Stockholm University

SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Hilbert's Invariance Theorem

av

Simon Hanson

2025 - No K35

Hilbert's Invariance Theorem

Simon Hanson

Hilbert's Invariance Theorem states that the ring of polynomials, which stays invariant under the group action of the finite matrix group G, is finitely generated.

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Jonas Bergström

2025

Contents

1 Abstract

In this thesis, we will work towards proving Hilbert's Invariance Theorem. We take invariance to mean how polynomials stay unchanged under group action from a finite matrix group.

We will work through the concepts of Ascending Chain Condition, Symmetric Polynomials, and the foundational Hilbert's Basis Theorem to grasp the concepts.

I detta Kandidat arbete kommer vi jobba os upp till Hilberts invariants sats. I detta arbete menar vi med invariants, hur polynom förblir oförändrade under verkan av en ändlig matris grupp.

För att kunna förstå denna sats kommer vi jobba med Ascending Chain Condition, Symetriska polynom, samt Hilberts Basis Theorem som är grundläggande förkunskaper.

2 Introduction

In this thesis, we will be working with the polynomial ring $k[x_1, ..., x_n]$ under the action of a finite matrix group G. In particular, we will study the polynomials that stay unchanged, the Invarinats. We will study the ring of these Invarinats $k[x_1, ..., x_n]^G$ and how it is finitely generated. We will also examine how these generators relate to each other algebraically.

We will approach this thesis by first working through some foundational definitions. We will then tackle Hilbert's Basis Theorem and Gröbner Basis, moving on to Symmetric Polynomials and Hilbert's Invariance Theorem. We will finish the thesis by studying the algebraic relation between the generators.

We will mainly work on the book Ideals, Varieties, and Algorithms, 3rd edition, by David Cox, John Little, and Donald O'Shea. Other resources were used to further my understanding or help write the code necessary to find a particular Gröbner Basis.

3 Basic Definitions

This chapter will closely follow chapters 1 and 2 of David Cox's book Ideals, Varieties, and Algorithms.

We will start this section with monomial ordering, followed by varieties. Ordering monomials becomes trivial in one variable. However, it becomes substantially more complex if we are working with multiple variables. Take the two monomials x^2y3z and xy^4z^5; how do we order them? In this chapter, we will discuss and order them; ironically, the two main orderings, Lexicographic order, and Garded Lexicographic order order the monomials differently.

Definition 3.1 *An s-tuple is a finite ordered list of s number of elements. [1]*

An s-tuple is a finite ordered set, and the term s-tuple will be used interchangeably with the term finite ordered set.

Definition 3.2 *Given a nonempty set A, ordered by $\leq$. We define the following,*

1. *Then a **chain** also called **ordered subset** is a subset $B \in A$ where$x_1, ..., x_n \in B$ for $x_i \leq x_i + 1$*
2. *We say that an element $a \in A$ is an **upper bound** of the subset B if for all $b \in B$, $b \leq a$.*
3. *While a **maximal element** is an element $a \in A$, is an element where $x \leq a$ for all $x \in A$.*

Definition 3.3 ***Lexicographic order**, also written as **Lex order**, is a way of ordering tuples in particular. Given $\alpha = (\alpha_1, ..., \alpha_n)$ and $\beta = (\beta_1, ..., \beta_n) \in \mathbb{Z}^n_{\geq 0}$. We will write that $\alpha \geq_{lex} \beta$ if the vector difference $\alpha - \beta \in Z^n$ the first non-zero term is positive.*

This means we order elements by the first differentiating term, meaning that:

$(2, 3, 4) \geq_{lex} (1, 5, 3)$ as $(2, 3, 4) - (1, 5, 3) = (1, -2, 1)$ and:
$(2, 3, 4) \geq_{lex} (2, 3, 3)$ as $(2, 3, 4) - (2, 3, 3) = (0, 0, 1)$.

We can now order the two monomials stated in the introduction of this chapter x^2y^3z and xy^4z^5. First, we must establish which variables x, y, z come first. It is ordered as stated in the case of x, y, z. Generally, we would write x_1, x_2, x_3; however, we often use different letters for small numbers of variables. In such cases, unless differently stated, we order by following the alphabet. Wich now allows us to define an order $x^2y^3z > xy^4z^5$, as x^2y^3z has the greatest order of x. However, xy^4z^5 has the greatest total order, this leads us to the following monomial order, Graded Lecixographical Order or Graded Lex Order:

Definition 3.4 ***Graded Lex Order****, for two s-tuples* $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$*,* $\alpha >_{grlex} \beta$ *if:*

$$\mid \alpha \mid = \sum_{i=1}^{n} \alpha_i > \mid \beta \mid = \sum_{i=1}^{n} \beta_i$$

,

in the case that $\mid \alpha \mid = \mid \beta \mid$*,* $\alpha >_{lex} \beta$*.*

Now we can see how Graded Lex order diverges from Lex order regarding our example polynomials. Lex order states $x^2y^3z > xy^4z^5$ whilst Graded Lex order $xy^4z^5 > x^2y^3z$ as the total order of xy^4z^5 is 10 whilst x^2y^3z is 6. But in the case of the polynomial xy^4z, we would get $x^2y^3z > xy^4z$ as both polynomials have total degree 6 however, x^2y^3z has a greater degree of the variable x.

Definition 3.5 *For a given ring* k*, the polynomial ring* $k[x_1, ..., x_n]$ *is defined as the ring of polynomials with variables in* $x_1, ..., x_n$*. And coeficients in* k

Definition 3.6 *A monomial expressed in the variables* $x_1, ..., x_n$ *is written as the product:*

$$x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{a_n}$$

where the exponents α_i *are non negative integers. The sum of the monomial is said to be the sum of the exponents* $\alpha_1, ..., \alpha_n$*.*

Because it is quite cumbersome to write $x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{a_n}$ we will instead simplify the notation:

$$x^\alpha = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{a_n}$$

where $\alpha = (\alpha_1, ..., \alpha_n)$ is an n-tuple. Where $\mid \alpha \mid = \alpha_1 + ... + \alpha_n$ represents the order of x^α, and when $\alpha = (0, ..., 0)$ then $x^\alpha = 1$.

Definition 3.7 *If* f *is a polynomial, then* f *can be written as a linear combination of a finite number of monomials with coefficients* a_i *in* k*,*

$$f = \sum_{\alpha} a_\alpha x^\alpha, \quad a_\alpha \in k.$$

The degree of a polynomial is the maximal order $\mid \alpha \mid$*.*

We express the set of all polynomials with coefficients in k *and variables* $x_1, ..., x_n$ *as* $k[x_1, ..., x_n]$*.*

Definition 3.8 *Lex order is not the only way to order monomials; hence, we discuss the general properties of* ***monomial order*** $>$ *on* $k[x_1, ..., x_n]$*. A monomial order is a relation* $>$ *which acts on the set of monomials* $x^\alpha, \alpha \in \mathbb{Z}^n_{\geq 0}$*, or simply on* $\mathbb{Z}^n_{\geq 0}$*, which satisfies the following properties:*

1. *The monomial order* $>$ *is a linear ordering in* $\mathbb{Z}^n_{\geq 0}$*. Meaning that for two monomials* x^α *and* x^β *exactly one of the following statements can be true,*

$$x^\alpha > x^\beta \qquad x^\alpha = x^\beta \qquad x^\beta > x^\alpha.$$

2. *Given that* $\alpha > \beta$ *then for any* $\gamma \in \mathbb{Z}^n_{\geq 0}$*,* $\alpha + \gamma > \beta + \gamma$*.*

3. $>$ *is also considered a well-ordering, this means that for any non-empty subset of* $\mathbb{Z}^n_{\geq 0}$ *there exists a smallest element under* $>$*.*

Definition 3.9 *Given the polynomial group* $k[x_1, ..., x_n]$ *and a given monomial order*$>$*, then we define the folowing properties for the polynomial* $f = \sum_\alpha a_\alpha x^\alpha$*.*

1. *The* ***multidegree*** *of a polynomial f, with the maximum defined in respect to* $>$*:*

$$multideg(f) = max(\alpha \in \mathbb{Z}^n_{\geq 0} : a_\alpha \neq 0).$$

2. *The leading coefficient of the polynomial f is defined as:*

$$LC(f) = a_{multideg(f)} \in k.$$

3. *Whilts the* ***leading monomial*** *of the polynomial f much as the name suggests is:*

$$LM(f) = x^{multideg(f)}$$

Where the coefficient of said monomial is 1.

Definition 3.10 *Given the polynomials* $f_i, ..., f_s$ *in* $k[x_1, .., x_n]$*, then we define:*

$$\langle f_1, ..., f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i : h_1, ..., h_s \in k[x_1, ..., x_n] \right\}.$$

It is important to note that $\langle f_1, ..., f_s \rangle$ *is itself an ideal.*

Lemma 3.11 *The ideal previously defined* $\langle f_1, ..., f_s \rangle$ *is called the ideal generated by* $f_1, ..., f_s$ *in* $k[x_1, ..., x_n]$

The proof that $\langle f_1, ..., f_s \rangle$ indeed is an ideal is found on page 30 of [3].

It is important to note that ideals are generated in a different manner from rings. A ring generated by a set of elements is self-contained: all of its elements are obtained from the generators using addition and multiplication within the ring. In contrast, an ideal generated by a set of elements consists of all finite sums of those generators multiplied by arbitrary elements of the ambient ring. The multipliers need not lie in the ideal itself.

For example, the subring $k[x^2, y^2] \subset k[x, y]$ consists of polynomials generated by x^2 and y^2, i.e. finite k-linear combinations of monomials of the form $x^{2a}y^{2b}$. On the other hand, the ideal $\langle x^2, y^2 \rangle \subset k[x, y]$ is the set of all polynomials of the form

$$f(x, y)x^2 + g(x, y)y^2,$$

where $f, g \in k[x, y]$. This ideal contains all polynomials whose monomials have degree at least 2, except terms such as xy, which has degree 2 but is not in the ideal since it cannot be expressed as a multiple of either x^2 or y^2.

Definition 3.12 *An **affine space** is define as:*

$$k^n = \{(\alpha_1, ..., \alpha_n) : \alpha_1, ..., \alpha_n \in k\}$$

Where k is a field and n is a positive integer.

Polynomials are strongly linked to affine spaces as a polynomial $f = \sum_\alpha a_\alpha x^\alpha$takes:

$$f : k^n \to k.$$

As each polynomial takes elements of the form $(a_1, ..., a_n) \in k^n$ and outputs an element of form $b \in k$. In the cases that $n = 1$ we call k^1 an affine line, while if $n = 2$ we call k^2 the affine plane.

