Generations and Relations for Rings of Invariants

by

Murat Can Askarogullari

B.Sc., Bilkent University, 2014

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF

Master of Science

in

THE FACULTY OF GRADUATE AND POSTDOCTORAL
STUDIES
(Mathematics)

The University of British Columbia
(Vancouver)

April 2016

Abstract

In this thesis we first prove that the algebra of invariants for reductive groups over the base field complex numbers are finitely generated. Then we focus on invariant algebras of finite groups. After showing the natural relation between invariant algebras and reflections in the group we prove the Chevalley-Shephard-Todd theorem. We conclude with classification of complex finite reflection groups and some examples. Throughout the thesis we follow similar arguments as in Springer[8] and Kane[6] where we give full details on the arguments.

Preface

The topic of this thesis and the roadmap were suggested by my supervisor Prof. Zinovy Reichstein. This thesis surveys known results that are not original under particular assumptions. The author tried to present and modify it to make things more fluent and clear than they were written in the original form according to the assumptions made in a way unique to the author.

Table of Contents

Acknowledgements

I wish to express my deepest thanks for my supervisor Prof. Zinovy Reichstein for his guidance and support. I would also want to thank my parents for their support and love throughout the years.

Chapter 1

Introduction

The roots of invariant theory goes back to 18th century. In the study of quadratic binary forms, the discriminant, an algebraic invariant is used to distinguish between equivalent forms. After the introduction of homogeneous coordinates by Moebius and Plucker at the beginning of 19th century people became more interested in invariant theory. Classically invariant theory looks for elements of polynomial algebra over a base field that doesn't change under the action of a given linear algebraic group- the algebra of invariants. During the first decades of invariant theory, people were looking for particular invariants. For instance, one of the major problems was finding the algebra of invariants where $SL_2(\mathbb{C})$ acting on $(d+1)$-dimensional vector space of binary forms of degree d. Is this invariant algebra generated by finitely many elements over $\mathbb{C}$? This question is a basic question in invariant theory which can be generalized and is proven for this case before Hilbert. Positive answer to this question was established by P. Gordan in 1868 [5]. However solving the same question in a more general setting, for instance for $SL_n(\mathbb{C})$, was at that time very hard. Hilbert introduced new methods in algebra to settle this question and this inspired the Hilbert's 14th problem. Hilbert's 14th problem asks whether or not finite generation of invariants continues to hold for every linear representation $G \to GL(V)$ of every linear algebraic group G. In this thesis we work over the base field $\mathbb{C}$ and this result is proven by Hermann Weyl in 1926 for reductive algebraic

groups over $\mathbb{C}$ [3]. We show this result in chapter 3 largely following [7] and [2]. However, in general, the answer to Hilbert's 14th problem is negative. The first counterexample was discovered by M.Nagata around 60 years later, he gave an example of non finitely generated algebra of invariants [4].

Given a finite set of generators for the invariant algebra, it is natural to ask about the natural relations among these generators. The answer to this question can be quite non-trivial even for finite groups. The algebra of invariants is a free polynomial algebra (i.e., has an algebraically independent set of generators) if and only if G is generated by reflections. This theorem is called Chevalley-Shephard-Todd theorem. It was first proven by Shephard and Todd[2] then later by Chevalley[1]. This is another main theorem of the thesis. Again our exposition in Chapter 6 largely follows the approach in [8] and [6]. In chapter 7 we will define irreducible complex reflection groups and show that every complex reflection group is a product of irreducible ones. Finitely generated irreducible complex reflection groups were first classified by Shephard and Todd. There are 37 cases; 34 exceptional cases and 3 infinite families. We don't give the whole table in here but rather give some examples.

Chapter 2

Reductive Groups and Complete Reducibility

Notation and Preliminaries

Let $G \leq GL(V)$ for a finite dimensional vector space V over the field $\mathbb{C}$. We consider the action of G on algebra of polynomial functions on V and we are interested in the invariant algebras induced by this action.

We will denote the polynomial functions on V by $S(V)$ or by S interchangeably. Let $\dim V = n$, we have $S(V) \simeq \mathbb{C}[T_1, T_2, \ldots, T_n]$ in the category of $\mathbb{C}$-algebras, so S is a graded $\mathbb{C}$-algebra. We denote the homogeneous elements of S of degree d ($d \in \mathbb{N}$) by S_d.

There is a natural left action of G on the vector space V since $g \in GL(V)$ an invertible linear transformation. This action induces a left action on S as follows: Let $f \in S$, $v \in V$, $g \in G$, define $g.f$ by $g.f(v) = f(g^{-1}.v)$. If we have $g.f = f$ for all $g \in G$ we say that f is G-invariant. The G-invariant polynomials form a $\mathbb{C}$-algebra which we denote by S^G (or $S(V)^G$). This is called the algebra of invariants. Note that for an arbitrary $g \in G$ we have $g.S_d \subset S_d$, meaning that S_d is a G-invariant $\mathbb{C}$-subspace of S for all $d \geq 0$. Note that $S_1 = V^*$; therefore action induced on V^* is defined. We define some of the actions G induces for the future reference in here.

Definition 2.1. Let $G \subset GL(V)$ and let W be a G-invariant subspace of V; in other words let $g.W \subset W$ for all $g \in G$. We define the induced action on the quotient vector space V/W as follows; let $[v] \in V/W$ denote the equivalence class of $v \in V$, then $g.[v] = [g.v]$. This action is well-defined because W is G-invariant.

Definition 2.2. Assume $G \subset GL(V)$ and $G \subset GL(W)$. Then both V and W are G-modules. We define the action induced on $Hom(V, W)$ as follows; let $h \in Hom(V, W)$, then define $g.h$ by

$$(g.h)(v) = g.(h(g^{-1}.v)),\ v \in V$$

Now, to be able to define a linear algebraic group we equip $GL(V)$ with a topology as follows: Let $E(V)$ be the vector space of all $\mathbb{C}$-linear transformations of the vector space V. This vector space is isomorphic to $M_{n\times n}(\mathbb{C})$ and therefore also isomorphic to $\mathbb{C}^{n^2}$. We can define the Zariski topology on $E(V)$ using that isomorphism; with respect to the Zariski topology on $E(V)$, $GL(V)$ is an open subset of $E(V)$ because $GL(V)$ is the complement of the zero set of the determinant function which is a polynomial in n^2 variables. However by adding one variable, we make $GL(V)$ into an affine algebraic variety. We identify the $GL(V)$ with the following closed set

$$Z(T_{n^2+1}.det(T_1, T_2, \ldots, T_{n^2}) - 1) \subset E(V) \times \mathbb{C} := \{(g, x) \,|\, g \in E(V), x \in \mathbb{C}\}$$

Define the map $\psi : GL(V) \to Z(T_{n^2+1}.det(T_1, T_2, \ldots, T_{n^2})-1)$ where $\psi(g) = (g, (\det g)^{-1})$. This map is clearly injective and surjective. From now on, when we talk about topology on $GL(V)$ or any subset of it we talk about topology induced by the Zariski topology on $E(V) \times \mathbb{C}$.

Remark 2.3. (i) The inverse map $\phi : GL(V) \to GL(V)$ where $\phi(g) = g^{-1}$ is continuous, bijective and involutory, i.e. its inverse is itself; therefore defines a homeomorphism from $GL(V)$ to $GL(V)$.

(ii) Fixing $a \in GL(V)$, define $\psi_a : G \to G$ where $\psi_a(g) = a.g$. This is also a continuous bijection which has the inverse $\psi_{a^{-1}}$.

Definition 2.4. A group G is called a linear algebraic group if and only if it is a closed subgroup of $GL(V)$ for some vector space V. That is, a linear algebraic group is also an affine variety.

Remark 2.5. Any finite subgroup of $GL(V)$ is linearly algebraic. This is because it represents finite set of points on $E(V) \times \mathbb{C}$ which is closed with respect to the Zariski topology.

Reductive Groups

The aim of this section is to investigate the reductivity of the linear algebraic groups. Reductive groups play a special role in invariant theory. As we shall see in the next chapter, invariant algebras for actions of these groups are always finitely generated.

Definition 2.6. A linear algebraic group G is called reductive if for any rational representation $\rho : G \to GL(V)$ and any $0 \neq w \in V$ such that $\rho(g).w = w$ for all $g \in G$, there exists a linear element $f \in S(V)^G$ with $f(w) \neq 0$.

Proposition 2.7. *If $G \subset GL(V)$ is a finite group, then it is reductive.*

Proof. Let $w \in V$ such that $g.w = w$ for all $g \in G$. Consider a $w^* \in V^*$ such that $w^*(w) = 1$. Such a $w*$ is not unique. If we apply the averaging operator over G to w^* we get the element $\frac{1}{|G|}\sum_{g\in G} g.w^*$ which is in V^*. This is the linear element we are looking for; observe that

$$\frac{1}{|G|}\sum_{g\in G} g.w^*(w) = \frac{1}{|G|}\sum_{g\in G} w^*(g^{-1}.w) = \frac{1}{|G|}\sum_{g\in G} w^*(w) = 1 \neq 0$$

□

Lemma 2.8. *If $\pi : V \to W$ is a homomorphism of G-modules, then the subset of $Hom(W, V)$ consisting of sections of π is G-invariant. That is, the set $R := \{r \in Hom(W, V) \mid \pi \circ r = id_W\}$ is G-invariant.*

Proof. Let $g \in G$, $r \in R$ and $w \in W$ be arbitrary. $(g.r)(w) = g.(r(g^{-1}.w))$, therefore $(\pi \circ (g.r))(w) = \pi(g.(r(g^{-1}.w))) = g.\pi(r(g^{-1}.w)) = g.(g^{-1}.w) = w$. Here we used the fact that π is a morphism of G-modules and the definition of R. $\square$

Lemma 2.9. *If $\pi : V \to W$ is a surjective homomorphism of G-modules where G is reductive, then there exists a section $r \in R := \{r \in Hom(W, V) \mid \pi \circ r = id_W\}$ such that $g.r = r$ for all $g \in G$. Note that we use the induced action introduced in Definition 2.2.*

Proof. From Lemma 2.8, $g.r \in R$ for any $g \in G$ and $r \in R$, therefore $Span_{\mathbb{C}}(g.r \mid g \in G, r \in R) = Span_{\mathbb{C}}R$. Let $f \in (Span_{\mathbb{C}}R)^*$ be defined as $f(\sum_{i=1}^n \lambda_i r_i) = \sum_{i=1}^n \lambda_i$ where $\lambda_i \in \mathbb{C}$ and $r_i \in R$. This is a natural definition because $\pi \circ (\sum_{i=1}^n \lambda_i r_i) = (f(\sum_{i=1}^n \lambda_i r_i))\, id_W$. Observe that f is G-invariant; let $g \in G$ be arbitrary, $(g.f)(\sum_{i=1}^n \lambda_i r_i) = f(\sum_{i=1}^n \lambda_i (g^{-1}.r_i)) = \sum_{i=1}^n \lambda_i = f(\sum_{i=1}^n \lambda_i r_i)$ since $g^{-1}.r_i \in R$ for $r_i \in R$. Let $R' := \ker f$ then R' is a G-invariant subspace of $Span_{\mathbb{C}}R$. This gives the following short exact sequence

$$0 \to R' \to Span_{\mathbb{C}}R \xrightarrow{f} \mathbb{C} \to 0$$

This is a short exact sequence because clearly f is not equal to zero and R' is a subspace of $Span_{\mathbb{C}}R$ of codimension 1 by definition. Now, by the reductivity of G there exists a G-invariant element $r' \in Span_{\mathbb{C}}R = ((Span_{\mathbb{C}}R)^*)^*$ such that $r'(f) = f(r') \neq 0$; so we can assume that $f(r') = 1$; this means $r' \in R$ since $\pi \circ r' = f(r') id_W = id_W$. So r' is a G-invariant section. Hence we are done.

