An Introduction to Hilbert's Finiteness Theorem in Invariant Theory

Matthew Ho

July 12, 2020

1 Introduction

Classical invariant theory is a topic of mathematics that was created in the early 19th century by Arthur Cayley, studying the properties of polynomials which are invariant under linear transformation of the coefficients. These invariants form a ring, called the invariant ring.

In 1868, Paul Gordan (often known as the "king of invariant theory") proved that the invariants of a binary form are finitely generated. Unfortunately, the method used to construct generating sets of invariants is so computationally difficult that to this day, we only know the generating set of invariants for binary forms of degree at most 10. We will state Gordan's theorem in this paper, but its proof, involving the symbolic method, is outside the scope of this paper. One can learn about the symbolic method in [KR84].

Because the method Gordan used was so computationally difficult, it could not be generalized to invariants of polynomials with more than 2 variables. In 1890, Hilbert found a brilliant new approach to this problem, using what is now known as Hilbert's basis theorem to prove his finiteness theorem, vastly generalizing Gordan's result. We include the proofs of Hilbert's basis theorem and Hilbert's finiteness theorem in this paper.

Hilbert's finiteness theorem led to the stagnation of the field of classical invariant theory. In more recent times, geometric invariant theory was developed by Mumford in 1965. [1]

In this expository paper, we introduce Gordan's result on invariants of binary forms, and then prove Hilbert's finiteness theorem using his basis theorem. This paper assumes basic knowledge of group theory and commutative ring theory.

2 Preliminaries

We will take all rings to be commutative. The base field will always be $\mathbb{C}$, unless otherwise specified.

We begin by defining a binary form:

Definition 1. A *binary form* of degree n is a homogeneous polynomial of the form

$$\sum_{i=0}^{n} \binom{n}{i} a_i x^i y^{n-i} = \binom{n}{n} a_n x^n + \binom{n}{n-1} a_{n-1} x^{n-1} y + \ldots + \binom{n}{0} a_0 y^n.$$

[1] [MFK94] is a more recent version of his book.

Now, we introduce the concept of a group acting linearly over a vector space:

Definition 2. A group G acts linearly on $\mathbb{C}[x]$ if there is a mapping $\Phi : G \times \mathbb{C}[x] \to \mathbb{C}[x]$, satisfying the following conditions:

1. For all $f \in \mathbb{C}[x]$, $\Phi(e, f) = f$, where e is the identity of G.
2. For all $f \in \mathbb{C}[x]$ and $g, h \in G$, $\Phi(gh, f) = \Phi(g, \Phi(h, f))$.
3. For all $f_1, f_2 \in \mathbb{C}[x]$ and $g \in G$, $\Phi(g, x + y) = \Phi(g, f_1) + \Phi(g, f_2)$
4. For all $f \in \mathbb{C}[x]$, $g \in G$, and $c \in \mathbb{C}$, $\Phi(g, cf) = c \cdot \Phi(g, x)$

We define $g \circ f(x) = f(g^{-1} \circ x)$, for all $f(x) \in \mathbb{C}[x]$, $x \in X$, where we denote $\Phi(g, f)$ as $g \circ f$ for brevity.

Example 3. The symmetric group S_n acts linearly over $\mathbb{C}^n$ by permuting the coordinates.

Example 4. SL_2, the group of all 2×2 matrices with determinant 1, acts on the coefficients of all binary forms of degree n. For example, the matrix

$$M = \begin{bmatrix} 5 & 2 \\ 7 & 3 \end{bmatrix}$$

applied to the binary form

$$f(x, y) = x^2 + 6xy + 4y^2$$

results in

$$f'(x, y) = f(5x + 2y, 7x + 3y) = 431x^2 + 362xy + 76y^2.$$

3 Invariants of Binary Forms

Definition 5. An *invariant* of a binary form is a polynomial in the variables $a_0, a_1, \ldots a_n$ which remains constant under transformation under a group action of G. For binary forms, we will take $G = \mathrm{SL}_2$, or the group of 2×2 matrices with determinant 1.