Definition 3.13 *For a given field, k let $f_1, ..., f_s$ be polynomials in $k[x_1, ..., x_n]$. Then we say the **affine variety** $\boldsymbol{V}(f_1, ..., f_s)$ defined by $f_1, ..., f_s$ to be:*

$$\boldsymbol{V}(f_1, ..., f_s) = \{(a_1, ..., a_n) \in k^n : f_i(a_1, ..., a_n) = 0 \, for \, all \, 1 \leq i \leq s\}.$$

In other words, an affine variety is the solution of the system of equations:

$$\begin{aligned} f_1(x_1, ..., x_n) &= 0 \\ f_2(x_1, ..., x_n) &= 0 \\ &\vdots \\ f_s(x_1, ..., x_n) &= 0. \end{aligned}$$

Definition 3.14 *For a given ideal $I \subset k[x_1, ..., x_n]$, we denot the variety $\boldsymbol{V}(I)$ as:*

$$\boldsymbol{V}(I) = \{(a_1, ..., a_n) \in k^n : f(a_1, ..., a_n) = 0 \, for \, all \, f \in I\}.$$

Proposition 3.15 *For a given affine variety $\boldsymbol{V}(I)$. Then if $I = \langle f_1, ..., f_s \rangle$, $\boldsymbol{V}(I) = \boldsymbol{V}(f_1, ..., f_s)$*

This is proven on page 80 [3].

Lemma 3.16 *Given two affine varieties $V, W \subset k^n$, then $V \cap W$ and $V \cup W$ are also affine varieties.*

The proof is provided on page 11 of [3].

Proposition 3.17 *Given two basis $f_1, ..., f_s$ and $g_1, ..., g_t$, in the case they both define the same ideal in $k[x_1, ..., x_n]$, meaning $\langle f_1, ..., f_s \rangle = \langle g_1, ..., g_s \rangle$. Then the affine varieties $\boldsymbol{V}(f_1, ..., f_s) = \boldsymbol{V}(g_1, ..., g_t)$*

Proof. Because every elements of $g_1, ..., g_t$ can be linearly constructed from $f_1, ..., f_s$ hence if for $a_1, ..., a_n$, $\mathbf{V}(f_1, ..., f_n) = \{(a_1, ..., a_n) \in k^n : f_i(a_1, ..., a_n) = 0 \, for \, all \, 1 \leq i \leq s\}$ then $g_i(a_1, ..., a_n) = 0 \, for \, all \, 1 \leq i \leq s\}$. The same argument can be applied to prove that $\mathbf{V}(f_1, ..., f_s) \in \mathbf{V}(g_1, ..., g_t)$.

Definition 3.18 *For a given affine variety $V \subset k^n$, then the **ideal of** V is defined as:*

$$\boldsymbol{I}(V) = \{f \in k[x_1, .., x_n] : f(a_1, ..., a_n) = 0 \, for \, all \, (a_1, ..., a_n) \in V\} \quad (1)$$

The ideal of V is hence the ideal of all the polynomials in $k[x_1, ..., x_n]$ that are zero for all the coordinates $(a_1, ..., a_n) \in V$. It is important to note that it is not only the polynomials $f_1, ..., f_s$, but it extends to all polynomials in $k[x_1, ..., x_n]$ that satisfy the condition in Equation 1

Proposition 3.19 *For a given set of polynomials $f_1, ..., f_n \in k[x_1, .., x_n]$ then $\langle f_1, .., f_s \rangle \subset \boldsymbol{I}(\boldsymbol{V}(f_1, ..., f_s))$.*

Proof. If $f \in \langle f_1, ..., f_s \rangle$ then $f = \sum_{i=1}^{s} h_i f_i$ for some $h_i, ..., h_s$ which are polynomials in $k[x_1, ..., x_n]$. We know that individually $f_1, ..., f_s$ become zero on $\mathbf{V}(f_1, ..., f_s)$, then the sum also becomes zero. As this proves f vanishes on $\mathbf{V}(f_1, ..., f_s)$ it must be an element in $\mathbf{I}(\mathbf{V}(f_1, ..., f_s))$, and the proposition is proven.

Definition 3.20 *We say that a affine variety V is* ***irreducible*** *if V can be written as the union $V_1 \bigcup V_2$ where both V_1 and V_2 are affine varieties then either $V_1 = 0$ or $V_2 = 0$.*

Proposition 3.21 *The affine variety $V \subset k^n$ is irreducible if and only if the ideal $\boldsymbol{I}(V)$ is prime.*

Definition 3.22 *We define the* ***coordinate ring*** *to be the ring $k[V]$ for an affine variety $V \in k^n$*

In other words, the coordinate ring is the polynomial ring generated by the coordinates $(a_1, ..., a_n) \in k^n$ in the affine variety V.

Definition 3.23 *For an affine variety $V \subset k^n$ we say:*

1. *Any ideal $J\langle \phi_1, ..., \phi_s \rangle$ of the coordinate ring $k[V]$, we define the sub variety $\boldsymbol{V}_V(J)$ of V as:*

$$\boldsymbol{V}_V(J) = (a_i, ..., a_n) \in V : \phi_i(a_1, ..., a_n) \, for \, all \, \phi_1 \in J$$

2. *For any given subset W of V, we say:*

$$\boldsymbol{I}_V(W) = \{\phi \in k[V] : \phi(a_1, ..., a_n) = 0 \, for \, all \, (a_1, ..., a_n) \in W\}$$

4 Hilbert's Basis Theorem and Gröbner Basis

In this chapter, we will closely follow chapter 2 of David Cox's book Ideals, Varieties, and Algorithms with the aim to establish and prove Hilbert's Basis Theorem. The Basis Theorem is foundational to understanding Hilbert's Invariance Theorem. To start, however, we will begin with The Division Algorithm.

Theorem 4.1 ***The Division Algorithm*** *in $k[x_1, ..., x_n]$. For a fixed monomial order $>$ on $\mathbb{Z}^n_{\geq 0}$, and a ordered s-tuple $F = (f_1, ..., f_s)$ of polynomials in $k[x_1, ..., x_n]$ then every $f \in k[x_1, ..., x_n]$ can be expressed as follows:*

$$f = a_1 f_1 + ... + a_s f_s + r.$$

Where both a_i and r are elements of $k[x_1, ..., x_n]$. We call r the ***remainder*** *of f with respect to F. Either the remainder $r = 0$ or it is a linear combination of monomials with coefficients in k. In cases r is non-zero, none of its monomials are divisible by the leading terms of $f_1, ..., f_s$. In cases where neither a_i and $f_i \neq 0$ then:*

$$multideg(f) \geq multideg(a_i f_i).$$

The proof of said theorem is given on page 64 of [3]. Instead of writing division under F, we will write modulo F. Much like we would say 4 is 0 modulo 2, a polynomial $f = x^2 + y^2$ would be 0 modulo $f_1 = x, f_2 = y$.

Lemma 4.2 *For a given monomial ideal $I = \langle x^\alpha \rangle$ for $\alpha \in A$, then a monomial x^β lies in I if and only if it is divisible by x^α for $\alpha \in A$.*

Proof. By the definition of an ideal if $x^\beta \in I$, then it will be a linear combination of the generators hence $x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)}$, where the coefficient $h_i \in k[x_1, ...x_n]$, and the exponent $a(i) \in A$. Hence all $x^\beta \in I$ must be divisible by x^α. If x^β is divisible by x^α, then it must be in I as it is the product of an element in I.

Definition 4.3 *For a given non-empty ideal, $I \subset k[x_1, ..., x_n]$.*

1. *Then the set of leading terms of I is denoted as $LT(I)$, written as:*

$$LT(I) = \{cx^\alpha : for\, some\, f \in I, given\, LT(f) = cx^\alpha\}$$

2. *The ideal generated by the elements of LT(I) is denoted by $\langle LT(I) \rangle$.*

Proposition 4.4 *For a given ideal $I \subset k[x_1, ..., x_n]$ then.*

1. *The ideal generated by the leading terms of I $\langle LT(I) \rangle$ is a monomial ideal.*

2. *The ideal* $\langle LT(I)\rangle$ *can be written as* $\langle LT(I)\rangle = \langle LT(g_1), ..., LT(g_t)\rangle$*, for some elements* $g_1, ..., g_t \in I$*.*

The proof of this proposition is found on page 79 [3]

Theorem 4.5 ***Hilbert's Basis Theorem*** *states that all ideals* $I \subset k[x_1, ..., x_n]$ *are finitely generated, meaning* $I = \langle g_1, ..., g_t\rangle$ *for some* $g_1, ..., g_t \in I$*.*

Proof. The empty set $\{0\}$ is clearly finitely generated by itself. For a nonempty set I, a finite set that generates I can be constructed as follows. By the previous proposition, we know that the set of leading terms can be finitely constructed, $\langle LT(I)\rangle = \langle LT(g_1), ..., LT(g_t)\rangle$, for some elements $g_1, ..., g_t \in I$. We claim that the whole ideal is generated by the set of elements $g_1, ..., g_t$ $I = \langle g_1, ..., g_t\rangle$.

To do this first we note that $\langle g_1, ..., g_t\rangle \subset I$, to prove that that $I \subset \langle g_1, ..., g_t\rangle$. We apply the division algorithm to do this, by dividing $f \in I$ by the set $\langle g_1, ..., g_t\rangle$, we get:

$$f = a_1g_1 + ... + a_tg_t + r$$

where the remainder r has no term divisible by $LT(g_1), ..., LT(g_t)$. If $r = 0$, the theorem is proven, to prove this, note:

$$r = f - a_1g_1 - \cdots - a_tg_t \in I.$$

If $r \neq 0$, then the monomial $LT(r)$ must lie in the ideal $LT(I)$ by the fact that $LT(f)\, and\, LT(a_ig_i) \in LT(I)$. Lemma 4.2 states that any monomial in $LT(I)$ must be divisible by some monomial in $LT(I)$; this would be a contradiction; hence $r = 0$. Giving us:

$$f = a_1g_1 + ... + a_tg_t,$$

and as all terms of $a_1g_1 + ... + a_tg_t$ are in $\langle g_1, ..., g_t\rangle$ so must f be. Which in turns shows that $I \subset \langle g_1, ..., g_t\rangle$ as all of $f \in I$ are in$\langle g_1, ..., g_t\rangle$. This finalises the proof as $I = \langle g_1, ..., g_t\rangle$.