$\square$

Definition 2.10. Let $\rho : G \to GL(V)$ be a representation;

(i) ρ is reducible if there exists a nonzero G-stable proper subspace W. That is if there exists $\{0\} \neq W \subsetneq V$ such that $\rho(G).W \subset W$. If there is no such proper subspace we say that the representation ρ is irreducible.

(ii) ρ is semi-simple if for any G-stable subspace $W \subset V$ there is a complementary G-stable subspace W' such that $V = W \oplus W'$.

Proposition 2.11. *The following properties of a representation $\rho : G \to GL(V)$ are equivalent;*

(i) For any irreducible G-stable subspace W of V there exists a G-stable complementary subspace,

(ii) ρ is semi-simple,

(iii) V is a direct sum of G-stable irreducible subspaces.

Proof. We will use induction on $\dim V$. For the $\dim V = 0$ equivalence of the statements is clear. Assume statements are equivalent for smaller dimensions.

(i)$\Rightarrow$ (ii) Let's take a proper G-stable subspace W of V. Let U be a nonzero irreducible G-stable subspace of W; U is also a subspace of V and by our assumption (i) we have a G-stable complementary subspace U' such that $V = U \oplus U'$. W is a G-stable subspace and for any $w \in W$ we have $w = u + u'$ where $u \in U, u' \in U'$ are unique, which implies $w - u = u' \in W$ since $U \subset W$. Therefore we have the decomposition $W = U \oplus (W \cap U')$. Note that W and U' are G-stable subspaces therefore $W \cap U'$ is also a G-stable subspace. Thus we have a G-stable complementary subspace for U in W. Here U was an arbitrary irreducible subspace of W therefore the statement (i) holds for W. By the induction assumption this implies $\rho|_W$ is semi-simple. To show that $\rho|_W$ is semi-simple we only used the fact that W is a G-stable subspace; therefore similar arguments show that $\rho|_{U'}$ is semi-simple. In particular we have a decomposition $U' = (W \cap U') \oplus U''$ where U'' is a G-stable subspace. Thus we have a decomposition $V = U \oplus (W \cap U') \oplus U'' = W \oplus U''$ concluding that ρ is semi-simple.

(ii)$\Rightarrow$ (iii) If V is irreducible we are done. If not, take an irreducible G-stable subspace U, there exists a complementary G-stable subspace W such that $V = U \oplus W$ by (ii). We claim that W is completely reducible. To show that, it is enough to prove that $\rho|_W$ is semi-simple because W is a proper

subspace so we can use the induction assumption. Now, let's take a nonzero G-stable subspace $W' \subset W$. Observe that $W' \subset V$ and ρ is semi-simple by our assumption. So we have a complementary G-stable subspace $\tilde{W}$ such that $V = W' \oplus \tilde{W}$. W is a G-stable subspace and $W' \subset W$ therefore we can say the following: $W = W' \oplus (W \cap \tilde{W})$. We know that W and $\tilde{W}$ are G-stable therefore $W \cap \tilde{W}$ is also G-stable. Thus we have found a G-stable complementary subspace for W' in W; meaning that $\rho|_W$ is semi-simple. Using the induction assumption, W is completely reducible, but we have $V = U \oplus W$ where U is irreducible. We are done.

(iii)$\Rightarrow$ (i) $V = U_1 \oplus U_2 \oplus \cdots \oplus U_m$ where $U_1, U_2, \ldots, U_m$ are G-stable irreducible subspaces of V. If we take an irreducible G-stable subspace of W we would have the restriction of usual projection maps $\pi_i|_W : W \to U_i$. Both W and U_i are irreducible therefore we have either $W \simeq U_i$ or $W \cap U_i = 0$. WLOG assume $W \simeq U_i$ for $1 \leq i \leq k$ and that $\dim W = n$. That is, we have $W \subset U_1 \oplus U_2 \oplus \cdots \oplus U_k$. Note that π_i's are G-module isomorphisms for $1 \leq i \leq k$, so we can define $f_i := \pi_i^{-1} : U_i \to W$ which is again a G-module isomorphism. Using these maps define

$$\begin{aligned} F :& U_1 \oplus U_2 \oplus \cdots \oplus U_k \twoheadrightarrow W \\ & u_1 + u_2 + \ldots + u_k \to f_1(u_1) + f_2(u_2) + \ldots + f_k(u_k) \end{aligned}$$

This is an G-module homomorphism;

$$\begin{aligned} g.F(u_1 + u_2 + \ldots + u_k) &= g.(f_1(u_1) + f_2(u_2) + \ldots + f_k(u_k)) \\ &= g.f_1(u_1) + g.f_2(u_2) + \ldots + g.f_k(u_k) \\ &= f_1(g.u_1) + f_2(g.u_2) + \ldots + f_k(g.u_k) \\ &= F(g.u_1 + g.u_2 + \ldots + g.u_k) \\ &= F(g.(u_1 + u_2 + \ldots + u_k)) \end{aligned}$$

Let $0 \neq w \in W$ and let $w = u_1 + u_2 + \ldots + u_n$ in the direct sum decomposition, then $f_i(u_i) = w$ by definition. This gives $F(w) = kw \neq 0$; that is, $W \cap \ker F = \{0\}$ and F is surjective. Thus if $W' := \ker F$ then $W \oplus W' =$

$U_1 \oplus U_2 \cdots \oplus U_k$. Note that W' is a G-stable subspace because it is kernel of a G-module homomorphism. Hence, $W' \oplus U_{k+1} \oplus \ldots \oplus U_m$ is a G-stable complementary subspace for W in the vector space V. We are done. $\square$

Definition 2.12. Let $G \subset$ be a linear algebraic group, a rational representation of G is a homomorphism $\rho : G \to GL(W)$ that is also morphism of algebraic varieties.

The following proposition tells us that every rational representation of a reductive group possesses properties (i), (ii) and (iii) of Proposition 2.11.

Proposition 2.13. *A linear algebraic group G is reductive if and only if any rational representation of G is semi-simple.*

Proof. "$\Leftarrow$"Let $\rho : G \to GL(V)$ be a rational representation. By assumption it is semi-simple. Let $w \in W$ such that $\rho(G).w = w$ then the subspace $\mathbb{C}w$ of V is a G-stable subspace. By the semi-simplicity there exists a G-stable complementary subspace W of V such that $V = \mathbb{C}w \oplus W$. We can define a linear function f on V such that $f|_W = 0$ and $f(w) = 1$ then f is G-invariant. This is because $(\rho(g).f)(v) = f(\rho(g)^{-1}.v)$ and if $v \in W$ then $\rho(g)^{-1}.v \in W$ for all $g \in G$ implying that $f(v) = (\rho(g).f)(v) = 0$; and if $v \in \mathbb{C}w$ then $g^{-1}.v = v$ again for all $g \in G$ implying that $f(v) = \rho(g.f(v)) = 0$. Thus we are done. G is reductive.
"$\Rightarrow$" Conversely assume that G is a reductive group and let $\rho : G \to GL(V)$ be a rational representation also let $\{0\} \neq W \subsetneq V$ be a G-stable subspace. We want to show that there exists a G-invariant complement of W. Consider the quotient vector space V/W . There is a canonical surjection $\pi : V \to V/W$. In fact, we can regard elements of V/W as equivalence classes of V formed by the canonical surjection as follows; for $v, w \in V$ $[v] = [w]$ if and only if $\pi(v) = \pi(w)$. Let $R = \{r \in Hom(V/W, V) \,|\, \pi \circ r = id_{V/W}\}$. Observe that $V = W \oplus r(V/W)$, direct sum of vector spaces, for any $r \in R$. Also note that we have $[r([v])] = [v]$ for any $v \in V$ since $\pi(r([v])) = \pi(v) = [v]$ by definition of r and V/W. However, of course $r(V/W)$ is not necessarily G-stable. Therefore if we can find an $r \in R$ such that $r(V/W)$ is G-stable then we would prove the implication that ρ is semi-simple. Note that the

induced action on Definition 2.1 gives another the rational representation $\overline{\rho} : G \to GL(V/W)$ as follows: $\overline{\rho}(g).[v] = [\rho(g).v]$ or equivalently $\overline{\rho}(g).\pi(v) = \pi(\rho(g).v)$. From Lemma 2.9 we know that there exists a G-invariant section $r' \in R$ i.e. $g.r' = r'$ for any $g \in G$. We claim that $r'(V/W)$ is a G-stable subspace. To see that this is correct, let $v \in V$, $g \in G$ be arbitrary and consider the action of g on $r'([v]) \in r'(V/W)$ as follows;

$$\begin{aligned}\rho(g).(r'([v])) &= \rho(g).(r'(\overline{\rho}(g^{-1})\overline{\rho}(g).[v])) = \rho(g).(r'(\overline{\rho}(g^{-1}).[\rho(g).v])) \\ &= (g.r')([\rho(g).v]) = r'([\rho(g).v]) \in r'(V/W)\end{aligned}$$

Hence, ρ is a semisimple representation.

$\square$

Chapter 3

Finite Generation of the Algebra of Invariants

Recall from the introduction that one of the main question was the following: Is algebra of invariants generated by finitely many elements over $\mathbb{C}$? The answer is yes for a particular case;

Theorem 3.1. *If $G \subset GL(V)$ is a reductive linear algebraic group, then $S(V)^G$ is a $\mathbb{C}$-algebra of finite type.*

In this chapter we will prove this theorem. In fact this will be deduced from a more general statement. Let's start with recalling some definitions and notions that will appear throughout this section.

Definition 3.2. A $\mathbb{C}$-algebra of finite type is a $\mathbb{C}$-algebra generated by finitely many elements.

Definition 3.3. A $\mathbb{C}$-algebra A is graded if A is a direct sum of its $\mathbb{C}$-subspaces

$$A = \bigoplus_{d \geq 0} A_d$$

where $A_d A_e \subset A_{d+e}$ for every d, $e \geq 0$. Nonzero elements of A_d are called homogeneous of degree d.

Definition 3.4. An ideal I of the graded $\mathbb{C}$-algebra A, that is not A itself, is called homogeneous if

$$I = \bigoplus_{d \geq 0} I \cap A_d$$

That is if $a = \sum_{d \geq 0} a_d$ where $a_d \in A_d$ lies in I then all a_d lies in I.

