INVARIANT THEORY AND ALGORITHMS

KISHAN JANI

Abstract. Invariant theory deals with finding quantities that remained unchanged due to certain group actions or transformations. In this expository paper, we lay emphasis on studying invariant theory from an algebraic point of view, focusing on the action of subgroups of $\mathrm{GL}_n(k)$ and $\mathrm{SL}_n(k)$ on polynomial rings. We will also prove the finite generation of invariant rings under action by a special type of $\mathrm{GL}_n(k)$ subgroup (namely linearly reductive groups) and also derive a significant bound on the degree of invariant polynomials. Stemming from this discussion, we will also present algorithmic approaches to the problem of finding the fundamental invariants of a ring under a given group action. Lastly, we will discuss applications of these algorithms in finding invariants of the dihedral group D_n and finding self-dual codes in coding theory. The paper assumes the knowledge of group and ring theory, linear algebra and some elementary calculus related to taylor expansions.

1. Introduction

Definition 1.1. For a group G and a set X, a **group action**, more specifically a left-group action, is defined as a function $\varphi : G \times X \to X$ such that

(1) $\varphi(e_G, x) = x$ where e_G is the identity of the group and $x \in X$
(2) $\varphi(g_1g_2, x) = \varphi((g_1, \varphi(g_2x)))$ for $g_1, g_2 \in G$

For the sake of brevity, if the left-group action is known, the notation $\varphi = \cdot$ is often used, simplifying the group action axioms to $e_G \cdot x = x$ and $(g_1g_2) \cdot x = g_1(g_2 \cdot x)$. Let us look at some examples of group actions.

Example 1.1. Let us consider the group action of $G_n = \{1, \omega, \omega^2, \ \ldots, \omega^n\}$, the multiplicative group of n^{th} roots of unity, on $\mathbb{C}$. The element $\omega^k \in G_n$ acts on a complex number $z \in \mathbb{C}$ by rotating it $2k\pi/n$ radians in the counter-clockwise direction.

Example 1.2. The special linear group $SL_2(\mathbb{C})$ acts on polynomials in $\mathbb{C}[x, y]$ by imposing the following linear transformation

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix} \text{ for } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{C})$$

A natural and interesting question that can be asked is about quantities that do not change after a group action. This question forms the basis for invariant theory, which analyzes such quantities called invariants.

Definition 1.2. Formally stated, an **invariant** is a quantity that does not change under a group action, that is for a group action φ, a quantity f would be invariant if $\varphi \circ f = f$.

The notion of an invariant is actually quite common in many fields of mathematics, and can be extended to any form of transformation in general. For example, if we consider the transformation of coordinates $P(x, y)$ by the rotation matrix R_θ, defined as

$$\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} x' \\ y' \end{pmatrix}$$

Then if we look at the distance between P and the origin O before and after the transformation,

$$\mathrm{dist}(P, O) = \sqrt{(x - 0)^2 + (y - 0)^2} = \sqrt{x^2 + y^2}$$

$$\begin{aligned}\mathrm{dist}(P', O') &= \sqrt{(x'-0)^2+(y'-0)^2} = \sqrt{(x\cos\theta - y\sin\theta)^2 + (x\sin\theta + y\cos\theta)^2} \\ &= \sqrt{x^2\cos^2\theta + y^2\sin^2\theta - 2xy\cos\theta\sin\theta + x^2\sin^2\theta + y^2\cos^2\theta + 2xy\cos\theta\sin\theta} \\ &= \sqrt{x^2+y^2} = \mathrm{dist}(P, O)\end{aligned}$$

Thus, the distance from the origin before and after the rotation is the same, and so we say that distance from the origin is an invariant under the given transformation. Additionally, since distance does not change under translation, we show that distance between any two points is invariant under rotation.

This paper will explore invariants from an algebraic perspective, and so our focus will be restricted to polynomials that remain invariant under certain specific group actions, namely those by the general linear and special linear groups. The following example shows one such invariance:

Example 1.3. Consider an action on the polynomial ring $\mathbb{C}[x, y]$ by the group

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\} \subset \mathrm{SL}_2(\mathbb{C})$$

For $f(x, y) \in \mathbb{C}[x, y]$, these four matrices correspond to the following actions: for post-transformation coordinates (x', y'), $f(x', y') = f(x, y)$, $f(x', y') = f(-x, -y)$, $f(x', y') = f(y, -x)$, and $f(x', y') = f(-y, x)$. Then, since an invariant polynomial must have $\varphi(f(x, y)) = f(x', y') = f(x, y)$, it must satisfy the following:

$$f(x, y) = f(-x, -y), \quad f(x, y) = f(-y, x), \quad f(x, y) = f(-x, y)$$

Multiple polynomials $p_i(x, y) \in \mathbb{C}[x, y]$ invariant under this group action can be found; for instance, consider the following:

(1) $p_1(x, y) = x^2 + y^2 + x^2y^2$
(2) $p_2(x, y) = \pi x^2y^2(x^2 + y^2) + 15$
(3) $p_3(x, y) = 2xy^3 - 2yx^3 + 5x^2y^2$

A natural yet non-trivial result that stems from the definition of such invariant polynomials is that for two such polynomials f_1 and f_2, $f_1 + f_2$ and f_1f_2 would also be invariant. A direct implication of this additive and multiplicative closure is the possibility that the set of all invariant polynomials under a certain group action is a ring. This is in fact true and can be easily verified.

2. Classical Invariant Theory

Definition 2.1. For $G \subset \mathrm{GL}_n(k)$, a polynomial $f \in k[\mathbf{x}] = k[x_1, x_2, \ldots, x_n]$ is **G-invariant** if $g \circ f = f$ for all $g \in G$. Furthermore, the set of G-invariants forms a sub algebra of $k[\mathbf{x}]$, more particularly a **ring of G-invariants** denoted by

$$k[\mathbf{x}]^G = \{f(x_1, x_2, x_3, \ldots x_n) : f \in k[\mathbf{x}],\ g \circ f = f\ \forall\, g \in G\}$$

Example 2.1. It so happens that in the case of **Example 0.3**, we are able to generate the complete ring of invariants $k[x, y]^G$ using three polynomials $f_1 = x^2 + y^2$, $f_2 = x^2y^2$, and $f_3 = x^3y - y^3x$. So then we have that

$$\mathbb{C}[x, y]^G \cong \mathbb{C}[x^2 + y^2, x^2y^2, xy^3 - yx^3]$$

Example 2.2. Consider the finite group G generated by

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}$$

where $\omega = e^{\frac{2\pi i}{3}}$ is a cube root of unity, so $\omega^3 = 1$. Then we have the group $H = \{\mathbb{I}, A, A^2\} \subset \mathrm{SL}_2\mathbb{C}$. For H acting on $\mathbb{C}[x, y, z]$, we have the following transformations on a polynomial p:

$$f(x, y, z) = f(x, y, z), \quad f(x, y, z) = f(x, \omega y, \omega^2 z), \quad f(x, y, z) = f(x, \omega^2 y, \omega z)$$

In this case, our invariant ring is finitely generated and obeys the following isomorphism,

$$\mathbb{C}[\mathbf{x}]^H \cong \mathbb{C}[x, y^3, z^3, yz]$$

In both examples, we encountered finite $\mathrm{SL}_n(k)$ subgroups whose actions upon the ring $\mathbb{C}[\mathbf{x}]$ produced finitely generated rings of invariants. One of the most celebrated results of invariant theory is Hilbert's Finiteness theorem, which states that for actions by linearly reductive groups, the ring of invariants can always be generated by a finite set of invariants.

Definition 2.2. If we have $k[\mathbf{x}]^G \cong k[I_1, I_2, \ldots, I_n]$ then the invariants $I_1, I_2, \ldots, I_n$ are called the **fundamental invariants** of the ring and a relation between these invariants is called a **syzygy**.

Example 2.3. Once again, alluding to **Example 0.3**, the fundamental invariants are $I_1 = x^2 + y^2$, $I_2 = x^2y^2$, and $I_3 = xy^3 - yx^3$. Additionally,

$$(xy^3 - yx^3)^2 = x^6y^2 + y^6x^2 - 2x^4y^2 = x^2y^2(x^4 + y^4) - 2x^2y^2 = x^2y^2\left[(x^2 + y^2)^2 - 2x^2y^2\right] - 2x^4y^4$$

So we have the syzygy

$$I_3^2 = I_2(I_1^2 - 2I_2) - 2I_2^2 = I_2I_1^2 - 4I_2^2$$

The study of invariants under $\mathrm{GL}_n(\mathbb{C})$ group actions on binary forms was of particular interest in 19th century research in the topic. One of the primary reasons for this was that the invariant quantities that are determined for quadratic forms are invariant under any finite or infinite subgroup of $\mathrm{GL}_2(\mathbb{C})$.