Theorem 4.6 ***Ascending Chain Condition****, for ideals* $I_i \in k[x_1, ..., x_n]$*, we say the ascending chain of ideals:*

$$I_1 \subset I_2 \subset I_3 \cdots .$$

Then there must exist an integer $N \leq 1$ *such that the ideals:*

$$I_N = I_{N+1} = I_{N+2=} \cdots .$$

Proof. For the ascending chain $I_1 \subset I_2 \subset I_3 \cdots$, take $I = \bigcup_{i=1}^{\infty} I_i$. We will prove that I is an ideal in $k[x_1, ..., x_n]$. First, note that $0 \in I$, since it is an element of all I_i. For two ideals I_i and I_j where $i \leq j$ then if $f \in I_i$ and $f \in I_i$, then by the ascending chain $f, g \in I_j$. As I is an ideal the sum $f + g \in I_j$ and as a consequence, an element of I.

Now take an element f of I, then $f \in I_j$ for some$j$. Hence for $r \in k[x_1, ..., x_n]$, $r \cdot f \in I$ because $r \cdot f \in I_j$. Which proves that I is an ideal.

By Hilbert's Basis Theorem, I is finitely generated, and hence, a finite set exists $\langle f_1, ..., f_s \rangle = I$. As each generator f_i must be an element of some I_j, we write $f_i \in I_{j_i}$, where $i = 1, ..., s$. Now take N to be the maximum of j_i, and as it is the maximum it implies that $f_i \in I_N$ for all f_i. Giving us:

$$I = \langle f_1, ..., f_s \rangle \subset I_N \subset I_{N+1} \subset I.$$

This proves the theorem.

Definition 4.7 *A commutative ring R for which its ideals satisfy the Ascending Chain Condition is called* ***Noetherian****. Named after Emmy Noether*

Emmy Noether was one of Hilbert´s greatest students who laid much of the foundations of ring theory.

Lemma 4.8 *A ring R is Noetherian if and only if all ideals are finitely generated.*

Proof. Shown on page 146 [6].

Since a ring R being Noetherian implies its ideals being finitely generated, a more general version of the **Hilbert Basis Theorem**:

Theorem 4.9 *If a commutative ring k with identity is Noetherian then so is the polynomial ring $k[x]$.*

The proof is given on page 147 [6]. A familiar example is the polynomial ring $\mathbb{R}[x]$. Since $\mathbb{R}$ is a field, its only ideals are $\{0\}$ and $\mathbb{R}$ itself. Therefore, $\mathbb{R}[x]$ is a finitely generated $\mathbb{R}$-algebra, generated by the element x.

However, this does not imply that $\mathbb{R}[x]$ has no proper ideals. For instance, consider the ideal consisting of all polynomials of degree at least two. This is indeed an ideal, since it is closed under addition and is preserved under multiplication by arbitrary polynomials in $\mathbb{R}[x]$. Moreover, this ideal is finitely generated: in fact,

$$(x^2) = \{\, x^2 f(x) \mid f(x) \in \mathbb{R}[x] \,\},$$

which is precisely the set of all polynomials of degree at least two. Thus, this ideal is generated by a single element x^2.

This motivates the second part of our chapter: Gröbner bases. Gröbner bases will be crucial for our understanding of invariance, which we will return to in the next chapter.

Definition 4.10 *A finite subset $G = \{g_1, ..., g_n\}$ of a given ideal I is said to be a **Gröbner basis** or also called **standard basis** if:*

$$\langle LT(g_1), ..., LT(g_n)\rangle = \langle LT(I)\rangle.$$

Where $LT(n)$ refers to the leading term of n. And $\langle LT(g_1), ..., LT(g_1)\rangle$ and $\langle LT(I)\rangle$ refers to the ideal generated by $LT(g_1), ..., LT(g_n)$ or $LT(I)$ respectively.

Lemma 4.11 *Given a Gröbner basis $G = \{g_1, ..., g_t\}$ of an ideal $I \subset k[x : 1, ..., x_n]$, let $f \in k[x_1, ..., x_n]$. Then there exists a unique element $r \in k[x_1, ..., x_n]$, which satisfies $f = g + r$ for some $g \in I$ and no term of r is divisible by any leading term of G $LT(g_1), ..., LT(g_t)$. We say r is the remainder of the division algorithm by G.*

Proof. We can use the division algorithm, by setting $f = a_1f_1, ..., a_tg_t + r$ then r satisfies both that $f = g + r$ by setting $g = a_1f_1, ..., a_tg_t$ and it is not divisible by any of $LT(g_1), ..., LT(g_t)$. Now we only have to prove uniqueness:

Suppose there is no unique r then $f = g + r = g' + r'$. As we know that g and g' are elements of I. Because $r - r' = g' - g$ then r and r' are in I. Hence $LT(r - r') \in \langle LT(g_1), ..., LT(g_n)\rangle$ by proposition 4.4 as the leading term is a monomial.

Corollary 4.12 *For any ideal $I \subset k[x_1, ..., x_n]$ then $f \in I$ if and only if the remainder of f is zero under division of the Gröbner basis $G = \{g_1, ..., g_t\}$*

This was proven on page 82 of [3].

To find the Gröbner basis of an ideal I, we will have to introduce the concept of an S-polynomial, which enables us to find the Gröbner Basis using Buchberger's Algorithm.

Definition 4.13 *We will denote the remainder of f under division of the ordered s-tuple $F = (f_1, ..., f_s)$ as $\overline{f}^F$. If F is a Gröbner basis for $\langle f_1, ..., f_s\rangle$, then we can regard it as a set and not worry about the order.*

Definition 4.14 *For two nonzero polynomials $f, g \in k[x_1, ..., x_n]$.*

1. *Taken the two vectors $multitdeg(f) = \alpha$ and $multitdeg(g) = \beta$, now take the vector$\gamma = (\gamma_1, ..., \gamma_n)$ $\gamma_i = max(\alpha_i, \beta_i)$ for each i. We call the monomial x^γ the Least Common Multiple of $\boldsymbol{LCM}(LM(f), LM(g))$.*
2. *We also define the **S-polynomial** of f and g as follows:*

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

The S-polynomial, takes two polynomials and creates another polynomial of smaller degree. It is remarkable how effective this trick is and is at the hart of generating the Gröbner basis.

Theorem 4.15 ***Buchberger's Criterion****, states that $G = \{g_1, ..., g_n\}$ is the Gröbner basis for the polynomial ideal I if and only if the remainder of $S(g_i, g_j)$ under division of G is zero, for all pairs where $i \neq j$.*

This was proven on page 85 of [3]

We can now use this criterion to generate the set of Gröbner basis with the following method.

Theorem 4.16 ***Buchberger's Algorithm****. For a non-zero ideal I generated by the set $F := (f_1, ..., f_s)$, we can construct the Gröbner basis of I, by first setting $G := F$. Note this is not the ideal just the generators. Now the iterative process can begin. We construct the set $\{S\} = \overline{S(p,q)}^G$ for all distinct pairs p, q. If $S \neq 0$ then we amend $G := G \cup \{S\}$. This is continued until $G = G \cup \{S\}$. A reminder that $\overline{S(p,q)}^G$ is not the $S-$polynomial but instead the remainder of the S-polynomial under division of G*

We can create a function in sagemath that does just this. Note that the generating set we obtain from simple reduction is not necessarily minimal. The SageMath command `I.groebner_basis()` produces a minimal Gröbner basis, and we will therefore rely on this command in the computations that follow. The proof that Buchberger's algorithm terminates after finitely many steps is provided on page 90 of [3]. Since these computations can become quite elaborate, we will make use of computer algebra systems and will not discuss the algorithmic details of Gröbner basis generation further.

Let us now compute an explicit example of a Gröbner basis. Consider the ideal generated by the polynomials x^2+y and xy^2+y. We first compute the corresponding S-polynomial. The leading monomials are x^2 and xy^2, respectively, whose least common multiple is x^2y^2. Thus we obtain

$$S(x^2 + y,\ xy^2 + y) = \frac{x^2y^2}{x^2}(x^2 + y) - \frac{x^2y^2}{xy^2}(xy^2 + y) = y^3 - xy.$$

Since the polynomial $y^3 - xy$ does not reduce to zero, we append it to our generating set. Continuing the algorithm, one verifies (and SageMath confirms) that the polynomials $x^2+y,\ xy^2+y,\ y^3-xy$ form a Gröbner basis for the ideal.

During this computation, the initial code I wrote encountered difficulties when performing reductions. The issue arises from the command `I.reduce(s)`, which performs reduction with respect to the ideal rather than directly against the current list of generators. While this distinction is usually harmless, it causes a problem in the present example. To address this, we define a custom reduction function `reduce(p, lis)` that performs reduction with respect to a given list of generators. The implementation is as follows:

```
P.<x,y,z> = PolynomialRing(QQ, order='deglex')

def S(p,q):
    L= lcm(p.lm(),q.lm())#takes least common multiple of leadin monomials
    Lp= L//p.lm()# // is to keep polynomial in polynomial ring and not fractional field
    Lq= L//q.lm()
    return Lp*(p/p.lc())-Lq*(q/q.lc()) #returns our S-polynomial not reduced

def reduce(p,lis):
    r= p
    count= True
    while count: # we will iterate until r is no longer reducible
        count= False
        for l in lis:
            if l.lm().divides(r.lm()) and l !=0 : # checks divisibility of leading term
                r = r-r.lc()/l.lc()*r.lm()//l.lm()*l #removes the leading term
                if r!=0:#stops infinite loops when r=0
                    count= True

    return r

def groebner(G):
    F=[]
    length= len(G)
    for f in range(length):# we will reduce the list G to F to remove redundent terms
        re= reduce(G[f], F)
        if re!= 0:
            F.append(G[f])

    count = True
    while count:
        count= False #We take count to be false to insure no infinite loops
        length= len(F)
        for i in range(length):
            for j in range(i+1,length):
                s = S(F[i],F[j]) #recalls the S function defined before
                red = reduce(s,F) #our reduced term
                if red != 0 and red not in F: # ensures we only iterate if there is
                #a non zero remainder
                    F.append(red)
                    count= True
    return F
```

This gives us the Gröbner basis $x^2 + y, xy^2 + y, y^3 - xy$, which is the correct answer. One might now wonder why Gröbner basis are relevant. We, by

construction, already have a basis, this can feel contrived, and mathematics for mathematics' sake. However, Gröbner basis are incredibly important. An immediate result is that they solve the problem of membership. To see if a polynomial f is an element of an ideal I, we can reduce it with respect to the Gröbner basis G of I. $f \in I$ if and only if the remainder of f under division of G is 0. Lets take an example, Set $I = \langle x^2 + y, x^3y \rangle$, we want to see if $f = xy^3$ is an element of I. Clearly f is not divisible by any generator. However $f = xy^2(x^2 + y) - y(x^3y)$, and hence an element of I. We can take the Gröbner Basis $G = (x^2 + y, x^3y, xy^2)$, now we can clearly see that f is a part of the ideal. In the general case where the polynomial is not a direct multiple of a particular Gröbner basis, we can use the Buchberger's Algorithm. If the remainder is 0 then the polynomial is a member if not then the polynomial is not part of the ideal. This was also discuses in [6].

