INVARIANT THEORY

ISHA SINHA

1. Introduction

The theory of algebraic invariants was at the forefront of mathematics in the 19th century. In England, eminent mathematicians such as Cayley and Sylvester worked on this theory. When Salmon made useful contributions to this theory, the three were christened the "Invariant Trinity" by Hermite. In 1841, George Boole wrote what is regarded as the first paper on invariant theory. In Germany, the first mathematician to draw attention to invariant theory was Aronhold, who was followed by Clebsch and Gordan; eventually Gordan came to be known as the "King of Invariants".

In the period from 1885 to 1893, Hilbert demolished this old-style invariant theory by solving the finiteness problem of invariant theory. It was in 1890 that Hilbert proved the existence of "fundamental systems" of invariants, i.e. finite sets such that any invariant would be a polynomial in the fundamental invariants, in a paper that launched him into fame overnight. This paper is regarded as the first paper in "modern algebra". Thus the 19th century invariant theory lost its significance. However, the classical invariant theory was revived ca. 1935 by H. Weyl, I. Schur, and E. Cartan, when it was realised that classical invariant theory was really a special case of the new theory: this was made especially clear in Weyl's book *"Classical Groups"*.

The recent work by D. Mumford shone the spotlight on invariant theory again, after a period in which there were no significant develeopments. Mumford realised that invariant theory provided him with the tools that he required for his solution to the problem of "moduli" of algebraic curves. In his book on "Geometrical Invariant Theory", Mumford modernised a paper written by Hilbert in 1893 that was long forgotten, using the theory of schemes as well as the contributions of Chevalley, Nagata, Iwahori, Tate, Tits and himself. See details here, [1] [2]

So, what is an invariant? An invariant is a quantity or expression that stays the same under certain operations.

Example 1.1. The total energy in a physical system is an invariant as the system evolves over time.

Example 1.2. Loop invariants can be used to prove the correctness of an algorithm.

In invariant theory, we restrict ourselves to invariants that are polynomial functions on a vector space and invariants that remain unchanged under group symmetries such as rotations, permutations etc.

Thus, in this paper we explore the intricacies of Invariant Theory. In section 2, you will find some group theory concepts that are pertinent to your understanding of invariant theory. Section 3 features a brief explanation of the classical invariant theory and section 4 deals with Hilbert's Basis Theorem. Sections 5 and 6 feature brief descriptions of invariant ring and the symmetric group. Section 7 talks about the theorems of Hilbert and Noether that

you require before you proceed to Hilbert's Finiteness Theorem in Section 8. Lastly section 9 speaks about Noether's bounds, thus concluding this expository paper on Invariant Theory.

2. Before You Proceed

The central objects here are the linear representations of groups. For any vector space V, we write $GL(V)$ for the group of all invertible linear maps from V to itself.

Definition 2.1. Let G be a group and X be a set. An *action of G on X* is a map $\alpha : G \times X \to X$ such that $\alpha(1, x) = x$ and $\alpha(g, \alpha(h, x)) = \alpha(gh, x)$ for all $g, h \in G$ and $x \in X$. We usually write gx instead of $\alpha(g, x)$. This is called a *left action* from G on X; *right actions* are defined analogously.

Definition 2.2. If G acts on two sets X and Y, then a map $\phi : X \to Y$ is called *G-equivariant* if $\phi(gx) = g\phi(x)$ for all $x \in X$ and $g \in G$.
If $X \subset Y$ and satisfies the condition $gx \in X$ for all$x \in X$ and $g \in G$ then X is called *G-stable* and the inclusion map is called G-equivalent.

Definition 2.3. Let G be a group and V be a vector space. A *linear representation of G on V* is a group homomorphism $\rho : G \to GL(V)$.
If ρ is a representation of G, then the map $(g, v) \mapsto \rho(g)v$ is an action of G on V. Conversely, if we have an action α of G on V such that $\alpha(g, .) : V \to V$ is a linear map for every $g \in G$, then the map $g \to \alpha(g, .)$ is a linear representation. A vector space with an action of G by linear maps is also called a *G-module*.
Given a linear representation $\rho : G \to GL(V)$, we obtain a linear representation $\rho^* : G \to GL(V^*)$ on the dual space V^*, called the *dual representation* defined by

$$(\rho^*(g)x := x(\rho(g)^{-1}v) \, \forall g \in G, x \in V^*, v \in V$$

See [3] for more details.

