INVARIANT THEORY OF FINITE GROUPS

DAVID WHITE

Let k have characteristic zero and let $G \leq \mathrm{GL}(n,k)$ be finite. We'll use the following notation: $(x_1, \dots, x_n) = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$ and $k[f_1, \dots, f_n]$ is the ring of polynomial expressions in $f_1, \dots, f_m$ with coefficients in k. It's a subring of $k[x_1, \dots, x_n]$.

1. Basic Definitions and Questions

Definition 1. *$f(\mathbf{x}) \in k[\underline{x}]$ is* **invariant under** *G if $f(\mathbf{x}) = f(A \cdot \mathbf{x})$ for all $A \in G$. The* **ring of invariants** *is the subring $k[\underline{x}]^G$ of such polynomials.*

Lemma 1. *If $G = \langle A_1, \dots, A_m \rangle$ then $f \in k[\underline{x}]^G$ iff $f(\mathbf{x}) = f(A_1 \cdot \mathbf{x}) = \cdots = f(A_m \cdot \mathbf{x})$*

Proof. Straight-forward induction on m. □

As an example, let's compute the ring of invariants for a the Klein four-group

$$V_4 = \left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \right\} = \left\langle A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle$$

The previous lemma tells us that a polynomial $f \in k[x,y]$ is invariant under V_4 if and only if

$$f(x,y) = f\Big(\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \Big) = f(-x,y) \text{ and } f(x,y) = f\Big(\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \Big) = f(x,-y).$$

$$f(x,y) = f(-x,y) \Leftrightarrow \sum_{ij} a_{ij} x^i y^j = \sum_{ij} a_{ij} (-x)^i y^j = \sum_{ij} (-1)^i a_{ij} x^i y^j$$

This occurs iff i is even. Similarly $f(x,y) = f(x,-y)$ iff j is even. So $f(x,y) = g(x^2,y^2)$, i.e. $k[x,y]^{V_4} = k[x^2,y^2]$.

Another example is $k[\underline{x}]^{S_n}$ which is the ring of symmetric functions (i.e. f s.t. $f(x_{i_1}, \dots, x_{i_n}) = f(x_1, \dots, x_n)$ for all permutations $i_1, \dots, i_n$ of $1, \dots, n$)

Two fundamental questions: Finite Generation and Uniqueness

2. Finite Generation

Definition 2. *The* **Reynolds operator** *of G is the map $R_G : k[\underline{x}] \to k[\underline{x}]$ defined by the formula*

$$R_G(f(\mathbf{x})) = R_G(f)(\mathbf{x}) = \frac{1}{|G|} \sum_{A \in G} f(A \cdot \mathbf{x})$$

We can think of $R_G(f)$ as measuring the average effect of the group G on a polynomial f.

Proposition 1. *If $f \in k[\underline{x}]$, then $R_G(f) \in k[\underline{x}]^G$.*

Proof. Show that $R_G(f)(B \cdot \mathbf{x}) = R_G(f)(x)$ for all $B \in G$. Because G is a group, $\{A \in G\} = \{AB : A \in G\}$, so

$$\sum_{A \in G} f(A \cdot \mathbf{x}) = \sum_{AB \in G} f(AB \cdot \mathbf{x})$$

$\square$

Proposition 2. *$f \in k[\underline{x}]^G \Rightarrow R_G(f) = f$. Also, R_G acts k-linearly*

This is clear from the definition ($f(A\mathbf{x}) = f(\mathbf{x})$ for all $A \in G$).

The Reynolds operator gives us a way to compute invariants.

$$R_{V_4}(f(x,y)) = \frac{1}{4}(f(x,y) + f(-x,y) + f(x,-y) + f(-x,-y))$$

$$R_{V_4}(x^2) = \frac{1}{4}(x^2 + (-x)^2 + x^2 + (-x)^2) = \frac{1}{4}(4x^2) = x^2$$

$$R_{V_4}(x^2y^3) = \frac{1}{4}\left(x^2y^3 + (-x)^2y^3 + x^2(-y)^3 + (-x)^2(-y)^3\right) = \frac{1}{4}(2x^2y^3 - 2x^2y^3) = 0 \in k[x,y]^{V_4}$$

Theorem 1. $k[\underline{x}]^G = k[R_G(\mathbf{x}^\beta) : |\beta| \leq |G|]$.

This theorem implies $k[\underline{x}]^G$ is generated over k by finitely many homogeneous invariants.

Proof. Every invariant $f = R_G(f) = R_G(\sum_a c_a x^a) = \sum_a c_a R_G(x^a)$ so only consider monomials.