Definition 2.3. A polynomial $p(\mathbf{x})$ of degree d is **homogeneous** if all its terms have the same degree. One of the interesting properties that result from this definition is that $p(a\mathbf{x}) = a^d p(\mathbf{x})$ for a constant a.

Definition 2.4. A **binary form** of degree d is a homogeneous polynomial in x and y of the form

$$\sum_{i=0}^{d} \binom{d}{i} a_i x^{d-i} y^i = a_0 x^d + \binom{d}{1} a_1 x^{d-1} y + \ldots a_{d-1} \binom{d}{d-1} x y^{d-1} + a_d y^d$$

for $a_1, a_2, \ldots a_d \in k$, generally taken to be $\mathbb{C}$ in this paper.

Example 2.4. The binary quadratic form is given by $p(x, y) = a_0x^2 + 2a_1xy + a_2y^2$ for $p \in \mathbb{C}[x, y]$.

Under $\mathrm{SL}_2(\mathbb{C})$ group action on the binary form, it can be shown, through rather exhaustive algebra, that under such a group action, the determinant $\Delta_2 = a_1^2 - a_0a_2$ is an invariant.
Note that the discriminant is a polynomial in the coefficients of $p(x, y)$. Invariants of binary forms under $\mathrm{SL}_2(\mathbb{C})$ group actions are traditionally polynomials in the coefficients of the original binary form.

Definition 2.5. For the linear action by matrices $A \in \mathrm{GL}_2(\mathbb{C})$ on $\mathbb{C}[X]$, binary forms transform in the following way

$$\sum_{i=0}^{d} \binom{d}{i} a_i x^{d-i} y^i = \sum_{i=0}^{d} \binom{d}{i} a'_i x^{d-i} y^i$$

where $a_i, a'_i \in \mathbb{C}$. A polynomial $I \in \mathbb{C}[a_0, a_1, a_2, a_3, \,.\,.\,, a_n]$ is the **invariant of a binary form** if

$$I(a_0, a_1, a_2, a_3, \,.\,.\,, a_d) = (\det A)^g I(a'_0, a'_1, a'_2, a'_3, \,.\,.\,, a'_d)$$

with the ring of all invariants defined as $\mathbb{C}[X_d]$. g is called the **index** or weight of the invariant. Naturally, in the case of $\mathrm{SL}_n(\mathbb{C})$ groups, the index of the invariant is zero.

Example 2.5. In the case of the invariant ring for binary quadratic forms $\mathbb{C}[X_2] \cong C[\Delta_2]$, for an arbitrary $\mathrm{GL}_2(\mathbb{C})$ action defined by

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x' \\ y' \end{pmatrix} \text{ for } A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

that $\Delta_2' = (\det A)^2 \Delta_2$ i.e, the discriminant has index 2.

Definition 2.6. Another useful notion when considering invariants of binary forms is the covariant. A polynomial $\mathcal{F} \in \mathbb{C}[a_0, a_1, a_2, a_3, .., a_d, x, y]$ is **covariant** if for the linear action of all $A \in \mathrm{GL}_2(\mathbb{C})$,

$$\mathcal{F}(a_0, a_1, a_2, a_3, \ .., a_d, x, y) = (\det A)^g \mathcal{F}(a_0', a_1', a_2', a_3', \ .., a_d', x, y)$$

The task of calculating all such invariants and covariants quickly becomes arduous and complex task. For example, the two fundamental invariants of the binary quartic

$$p_4(x, y) = a_0 x^4 + 4a_1 x^3 y + 6a_2 x^2 y^2 + 4a_3 x y^3 + a_4 y^4$$

are the following

$$f_1 = a_0 a_4 - 4a_1 a_3 + 3a_2^2, \quad f_2 = a_0 a_2 a_4 - a_0 a_3^2 - a_1^2 a_4 - a_2^3 + 2a_1 a_2 a_3$$

Interestingly, the latter can be represented as

$$f_2 = \det \begin{pmatrix} a_0 & a_1 & a_2 \\ a_1 & a_2 & a_3 \\ a_2 & a_3 & a_4 \end{pmatrix}$$

This particular quantity is known as the **catalecticant**. One can form the catalecticant of a $2n$ binary form in a similar way by shifting a_i to the right by one after each row for an $(n+1) \times (n+1)$ matrix. The catalecticant of the coefficients of a binary form gives an invariant; a proof for this can be found in [Lor18].

Modern computational tools have allowed the computation of fundamental invariants for binary forms upto degree $d = 10$. These invariants can be found in [PD14] along with an efficient computational method.

The computation of invariants in $\mathbb{C}[\mathbf{x}]$ motivates more general theorems about the structure of the invariant ring. One of the key questions posed by invariant theory in the nineteenth century was that about the finiteness of the set of generators: does an invariant ring $\mathbb{C}[\mathbf{x}]^G$ exist for all kinds of groups? If not, for what kinds of groups does it exist? Gordan managed to prove finiteness for the specific case of binary forms under $\mathrm{SL}_2(\mathbb{C})$ group actions. However, his method, while constructive, could not be extended beyond the $\mathrm{SL}_2(\mathbb{C})$ group. A proof for this theorem using bracket functions can be found in [KR84]. Hilbert's 1890 and 1893 papers extended Gordan's result to linearly reductive groups through a novel method.

3. Some Representation Theory

One of the key restrictions of Hilbert's Finiteness Theorem is the linear reductivity of the group causing a specific group action. A justification for this restriction and the proof of the theorem in general requires the motivation of an alternate representation-theoretic characterization of $\mathbb{C}[\mathbf{x}]^G$ in terms of vector spaces. Consequently, we first introduce the necessary tools required for creating this new definition.

Definition 3.1. A **representation** of a group G is the homomorphism $\varphi : G \longrightarrow \mathrm{GL}(V)$ where V is a vector space. The dimension $\dim(V) = n$ of the vector space is the cardinality of the basis vectors, enabling us to express the group action of G as an $n \times n$ matrix transformation. For our purposes, we assume that $\dim(n) < \infty$. Another equivalent definition that is often used defines the representation of G as the group action of G on the vector space V, namely $\phi : G \times V \longrightarrow V$.

Definition 3.2. A **subrepresentation** W of V is a G-invariant subspace of V, that is to say

$$W = \{w : g \circ w \in W \ \forall \ g \in G\}$$

Definition 3.3. This definition can be extended to define a representation-theoretic generalization of our polynomial ring; for a vector space V over k and a group G, $k[V]$ denotes the **k-algebra of polynomial functions** $f(\mathbf{x})$ on V. Furthermore, we then call $f \in k[V]$ **G-invariant** if $g \circ f = f$ for all $g \in G$. The set of G-invariants forms a sub-algebra $k[V]^G$, defined as

$$k[V]^G = \{f \in k[V] : g \circ f = f \, \forall \, g \in G\}$$

Definition 3.4. A representation is called **irreducible** if it has no subrepresentations except the trivial subrepresentations 0 and V. It is reducible otherwise. Additionally, a representation is called **completely reducible** if it can be expressed as the direct sum of irreducible subrepresentations. A group is called **linearly reductive** if it has completely reducible finite-dimensional representations.

Equipped with this background, we can provide a brief explanation of why we require the condition of linear reductivity. Hilbert's original proof and the proof mentioned here, both involving defining an equivariant map $\rho_G : k[V] \longrightarrow k[V]^G$, called the Reynolds operator. For such a map to be defined, we require that every finite-dimensional representations of G is completely reducible, which then forces the group to be linearly reductive. For a more detailed and rigorous explanation of the condition of linear reductivity, we refer the reader to [KP], [Mil12].

4. The Reynolds operator

As mentioned in the previous section, our proof hinges on defining a map $\rho_G : k[V] \longrightarrow k[V]^G$, which is called the Reynolds operator. In this section, we prove a few basic properties of this operator. It is much more convenient to work with the non-representation theoretic definition of the invariant ring, and so it has been used here.

