BASIC SETS OF INVARIANTS FOR FINITE REFLECTION GROUPS

BY LEOPOLD FLATTO[1]

Communicated by J. K. Moser, February 21, 1968

1. **Introduction.** Let V be an n-dimensional vector space over a field K of characteristic zero. Let G be a finite group of linear transformations of V. G acts naturally as a group of automorphisms of the ring of polynomials $K[x]$ if we define $(gP)(x)=P(g^{-1}x)$ for $g\in G$, $P(x)\in K[x]$. The polynomials which are invariant under G form an algebra I over K called the algebra of invariants of G. A linear transformation is said to be a reflection if it has finite order and leaves fixed an $(n-1)$-dimensional hyperplane, called its reflecting hyperplane. G is a finite reflection group if it is of finite order and is generated by reflections. Chevalley [5] has proved that for finite reflection groups, I has an integrity basis consisting of n algebraically independent forms $I_1, \cdots, I_n$. Furthermore, Shephard and Todd [10] have shown that this property of I characterizes the finite reflection groups.

If K is the real field R, then G leaves invariant a positive definite quadratic form [2] so that G is orthogonal after a linear change of variables. Coxeter [3], [4] has classified all irreducible finite orthogonal reflection groups and has computed the degrees $m_1, \cdots, m_n$ of the forms $I_1, I_2, \cdots, I_n$. These degrees are independent of the particularly chosen basis. We provide a method for computing an explicit integrity basis of I for these groups. We will relate this problem to a certain mean value problem.

2. **Construction of the basic set of invariants.** We now state several theorems and sketch some of the proofs. Full details will appear elsewhere. Our first theorem yields a formula for the product of homogeneous invariants forming an integrity basis of I.

THEOREM 2.1. *Let G be an irreducible finite orthogonal reflection group acting on the real n-dimensional space E_n. Let $P_m(x, y) = \sum_{\sigma\in G}(x\cdot\sigma y)^m$ $(1\leqq m<\infty)$, where $x\cdot y=x_1y_1+\cdots+x_ny_n$. Let $J(x, y)=\partial(P_{m_1}, \cdots, P_{m_n})/\partial(x_1, \cdots, x_n)$, where $m_1, \cdots, m_n$ denote the respective degrees of the basic invariant forms $I_1, \cdots, I_n$. Then $J(x, y)=\prod_{i=1}^n J_i(y)\prod_{i=1}^r L_i(x)$. The J_i's are homogeneous invariants*

[1] Supported by National Science Foundation Grant GP-7352.

(deg $J_i = m_i$) forming an integrity basis for I. The L_i's are linear forms and $L_i(x) = 0$ ($1 \leq i \leq r$) are the r reflecting hyperplanes corresponding to the reflections of G.

To prove the above theorem, we first establish the following lemma.

LEMMA: *Let $\mathcal{P}$ be the ideal generated by $P_m(x, y)$, where $1 \leq m < \infty$ and y ranges over all vectors. Let S_0 be the ideal generated by all invariants of G vanishing at 0. Then $\mathcal{P} = S_0$.*

PROOF. Let $f(x)$ be a continuous function on E_n satisfying the mean value property

$$(2.1) \qquad f(x) = \frac{1}{|G|} \sum_{\sigma \in G} f(x + t\sigma y) \quad \text{for } x \in E_n,\ t > 0,$$

y denoting a fixed vector $\neq 0$ and $|G|$ = order of G. The vectors $\sigma y (\sigma \in G)$ do not lie in a hyperplane, as G is irreducible. It follows [9] that (2.1) is equivalent to

$$(2.2) \qquad f(x) \in C^\infty \quad \text{and} \quad P_m\left(\frac{\partial}{\partial x}, y\right) f = 0, \qquad 1 < m < \infty.$$

It is shown in [11] that the mean value property

$$(2.3) \quad f(x) \in C \quad \text{and} \quad f(x) = \frac{1}{|G|} \sum_{\sigma \in G} f(x + \sigma y) \quad \text{for all } x \text{ and } y$$

is equivalent to

$$(2.4) \qquad f(x) \in C^\infty \quad \text{and} \quad s\left(\frac{\partial}{\partial x}\right) f = 0, \qquad s \in S_0.$$

Now (2.3) is clearly equivalent to (2.1) holding for all y. We conclude that (2.4) is equivalent to (2.2) holding for all y. It follows that $S_0 = \mathcal{P}$ [6].

We now outline the proof of Theorem 2.1.

