_1^{a_{i_1}}t_2^{a_{i_2}}\cdots t_n^{a_{i_n}}$ by t^{A_i}. We will prove by induction on m that I is generated by monomials.

$\underline{m=2}$: In this case $f = \lambda_1 x^{A_1} + \lambda_2 x^{A_2}$. Then $t{\cdot}f = t^{A_1}\lambda_1 x^{A_1} + t^{A_2}\lambda_2 x^{A_2}$. Since I is fixed by $T_n(k)$, then $t{\cdot}f \in I$. Also $t^{A_2}f \in I$ by ideal membership since $f \in I$. Hence

$t{\cdot}f - t^{A_2}f = t^{A_1}\lambda_1 x^{A_1} + t^{A_2}\lambda_2 x^{A_2} - t^{A_2}(\lambda_1 x^{A_1} + \lambda_2 x^{A_2}) = (t^{A_1} - t^{A_2})\lambda_1 x^{A_1}$. So we just need to choose t_1 and t_2 in k such that $t^{A_1} - t^{A_2} \neq 0$ and then by ideal membership $t{\cdot}f - t^{A_2}f = (t^{A_1} - t^{A_2})\lambda_1 x^{A_1} \in I$ and so $\lambda_1 x^{A_1} \in I$ since $t^{A_1} - t^{A_2} \in$ k so it has a multiplicative inverse in k (since k is a field and $t^{A_1} - t^{A_2} \neq 0$). So if we multiply $(t^{A_1} - t^{A_2})\lambda_1 x^{A_1}$ by $(t^{A_1} - t^{A_2})^{-1}$, then this is again in I. Therefore, again by ideal membership

$f - \lambda_1 x^{A_1} = \lambda_1 x^{A_1} + \lambda_2 x^{A_2} - \lambda_1 x^{A_1} = \lambda_2 x^{A_2} \in I$.

$\underline{\text{Assume the statement is true for } m = l-1\text{, prove for } m = l}$: In this case $f = \lambda_1 x^{A_1} + \lambda_2 x^{A_2} + \cdots + \lambda_{l-1} x^{A_{l-1}} + \lambda_l x^{A_l}$. Then

$t{\cdot}f = t^{A_1}\lambda_1 x^{A_1} + t^{A_2}\lambda_2 x^{A_2} + \cdots + t^{A_{l-1}}\lambda_{k-1} x^{A_{l-1}} + t^{A_l}\lambda_l x^{A_l}$. Since I is fixed by $T_n(k)$, then $t{\cdot}f \in I$. Also $t^{A_l}f \in I$ by ideal membership since $f \in I$. Hence

$t{\cdot}f - t^{A_l}f = t^{A_1}\lambda_1 x^{A_1} + t^{A_2}\lambda_2 x^{A_2} + \cdots + t^{A_{l-1}}\lambda_{k-1} x^{A_{l-1}} + t^{A_l}\lambda_k x^{A_l} -$

$(t^{A_l}\lambda_1 x^{A_1} + t^{A_l}\lambda_2 x^{A_2} + \cdots + t^{A_l}\lambda_{l-1} x^{A_{l-1}} + t^{A_l}\lambda_l x^{A_l}) =$

$(t^{A_1} - t^{A_l})\lambda_1 x^{A_1} + (t^{A_2} - t^{A_l})\lambda_2 x^{A_2} + \cdots + (t^{A_{l-1}} - t^{A_l})\lambda_{l-1} x^{A_{l-1}}$. We need to choose the t_i's so that the coefficients $t^{A_i} - t^{A_l} \neq 0$ which is possible since A_i and A_l are distinct for all i so t^{A_i} and t^{A_l} are distinct for all i. Since $t{\cdot}f - t^{A_l}f$ is a polynomial where $m = l-1$, then by our induction hypothesis

$\lambda_i x^{A_i} \in < t{\cdot}f : t \in T_n(k) >$ for $1 \leq i \leq l-1$. Thus

$f - (\lambda_1 x^{A_1} + \lambda_2 x^{A_2} + \cdots + \lambda_{l-1} x^{A_{l-1}}) = \lambda_1 x^{A_1} + \lambda_2 x^{A_2} + \cdots + \lambda_{l-1} x^{A_{l-1}} +$

$\lambda_l x^{A_l} - (\lambda_1 x^{A_1} + \lambda_2 x^{A_2} + \cdots + \lambda_{l-1} x^{A_{l-1}}) = \lambda_l x^{A_l} \in I$ as well.