Definition 4.1. The **Reynolds operator** $\rho_G(f)$ for a group G acting on a set X with $f \in X$ is defined as

$$\rho_G : f \longmapsto \frac{1}{|G|} \sum_{g \in G} g \circ f$$

In the case of actions by matrix subgroups G of $GL_n(\mathbb{C})$ on the polynomial $k[\mathbf{x}]$, $\rho_G(f)$ for $f(\mathbf{x}) \in k[\mathbf{x}]$ is defined by the map

$$\rho_G : f \longmapsto \frac{1}{|G|} \sum_{A \in G} f(A \cdot \mathbf{x})$$

It then follows that in the case of action by matrix subgroups, the Reynolds operator preserves the degree of polynomial since it only imposes a linear transformation of the variables.

Intuitively, one can consider the Reynolds operator as a form of average of the action of G on f. As a result of this averaging action, it turns out that this operator has a form of absorption property with respect to the ring of invariants: the Reynolds operator applied to any element f returns an element of the invariant ring. This property becomes extremely useful when it comes to the computation of fundamental invariants as it gives us a method of generating invariants from a given base of polynomials. We will develop this method in an algorithmic way in Section 6. It is also important to note that this averaging effect of $\rho_G(f)$ imposes a significant restriction upon our choice of the underlying field: since we are dividing by $|G|$, we must have that $\text{char}(k) = 0$. For our purposes, we will assume this to be the case.

Proposition 1 (Absorption Property). *Let $\rho_G(f)$ be the Reynolds operator.*

(1) *For a polynomial ring $k[\mathbf{x}]$ and its invariant ring $k[\mathbf{x}]^G$, $\rho_G(f)$ maps $k[\mathbf{x}]$ to $k[\mathbf{x}]^G$*
(2) *If $f \in k[\mathbf{x}]^G$, then $\rho_G(f) = f$.*

(3) *For $f_0 \in k[\mathbf{x}]^G$ and $f \in k[x]$, $\rho_G(ff_0) = f_0\rho_G(f)$*

Proof. Suppose we have $f \in k[\mathbf{x}]$ and $B \in G$. Then

$$\rho_G(f)(B \cdot \mathbf{x}) = \frac{1}{|G|}\sum_{A\in G} f(B \cdot A \cdot \mathbf{x}) = \frac{1}{|G|}\sum_{BA\in G} f(BA \cdot \mathbf{x})$$

Now for $A_1, A_2 \in G$, suppose $BA_1 = BA_2$, then since $B \in G \subset GL_n(\mathbb{C})$, we can multiply both sides by B^{-1} to get that $A_1 = A_2$. This means that the product $BA \in G$ always maps to a unique element in G. But then since A covers the length of G and since G is finite, we must have $|G|$ distinct matrices BA, and so BA also covers the entire group. Then we have that

$$\frac{1}{|G|}\sum_{BA\in G} f(BA \cdot \mathbf{x}) = \rho_G(f)(\mathbf{x})$$

and so $\rho_G(f)(B \cdot \mathbf{x}) = \rho_G(f)(\mathbf{x})$, which means ρ_G maps f to an invariant polynomial. So then we get the map $\rho_G(f) : k[\mathbf{x}] \longrightarrow k[\mathbf{x}]^G$. We have proved the result only for $\mathrm{GL}_2(\mathbb{C})$ matrices; the general proof is very similar to this, and can be found in [Dan17].

For (2), suppose $f \in k]\mathbf{x}]^G$. Then

$$\rho_G(f) = \frac{1}{|G|}\sum_{g\in G} g \circ f(\mathbf{x}) = \frac{1}{|G|}\sum_{g\in G} f(\mathbf{x}) = f(\mathbf{x})$$

This also implies that $\rho_G \circ \rho_G(f) = \rho_G(f)$ since $\rho_G(f) \in k[V]^G$, which means that the operator ρ_G is idempotent in this case.

Now for (3), since f_0 is invariant, we have $g \circ f_0 = f_0$. Then

$$\rho_G(ff_0) = \frac{1}{|G|}\sum_{g\in G} g \circ [ff_0(\mathbf{x})] = \frac{1}{|G|}\sum_{g\in G}(g \circ f(\mathbf{x})) \cdot (g \circ f_0(\mathbf{x})) = f_0 \cdot \frac{1}{|G|}\sum_{g\in G} g \circ f(\mathbf{x}) = f_0\rho_G(f)$$

□

5. Finiteness and Degree Bounds

In this section, we focus on proving Hilbert's finiteness theorem and other related results about the finite-generation of the $k[V]^G$.

Theorem 1 (Hilbert 1890)**.** *If G is linearly reductive, then $k[V]^G$ is a finitely generated ring.*

Before beginning the proof for this theorem, we first need to prove Hilbert's Basis Theorem, which by its own is a crucial result in ring theory.

Theorem 2 (Hilbert Basis Theorem)**.** *If R is noetherian, the $R[\mathbf{x}] = R[x_1, x_2, \ldots x_n]$ is noetherian.*

Proof of Hilbert Basis Theorem. It is sufficient to prove that if R is noetherian then $R[x]$ is noetherian, since our argument can then be extended by induction on n for $R[\mathbf{x}]$.

Let $I \subset R[x]$ be an ideal. We will construct a finite generating set for I. Let f_1 be the non-zero polynomial of least degree in I. Next, for $i \geq 1$, we recursively define functions f_{i+1} as follows: f_{i+1} is the polynomial of least degree in $I \,/\, (f_1, f_2, \ldots f_i)$. The sequence terminates when $I = (f_1, f_2, \ldots f_n)$. We claim that I is finitely generated, so $I = (f_1, f_2, \ldots f_n)$ for some $n \in \mathbb{N}$.
Aiming for a contradiction, suppose this recursive process leads to an infinite set of polynomials $(f_1, f_2, \ldots)$. Let a_i denote the leading coefficient of polynomial f_i and let J be the ideal in R defined as $J = (a_1, a_2, \ldots)$. Since R is noetherian, J must be a finitely generated ideal and so $J = (a_1, a_2, \ldots a_m)$ for $m \in \mathbb{N}$. So then we can have an element $a_{m+1} = \sum_{i=1}^{m} r_i a_i$ for $r_i \in R$. It

follows from our construction that f_{m+1} will have degree greater than or equal to f_i for $1 \leq i \leq m$. Consider the polynomial

$$g := \sum_{j=1}^{m} r_j f_j x^{\deg f_{m+1} - \deg f_j}$$

It follows from this definition that $g \in (f_1, f_2, \ldots f_m)$ and that g has the same leading coefficient and degree as f_{m+1}. Then $f_{m+1} - g \notin (f_1, f_2, \ldots f_m)$ but it has a degree less than that of f_{m+1}. This raises a contradiction, since we chose f_{m+1} to be the polynomial of least degree not in $(f_1, f_2, \ldots f_n)$. So then we cannot have an infinitely generated ideal of $R[x]$, and further we can say that $R[x]$ is noetherian. □

Now we can provide a satsifactory albeit nonconstructive proof of the Finiteness theorem:

Proof of Hilbert's Finiteness Theorem. Let $\mathfrak{m}$ be the ideal of $k[V]$ generated by all invariant homogeneous polynomials of degree $d > 0$. Let V be a finite dimensional vector space. Since $k[V]$ is noetherian, by the Hilbert Basis Theorem, $\mathfrak{m}$ is finitely generated by a set of invariant homogeneous elements, say $\{f_1, f_2, f_3, \ \ldots f_n\}$. We will prove that $k[V]^G = k[f_1, f_2, f_3, \ldots, f_n]$.