Proposition 2.4. *Suppose $V = \mathbb{C}^n$ is a representation of a group G. This means that every element g such that $g \in G$ acts by some $n \times n$ matrix $M_g : V \to V$.*
Therefore $g \cdot v = M_g \cdot v$ and $M_e = I$, $M_{gh} = M_g M_h$. This implies that $M_{g^{-1}} = (M_g)^{-1}$.
if $f(x) \in \mathbb{C}[x]$ and $M = (m_{i,j})$ is a $n \times n$ matrix then $v \mapsto f(Mv)$ is a polynomial function given by the formula

$$f\left(\sum_{j=1}^{n} m_{1,j\times j}, \ldots, \sum_{j=1}^{n} m_{n,j\times j}\right)$$

G acts on $\mathbb{C}[x]$ as follows:
If $g \in G$ and $f(x) \in \mathbb{C}[x]$ then $(g \cdot f)(x) \in \mathbb{C}[x]$ is defined as $(g \cdot f)(v) = f(M_{g^{-1}}v)$. $M_{g^{-1}}$ is used in place of M_g to make it a *left action*. We know that $\mathbb{C}[x]$ is a ∞-dimensional $\mathbb{C}-$ vector space. The monomials here form a basis. G acts by linear transformations on $\mathbb{C}[x]$. $\mathbb{C}[x]$ is a ∞-dimensional representation of G. Refer to [4] for further details.

3. Classical Invariant Theory

What is a binary form? A binary form is simply a homogeneous polynomial in two variables. Classical Invariant Theory is defined in terms of binary forms.

Let us consider the binary quadratic form: $f(x,y) = ax^2 + bxy + cy^2$ where $a, b, c \in \mathbb{C}$.

$$SL_2 = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} : \alpha\delta - \beta\gamma = 1 \right\}$$

is the group of 2×2 matrices with determinant 1 and a matrix $A \in SL_2$ gives a linear change of coordinates in $\mathbb{C}^2$. The group SL_2 acts on the coefficients of the binary form. We make the transformation $(x,y) \mapsto (\alpha x + \gamma y, \beta x + \delta y)$. We get another polynomial $g(x,y)$ where

$$g(x,y) = f(\alpha x + \gamma y, \beta x + \delta y) = px^2 + qxy + ry^2$$

Thus, A $= \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2$, and $\begin{pmatrix} p \\ q \\ r \end{pmatrix} = M_A \begin{pmatrix} a \\ b \\ c \end{pmatrix}$,

where $M_A = \begin{pmatrix} \alpha^2 & \alpha\beta & \beta^2 \\ \alpha\gamma & \alpha\delta + \beta\gamma & \beta\delta \\ \gamma^2 & \gamma\delta & \delta^2 \end{pmatrix}$

Example 3.1. Let us consider the polynomial $f(x_1, x_2, x_3) = x_2^2 - 4x_1x_3 \in \mathbb{C}[x_1, x_2, x_3]$, knows as *the discriminant*. This can be perceived as a function from $\mathbb{C}^3$ to $\mathbb{C}$. We find that

$$f \begin{pmatrix} a \\ b \\ c \end{pmatrix} = b^2 - 4ac = q^2 - 4pr = f \begin{pmatrix} p \\ q \\ r \end{pmatrix}$$

Therefore, we can say that $f(x_1, x_2, x_3)$ is *invariant* under the action of SL_2.

Definition 3.1. From the above example, it is obvious that the discriminant is an invariant. Not only this but it is also a *fundamental invariant*, from which all other invariants can be generated. Suppose $p(x_1, x_2, x_3)$ is another polynomial invariant. Then we can say that there exists some polynomial $g(y)$ such that $p(x_1, x_2, x_3) = g(f(x_1, x_2, x_3))$.

Theorem 3.2. (Gordan) *For binary forms of degree there exists a finite system of fundamental invariants that generate all invariants (i.e., every invariant is a polynomial expression in the fundamental invariants)*

Proposition 3.3. *We may identify binary forms of degree n with vectors in $\mathbb{C}^{n+1}$: the vector space of binary forms of degree n is an $(n+1)-$dimensional representation of SL_2.*

Refer to [4] for more information.