Thus, by induction, I is generated by monomials.

2. Denote elementary matrices which have ones on the diagonal entry, λ at the $(i,j)^{th}$ position in the matrix, and the rest of the entries as zeros by $e_{ij}(\lambda)$, $1 \leq i < j \leq n$. Then the Borel-subgroup, $B_n(k)$, and is generated by $e_{ij}(\lambda)$ and $T_n(k)$

   ($\Rightarrow$) Suppose that I is a strongly stable monomial ideal. Let $x^A = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} \in I$ and let $t \in T_n(k)$. By (1) we know that $t \cdot x^A \in I$. Now consider $e_{ij}(\lambda) \cdot x^A = x_1^{a_1} x_2^{a_2} \cdots (\lambda x_i + x_j)^{a_j} \cdots x_n^{a_n}$. We can expand this sum by binomial expansion and distribute so $e_{ij}(\lambda) \cdot x^A = \sum_{l=1}^{a_j} x_1^{a_1} x_2^{a_2} \cdots \binom{a_j}{l} x_i^l x^{a_j - l} \cdots x_n^{a_n}$. But since I is a strongly stable monomial ideal, then each term in this sum is in I. Thus, $e_{ij}(\lambda) \cdot x^A \in I$. Since $B_n(k)$ is generated by $e_{ij}(\lambda)$ and $T_n(k)$ and I is fixed by each of the generators, then I is fixed by the Borel subgroup, $B_n(k)$.

   ($\Leftarrow$) Suppose that I is Borel-fixed (i.e. fixed by the Borel subgroup, $B_n(k)$). Then, since $T_n(k) \subseteq B_n(k)$, I is fixed by $T_n(k)$ so I is a monomial ideal by (1). Let $m = x^A = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ be a monomial in I such that $a_j \neq 0$ (so $x_j | m$). Since I is fixed by $B_n(k)$, then $e_{ij}(1) \cdot m = x_1^{a_1} x_2^{a_2} \cdots (x_i + x_j)^{a_j} \cdots x_n^{a_n} \in I$ and since I is a monomial ideal then each of the terms are in I. One of the terms in the expansion, in particular, is $\binom{a_j}{1} x_i x^{a_j - 1} = a_j x_i \frac{m}{x_j} \in I$. Since $char(k) = 0$,

then $x_i\frac{m}{x_j} \in I$. Thus, I is a strongly stable monomial ideal by definition.

Note that we can rearrange the order of the variables so that $x_n < x_{n-1} < \cdots < x_2 < x_1$ then the statement I is fixed by $B'_n(k)$) if and only if I is a strongly stable monomial ideal holds but since the order of the variables changed we have that for all $i < j$, $x_j\frac{m}{x_i} = x_1^{a_1}x_2^{a_2}\cdots x_i^{a_i-1}\cdots x_j^{a_j+1}\cdots x_n^{a_n} \in I$).

