Schur-Weyl Duality and Classical Invariant theory of finite groups

April 28, 2016

Harshit Yadav
Department of Mathematics and Statistics
IIT Kanpur

Nihar Prakash Gargava
Department of Mathematics and Statistics
IIT Kanpur

Project Supervised by:
Prof. Preena Samuel
Indian Institute of Technology, Kanpur

Abstract

We will try to understand the proof of Schur-Weyl duality from scratch. For this we will need to understand a few key results from algebra like Artin-Wedderburn theorem, double centralizer theorem, etc. We will understand the proofs of these results from basics and then use them to prove Schur-Weyl duality. We also give a brief introduction to the work of Claudio Processi on invariants of m-tuples of $n \times n$ matrices.

The next section deals with invariant ring created by finite groups. We will see some important founding theorems of this area and then look at the important computable results of Noether and Molien.

Contents

1 Schur-Weyl Duality

1.1 Introduction

We shall devote the first four sections to introducing key concepts from algebra which we will be using to prove Schur-Weyl duality.In section 2 we will look at the basics of modules theory. In section 3, we will look at Wedderburn theory with the aim of classifying semisimple algebras. In section 4 we will try to prove the Schur-Weyl duality. This will involve proving the double centralizer theorem using Wedderburn theory. We end in section 5 by having a brief look at the work of Processi pertaining to the invariant ring of m copies (m-tuple) of $GL(V)$ ($n \times n$ matrices where $n = dim(V)$) under adjoint action by a product of general linear groups. We aim to completely understand this work in later projects.

1.1.1 Invariant theory

Invariant theory deals with the actions of groups on vector spaces (algebraic varieties in general), from the point of view of their effect on functions. Let W be a finite dimensional K-vector space where K is a field. A function $f : W \to K$ is called polynomial or regular if it is given by a polynomial in the coordinates with respect to a basis of W. We denote by $K[W]$ the K-algebra of polynomial functions on W which is usually called the coordinate ring of W or the ring of regular functions on W. If $w_1, \ldots, w_n$ is a basis of W and $x_1, \ldots, x_n$ the dual basis of the dual vector space $W*$ of W , i.e., the coordinate functions, we have $K[W] = K[x_1, \ldots, x_n]$. This is a polynomial ring in the x_i because the field K is infinite.

Let $G \subset GL(W)$ have a action defined on E. Then, a function $f \in K[W]$ is called G-invariant or shortly invariant if $f(gw) = f(w)$ for all $g \in G$ and $w \in W$. The invariants form a subalgebra of $K[W]$ called invariant ring and denoted by $K[W]^G$. So, our major problems studied in invariant theory are studying the invariant ring. We want to know what are the generators of the invariant ring and if there are any relations between them.

1.2 Modules

Let F be a field, and let let G be a group acting on a $F-$vector space V. A representation of G on V is a group homomorphism $\Phi : G \to GL(V, F)$.

Let R be a ring with unit, meaning that R has a multiplicative identity 1, and let M be an abelian group written additively. We say that M is a left R-module if there is a map from $R \times M$ to M, with the image of $(r, m) \in R \times M$ being written rm, which satisfies the following properties:

- $1m = m$ for all $m \in M$.
- $r(m + n) = rm + rn$ for all $r \in R$ and $m, n \in M$.

- $(r+s)m = rm + sm$ for all r, $s \in R$ and $m \in M$.
- $r(sm) = (rs)m$ for all $r, s \in R$ and $m \in M$.

If F is a field, then the definition of an F-module is precisely that of an $F-$vector space. Let N be a subgroup of M. We say that N is an R-submodule (or just submodule) of M if $rn \in N$ for every $r \in R$ and $n \in N$. The module whose only submodules are 0 and itself is called a simple module.

Let N_1 and N_2 be submodules of an $R-$module M. We define their sum to be $N_1 + N_2 = x + y | x \in N_1, y \in N_2 \subseteq M$; this is a submodule of M, as is $N_1 \bigcap N_2$. If $N_1 \bigcap N_2 = 0$, then we say that the sum of N_1 and N_2 is direct, and we write $N_1 \oplus N_2$ instead of $N_1 + N_2$. We also have an external notion of direct sum: If M and N are R-modules, then we give $M \times N$ an $R-$ module structure via $r(m, n) = (rm, rn)$, and we write $M \oplus N$ instead of $M \times N$. A composition series of an $R-$module M is a descending series of submodules of M which terminates in the zero submodule and in which each successive quotient is a simple module.

We say that a submodule N of a module M is a direct summand of M if there is some other submodule N' of M such that $M = N \oplus N'$. Let M and N be R-modules, and let $\phi : M \to N$ be a group homomorphism. We say that ϕ is an $R-$module homomorphism if $\phi(rm) = r\phi(m)$ for any $r \in R$ and $m \in M$. Fundamental theorem on homomorphisms for modules states that the R-modules $M/ker\phi$ and $im\phi$ are isomorphic via the map induced by ϕ; The first isomorphism theorem for modules states that if M is an $R-$module having submodules N_1 and N_2, then $N_1 + N_2/N_1 \cong N2/N1 \bigcap N2$.

Lemma 1.1 (Schur's Lemma)**.** *Any non-zero homomorphism between simple R-modules is an isomorphism*

The group ring of G over R, denoted by RG, consists of all finite formal R-linear combinations of elements of G, with the obvious rule for addition and with multiplication defined by extending the multiplication in G; explicitly, we have

$$(\sum_{x \in G} a_x x)(\sum_{y \in G} b_y y) = \sum_{x \in G} \sum_{y \in G} a_x b_y xy$$

The group ring has a unit element, namely the identity element of the underlying group. We will be primarily interested in the case where $R = F$ is a field and G is finite, in which case FG is not only a ring but also an F-vector space having G as a basis and hence having finite dimension $|G|$. FG is called a group algebra.