The $\supseteq$ inclusion is obvious since the invariant ring consists of the set of invariant homogeneous generators and also non-homogeneous invariants if they exist.
For the $\subseteq$ inclusion, suppose $f \in k[V]^G$. We will prove by induction on $d = \deg(f)$ that $f \in k[f_1, f_2, f_3, \ldots, f_n]$. The base case for $d = 0$ is trivial. If $d > 0$, then we have that $f \in \mathfrak{m}$ and so it can be expressed as

$$f = \sum_{i=1}^{n} \alpha_i f_i \text{ for } \alpha_i \in k[V]$$

Now we apply the Reynolds operator $\rho_G(f) : k[V] \longrightarrow k[V]^G$ on both sides of the equation(Note that due to this map, we must have G a linearly reductive group and $\operatorname{char}(k) = 0$):

$$\rho_G(f) = \sum_{i=1}^{n} \rho_G(a_i f_i)$$

But since $f, f_i \in k[V]^G$, we get

$$f = \sum_{i=1}^{n} f_i \rho_G(a_i)$$

Clearly, $\rho_G(a_i) \in k[V]^G$ has to be a homogeneous invariant, which will have degree $\deg[\rho_G(a_i)] = \deg(f) - \deg(f_i) < \deg(f)$. Now since $\deg[\rho_G(a_i)] < \deg(f)$, we can conclude under our induction hypothesis that $\rho_G(a_i) \in k[f_1, f_2, f_3, \ldots, f_n]$. But then we can reinterpret f as

$$f = \sum_{i=1}^{n} f_i \rho_G(a_i) \in k[f_1, f_2, f_3, \ldots, f_n] \text{ since } \rho_G(a_i) \in k[f_1, f_2, f_3, \ldots, f_n]$$

So then our second forward inclusion holds, and $k[V]^G = k[f_1, f_2, f_3, \ldots, f_n]$. Thus, $k[V]^G$ is finitely generated. □

Theorem 3 (Noether 1916). *If G is a finite matrix subgroup of $GL_n(k)$, then*

$$k[\mathbf{x}]^G = k\left[\rho_G(\prod_{i=1}^{n} x_i^{k_i}) : k_i \geq 0, \ \ \sum_{i=1}^{n} k_i \leq |G|\right]$$

that is to say that the degree of the fundamental invariants is limited by the order of the group.

Proof. For the sake of brevity, let $X^d \equiv \prod_{i=1}^n x_i^{k_i}$ where $k_1 + k_2 + \ldots k_n = d$ denote a monomial in $k[\mathbf{x}]$ of degree d in n different variables. Let $f = \sum_{d=1}^N c_d X^d \in k[\mathbf{x}]^G$ be an invariant, where $c_d \in k$. Then since $\rho_G(f) = f$,

$$f = \rho_G(f) = \rho_G\left(\sum_{d=1}^N c_d X^d\right) = \sum_{d=1}^N c_d \rho_G(X^d)$$

and so every invariant is a linear combination of $\rho_G(X^d)$ over k. So then our approach will be to instead prove that $\rho_G(X^d)$ is a polynomial in $\rho_G(X^\beta)$ for all d where $|\beta| \leq |G|$. First let us analyze $\rho_G(X^d)$:

$$\rho_G(X^d) = \frac{1}{|G|}\sum_{A \in G}(A \cdot \mathbf{x})^d \tag{1}$$

where $(A \cdot \mathbf{x})^d$ represents the represents our monomial X^d after transformation, which stated explicitly gives

$$(A \cdot \mathbf{x})^d = \prod_{i=1}^n (A_i \cdot \mathbf{x})^{k_i}$$

where A_i denotes the ith row of matrix A. Now consider the expansion of $(y_1 A_1 \cdot \mathbf{x} + y_2 A_2 \cdot \mathbf{x} \ldots + y_n A_n \mathbf{x})^d$ so that by the multinomial theorem we get on the right hand side

$$(y_1 A_1 \cdot \mathbf{x} + y_2 A_2 \cdot \mathbf{x} \ldots + y_n A_n \mathbf{x})^d = \sum_{k_1 + \ldots + k_n = d} \frac{d!}{k_1! k_2! \ldots k_n!}(A \cdot \mathbf{x})^d Y^d$$

For the sake of brevity, Let $\binom{d}{k_i}$ denote the multinomial coefficient. Summing both sides over all possible $A \in G$,

$$\sum_{A \in G}(y_1 A_1 \cdot \mathbf{x} + y_2 A_2 \cdot \mathbf{x} \ldots + y_n A_n \mathbf{x})^d = \sum_{A \in G}\left(\sum_{k_1 + \ldots + k_n = d}\binom{d}{k_i}(A \cdot \mathbf{x})^d Y^d\right) \tag{2}$$

$$= \sum_{k_1 + \ldots + k_n = d}\binom{d}{k_i} Y^d \Big(\sum_{A \in G}(A \cdot \mathbf{x})^d\Big) = \sum_{k_1 + \ldots + k_n = d}\binom{d}{k_i} \cdot Y^d \cdot |G| \cdot \rho_G(X^d) \quad \text{(From (1))} \tag{3}$$

Before progressing further, we first assert the following lemma about symmetric polynomials

Lemma 1. *For a field k, every symmetric polynomial in $k[\mathbf{x}]$ can be written as a polynomial in $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3, \ldots \mathcal{P}_n$, where $\mathcal{P}_k = x_1^k + x_2^k + \ldots x_n^k$ is called a power sum.*

Proof. The proof of this lemma is rather involved and requires a substantial background in the theory of symmetric functions. A proof of this lemma using Newton's Identities has been motivated in [CLO97]. We provide a brief outline of this proof. Newton's identities relate power sums defined above and the elementary symmetric functions $e_k = \sum_{1 \leq j_i \leq n} x_{j_1} x_{j_2} \ldots x_{j_n}$:

$$\sum_{j=0}^k (-1)^j j \mathcal{P}_{k-j} e_j = 0 \text{ for } 1 \leq k \leq n$$

$$\sum_{j=0}^n (-1)^j \mathcal{P}_{k-j} e_j \text{ for } k > n$$

Then it can be shown by induction that e_j can be expressed as a polynomial in $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3, \ldots \mathcal{P}_n$. Then since any symmetric polynomial can be expressed as a polynomial in elementary symmetric functions, we get the lemma. We refer the reader to Kieth Conrad's Notes on Symmetric Functions [Con] to obtain the necessary background required for this proof.

We use Lemma 2. on the left hand side of (2) in the following way: let $\mathcal{Y}_A \equiv y_1 A_1 \cdot \mathbf{x} + y_2 A_2 \cdot \mathbf{x} \ldots + y_n A_n \mathbf{x}$. Then we get on the left hand side of (2) $\sum_{A \in G} \mathcal{Y}_A^d$, which is the dth power sum of $\mathcal{Y}_A$ over a total of $|G|$ such elements, and so a symmetric polynomial. But now we can apply Lemma 2. over our $|G|$ objects. Since we have that $\mathcal{Y}_A^d$ as a symmetric function in $\mathcal{S} = \{A : A \in G\}$ with $|\mathcal{S}| = |G|$,it can be expressed as a polynomial in the power sums $Q(\mathcal{P}_1,\ \mathcal{P}_2,\ \ldots \mathcal{P}_{|G|})$ by Lemma 2. Combining this with (3), we get

$$\sum_{k_1 + . . + k_n = d} \binom{d}{k_i} \cdot Y^d \cdot |G| \cdot \rho_G(X^d) = Q(\mathcal{P}_1,\ \mathcal{P}_2,\ \ldots \mathcal{P}_{|G|}) \tag{4}$$

Now in the polynomial $Q(\mathcal{P}_1,\ \mathcal{P}_2,\ \ldots \mathcal{P}_{|G|})$, each $\mathcal{P}_\beta$ where $\beta \leq |G|$ can be written as:

$$\mathcal{P}_\beta = \sum_{k_1 + . . + k_n = \beta} \binom{\beta}{k_i} \cdot Y^\beta \cdot |G| \cdot \rho_G(X^\beta) = q(Y^\beta,\ \rho_G(X^\beta))$$

for some polynomial q. Then we essentially have Q as a polynomial in Y^β and $\rho_G(X^\beta)$. Then if we look at (4) again,

$$\sum_{k_1 + . . + k_n = d} \binom{d}{k_i} \cdot Y^d \cdot |G| \cdot \rho_G(X^d) = Q\Big[q\big(Y^1,\ \rho_G(X^1)\big), q\big(Y^2,\ \rho_G(X^2)\big), \ldots q\big(Y^{|G|},\ \rho_G(X^{|G|})\big)\Big]$$

Now, if we equate the coefficients of Y^n, we finally get that

$$\binom{d}{k_i} \cdot |G| \cdot \rho_G(X^d) = q'(\rho(X^\beta)) \text{ for some } \beta \leq |G| \text{ and some polynomial } q'$$

In our char$(k) = 0$, the coefficient of $\rho_G(X^d)$ is non zero, and we have $\rho_G(X^d)$ as a polynomial in $\rho(X^\beta)$. □

This theorem is an extremely crucial result as it not only provides a bound for the degree of fundamental invariants under finite $\mathrm{GL}_n(k)$ action, but it also suggests an algorithmic approach that can be used to find the set of fundamental invariants. This approach will be discussed in section 6.