Definition 3.5. Let A be a subring B. The A-algebra B is said to be finite type over A if there are elements $b_1, b_2, \ldots, b_s \in B$ such that $B = A[b_1, b_2, \ldots, b_s]$

Definition 3.6. Let A be a subring of B. We say that $b \in B$ is integral over A if $f(b) = 0$ for some monic $f \in A[x]$. In other words $b \in B$ is integral over A if it is root of a monic polynomial which has coefficients from A. B is integral over A if every element of B is integral over A.

Lemma 3.7. *Let B be a $\mathbb{C}$-algebra and let A be a subalgebra. Assume that B is finite type over $\mathbb{C}$, and is integral over A. Then A is finite type over $\mathbb{C}$.*

Proof. Let $B = \mathbb{C}[b_1, b_2, \ldots, b_s]$. Each b_i satisfies a monic polynomial equation with coefficients in A as follows

$$b_i^{n_i} + a_{i1} b_i^{n_i - 1} + a_{i2} b_i^{n_i - 2} + \ldots + a_{in_i} = 0$$

Let $a_1, a_2, \ldots, a_t$ be the set of elements appearing as a coefficient in these equations. Define $A' := \mathbb{C}[a_1, a_2, \ldots, a_t]$. Observe that A' is a Noetherian ring because A' is a finitely generated $\mathbb{C}$-algebra. By the choice of generators of A', B is integral over A' which means that B is generated, as an A'-module, by finitely elements of type $b_1^{h_1} b_2^{h_2} \ldots b_s^{h_s}$ where $0 \leq h_i < n_i$. By construction A is an A'-submodule of B. We know that B is finitely generated module over a Noetherian ring A' therefore every submodule of B is finitely generated over A'. The relationship among A, A' and B is illustrated in the diagram below. Thus A is a finitely generated A'-module i.e. A is finite type over A'. The lemma follows.

$$\begin{array}{c} B \\ | \\ A \\ | \\ A' \\ | \\ \mathbb{C} \end{array}$$

□

Lemma 3.8. *If $G \subset GL(V)$ is a finite group then $S(V)$ is integral over $S(V)^G$.*

Proof. Let $f \in S(V)$; consider the polynomial $\prod_{g \in G}(x - g.f) \in S(V)[x]$. Clearly f is a root of this polynomial. Also observe that coefficient of $x^{|G|-i}$ is given by

$$(-1)^i \sum_{\substack{g_1, g_2, \ldots, g_i \in G \\ \text{all distinct}}} (g_1.f)(g_2.f)\ldots(g_i.f) \quad \in S(V)^G$$

□

Proposition 3.9. *Let $G \subset GL(V)$ be a finite group. $S(V)^G$ is a $\mathbb{C}$-algebra of finite type over $\mathbb{C}$.*

Proof. By Lemma 3.8 we can take $A = S(V)$ and $B = S(V)^G$ in the lemma 3.7. The result follows.

□

Now, let $G \subset GL(V)$ be a linear algebraic group. Let I and J be two G-stable ideals in $S(V)$. Assume that $I \subset J$. Define $A := S/I$ and $B := S/J$. There exists a canonical $\mathbb{C}$-algebra homomorphism as follows

$$\phi : A \twoheadrightarrow B$$

$$k + I \to k + J$$

Since I and J are G-stable ideals the action of G on S induces an action on the algebras A and B as follows; $g.(k+I) = g.k + I$ and $g.(k+J) = g.k + J$ which is a linear group action. That is, every element of G induces an automorphism on the algebras A and B. In that respect we have the following property for all $g \in G$;

$$\phi \circ g = g \circ \phi : A \to B$$

If I and J are homogeneous ideals then A and B are graded rings. Since G stabilizes the subspace S_d; it also stabilizes A_d and B_d. Moreover the action of G gives representations for the vector spaces A_d and B_d which are rational representations due to the fact that G is a linear algebraic group. Let A^G and B^G denote the algebra of invariants in A and B.

Lemma 3.10. *Using the notation and setup above, assume that G is linearly reductive. If $b \in B^G$ then there exists $a \in A^G$ such that $\phi(a) = b$. Equivalently, $\phi(A^G) = B^G$.*

Proof. Let $b \in B^G$. The case $b = 0$ is trivial. Let's assume $b \neq 0$. Choose $a_1 \in A$ such that $\phi(a_1) = b$. Since G is a linear algebraic group, the action of G on A is rational. Therefore the following set is a finite dimensional subspace of A;

$$W := Span_{\mathbb{C}}(g.a_1 | g \in G) \subset A$$

Define the following subspace

$$W' := Span_{\mathbb{C}}(g.a_1 - a_1 | g \in G) \subset W$$

First observe that W' is G-invariant; therefore by Proposition 2.13 it has a G-invariant complement W''. The equality $W = \mathbb{C}a_1 + W'$ is clear therefore $\dim W'' = 1$. This implies that $W'' \subset A^G$. Also observe that $\phi(g.a_1 - a_1) = g.\phi(a_1) - \phi(a_1) = g.b - b = 0$ but $\phi(g.a_1) = g.\phi(a_1) = g.b = b \neq 0$ by the commutativity of ϕ and g and by the fact that $b \in B^G$. So this means that there exists $a \in W'' \subset A^G$ such that $\phi(a) = \phi(a_1) = b$. Hence we are done. $\square$

Lemma 3.11. *Let A be a graded $\mathbb{C}$-algebra and let $I \subsetneq A$ be a finitely generated homogeneous ideal. If A/I is finite type over $\mathbb{C}$ then so is A.*

Proof. Let $I = y_1A + y_2A + \ldots + y_kA$ where all y_i are homogeneous of positive degree. Let $A/I = \mathbb{C}[\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n}]$ where $a_i \in A$ and $\overline{a_i}$ is its image under canonical surjective homomorphism $\pi : A \to A/I$. Then we claim that $A = \mathbb{C}[y_1, y_2, \ldots, y_k, a_1, a_2, \ldots, a_n]$. Let $x_0 \in A$ then $x_0 = y_1x_1 + y_2x_2 + \ldots + y_kx_k + p(a_1, a_2, \ldots, a_n)$ where $x_i \in A$ and $p \in \mathbb{C}[T_1, T_2, \ldots, T_n]$ a polynomial with n variables. For $x_i \in A$ again there is an expansion $x_i = y_1x_{i1} + y_2x_{i2} + \ldots + y_kx_{ik} + p_i(a_1, a_2, \ldots, a_n)$ where $x_{ij} \in A$. We can continue in this fashion; we know that it will stop because y_i's are of positive degree and as we iterate degrees of x_{ij}'s get smaller, eventually will become zero. Starting from the last step where every element from A is a combination of a_i's and plugging expansions back in to previous steps, we get $x = P(y_1, y_2, \ldots, y_k, a_1, \ldots, a_n)$ where $P \in \mathbb{C}[T_1, T_2, \ldots, T_{n+k}]$. Thus our claim holds.

□

Theorem 3.12. *Let G be a linearly reductive algebraic group. Let $I \subsetneq S$ be a homogeneous G-stable ideal of S, then $(S/I)^G$ is a $\mathbb{C}$-algebra of finite type.*

Proof. Assume that the statement does not hold. By the Noetherianity of S, we can take a maximal G-stable homogeneous ideal I of S where $(S/I)^G$ is not of finite type over $\mathbb{C}$. Notice that defining $A := S/I$, by maximality of I, for any nonzero G-invariant homogeneous ideal J of A the algebra $(A/J)^G$ must be finitely generated over $\mathbb{C}$. We have the canonical homomorphism $\psi : A^G \to (A/J)^G$ that is surjective by Lemma 3.10. Therefore $\psi(A^G)$ is of finite type over $\mathbb{C}$. It is easy to see that $\psi(A^G) \cong A^G/(A^G \cap J)$. Thus for any nonzero G-invariant homogeneous ideal J of A we can say that $A^G/(A^G \cap J)$ is of finite type over $\mathbb{C}$.

Now assume that $a \in A^G$ is homogeneous with positive degree. Consider two cases in here; a is not a zero divisor in A or a is a zero divisor in A. Assume the first case. Consider $ax \in aA \cap A^G$ for some $x \in A$, then

$g.(ax) = (g.a)(g.x) = a(g.x)$ and $g.(ax) = ax$ holds for all $g \in G$ by our choice of ax. That is $a(g.x - x) = 0$ for all $g \in G$ and a is not a zero divisor therefore $x \in A^G$ holds, proving that $aA \cap A^G \subset aA^G$. The other inclusion is trivial. We conclude that $aA \cap A^G = aA^G$. Taking the homogeneous ideal aA, by the previous paragraph $A^G/(A^G \cap aA) = A^G/(aA^G)$ is finitely generated over $\mathbb{C}$. Let $A^G/(aA^G) = \mathbb{C}[\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n}]$ where $a_i \in A^G$ and $\overline{a_i}$ is its image under canonical surjective homomorphism. Then Lemma 3.11 gives $A^G = \mathbb{C}[a, a_1, a_2, \ldots, a_n]$ which contradicts the definition of A. Thus we get a contradiction if a is not a zero divisor in A.

We may now assume that any homogeneous element of positive degree belonging to A^G is a zero divisor in A. Fix such an a and define $I_a := \{x \in A \,|\, ax = 0\}$. Clearly this is a G-invariant and homogeneous ideal and we proved that it is nonzero. Therefore $(A/I_a)^G \cong A^G/(A^G \cap I_a)$. We claim that $(A/I_a)^G$ is isomorphic to $(aA)^G$ as A^G-module. Define $\phi : (A/I_a)^G \to (aA)^G$ as follows; let $b \in A$ such that $\bar{b} \in (A/I_a)^G$; let $\phi(\bar{b}) = ab$. By choice of b, $g.b - b \in I_a$ implying that $g.(ab) - ab = (g.a)(g.b) - ab = a(g.b) - ab = a(g.b - b) = 0$, this verifies well-definedness. Let $ab_1 = ab_2$, then we have $a.(b_1 - b_2) = 0$, yielding $\overline{b_1} = \overline{b_2}$, thus ϕ is injective. Let $ab \in A^G$, then going backwards in the same equations above we get $\bar{b} \in (A/I_a)^G$ proving the surjectivity of ϕ. Now let $x \in A^G$, $x.\bar{b} = \overline{xb}$ showing that ϕ is an A^G-module homomorphism. As a result of the claim, $(aA)^G \cong (A/I_a)^G \cong A^G/(A^G \cap I_a)$ which shows that $(aA)^G$ is a finitely generated A^G-module. Recall that $A^G/(aA)^G \cong A^G/(aA \cap A^G)$ was finite type over $\mathbb{C}$ by the arguments in the first paragraph, and we know that $aA \cap A^G$ is a finitely generated A^G-module. Therefore using Lemma 3.11 we conclude that A^G is finitely generated over $\mathbb{C}$. Again a contradiction. Hence statement holds. $\square$

Corollary 3.13. *If $G \subset GL(V)$ is a reductive linear algebraic group, then $S(V)^G$ is a $\mathbb{C}$-algebra of finite type.*

Chapter 4

Poincarè Series

We introduce Poincarè series of graded algebras. This will help us to understand the structure of invariant algebra. We will prove Molien's theorem and use it to study reflection groups.
Throughout this chapter for all graded $\mathbb{C}$-algebras $M = \oplus_{d\in\mathbb{N}} M_d$ we will assume that $\dim_{\mathbb{C}} M_d < \infty$.