4. Hilbert's Basis Theorem

Theorem 4.1. *Hilbert's Basis Theorem states that if A is noetherian, then the polynomial ring $A[x_1, ..., x_n]$ is noetherian.*

Corollary 4.2. *If A is noetherian and B is a finitely generated k-algebra, then B is noetherian.*

Therefore, any algebraic variety $Y \subseteq \mathbb{A}^n$ is a set of solutions of a finite system of polynomial equations.

$$f_1(x_1, ..., x_n) = 0$$
$$\vdots$$
$$f_m(x_1, ..., x_n) = 0$$

Corollary 4.3. *Every affine algebraic variety is a noetherian topological space and can be expressed uniquely as an irredundant union of irreducible varieties.*

Proof. $\phi(Y)$ is a finitely generated k-algebra and a field k is trivially noetherian, so $\phi(Y)$ is a noetherian ring. A descending chain of closed subsets $Y_1 \supseteq Y_2 \supseteq ...$ in Y gives rise to an ascending chain of ideals $I(Y_1) \subseteq I(Y_2) \subseteq ...$ in $\phi(Y)$. For more information, see, [5] ■

Given that $S \subset \mathbb{C}[x]$, we know that ideal $(S) = \{a_1(x)f_1(x) + ... + a_r(x)f_r(x) : r \in \mathbb{N}, \forall i\ a_i(x) \in \mathbb{C}[x], f_i(x) \in S\}$

Theorem 4.4. (Hilbert) *Every ideal $I \subseteq C[x]$ is generated by a finite set ($\mathbb{C}[x]$ is noetherian). Therefore, if $S \subseteq \mathbb{C}[x]$ then $(S) = (T)$ for some finite subset $T \subseteq S$. For more information, see [4]*

5. Invariant Ring

$f(x) \in \mathbb{C}[x]$ is *G-invariant* if $(g \cdot f)(x) = f(x)$ for all $g \in G$. $f(x) \in \mathbb{C}[x]$ is *G-invariant* iff it is constant on all *G-orbits* in V.

Definition 5.1. $\mathbb{C}[x]^G$ is the set of all G-invariant polynomials in $\mathbb{C}[x]$.

$\mathbb{C}[x]^G$ is a *subalgebra*. This means that it contains $\mathbb{C}$ and is closed under addition, subtraction and multiplication.
If $f_1(x), ..., f_r(x) \in \mathbb{C}[x]$ then $\mathbb{C}[f_1(x), ..., f_r(x)] := \{p(f_1(x), ..., f_r(x))|p(y_1, ..., y_r) \in \mathbb{C}[y_1, ..., y_r]\}$ is a subalgebra generated by $f_1(x), ..., f_r(x)$. To know more, see [4].

6. The Symmetric Group

$G = S_n$ acts on $V = \mathbb{C}^n$ by permuting the coordinates for $\sigma \in S_n$, M_σ is the corresponding permutation matrix S_n acts on $\mathbb{C}[x]$ as

$$(\sigma \cdot f)(x_1, ..., x_n) = f(x_{\sigma(1)}, ..., x_{\sigma(n)})$$

. The k-th elementary symmetric function is defined as

$$e_k(x) = \sum_{1 \le i_1 \le i_2 \le \cdots \le i_k \le n} x_{i_1} x_{i_2} \cdots x_{i_k}$$

Example 6.1. $e_1 = x_1 + x_2 + \cdots + x_n$ and $e_n = x_1 x_2 \cdots x_n$.

Theorem 6.1. $\mathbb{C}[x]^{S_n} = \mathbb{C}[e_1(x), \cdots, e_n(x)]$

To know more, refer to [4]

7. Theorems of Hilbert and Noether

Let $k[x]$ denote the polynomial ring in the indeterminates $x_1, x_2, ..., x_n$. Let $G < GL(n, k)$ be a finite subgroup. the ring of invariants of G is the ring

$$k[x]^G = \{f \in k[x]|M(f) = f\ \forall M \in G\}$$

Any $M \in GL(n, k)$ acts on the indeterminates linearly by the rule $(x_1, x_2, ..., x_n)^t \mapsto M(x_1, x_2, ..., x_n)^t$. This action extends to all $f \in k[x]$ so that $f \mapsto M(f)$ is an autmorphism of $k[x]$.