Example 6. Consider the group action of SL_2 on the coefficients of binary forms of degree 2. Let

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

(with $ad - bc = 1$) and

$$f(x, y) = px^2 + qxy + ry^2.$$

Then, in general, we have

$$\begin{aligned} f'(x, y) &= p'x^2 + q'xy + r'y^2 \\ &= p(ax + cy)^2 + q(ax + cy)(bx + dy) + r(bx + dy)^2 \\ &= x^2(pa^2 + qab + rb^2) + xy(2pac + qad + qbc + 2rbd) + y^2(pc^2 + qcd + rd^2) \end{aligned}$$

Now, consider the polynomial $g(p,q,r) = q^2 - 4pr$, which acts on the coefficients of $f(x)$. Then:

$$\begin{aligned} g(p',q',r') &= (2pac + qad + qbc + 2rbd)^2 - 4(pa^2 + qab + rb^2)(pc^2 + qcd + rd^2) \\ &= -4a^2d^2pr + a^2d^2q^2 + 8abcdpr - 2abcdq^2 - 4b^2c^2pr + b^2c^2q^2 \\ &= a^2d^2(q^2 - 4pr) - 2abcd(q^2 - 4pr) + b^2c^2(q^2 - 4pr) \\ &= (ad - bc)^2(q^2 - 4pr) \\ &= q^2 - 4pr \end{aligned}$$

This shows that $g(p,q,r)$ is an invariant under the action of SL_2.

It turns out that this invariant is a *fundamental invariant*: that is, any other invariant $g'(p,q,r)$ can be written as $g'(p,q,r) = h(g(p,q,r))$, where h is a polynomial of a single variable.

Gordan's theorem states the following:

Theorem 7 (Gordan, 1868)**.** *For binary forms of degree d there exists a finite system of fundamental invariants that generate all invariants (i.e., every invariant is a polynomial expression in the fundamental invariants)*

Notice this is not the same as saying the ideal of invariants of binary forms of degree d is finitely generated.

The proof of this theorem involves the symbolic method, which is beyond the scope of this expository paper (again, one may learn about the symbolic method from [KR84]). This method is quite computationally difficult.

4 Hilbert's Basis Theorem

The ideal generated by elements $a_1, a_2, \ldots, a_n$ of a ring R will be denoted as $(a_1, a_2, \ldots a_n)$.

Definition 8. A ring R is *noetherian* if and only if every ideal is finitely generated.

Remark. This definition is equivalent to the following alternative definitions:

1. Every sequence of ascending ideals $I_1 \subset I_2 \subset \cdots$ stabilizes; that is, for every sequence of ascending ideals there exists some positive integer N such that for all $M \geq N$ we have $I_M = I_N$.
2. Every nonempty collection of ideals of R has a maximal element.

Theorem 9 (Hilbert's Basis Theorem)**.** *If R is a noetherian ring, then so is the polynomial ring $R[x_1, x_2, \ldots, x_n]$ for finite n.*

Proof. Assume that R is a noetherian ring. We shall prove $R[x]$ is noetherian as well, and proceed by induction.

Consider any ideal $I \in R[x]$; we shall prove I is finitely generated. Assume for the sake of contradiction that I is not finitely generated. Recursively define a series of polynomials $f_1(x), f_2(x), \ldots \in I$ as follows: $f_1(x)$ is a polynomial of least degree in I, and for any $i \geq 2$, $f_i(x)$ is a polynomial of least degree in $I \setminus (f_1(x), f_2(x), \ldots, f_{i-1}(x))$. If this sequence terminates, then we by definition have I is finitely generated, so we assume this sequence is infinite.

Now, define a new sequence $a_1, a_2, \ldots \in R$ so that a_i is the leading coefficient of f_i. Consider the ideal generated by $I' = (a_1, a_2, \ldots) \in R$. Because R is noetherian, I' is finitely generated. That is, there exists some finite n such that $I' = (a_1, a_2, \ldots, a_n)$.