Definition 4.1. For a graded algebra $M = \oplus_{d\in\mathbb{N}} M_d$, Poincarè series of M is given by

$$P_T(M) = \sum_{i=0}^{\infty} (\dim_{\mathbb{C}} M_i) T^i$$

Proposition 4.2. *Let M, M', M'' be graded $\mathbb{C}$-algebras;*

i. $P_T(M \otimes_{\mathbb{C}} M') = P_T(M) P_T(M')$

ii. If $0 \to M' \to M \to M'' \to 0$ is an exact sequence of $\mathbb{C}$-algebras where M' is an ideal of M and homomorphisms of exact sequence are compatible with degrees, then

$$P_T(M) = P_T(M') + P_T(M'')$$

In particular, if $M = M' \oplus M''$ then equation above holds.

Proof. i. $(M \otimes_{\mathbb{C}} M')_d = \sum_{i+j=k} M_i \otimes_{\mathbb{C}} M'_j$. This implies

$$\dim_{\mathbb{C}}(M \otimes_{\mathbb{C}} M')_d) = \sum_{i+j=d} \dim_{\mathbb{C}}(M_i) \dim_{\mathbb{C}}(M'_j)$$

Thus, the equality follows.

ii. By the assumption on homomorphisms, $0 \to M'_d \to M_d \to M''_d \to 0$ is also an exact sequence. This gives $\dim_{\mathbb{C}}(M_d) = \dim_{\mathbb{C}}(M'_d) + \dim_{\mathbb{C}}(M''_d)$. Using this identity, the equality follows from definition.

□

Example 4.3. Let $M = \mathbb{C}[f]$ where $\deg(f) = d$. Then

$$P_T(M) = 1 + T^d + T^{2d} + T^{3d} + \ldots = \frac{1}{1 - T^d}$$

Example 4.4. Let $M = \mathbb{C}[f_1, f_2, \ldots f_n]$ where $\deg(f_i) = d_i$. Then $M = \mathbb{C}[f_1] \otimes \mathbb{C}[f_2] \otimes \cdots \otimes \mathbb{C}[f_n]$. By Proposition 4.2 (i) and previous example we have

$$P_T(M) = \left(\frac{1}{1 - T^{d_1}}\right)\left(\frac{1}{1 - T^{d_2}}\right) \cdots \left(\frac{1}{1 - T^{d_n}}\right)$$

From now on we will focus on finite groups, their invariant algebras. and Poincarè series of those invariant algebras. Therefore it is worth making a few remarks and showing some properties for this particular case. If $G \subset GL(V)$ is finite then it is a linear algebraic group, see Remark 2.5. Moreover it is reductive from Proposition 2.7. We also know that algebra of polynomial functions is integral over invariant algebra in that case from Lemma 3.8.

For the Poincarè series of invariant algebra of finite groups, we have a very useful theorem telling us description of it and using the theorem we can extract information about structure of invariant algebras. In particular, this theorem will help us to establish the natural connection between invariant algebras and finite reflection groups.

Theorem 4.5. *Let V be an n-dimensional $\mathbb{C}$-vector space and let $G \subset$*

$GL(V)$ be a finite group. Then we have

$$P_T(S^G) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I_{n\times n} - gI_T)} \quad , \quad I_T := TI_{n\times n}$$

To prove the Theorem, first we need to introduce new definitions and prove some lemmas using those.

Definition 4.6. A linear operator $g \in GL(V)$ induces an action on $S(V)$, in particular it induces a linear operator on S_d. We define $g_d : S_d(V) \to S_d(V)$ to be this induced linear operator.

Lemma 4.7. *Given V and $g \in GL(V)$ as above, then the following equality holds*

$$\sum_{d=0}^{\infty} \mathrm{tr}(g_d)T^d = \frac{1}{\det(I_{n\times n} - g^{-1}I_T)}$$

Proof. Choose a basis $\beta = \{t_1, t_2, \dots t_n\}$ for V such that $[g]_\beta$ is upper-triangular. Let $\lambda_1^{-1}, \lambda_2^{-1}, \dots, \lambda_n^{-1} \in \mathbb{C}$ be the diagonal entries of $[g]_\beta$. Such a basis exists because $\mathbb{C}$ is algebraically closed. Let $\beta' = \{T_1, T_2, \dots, T_n\}$ be the basis of V^* where $T_i = t_i^*$. Clearly $S(V) = \mathbb{C}[T_1, T_2, \dots, T_n]$. Observe that $[g_1]_{\beta'} = [g]_\beta^{-1}$. This shows that $[g_1]_{\beta'}$ is also an upper-triangular matrix with diagonal entries $\lambda_1, \lambda_2, \dots, \lambda_n \in \mathbb{C}$. Now for $S_d(V)$ we have the basis $\beta_d := \{T_1^{e_1} T_2^{e_2} \dots T_n^{e_n} \mid e_1 + e_2 + \dots + e_n = d\}$. Consider $[g_d]_{\beta_d}$ where β_d has lexicographic order; it is an upper-triangular matrix because $g.T_i \subset Span_{\mathbb{C}}(T_1, T_2, \dots, T_i)$. Moreover diagonal entries of $[g_d]_{\beta_d}$ is given by $\{\lambda_1^{e_1}\lambda_2^{e_2} \dots \lambda_n^{e_n} \mid e_1 + e_2 + \dots + e_n = d\}$. Thus we get

$$\mathrm{tr}(g_d) = \sum_{e_1+e_2+\dots+e_n=d} \lambda_1^{e_1}\lambda_2^{e_2} \dots \lambda_n^{e_n}$$

It follows from that

$$\begin{aligned}\sum_{d=0}^{\infty} \operatorname{tr}(g_d)T^d &= \sum_{d=0}^{\infty} \left(\sum_{e_1+e_2+\ldots+e_n=d} \lambda_1^{e_1}\lambda_2^{e_2}\ldots\lambda_n^{e_n} \right) T^d \\ &= \left(\sum_{e_1} \lambda_1^{e_1}T^{e_1}\right)\left(\sum_{e_2} \lambda_2^{e_2}T^{e_2}\right)\cdots\left(\sum_{e_n} \lambda_1^{e_n}T^{e_n}\right) \\ &= \frac{1}{1-\lambda_1 T}\frac{1}{1-\lambda_2 T}\cdots\frac{1}{1-\lambda_n T} = \frac{1}{\det(I_{n\times n} - g^{-1}I_T)}\end{aligned}$$

□

Lemma 4.8. *Let G be a finite group and let V be a G-module; then we have*

$$\dim_{\mathbb{C}} V^G = \frac{1}{|G|}\sum_{g\in G} \operatorname{tr}(g)$$

Proof. Here Maschke's theorem applies therefore V is completely reducible. Completely reducibility can be also shown using Proposition 2.11. V^G is the multiplicity of the trivial 1-dimensional representation in V. Each irreducible one dimensional subspace gives us trivial representation. Let $\varepsilon : G \to \mathbb{C}$ be the character of trivial representation; $\varepsilon(g) = 1$ for all $g \in G$. If we let $\chi : G \to \mathbb{C}$ to be character of the corresponding representation $\rho : G \to GL(V)$ i.e. $\chi(g) := tr(g)$ for all $g \in G$, then taking the standard inner product of χ with ε gives the number of trivial representations in ρ. Thus we write

$$\langle \chi, \varepsilon \rangle = \frac{1}{|G|}\sum_{g\in G} \chi(g)\overline{\varepsilon(g)} = \frac{1}{|G|}\sum_{g\in G} \chi(g) = \frac{1}{|G|}\sum_{g\in G} \operatorname{tr}(g) = \dim_{\mathbb{C}} V^G$$

□

Now we can prove Theorem 4.5.

Proof. It is already established that $S_d(V)$ is a G-module under the action

of g_d where $g \in G$ and $d \in \mathbb{N}$. Therefore by Lemma 4.8 we have the identity

$$\dim S_d^G(V) = \frac{1}{|G|} \sum_{g \in G} tr(g_d)$$

Substituting this in the Poincarè series and applying Lemma 4.7 gives the desired identity.

$$\begin{aligned} P_T(S(V)^G) &= \sum_{d=0}^{\infty} \dim S_d^G(V) T^d = \sum_{d=0}^{\infty} \frac{1}{|G|} \sum_{g \in G} tr(g_d) T^d \\ &= \frac{1}{|G|} \sum_{g \in G} \left(\sum_{d=0}^{\infty} tr(g_d) T^d \right) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I_{n \times n} - g^{-1} I_T)} \\ &= \sum_{g \in G} \frac{1}{\det(I_{n \times n} - g I_T)} \end{aligned}$$

□

Definition 4.9. An element $g \in GL(V)$, which is not identity, is called a reflection if it is diagonalizable, of finite order and fixes a hyperplane $H_g \subset V$ pointwise.

Lemma 4.10. *With the notation above,*

$$P_T(S(V)^G) = \frac{1}{|G|} \left(\frac{1}{(1-T)^n} + \frac{C_{n-1}}{(1-T)^{n-1}} + \cdots \right)$$

where $2C_{n-1} =$ *number of reflections in* G.

Proof. $P_T(S(V)^G)$ is a finite sum of rational polynomial functions. We consider the Laurent series expansion of $P_T(S(V)^G)$ at $1 \in \mathbb{C}$. Let $\lambda \neq 1$; then we expand $\frac{1}{1-\lambda T}$ around 1 as follows;

$$\begin{aligned} \frac{1}{1-\lambda T} &= \frac{1}{(1-\lambda) - \lambda(T-1)} = \frac{1}{1-\lambda} \frac{1}{1 - \frac{\lambda}{1-\lambda}(T-1)} \\ &= \frac{1}{(1-\lambda)} \left(1 + \frac{\lambda}{1-\lambda}(T-1) + \left(\frac{\lambda}{1-\lambda} \right)^2 (T-1)^2 + \cdots \right) \end{aligned}$$

This shows that only contribution to the principal part of Laurent series comes from elements in G which has 1 in the diagonal of its upper-triangular matrix form. Therefore $P_T(S(V)^G)$ has a pole of order n at 1 coming from $I_n \in G \subset GL(V)$. Note that only contribution to the term $\frac{1}{(1-T)^n}$ comes from identity element in G. To see this, assume that there exists an element $g \in G$ other than identity such that all diagonal entries in the upper-triangular form of its matrix is equal to 1. Then minimal polynomial of g is $(x-1)^k = 0$ for some integer $k \geq 2$. However $g^{|G|} = I_n$ and $(x-1)^k = 0$ does not divide $x^{|G|} - 1 = 0$ which is a contradiction since $x - 1$ is not minimal polynomial of g. Arguing similarly, observe that for any $g \in G$ minimal polynomial of g divides $x^{|G|} - 1$ which has $|G|$ many distinct complex roots,namely roots of unity; therefore minimal polynomial of g does not contain any linear polynomial with multiplicity more than one. This, together with the expansion above shows that only contribution to the term $\frac{1}{(1-T)^{n-1}}$ in the Laurent expansion comes from reflections. Thus, for a reflection s with the eigenvalue $\zeta_s \neq 1$, that contribution is $\frac{1}{1-\zeta_s}$.This tells us

$$C_{n-1} = \sum_{\substack{s \in G \\ s \text{ reflection}}} \frac{1}{1-\zeta_s}$$

Furthermore observe that if $s \in G$ is a reflection then so is $s^{-1} \in G$ and we have the identity

$$\frac{1}{1-\zeta_s} + \frac{1}{1-\zeta_s^{-1}} = 1$$

Note that if $\zeta_s = -1$ then $s = s^{-1}$ and this identity still holds. Moreover this also gives

$$C_{n-1} = \sum_{\substack{s \in G \\ s \text{ reflection}}} \frac{1}{1-\zeta_s^{-1}}$$

The lemma follows from these three identities

$$2C_{n-1} = \sum_{\substack{s \in G \\ s \text{ reflection}}} \frac{1}{1-\zeta_s} + \sum_{\substack{s \in G \\ s \text{ reflection}}} \frac{1}{1-\zeta_s^{-1}} = \sum_{\substack{s \in G \\ s \text{ reflection}}} 1$$

□

Here G is linearly reductive and by Theorem 3.12 S^G is finitely generated over $\mathbb{C}$. Moreover, S is integral over S^G therefore Noether normalization Theorem tells us that there exists n algebraically independent elements $f_1, f_2, \ldots, f_n$ such that S^G is integral over $\mathbb{C}[f_1, f_2, \ldots, f_n]$. This gives us an idea of the Poincarè series.