3. ($\Rightarrow$) Suppose that $I = M^d$ for some d. The $GL_n(k)$-action preserves degree since $x_i \mapsto t_i x_i$ for some $t_i \in$ k. Thus, $I = M^d$ is invariant under the $GL_n(k)$-action since degree is preserved, so is still homogeneous of degree d.
($\Leftarrow$) Suppose that I is invariant under the $GL_n(k)$-action. $GL_n(k)$ is generated by $T_n(k)$, $B_n(k)$, and $B'_n(k)$. By (1) we have that since I is fixed by $T_n(k)$, I is a monomial ideal. Let m be a monomial in I of least degree, say that degree is d. Let $m = x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}$ where $\sum_{i=1}^n a_i = d$. Then $I \subseteq M^d$ since all other monomials have degree greater than or equal to d so each monomial in I can be written as a monomial of degree d multiplied by some other monomial. By (2) we have that I is a strongly stable monomial ideal (for all $i < j$, $x_i\frac{m}{x_j} = x_1^{a_1}x_2^{a_2}\cdots x_i^{a_i+1}\cdots x_j^{a_j-1}\cdots x_n^{a_n} \in I$) since I is fixed by $B_n(k)$. We can also think of rearranging the variables so that $x_n < x_{n-1} < \cdots < x_2 < x_1$ and hence for all $i < j$, $x_j\frac{m}{x_i} = x_1^{a_1}x_2^{a_2}\cdots x_i^{a_i-1}\cdots x_j^{a_j+1}\cdots x_n^{a_n} \in I$. Therefore, applying these two statements to m, $\sigma \cdot m = \sum_{|B|=d} \lambda_B x^B$ for some $\sigma \in B_n(k)$ or $\sigma \in B'_n(k)$ (in other words, by a matrix in $B_n(k)$ or $B'_n(k)$ acting on m we

can generate all monomials of degree d since we can replace any variable by another and it will remain in I by our strongly stable monomial ideal properties from $B_n(k)$ and $B'_n(k)$). Therefore $M^d \subseteq I$.

Thus we have that $I = M^d$.

□

Tensor algebras: Let R be a commutative ring with 1 and M an $R-module$. Then $T_R(M) = R \bigoplus M \bigoplus (M \otimes M) \bigoplus (M \otimes M \otimes M) \bigoplus \cdots$. We define $(m_1 \otimes m_2 \otimes \cdots \otimes m_k) \cdot (n_1 \otimes n_2 \otimes \cdots \otimes n_l) = m_1 \otimes m_2 \otimes \cdots \otimes m_k \otimes n_1 \otimes n_2 \otimes \cdots \otimes n_l$.

Exterior algebras: The exterior algebra $\Lambda_R(M)$ of M over R is defined as $\Lambda_R(M) = T_R(M)/ < x \otimes x : x \in M >$. $\Lambda_R(M)$ is a graded ring where the ith component is denoted $\Lambda^i_R(M)$. And the image of $m_1 \otimes m_2 \otimes \cdots \otimes m_k$ under the natural projection into $\Lambda^k_R(M)$ is denoted by $m_1 \wedge m_2 \wedge \cdots \wedge m_k$.

Notation 6.3. [11] Let τ be a monomial ordering on $R = k[x_1, x_2, \ldots, x_n]$. Let $V =< f_1, f_2, \ldots, f_t > \subseteq R_d$ be a k-vector space of dimension t. Set $f = f_1 \wedge f_2 \wedge \cdots \wedge f_t \in \Lambda^t(R_d)$. The monomials of degree d form a k-basis for R_d and hence $\Lambda^t(R_d)$ has a basis of "exterior monomials" of the form $m_1 \wedge m_2 \wedge \cdots \wedge m_k$ where $m_1, m_2, \ldots, m_k$ are distinct monomials of degree d with $m_1 > m_2 > \cdots > m_k$. We order the exterior monomials by extending the ordering of τ lexographically. In other words, $m_1 \wedge m_2 \wedge \cdots \wedge m_k >_\tau n_1 \wedge n_2 \wedge \cdots \wedge n_k$ if either $m_1 >_\tau n_1$ or $m_j = n_j$ for $j = 1, 2, \ldots, i$ and $m_{i+1} >_\tau n_{i+1}$ (only look at the first term that is different in the exterior product to determine which greater).

Define $\text{in}_\tau(f)$ = largest "monomial" of f in this basis. We can change the f_i by elementary transformations to assume $\text{in}_\tau(f_i) \neq \text{in}_\tau(f_j)$ if $i \neq j$. Then, without loss of generality, we may assume that $\text{in}_\tau(f_1) >_\tau \text{in}_\tau(f_2) >_\tau \cdots >_\tau \text{in}_\tau(f_t)$. Thus $\text{in}_\tau(f) = \text{in}_\tau(f_1) \wedge \text{in}_\tau(f_2) \wedge \cdots \wedge \text{in}_\tau(f_t)$.