Definition 4.17 *The l-th elimination ideal I_l is defined by,*

$$I_l = I \cap k[x_{l+1}, ..., x_n],$$

given that $I = \langle f_1, ..., f_n \rangle \subset k[x_1, ..., x_n]$. I_l is a ideal of $k[x_{l+1}, ..., x_n]$.

It is important to note that I_l eliminates all variables up to order l. It does not itself contain any element of *l-th* order.

Theorem 4.18 ***The Elimination Theorem*** *states that for a given ideal $I \subset k[x_1, ..., x_n]$ with the Gröbner basis G. Then a Gröbner basis of the l-th elimination ideal I_l can be constructed by:*

$$G_l = G \cap k[x_{l+1}, ..., x_n]$$

where $0 \leq l \leq n$ and everything is in respect to lex order where $x_1 > x_2 > \cdots > x_n$.

Proof. For any fixed $0 \leq l \leq n$ we know that $G_l \subset I_l$ as a result of its construction. This leaves us only needing to prove:

$$\langle LT(I_l) \rangle = \langle LT(G_l) \rangle$$

as the definition of a Gröbner basis. The fact that $\langle LT(G_l) \rangle \subset \langle LT(I_l) \rangle$ is obvious. To prove the other implication that $\langle LT(I_l) \rangle \subset \langle LT(G_l) \rangle$. It suffices to prove that for any $f \in I_l$ that its leading term $LT(f)$ is divisible by $LT(g)$ for some $g \in G_l$.

Since f also lies in I, By the fact that G was the Gröbner basis of I, we know that $LT(f)$ is divisible by some $LT(g)$ for a given $g \in G$. As we are working in lex order where the variables $x_i > x_{i+1}$, and because of $f \in k[x_{l+1}, ..., x_n]$ we know that $LT(g)$ only involves $x_{l+1}, ..., x_n$. Lex order states that any monomial involving the variables $x_1, ..., x_l$ is greater than a monomial in $k[x_{l+1}, ..., x_n]$. Hence if g was not strictly in $k[x_{l+1}, ..., x_n]$ it would be the leading term hence $g \in k[x_{l+1}, ..., x_n]$.

5 Hilbert's Invariants Theorem

In this section, we will closely follow chapters 7.1-7.3 of David Cox's book Ideals, Varieties, and Algorithms. We will tackle the bread and butter of this thesis, Hilbert's Invariance Theorem. Hilbert published this paper in 1893 with some scepticism; he quickly silenced the criticism and was promptly celebrated [5]. We will first lay some groundwork and then prove his theorem in a more modern way, then we will follow in the steps he himself took.

To begin with, we will discuss symmetric polynomials, which are the foundation of our understanding of Hilbert's Invariance Theorem.

Definition 5.1 *A polynomial is called a* ***symmetric polynomial*** $f \in k[x_1, ..., x_n]$ *if:*

$$f(x_{i_1}, ..., x_{i_n}) = f(x_1, ..., x_n)$$

for any permutation $(i_1, ..., i_n)$ *of* $(1, ..., n)$.

An example would be given the variables x, y, and z would be $x^2 + y^2 + z^2$ and $xy + yz + xz$. In the last example, it is important to remember that we are working with commutative rings, and hence, any change in variables will not change the result.

Definition 5.2 *We define the* ***elementary symmetric function*** $\sigma_1, ...\sigma_n \in k[x_1, ..., x_n]$ *given the variables* $x_1, ..., x_n$ *by:*

$$\sigma_1 = x_1 + ... + x_n,$$

$$\sigma_r = \sum_{i_1 < i_2 < i_r} x_{i_1} x_{i_2} \cdots x_{i_r},$$

$$\sigma_n = x_1 x_2 ... x_n.$$

Theorem 5.3 ***The Fundamental Theorem of Symmetric Polynomials*** *states that every symmetric polynomial in* $k[x_1, ..., x_n]$*can be uniquely constructed by the elementary symmetric functions* $\sigma_1, ...\sigma_n$.

Proof. Throughout this proof we will use Lex order $x_1 > x_2 > ... > x_n$. The first step is to assure ourselves of the form of the Leading term $LT(f)$ given the nonzero symmetric function $f \in k[x_1, ..., x_n]$. Given $LT(f) = ax^\alpha$ where $\alpha = (\alpha_1, ..., \alpha_n)$ we claim that $\alpha_1 \geq \alpha_2 ... \geq \alpha_n$. We will proof this by contradiction, if our claim was untrue there must be some i where $\alpha_i < \alpha_{i+1}$. We now let β denote the exponent vector $\beta = (..., \alpha_{i+1}, \alpha_i, ...)$. By the fact that ax^α is a term of f we know that ax^β must be a term of $f(..., x_{i+1}, x_i, ...)$ but as f is symmetric $f(..., x_{i+1}, x_i, ...) = f$, hence ax^β must be a term in f. Because

by Lex order $\beta > \alpha$ it implies that ax^α can not be the leading term of f which was our founding assumption hence we proved that $\alpha_1 \geq \alpha_2 ... \geq \alpha_n$.

To continue the proof, we will start by letting:

$$h = \sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3}\cdots\sigma_{n-1}^{\alpha_{n-1}-\alpha_n}\sigma_n^{a_n}$$

To find the leading term of h we first need to note that the leading term $LT(\sigma_r) = x_1x_2\cdots x_r$ for $1 \leq r \leq n$, this means that:

$$\begin{aligned} LT(h) &= LT(\sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3}\cdots\sigma_{n-1}^{\alpha_{n-1}-\alpha_n}\sigma_n^{\alpha_n}) \\ &= LT(\sigma_1)^{\alpha_1-\alpha_2}LT(\sigma_2)^{\alpha_2-\alpha_3}LT(\sigma_{n-1})^{\alpha_{n-1}-\alpha_n}LT(\sigma_n)^{\alpha_n} \\ &= x_1^{\alpha_1-\alpha_2}(x_1x_2)^{\alpha_2-\alpha_3}\cdots(x_1\cdots x_n)^{\alpha_n} \\ &= x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n} = x^\alpha. \end{aligned} \tag{2}$$

As the leading term of f is ah, where the coefficient a is the same as in ax^α. This gives us that if $LT(f) - ah \neq 0$:

$$multideg(f - ah) < multideg(f).$$

This allows us to construct other symmetric functions $f_1 = f - ah$, which only differ from f by not containing $LT(f)$. f_1 is symmetric as both f and ah are symmetric. This process can be continued giving us $f_2 = f_1 - a_1h_1$, where a_1 is a constant and h_1 is like h is a product of various powers of $\sigma_1, ..., \sigma_n$. We also know that if $f_2 \neq 0$ then $LT(f_2) < LT(f_1)$. By continuing this cycle for the polynomials $f, f_1, f_2, ...$ where:

$$multideg(f) > multideg(f_1) > multideg(f_2) > \cdots .$$

This sequence is finite as Lex order is **well-ordering**, which implies there is a smallest element under $>$. This implies that the process terminates at an element $f_{t+1} = 0$ for some t giving us:

$$f = ah + a_1h_1 +, ..., +a_th_t.$$

This clearly shows that f can be expressed as a polynomial of elementary symmetric functions, as all h_i for all i are constructed from elementary symmetric functions. This leaves us to prove uniqueness of said polynomial. We will prove this by first supposing that for two polynomials g_1 and $g_2$in n variables, $y_1, .., y_n$:

$$f = g_1(\sigma_1, ..., \sigma_n) = g_2(\sigma_1, ..., \sigma_n),$$

we now have too prove that $g_1 = g_2$ in $k[y_1, ..., y_n]$.

We will start by setting $g = g_1 - g_2$, then if $g_1 = g_2$, $g(\sigma_1, ..., \sigma_n) = 0$ in $k[x_1, ..., x_n]$. If we prove that g is the zero polynomial in $k[y_1, ..., y_n]$, then we will have proven uniqueness. Lets assume that $g \neq 0$, and we write $g(\sigma_1, ..., \sigma_n)$

as a sum of polynomials $g = \sum_\beta a_\beta y^\beta$, then $g_\beta = a_\beta \sigma_1^{\beta_1}\sigma_2^{\beta_2}\cdots\sigma_n^{\beta_n}$, were $\beta = (\beta_1, ..., \beta_n)$. We know by Equation 2 that:

$$LT(g_\beta) = a_\beta x_1^{\beta_1+...+\beta_n} x_2^{\beta_2+...+\beta_n} x_n^{\beta_n}$$

We need to assure ourselves of the fact that:

$$(\beta_1, ..., \beta_n) \mapsto (\beta_1 + ..., \beta_n, \beta_2 + ... + \beta_n, ..., \beta_n)$$

is injective. Assume that $\gamma_1 = (\beta_{1,1}, ..., \beta_{1,n})$ and $\gamma_2 = (\beta_{2,1}, ..., \beta_{2,n})$ and:

$$(\beta_{1,1}+..., \beta_{1,n}, \beta_{1,2}+...+\beta_{1,n}, ..., \beta_{1,n}) = (\beta_{2,1}+..., \beta_{2,n}, \beta_{2,2}+...+\beta_{2,n}, ..., \beta_{2,n}.)$$

The map is injective if $\gamma_1 = \gamma_2$. We will prove this by contradiction, if $\gamma_1 \neq \gamma_2$ then there must be an i where $\beta_{1,i} \neq \beta_{2,i}$ yet because we assumed the both γ_1 and γ_2 to have the same image we get:

$$\beta_{1,i} + ... + \beta_{1,n} = \beta_{2,i} + ... + \beta_{2,n}$$

however

$$\beta_{1,i+1} + ... + \beta_{1,n} = \beta_{2,i+1} + ... + \beta_{2,n} = b.$$

This is a clear contradiction as it implies $\beta_{1,i} + b = \beta_{2,i} + b$ when we assumed $\beta_{1,i} \neq \beta_{2,i}$. Injectivity implies that the leading terms of g_β are distinct. By choosing β so that $LT(g_\beta) > LT(g_\gamma)$ for all $\gamma \neq \beta$. Hence $LT(g_\beta)$ is greater than any term of the g_y's. This, in turn, means that there is no term of g_γ that can cancel the $LT(g_\beta)$; this means that $g(\sigma_1, ..., \sigma_n)$ can not be zero as it is defined as $g = g_1 - g_2$. Hence uniqueness is proved.

and that if $LT(g_\beta) > LT(g_\gamma)$ for all $\beta \neq \gamma$, then $LT(g_\beta)$ will be greater than all terms of all g_y's. This, in turn, means that there is no term of g_γ that can cancel the $LT(g_\beta)$; this means that $g(\sigma_1, ..., \sigma_n)$ can not be zero as it is defined as $g = g_1 - g_2$. Hence uniqueness is proved.