Lemma 10. *The set $\{f_1(x), f_2(x), \ldots, f_n(x)\}$ generates all of I.*

Proof. We prove that $f_{n+1}(x)$ can be generated using $f_1(x), f_2(x), \ldots, f_n(x)$, and then we finish by induction. Because of how the sequence a is defined, we have $a_{n+1} = c_1'a_1 + c_2'a_2 + \ldots + c_n'a_n$, for $c_1', c_2', \ldots \in R$. We define $f_{n+1}'(x)$ as:

$$f_{n+1}'(x) := \sum_{i=1}^{n} c_i' f_i(x) \cdot x^{\deg(f_{n+1}(x)) - \deg(f_i(x))}$$

By our construction, $f_{n+1}'(x)$ clearly has the same leading coefficient as $f_{n+1}(x)$. Then consider $g_{n+1} := f_{n+1}'(x) - f_{n+1}(x)$. Clearly, $\deg(g) < \deg(f_{n+1}(x))$. Then $g \in (f_1(x), f_2(x), \ldots, f_n(x))$, because $f_{n+1}(x)$ was defined to be a polynomial of least degree in $I \setminus (f_1(x), f_2(x), \ldots, f_n(x))$. As $f_{n+1}'(x) \in I$ by construction, we therefore must have $f_{n+1}(x) \in I$. We can now apply induction to conclude that $I = (f_1(x), \ldots f_n(x))$ □

Now that we have that I is finitely generated, we can conclude that all ideals of $R[x]$ are finitely generated. This implies that $R[x_1, x_2, \ldots, x_{n+1}]$ is finitely generated whenever $R[x_1, x_2, \ldots, x_n]$ is finitely generated, so we can induct to a polynomial ring over R with finitely many variables, as desired. □

5 Hilbert's Finiteness Theorem

Assume that we have a group G which acts on $\mathbb{C}[x]$. We will introduce several definitions that will allow us to prove Hilbert's Finiteness Theorem. [2]

Definition 11. The *invariant ring*, denoted $\mathbb{C}[x]^G$, is defined as follows:

$$\mathbb{C}[x]^G := \{f \in C[x] \mid g \circ f = f \text{ for every } g \in G\}$$

.

Definition 12. A set X is *G-invariant* if for all elements $g \in G, x \in X$ we have $g \cdot x \in X$. In other words, it is closed under the group action of G.

By definition, we have $\mathbb{C}[x]^G$ is G-invariant.

Definition 13. A *linear algebraic group* is a subgroup of GL_n for some fixed n defined by polynomials (in other words, it has to be an affine variety).

Example 14. Any finite subgroup of GL_n is a linear algebraic group.

Example 15. SL_n is a linear algebraic group, because the determinant is a polynomial function in a matrix's entries.

Definition 16. A *Reynolds operator* $\boldsymbol{R}$ is a projection $\boldsymbol{R} : \mathbb{C}[x] \to \mathbb{C}[x]^G$, for a linear algebraic group G. It must satisfy $\boldsymbol{R}(1) = 1$ and $\boldsymbol{R}(g \circ f) = \boldsymbol{R}(f)$ for all $g \in G, f \in \mathbb{C}[x]$.

[2] Much of this setup was adapted from [DK04].

For a function $f \in \mathbb{C}[x]$, and for finite G, we define the Reynolds operator of f as follows:

$$\boldsymbol{R}(f) = \frac{1}{|G|} \sum_{g \in G} g \circ f.$$

For infinite G, an analogous expression holds with an integral instead of a sum, integrating over a *Haar measure* $d\mu$ (outside the scope of this paper).

The Reynolds operator is not defined for all groups, but it is defined for all linearly reductive groups. We will let $G = \mathrm{SL}_n$ from here, which is linearly reductive, but an identical argument holds for other linearly reductive groups.