If F is a field, then an algebra over F (or simply an F-algebra) is a set A with a ring structure and an F-vector space structure that share the same addition operation, and with the additional property that $(\lambda a)b = \lambda(ab) = a(\lambda b)$ for any $\lambda \in F$ and a, $b \in A$. An algebra is called finite-dimensional if it has finite dimension as an F-vector space. A homomorphism of F-algebras is a ring homomorphism which is also an F-linear transformation.

Modules over a group algebra FG can also be regarded as F-vector spaces, with) $\lambda \in F$ acting by $\lambda 1 \in FG$, and when G is finite we have the following nice relationship between these structures:

Proposition 1.2. *If F is a field and G a finite group, then an $FG-$module is finitely generated iff it has finite dimension as an F-vector space.*

Theorem 1.3 (MASCHKE'S THEOREM)**.** *Let G be a group, and suppose that the characteristic of F is either zero or coprime to $|G|$. If U is an FG-module and V is an FG-submodule of U, then V is a direct summand of U as FG-modules.*

A module is said to be semisimple if it is a direct sum of simple modules.

Corollary 1.4. *Let G be a group, and let F be a field whose characteristic does not divide $|G|$. Then every non-zero FG-module is semisimple.*

1.3 Artin-Wedderburn theorem

All algebras in this section will be finite-dimensional F-algebras, where F is an arbitrary field, and unless explicitly stated otherwise will be algebras with unit. All modules over algebras are assumed to be finitely generated, or equivalently finite-dimensional as F-vector spaces. All direct sums of modules are assumed to be finite. Now we will look at a series of lemmas and propositions which will finally lead to the Artin-Wedderburn theorem. We will skip a few not so important proofs. One can refer [5] for the details.

Lemma 1.5. *The following statements about an A-module M are equivalent:*

- *Any submodule of M is a direct summand of M.*
- *M is semisimple.*
- *M is a sum (but not, a priori, a direct sum) of simple submodules.*

Lemma 1.6. *Submodules and quotient modules of semisimple modules are semisimple.*

Definition 1.1 (Semisimple algebra)**.** An algebra A is called semisimple if all nonzero A-modules are semisimple.

Lemma 1.7. *The algebra A is semisimple iff the A-module A is semisimple.*

PROOF : Suppose that the A-module A is semisimple, and let M be an A-module generated by $m_1, \ldots, m_r$ Let A_r denote the direct sum of r copies of A. We define a map from A^r to M by sending $(a_1, \ldots, a_r)$ to $a_1m_1 + \ldots + a_rm_r$; this map is an A-module epimorphism. Thus, M is isomorphic with a quotient module of the semisimple module A_r and hence is semisimple by Lemma 3.5. It follows that A is a semisimple algebra. The converse is trivial.

Proposition 1.8. *Let A be a semisimple algebra, and suppose that as A-modules we have $A \cong S_1 \oplus \ldots \oplus S_r$ where the S_i are simple submodules of A. Then any simple A-module is isomorphic with some S_i.*

PROOF : Let S be a simple A-module, fix some $0 \neq s \in S$, and define an A-module homomorphism $\phi : A \to S$ by $\phi(a) = as$ for $a \in A$. As S is simple, ϕ is surjective. For each i, let $\phi : S_i \to S$ be the restriction of ϕ to S_i. If $\phi = 0$ for all i, then we would have $\phi = 0$; hence ϕ is non-zero for some i, and it now follows from Schur's lemma that $\phi : S_i \to S$ is an isomorphism.

Proposition 1.9. *Suppose that A is a semisimple algebra, and let $S_1, \ldots, S_r$ be a collection of simple A-modules such that every simple A-module is isomorphic with exactly one S_i. Let M be an A-module, and write $M \cong n_1S_1 \oplus \ldots \oplus n_rS_r$ for some non-negative integers n_i. Then the n_i are uniquely determined.*

If D is a finite-dimensional F-algebra, then for any $n \in N$ the set $M_n(D)$ of $n \times n$ matrices with entries in D is a finite-dimensional F-algebra of dimension $n^2 dim_F D$. Algebras of the form $M_n(D)$ are called matrix algebras over D. Let D_n be the set of column vectors of length n with entries in D; this forms an $M_n(D)$-module under matrix multiplication.

Definition 1.2 (Division algebra)**.** An algebra D is said to be a division algebra if the non-zero elements of D form a group under multiplication.

Theorem 1.10. *Let D be a division algebra, and let $n \in N$. Then any simple $M_n(D)$-module is isomorphic with D^n, and $M_n(D)$ is isomorphic as $M_n(D)$-modules with the direct sum of n copies of D^n. In particular, $M_n(D)$ is a semisimple algebra.*

Definition 1.3 (Simple algebra)**.** An algebra is called simple if its only two-sided ideals are itself and the zero ideal.

Lemma 1.11. *Simple algebras are semisimple.*

Theorem 1.12. *Let D be a division algebra, and let $n \in N$. Then $M_n(D)$ is a simple algebra.*

If $B_1, \ldots, B_r$ are algebras, then their external direct sum is the algebra B whose underlying set is the Cartesian product of the B_i and whose addition, multiplication, and scalar multiplication operations are defined componentwise. As the name suggests, we write $B = B_1 \oplus \ldots \oplus B_r$. If M is a B_i-module for some i, then we give M a B-module structure by $(b_1, \ldots, b_r)m = b_i m$. Clearly, if M is simple (resp., semisimple) as a B_i-module, then it is also simple (resp., semisimple) as a B-module.