Proposition 4.11. *Let M be a graded $\mathbb{C}$-algebra that is integral over $\mathbb{C}[f_1, f_2, \ldots, f_n]$ with f_i's algebraically independent and $\deg f_i = d_i$. Then there exists a polynomial $h(T) \in \mathbb{C}[T]$ such that*

$$P_T(M) = h(T) \prod_{i=1}^{n} \frac{1}{1 - T^{d_i}}$$

Proof. We prove this statement by induction on n. If $n = 0$ then $P_T(M) = 1$ which is a polynomial. Assume that the statement holds for algebras that are integral over polynomial algebras with fewer than n generators. Consider the $\mathbb{C}$-algebra homomorphism

$$\begin{aligned} \pi : M &\to M \\ s &\to s f_n \end{aligned}$$

This gives $\mathbb{C}$-algebra isomorphism $M/\ker \pi \cong \text{Im } \pi$. By definition of π we then have $(M/\ker \pi)_d \cong (\text{Im } \pi)_{d+d_n}$. Therefore

$$P_T(M/\ker \pi) = T^{-d_n} P_T(\text{Im } \pi)$$

We have exact sequences of $\mathbb{C}$-algebras that are compatible with degrees

$$0 \to \ker \pi \to M \to M/\ker \pi \to 0$$
$$0 \to \text{Im } \pi \to M \to M/\text{Im } \pi \to 0$$

Clearly $\ker \pi$ and $\text{Im } \pi$ are ideals of M so we can apply Proposition 4.2 part

(i). This and a previous remark gives

$$P_T(M) = P_T(\ker \pi) + P_T(M/\ker \pi) = P_T(\ker \pi) + T^{-d_n} P_T(\mathrm{Im}\ \pi) \quad (4.1)$$

$$P_T(M) = P_T(\mathrm{Im}\ \pi) + P_T(M/\mathrm{Im}\ \pi) \quad (4.2)$$

Multiplying (4.1) by T^{d_n} and subtracting from (4.2) gives

$$(1 - T^{d_n}) P_T(M) = P_T(M/\mathrm{Im}\ \pi) - T^{d_n} P_T(\ker \pi) \quad (4.3)$$

We will show that we can use induction argument for the RHS of (4.3). Firstly we claim that $M/\mathrm{Im}\ \pi$ is integral over $\mathbb{C}[\overline{f_1}, \overline{f_2}, \ldots, \overline{f_{n-1}}]$ where $\overline{f_i} \in M/\mathrm{Im}\ \pi$ is the image of f_i under the canonical projection map. Let $s \in S^G$, it is integral over $\mathbb{C}[f_1, f_2, \ldots, f_n]$ by assumption which gives us a monic polynomial $\sum_{i=0}^{k_s} a_i X^i$ where $a_i \in \mathbb{C}[f_1, f_2, \ldots, f_n]$ such that s is a root. Using this polynomial, construct the monic polynomial $\sum_{i=0}^{k_s} \overline{a_i} X^i$; clearly $\overline{s}$ is a root for this and $\overline{a_i} \in \mathbb{C}[\overline{f_1}, \overline{f_2}, \ldots, \overline{f_{n-1}}]$ since $\overline{f_n} = 0$ so our claim holds. Therefore induction hypothesis is valid for $P_T(M/\mathrm{Im}\ \pi)$. That is, there exists a polynomial $h_1(T) \in \mathbb{C}[T]$ such that

$$P_T(M/\mathrm{Im}\ \pi) = h_1(T) \prod_{i=1}^{n-1} \frac{1}{1 - T^{d_i}}$$

Similarly, any element $s \in \ker \pi$ is integral over $\mathbb{C}[f_1, f_2, \ldots, f_{n-1}]$ because $s f_n = 0$. Therefore induction hypothesis also holds for $\ker \pi$ which gives

$$P_T(\ker \pi) = h_2(T) \prod_{i=1}^{n-1} \frac{1}{1 - T^{d_i}}$$

for some polynomial $h_2(T) \in \mathbb{C}[T]$. Plugging in last two expansions and dividing both sides of (4.3) by $(1 - T^{d_n})$ gives us the desired result. $\square$

Corollary 4.12. *Let $G \subset GL(V)$ be finite and S^G is integral over $\mathbb{C}[f_1, f_2, \ldots, f_n]$ with f_i's algebraically independent and $\deg f_i = d_i$. Then there exists*

a polynomial $h(T) \in \mathbb{C}[T]$ *such that*

$$P_T(S^G) = h(T) \prod_{i=1}^{n} \frac{1}{1 - T^{d_i}}$$

In the next chapter we will show that S^G is not just integral over $\mathbb{C}[f_1, f_2, \ldots, f_n]$ for some $f_i \in S^G$ algebraically independent but also equal to it if G is finitely generated reflection group. We will also show that the converse of this statement holds, thus we have a characterization. The following lemma helps us to prove converse of the statement in the next chapter. We put it in this chapter because we use the arguments in this chapter.

Lemma 4.13. *Suppose* $S^G = \mathbb{C}[f_1, f_2, \ldots, f_n]$ *where* $\deg f_i = d_i$. *Then*

i. $|G| = d_1 d_2 \ldots d_n$

ii. the number of reflections in G *is* $\sum_{i=1}^{n}(d_i - 1)$

Proof. It follows from Example 4.4 that

$$P_T(S^G) = \left(\frac{1}{1 - T^{d_1}}\right)\left(\frac{1}{1 - T^{d_2}}\right)\cdots\left(\frac{1}{1 - T^{d_n}}\right)$$

$$= \frac{1}{(1-T)^n \prod_{i=1}^{n}(1 + T + T^2 + \ldots + T^{d_i - 1})}$$

On the other hand from the Lemma 4.10

$$P_T(S^G) = \frac{1}{|G|}\left(\frac{1}{(1-T)^n} + \frac{C_{n-1}}{(1-T)^{n-1}} + \cdots\right)$$

and $2C_{n-1}$ is number of reflections in G. Multiplying both expressions by $(1-T)^n$ gives the following equality

$$\frac{1}{\prod_{i=1}^{n}(1 + T + \ldots + T^{d_i - 1})} = \frac{1}{|G|}\left(1 + C_{n-1}(1-T) + \ldots\right) \tag{4.4}$$

Rewriting the same equality as follows

$$|G| = \left(1 + C_{n-1}(1-T) + C_{n-2}(1-T)^2 + \dots\right) \prod_{i=1}^{n} (1 + T + T^2 + \dots + T^{d_i - 1})$$

Plug in $T = 1$ and we get $|G| = d_1 d_2 \dots d_n$
For the second part take derivative of (4.4) and we get

$$\frac{1}{\prod_{i=1}^{n}(1 + T + T^2 + \dots + T^{d_i-1})} \left(-\sum_{i=1}^{n} \frac{1 + 2T + \dots + (d_i - 1)T^{d_i - 2}}{1 + T + \dots + T^{d_i - 1}} \right)$$

$$= \frac{1}{|G|} \left(-C_{n-1} - 2C_{n-2}(1-T) - \dots\right)$$

Again evaluating both sides at $T = 1$ gives

$$\frac{1}{d_1 d_2 \dots d_n} \left(-\sum_{i=1}^{n} \frac{d_i(d_i - 1)}{d_i} \right) = -\frac{1}{|G|} C_{n-1}$$

After using the identity in part *i.* and simplification this gives $C_{n-1} = \sum_{i=1}^{n}(d_i - 1)$. $\square$

Chapter 5

Invariant Algebras of Finite Reflection Groups

In this chapter I denotes the ideal of S generated by homogeneous elements of S^G of positive degree.

Lemma 5.1. *Let $(e_\alpha)_{\alpha\in A}$ be a set of homogeneous elements from S such that $(\overline{e_\alpha})_{\alpha\in A}$ is a basis for the vector space S/I, then S is generated by $(e_\alpha)_{\alpha\in A}$ as an S^G-module.*

Proof. Let M be the S^G-module generated by elements $(e_\alpha)_{\alpha\in A}$. We want to show that $M = S$, in particular $M_d = S_d$. We apply induction on d. The base case $d = 0$ is clear as $M_0 = S_0 = \mathbb{C}$. Assume the lemma holds for S_e, where $e < d$ and let $f \in S_d$. Considering $\overline{f} \in S/I$ and our assumption, we can expand f in S as follows;

$$f = \sum_\alpha c_\alpha e_\alpha + \sum_\beta f_\beta i_\beta$$

where the sums are finite with $c_\alpha \in \mathbb{C}$, $i_\beta \in S^G$ and $f_\beta \in S$ homogeneous with degree smaller than d. By the induction assumption $f_\beta \in M$ therefore $f \in M_d$. $\square$

Definition 5.2. A finite group $G \subset GL(V)$ is called a finite reflection group if it is generated by reflections.

Proposition 5.3. *Let G be a finite reflection group and let $y_1, y_2, \ldots, y_n$ be homogeneous elements of S such that $\overline{y_1}, \overline{y_2}, \ldots, \overline{y_n} \in S/I$ linearly independent in S/I with the previous notation. Then $y_1, y_2, \ldots, y_n$ are linearly independent over S^G.*

The proof of this proposition relies on Lemma 5.5 which uses the maps $\Delta_s : S(V) \to S(V)$ associated to reflections s in G. This map has a nice multiplicative property. We deal with the maps first then prove the lemma.

