Invariant Theory

Rajeev Sharma

July 2020

Chapter 1

Introduction

Invariant theory is a subsection of Abstract Algebra that studies the group actions on algebraic constructs, specifically on their polynomial functions. The field originally studied the effect on non-changing polynomial functions, which are deemed invariant, in the face of this mathematical action, generally against a linear group.

The field is primarily based off of the advances made by British mathematician Arthur Cayley. A majority of his work centered around the linear transformations of invariant algebraic forms. The advances made within this field have led to remarkable growth in other areas of math including study of symmetric groups and functions, commutative algebra, and Lie group representation.

The following sections will include mathematical background on Invariant Theory, Hilbert's proof of the Basis Theorem, and Hilbert's Invariant Theorem.

Chapter 2

Invariant Theory: an Overview

2.1 Background

For a brief introduction, let G be a group, and V a finite vector space over k (field). For our purposes, let k be a representation of complex numbers.

Representing our group G in V, we get the group homomorphism $\pi : G \to GL(V)$.

If $k[V]$ is our ring of polynomial functions $\in V$, then actions of $G \in V$ produce another action on $k[V]$. This is realized through this formula:

$$(g \cdot f)(x) := f(G^{-}1(x)) \text{ for all } x \in V, g \in G, f \in k[V].$$

This thus brings us to consideration of the subspaces which contain invariant polynomial functions within this group. Therefore, we want to find an f such that $g \cdot f = f$, for all $g \in G$. This is our first space of invariant polynomials, an it can be denoted $k[V]^G$.

Chapter 3

Hilbert's Theorem

A particularly important part of invariant theory are Hilbert's set of theorems. First researched by the German mathematician David Hilbert, the theorems build on advances established by various other European mathematicians. A detailed analysis of the proof follows.

3.1 Introductory Definitions

The German mathematician David Hilbert used invariant theory in one of his most groundbreaking theorems, written in 1890, that rigorously proved an open question in Invariant Theory:

If V is a finite representation of our complex group G, with $G = SL_n(C)$, then does our invariant ring G, which acts on our polynomial $R = S(V)$, produce a finitely generated result?

The proof introduced the novel usage of the Reynolds operator. A common definition defines it as $R(R(\phi)\psi) = R(\phi)R(\psi)$ for all ϕ and ψ.

Alternatively, this can also be defined via group notation. If G acts on V, with $V = C^2$, then G is also active on $R = C[V] = C[x, y]$. This is due to the identity $(g \bullet F)(x, y) = F(g^{-1} \bullet (x, y))$. Additionally, note that R^G is a subring R of functions $F(x, y)$ such that $g \bullet F = F$.

When group G is linearly reductive, every G-invariant subspace W of V has a G-invariant complement. This is noted as:

$$V = W \oplus W^C$$

Whenever group G is linearly reductive, R^G can be split as $R^G \to R : R_d = R_d^G \oplus T$.
This projection $R \to R^G$ is the R^G linear map that is referred to at the Reynolds operator.
Furthermore, when G is finite,

$$\mathrm{R(f)} = \tfrac{1}{|G|} \textstyle\sum_{g \in G} g \bullet f.$$

The operator can also be obtained via integration.

Within the Hilbert proof, the Reynolds operator was modified, defined as an operator ρ from $R \to R^G$, such that:

$$\rho(1) = 1$$
$$\rho(a + b) = \rho(a) + \rho(b)$$
$$\rho(ab) = a\rho(b)$$

This applies when a is our set of invariants.
Using this definition, Hilbert was able to answer the above question.

3.2 Basis Theorem - Hilbert

Theorem: If R is a ring, let $R[X]$ denote the ring of indeterminate polynomials of X over R. The basis theorem states:

If ring R is a left Noetherian ring, then (polynomial) ring $R[X]$ is also a left Noetherian ring.

Suppose $a \subseteq R[X]$ is a generated, non-finite ideal. Then, observe the sequence $f_0, f_1, \ldots$ such that b_n is the left ideal of $f_0, \ldots, f_{n-1}$, with $f_n \in a\ b_n$ being of a minimal degree.

Through this, it can be determined that $deg(f_0), deg(f_1), \ldots$ are a non decreasing natural sequence.

Additionally, let a_n be the leading coefficient of f_n, while also letting b be the left ideal in R. This can be generated by the sequence $a_0, a_1, \ldots$.

Since R is the Noetherian chain of ideals, $(a_0) \subset (a_0, a_1) \subset (a_0, a_1, a_2) \subset \ldots$ will eventually terminate.

Then, consider $b = (a_0, \ldots, a_{N-1})$ for some set of integers N. In particular, observe the form a_N

$$= \sum_{i<N} u_i a_i, u_i \in R$$

Then, observe

$$g = \sum_{i<N} u_i X^{deg(f_n)-deg(f_i)}$$

The leading term of the above is equal to f_n. Furthermore, $g \in b_N$. That being said, $f_N \notin b_N$, meaning that $f_N - g \in a\ b_N$ has a degree less than f_N, thus contradicting and completing our proof.

3.3 Proof

Begin with a ring R. Grade this ring with the use of degrees. Ideal I is defined to be the ideal that is generated by the invariants of positive outputs. Using Hilbert's basis theorem (referred above) the ideal I is finitely generated (solely as an ideal). Thus I is generated by a finite number of G related invariants.

Let $i_1, \ldots, i_n$ be a finite set of G invariants, which generate the ideal I. Then, show that these generate the invariant ring R_G.

Describe x as a homogeneous invariant of degree d greater than 0. Then, define x as the following: $x = a_1 1_i + \cdots + a_n i_n$ for any a_j in the noted ring R because x is part of ideal I.

Then, assume that note that a_j is homogeneous for degree d through degree i_j for all j. Finally, applying the Reynolds operator to our x gives us:

$$x = \rho(a_1)i_1 + \cdots + \rho(a_n)i_n$$

After that, we now have to show that x lies within R that is generated via $i_1 \ldots i_n$.

Begin by analyzing the first case, where elements of $\rho(a_k)$ are lesser than d in regards to their degree. Via an induction assumption, all elements within this case are in the respective R algebraic operator. Thus, our x is also within this grouping. $(x = \rho(a_1)i_1 + \cdots + \rho(a_n)i_n)$

In the second case, it is impossible to determine whether all elements have a degree lesser than d. However, it is still possible to prove the above theorem in an inductive manner. Begin by replacing each $\rho(a_k)$ with its component between degree d and degree i_j. This modified set of $\rho(a_k$ still remain as invariants, while also having a degree lesser than d. Additionally, the equation $x = \rho(a_1)i_1 + \cdots + \rho(a_n)i_n$ continues to be true. Thus, it can be determined that x, in all magnitude, lies within the $i_1, \ldots, i_n$ R algebra, meaning, via induction, that all elements of R^G continue to lie in the above R algebra.