Lemma 1.13. *Let $B = B_1 \oplus \ldots \oplus B_n$ be a direct sum of algebras. Then the two-sided ideals of B are exactly the sets of the form $J_1 \oplus \ldots \oplus J_n$, where J_i is a two-sided ideal of B_i for each i.*

Theorem 1.14. *Let $r \in N$. For each $1 \leq i \leq r$, let D_i be a division algebra over F, let $n_i \in N$, and let $B_i = M_{n_i}(D_i)$ Let B be the external direct sum of the B_i. Then B is a semisimple algebra having exactly r isomorphism classes of simple modules and exactly 2^r two-sided ideals, namely every sum of the form $\oplus_{j \in J} B_j$, where J is a subset $1, \ldots, n$.*

PROOF : For each i, we can write $B_i = C_{i1} \oplus \ldots \oplus C_{in_i}$ by Theorem 3.10, where the C_{ij} are mutually isomorphic simple B_i-modules. As noted above, each C_{ij} is also simple as a B-module. Therefore, we have $B \cong \oplus_{i,j} C_{ij}$ as B-modules, and hence B is a semisimple algebra by Lemma 3.7. It now follows from Proposition 3.8 that any simple B-module is isomorphic with some C_{ij}; but $C_{ij} \cong C_{kl}$ as B-modules iff $i = k$, so there are exactly r isomorphism classes of simple B-modules. The statement about two-sided ideals of B is an easy consequence of Theorem 3.12 and Lemma 3.13.

So, we have proved that the direct sum of matrix algebras over division rings is semisimple. After a few more results we will that the converse of this statement also holds.

Definition 1.4 (Endomorphism algebra)**.** If M is an A-module, then $End_A(M)$ with the composition of mappings as a multiplication is an F-algebra called the endomorphism algebra of M.

Definition 1.5 (Opposite algebra)**.** The opposite algebra B^{op} of an algebra B is defined to be the set B endowed with the usual addition and scalar multiplication but the opposite multiplication. Multiplication in B^{op} is denoted by $a \cdot b := ba$.

Observe that $(B^{op})^{op} \cong B$. If B is a division algebra, then so is B^{op}. The opposite of a direct sum of algebras is the direct sum of the opposite algebras, since multiplication in the direct sum is defined componentwise.

Lemma 1.15. *Let B be an algebra. Then $B^{op} \cong End_B(B)$.*

This lemma suggests that we can gain information about semisimple algebras by studying the properties of endomorphism algebras of semisimple modules.

Lemma 1.16. *Let $S_1, \ldots, S_r$ be the distinct simple A-modules; for each i, let U_i be a direct sum of copies of S_i, and let $U = U_1 \oplus \ldots \oplus U_r$. Then we have $End_A(U) \cong End_A(U_1) \oplus \ldots \oplus End_A(U_r)$*

Lemma 1.17. *If S is a simple A-module, then for any $n \in N$ we have $End_A(nS)$ $\cong M_n(End_A(S))$.*

Lemma 1.18. *Let B be an algebra. Then $M_n(B)^{op} \cong M_n(B^{op})$ for any $n \in N$.*

Finally using all the previous results we look at the Artin-Wedderburn theorem.

Theorem 1.19. *The algebra A is semisimple iff it is isomorphic with a direct sum of matrix algebras over division algebras.*

PROOF : Suppose that the algebra A is semisimple. Then we can write A in the form $A = U_1 \oplus \ldots \oplus U_r$, where each U_i is the direct sum of n_i copies of a simple A-module S_i, and no two of the S_i are isomorphic. We have

$$\begin{aligned} A^{op} &\cong End_A(A)(\text{by lemma 3.15}) \\ &\cong End_A(U_1) \oplus \ldots \oplus End_A(U_r)(\text{by lemma 3.16}) \\ &\cong End_A(n_1 S_1) \oplus \ldots \oplus End_A(n_r S_r) \\ &\cong M_{n_1}(End_A(S_1)) \oplus \ldots M_{n_r}(End_A(S_r))(\text{by lemma 3.17}) \end{aligned}$$

this gives us that

$$\begin{aligned} A &\cong [M_{n_1}(End_A(S_1)) \oplus \ldots M_{n_r}(End_A(S_r))]^{op} \\ &\cong M_{n_1}(End_A(S_1))^{op} \oplus \ldots M_{n_r}(End_A(S_r))^{op} \\ &\cong M_{n_1}(End_A(S_1)^{op}) \oplus \ldots M_{n_r}(End_A(S_r)^{op})(\text{by lemma 3.18}) \end{aligned}$$

Since the endomorphism algebra of a simple module is a division algebra, and since the opposite algebra of a division algebra is also a division algebra, we now see that any semisimple algebra is isomorphic with a direct sum of matrix algebras over division algebras. The converse was established in Theorem 3.14.

1.4 Schur-Weyl Duality

Schur-Weyl duality relates irreducible finite-dimensional representations of the general linear and symmetric groups. It forms a standard situation is representation theory when two different kinds of symmetries determine each other. We have followed [3] throughout this section. Let V be a vector space of dimension n over field K. Now consider the m-fold product

$$V^{\otimes m} := V \otimes \ldots \otimes V \ (m \text{ times})$$

The usual linear action of $GL(V)$ on this vector space is given by

$$g(v_1 \otimes \ldots \otimes v_m) := gv_1 \otimes \ldots \otimes gv_m$$

The symmetric group S_m on m letters acts on $V^{\otimes m}$ as

$$\sigma(v_1 \times \ldots \otimes v_m) := v_{\sigma^{-1}(1)} \otimes \ldots \otimes v_{\sigma^{-1}(m)}.$$

The two actions commute with each other. If we let $\langle GL(V) \rangle$ denote the linear subspace of $End(V^{\otimes m})$ spanned by the image of $\langle GL(V) \rangle$ in $End(V^{\otimes m})$ under the representation considered above. Similarly, we define the subspace $\langle S_m \rangle \subset End(V^{\otimes m})$. Both of these are subalgebras and they centralise each other, that is

$$ab = ba \ \forall \ a \in \langle GL(V) \rangle, \forall \ b \ in \ \langle S_m \rangle$$

For any subalgebra $A \subset End(W)$ where W is an arbitrary vector space the centralizer (or commutant) of A is the subalgebra consisting of those elements of $End(W)$ which commute with all element of A. It will be denoted by A' :