Proposition 5.4 *Given the ring $k[x_1, ..., x_n, y_1, ..., y_n]$, for a fixed monomial order where all monomials containing $x_1, ..., x_n$ are greater than all monomials in $k[y_1, ..., y_n]$. Given the ideal $\langle \sigma_1 - y_1, ..., \sigma_2 - y_2 \rangle \subset k[x_1, ..., x_n, y_1, ..., y_n]$ let G be a Gröbner basis of ideal. Let $g = \overline{f}^G$ be the remainder for a given function $f \in k[x_1, ..., x_n]$ for division over G then:*

1. *The polynomial f is symmetric if and only if the remainder $g \in k[y_1, ..., y_n]$*
2. *A symmetric polynomial f can be uniquely expressed as the polynomial in the elementary symmetric functions $f = g(\sigma_1, ..., \sigma_n)$ where g is the remainder as defined above.*

Proof. Recall that $g \in k[x_1, ..., x_n, y_2, ..., y_n]]$ is the remainder of $f \in k[x_1, ..., x_n]$ under $G = \{g_1, ..., g_t\}$, meaning for $A_1, ..., A_t \in k[x_1, ..., x_n, y_1, ..., y_n]$:

$$f = A_1 g_1 + ... + A_t g_t + g.$$

We will start by assuming that for all i, $g_i \neq 0$. To prove *1* we will start by proving that g being an element of $k[y_1, ..., y_n]$ implies that f is symmetric. We will do this by substituting σ_i for $y_i$in $f = A_1 g_1 + ... + A_t g_t + g$. As $f \in k[x_1, ..., x_n]$ and is hence only determined by $x_1, ..., x_n$ and is hence not affected by the substitution. As $G = \{g_1, ..., g_t\}$ is the Gröbner basis of the ideal $\langle \sigma_1 - y_1, ..., \sigma_2 - y_2 \rangle$, where all polynomials go to zero under this substitution, implying:

$$f = g(\sigma_1, ..., \sigma_n).$$

This shows that f must be symmetric.

Now to prove that given $f \in k[x_1, ..., x_n]$ is symmetric, $f = g(\sigma_1, ..., \sigma_n)$ for some $g \in k[y_1, ..., y_n]$ then under division of G, g is the remainder of f. We begin by noting that a monomial expressed in $\sigma_1, .., \sigma_n$ in $k[x_1, .., x_n, y_1, ..., y_n]$can be written as:

$$\begin{aligned} \sigma_1^{\alpha_1} \cdots \sigma_n^{\alpha_n} &= (y_1 + (\sigma_1 - y_1))^{\alpha_1} \cdots (y_n + (\sigma_n - y_n))^{\alpha_n} \\ &= y_1^{\alpha_1} \cdots y_n^{\alpha_n} + B_1 \cdot (\sigma_1 - y_1) + ... + B_n \cdot (\sigma_n - y_n) \end{aligned}$$

where all $B_1, ..., B_n$ are elements of $k[x_1, ..., x_n, y_1, ..., y_n]$. We will express $g(\sigma_1, ..., \sigma_n)$ in the same way. As $g(\sigma_1, ..., \sigma_n)$ can be seen as a sum of monomial orders, we can write it as:

$$g(\sigma_1, .., \sigma_n) = g(y_1, ..., y_n) + C_1 \cdot (y_1 - \sigma_1) + ... + C_n \cdot (y_n - \sigma_n),$$

for some $C_1, ..., C_n \in k[x_1, ..., x_n, y_1, ..., y_n]$. We know that $f = g(\sigma_1, .., \sigma_n)$, we can then rewrite f as:

$$f = C_1 \cdot (y_1 - \sigma_1) + ... + C_n \cdot (y_n - \sigma_n) + g(y_1, ..., y_n). \tag{3}$$

We now want to show that $g(y_1, ..., y_n)$ is the remainder of f under division by G, to do this, we will show that g is not divisible by any element of $LT(G)$. Lets assume that for some $g_i \in G$, $LT(g_1)$ divides some term of g. Because $g \in k[y_1, ..., y_n]$ it implies that g_i only involves $y_1, ..., y_n$. But since $g_i \in G$ and hence an element of $\langle \sigma_1 - y_1, ..., \sigma_2 - y_2 \rangle$. We already know that under the substitution $y_i \mapsto \sigma_i$ g_i becomes zero. This implies that $g_i(\sigma_1, ..., \sigma_n) = 0$ by the uniqunes implied by Theorem 5.3 we know that $g_i = 0$ which is not posible by our founding assumption.

2 follows directly from Equation 3, where g is the remainder.

Lemma 5.5 *For any given polynomial f in $k[x_1, .., x_n]$, then f is symmetric if and only if every* ***homogeneous components*** *of f also is.*

Proof. It is obvious that if the homogeneous components of f are symmetric so is f. Now we have to prove that if f is symmetric, then so are its homogeneous components. Let $x_{i_1}, ..., x_{i_n}$ be a permutation of $x_1, ..., x_n$. Each homogeneous component of a symmetric polynomial is itself symmetric. If not, then f could not possibly be symmetric.

Theorem 5.6 *All symmetric polynomials in $k[x_1, ..., x_n]$ for a given field k which contains the rational numbers $\mathbb{Q}$ can be expressed as a polynomial in the power sums, $s_1, ..., s_n$.*

The proof of this theorem is given on page 324 of [3].

Now that we have tackled the symmetric polynomials, we will start working towards Hilbert's Invariance Theorem. First, however, we will focus on matrix groups and the concept of invariance.

Definition 5.7 *The* ***General Linear Group*** *$GL(n, k)$ is the set of invertible $n \times n$ matrices where the entries are from field k.*

Note that $GL(n, k)$ is a group, given A and B being invertible matrices then so is A^{-1} and $A \cdot B$, and given the identity matrix I_n: $I_n \cdot A = A \cdot I_n = A$ and $A \cdot A^{-1} = I_n$. Examples of, General Linear Group would be non zero diagonal matrices or upper triangular matrices with complete diagonal.

Definition 5.8 *A* ***finite matrix group*** *G is a finite nonempty subset of $GL(n, k)$ which is closed under matrix multiplication; the number of elements in G is referred to as its* ***order****.*

The most obvious example would be the identity group, the group with only the identity matrices of a given order. Another example would be the matrix group:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

where both matrices are their own inverses.

Definition 5.9 *Given a finite matrix group $G \in GL(n, k)$, a polynomial $f(\boldsymbol{x}) \in k[x_1, ..., x_n]$ is said to be* ***invariant under*** *G if:*

$$f(\boldsymbol{x}) = f(A \cdot \boldsymbol{x})$$

for all $A \in G$, we denote the set of invariant polynomials $k[x_1, ..., x_n]^G$.

It is important to note that we are not transforming the polynomial itself over a matrix, but the variables. If we would have the common three variables x, y, z we would be working with 3×3 matrices. One might immediately spot how transforming the polynomial itself falls flat when observing the dimension of the matrix. What would be transformed and how. What we are really trying to do is transform the variables, and seeing if the polynomial can remain the same, an example can help illustrate this:

$$f\left(\begin{pmatrix}1 & 2 & 1\\ 0 & 0 & 1\\ 2 & 3 & 1\end{pmatrix}\begin{pmatrix}x\\ y\\ z\end{pmatrix}\right) = f(x+2y+z, z, 2x+3y+z).$$

Let us take a more manageable example and actually calculate its invariance:

Example 5.10 *Take G to be generated by$A = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$, this gives us that $G = \{I, A\}$, for f to be invariant under G is the same as $f(x, y) = f(y, x)$, since every polynomial is invariant under the identity. This matches the symmetric polynomials in two variables, giving us that $k[x, y]^G = k[x + y, xy]$ by Theorem 5.6.*

Lemma 5.11 *The set of polynomials $k[x_1, ..., x_n]^G$ is closed under multiplication and addition and contains the constant polynomial.*

Proof. It is obvious that $k[x_1, ..., x_n]^G$ contains the constant polynomials. So we will show that it is closed under addition and multiplication. It follows directly by the fact that $(f + g)(\mathbf{x})$ and $fg(\mathbf{x}) = f(\mathbf{x})g(\mathbf{x})$.

Lemma 5.12 *For a given finite matrix group $G \subset GL(n, k)$, if we can express all $A_1, ..., A_m \in G$ in terms*

$$A = B_1 B_2 ... B_t$$

where all $B_i \in \{A_1, ..., A_m\}$, $A_1, ..., A_m$ is said to generate G, and $f \in k[x_1, ..., x_n]$ is in $k[x_1, ..., x_n]^G$ if and only if:

$$f(\boldsymbol{x}) = f(A_1 \cdot \boldsymbol{x}) = ... = f(A_m \cdot \boldsymbol{x}).$$

Proof. To prove this, we will start by proving that if f is invariant under $B_1, ..., B_t$ individually, then it is also invariant under their product. To do this, we will use induction. It is obvious that for $t = 1$, then, the assertion is true. Under the assumption that it holds for $t - 1$, then:

$$\begin{aligned} f((B_1 \cdots B_t)\mathbf{x}) &= f((B_1 \cdots B_{t-1})B_t\mathbf{x}) \\ &= f(B_t\mathbf{x}) \text{ (by our asuumption that for } t-1\ B_1 \cdots B_{t-1} \text{ is invariant)} \\ &= f(\mathbf{x}) \text{ (because of the invariance under } B_t) \end{aligned}$$

As all elements of $A_1, ..., A_m$ can be expressed as a product of $B_1, ..., B_t$, we know that if f is invariant under $A_1, ..., A_m$ that f must be in $k[x_1, ..., x_n]^G$. By the definition of invariant, the converse follows.

Definition 5.13 *Given a finite matrix group $G \in GL(n, k)$, the **Reynolds Operator** of G is the map $R_G : k[x_1, ..., x_n] \to k[x_1, ..., x_n]$ defined by the formula:*

$$R_G(f)(\boldsymbol{x}) = \frac{1}{\mid G \mid} \sum_{A \in G} f(A \cdot \boldsymbol{x})$$

for $f(\boldsymbol{x}) \in k[x_1, ..., x_n]$.