Remark 6.4. [11]

1. The general linear group $GL_n(k)$ is an "algebraic group." Let $R = k[x_{ij}][\Delta^{-1}]$ with $1 \leq i, j \leq n$ where $\Delta = \det(x_{ij})$.

2. A k-rational point of R is a maximal ideal of the form $(x_{ij} - \alpha_{ij})$ for $\alpha_{ij} \in k$. An open set $U \subseteq GL_n(k)$ is of the form $U = V \cap \{k\text{-rational points}\}$ for some open subset V of $Spec(R)$ under the Zariski Topology.

3. Since R is a domain, it is irreducible and so the intersection of two non-empty open sets is also non-empty.

Theorem 6.5 ((Galligo) Existence of Generic Initial Ideal)**.** *[7] [5] Let τ be a monomial ordering on $R = k[x_1, x_2, \ldots, x_n]$ and $I \subseteq R$ be a homogeneous ideal. Then:*

- *there is a non-empty open subset $U \subseteq GL_n(k)$ and a monomial ideal $J \subseteq R$ such that for each $g \in U, \text{in}_\tau(gI) = J$.*

- *for each $d \geq 0$, if $dim_k(I_d) = t$, then J_d is spanned by the greatest monomial that appears in $\Lambda^t(gI_d)$ as g ranges over all of $GL_n(k)$.*

J is called the ***generic initial ideal of I*** *(with respect to τ) and denoted $gin_\tau(I)$.*

Proof. [5] Consider I_d. Let $dim_k(I_d) = t$. Then we can choose a basis $\{f_1, f_2, \ldots, f_t\}$ of I_d. Let $\sigma = (z_{ij})$ be an $n \times n$ matrix of variables which acts on R by $\sigma(x_i) = \sum_{j=1}^{n} z_{ij}x_j$ and extend to a k-algebra endomorphism. Then we can write $\sigma(f_1) \wedge \sigma(f_2) \wedge \cdots \wedge \sigma(f_t) = \sum p_n(z_{ij})(n_1 \wedge n_2 \wedge \cdots \wedge n_t)$ where the sum is taken over the various monomial exterior products after linear distribution after applying σ to $f_1, f_2, \ldots, f_t$ and $p_n(z_{ij})$ is a polynomial in the Z_{ij}'s where n depends on the exterior product.

Let $m_1 \wedge m_2 \wedge \cdots \wedge m_t$ be the largest exterior product in the sum with non-zero coefficient $p_m(z_{ij})$. Define $U_d \subseteq GL_n(k)$ by $U_d = \{g = (\alpha_{ij}) \in GL_n(k) : p_m(\alpha_{ij}) \neq 0\}$. This is a non-empty open set since we can find values such that the polynomial will not be equal to zero for any polynomial that is not identically zero. If $g \in U_d$, then $\text{in}_\tau(gI_d) = (m_1, m_2, \ldots, m_d) =: J_d$.

Claim. $J = \bigoplus_{d \geq 0} J_d$ is an ideal.

Proof. (of Claim) We know that J_d is closed under addition and addition in J takes place within each of the J_d so J is also closed under addition. Hence, it is enough to show $x_iJ \subseteq J$ for all i, i.e. it is enough to show that $R_1J_d \subseteq J_{d+1}$. This is because if we multiply any polynomial to an element in J then we can first distribute linearly and then apply $x_iJ \subseteq J$ for each i in the term of the polynomial inductively. This will show that J satisfies the condition that $rj = jr \in J$ for any $r \in R, j \in J$.