$A' := \{b \in End(W) \mid ab = ba \text{ for all } a \in A\}$

Equivalently, A' is the algebra of A-linear endomorphisms of W considered as an A-module:

$$A' = End_A(W)$$

Theorem 1.20. *Consider the usual linear actions of $GL(V)$ and S_m on $(V^{\otimes m})$ and denote by $\langle GL(V)\rangle$ and $\langle S_m\rangle$ the subalgebras of $End(V^{\otimes m})$ spanned by the linear operators from $GL(V)$ and S_m , respectively. Then*

- $End_{S_m}(V^{\otimes m}) = \langle GL(V)\rangle$
- *If char $K = 0$ then $End_{GL(V)(V^{\otimes m}) = \langle S_m\rangle}$*

PROOF of (a) : We use the natural isomorphism $\gamma : End(V)^{\otimes m} End(V^{\otimes m})$ given by $\gamma(A_1 \otimes \ldots \otimes A_m)(v_1 \otimes \ldots \otimes v_m) = A_1v_1 \otimes \ldots \otimes A_mv_m$. Then the corresponding representation $GL(V) \to End(V)^{\otimes m}$ is $g \mapsto g\otimes \ldots \otimes g$. We claim that the corresponding action of S_m on $End(V) \otimes m$ is the obvious one:

$$\sigma(A_1 \otimes \ldots \otimes A_m) = A_{^1}(1) \otimes \ldots \otimes A_{^1}(m).$$

In fact, $\sigma(\gamma(A_1 \otimes \ldots \otimes A_m)(\sigma^{-1}(v_1 \otimes \ldots \otimes v_m)))$

$$= \sigma(A_1v_{\sigma(1)} \otimes \ldots \otimes A_mv_{\sigma(m)})$$

$$= A_{^1(1)}v_1 \otimes \ldots \otimes A_{^1(m)}v_m$$

$$= \gamma(A_{^1(1)} \otimes \ldots \otimes A_{^1(m)})(v_1 \otimes \ldots \otimes v_m).$$

This implies that γ induces an isomorphism between the symmetric tensors in $End(V)^{\otimes m}$ and the subalgebra $End_{S_m}(V^{\otimes m}$ of $End(V^{\otimes m})$. The claim now follows from the next lemma applied to $X := GL(V) \subset W := End(V)$.

Lemma 1.21. *Let W be a finite dimensional vector space and $X \subset W$ a Zariski-dense subset. Then the linear span of the tensors $x \otimes \ldots \otimes x, x \in X$, is the subspace $\sum_m \subset W^{\otimes m}$ of all symmetric tensors.*

Recall that a subset $X \subset W$ is Zariski-dense if every function $f \in K[W]$ vanishing on X is the zero function. We skip the proof here and the reader can refer to Kraft and Processi for it.

In order to prove part (b) of the theorem, we will need the double centralizer theorem

1.4.1 Double centralizer theorem

After all the hardwork of proving the Weddweburn theorem, we are going to extensively use it to prove the double centralizer theorem. Let W be a vector space over a field K. Since, char $K = 0$, we can use Maschke's theorem to infer that the group algebra $\mathbb{C}[G]$ is semisimple. Due to this, the homomorphic image $\rangle S_m \langle$ of $K[S_m]$ is a semisimple subalgebra of $End(V^{\otimes n}$. We will widely use this fact in our proof of double centralizer theorem

Definition 1.6 (Isotypic decomposition)**.** For a G-module W and a simple module U the isotypic component of W of type U is the sum of all submodules of W isomorphic to U . The isotypic components form a direct sum which is all of W if and only if W is semisimple. In that case it is called the isotypic decomposition.

Lemma 1.22. *Let A be a semisimple algebra and let $A = A_1 \oplus \ldots \oplus A_r$, where A_i corresponds to the simple A-module U_i, then $End_A(U_i) = End_{A_i}(U_i)$*

PROOF : It is clear that $End_A(U_i) \subset End_{A_i}(U_i)$. Also, there is an algebra homomorphism between $End_A(U_i)$ and $End_{A_i}(U_i)$. So, we just need to show that $End_A(U_i) \supset End_{A_i}(U_i)$. Let $\phi \in End_{A_i}(U_i)$, then ϕ is A_i linear. It is A-*linear* as well because, $\phi(au_i) = \phi((a_1, \ldots, a_r)(0, \ldots, u_i, \ldots, 0) = \phi(a_iu_i) = a_i\phi(u_i) = a\phi(u_i)$. Hence, $\phi \in End_A(U_i)$.

Lemma 1.23. *If A is central simple algebra over K and B is a K-algebra which is simple, then $A \otimes B$ is simple.*

Theorem 1.24. *Let$A \in End(W)$ be a semisimple algebra and A' : $\{b \in End(W)|\ ab = ba\ \forall\ a \in A\}$ its centralizer. Then:*

1. *A' is semisimple and $(A')' = A$*
2. *W has a unique decomposition $W = W_1 \oplus \ldots \oplus W_r$ into simple non-isomorphic $A \otimes A'$-modules W_i. In addition this is the isotypic decomposition as an A-module and as an A'-module.*
3. *Each simple factor W_i is of the form $U_i \otimes_{D_i} U_i'$ where U_i is a simple A- module, U_i' a simple A'-module, and D_i is the division algebra $End_A(U_i)^{op} = End'_A U_i'^{op}$*

PROOF : Since A is a semisimple algebra, every A-module is semisimple. Also $A \in End(W)$, so W is an A-module Hence, let $W = W_1 \oplus \ldots \oplus W_r$ be the isotypic decomposition of W as an A-module. Here $W_i \cong U_i^{s_i}$ where U_i are simple A-modules which are pairwise non-isomorphic. Corresponding to this decomposition of W, the semisimple algebra A decomposes as follows:

$$A \cong \textstyle\prod_{i=1}^r A_i, \qquad A_i \cong M_{n_i}(D_i) \qquad \text{(using theorem 3.19)}$$

with $D_i = End_A(U_i)^{op} = End_{A_i}(U_i)^{op}$ (using lemma 3.17) being a division algebra containing K. Furthermore, $U_i \cong D_i^{n_i}$ (using theorem 3.10) as an A-module where the module structure on $D_i^{n_i}$ is given by $A \xrightarrow{projection} A_i \xrightarrow{\sim} M_{n_i}(D_i)$.