Even though the Reynolds Operator might feel out of place, it is a hugely important operator, and it is the key to proving Hilbert's Invariance Theorem of rings with characteristic 0. If the characteristic was not 0, then we can not ensure that $\mid G \mid \neq 0$, and as we divide by $\mid G \mid \neq 0$, it creates a problem. We will use the following properties of the Reynolds operator, in particular.

Lemma 5.14 *Given a finite matrix group G, let R_G be the Reynolds Operator of G, the Reynolds Operator has the following properties:*

1. *R_G is k-linear in terms of f.*
2. *If $f \in k[x_1, ..., x_n]$, then $R_G(f) \in k[x_1, ..., x_n]^G$.*
3. *If $f \in k[x_1, ..., x_n]^G$, then $R_G(f) = f$.*

Where k-linear refers to a map that satisfies $R_G(sf + rg) = sR_G(f) + rR_G(g)$ where f and $g \in k[x_1, ..., x_n]$ and, s and $r \in k$. In this case, the Reynolds operator R_G is our map. We are not saying that the Reynolds operator is linear in terms of $[x_1, ..., x_n]$.

Proof. To prove that R_G is linear we first write:

$$R_G(sf + rg) = \frac{1}{\mid G \mid} \sum_{A \in G} (sf + rg)(A \cdot \mathbf{x}) = \sum_{A \in G} sf(A \cdot \mathbf{x}) + \sum_{A \in G} rg(A \cdot \mathbf{x})$$

as both $s and r \in k$ it follows immediately that $R_G(sf + rg) = sR_G(f) + rR_G(g)$.

We will prove *2* by taking an element $B \in G$, then we get:

$$R_G(f)(B\mathbf{x}) \frac{1}{\mid G \mid} \sum_{A \in G} f(A \cdot B\mathbf{x}) = \frac{1}{\mid G \mid} \sum_{A \in G} f(AB \cdot \mathbf{x}).$$

It is important too note that if we write $G = \{A_1, A_2, ..., A_{|G|}\}$ then $A_i B \neq A_j B$ if $i \neq j$ as it would imply $A_i = A_j$ by the fact of multiplying B^{-1} to

both sides. This implies the subset $\{A_1B, ..., A_{|G|}\} \in G$, contains $\mid G \mid$ distinct elements, all in G hence:

$$G = \{AB : A \in G\}.$$

It is important to once again note that we are working in characteristic 0. If the ring was not of characteristic 0 this argument would fail. An example is $mod\, 6$ where $2 \cdot 2 \mid mod\, 6 = 2 \cdot 5 \mid mod\, 6 = 4$.

Knowing $G = \{AB : A \in G\}$ we $f(AB\mathbf{x})$ are the same polynomials contained in $f(a\mathbf{x})$ possibly in a different order. This gives us that:

$$\frac{1}{\mid G \mid} \sum_{A \in G} f(AB \cdot \mathbf{x}) = \frac{1}{\mid G \mid} \sum_{A \in G} f(A \cdot \mathbf{x}) = R_G(f)(\mathbf{x})$$

as a result $R_G(f)(B \cdot \mathbf{x}) = R_G(f)(\mathbf{x})$ for all $B \in G$, that $R_G(f) \in k[x_1, ..., x_n]^G$, which proves *2*.

To prove *3* by the fact that $f(\mathbf{x})$ is invariant under G, giving us that:

$$R_G(f)(\mathbf{x}) = \frac{1}{\mid G \mid} \sum_{A \in G} f(A \cdot \mathbf{x}) = \frac{1}{\mid G \mid} \sum_{A \in G} f(\mathbf{x}) = f(\mathbf{x}.)$$

Theorem 5.15 *For any finite matrix group $G \in GL(n, k)$, $k[x_1, ..., x_n]^G$ is finitely generated by homogeneous invariants, written as:*

$$k[x_1, ..., x_n]^G = k[R_G(x^\beta) :\mid \beta \mid \leq \mid G \mid].$$

Proof. If, $f = \sum_a c_a x^a \in k[x_1, ..., x_n]^G$ then by the fact that $R_G(f) = f$ as $f \in k[x_1, ..., x_n]^G$ we get that:

$$f = R_G(f) = R_G(\sum_\alpha c_\alpha x^\alpha) = \sum_\alpha c_\alpha R_G(x^\alpha).$$

Meaning that every invariant is a linear combination (over k) of elements in form $R_G(x^\alpha)$. Which in turn means that we only have to prove that for every α, $R_G(x^\alpha)$ is a polynomial in $R_G(x^\beta), \mid \beta \mid \leq \mid G \mid$. Emmy Noether solved this by combining all $R_G(x^\beta$ of total degree l, which is a fixed integer. Here is where the study of symmetric functions becomes relevant; for a power sum much as we discussed, we know that said power sum can be expressed as finitely many power sums. We will follow her proof.

We will first start by expanding $(x_1 + ... + x_n)^l$ into a sum of monomials x^α as follows:

$$(x_1 + ... + x_n)^l = \sum_{|\alpha| = l} a_\alpha x^\alpha$$

We will start by proving that every coefficient a_α is a positive integer for all $|\alpha| = l$.

If $A = (a_{ij})$ is an element of the matrix group G, we denote A_i to be the i-th row of A. Then $A_i\mathbf{x} = a_{i1}x_1 + ... + a_{in}x_n$ as $\mathbf{x}$ refers to the column vector of n elements, and if $\alpha = (a_1, ..., a_n) \in Z^n_{\geq 0}$, given this we construct the notation:

$$(A \cdot \mathbf{x})\alpha = (A_1 \cdot \mathbf{x})^\alpha \cdots (A_n \cdot \mathbf{x})^\alpha.$$

Giving us:

$$R_G(x^\alpha) = \frac{1}{\mid G \mid} \sum_{A \in G} (A \cdot X)^\alpha$$

We will now introduce new variables $u_1, ..., u_n$ this is to be able to rewrite $(x_1 + ... + x_n)^l$ where $u_i A_i \mathbf{x} = x_i$ which gives us:

$$(u_1 A_1 \cdot \mathbf{x} + ... + u_n A_n \cdot \mathbf{x})^l = \sum_{|\alpha|=l} a_\alpha (A \cdot \mathbf{x})^\alpha u^\alpha.$$

If we now sum over all $A \in G$ we get that:

$$S_l = \sum_{A \in G} (u_1 A_1 \cdot \mathbf{x} + ... + u_n A_n \cdot \mathbf{x})^l = \sum_{|\alpha|=l} a_\alpha (\sum_{A \in G} (A \cdot \mathbf{x})^\alpha) u^\alpha. \tag{4}$$

If we introduce b_n where $b_n \mid G \mid = a_n$ we get that:

$$\sum_{|\alpha|=l} a_\alpha (\sum_{A \in G} (A \cdot \mathbf{x})^\alpha) u^\alpha = \sum_{|\alpha|=l} b_\alpha R_G(x^\alpha) u^\alpha \tag{5}$$

This reveals the reason we introduced the variables $u_1, ..., u.n$, as we take the sum of all $R_G(x^\alpha)$ with $\mid \alpha \mid = l$. To avoid cancellation to occur, we use $u_1, ..., u.n$.

Since $S_l = \sum_{A \in G} (u_1 A_1 \cdot \mathbf{x} + ... + u_n A_n \cdot \mathbf{x})^l$ is a l-th power sum with $\mid G \mid$ quantities

$$U_A = u_1 A_1 \cdot \mathbf{x} + ... + u_n A_n \cdot \mathbf{x}$$

indexed $A \in G$. We use the notation $S_l = S_l(U_A : A \in G)$ to describe this. By Theorem 5.6 and since S_l is symmetric in U_A, and as all symmetric function in the $\mid G \mid$ quantities in U_A can be written as a polynomial in $S_1, ..., S_{|G|}$. This then gives us:

$$S_l = F(S_1, ..., S_{|G|}),$$

where F is polynomial with coefficients of total order equal to l. If we now substitute this into Equations 4 and then Equation 5 we get that:

$$\sum_{|\alpha|=l} b_\alpha R_G(x^\alpha) u^\alpha = F\left(\sum_{|\beta|=l} b_\beta R_G(x^\beta) u^\beta, ..., \sum_{|\beta|=|G|} R_G(x^\beta) u^\beta \right)$$

By expanding the right-hand side, we would get a sum where the only thing left to do was to equate the coefficients u^α we get:

$$b_\alpha R_G(x^\alpha) \textit{ is a polynomial in } R_G(x^\beta)$$

By the fact that k has characteristic 0 $b_\alpha =\mid G \mid a_\alpha$ as $\mid G \mid$ can not be 0. This means that $R_G(x^\alpha)$ can be expressed as a polynomial in $k[R_G(x^\beta)]$ and the theorem is proven.

We have tecnicly proven **Hilbert Invariance Theorem**; however, this was not the way he himself did it. We will now follow a proof more in line with his methods.

Theorem 5.16 ***Hilbers't Invariance Theorem.*** *The ring of invariance $k[x_1, ..., x_n]^G$ is finitely generated by homogeneous invariants.*

Proof. We will prove this by contradiction. Take a given finite matrix group $G \subset GL(n, k)$; we want to show that it is finitely generated. To do this, imagine the ideal $I \subset k[x_1, ..., x_n]$, which is generated by all invariants that have positive total degree. This means that for a monomial:

$$x^\alpha = x^{\alpha_1} \cdots x^{\alpha_n},$$

where the total degree is $\alpha_1 + ... + \alpha_n$.

By Hilbert's Basis Theorem, we know that the ideal $I\langle f_1, ..., f_m\rangle$ is finitely generated. We now want to show that $k[f_1, ..., f_n] = k[x_1, ..., x_n]^G$. It is trivial to see that $k[f_1, ..., f_n] \subset k[x_1, ..., x_n]^G$, however $k[x_1, ..., x_n]^G \subset k[f_1, ..., f_n]$ is not.

Imagine if $k[x_1, ..., x_n]^G \not\subset k[f_1, ..., f_n]$ then there must be an element in $k[x_1, ..., x_n]^G$, and as a result, there must be a homogeneous invariant f not in $k[f_1, ..., f_n]$, as if all its homogeneous invariants are in $k[f_1, ..., f_n]$ so is the invariant itself.
From this point on, we will choose f to have minimal degree d.

By definition, $f \in I = \langle f_1, ..., f_m\rangle$ meaning we can express f as the sum:

$$f = \sum_{i=0}^{m} h_i f_i,$$

where $h_1, ..., h_m \in k[x_1, ..., x_n]$. By the fact that f_i is of homogeneous degree as it is an element of $I = \langle f_1, ..., f_m\rangle$, we can pick h_i to ensure that $h_i f_i$ is also of homogeneous degree or simply 0.