Since $GL_n(k)$ is irreducible (i.e. any finite set of polynomials has a substitution that is nonzero for all of them), we can choose $g \in U_d \cap U_{d+1}$. By construction, $J_d = \text{in}_\tau(gI_d)$ and $J_{d+1} = \text{in}_\tau(gI_{d+1})$. Since I is an ideal of R then gI is also an ideal of R. Hence $R_1(gI_d) \subseteq gI_{d+1}$. So

$\text{in}_\tau(R_1(gI_d)) \subseteq \text{in}_\tau(gI_{d+1}) \Rightarrow R_1\text{in}_\tau(gI_d) \subseteq \text{in}_\tau(gI_{d+1})$ since $\text{in}_\tau(R_1) = R_1$.

$\Rightarrow R_1 J_d \subseteq J_{d+1}$. □

Thus J is an ideal of R. By 2.3 J is finitely generated. So J has generators up to some degree e.

Claim. $U = \bigcap_{d\geq 0} U_d = U_0 \cap U_1 \cap \cdots \cap U_e$ and is therefore a non-empty open set of $GL_n(k)$.

Proof. (of Claim) Let $g \in U_0 \cap U_1 \cap \cdots \cap U_e$. We know that $\text{in}_\tau(gI_d) = J_d$ for all $d \leq e$. Thus $J \subset \text{in}_\tau(gI)$. Since $dim_k(gI_d) = dim_k(I_d) = dim_k(J_d)$, then the Hilbert functions for I and J are the same. Thus $\text{in}_\tau(gI) = J$, which proves the claim. □

Thus for all $g \in U$, $\text{in}_\tau(gI) = J$. □

Theorem 6.6. *Let k be a field of characteristic 0, $R = k[x_1, x_2, \ldots, x_n]$ be a polynomial ring over k, $I \subseteq R$ a homogeneous ideal and τ a monomial ordering on R. Then $gin_\tau(I)$ is Borel-fixed (i.e. strongly stable).*

We will not provide the proof of the theorem in this thesis.

Discussion 6.7. A great application of revlex and generic initial ideals is in a paper from Bayer and Stillman that shows that the generic initial ideal of a homogeneous ideal under the revlex monomial ordering preserves many properties of the original ideal. We will not be discussing this topic in this thesis since discussion of this topic would require a lot of extra material. But if the reader is interested in this topic then they can refer to [2] in the bibliography.

Bibliography

[1] W. Adams and P. Loustaunau (1996). *An Introduction to Gröbner Bases*, Graduate Studies in Mathematics, 3. Reprinted with corr. ed. American Mathematical Society.

[2] D. Bayer and M Stillman. "A criterion for detecting m-regularity." *Invent Math* **87**, 1–11 (1987). `https://doi.org/10.1007/BF01389151`

[3] B. Buchberger (1985): *Gröbner bases: an algorithmic method in polynomial ideal theory*, Recent Trends in Multidimensional System Theory, N.K. Bose (ed.), Reidel.

[4] D. S. Dummit and R. M. Foote (1999). *Abstract Algebra*(2nd ed.). Upper Saddle River, N.J.: Prentice Hall.

[5] D. Eisenbud (1994). *Commutative Algebra with a View Toward Algebraic Geometry*, Graduate Text in Mathematics, 150. Springer-Verlag, New York. [Online PDF]

[6] V. Ene and J. Herzog (2012). *Gröbner Bases In Commutative Algebra*, Graduate Studies in Mathematics, 130. American Mathematical Society, Providence, Rhode Island.

[7] A. Galligo (1979). *Theoreme de division et stabilite en geometrie analytique.* Ann. Inst. Fourier (Grenoble) 29.

[8] D. Grayson and M. Stillman. *Macaulay2.* Macaulay2. `http://www2.macaulay2.com/Macaulay2/`

[9] M. Green (2010). *Generic initial ideals. Six lectures on commutative algebra*, 119–186, Mod. Birkhäuser Class., *Birkhäuser Verlag, Basel.* [MR1648665]

[10] C. Huneke (2012). *Commutative Algebra I.* [Unpublished notes].

[11] C. Huneke (2006). *Topics in Commutative Algebra.* [Unpublished notes].

[M2] Macaulay2 - a system for computation in algebraic geometry and commutative algebra programmed by D. Grayson and M. Stillman, `http://www.math.uiuc.edu/Macaulay2/`.