Δ maps

Let $s \in G$ be a reflection; s fixes a hyperplane of V, call this H_s. There exists a nonzero element $l_s \in V^*$ such that $l_s(H_s) = 0$ and such an l_s is unique up to a nonzero constant. Let ζ_s be the eigenvalue of s different from 1 and let $v_s \in V$ be the eigenvector of ζ_s. Now take l_s so that

$$s.v = v + l_s(v)v_s$$

That is, choose it so that $l_s(v_s) = \zeta_s - 1$. Recall that if s is a reflection then so is s^{-1} with eigenvalue ζ_s^{-1} different from 1. It follows that

$$s^{-1}.v = v - \zeta_s^{-1} l_s(v)v_s$$

Let $f \in S$ and $v \in V$ be arbitrary, then we have

$$(s.f)(v) = f(s^{-1}.v) = f(v - \zeta_s^{-1} l_s(v)v_s) = f(v) - \zeta_s^{-1} l_s(v) f(v_s)$$

This shows l_s divides $s.f - f$ for all $f \in S$. This allows us to write

$$s.f = f + l_s \cdot (\Delta_s(f))$$

This is how Δ_s is defined. It is apparent from the definition that Δ_s maps S_d into S_{d-1}.

Lemma 5.4. *For the map $\Delta_s : S(V) \to S(V)$ we have the multiplicative*

identity for any $f, g \in S$

$$\Delta_s(fg) = f \cdot (\Delta_s(g)) + g \cdot (\Delta_s(f)) + l_s \cdot (\Delta_s(f)) \cdot (\Delta_s(g))$$

Proof. This follows from

$$s.(fg) = (s.f) \cdot (s.g) = (f + l_s \cdot (\Delta_s(f)) \cdot (g + l_s \cdot (\Delta_s(g))$$

□

Lemma 5.5. *Let* $x_i \in S^G$ *and* $y_i \in S$ *for* $1 \leq i \leq m$ *be homogeneous elements such that* $x_1y_1 + x_2y_2 + \ldots + x_my_m = 0$. *If* $x_1 \notin S^Gx_2 + S^Gx_3 + \ldots + S^Gx_m$ *then* $y_1 \in I$.

Proof. We will apply induction on $d = \deg y_1$. We will denote the Reynolds operator by $P = |G|^{-1} \sum_{g \in G} g$. Consider the base case $d = 0$. We have $y_1 \notin I$ because I is generated by elements which has positive degree. For the base case we are trying to prove contrapositive of the statement. Notice that $x_1 = x_2z_2 + x_3z_3 + \ldots + x_mz_m$ where $z_i = y_i/y_1$. Applying Reynold's operator on both sides we get; $x_1 = x_2P(z_2) + x_3P(z_3) + \ldots + x_mP(z_m) \in S^Gx_2 + S^Gx_3 + \ldots + S^Gx_m$, since P is a projection onto S^G. Now assume the assertion for lower degrees and let $d = \deg y_1$. We are trying to prove the statement itself. Fixing a reflection $s \in G$, apply the Δ_s operator to the equality $x_1y_1 + x_2y_2 + \ldots + x_my_m = 0$. We have $\Delta_s(x_i) = 0$ because $s.x_i = x_i$; combining this with the multiplicative identity for Δ_s we get $x_1\Delta_s(y_1) + x_2\Delta_s(y_2) + \ldots + x_m\Delta_s(y_m) = 0$. $\deg \Delta_s(y_1) < \deg y_1$, therefore by induction assumption $\Delta_s(y_1) \in I$; implying that $s.y_1 - y_1$ is in I. This holds for any reflection $s \in G$. Consider $g.y_1 - y_1$; $g = s_1s_2 \ldots s_k$ for some reflections $s_1, s_2, \ldots, s_k \in G$ using this we can rewrite $g.y_1 - y_1$ as the following telescoping sum:

$$s_1s_2 \ldots s_{k-1}(s_k.y_1 - y_1) + s_1s_2 \ldots s_{k-2}.(s_{k-1}y_1 - y_1) + \ldots + (s_1y_1 - y_1) \in I$$

knowing that $s_iy_1 - y_1 \in I$. That is $g.y_1 - y_1 \in I$ for any $g \in G$. Therefore $P(y_1) - y_1 \in I$, which in turn implies that $y_1 \in I$ because $P(y_1) \in S^G$ and

$\deg P(y_1) > 0$. This establishes the claim. $\square$

Proof of Proposition 5.3. We use induction on n. Base case is $n = 1$ and it is trivial. Assume that statement holds numbers smaller than n. Let $x_1y_1 + x_2y_2 + \cdots + x_ny_n = 0$ where $x_i \in S^G$. By the previous lemma and the fact that $y_1 \notin I$ we are able to write $x_1 = z_2x_2 + z_3x_3 + \cdots + z_nx_n$ with $z_i \in S^G$. Thus the former equality becomes

$$x_2(y_2 + z_2y_1) + \ldots + x_n(y_n + z_ny_1) = 0$$

Observe that $\overline{y_2 + z_2y_1} = \overline{y_2}$ since $\deg z_2 > 0$ i.e. $z_2 \in I$ (otherwise we get a contradiction with the assumption that $\overline{y_1}, \overline{y_2}, \ldots, \overline{y_n}$ are linearly independent in S/I). This tells us that $\overline{y_2 + z_2y_1}, \ldots, \overline{y_n + z_ny_1}$ are linearly independent and by induction assumption $y_2 + z_2y_1, \ldots, y_n + z_ny_1$ are linearly independent over S^G. That is $x_2 = x_3 = \cdots = x_n = 0$. This makes $x_1 = 0$. Thus we are done.

$\square$

Theorem 5.6. *The following are equivalent for a finite group $G \subset GL(V)$ where $\dim V = n$:*

1. *G is a finite reflection group;*
2. *S is a free graded module over S^G with a finite basis;*
3. *S^G is generated by n algebraically independent homogeneous elements.*

Proof. $1 \Rightarrow 2$: Define the quotient field of S, call it K; and the quotient field of S^G, call it K^G. We can view G as a finite group of automorphisms on K. In this case K^G is the fixed field of G therefore K is a finite extension of K^G (see [7] pg.264). Now let the set $(e_\alpha)_{\alpha \in A}$ be as defined in Lemma 5.1; Proposition 5.3 together with Lemma 5.1 gives us that S is a free module over S^G with basis $(e_\alpha)_{\alpha \in A}$. So we only need to show that the basis is finite. To see that, observe that $(e_\alpha)_{\alpha \in A}$ is also a basis for K over K^G. Let $\frac{a}{b} \in K$,

$a, b \in S$ be arbitrary; then

$$\frac{a}{b} = \frac{a \prod\limits_{\substack{g \in G \\ g \neq 1_G}} g.b}{\prod\limits_{g \in G} g.b}$$

Denominator is in S^G and nominator can be rewritten as finite S^G-linear combination of $(e_\alpha)_{\alpha \in A}$'s. That is, any element in K is a K^G-linear combination of $(e_\alpha)_{\alpha \in A}$'s. Moreover the set $(e_\alpha)_{\alpha \in A}$ is clearly linearly independent over K^G by Proposition 5.3. Here we already know that K is a finite extension of K^G therefore this information is enough to conclude that $(e_\alpha)_{\alpha \in A}$ is a basis for K over K^G. In fact degree of extension is $|G|$, i.e. basis consists of $|G|$ many elements(see [7] pg.264).

$2 \Rightarrow 3$: S is integral over S^G. It follows from Lemma 3.7 that S^G is finite type over $\mathbb{C}$ because S is finite type over $\mathbb{C}$. Let $\{f_1, f_2, \ldots, f_m\}$ be the set of generators with minimum cardinality where every element is homogeneous. That is $S^G = \mathbb{C}[f_1, f_2, \ldots, f_m]$. Now we will prove that these elements are algebraically independent.

Assume that $f_1, f_2, \ldots, f_m$ are not algebraically independent. Then there exists a polynomial $P(x_1, x_2, \ldots, x_m) \in \mathbb{C}[x_1, x_2, \ldots, x_m]$ such that

$$P(f_1, f_2, \ldots, f_m) = 0$$

Assume that P has minimal degree and that each monomial in P has the same weight. Note that weight of a monomial $x_1^{e_1} x_2^{e_2} \ldots x_m^{e_m}$ is given by $d_1 e_1 + d_2 e_2 + \ldots + d_m e_m$ where $d_i = \deg f_i$. We write $S = \mathbb{C}[T_1, T_2 \ldots, T_n]$ and let

$$P_i = \frac{\partial P}{\partial x_i}(f_1, f_2, \ldots, f_m) \ (1 \leq i \leq m) \text{ and } f_{ij} = \frac{\partial f_i}{\partial T_j} \ (1 \leq i \leq m, \ 1 \leq j \leq n)$$

Observe that $P_i \in S^G$ and not all of them are zero since $P \neq 0$. Consider all monomials $x_1^{e_1} \ldots x_i^{e_i} \ldots x_m^{e_m}$ in P with $e_i \neq 0$; then $\frac{\partial P}{\partial x_i}$ is sum of $e_i x_1^{e_1} \ldots x_i^{e_i - 1} \ldots x_m^{e_m}$ and all this monomials have the same weight;

$d_1e_1 + \ldots + d_i(e_i - 1) + \ldots + d_me_m$. Therefore P_i's are sums of monomials of the same weight evaluated at $(f_1, f_2, \ldots, f_m)$; which tells us that P_i's are homogeneous elements of S^G. Consider the ideal $(P_1, P_2, \ldots, P_m) \subset S$ and assume that $\{P_1, P_2 \ldots, P_k\}$ is a minimal set of generators for this ideal.

Write

$$P_j = \sum_{i=1}^{k} s_{ij}P_i \ , \ s_{ij} \in S \ , \ k+1 \leq j \leq m \tag{5.1}$$

If we differentiate $P(f_1, f_2, \ldots, f_m) = 0$ with respect to T_j, the chain rule gives

$$\sum_{i=1}^{m} P_i f_{ij} = 0$$

Substituting (5.1) for P_i where $k+1 \leq i \leq m$ we get

$$\sum_{i=1}^{k} P_i \cdot (f_{ij} + \sum_{l=k+1}^{m} s_{il} f_{lj}) = 0$$

Put

$$u_{ij} = f_{ij} + \sum_{l=k+1}^{m} s_{il} f_{lj} \tag{5.2}$$

This gives

$$\sum_{i=1}^{k} P_i u_{ij} = 0 \tag{5.3}$$

Now since S is a free S^G-module, we can choose a homogeneous basis e_r such that

$$S = \bigoplus_r S^G e_r$$

In particular, it can be arranged so that $e_r = 1$ for some r. That is, we can arrange so that S^G is a summand in this direct sum.