A_i is the i-th row of $A \in G$ and $\alpha = (\alpha_1, \ldots, \alpha_n)$. Define $(A \cdot \mathbf{x})^\alpha = (A_1 \cdot \mathbf{x})^{\alpha_1} \cdots (A_n \cdot \mathbf{x})^{\alpha_n}$

$$\text{Define } S_k = \sum_{A \in G} (u_1 A_1 \cdot \mathbf{x} + \cdots + u_n A_n \cdot \mathbf{x})^k = \sum_{|a|=k} b_a R_G(x^a) u^a$$

where the u_i are new variables we introduce to prevent cancellation. These S_k are symmetric.

Define $y_i = u_1 A_1 \cdot \mathbf{x} + \cdots + u_n A_n \cdot \mathbf{x}$ where i runs from 1 to $|G|$. By the Theorem of Gauss on elementary symmetric functions, $S_k = F(y_1, \ldots, y_{|G|})$ for some polynomial F with coeffs in k.

$$\text{Therefore } \sum_{|a|=k} b_a R_G(x^a) u^a = F\Big(\sum_{|\beta|=1} b_\beta R_G(x^\beta) u^\beta, \ldots, \sum_{|\beta|=|G|} b_\beta R_G(x^\beta) u^\beta\Big).$$

Expand the right side to get $b_a R_G(x^a) u^a$ as a polynomial in the $R_G(x^\beta)$. $\square$

This answers Finite Generation. But it can be hard to compute the Reynolds operator for so many polynomials

3. Finding the generators

From here on let $F = (f_1, \ldots, f_m)$ and $J_F = \langle f_1 - y_1, \cdots, f_m - y_m \rangle \subset k[x_1, \ldots, x_n, y_1, \ldots, y_m]$

How we can check if $f \in k[\underline{x}]$ is in $k[\underline{x}]^G$ and how to write f in terms of $f_1, \ldots, f_m$.

Fix a monomial order in $k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ where any monomial involving an x_i is greater than all monomials in $k[\underline{y}]$.

Proposition 3. *Let B be a Gröbner basis for J_F and let $g = f \mod B$. Then $f \in k[f_1, \ldots, f_n]$ if and only if $g \in k[\underline{y}]$. Furthermore, if this is the case $f = g(f_1, \ldots, f_m)$.*

Proof. Let $B = \{g_1, \ldots, g_\ell\}$. Then $f = A_1 g_1 + \cdots + A_\ell g_\ell + g$ for some $A_i, g \in k[x_1, \ldots, x_n, y_1, \ldots, y_m]$.

$(\Leftarrow)$: Given $g \in k[\underline{y}]$, note that substituting f_i for y_i in the above formula does not affect f but sends every polynomial in J to zero, including $g_1, \ldots, g_\ell$. This leaves us with $f = g$, showing $f \in k[f_1, \ldots, f_n]$. This substitution proves the remark.

$(\Rightarrow)$: Given $f = h(f_1, \ldots, f_m)$ for some $h \in k[\underline{y}]$, note that we can write $f = h(f_1, \ldots, f_m) = h(y_1, \ldots, y_m) + D_1(f_1 - y_1) + \cdots + D_m(f_m - y_m)$ after some algebraic manipulations.

Let $B' = B \cap k[\underline{y}] = \{g_1, \ldots, g_k\}$ for $k \leq \ell$ after relabeling. Let $h' = h \mod B'$. Then $f = h'(y_1, \ldots, y_m) + D'_1(f_1 - y_1) + \cdots + D'_m(f_m - y_m)$ and no term of h' is divisible by an element of $\mathrm{LT}(B)$. This proves that $h' = g$ so $g \in k[\underline{y}]$. □

4. Uniqueness

Uniqueness fails iff $g_1(f_1, \ldots, f_m) = g_2(f_1, \ldots, f_m)$ for $g_1, g_2 \in k[\underline{y}]$ iff $h(f_1, \ldots, f_m) = 0$ where $h = g_1 - g_2$.

Define the **ideal of relations** as $I_F = \{h \in k[\underline{y}] : h(f_1, \ldots, f_m) = 0 \text{ in } k[\underline{x}]\}$, where $F = (f_1, \ldots, f_m)$. It's prime because $char(k) = 0$. It captures all algebraic relations among the f_i.