Hilbert's Finiteness Theorem is an extremely powerful result that limits the finite generation of invariaints only on the basis of linear reductivity of a group, which stems from our use of the Reynolds operator. Hilbert provided another proof in 1893 using the Cayley Ω-operator and the nullcone $\mathcal{N}_0$ which was constructive and algorithmic in nature and can be found in [Hil93]. This proof was a groundbreaking achievement in Invariaint theory since it provided a pathway to generate the fundamental invariants of any linearly reductive group. One can find this proof, along with the aforementioned algorithm, in [Stu08]. It is then a natural to ask whether there is some way to extend this result to all group actions. This was Hilbert's 14th problem.

Question 5.1 (Hilbert's 14th Problem)**.** Is the ring of invariants $\mathbb{C}[\mathbf{x}]^G$ always finitely generated for $G \subset \mathrm{GL}_n(\mathbb{C})$?

This question remained unsolved for many years until Nagata managed to produce a counterexample in 1959, which can be found in [Nag59].

6. Computational Aspects of Invariant Theory

As mentioned in the previous section, one of the most important corollaries to the constructive proofs for finiteness in Section 5 is that they produce the scope of generating algorithms to compute fundamental invariants. In this section, we will discuss some algorithms pertaining to invariants under finite group actions.

Recall Theorem 3. in Section 5, which states that the ring of invariants $k[\mathbf{x}]^G$ can be generated by $\rho_G(\prod_{i=1}^n x_i^{k_i})$ for $k_i \geq 0$ and degree of monomial less than $|G|$. This means that the ring of invariants for action by finite $G \subset GL_2(\mathbb{C})$ can be determined by applying the Reynolds operator to all monomials with degree $\beta \leq |G|$. This gives us our first algorithm:

Algorithm 6.1. (Generating $\mathbb{C}[\mathbf{x}]^G$ using Reynolds operator) We can generate the fundamental invariants of the invariant ring $\mathbb{C}[\mathbf{x}]^G$ for finite subgroups $G \subset \mathrm{GL}_n(\mathbb{C})$ using the Reynolds operator $\rho_G(\prod x_i^{k_i})$ for $k_1 + k_2 + \ldots + k_n \leq |G|$.

Suppose we are looking for all monomials f such that $\deg(f) = \beta \leq |G|$. Then $k_1 + k_2 + \ldots k_n = \beta$ for $k_i \geq 0$. Then the total number of possible monomials in this particular case becomes $\binom{\beta+n-1}{n-1}$. $\deg(f) = 0$ is trivial, so then for all possible values of β,

$$\text{Number of monomials } = \sum_{\beta=1}^{|G|} \binom{\beta+n-1}{n-1} \tag{5}$$

Example 6.1. Consider group action on $\mathbb{C}[x, y, z]$ by $H = \{I, A, A^2\}$ as in Example 2.2. Since $\omega = e^{\frac{2\pi i}{3}}$ is a cube root of unity, we have $\omega^3 = 1$ and also $\omega^2 + \omega + 1 = 0$. By equation 5, we have to consider a total of 19 monomials. Let us first look at the three transformations to consider due to elements of H:

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad (x, y, z) \longmapsto (x, y, z) \quad A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix} \quad (x, y, z) \longmapsto (x, \omega y, \omega^2 z)$$

$$A^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega^2 & 0 \\ 0 & 0 & \omega \end{pmatrix} \quad (x, y, z) \longmapsto (x, \omega^2 y, \omega z)$$

Fundamental Invariaints using ρ_H

Monomial (f)	$\frac{1}{G}\sum_{A\in G} f(A\cdot\mathbf{x})$	Monomial (f)	$\frac{1}{G}\sum_{A\in G} f(A\cdot\mathbf{x})$
x	$\frac{1}{3}(x+x+x) = x$	x^2y	$\frac{1}{3}x^2(y+\omega y+\omega^2 y) = 0$
y	$\frac{1}{3}(y+\omega y+\omega^2 y) = 0$	x^2z	$\frac{1}{3}x^2(z+\omega z+\omega^2 z) = 0$
z	$\frac{1}{3}x^2(z+\omega z+\omega^2 z) = 0$	xy^2	$\frac{1}{3}x(y^2+\omega^2 y^2+\omega y^2) = 0$
xy	$\frac{1}{3}x(y+\omega y+\omega^2 y) = 0$	xz^2	$\frac{1}{3}x(z^2+\omega^2 z^2+\omega z^2) = 0$
yz	$\frac{1}{3}(yz+\omega^3 yz+\omega^3 yz) = yz$	yz^2	$\frac{1}{3}(yz^2+\omega^5 yz^2+\omega^4 yz^2) = 0$
zx	$\frac{1}{3}x(z+\omega z+\omega^2 z) = 0$	x^3	$\frac{1}{3}(x^3+x^3+x^3) = x^3$
x^2	$\frac{1}{3}(x^2+x^2+x^2) = x^2$	y^3	$\frac{1}{3}(y^3+y^3+y^3) = y^3$
y^2	$\frac{1}{3}(y^2+\omega^2 y^2+\omega y^2) = 0$	z^3	$\frac{1}{3}(z^3+z^3+z^3) = z^3$
z^2	$\frac{1}{3}(z^2+\omega^2 z^2+\omega z^2) = 0$	y^2z	$\frac{1}{3}(y^2z+\omega^4 y^2z+\omega^5 y^2z) = 0$
xyz	$\frac{1}{3}x(yz+\omega^3 yz+\omega^3 yz) =$ xyz		

So then we get the list of invariants $\{x, yz, x^2, xyz, x^3, y^3, z^3\}$. However, we only have 4 fundamental invariants since $\{x^2, xyz, x^3\}$ can be generated by $f_1 = x$, $f_2 = yz$, $f_3 = y^3$, $f_4 = z^3$. So then

$$\mathbb{C}[\mathbf{x}]^H \cong \mathbb{C}[x, y^3, z^3, yz]$$

Next, we consider another powerful quantative algorithm that determines, for action by a finite group, how many invariants are of a given degree. The algorithm stems from Molien's Formula for the Hilbert or Poincare Series, of which we first present a linear algebraic proof.

Definition 6.1 (Hilbert Series)**.** The **Hilbert Series** of the graded algebra $\mathbb{C}[\mathbf{x}]^G$ is the generating function

$$\Phi_G(z) = \sum_{d=0}^{\infty} \dim(C[\mathbf{x}]_d^G) z^d$$

The Hilbert series bears an immense significance when it comes to G-invariant algebras; since we find the dimension of each degree-based subspace of the invariant ring and express it as a formal power series, we have that the coefficient of z^j, expressed as $C_{\Phi_G}(z^j)$, gives the number of linearly independent invariants that exist at that degree.

Theorem 4 (Molien 1897)**.** *The Hilbert Series $\Phi_G(z)$ of the invariant ring $\mathbb{C}[\mathbf{x}]^G$ is given by*

$$\Phi_G(z) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(\mathbb{I}_n - gz)}$$

where $\mathbb{I}_n$ represents the $n \times n$ identity matrix.

Proof. We first need to introduce the following lemma which relates the dimensions of our graded algebra to the trace of the matrix acting upon the algebra.

Lemma 2. *If $G \subset GL_n(\mathbb{C})$ is a finite dimensional group, then the dimension of the invariant subspace $\mathbb{C}[\mathbf{x}]^G$ is given by*

$$\dim(\mathbb{C}[\mathbf{x}]^G) = \frac{1}{|G|} \sum_{A \in G} tr(A)$$

where $tr(A)$ represents the trace of the matrix A.