Now we claim that $u_{ij} \in (f_1, f_2, \ldots, f_m) \subset S$. We know that $u_{ij} \in S$, therefore we have the decomposition

$$u_{ij} = \sum_r \rho_{ijr} e_r \ , \ \rho_{ijr} \in S^G \tag{5.4}$$

Plug this expansion into (5.3)

$$0 = \sum_{i=1}^{k} P_i u_{ij} = \sum_{i=1}^{k} P_i \cdot (\sum_r \rho_{ijr} e_r) = \sum_r (\sum_{i=1}^{k} P_i \rho_{ijr}) e_r$$

This tells us that $\sum_{i=1}^{k} P_i \rho_{ijr} = 0$ for any j, r. Here ρ_{ijr} are viewed as polynomials with variables $T_1, T_2, \ldots, T_n$ and they can be taken to be homogeneous. This tells us that for these polynomials, if the constant term is nonzero then they are constants. Observe that none of ρ_{ijr} is constant because otherwise we get a contradiction with the minimality of the generating set $\{P_1, P_2 \ldots, P_k\}$. We see that $\rho_{ijr} \in S^G = \mathbb{C}[f_1, f_2, \ldots, f_m]$ and has constant term zero, therefore it is equal to combination of $f_1, f_2, \ldots, f_m$, plugging this expansion of ρ_{ijr} into the (5.4) we see that u_{ij} belongs to the ideal of S generated by $f_1, f_2, \ldots, f_m$. Claim is proved.

We have the Euler identity;

$$d_i f_i = \sum_{j=1}^{n} f_{ij} T_j \ , \text{ where } d_i = \deg f_i$$

Using u_{ij} and Euler identity again along the way, we can rewrite RHS as follows;

$$\begin{aligned} d_i f_i &= \sum_{j=1}^{n} (u_{ij} T_j - \sum_{l=k+1}^{m} s_{il} f_{lj}) T_j = \sum_{j=1}^{n} u_{ij} T_j - \sum_{j=1}^{n} \sum_{l=k+1}^{m} s_{il} f_{lj} T_j \\ &= \sum_{j=1}^{n} u_{ij} T_j - \sum_{l=k+1}^{m} s_{il} \cdot (\sum_{j=1}^{n} f_{lj} T_j) = \sum_{j=1}^{n} u_{ij} T_j - \sum_{l=k+1}^{m} s_{il} \cdot (d_l f_l) \\ &= \sum_{j=1}^{n} u_{ij} T_j - \sum_{l=k+1}^{m} d_l s_{il} f_l \end{aligned}$$

We know that u_{ij} can be written as S-linear combination of $f_1, f_2, \ldots, f_m$ and clearly the second term on the RHS is also S-linear combination of $f_1, f_2, \ldots, f_m$. Therefore, expanding RHS and taking the degree d_i compo-

nent of both sides, we get

$$f_i = \sum_{i \neq j} \lambda_j f_j \ , \ \lambda_j \in S$$

We have $f_i \in S^G$ and $e_r = 1$ for some r. Now if we expand the coefficients λ_j with respect to decomposition $S = \bigoplus_r S^G e_r$ and take the component lying in the summand S^G; we get the following relation

$$f_i = \sum_{i \neq j} \bar{\lambda_j} f_j \ , \ \bar{\lambda_j} \in S^G$$

Note that none of the $\bar{\lambda_j}$'s contains f_i as a component because we only took degree d_i component of each side earlier. Thus, this relation contradicts the choice of $\{f_1, f_2, \ldots, f_m\}$. This set is algebraically independent. The quotient field of S is integral over the quotient field of S^G and transcendence degree former field is n, therefore $m = n$.

$3 \Rightarrow 1$: Assume $S^G = \mathbb{C}[f_1, f_2, \ldots, f_n]$ with $d_i = \deg f_i$. Let H be the subgroup of G generated by reflections of G. H is a finite reflection group and we proved that $S^H = \mathbb{C}[g_1, g_2, \ldots, g_n]$ where $e_i = \deg g_i$ and g_i's are homogeneous. We can assume that

$$d_1 \leq d_2 \leq \ldots \leq d_n \ \text{ and } \ e_1 \leq e_2 \leq \ldots \leq e_n$$

We claim that $d_i \geq e_i$ for all i. To see that first observe $S^G \subset S^H$. Now assume $d_i < e_i$, this implies that f_i can be written as a polynomial in $\{g_1, g_2, \ldots g_{i-1}\}$. Since $d_{i-1} \leq d_i$, f_{i-1} can be written as a polynomial in $\{g_1, g_2, \ldots, g_{i-1}\}$. In general we find that there is an inclusion $\mathbb{C}[f_1, f_2, \ldots, f_i] \hookrightarrow \mathbb{C}[g_1, g_2, \ldots, g_{i-1}]$ which is a contradiction with $\{f_1, f_2, \ldots, f_i\}$ being algebraically independent.

Both G and H contain the same number of reflections by the choice of H; and by the second part of Lemma 4.13 the number of reflections in G and H respectively are $\sum_{i=1}^n (d_i - 1) = \sum_{i=1}^n (e_i - 1)$.

Combining these two, we see that $d_i = e_i$ for all i. By the first part of

Lemma 4.13 $|G| = \prod_{i=1}^{n} d_i$ and $|H| = \prod_{i=1}^{n} e_i$. Having $H \leq G$, we conclude that $H = G$. Thus G is a finite reflection group.

$\square$

Chapter 6

Classification and Examples

Proposition 6.1. *Suppose $G \subset GL(V)$ is a finite reflection group, then there exists a decomposition $V = V_1 \oplus V_2 \oplus \cdots \oplus V_r$ and a decomposition $G = G_1 \times G_2 \times \ldots \times G_r$ such that $G_i \subset GL(V_i)$ where V_i is an irreducible G-invariant subspace and G_i is a finite reflection group.*

Proof. Let $H := \{g_1, \ldots, g_n\}$ where g_i's are reflections and $G = \langle H \rangle$. G is a finite group therefore reductive therefore V is completely reducible. i.e we have G-invariant irreducible subspaces V_i such that $V = V_1 \oplus V_2 \oplus \cdots \oplus V_r$. Take a reflection $g \in G$ with eigenvalues 1 and ζ. Observe that $g.V_i = V_i$ therefore V_i should be generated by eigenvectors of g. If V_i doesn't contain the eigenvector of g corresponding to the eigenvalue ζ, then it fixes V_i. Observe also that there is only one irreducible subspace V_i that g doesn't fix. For that V_i, $g|_{V_i}$ has eigenvalues $+1, \zeta$ corresponding to $(\dim V_i - 1)$ and 1 many eigenvectors respectively. That is, $g|_{V_i} \in GL(V_i)$ is a reflection in that case. This property gives a partition on H. Define $G_i := \langle \{g \in H | \ g \text{ doesn't fix } V_i\} \rangle$. Clearly for $1 \leq i \leq r$, G_i is a finite reflection group and $G_i \subset GL(V_i)$ by previous remark. Note that $G_i \cap G_1 G_2 .. \widehat{G_i} .. G_r = 1_G$ by construction. Take two arbitrary elements g_i, g_j such that $g_i \in G_i$, $g_j \in G_j$. We claim that they commute. Take an arbitrary element $v \in V$, we have decomposition $v = v_1 + v_2 + \ldots + v_r$ where $v_i \in V_i$. Observe that g_j fixes every component but v_j and similarly g_i fixes every component but v_i because of the choice of g_i and g_j. Therefore we have $(g_i g_j).v =$

$g_i.(g_j.(v_1+v_2+\ldots+v_r)) = g_i.(v+g_j.v_j-v_j) = v+g_j.v_j-v_j+g_i.v_i-v_i$. Similarly we have $(g_jg_i).v = g_j.(g_i.(v_1+v_2+\ldots+v_r)) = g_j.(v+g_i.v_i-v_i) = v+g_i.v_i-v_i+g_j.v_j-v_j$. Thus $g_ig_j = g_jg_i$. Next we claim that there is an isomorphism $\varphi : G_1\times G_2\times\ldots\times G_r \to G$. Define $\varphi(g_1,g_2,\ldots g_r) = g_1g_2\ldots g_r$. It is well defined; let $\varphi(g_1,g_2,\ldots g_r) = g_1g_2\ldots g_r = g$ and $\varphi(g_1',g_2',\ldots g_r') = g_1'g_2'\ldots g_r' = g'$ then $gg' = g_1g_1'g_2g_2'\ldots g_rg_r'$ and $g'g = g_1'g_1g_2'g_2\ldots g_r'g_r$. This map is surjective; take any element g in G. It can be written as product of reflections from H i.e $g = h_1h_2\ldots,h_k$ for some $k\in\mathbb{N}$ and $h_1,h_2\ldots h_k\in H$. Using the commutativity of the elements belonging to different G_i's, we can regroup $h_1,h_2,\ldots,h_k$ so that we get $g = g_1g_2\ldots g_r$ where $g_i\in G_i$. φ is also injective; assume $g = g_1g_2\ldots g_r$ and also $g = g_1'g_2'\ldots g_r'$ then multiplying both products by $g_1'^{-1}g_2^{-1}\ldots g_r^{-1}$ and using commutativity gives $g_1g_1'^{-1} = g_2'g_2^{-1}\ldots g_r'g_r^{-1}$. LHS belongs to G_1 whereas RHS belongs to $G_2G_3...G_r$ therefore both are equal to 1_G which proves the injectivity. Thus φ gives an isomorphism. To establish the last statement, define $\phi_i(g_i) := \phi(g_i)|_{V_i}$ for $g\in G_i$. The map $\phi_i : G_i\to GL(V_i)$ gives a reflection group by a previous remark. Now take an arbitrary element $v\in V$, we have decomposition $v = v_1+v_2\ldots+v_r$ where $v_i\in V_i$. Take an arbitrary $g\in G$ we have decomposition $g = g_1g_2\ldots g_r$ where $g_i\in G_i$. Therefore we have following equalities: $g.v = \phi(g).v = \phi(g_1g_2\ldots g_r).v = \phi(g_1)\phi(g_2)\ldots\phi(g_r).v = \phi(g_1)\phi(g_2)\ldots\phi(g_r).(v_1+v_2\ldots+v_r) = \phi(g_1).v_1+\phi(g_2)v_2\ldots\phi(g_r)v_r$. Hence the result follows.

□

Definition 6.2. Let $G\subset GL(V)$ be a finite reflection group. If V is an irreducible G-module then we call G an irreducible finite reflection group. In that case the rank of G is given by $\dim_{\mathbb{C}} V$.

It follows from this proposition that any complex finite reflection group is a product of irreducible complex finite reflection groups. So it is enough to study irreducible complex finite reflection groups and their invariant algebras. This classification is due to Shephard and Todd in 1954 [2]. It consists of 3 infinite families and 34 exceptional groups. The 3 infinite families are symmetric groups as will be shown in the following proposition, cyclic groups

$\mathbb{Z}/m\mathbb{Z}$ and imprimitive reflection groups which is defined below.