Proof of Theorem 2.1. Let $\tau \in G$. Then $P_m(\tau x, y) = \sum_{\sigma \in G} (\tau x \cdot \sigma y)^m = \sum_{\sigma \in G} (x \cdot \tau^{-1} \sigma y)^m = \sum_{\sigma \in G} (x \cdot \sigma y)^m = P_m(x, y)$. Thus, for fixed y, $P_m(x, y)$ is an invariant of G and is therefore a polynomial in $I_1(x), \cdots, I_n(x)$. The m_i's are distinct [4], so that we may assume $m_1 < m_2 < \cdots < m_n$. A standard degree argument then shows

$$(2.5) \qquad P_{m_i}(x, y) = Q_i(x, y) + J_i(y) I_i(x), \qquad 1 \leq i \leq n,$$

where $Q_1 = 0$, $Q_i \in (I_1(x), \cdots, I_{i-1}(x))$ $(2 \leq i \leq n)$, $J_i(y)$ is a homogeneous polynomial of degree m_i. $(I_1(x), \cdots, I_{i-1}(x))$ denotes as usual the ideal generated by $I_1(x), \cdots, I_{i-1}(x)$. A direct computation yields $\partial(P_{m_1}, \cdots, P_{m_n})/\partial(x_1, \cdots, x_n) = J_i(y) \cdots J_n(y) \cdot \partial(I_1, \cdots, I_n)/\partial(x_1, \cdots, x_n)$. It is shown in [4] that $\partial(I_1, \cdots, I_n)/\partial(x_1, \cdots, x_n) = \prod_{i=1}^r L_i(x)$. We will now show that $J_i(y)$ $(1 \leqq i \leqq n)$ is an invariant of G and $\partial(J_1, \cdots, J_n)/\partial(y_1, \cdots, y_n) \neq 0$. This condition, which is equivalent to saying that $J_1, \cdots, J_n$ are algebraically independent, is precisely the criterion that the J_i's form and integrity basis of I [10]. We first obtain a formula for the J_i's.

We employ the following notation. For any sequence of nonnegative integers $a_1, \cdots, a_n$ let $a = (a_1, \cdots, a_n)$, $a! = a_1! \cdots a_n!$, $|a| = a_1 + \cdots + a_n$, $x^a = x_1^{a_1} \cdots x_n^{a_n}$. Thus $(x \cdot y)^m = \sum_{|a|=m} m!/a!(x^a y^a)$. Now

$$
\begin{aligned}
\sum_{\sigma_1 \in G} \sum_{\sigma_2 \in G} (\sigma_1 x \cdot \sigma_2 y)^m &= \sum_{\sigma_1 \in G} \sum_{\sigma_2 \in G} (x \cdot \sigma_1^{-1} \sigma_2 y)^m \\
&= \sum_{\sigma_1 \in G} \sum_{\sigma_2 \in G} (x \cdot \sigma_2 y)^m = |G| \, P_m(x, y).
\end{aligned} \tag{2.6}
$$

Hence

$$
\begin{aligned}
P_m(x, y) &= \frac{1}{|G|} \sum_{\sigma_1 \in G} \sum_{\sigma_2 \in G} \sum_{|a|=m} \frac{m!}{a!} (\sigma_1 x)^a (\sigma_2 y)^a \\
&= \frac{1}{|G|} \sum_{|a|=m} \frac{m!}{a!} J_a(x) J_a(y),
\end{aligned} \tag{2.7}
$$

where $J_a(x) = \sum_{\sigma \in G} (\sigma x)^a$. Since $J_a(x)$ is invariant under G, we have for $m = m_i$

$$
J_a(x) = F_a(I_1(x), \cdots, I_{i-1}(x)) + c_a I_i(x), \qquad |a| = m_i, \tag{2.8}
$$

where F_a is a polynomial in $I_1, \cdots, I_{i-1}$ ($F_a = 0$ for $|a| = m_1$) and the c_a's are constants. As a polynomial in $x_1, \cdots, x_n$, F_a is homogeneous of degree m_i. If $c_a = 0$ for all a ($|a| = m_i$), then we readily conclude that $I_i \notin \mathcal{P}$, contradicting the lemma. Thus $c_a \neq 0$ for some a, $|a| = m_i$. Substituting (2.8) into (2.7) and comparing with (2.5) we obtain,

$$
\begin{aligned}
J_i(y) &= \frac{1}{|G|} \sum_{|a|=m_i} \frac{m!}{a!} c_a F_a(I_1(y), \cdots, I_{i-1}(y)) \\
&\quad + \left(\frac{1}{|G|} \sum_{|a|=m_i} \frac{m!}{a!} c_a^2 \right) I_i(y),
\end{aligned} \tag{2.9}
$$

so that $J_i(y)$ is invariant under G $(1 \leqq i \leqq n)$. A direct computation shows

$$\frac{\partial(J_1, \cdots, J_n)}{\partial(y_1, \cdots, y_n)} = \frac{1}{|G|^n} \prod_{i=1}^{n} \left(\sum_{|a|=m_i} \frac{m!}{a!} c_a^2 \right) \frac{\partial(I_1, \cdots, I_n)}{\partial(y_1, \cdots, y_n)} .$$

Since $\sum_{|a|=m_i}(m!/a!)c_a^2 \neq 0$ for $1 \leqq i \leqq n$, we conclude $\partial(J_1, \cdots, J_n)/\partial(y_1, \cdots, y_n) \neq 0$. We obtain immediately from Theorem 2.1 the

COROLLARY. *Let y be a fixed vector $\neq 0$. $P_{m_1}(x, y), \cdots, P_{m_n}(x, y)$ form an integrity basis of I iff $J_1(y) \cdots J_n(y) \neq 0$.*

The following theorem gives an algorithm for computing the J_i's.