This is where Reynolds Operators come in, we know by Lemma 5.14 $R_G(f) = f$, and at the beginning of the proof of Theorem 5.15 we showed $f = \sum_{i=0}^{m} R_G(h_i) f_i$. As f_i is of positive degree, it follows that $R_G(h_i)$ has degree smaller than d.

By the definition of the Reynolds Operator, $R_G(h_i) = \frac{1}{G}\sum_{A\in G} h_i(A\cdot \mathbf{x})$ we know it must be invariant by Lemma 5.14. We also know that it must be of homogeneous order as it is a sum of homogeneous elements. Hence $R_G(h_i) \in k[f_1, ..., f_m]$ of order strictly less than f this is where the contradiction lies, as we choose f to have minimal degree.

Example 5.17 *We can now apply these concepts to an actual example. Take the matrix group generated by A:*

$$A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \in GL(2, k).$$

It is actually the cyclic matrix group of order 3 C_3, as shown below.

$$A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, A^2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, A^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

We can now use Theorem 5.15 knowing that $k[x_1, ..., x_n]^G$ will be generated by monomials of order 3 or less. First, however, we make our life easy and calculate the general case:

$$R_{C_3}(f)(x, y) = \frac{1}{3}(f(x, y) + f(-y, x - y) + f(-x + y, -x)).$$

This allows us to construct the list of Reynolds Operators:

$$R_{C_3}(x) = \frac{1}{3}(x + (-y) + (-x + y)) = 0$$

$$R_{C_3}(x^2) = \frac{1}{3}(x^2 + y^2 + (-x + y)^2) = \frac{1}{3}(2x^2 + 2y^2 - 2xy)$$

$$R_{C_3}(x^3) = \frac{1}{3}(x^3 + y^3 + (-x + y)^3 = \frac{1}{3}(3x^2y - 3xy^2)) = x^2y - xy^2$$

$$R_{C_3}(y) = \frac{1}{3}(y + x - y + -x) = 0$$

$$R_{C_3}(y^2) = \frac{1}{3}(y^2 + (x - y)^2 + (-x)^2) = \frac{1}{3}(2x^2 + 2y^2 - 2xy)$$

$$R_{C_3}(y^3) = \frac{1}{3}(y^3 + (x - y)^3 + (-x)^3) = \frac{1}{3}(3xy^2 - 3x^2y) = xy^2 - x^2y$$

$$R_{C_3}(xy) = \frac{1}{3}(xy + (-y)(x - y) + (-x + y)(-x)) = \frac{1}{3}(x^2 + y^2 - xy)$$

$$R_{C_3}(x^2y) = \frac{1}{3}(x^2y + (-y)^2(x-y) + (-x+y)^2(-x)) = \frac{1}{3}(-x^3 + 3x^2y - y^3)$$

$$R_{C_3}(xy^2) = \frac{1}{3}(xy^2 + (-y)(x-y)^2 + (-x+y)(-x)^2) = \frac{1}{3}(-x^3 + 3xy^2 - y^3)$$

$$k[x_1, ..., x_n]^G = k[u, v, s, t]$$

where:

$$u = x^2 + y^2 - xy, v = x^2y - xy^2, s = -x^3 + 3x^2y - y^3, t = x^3 + 3xy^2 - y^3$$

However we can see that $(-x^3+3x^2y-y^3)-3(x^2y-xy^2) = -x^3+3xy^2-y^3$ *hence,*

$$k[x_1, ..., x_n]^G = k[u, v, s]$$

where:

$$u = x^2 + y^2 - xy, v = x^2y - xy^2, s = -x^3 + 3x^2y - y^3.$$

To verify that none of $x^2+y^2-xy, x^2y-xy^2, -x^3+3x^2y-y^3$ *can be generated by the other two generators, we come to this chapter's last theorem.*

```
P.<x,y,z> = PolynomialRing(QQ, 3, order='lex')


def reduce(p,lis):
    r= p
    count= True
    while count: # we will iterate until r is no longer reducible
        count= False
        for l in lis:
            if  l !=0 and l.lm().divides(r.lm()) : # checks divisibility of leading term
                r = r-r.lc()/l.lc()*r.lm()//l.lm()*l #removes the leading term
                if r!=0:#stops infinite loops when r=0
                    count= True
    return r


def reynolds(t):
    m= matrix([[x],[y]])
    G = MatrixGroup(t)
    car = G.cardinality()
```

```
    listvar= []
    for g in G:
        gm= g*m
        gx= gm[0,0] #x variable
        gy= gm[1,0] #y variable
        listvar.append([gx,gy])
    listRey= []
    for r in range(car+1): #we will use this to iterate over all posible powers.
        for h in range(car+1-r):
            if r==0 and h==0: #ensures we do not generate constant which break following coc
                continue
            Reynolds= 0
            for a in range(car):
                gx, gy = listvar[a] #gathers the x,y variables
                Reynolds += gx**r * gy**h #generates Reynolds

            if Reynolds !=0: #Asures no 0's can cause problems
                listRey.append(Reynolds)
    I =[]
    for f in listRey:# we will reduce the list G to F to remove redundent terms
        re= reduce(f, I)
        if re!= 0:
            I.append(re) #We reduce the terms
    return I
A= matrix([[0,-1],[1,-1]])
reynolds(A)
```

The code yields $[2*x^2-2*x*y+2*y^2, 3*y^3, 3*x*y^2]$*, these generators satisfy the same algebraic relations and hence the invariant rings are isomorphic.*

Theorem 5.18 *For the given set of polynomials* $f_1, ..., f_m \in k[x_1, ..., x_n]$*. Take a fixed monomial order* $k[x_1, ..., x_n, y_1, ..., y_m]$*, where monomials in* $k[x_1, .., x_n]$ *are said to be greater than monomial involving any element in* $k[y_1, ..., y_n]$*. Now take the ideal* $\langle f_1 - y_1, ..., f_m - y_m\rangle \subset k[x_1, ..., x_n, y_1, ..., y_m]$ *and let* G *be its Gröbner basis. Then the polynomial* $f \in k[x_1, ..., x_n]$*, and let* $g = \overline{f}^G$ *be the remainder of the division algorithm of* f *under* G*, the following properties hold true.*

1. *f is an element of $k[f_1, ..., f_m]$ if and only if the remainder g is an element of $k[y_1, ..., y_m]$.*
2. *If the polynomial $f \in k[f_1, ..., f_m]$ then f can be expressed as the polynomial $f = g(f_1, ..., f_m)$ where g is said remainder.*

the proof broadly follows the proof of Proposition 5.4 and is found on page 341 of [3].

Example 5.19 *We can now use this theorem to determine whether the generators of the last example can be constructed by the other two.*

First set

$$J = \langle x^2 + y^2 - xy - t, x^2y - xy^2 - u \rangle \subset k[x, y, t, u]$$

We first used Sage Math to find the Gröbner basis of J:

$$y^3 - yt + u, x^2 - xy + y^2 - t$$

We then use Sage Math to find the remainder of $-x^3 + 3x^2y - y^3$ *under the division of the Gröbner basis of J.*

$$3xy^2 - xt - yt + 3u.$$

Which is not an element of $k[t, u]$ *hence* $-x^3 + 3x^2y - y^3 \not\subset k[x^2 + y^2 - xy, x^2y - xy^2]$ *and hence we need all three generators to generate the ideal of invariance. Which is why the code above ends with finding the Gröbner basis.*

The code used in this example:

The resources which I used to write this code are found at [9]

6 The Generators of the Set of Invariants

In the previous section, we showed that for any finite matrix group $g \in GL(n,k)$ that:

$$k[x_1,...,x_n]^G = k[f_1,...,f_n]$$

for finitely many invariants $f_1,...,f_n$. However, we have not shown the algebraic relations between the invariants. Invariants are often used in Algebraic Geometry, and the consequences of the theorems often have geometric implications.

As a result of The Fundamental Theorem of Symmetric Polynomials we know that every symmetric polynomial can be written in elementary symmetric functions. This means that every invariant can be written uniquely expressed as a polynomial of finitely many invariants,

$$k[x_1,...,x_n]^{S_n} = k[\sigma_1,...,\sigma_n].$$

The natural question would be if this uniqueness holds for the case of the finite matrix group $G \subset GL(n,k)$. For $k[x_1,...,x_n]^G = k[f_1,...,f_m]$, then we can write an element uniquely in terms of $f_1,...,f_m$, if the polynomials $g_1(f_1,...,f_m) = g_2(f_1,...,f_m)$ if and only if $g_1 = g_2$. But now, take the case

$$g_1(f_1,...,f_m) = g_2(f_1,...,f_m) \Leftrightarrow h(f_1,...,f_m) = 0,$$

where $h = g_1 - g_2$. Here is where the issue is: uniqueness holds in all cases except if and only if there exists a nonzero polynomial $h(f_1,...,f_m) = 0$. This is what we are largely interested in this chapter as it is a nontrivial relation between the polynomials $f_1,...,f_m$.

For $F = (f_1,...,f_m)$, the set of algebraic relations of $f_1,...,f_m$:

$$I_F = \{h \in k[y_1,...,y_n] : h(f_1,...,f_n) = 0 \, in \, k[x_1,...,x_n]\},$$

has the following properties.

Proposition 6.1 *Given $k[x_1,...,x_n]^G = k[f_1,...,f_m]$, let $I_F = \{h \in k[y_1,...,y_n] : h(f_1,...,f_n) = 0$ in $k[x_1,...,x_n]\}$ then:*

1. *I_F is a prime ideal of $k[y_1,...,y_n]$.*
2. *Given that $k[x_1,...,x_n]^G$ and $f = g(f_1,...,f_n)$ all representations in terms of $f_1,...,f_n$ can be written as:*

$$f = g(f_1,...,f_n) + h(f_1,...,f_n)$$

for $h \in I_F$.

Proof To prove that I_F is indeed an ideal then we have to show that for any $f \in I_F$ and $h \in k[x_1, ..., x_n]$ then $hf \in I_F$, we know this as $f(f_1, ..., f_m) = 0$ then so must $h(f_1, ..., f_m)f(f_1, ..., f_m)$. To prove that I_F is also prime we have to, prove that if $fg \in I_F$ then f or g is an element of I_F. As both fg is an element of I_F means that $f(f_1, ..., f_m)g(f_1, ..., f_n) = 0$. Because $fg \in k[x_1, ..., x_n]$ and is product of polynomials then either f or g must be in I_F, as there are no zero divisors.