Proposition 6.3. *Let $V = \mathbb{C}^n$ and S_n permutes the coordinates $(x_1, x_2, \ldots, x_n)$. Define the hyperplane $W := \{(x_1, x_2, \ldots, x_n) \in \mathbb{C}^n | \sum_{i=1}^{n} x_i = 0\}$. S_n stabilizes W and therefore $S_n \subset GL_{n-1}(\mathbb{C})$. Using this inclusion, S_n is a finite reflection group. Moreover $S(W)^{S_n} = \mathbb{C}[f_2, f_3, \ldots, f_n]$ where $f_2, f_3, \ldots, f_n \in S(W)$ with $\deg f_i = i$.*

Proof. By definition we have $S(W) \cong \mathbb{C}[x_1, x_2 \ldots, x_n]/\langle x_1 + x_2 + \ldots + x_n\rangle$. Let $\pi : S(V) \cong \mathbb{C}[x_1, x_2, \ldots, x_n] \to S(W) \cong \mathbb{C}[x_1, x_2, \ldots, x_n]/\langle x_1+x_2+\ldots+x_n\rangle$ be the natural projection. We know that $S(V)^{S_n} = \mathbb{C}[f_1, f_2, \ldots, f_n]$ where f_i are the elementary symmetric polynomials of degree i (see [7] pg. 191). That is we have $S(W) \cong \mathbb{C}[x_1, x_2, \ldots, x_n]/\langle f_1\rangle$. Let $\overline{f_i} := \pi(f_i)$. Note that we have $\sigma.\overline{f_i} = \overline{\sigma.f_i}$ for any $\sigma \in S_n$. From this we conclude that $\mathbb{C}[\overline{f_2}, \overline{f_3}, \ldots, \overline{f_n}] \subset S(W)^{S_n}$. Now let's take an arbitrary element $\overline{f} \in S(W)^{S_n}$. We claim that there exists a $g \in \pi^{-1}(\overline{f})$ such that $g \in S(V)^{S_n}$. Clearly $f \in \pi^{-1}(\overline{f})$. Averaging f over S_n, we obtain $g := \frac{1}{|S_n|}\sum_{\sigma\in S_n} \sigma.f$. We had that $\sigma.\overline{f} = \overline{\sigma.f}$ for any $\sigma \in S_n$ therefore we have $\overline{g} = \overline{f}$. We also have $g \in S(V)^{S_n}$. So our claim holds. We know that $g = P(f_1, f_2, \ldots, f_n)$ for some polynomial $P \in \mathbb{C}[T_1, T_2, \ldots, T_n]$ which means $\overline{g} = P(0, \overline{f_2}, \ldots, \overline{f_n}) = \overline{f}$ i.e. $\overline{f} \in \mathbb{C}[\overline{f_2}, \overline{f_3}, \ldots, \overline{f_n}]$. Thus $S(W)^{S_n} \subset \mathbb{C}[\overline{f_2}, \overline{f_3}, \ldots, \overline{f_n}]$ holds as well.Clearly $\deg \overline{f_i} = i$. Hence we are done. $\square$

Proposition 6.4. *Let $W \subset \mathbb{C}^n$ be as in the previous proposition. Define $\phi : S_n \times \mathbb{Z}/2\mathbb{Z} \to GL(W)$ where the action on $\mathbb{C}^n$ is defined as follows; S_n permutes coordinates $(x_1, x_2, \ldots, x_n)$ and $\mathbb{Z}/2\mathbb{Z}$ takes $(x_1, x_2, \ldots, x_n)$ to $\pm(x_1, x_2, \ldots, x_n)$. The group $S_n \times \mathbb{Z}/2\mathbb{Z}$ is generated by reflections only for $n = 2, 3, 4$.*

Proof. We know that S_n is generated by transpositions and we know from the Proposition 6.3 that they are reflections. Therefore $(\sigma, +1)$ is a reflection where σ is a transposition . This tells us that any $(\pi, 1)$ where $\pi \in S_n$ is product of reflections. Similarly, if we can find an element $\tau \in S_n$ such that

$(\tau, -1)$ is a reflection then $(\pi\tau^{-1}, +1)(\tau, -1) = (\pi, -1)$ is product of reflections for an arbitrary $\pi \in S_n$. We conclude that $S_n \times \mathbb{Z}/2\mathbb{Z}$ is generated by reflections if and only if it contains a reflection of the form $(\tau, -1)$ for some $\tau \in S_n$. Let $\tau \in S_n$, $(\tau, -1)$ is a reflection if and only if $\phi(\tau) \in GL(W)$ has characteristic polynomial $(x-1)^{n-2}(x+1)$. If we consider the usual representation where the codomain is $GL_n(\mathbb{C})$, the range would be plus and minus n-dimensional permutation matrices. $(\tau, -1)$ takes $(c, c, \ldots, c)$ to $-(c, c, \ldots, c)$ so τ being a reflection in the previous representation ϕ is equivalent to image of τ having a characteristic polynomial $(x-1)^{n-2}(x+1)^2$ in the usual representation. It is easy to examine the characteristic polynomials of permutation matrices because two permutations are conjugate if and only if they have the same cycle structure. Let $\sigma \in S_n$ be an n-cycle, then it is conjugate to the cycle $(12\ldots n)$ i.e. $(12\ldots n) = \kappa\sigma\kappa^{-1}$ for some $\kappa \in S_n$ therefore the images of $(\sigma, -1)$ and $((12\ldots n), -1)$ in the usual representation are similar. Thus the characteristic polynomials of images are the same. Let's compute the characteristic polynomial of $((12\ldots n), -1)$; the image of $((12\ldots n), -1)$ in the usual representation is given by

$$\begin{bmatrix} 0 & -1 & 0 & \ldots & 0 \\ 0 & 0 & -1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & -1 \\ -1 & 0 & 0 & \ldots & 0 \end{bmatrix}_{n\times n} \tag{6.1}$$

Therefore characteristic polynomial is given as follows:

$$\begin{vmatrix} x & 1 & 0 & \ldots & 0 & 0 \\ 0 & x & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & x & 1 \\ 1 & 0 & 0 & \ldots & 0 & x \end{vmatrix} = x^n - (-1)^n = \begin{cases} x^n - 1 & \text{if n is even} \\ x^n + 1 & \text{if n is odd} \end{cases} \tag{6.2}$$

This can be used to write a general formula for every permutation in S_n.

If there exists c_l many disjoint l-cycles in an arbitrary permutation $\pi \in S_n$ then π is conjugate to

$$(12\dots l_1)((l_1+1)\dots l_2)\dots((l_{n-1}+1)\dots l_n) \tag{6.3}$$

for some $l_1, \dots, l_n$ depending on c_l's. That is, if we have a disjoint l-cycle then it appears as a $l \times l$ block matrix of the form (6.1) on the diagonal of $n \times n$ matrix. Therefore the characteristic polynomial is given as

$$\prod_{l=1}^{n}(x^l - (-1)^l)^{c_l} \tag{6.4}$$

Now it only remains to analyse for which values of n we can get $(x-1)^{n-2}(x+1)^2$ with a suitable choose of c_l's using the (6.4).
τ should only contain 2-cycles to make $(\tau, -1)$ a reflection. Otherwise we would get a root different than ± 1 in the characteristic polynomial of $(\tau, -1)$. Also observe that it cannot have more than two 2-cycles because in that case $(x+1)^3$ divides the characteristic polynomial. Now let's look at the remaining possibilities case by case. Our first case is that τ consists of 2 2-cycles. τ cannot fix an element because otherwise $(x+1)^3$ divides the characteristic polynomial of $(\tau, -1)$. Therefore the only possibility where $(\tau, -1)$ is a reflection in this case is where n is equal to 4. Our second case is that τ is a transposition. In this case if $n > 3$ then τ fixes at least 2 elements which means $(x^2-1)(x+1)^2$ divides the characteristic polynomial therefore $(x+1)^3$ divides the characteristic polynomial of $(\tau, -1)$. If n is 3 then $(\tau, -1)$ is a reflection because it has characteristic polynomial $(x^2-1)(x+1) = (x+1)^2(x-1)$. If n is 2 then $(\tau, -1)$ would also be a reflection on $GL_1(\mathbb{C})$ trivially. Our third case is that τ fixes all elements. If $n > 2$ then again $(x+1)^3$ is a factor in characteristic polynomial of $(\tau, -1)$ so it is not a reflection. If n is 2 then it is a reflection. We have already established that if n is 2 then the given group is generated by reflections. We conclude that $S_n \times \mathbb{Z}/2\mathbb{Z}$ is generated by reflections if and only if $n = 2$, 3 or 4, as desired. $\square$

Proposition 6.5. *A permutation group $G \subset S_n$ is generated by reflections if and only if it is direct product of symmetric groups of smaller dimension.*

Proof. The only reflections in S_n are transpositions. It is clear from the characteristic polynomials coming from the natural representation. So any $G \leq S_n$ reflection group is generated by transpositions. Fixing such G define an equivalence relation on the set $\{1, 2 \ldots, n\}$ as follows: $i \sim j$ if and only if $(ij) \in G$. Let's check the well-definedness. It is reflexive; $(ii) = 1_{S_n} \in G$. Clearly $(ij) = (ji)$ so it is a symmetric relation. Assume $i \sim j$ and $j \sim k$ i.e $(ij), (jk) \in G$ then $(ij)(jk)(ij) = (ik)$ belongs to G therefore we have $j \sim k$. That is our relation is also transitive, thus an equivalence relation. This gives a partition on the set $\{1, 2 \ldots, n\}$. Let $O_1, O_2, \ldots, O_r$ be the set of all equivalence classes. If $(ab) \in G$ then $a, b \in O_k$ for some k with $1 \leq k \leq r$. Define $G_k := \langle (ij) \in G \mid i, j \in O_k \rangle$. G_k is a subgroup of G. Let $\sigma_i \in G_k$, $\sigma_j \in G_l$, then we have $\sigma_i \sigma_j = \sigma_j \sigma_i$ because any element in G_k fixes all elements from all equivalence classes except O_k. Therefore we have following three properties by definition and previous remarks; $G = G_1 G_2 \ldots G_r$; $G_k G_l = G_l G_k$; $G_k \cap G_1 G_2 .. \widehat{G_k} .. G_r = \{1_{S_n}\}$. These three together gives $G \cong G_1 \times G_2 \times \ldots \times G_r$. Next we claim that $G_k \cong S_{|O_k|}$. Let $O_k = a_1, a_2, \ldots, a_{|O_k|}$. Define the isomorphism as follows: $\varphi : G_k \to S_{|O_k|}$ where $\varphi(a_m a_n) = (mn)$. Clearly this is a bijective homomorphism of groups. Thus such a G is isomorphic to $S_{|O_1|} \times S_{|O_2|} \times \ldots \times S_{|O_r|}$ $\square$

Bibliography

[1] C.Chevalley, *Invariants of a group in an affine ring*, **77** (1955), 778–782.

[2] J.A.Todd G.C.Shephard, *Finite unitary reflection groups*, **6** (1954), 274–304.

[3] H.Weyl, *Theorie der darstellung kontinuierlichen halb einfacher gruppen durch lineare transformationen*, **24** (1926), 328–395.

[4] M.Nagata, *Invariants of a group in an affine ring*, **3** (1964), 379–382.

[5] P.Gordan, *Beweis, dass jede covariante und invariante einer binären form eine ganze funktion mit numerischen coeffizienten einer endlichen anzahl solcher formen ist*, **69** (1868), 323–354.

[6] R.Kane, *Reflection groups and invariant theory*, Springer-Verlag, New York City, 2001.

[7] S.Lang, *Algebra*, 3rd ed., Springer-Verlag, New York City, 2003.

[8] T.A.Springer, *Invariant theory*, Springer-Verlag, Berlin, 1977.