Proposition 4. *Suppose $f = g(f_1, \ldots, f_m) \in k[\underline{x}]^G$ is one representation of f. Then all such representations are given by $f = g(f_1, \ldots, f_m) + h(f_1, \ldots, f_m)$, as h varies over I_F.*

Corollary 1. *A given element $f \in k[\underline{x}]^G$ can be written uniquely in terms of $f_1, \ldots, f_m$ iff $I_F = \{0\}$*

Proposition 5. *$I_F = J_F \cap k[\underline{y}]$ and if B is a Gröbner basis of J_F then $B \cap k[\underline{y}]$ is a Gröbner basis for I_F.*

Proof. The proof of (1) is similar to the our earlier proof. Then (2) is elimination theory. □

Fixing a Gröbner basis gives us a unique remainder, so even if $I_F \neq \{0\}$ we can find a unique representative mod G for each f_i and so get an essentially unique generating set.

5. Geometric Applications

Define $V_F = V(I_F) \subset \mathbb{A}^m_k$. Then V_F is a variety because I_F is prime. Also, $I_F = I(V_F)$.

Proposition 6. $k[V_F] \cong k[\underline{y}]/I_F \cong k[\underline{x}]^G$

Proof. The first isomorphism is true because $I_F = I(V_F)$.

The second can be defined by a map $\phi : k[\underline{y}]/I_F \to k[\underline{x}]^G$ s.t. $\phi([g]) = g(f_1, \ldots f_m)$. It's a surjective ring homomorphism, so use the First Isomorphism Theorem. □

Corollary 2. *Suppose that* $k[\underline{x}]^G = k[f_1, \dots, f_n] = k[f'_1, \dots, f'_m]$*. Then* $V_F \subset k^m$ *and* $V_{F'} \subset k^{m'}$ *are isomorphic.*

So V_F is unique up to isomorphism.

Proof. This follows from applying the above twice and by transitivity of isomorphism. □

Suppose now that k is algebraically closed and $k[\underline{x}]^G = k[f_1, \dots, f_n]$.

Theorem 2.

(1) *The map* $F : k^n \to V_F$ *defined by* $F(\mathbf{a}) = (f_1(\mathbf{a}), \dots, f_m(\mathbf{a}))$ *is surjective. Geometrically this means that the parametrization* $y_i = f_i(x_1, \dots, x_n)$ *covers all of* V_F*.*

(2) *The map sending the* G*-orbit* $G \cdot \mathbf{a} \subset k^n$ *to the point* $F(\mathbf{a}) \in V_F$ *induces a one-to-one correspondence* $\mathbb{A}^n/G \cong V_F$*.*

Proof. Part (1) will follow from elimination theory and two lemmata:

(1) There are invariants $g_1, \dots, g_{|G|} \in k[\underline{x}]^G$ such that $f^{|G|} + g_1 f^{|G|-1} + \cdots + g_{|G|} = 0$.

    This is proven by multiplying out $\prod_{A \in G} X - f(A \cdot \mathbf{x})$ and factoring.

(2) For each i there is a $p_i \in J_F \cap k[x_1, \dots, x_n, y_1, \dots, y_m]$ such that $p_i = x_i^{|G|}+$ terms in which x_i has degree $< |G|$.

    This is proven inductively.

For part (2) define $\widetilde{F} : k^n/G \to V_F$ s.t. $G \cdot \mathbf{a} \mapsto F(\mathbf{a})$. Prove it's well-defined (easy) and 1-1...

Take $G \cdot \mathbf{a}$ and $G \cdot \mathbf{b}$ and construct invariant g s.t. $g(\mathbf{a}) \neq g(\mathbf{b})$.

$$h(A \cdot \mathbf{a}) = \begin{cases} 0 & A \cdot \mathbf{a} \neq \mathbf{a} \\ h(\mathbf{a}) \neq 0 & A \cdot \mathbf{a} = \mathbf{a} \end{cases}$$

Set $g = R_G(h)$ and note that $h(A \cdot \mathbf{b}) = 0$. Then $g(\mathbf{b}) = 0$ and $g(\mathbf{a}) = \frac{M}{|G|} f(\mathbf{a}) \neq 0$. Here M is the number of elements $A \in G$ such that $A \cdot \mathbf{a} = \mathbf{a}$ and s.t. g takes different values on each of the starting orbits. □

Summary: We solved the finite generation and uniqueness problems. We moved into geometry and established the ring isomorphism between $k[V_F]$ and $k[\underline{x}]^G$. Finally, $\mathbb{A}^n/G \cong V_F$. The next step is to take other interesting objects (not just G-orbits) and give them the structure of affine varieties in a similar way.