Invariant theory for finite groups

June 8, 2016

Nihar Prakash Gargava
Department of Mathematics and Statistics
IIT Kanpur

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

Acknowledgements

I acknowledge Prof. Preena Samuel for providing her invaluable guidance and mentorship.

Contents

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 Invariant ring

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 $x_1, x_2 \dots x_n$ 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 $K[W] = K[x_1, x_2 \dots x_n]$. 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 $x_1 \dots x_n$ tells us that $K[W]_i$ is spanned by the monomials ${x_1}^{\alpha_1}{x_2}^{\alpha_2} \dots {x_n}^{\alpha_n}$ such that $\sum_j \alpha_j = i$.

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 $K[W]^G = \bigoplus_i K[W]_i^G$

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 3.1. 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 3.1. *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. □

3.1 Hilbert's finiteness theorem

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

Theorem 3.1 (**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.

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 3.2 (**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 3.3. *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 $p_j = x_1^j + x_2^j + x_3^j + \cdots + x_n^j$ 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.

□

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.

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 4.1 (**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 $\sum_{i=0}^{\infty} trace(M|_{R_i}) = \frac{1}{\mathsf{det}(I - tM)}$

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 $x_1', x_2', \ldots x_n'$ for the vector space that will yield corresponding eigenvectors of $\lambda_1, \lambda_2, \ldots \lambda_n$.

More than this, it should be noted that the eigenvectors of $M|_{R_i}$ are precisely monomials of $x_1', x_2', \ldots x_n'$ of degree i and the corresponding eigenvectors are $\lambda_1^{\alpha_1} \lambda_2^{\alpha_2} \ldots \lambda_n^{\alpha_n}$ such that $\sum_j \alpha_j = i$.

Hence

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

□

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.

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] Classical Invariant Theory by Kraft, Processi (1996)

[2] Invariant Theory, Victor Kac (2006)

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