THEOREM 2.2. *Let $J(x, y) = (\partial P_i/\partial x_j)$. Choose from the first i rows of $J(x, y)$ an $i \times i$ minor $D_i(x, y)$ which is not identically zero. Then $D_i(x, y) = A_i(x)B_i(y)$, where $A_i(x)$ and $B_i(y)$ are polynomials not identically zero. $B_i(y) = J_i(y) \cdots J_i(y)$ so that $J_i(y) = B_i(y)/B_{i-1}(y)$ $(1 \leqq i \leqq n)$ with $B_0(y) = 1$.*

It is shown in [11] that the solution space to (2.4) is given by $D\Pi$ where $D\Pi$ denotes the linear span of the partial derivatives of $\Pi(x) = \prod_{i=1}^{n} L_i(x)$. Let $\mathcal{P}_y$ be the ideal generated by $P_m(x, y)$ $(1 \leqq m < \infty)$ where y is a fixed vector $\neq 0$. The solution space S to (2.1) (or its equivalent (2.2)) $= D\Pi$ iff $S_0 = \mathcal{P}_y$ [6]. It follows easily from (2.5) that $S_0 = \mathcal{P}_y$ iff $J_1(y) \cdots J_n(y) \neq 0$. We thus obtain

THEOREM 3.1. *Let y be a fixed vector $\neq 0$. The solution space S to* (2.1) $= D\Pi$ iff $J_1(y) \cdots J_n(y) \neq 0$.

3. The "vertex" conjecture. In view of Theorem (3.1) it is natural to ask whether there exists some canonical procedure for obtaining a vector y such that $J_1(y) \cdots J_n(y) \neq 0$. The symmetry groups of the regular polyhedra centered at the origin form a subclass of the irreducible finite orthogonal reflection groups [3]. For these groups, it is conjectured that y may be chosen as any vertex of the regular polyhedron. We refer to this conjecture as the "vertex" conjecture. It is equivalent to the following theorem.

THEOREM 3.1. *Let $y_1, \cdots, y_N$ denote the vertices of the n-dimensional polyhedron π_n centered at the origin. Let $f(x)$ be continuous in the n-dimensional region R and let it satisfy the mean value property*

$$(3.1) \qquad f(x) = \frac{1}{N} \sum_{i=1}^{N} f(x + ty_i), \qquad x \in R, \quad 0 < t < \epsilon_x.$$

Then the solution space S to (3.1) $= D\Pi$.

The "vertex" conjecture has previously been established for special polyhedra [1], [8], [12]. We have verified it for all cases, with the exception of the n-dimensional cube. In the latter case, it is equivalent to the following

UNSOLVED PROBLEM. Let $P_{2k}(x) = \sum_{\pm}(\pm x_1 \pm x_2 \pm \cdots \pm x_n)^{2k}$. Are $P_2(x), P_4(x), \cdots, P_{2n}(x)$ algebraically independent?

REFERENCES

1. E. F. Beckenbach and M. Reade, *Regular solids and harmonic polynomials*, Duke Math J. 12 (1945), 629–644.

2. W. Burnside, *Theory of groups of finite order*, 2nd ed., Cambridge Univ. Press, New York, 1911.

3. H. S. M. Coxeter, *Regular polytopes*, Methuen, London, 1948.

4. ———, *The product of the generators of a finite group generated by reflections*, Duke Math J 18 (1951), 765–782.

5. C. Chevalley, *Invariants of finite groups generated by reflections*, Amer. J. Math. 77 (1955), 778–782.

6. E. Fischer, *Über algebraische Modulsysteme und lineare homogene partiel Differentialgleichungen mit konstaten Koeffizienten*, J. Reine Angew. Math. 140 (1911), 48–81.

7. L. Flatto, *Functions with a mean value property*, J. Math. Mech. 10 (1961), 11–18.

8. ———, *Functions with a mean value property*. II, Amer. J. Math. 85 (1963), 248–270.

9. A. Friedman and W. Littman, *Functions satisfying the mean value property*, Trans. Amer. Math. Soc. 102 (1962), 167–180.

10. G. C. Shephard and J. A. Todd, *Finite unitary reflection groups*, Canad. J. Math. 6 (1954), 274–304.

11. R. Steinberg, *Differential equations invariant under finite reflection groups*, Trans. Amer. Math. Soc. 112 (1964), 392–400.

12. J. L. Walsh, *A mean value theorem for polynomials and harmonic polynomials*, Bull. Amer. Math. Soc. 42 (1936), 923–926.

BELFER GRADUATE SCHOOL OF SCIENCE, YESHIVA UNIVERSITY