Proof. For proving this lemma, we construct an average matrix verson of the Reynolds operator. Consider the matrix

$$\Gamma = \frac{1}{|G|} \sum_{A \in G} A$$

Suppose we have Γ acting as a linear transformation on the vector space $\mathbb{C}[\mathbf{x}]$. This transformation clearly would be a matrix variant of the Reynolds operator, causing the matrix linear transformation $\Gamma : C[\mathbf{x}] \longrightarrow C[\mathbf{x}]^G$ defined on individual elements by the Reynolds operator $\rho_G(f)$. It then follows that Γ satisfies the properties of $\rho_G(f)$ mentioned in Section 4 Proposition 1 adjusted for matrices. Of particular importance is the property that $\Gamma^2 = \Gamma$, since this implies that the matrix is idempotent. Then it has eigenvalues $\lambda = 0, 1$. Now since the multiplicity of the eigenvalues gives the rank and the trace can be defined as the sum of all eigenvalues, we get that $\text{rank}(\Gamma) = \text{trace}(\Gamma)$. From this, we get that

$$\dim(C[\mathbf{x}]) = \text{rank}(\Gamma) = \text{trace}(\Gamma) = \frac{1}{|G|} \sum_{A \in G} \text{trace}(A)$$

Now let $\mathbb{C}[\mathbf{x}]_d$ denote the vector subspace of d-forms in $\mathbb{C}[\mathbf{x}]$, so then for linear transformations $\varphi \in G$ we have an induced linear transformation $\varphi_d \in \mathbb{C}[\mathbf{x}]_d$. The set of these linear transformations creates an induced group of linear transformations G_d. Naturally, $\mathbb{C}[\mathbf{x}]_d^G$ is our invariant subspace. A form consists of monomials $x_1^{k_1} x_2^{k_2} x_3^{k_3} \dots x_n^{k_n}$ such that $k_1 + k_2 + k_3 \dots k_n = d$, so then the total distinct monomials, and hence the dimension of $\mathbb{C}[\mathbf{x}]_d$, is $\binom{n+d-1}{n-1}$. Then the induced linear transformation group G_d consists of $\binom{n+d-1}{n-1} \times \binom{n+d-1}{n-1}$ invertible matrices.

Let us examine the case when $d = 1$, where we have the induced transformation matrix φ_1. The eigenvectors would be $x_{\varphi,1},\ x_{\varphi,2}, \dots, x_{\varphi,n}$ and the eigenvalues would be $\lambda_{\varphi,1},\ \lambda_{\varphi,2}, \dots, \lambda_{\varphi,n}$ for $\lambda_{\varphi,i} \in \mathbb{C}$. But since $x_{\varphi,1},\ x_{\varphi,2}, \dots, x_{\varphi,n}$ are our base variables, the transformation φ_1 represents the standard linear transformation caused by φ acting on $\mathbb{C}[\mathbf{x}]$, that is to say $\varphi = \varphi_1$. Furthermore, each φ is diagonalizable since the eigenvectors are linearly independent.

Since d-forms are homogeneous and the basis of our vector space $\mathbb{C}[\mathbf{x}]_d$, it follows that the basis vector of $\binom{n+d-1}{n-1}$ monomial d-forms is also the eigenvector. Let the eigenvectors of φ_d be denoted by $x_{\varphi,1}^{k_1},\ x_{\varphi,2}^{k_2}, \dots, x_{\varphi,n}^{k_n}$ where $k_1 + k_2 + k_3 \dots k_n = d$ and let the eigenvalues be denoted by $\lambda_{\varphi,1}^{k_1},\ \lambda_{\varphi,2}^{k_2},\ \dots, \lambda_{\varphi,n}^{k_n}$ where $\lambda_{\varphi,i}^{k_i} \in \mathbb{C}$.

$$\mathrm{trace}(\varphi_d) = \sum_{k_1 + \dots k_n = d} \lambda_{\varphi,1}^{k_1} \lambda_{\varphi,2}^{k_2} \dots \lambda_{\varphi,n}^{k_n}$$

Then from Lemma 2 and Definition 6.1,

$$\begin{aligned}
\Phi_G(z) &= \sum_{d=0}^{\infty} \dim(C[\mathbf{x}]_d^G) z^d = \sum_{d=0}^{\infty} \frac{1}{|G|} \sum\nolimits_{\varphi \in G} \mathrm{trace}(\varphi) z^d \\
&= \sum_{d=0}^{\infty} \frac{1}{|G|} \Bigg(\sum_{\varphi \in G} \Big(\sum_{k_1 + \dots k_n = d} \lambda_{\varphi,1}^{k_1} \lambda_{\varphi,2}^{k_2} \dots \lambda_{\varphi,n}^{k_n} z^d \Big) \Bigg) \\
&= \sum_{d=0}^{\infty} \frac{1}{|G|} \Bigg(\sum_{\varphi \in G} \Big(\sum_{k_1 + \dots k_n = d} \lambda_{\varphi,1}^{k_1} \lambda_{\varphi,2}^{k_2} \dots \lambda_{\varphi,n}^{k_n} z^{k_1 + k_2 + k_3 \dots k_n} \Big) \Bigg) \\
&= \sum_{\varphi \in G} \frac{1}{|G|} \Bigg(\sum_{d=0}^{\infty} \Big(\sum_{k_1 + \dots k_n = d} \lambda_{\varphi,1}^{k_1} z^{k_1} \cdot \lambda_{\varphi,2}^{k_2} z^{k_2} \cdot \dots \cdot \lambda_{\varphi,n}^{k_n} z^{k_n} \Big) \Bigg) \\
&= \sum_{\varphi \in G} \frac{1}{|G|} \Bigg(\sum_{(k_1, \dots k_n) \in \mathbb{N}^n} \lambda_{\varphi,1}^{k_1} z^{k_1} \cdot \lambda_{\varphi,2}^{k_2} z^{k_2} \cdot \dots \cdot \lambda_{\varphi,n}^{k_n} z^{k_n} \Bigg) \qquad (6)
\end{aligned}$$

Observe that $\sum_{k_i \in \mathbb{N}} \lambda_{\varphi,i}^{k_i} z^{k_i}$ can be expressed as its generating function

$$\sum_{k_i \in \mathbb{N}} (\lambda_{\varphi,i} z)^{k_i} = \frac{1}{1 - \lambda_{\varphi,i} z}$$

And so we then get in (6)

$$\sum_{\varphi \in G} \frac{1}{|G|} \left(\frac{1}{1 - \lambda_{\varphi,1} z} \cdot \frac{1}{1 - \lambda_{\varphi,2} z} \cdot \dots \cdot \frac{1}{1 - \lambda_{\varphi,n} z} \right) = \sum_{\varphi \in G} \frac{1}{|G|} \frac{1}{(1 - \lambda_{\varphi,1} z)(1 - \lambda_{\varphi,2} z) \cdot \dots \cdot (1 - \lambda_{\varphi,n} z)}$$

Now notice that

$$(1 - \lambda_{\varphi,1} z)(1 - \lambda_{\varphi,2} z) \cdot \dots \cdot (1 - \lambda_{\varphi,n} z) = \begin{vmatrix} 1 - \lambda_{\varphi,1} z & . & 0 \\ . & . & . \\ 0 & . & 1 - \lambda_{\varphi,n} z \end{vmatrix} = \det(\mathbb{I}_n - \varphi z)$$

since $\varphi = \varphi_1$ has eigenvalues $\lambda_{\varphi,1},\ \lambda_{\varphi,2}, \dots, \lambda_{\varphi,n}$. And so we get the formula

$$\Phi_G(z) = \frac{1}{|G|} \sum_{\varphi \in G} \frac{1}{\det(\mathbb{I}_n - \varphi z)}$$

□

Example 6.2. Suppose we have the group from Example 2.2 $H = \{\mathbb{I}, A, A^2\}$ acting on $\mathbb{C}[x, y, z]$. Recall that $1 + \omega + \omega^2 = 0$ and $\omega^3 = 1$. Then we have

$$\det(\mathbb{I}_3 - \mathbb{I}z) = \begin{vmatrix} 1-z & 0 & 0 \\ 0 & 1-z & 0 \\ 0 & 0 & 1-z \end{vmatrix} = (1-z)^3$$

$$\det(\mathbb{I}_3 - Az) = \begin{vmatrix} 1-z & 0 & 0 \\ 0 & 1-\omega z & 0 \\ 0 & 0 & 1-\omega^2 z \end{vmatrix} = (1-z)(1-\omega z)(1-\omega^2 z) = 1-z^3$$

$$\det(\mathbb{I}_3 - A^2 z) = \begin{vmatrix} 1-z & 0 & 0 \\ 0 & 1-\omega^2 z & 0 \\ 0 & 0 & 1-\omega z \end{vmatrix} = (1-z)(1-\omega^2 z)(1-\omega z) = 1-z^3$$

And so we have

$$\Phi_H(z) = \frac{1}{3}\left(\frac{1}{(1-z)^3} + \frac{2}{1-z^3}\right)$$

The maclaurin series of $\frac{1}{1-z^3}$ is simply $1 + z^3 + z^6 \dots$. For $1/(1-z)^3$, we first consider the following

$$\frac{1}{1-z} = 1 + z + z^2 + z^3 + z^4 + z^5 + \dots$$

Twice-differentiating both sides, we obtain

$$\frac{1}{(1-z)^3} = 1 + 3z + 6z^2 + 10z^3 + \dots$$

Combining both series in accordance with the mentioned formula, we get that

$$\Phi_H(z) = 1 + z + 2z^2 + 4z^3 + \dots$$

Note that we are not concerned about terms with degree greater than 3 since the Noether bound states that the fundamental invariants are of degree less than $|G| \leq 3$. From the Hilbert Series, we can gather that there is one invariant of degree 0, one invariant of degree 1, two invariants of degree 2, and four invraiants of degree 3. This matches the results obtained using the Reynolds operator in Example 6.1, since we obtained the list of invariants $\{x, yz, x^2, xyz, x^3, y^3, z^3\}$.