Now define A' as follows:

$$A' := End_A(W) = \prod End_A(W_i), \text{ and} \qquad \text{(using lemma 3.16)}$$

$$A'_i := End_A(W_i) = End_{A_i}(W_i) \cong M_{s_i}(D') \qquad \text{(using lemma 4.3)}$$

$$End_{A_i}(W_i) \cong End_{A_i}(U_i^{s_i}) \cong M_{s_i}(End_{A_i}(U_i)) \qquad \text{(using lemma 3.17)}$$

$D'_i := End_{A_i}(U_i) = D_i^{op}$. So, D'_i is also a division ring. Since, we have written A as a direct sum of matrix algebra over division rings, it is semisimple. Note that

$$(dimA_i)(dimA'_i) = n_i^2(dimD_i)s_i^2(dimD'_i) = (n_i s_i(dimD_i))^2$$

$$= (dimW_i)^2 = dimEnd(W_i) \qquad \text{(since } dimD_i = dimD'_i\text{)}$$

Both $A_i(\cong M_{n_i}(D_i))$ and $A'_u(\cong M_{s_i}(D'_i))$ are simple algebras (using theorem 3.12). A_i is a central simple D_i-algebra . Also, A'_i is also a simple D_i-algebra. Using lemma 4.4, we conclude that $A_i \otimes A'_i$ is also a simple algebra. Now look at the canonical algebra homomorphism $A_i \otimes A'_i \xrightarrow{\sim} End(W_i)$. This homomorphism will be injective because $A_i \otimes A'_i$ is simple implies that the kernel of this map cam be either 0 or whole. Since the map is non-zero, the kernel is 0 and hence this homomorphism is injective. This along with the dimension argument above implies that this is an algebra isomorphism.

So, W_i is a simple $A_i \otimes A'_i$-module. Then it is a simple $A \otimes A'$-module. Now, consider $U_i = D_i^{n_i}$ as a right D_i-module and $U'_i := (D_i^{op})^{s_i}$ as a left D_i-module. These module structures commute with A- resp. A'-module structure,i.e. U_i is a left A-module and U'_i is a right A'-module. Hence $U_i \otimes_{D_i}$ is an $A \otimes A'$-module. We get an $A \otimes A'$-module homomorphism from $U_i \otimes_{D_i} \to U_i^{s_i} \cong W_i$. But W_i is a simple module and this homomorphism is not zero. So using Schur's lemma, we can say that it will be an isomorphism. So we have finally that $U_i \otimes_{D_i} U'_i \xrightarrow{\sim} U_i^{s_i} \xrightarrow{\sim} W_i$ as $A \otimes A'$-modules.

Finally, inorder to show $(A')' = A$, notice that $dimA'_i dimA''_i = dimEnd(W_i) = dimA_i dimA'_i$. Hence, $dimA''_i = dimA_i$. But $A'' \supset A$, so we conclude that $(A')' = A$.

Now we look at a final result which will prove part and it will also tell us about the decomposition of $V^{\otimes m}$ as a $S_m \times GL(V)$-module

Theorem 1.25 (Decomposition theorem)**.** *Assume char $K = 0$.*

1. *The two subalgebras $\langle S_m \rangle$ and $\langle GL(V) \rangle$ are both semisimple and are the centralizers of each other.*

2. *There is a canonical decomposition of $V^{\otimes m}$ as an $S_m \times GL(V)$-module into simple non-isomorphic modules V_λ :*

   $$V^{\otimes m} = \bigoplus_\lambda V_\lambda$$

3. *Each simple factor V_λ is of the form $M_\lambda \otimes L_\lambda$ where M is a simple S_m-module and L_λ a simple $GL(V)$-module. The modules M_λ (resp. L_λ) are all non-isomorphic.*

PROOF : In theorem 4.1 part (1), we have already proved that $\langle S_m\rangle' = \langle GL(V)\rangle$, and so (1) and (2) follow from the Double Centralizer Theorem. For the last statement it remains to show that the endomorphism ring of every simple S_m-modules M_λ is the base field K. This is clear if K is algebraically closed. For arbitrary K of characteristic zero it will be proved later.

1.4.2 Schur-Weyl duality in action

Now we see how to use the results obtained to get irreducible representations of $GL(V)$ from irreducible representations of S_n. Let G be a finite group, $A = \mathbb{C}[G]$, and U a right A-module. Define $B = End_G(U) = \{\phi : U \to U : \phi(ug) = \phi(u)g, \forall u \in U, g \in G\}$; B is the commutator algebra of U and U is a left B-module in a natural way. Let W be a left -module. Then $U \otimes_A W$ is a left B-module, acting through the first factor.

Lemma 1.26. *With notation as above, letting U be finite dimensional, we have the following.*

1. *For c$\in$ A, the canonical map from $U \otimes_A$ A. to $U.c$ is an isomorphism of B-modules.*

2. *Let $W =$. be an irreducible left A-module, then $U \otimes$ W is an irreducible left -module.*

3. *If $W_i = A \cdot c_i$ are all of the irreducible -modules (up to equivalence), with $dimW_i = m_i$ so that $A = \bigoplus W_i^{\oplus m_i}$; then $U = \bigoplus U \cdot c^{\oplus m_i}$ is the decomposition into irreducibles for the B-module U.*

PROOF : We skip the proof. The reader can refer to Brown and Lakshmibai's book on flag varieties for more details.