Definition 7.1. Let $r \in R$ be a field extension. A *transcendence basis* of R over r is a collection of elements $\{x_i\}_{i\in I}$ which are algebraically independent over r such that the extension $r(x_i \cdot i \in I) \subset R$ is algebraic.

Definition 7.2. Let $r \subset R$ be a field extension. The *transcendence degree* of R over r is the cardinality of a transcendence basis of R over r. It is a rough measure of the "size" of the extension. It is denoted as $trgdeg_r(R)$. For more information about transcendence degrees, refer to [6, Section 030D]

We know that $k[x]^{S_n}$ is generated by n elementary symmetric polynomials, that are algebraically independent. Thus $k[x]^{S_n}$ has transcendence degree n over k. This property is shared by $k[x]^G$ for all finite subgroups G of $GL(n,k)$.

Proof. We know that $trddeg_k k[x] = n$. This is sufficient to show that $x_1, x_2, \cdots, x_n$ are algebraic over $k[x]^G$. Define for $i = 1, 2, \cdots, n$;

$$P_i(t) = \prod_{g\in G}(t - g(x_i))$$

The coefficients of $P_i(t)$ are in $k[x]^G$. As $P_i(x_i)$ is integral over $k[x]^G$, for $i = 1, 2, \cdots, n$. Hence $k[x]$ and $k[x]^G$ have the same transcendence degree over k. ∎

Definition 7.3. Let R be any ring, G a finite group of automorphisms of R such that $|G|$ is invertible in R. Now if we put $S = R^G$ i.e. the ring of invariants of G acting on R. The map $\rho : R \to S$ is defined as

$$\rho(r) = \frac{1}{|G|}\sum_{g\in G} g(r)$$

Then ρ is S-linear and $\rho|s = id_s$. Such a map ρ is called a *Reynold's operator* of the pair $S \subset R$. To know more about the theorems of Hilbert and Noether, refer to [7].

8. Hilbert's Finiteness Theorem

Theorem 8.1. *Let G be a subgroup of $GL(n,k)$, acting linearly on $k[x] = R$. $S = k[x]^G$. Suppose that there is a Reynold's operator $\rho : R \to S$. Then S is a finitely generated k-algebra.*

Proof. Let M be the maximal ideal of S generated by homogeneous elements of positive degree. Since R is noetherian, MR has finitely many generators. Let these be homogeneous elements $f_1, f_2, \cdots, f_s \in M$.
We claim that $R = k[x]^G = k[f_1, f_2, \cdots, f_s]$. Let $f \in R$ be homogeneous of degree d. We apply induction on d. If $d = 0, f \in k$. Suppose that $d > 0$. Then $f \in M$. Hence $\exists\, g_1, g_2, \cdots, g_s \in R$ such that $f = \rho(g_1)f_1 + \cdots + \rho(g_s)f_s$. We assume that g_i are homogeneous. Then $deg\ \rho(g_i) = deg\ g_i = deg\ f - deg\ f_i < deg\ f$.
Since, $deg\rho(g_i)$ are of smaller degree than $degf$, by induction, $\rho(g_1), \cdots, \rho(g_s) \in k[f_1, f_2, \cdots, f_s]$.
Hence, $f \in k[f_1, f_2, \cdots, f_s]$. ∎

Definition 8.2. The characteristic of a ring R, denoted char R, is the least number of times its multiplicative identity must be used in a sum to yield the additive identity. If this sum never yields the additive identity of the ring, then the ring is said to have characteristic zero. If $1 + 1 + \cdots$ (n times) $= 0$ (where 1 is the multiplicative identity and 0 is the additive identity of a ring R, then char R $= n$ for all $n \in \mathbb{N}$.

Corollary 8.3. *Let G be a finite subgroup of $GL(n,k)$ acting linearly on $k[x]$. Suppose that $(|G|,\ char\ k)=1$. Then $k[x]^G$ is a finitely generated k-algebra.*

See, [7]

9. Noether's Bound

Theorem 9.1. *Let $G \subset GL(n,k)$ be a finite subgroup of order g such that $(g,\ char\ k)=1$. Then $k[x]^G$ is generated by atmost $\binom{n+g}{n}$ invariants of degree atmost g.*