Example 6.3. Let us look at an implementation of this algorithm for finding the invariant ring of $\mathbb{C}[x, y]$ under action by the dihedral group D_3, which represents the group of symmetries of the equilateral triangle. The matrix representation of the dihedral group is

$$D_3 = \{r_0, r_1, r_2, s_0, s_1, s_2\}$$

where r_k and s_k can be represented by the following 2×2 matrices

$$r_k = \begin{pmatrix} \cos\frac{2k\pi}{3} & -\sin\frac{2k\pi}{3} \\ \sin\frac{2k\pi}{3} & \cos\frac{2k\pi}{3} \end{pmatrix}, \quad s_k = \begin{pmatrix} \cos\frac{2k\pi}{3} & \sin\frac{2k\pi}{3} \\ \sin\frac{2k\pi}{3} & -\cos\frac{2k\pi}{3} \end{pmatrix}$$

We first calculate the Hilbert Series $\Phi_{D_3}(z)$ using Molein's Formula to find the number of invariants of each degree. First, for any s_k,

$$\det(\mathbb{I} - s_k z) = \begin{vmatrix} 1 - z\cos\frac{2k\pi}{3} & -z\sin\frac{2k\pi}{3} \\ -z\sin\frac{2k\pi}{3} & 1 + z\cos\frac{2k\pi}{3} \end{vmatrix} = (1 - z^2\cos^2\frac{2k\pi}{3}) - z^2\sin^2\frac{2k\pi}{3} = 1 - z^2$$

As for r_k, we require a more case-by-case evaluation of the determinants,

$$\det(\mathbb{I} - r_0 z) = \begin{vmatrix} 1-z & 0 \\ 0 & 1-z \end{vmatrix} = (1-z)^2$$

$$\det(\mathbb{I}-r_1z)=\begin{vmatrix}1-z\cos\frac{2\pi}{3} & z\sin\frac{2\pi}{3}\\ -z\sin\frac{2\pi}{3} & 1-z\cos\frac{2\pi}{3}\end{vmatrix}=(1+\frac{z}{2})^2+\frac{3z^2}{4}=z^2+z+1$$

$$\det(\mathbb{I}-r_2z)=\begin{vmatrix}1-z\cos\frac{4\pi}{3} & z\sin\frac{4\pi}{3}\\ -z\sin\frac{4\pi}{3} & 1-z\cos\frac{4\pi}{3}\end{vmatrix}=z^2+z+1$$

And so we have

$$\Phi_{D_3}(z)=\frac{1}{6}\left(\frac{3}{1-z^2}+\frac{1}{(1-z)^2}+\frac{2}{1+z+z^2}\right)$$

$$=\frac{1}{6}\big[3(1+z^2+z^4+\dots)+(1+2z+3z^2+4z^3+\dots)+2(1-z)(1+z^3+z^6+\dots)\big]$$

$$=1+z^2+z^3+z^4+z^5+2z^6+\mathcal{O}(x^7)$$

And so we must have one invariant for degrees 2 to 5 and two invariants for degree 6.

The general case of invariants of D_n is worth analyzing. Note that D_n would be generated by elements r and s that are

$$r=\begin{pmatrix}\cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n}\\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n}\end{pmatrix},\quad r^k=\begin{pmatrix}\cos\frac{2k\pi}{n} & -\sin\frac{2k\pi}{n}\\ \sin\frac{2k\pi}{n} & \cos\frac{2k\pi}{n}\end{pmatrix}$$

$$s=\begin{pmatrix}\cos\frac{2\pi}{n} & \sin\frac{2\pi}{n}\\ \sin\frac{2\pi}{n} & -\cos\frac{2\pi}{n}\end{pmatrix},\quad s^k=\begin{pmatrix}\cos\frac{2k\pi}{n} & \sin\frac{2k\pi}{n}\\ \sin\frac{2k\pi}{n} & -\cos\frac{2k\pi}{n}\end{pmatrix}$$

Then our group D_n of order $2n$ is as follows: $D_n=\{1,r,r^2,r^3,\dots.\,r^{n-1},s^0,s,s^2,s^3,\dots s^{n-1}\}$. We take a similar approach to that used in finding the distribution of invariants by degree under action by D_3, and so we first compute the Hilbert Series for each using Molien's Formula.

$$\det(\mathbb{I}-sz)=\begin{vmatrix}1-z\cos\frac{2k\pi}{n} & -z\sin\frac{2k\pi}{n}\\ -z\sin\frac{2k\pi}{n} & 1+z\cos\frac{2k\pi}{n}\end{vmatrix}=1-z^2$$

The process is a little more involved in the case of r^k,

$$\det(\mathbb{I}-r^kz)=\begin{vmatrix}1-z\cos\frac{2k\pi}{n} & z\sin\frac{2k\pi}{n}\\ -z\sin\frac{2k\pi}{n} & 1-z\cos\frac{2k\pi}{n}\end{vmatrix}=(1-2z\cos\frac{2k\pi}{n}+z^2)$$

Next, we wish to factor the expression obtained for $\det(\mathbb{I}-r^kz)$. Setting the polynomial equal to zero, we find

$$(1-2z\cos\frac{2k\pi}{n}+z^2)=0,\quad z=\cos\frac{2k\pi}{n}\pm\sqrt{\cos^2\frac{2k\pi}{n}-1}=\cos\frac{2k\pi}{n}\pm i\sin\frac{2k\pi}{n}=e^{\pm i\frac{2k\pi}{n}}$$

Let $\lambda\equiv e^{\frac{2\pi}{n}}$, so then $\det(\mathbb{I}-r^kz)=(z-\lambda^k)(z-\lambda^{-k})$. Consequently, we have our expression for the Hilbert Series as

$$\Phi_{D_n}(z)=\frac{1}{2n}\left[\frac{n}{1-z^2}+\sum_{k=0}^{n-1}\frac{1}{(z-\lambda^k)(z-\lambda^{-k})}\right]$$

The series representation of the latter term is

$$\frac{1}{(z-\lambda^k)(z-\lambda^{-k})}=\sum_{n=0}^{\infty}\frac{\lambda^{kn}(z^n+z^{-n})}{1-z^2}=\frac{1}{1-z^2}\left(\frac{1}{1-z^n}+\frac{1}{1-z^{-n}}\right)=\frac{1}{1-z^2}\cdot\frac{1+z^n}{1-z^n}$$

So our Hilbert series is simplified to

$$\Phi_{D_n}(z)=\frac{1}{2n}\left[\frac{n}{1-z^2}+\frac{n}{1-z^2}\cdot\frac{1+z^n}{1-z^n}\right]=\frac{1}{(1-z^2)(1-z^n)}$$

From here, it can be shown that the invariant ring $\mathbb{C}[x,y]^{D_n}$ can be generated by two fundamental invariants (See [Ver]). These invariants, of degree 2 and degree k, are

$$f_1 = x^2 + y^2, \quad f_2 = \prod_{k=0}^{n-1} (x \cos \frac{2k\pi}{n} + y \sin \frac{2k\pi}{n})$$

Note that the f_1 as an invariant is an expected outcome: in the rotation of a point $P(x,y)$, we observed that the distance is an invariant quantity; the polynomial f_1 is just the square of that. [Bor12] provides a relatively straightforward reasoning behind the occurence of these invariants by considering the geometry of the transformations. If we consider the action of the dihedral group on $\mathbb{C}$, a complex number $z = x + iy$ and its conjugate $\overline{z} = x - iy$ are transformed in the following way: r^1 (rotation) moves z to ηz and $\overline{z}$ to $\eta\overline{z}$ for $\eta = e^{\frac{2k\pi}{n}}$, whereas s^0 (reflection) exchanges z and $\overline{z}$. Then two invariant quantities $z\overline{z}$ and $z^n + \overline{z}^n$ emerge. Their equivalence to the invariants f_1 and f_2 can be shown.