Let $\lambda \vdash d$ be a partition. Then $a_\lambda := \sum_{\sigma\in R(T_\lambda)} \sigma$, $b_\lambda := \sum_{\sigma\in C(T_\lambda)} sign(\sigma)\sigma$ where $R(T_\lambda)$ (resp $C(T_\lambda)$) is the set of row (resp column) preserving permutations of T_λ. $c_\lambda := a_\lambda b_\lambda$.
We know from representation theory of S_d that $V_\lambda = \mathbb{C}[G].c_\lambda$ are all the irreducible S_d modules as λ varies over all the partitions of d. These modules are called as Young's modules. Now, we will apply the previous lemma here. Here, $U = V^{\otimes d}$, $A = \mathbb{C}[S_d]$, $c = c_\lambda$, $A.c = V_\lambda$, $B = \langle GL(V)\rangle$ so using lemma 4.17(1), we get that $V^{\otimes d} \otimes V_\lambda \cong V^{\otimes d}.c_\lambda$ as irreducible left $GL(V)$-modules.
We can write $\mathbb{C}[S_d] = \bigoplus V_\lambda^{\oplus m_\lambda}$ where $m = dim(V_\lambda)$
So, we see that from part (3) of lemma that $V^{\otimes d} = \bigoplus (V^{\otimes d} \cdot c_\lambda)^{\oplus m_\lambda}$ as irreducible GL(V)-modules. For more details, the reader can refer [4].

1.5 The Invariant Theory of m-tuples of $n \times n$ Matrices

Processi's paper 'The Invariant Theory of $n \times n$ Matrices' deals with the problem of describing invariants of m-tuples of matrices. Let $V \cong K^n$, where K is a field and let $(K)_n \cong End(V)$ denote the full ring of $n \times n$ matrices. $V*$ is the dual space of V and $G = GL(n, K)$ is the group of invertible matrices. Processi's paper discusses the following problem:
Consider the space $(K)_n^i$ of i-tuples in $n \times n$ matrices. If $A \in G$, $B_j \in (K)_n$, then $A.(B_1, \ldots, B_i) = (AB_1A^{-1}, \ldots, AB_iA^{-1})$. He describes the ring $T_{i,n}$ of polynomial functions on W, invariant under the action of G.

Theorem 1.27. *Any polynomial invariant of i $n \times n$ matrices $A_1, A_2, \ldots A_i \in (K)_n$ is a polynomial in the invariants $tr(A_{i_1}A_{i_2} \ldots A_{i_j})$; $A_{i_1}A_{i_2} \ldots A_{i_j}$, running over all possible (noncommutative) monomials.*

Processi also found all relations among the elements $tr(M)$ and M, M varying on the monomials in the $n \times n$ matrix variables $X_1, X_2, , \ldots, X_i, \ldots, i = 1, \ldots, \infty$

2 Invariant theory for finite groups

2.1 Introduction

When we have a group represenation, we have a vector space being acted upon the group. Such an action can be extended to an action on the set of polynomial functions over the vector space. Invariant theory is the mathematics that deals with these actions of groups on polynomial rings. More specifically, it tries to understand those polynomial functions that are invariant under the said action.

In this report, we will look at some of the concepts of classical invariant theory with some special emphasis on the invariant theory of finite groups.

2.2 Invariant ring

2.2.1 Coordinate ring

Assume that K is an algebraically closed field. Let W be a finite dimensional vector space defined over over K.

Now consider the set of all K-valued K-linear functions on W. It is not very difficult to see that this set itself will form a finite dimensional K-vector space (having the same dimension as W). We denote this space by the dual space $W*$ of W.

Consider a K-algebra of K-valued functions on W generated by the elements of $W*$. Here, multiplication and addition are as $(fg)(v) = f(v)g(v)$ and $(f + g)(v) = f(v) + g(v)$ respectively, where f and g are K-valued functions of W and $v \in W$.

Definition 2.1. We call this K-algebra the *coordinate ring* or the *polynomial ring* on W. This algebra is denoted by $K[W]$. Individual elements of this ring are called *regular functions* or *polynomial functions* on W.

If $x_1, x_2 \ldots x_n$ form a basis of $W*$ then $K[W]$ can be generated by these elements (as any other linear function will be a linear combination of these). Hence $K[W] = K[x_1, x_2 \ldots x_n]$. This is a polynomial ring in x_is because the K is infinite and x_is are algebraically independent.

A polynomial function f is called homogeneous of degree d if $f(tw) = w^d f(t)$, for all $f \in K[W],\ w \in W$. This tells us about the graded structure $K[W] = \bigoplus_i K[W]_i$ where $K[W]_i$ is the subspace of homogenous polynomials of degree d. Choosing some basis $x_1 \ldots x_n$ tells us that $K[W]_i$ is spanned by the monomials ${x_1}^{\alpha_1} {x_2}^{\alpha_2} \ldots {x_n}^{\alpha_n}$ such that $\sum_j \alpha_j = i$.

2.2.2 Invariant functions

Suppose G is a subgroup of $GL(W)$ (general linear group) through a homomorphism (representation) or otherwise. This forms a group of K-linear automorphisms of the K-vector space W. Hence we can unerstand W as a G-module with the G-action defined as $(g, w) \mapsto gw$.

Definition 2.2. A polynomials function f is said to be *G-invariant* if $f(g(w)) = f(w)$, for all $g \in G,\ w \in W$. The invariants form a subalgebra of $K[W]$ which is denoted by $K[W]^G$ and is called the *invariant ring of* $K[W]$.

There is another, perhaps more helpful, way to look at this action. The action of G on W can be extended to an automorphic action of G on $K[W]$. That means, if $f \in K[w]$ and $g \in G$, we define the action as $(g, f) \mapsto fog^{-1}$. So $(gf)(w) = f(g^{-1}(w))$, for all $w \in W$. With this action, $K[W]^G$ is actually the ring of polynomials fixed pointwise by the automorphic action of G on $K[W]$.