We shall now quickly verify that this definition of $\boldsymbol{R}(f)$ satisfies the conditions set earlier, for $G = \mathrm{SL}_n$. Let us define $f(x) = 1$, the constant polynomial. $\boldsymbol{R}(1) = \sum_{g \in G} g \circ f = \sum_{g \in G} f(g \circ x) = 1$. We also have $\boldsymbol{R}(g' \circ f) = \sum_{g \in G} g \circ (g' \circ f) = \sum_{g \in G} (g \circ g') \circ f = \sum_{g \in G} g \circ f = \boldsymbol{R}(f)$, as desired.

Now, we move on to proving the main result of this expository paper: [3]

Theorem 17 (Hilbert's Finiteness Theorem)**.** *Let $G = SL_n$. Then $\mathbb{C}[x]^G$ is finitely generated; that is, there exist invariants $f_1, f_2, f_3, \ldots, f_n$ such that $f_1, f_2, \ldots \in \mathbb{C}[X]^G$ and $\mathbb{C}[x]^G = (f_1, f_2, f_3, \ldots f_n)$.*

Hilbert's original proof used the Cayley Ω process, which is outside the scope of this paper, so here we use the Reynolds operator to simplify the proof.

Proof. Consider the ideal I containing every element of $\mathbb{C}[x]^G$. Then I must be finitely generated, by Hilbert's basis theorem. Let $I = (f_1, f_2, \ldots, f_n)$, where $f_1, f_2, \ldots, f_n$ are homogeneous invariants of postive degree.

We wish to show $\mathbb{C}[x] = \mathbb{C}[f_1, f_2, \ldots, f_n]$. We shall prove this by inducting on degree. Clearly, the degree 0 portion of both rings are the same. Now, we assume that these rings agree for degrees $0, 1, \ldots, n$. Take any element $f(x) \in \mathbb{C}[x]^G$, with $\deg(f) = n + 1$. Because $f \in I$, we can write

$$f = \sum_{i=1}^{m} p_i f_i,$$

for some polynomials $p_i \in \mathbb{C}[x]$.

Because $f \in \mathbb{C}[x]^G$, $\boldsymbol{R}(f) = f$. So:

$$\begin{aligned}
f = \boldsymbol{R}(f) &= \int_{g \in G} g \circ f d\mu \\
&= \int_{g \in G} g \circ \sum_{i=1}^{m} p_i f_i d\mu \\
&= \sum_{i=1}^{m} \int_{g \in G} (g \circ p_i)(g \circ f_i) d\mu \\
&= \sum_{i=1}^{m} \int_{g \in G} (g \circ p_i) f_i d\mu \\
&= \sum_{i=1}^{m} f_i \int_{g \in G} (g \circ p_i) d\mu
\end{aligned}$$

[3] This proof was adapted from [Bor12].

$$= \sum_{i=1}^{m} f_i \boldsymbol{R}(p_i).$$

It can easily be shown $\boldsymbol{R}$ preserves degree, so $\deg(\boldsymbol{R}(p_i))\deg(p_i) = \deg(f) - \deg(f_i) < \deg(f)$. Furthermore, because $\boldsymbol{R} : \mathbb{C}[x] \to \mathbb{C}[x]^G$, we have it is an invariant. Then by induction, $\boldsymbol{R}(p_i) \in \mathbb{C}[x]^G$, implying $f \in \mathbb{C}[x]^G$, as desired. □

References

[Bor12] Richard Borcherds. Lie groups, 2012.

[DK04] Harm DERKSEN and Hanspeter KRAFT. Constructive invariant theory. In *Invariant Theory in All Characteristics, in: CRM Proc. Lecture Notes*, volume 35, pages 11–36, 2004.

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

[MFK94] David Mumford, John Fogarty, and Frances Kirwan. *Geometric invariant theory*, volume 34. Springer Science & Business Media, 1994.