Proof. For an integral vector $(\alpha_1, \alpha_2, \cdots, \alpha_n) \in \mathbb{N}^n$, we have

$$\rho(x^\alpha) = \frac{1}{g}\sum_{M\in G} M(x^\alpha).$$

The action of M on $k[x]$ gives rise to an automorphism of $k[x]$. We must keep in mind that $M(x_i)$ is the i^{th} entry of the column vector $M(x_1, x_2, \cdots, x_n)^t$. Let

$$f(x) = \sum_\alpha f_\alpha x^\alpha,\ f_\alpha \in k$$

be an invariant and put $M(x^\alpha) = M(x_1^{\alpha_1})\cdots M(x_n^{\alpha_n})$. Then

$$f = \rho(f(x_1, x_2, \cdots, x_n)) = \frac{1}{g}\sum_{\alpha, M} f_\alpha M(x_1)^{\alpha_1}\cdots M(x_n)^{\alpha_n}.$$

Thus each invariant is the k-linear combination of the invariants $\sum_M M(x^\alpha) := J_\alpha$. Let $u_1, u_2, \cdots, u_n$ be another set of variables. In the polynomial

$$S_d(u) = \sum_M (u_1 M(x_1) + \cdots + u_n M(x_n))^d,\ d = |\alpha|$$

J_α appears upto a constant factor as the coefficient of $u_1^{\alpha_1}u_2^{\alpha_2}\cdots u_n^{\alpha_n}$. The polynomial $S_d(u)$ is the d^{th} power sum in the g polynomials $u_1M(x_1)+\cdots+u_nM(x_n)$. By Newton's identities, we now know that $S_d(u)$ are polynomials in the first g power sums $S_1(u), S_2(u), \cdots, S_g(u)$. Hence all invariants J_α where $|\alpha| > g$ are in the subring $k[J_\alpha |\ |\alpha| \le g]$. Hence

$$k[x]^G = k[J_\alpha |\ |\alpha| \le g]$$

which shows that $k[x]^G$ can be generated by $\binom{n+g}{n}$ of $\rho(x^\alpha)$ where $|\alpha| \le g$. ∎

Example 9.1. Let p be a prime number and $n \ge 2$. Let us consider the cyclic group

$$G = \{diag(w^k, w^k, \cdots, w^k) : k = 0, 1, \cdots, p-1\}$$

where $w = e^{2\pi i/p}$. Then $\mathbb{C}[x]^G = C[\{x^\alpha |\ |\alpha| = p\}]$.

Proof. Let $\rho : \mathbb{C}[x] \to \mathbb{C}[x]^G$ be the Reynold's operator. Then

$$\rho(x^\alpha) = \frac{1}{p}\sum_{k=0}^{p-1}(w^k x_1)^{\alpha_1}\cdots(w^k x_n)^{\alpha_n} = \frac{1}{p}\sum_{k=0}^{p-1} w^{k|\alpha|}x^\alpha = \frac{x^\alpha}{p}\sum_{k=0}^{p-1} w^{k|\alpha|}$$

If $(p, |\alpha|) = 1$ then $w^{|\alpha|}$ is a primitive p^{th} complex root of 1. Hence $\sum_{k=0}^{p-1} w^{k|\alpha|} = 0$. If $p |\ |\alpha|$ then $\rho(x^\alpha) = x^\alpha$. Hence $\mathbb{C}[x]^G$ is generated as a $\mathbb{C}$-algebra by all monomials of total degree p. ∎

From the above example, it is clear that *Noether's bound* is the best possible under the given assumptions. For further information, refer to [7].

Bibliography

[1] Jean A Dieudonné and James B Carrell. Invariant theory, old and new. *Advances in mathematics*, 4(1):1–80, 1970.

[2] David W Lewis. David hilbert and the theory of algebraic invariants. *Irish Math. Soc. Bull*, 33:42–54, 1994.

[3] Jan Draisma and Dion Gijswijt. Invariant theory with applications. *Lectures, October*, 8, 2009.

[4] Harm Derksen. An introduction to invariant theory. `https://www.youtube.com/watch?v=3jksqrYuvuk`, 2018.

[5] Bullett Shaun, Fearn Tom, and Smith Frank. *Geometry in Advanced Pure Mathematics*, volume 4. World Scientific, 2017.

[6] The Stacks project authors. The stacks project. `https://stacks.math.columbia.edu`, 2020.

[7] JK Verma. Ring of invariants of finite groups.