Moreover, it follows from this arrangement that the homogenous comoponents $K[W]_i$ of $K[W]$ are stable (as a set, or in other words, is a perfect union of G-orbits) by G-action (that is, the degree of a homogeneous polynomial is preserved by the action of G). This makes the invariant ring a graded algebra as $K[W]^G = \bigoplus_i K[W]_i^G$

2.3 Finite generation of invariants

For a given subgroup G lying in $GL(W)$, the problem of deciding whether the invariant ring $K[W]^G$ is finite is called *Hilbert's 14th problem.*

In some nice cases, for example when K has a good characteristic and G is finite or when the action of G on $K[W]$ is completely reducible, it turns out that the invariant ring is actually finitely generated. We will see the proof of this soon.

We start with the following definition.

Definition 2.3. Given a ring R and a subring $S \subset R$. A map $\rho : R \to S$ is called a *Reynold's operator* if the following conditions are satistfied.

1. ρ is S-linear (i.e. $\rho(sr) = s\rho(r),\ \forall s \in S,\ r \in R$)
2. $\rho|_S = id_S$

We are specifically interested in the case when R is $K[W]$ and S is $K[W]^G$. When this happens, there might be a way to define a Reynold's operator for the following cases.

1. When the action of G on W is completely reducible, $K[W]$ as a module splits into a direct sum irreducible modules under this action and the submodule $K[W]^G$ is a perfect direct sum of some of these modules. The Reynold's operator can then be defined as a canonical projection on the invariant ring. It can be checked that this choice works.

2. When the group G is finite and $|G|^{-1}$ is defined in the field K, choose the map $\rho : K[W] \to K[W]^G$ given by $\rho(f) = \frac{1}{|G|}\sum_{g \in G} g(f)$, where $f \in K[W]$. It is easy to check that this map will work as a Reynold's operator.

Note that the Reynold's operator has to be K-linear (because of $K[W]^G$-linearity). After the upcoming proposition, we will see some good consequences of there being a Reynold's operator available.

Proposition 2.1. *Let R be a ring and let $S \subset R$ be a subring with a Reynold's operator $\rho : R \to S$. Then,*

1. *$IR \cap S = I$ for any ideal $I \subset S$*
2. *R is noetherian $\implies$ S is noetherian*

Proof. We note that $I \subset IS \subset IS \cap S \subset IR \cap S$. Now, $a \in IR \cap S \implies$ for some p, $a = \sum_{i=1}^{p} a_i r_i$, where $a_j \in I$ and $r_j \in R$, $\forall j$. This means that $\rho(a) = a = \sum_{i=1}^{p} a_i \rho(r_i) \in I$

For the other part, consider an increasing chain of ideals $I_1 \subset I_2 \subset I_3 \dots$ in S. Suppose R is noetherian, for some n, $I_n R = I_{n+1}R$. Then by the first part, $I_n = I_n R \cap S = I_{n+1} R \cap S = I_{n+1}$. Hence S is noetherian. □

2.3.1 Hilbert's finiteness theorem

Now we move on to a big result in the theory.

Theorem 2.2 (Hilbert's finiteness theorem). *Let G be a group of automorphisms acting on $K[W] = \bigoplus_i K[W]_i$. Let there be a Reynold's operator $\rho : K[W] \to K[W]^G$. Then $K[W]^G$ is a finitely generated K-algebra.*

Proof. Take I to be the ideal of $K[W]$ generated by all the invariant homogeneous elements of positive degree. Since $K[W]$ is noetherian, there exists a finite subset of these invariant homoegeneous polynomials that completely generate I. Let these polynomials be $P_1, P_2 \dots P_k$ of degree $k_1, k_2 \dots k_n$ respectively.

We claim that the same invariant generators $P_1 \dots P_n$ generate $K[W]^G$. To establish this, we show that an invariant homogeneous function $P \in K[W]^G$ of degree $k > 0$ can be expressed as a polynomial of P_is. We prove this by induction on k.

Since $P \in I$, we know that $P = \sum_i Q_i P_i$, where $Q_i \in R$ are homogeneous polynomials of degree $k - k_i$. Applying ρ to this equation gives that $P = \rho(P) = \sum_i \rho(Q_i) P_i$. Now all the $\rho(Q_i)$s are invariants of degree $k - k_i$. Hence, in order to represent P as a polynomial of P_is, we now need to obtain the lower degree Q_is as a polynomial of P_is which can be done inductively. Therefore, the proof is complete.

□

Since we have shown that a Reynold's operator could be costructing for finite group actions, invariant rings of finite groups are finitely generated, thanks to Hilbert's theorem.

2.3.2 Noether's bound

We will now see a bound on the number of generators and degree of generators for the case of finite group action. This bound is called *Noether's bound.*

Theorem 2.3 (**Noether's bound**). *Suppose char$(K) = 0$ and G be a finite group. Then the invariant ring $K[W]^G$ is generated by at most $\binom{n+|G|}{n}$ invariants of degree at most $|G|$.*

Proof. With a choice of a basis, let $K[W] = K[x_1, x_2 \dots x_n]$. Now for any tuple $\mu = (\mu_1, \mu_2 \dots \mu_n) \in \mathbb{N}^n$, define $j_\mu = \sum_{g \in G} g(x_1^{\mu_1} x_2^{\mu_2} \dots x_n^{\mu_n})$

Now let $f = \sum_\mu a_\mu x_1^{\mu_1} x_2^{\mu_2} \dots x_n^{\mu_n} \in K[W]^G$ be an invariant function. Then $|G|\dot{f} = \sum_\mu a_\mu j_\mu$. Hence the j_μs are capable of generating the invariant ring. We now need to show that the subset $D = \{j_\mu : |\mu| = \sum_j \mu_j \leq |G|\}$ will do, as there are exactly $\binom{n+|G|}{n}$ of these.