To prove *2* we will prove that for the representation of f, $g_1(f_1, ..., f_n)$ then is an representation $g_2(f_1, ..., f_n)$ if and only if g_2 satisfies $g_1(f_1, ..., f_n) + l(f_1, ..., f_n) = g_2(f_1, ..., f_n)$ where $l(f_1, ..., f_n) \in I_F$). The first part is obvious if $g_1(f_1, ..., f_n) + l(f_1, ..., f_n) = g_2(f_1, ..., f_n)$ then $l(f_1, ..., f_n)$ must be in I_F. To prove the second part, we need to remember that for any g_1 and g_2, then $g_1 + (g_2 - g_2) = g_2$. Meaning for any two elements there exists an $l(f_1, ..., f_2)$ that satisfies $g_1(f_1, ..., f_n) + l(f_1, ..., f_n) = g_2(f_1, ..., f_n)$, and by the first part $l(f_1, ..., f_n) \in I_F$

Proposition 6.2 *There exists a ring isomorphism between the quotient ring of the ideal of relation I_F and the ring of invariants, given that $k[x_1, .., x_n]^G = k[f_1, ..., f_n]$ and $I_F \subset k[y_1, ..., y_m]$:*

$$k[y_1, ..., y_m]/I_F \cong k[x_1, ..., x_n]^G.$$

The proof is provided on page 346 of [3]

The following properties will be crucial, as the elimination ideal, as defined below, will be the key to finding such relations.

Proposition 6.3 *If $k[x_1, ..., x_n]^G = k[f_1, ..., f_m]$ then the ideal defined as :*

$$J_F = \langle f_1 - y_1, ..., f_m - y_m \rangle \subset k[x_1, ..., x_n, y_1, ..., y_m].$$

1. *$I_F = J_F \cap k[y_1, ..., y_m]$, in other words, I_F is the n-th elimination ideal of J_F.*
2. *For a fixed monomial order in $k[x_1, ..., x_n, y_1, ..., y_m]$ where all monomial involving $x_1, ..., x_n$ are greater than any monomial only involving $y_1, ..., y_m$, where G is the Gröbner basis of J_F. Then $G \cap k[y_1, ..., y_m]$ would be a Gröbner basis for I_F for monomial orders in $k[y_1, ..., y_n]$.*

Proof. We will prove the relation between I_F and J_F, by focusing on the elements of J_F, $p \in k[x_1, ..., x_n, y_1, ..., y_m]$. To start, we claim:

$$p \in J_F \Leftrightarrow p(x_1, ..., x_n, f_1, ..., f_m) = 0 \, in \, k[x_1, ..., x_n]. \tag{6}$$

It is straight forward to prove that for $p \in J_F$ then $p(x_1, ..., x_n, f_1, ..., f_m) = 0$ as all elements of $J_F = \langle f_1 - y_1, ..., f_m - y_m \rangle$ go to zero under the substitution$y_i \rightarrow$

f_i. To prove both implications, we can make another substitution, $y_i \to f_i - (f_i - y_i)$, which gives us,

$$p(x_1, ..., x_n, y_1, ..., y_m) = p(x_1, ..., x_n, f_1, ..., f_m) + B_1 \cdot (f_1 - y_1) + ... + B_m \cdot (f_m - y_m) \tag{7}$$

where B_i is some element in $k[x_1, ..., x_n, y_i, ..., y_m]$, chosen to eliminate the difference in variables f_i and y_i. We stated that $p(x_1, ..., x_n, f_1, ..., f_m) = 0$ hence,

$$p(x_1, ..., x_n, y_1, ..., y_m) = +B_1 \cdot (f_1 - y_1) + ... + B_m \cdot (f_m - y_m) \in J_F. \tag{8}$$

The reason we know that $p(x_1, ..., x_n, y_1, ..., y_m) \in J_F$ is because J_F is an ideal of $k[x_1, ..., x_n, y_i, ..., y_m]$. Each of $f_i - y_i \in J_F$ and $B_i \in k[x_1, ..., x_n, y_i, ..., y_m]$.

To prove *1* we now intersect both sides of the previous equation with $k[y_1, ..., y_m]$ giving us:

$$p \in J_F \cap k[y_1, ..., y_m] \Leftrightarrow p(f_1, ..., f_m) = 0 \, in \, k[x_1, ..., x_n], \tag{9}$$

which in turn means $J_F \cap k[y_1, ..., y_m] = I_F$.

2 follows from the Elimination Theorem 4.18.

Definition 6.4 *Just as before $k[x_1, ..., x_n]^G = k[f_1, ..., f_m]$ and $I_F \subset k[y_1, ..., y_m]$ the ideal of relation for $F = (f_1, ..., f_n)$. Which gives us that the affine variety is defined below:*

$$V_F = \boldsymbol{V}(I_F) \subset k^m$$

Said affine variety has the following properties:

1. *There is no smaller variety then V_F in I_F, which also contains the parametrization:*

$$\begin{aligned} y_1 &= f_1(x_1, ..., x_n) \\ y_2 &= f_2(x_1, ..., x_n) \\ &\vdots \\ y_m &= f_m(x_1, ..., x_n) \end{aligned}$$

2. *$I_F = \boldsymbol{I}(V_F)$, meaning I_F consists of all polynomial functions which is zero over the entirety of V_F.*

3. *The variety V_F is irreducible.*

4. *Given the coordinate ring of the variety V_F defined as $k[V_F]$, then the following ring isomorphism exists:*

$$k[V_F] \cong k[x_1, ..., x_n]^G.$$

Proof. Recall that I_F is the n-th elimination ideal of $J_F = \langle f_i - y_i, ..., f_m - y_m \rangle$. Then *1* follows directly from the Polynomial Implicitization Theorem.

To prove *2* note that $I_F \subset \mathbf{I}(\mathbf{V}(I_F) = \mathbf{I}(V_F)$ always hold true. Hence we have to prove $\mathbf{I}(V_F) \subset I_F$. To do this take $h \in \mathbf{I}(V_F)$, and for any given point $(a_1, ..., a_n) \in k^n$, by *1* we know that:

$$(f_1(a_1, .., a_n), ..., f_m(a_1, ..., a_n)) \in V_F. \tag{10}$$

By the fact that h is zero on V_F, we get:

$$h(f_1(a_1, .., a_n), ..., f_m(a_1, ..., a_n)) = 0 \tag{11}$$

for all points $(a_1, ..., a_n) \in k^n$. As we are working in characteristic zero, so is k, hence k is also infinite. We know by Theorem **??** $h(f_1, ..., f_m) = 0$, hence $h \in I_F$ which in turn proves that $\mathbf{I}(V_F) \subset I_F$.

We know that $I_F = \mathbf{I}(V_F)$ is prime by Proposition 6.1, hence *3* since we proved that rime ideals are irreducible in Proposition **??**.

Too prove the isomorphism $k[V_F] \cong k[x_1, ..., x_n]^G$ we will use that:

$$k[V_F] \cong k[y_1, .., y_m]/\mathbf{I}(V_F), \tag{12}$$

which was established in the previous chapter. We also know by *2* that $I_F = \mathbf{I}(V_F)$ hence:

$$k[V_F] \cong k[y_1, .., y_m]/I_F \cong k[x_1, ..., x_n]^G \tag{13}$$

and *4* is proven.

Corollary 6.5 *Let $F = (f_1, ..., f_m)$ and $F' = (f'_1, ..., f'_m)$ where given $k[x_1, ..., x_n]^G = k[f_1, ..., f_m] = k[f'_1, ..., f'_m]$, then there is a isomorphism between the two varieties $V_F \subset k^m$ and $V'_F \subset k^{m'}$ defined by.*

Proof. By applying the previous proposition to both F and F' we get: $k[V_F] \cong k[x_1, ..., x_n]^G \cong k[V_{F'}]$.

Definition 6.6 *For a finite matrix group $G \subset GL(n, k)$, where $\boldsymbol{a}$ is an element of k^n, then the G-**orbit** of $\boldsymbol{a}$ is the set defined by:*

$$G \cdot \boldsymbol{a} = \{A \cdot \boldsymbol{a} : A \in G\}.$$

*We call the set of all G-orbits in k^n the **orbit space**, and we denote it as $k^n b/G$.*

Example 6.7 *Take the example from the last section. The finite matrix group generated by:*

$$A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \in GL(2,k).$$

We want to see the algebraic relation of the generators:

$$x^2 + y^2 - xy,\ x^2y - xy^2,\ -x^3 + 3x^2y - y^3$$

Set:

$$t = x^2 + y^2 - xy$$

$$u = x^2y - xy^2$$

$$v = -x^3 + 3x^2y - y^3$$

To do this we will use Proposition 6.3, first set:

$$J = \langle t - (x^2 + y^2 - xy), u - (x^2y - xy^2), v - (-x^3 + 3x^2y - y^3) \rangle \subset k[x, y, t, u, v]$$

We will now use Sage Math to find the Gröbner basis G and then find $G \cap k[t, u, v]$ using the following code.

```
R.<x,y,t,u,v> = QQ['x,y,t,u,v']
K.<t,u,v>= QQ['t,u,v']
J = ideal(t-(x^2+y^2-x*y), u-(x^2*y-x*y^2), v-(-x^3+3*x^2*y-y^3))
C = J.groebner_basis()

lis=[]
for c in C:
    if c in K:
        lis.append(c)
```

The resources to write this code are found on [8]

We find that the generators satisfy the folowing:

$$t^3 - 9u^2 + 3tv - v^2 = 0$$

This gives us the algebraic relation between the generators. We can now use Proposition 6.2, to write the ring of invariants as:

$$k[x, y]^{C_3} = k[t, u, v]/\langle t^3 - 9u^2 + 3tv - v^2 \rangle$$

I want to thank Jonas Bergström who helped me a huge amount, I would not have been able to do this without him. I have used ChatGPT to find errors in my code and writing, and at times help me correct them this includes grammatical errors and the use with the aim for more professional language.

References

[1] https://en.wikipedia.org/wiki/Tuple

[2] Dummit and Foote, *Abstract Algebra*

[3] David Cox, Jhon Little, Donald O'Shea Ideals, Varieties and Algorithms, 3rd eddition

[4] https://math.libretexts.org/Bookshelves/

[5] David Eisenbud Commutativ Algebra

[6] Pierre Antoine Grillet Abstract Algebra Second Edition

[7] Representation Theory William Fulton Joe Harris

[8] https://doc.sagemath.org/html/en/reference/polynomial_rings/sage/rings/polynomial/multi_polynomial_ideal.html
`https://doc.sagemath.org/html/en/tutorial/tour_polynomial.html`

[9] https://ask.sagemath.org/question/32932/how-to-implement-the-multivariable-division-algorithm-without-passing-to-grobner-bases/