And thus we can compute the invariants of any finite group by a combination of the Reynolds operator method and the Molien Series method.

Algorithm 6.2 (Completeness of Fundamental Invariants)**.** The Invariant ring is equal to a proposed subalgebra of fundamental invariants iff

$$\Phi_G(z) - \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(\mathbb{I}_n - gz)} = 0$$

Otherwise, the remaining invariants can be computed using the Reynolds operator and be appended to the set of fundamental invariants.
In general, we can use the Molien Series to determine the distribution of invariants by degree upto the Noether Bound and then use the Reynolds operator to find invariants in those degrees.

7. Applications to Coding Theory

A striking application of invariant theory comes in the study of error-correcting codes, realized mostly because of [Slo77]. The paper explores a connection between coding theory and invariant theory of finite groups. We provide a brief overview of Sloane's work along with the basics of coding theory in order to demonstrate the applicability of invariants.

Consider a telegraph line from New York to Boston which transmits only 0's and 1's, except it is faulty in that a 1 is ocassionally received as a 0 in Boston and vice versa. The solution to this problem relies in sending certain code words; for the sake of simplicity, say 00000 for NO and 11111 for YES. Then if Boston receives 01010, it is more likely that the message was actually 00000 than 11111 since the faulty code was closer to 00000 in that it had more 0s than 1s.
This leads to the notion of a **Hamming distance** $\text{dist}(\mathbf{u}, \mathbf{v})$ between vectors $\mathbf{v} = \langle v_1, v_2, \ldots v_n \rangle$ and $\mathbf{u} = \langle u_1, u_2, \ldots u_n \rangle$, which is the number of places where $u_i \neq v_i$. A **binary code** is a collection of code words represented by $[n, k, d]$, where n is called the **length** of the code, k the **dimension** and d is the **minimum Hamming distance** between two code words. Good codes are often characterized by small n for faster transmission, large k for more efficiency, and large d so that deviations from an original code word can be corrected with less nuances.
A useful method of analyzing code comes from its **weight enumerator**, which is a bivariate polynomial giving the number of code words of a certain weight. The weight $\text{wt}(\mathbf{u})$ measures the number of non-zero u_i. So then the Weight enumerator of a code $\mathcal{C}$ is given by

$$\mathcal{W}_{\mathcal{C}}(x,y) = \sum_{i=0}^{n} N_i x^{n-i} y^i$$

where N_i is the number of codes of a weight i.
The weight enumerator leads to invariants when one considers codes that are self-dual. A **dual code** $\mathcal{C}^*$ is a code consisting of all vectors orthogonal to a code $\mathcal{C}$. That is,

$$\mathcal{C}^* = \{\mathbf{v} : \sum_{i=1}^{n} u_i v_i = 0 \text{ for all } \mathbf{u} \in \mathcal{C}\}$$

A code for which $\mathcal{C} = \mathcal{C}^*$ is called a **self-dual code**. This particular class of codes are of special interest because restrictive conditions like the Gilbert-Varshamov bound are met by such codes (See [MST72]). Furthermore, self dual codes are often the optimal possible option for a class of codes (See [Slo77] for examples) and the self duality of a certain code can be used to simplify the decoding process in certain situations. We refer the reader to [Slo77] and [NRS06] for more on the utility of self-dual codes.
As a consequence of the MacWilliams Identity (proof in [Slo77] for binary case), there is a direct relationship between the weight enumerator of a code and that of its dual. To study the relationship of invariants and weight enumerators, we consider the following corollary of the MacWilliams Identity stated in [Stu08]: the weight enumerator of a self-dual binary code satisfies the following

$$\mathcal{W}(x, y) = \mathcal{W}(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}})$$

$$\mathcal{W}(x, y) = \mathcal{W}(x, -y)$$

This corollary clearly links to the invariant theory in this paper: this invariance of $\mathcal{W}$ is occuring under transformations by matrices

$$r = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}, \quad s = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$$

which are the generators of the D_8 group. So then our task becomes to find polynomials invariant under action by the group of symmetries of the octagon. This specific group was considered in Example 6.3, and so we have invariant polynomials

$$\mathcal{W}_1 = x^2 + y^2, \quad \mathcal{W}_2 = \prod_{k=0}^{7}(x \cos\frac{k\pi}{4} + y \sin\frac{k\pi}{4}) = x^2y^2(x^2 - y^2)^2$$

Properties that are often desired in codes can be quantified in terms of weight enumerators. The main application of the work in [Slo77] was that it showed the sparseness of codes that satisfied desired properties. One can show that the weight enumerators, which are invariant under transformations, often do not exist when it comes to certain types of codes. Thus, the methods in Invariant theory prove useful in assessing the possibility of certain types of codes.

8. Further Research

While this expository paper covers most major topics in Invariant Thoery, there are multiple avenues in which one can further explore this field. To a certain extent, the finiteness theorem marked the end of Classical Invariant Theory as no substantial problems remained to be solved. However, the theory was revived by Mumford through his book *Geometric Invariant Theory*, which broadly deals with constructing quotient groups of algebraic varieties through some linear group action. While the theory greatly broadens the scope of Invariant Theory, it is technical in nature and accessible only with a considerable background in category theory and homological algebra, and hence has not been discussed in this paper. Apart from Mumford's own book [MF82], [Dol03] is another great source for learning GIT.
Lastly, while the algorithms mentioned in Section 6 work well for finite groups, they clearly involve heavy and complex calculations. With the deeper understanding of computational techniques today,

better algorithms for computing invariants have been developed. We refer the reader to [Stu08], [PD14], and [DK09] for more research into these algorithms.

References

[Bor12] Borcherds. Lie groups. 2012.

[CLO97] David Cox, John Little, and Donal O'Shea. Ideals, varieties, and algorithms. undergraduate texts in mathematics, 1997.

[Con] Keith Conrad. Symmetric polynomials.

[Dan17] Daniel. An introduction to invariant theory (dissertation). 2017.

[DK09] Harm Derksen and Gregor Kemper. *Computational invariant theory*. Springer, 2009.

[Dol03] Igor Dolgachev. *Lectures on invariant theory*. Number 296. Cambridge University Press, 2003.

[Hil93] David Hilbert. Über die vollen invariantensysteme. *Mathematische annalen*, 42(3):313–373, 1893.

[KP] H Kraft and C Procesi. A primer in invariant theory (unpublished). *Text available from http://www. math. unibas. ch/˜ kraft/Papers/KP-Primer. pdf.*

[KR84] Joseph PS Kung and Gian-Carlo Rota. The invariant theory of binary forms. *Bulletin of the American Mathematical Society*, 10(1):27–85, 1984.

[Lor18] G Loria. Elliot, eb-an introduction to the algebra of quantics. 1918.

[MF82] D Munford and J Fogarty. Geometric invariant theory, ergeb springer, berlin, heidelberg, new york, math. grenzgeb.(3), vol. 34, 1982.

[Mil12] James S Milne. Reductive groups. *Courses Notes, Version*, 1, 2012.

[MST72] F Jessie MacWilliams, Neil JA Sloane, and John G Thompson. Good self dual codes exist. *Discrete Mathematics*, 3(1-3):153–162, 1972.

[Nag59] Masayoshi Nagata. On the 14-th problem of hilbert. *American Journal of Mathematics*, 81(3):766–772, 1959.

[NRS06] Gabriele Nebe, Eric M Rains, and Neil James Alexander Sloane. *Self-dual codes and invariant theory*, volume 17. Springer, 2006.

[PD14] Mihaela Ileana Popoviciu Draisma. *Invariants of binary forms*. PhD thesis, University_of_Basel, 2014.

[Slo77] Neil JA Sloane. Error-correcting codes and invariant theory: new applications of a nineteenth-century technique. *The American Mathematical Monthly*, 84(2):82–107, 1977.

[Stu08] Bernd Sturmfels. *Algorithms in invariant theory*. Springer Science & Business Media, 2008.

[Ver] Verma. Ring of invariants of finite groups.