To show this, we assume the following lemma which can be proved using *Newton's identities.*

Lemma 2.4. *If char$(K) = 0$, the ring of symmetric polynomials of $K[x_1, x_2, \dots x_n$ can be generated by the power sum symmetric polynomials $p_j = x_1^j + x_2^j + x_3^j + \dots + x_n^j$ for $j = 0, 1, 2 \dots n$*

Now we define

$$p_j(x_1, x_2, \dots, x_n, z_1, z_2, \dots, z_n) = \sum_{g \in G} (gx_1.z_1 + gx_2.z_2 + \dots gx_n.z_n)^j$$

Clearly, we have $p_j = \sum_{|\mu| = j} j_\mu z_1^{\mu_1} z_2^{\mu_2} \dots z_n^{\mu_n}$. Now, by the lemma written earier, we have that each p_j with $j > |G|$ can be expressed as a polynomial in the simpler in the p_i for $i \leq |G|$. This hence means, by matching the corresponding coefficients, j_μ with $|\mu| > |G|$ can be broken down into smaller j_λ belonging to the subset D that needs to be proved the set of generators as above. This concludes the proof.

$\square$

The above theorem gives us a bound for the degree and number of generators. In fact, via the proof, we actually know which invariants should we expect to be the generators (which is, the set D).

Via examples, we can show that this bound cannot be made better universally for all finite groups.

2.4 Molien's theorem

A very beautiful and important theorem relevant for invariant theory of finite groups is the Molien's theorem. Here we will see a version of the theorem and a note about its use. From now on, for simplicity, we take the field K to be the complex field $\mathbb{C}$ and $W = \mathbb{C}^n$.

Theorem 2.5 (**Molien's theorem**). *If G is a finite subgroup of $GL_n(\mathbb{C})$ acting linearly on $K[W]$. Let $\mathbb{C}[W]_i^G$ denote the vector space generated by all homogeneous invariants of degree i. Put $H(\mathbb{C}[W]^G, t) = \sum_{i=0}^{\infty} dim(\mathbb{C}[W]_i^G)t^i$.*

The theorem then states that

$$H(\mathbb{C}[W]^G, t) = \frac{1}{|G|} \sum_{M \in G} \frac{1}{\det(I - tM)}$$

Proof. Let $g = |G|$ and $R = \mathbb{C}[W]$.

Since we have a finite group, we have a Reynold's operator $\rho : R \to R^G$ at your disposition. Also, ρ induces a map on each vector space R_i (the graded component of R). We denoted this map by $\rho_i = \rho|_{R_i}$

Note that $\rho_i^2 = \rho_i$, which means that the only eigenvalues are 1 and 0. Hence

$$dim(R_i^G) = rank(\rho_i) = trace(\rho_i) = \frac{1}{g} \sum_{M \in G} trace(M|_{R_i})$$

Notice here that by $M|_{R_i}$, we mean an endomorphism of R_i as a vector space. The above equation implies the following.

$$H(\mathbb{C}[W]^G, t) = \sum_{i=0}^{\infty} dim(\mathbb{C}[W]_i^G)t^i = \frac{1}{g} \sum_{M \in G} \sum_{i=0} trace(M|_{R_i})$$

Hence it would be sufficient to prove that $\sum_{i=0}^{\infty} trace(M|_{R_i}) = \frac{1}{\det(I - tM)}$

Since $\mathbb{C}$ is algebraically closed, and M is a matrix of finite order, M is diagnolizable. Tho argue this, take the representation of the cyclic group generated by M that agrees with this representation and diagonalize it into irreducibles (all irreducible representation of a cyclic group are 1-dimensional).

Moreover, we have that $M|_{R_i}$ is diagnolizable, similarly. Now focus on $M|_{R_1}$. It is easy to see that $M_{R_1} = M$, because R_1 is actually the vector space W.

Hence, we can choose a basis $x'_1, x'_2, \dots x'_n$ for the vector space that will yield corresponding eigenvectors of $\lambda_1, \lambda_2, \dots \lambda_n$.

More than this, it should be noted that the eigenvectors of $M|_{R_i}$ are precisely monomials of $x'_1, x'_2, \dots x'_n$ of degree i and the corresponding eigenvectors are $\lambda_1^{\alpha_1}\lambda_2^{\alpha_2}\dots\lambda_n^{\alpha_n}$ such that $\sum_j \alpha_j = i$.

Hence

$$\sum_{i=0}^{\infty} trace(M|_{R_i}) = \sum_{\alpha} \lambda_1^{\alpha_1}\lambda_2^{\alpha_2}\dots\lambda_n^{\alpha_n} = \prod_{i=0}^{\infty} \frac{1}{(1-\lambda_i t)} = \frac{1}{\det(I - tM)}$$

□

Molien's theorem explicitly gives out the generating function of the dimensions of the graded components of the invariant ring. Such a generating function is called a *Hilbert series* and is a very powerful tool in commutative algebra.

Evaluating the Hilbert series of an invariant ring series assists us in finding homogeneous basis elements of each degree. When we try to collect some of those homogeneous elements and try to evaluate the corresponding Hilbert series, if we obtain the same series given by the Molien's theorem, we are done! Hence this can be a very powerful tool to find the generators of invariant rings.

2.5 Conclusion

Classically, invariant theory has dealt with trying to understand the action of groups on polynomial rings, or more generally, on coordinate rings of algebraic varieties. A lot of work has been done in trying to find efficient ways of finding generators of invariant rings.

Invariant theory has applications modular representation theory, algebraic topology, Galois theory, quadratic forms, projective geometry and representation theory of semisimple Lie groups.

References

[1] Invariant Theory, Victor Kac (2006)

[2] Ring of invariants of finite groups, J.K Verma

[3] Kraft H., Processi C. *Classical Invariant Theory, a primer*, July 1996

[4] V. Lakshmibai, Justin Brown-Flag *Flag Varieties An Interplay of Geometry, Combinatorics, and Representation Theory* (Texts and Readings in Mathematics) (2009)

[5] J. L. Alperin, Rowen B. Bell *Groups and Representations*, Graduate Texts in Mathematics 162, Springer-Verlag New York (1995)