Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 24 (1978)

Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: INVARIANTS OF FINITE REFLECTION GROUPS

Autor: Flatto, Leopold

Kapitel: CHAPTER II INVARIANT THEORETIC CHARACTERIZATION OF FINITE REFLECTION GROUPS

DOI: https://doi.org/10.5169/seals-49704

(1.10) and Lemma 1.2 yield

$$(1.11) \qquad \delta_m = \frac{1}{|G|} \sum_{\sigma \varepsilon G} (Tr\,\sigma)_m = \frac{1}{|G|} \sum_{\sigma \varepsilon G} \sum_{|a|=m} \omega^a(\sigma).$$

Multiply both sides of (1.11) by t^m and sum over m from 0 to ∞. We get

$$\sum_{m=0}^{\infty} \delta_m t^m = \frac{1}{|G|} \sum_{m=0}^{\infty} \sum_{\sigma \varepsilon G} \sum_{|a|=m} \omega^a(\sigma)\, t^m$$

$$= \frac{1}{|G|} \sum_{\sigma \varepsilon G} \left\{ \sum_{m=0}^{\infty} \omega_1^m(\sigma)\, t^m \ldots \sum_{m=0}^{\infty} \omega_n^m(\sigma)\, t^m \right\}$$

$$= \frac{1}{|G|} \sum_{\sigma \varepsilon G} \frac{1}{(1-\omega_1(\sigma)\,t) \ldots (1-\omega_n(\sigma)\,t)}$$

CHAPTER II

INVARIANT THEORETIC CHARACTERIZATION OF FINITE REFLECTION GROUPS

1. Chevalley's Theorem

We showed in chapter I that we can always find a finite number of homogeneous invariants forming a basis for the invariants of G and that this set must contain at least n elements, where $n = \dim V$. We show that this lower bound is attained only for the finite reflection groups. We first define these groups.

Definition 2.1. Let σ be a linear transformation acting on the n-dimensional vector space V. σ is a reflection $\Leftrightarrow$ σ fixes an $n-1$ dimensional hyperplane π and σ is of finite order > 1. π is called the reflecting hyperplane (r.h.) of σ.

Remark. Choose $v \notin \pi$. and let $\sigma v = \zeta v + p$, $p \in \pi$. If $\zeta = 1$, then $\sigma^m v = v + mp$, contradicting that σ is of finite order. Hence $\zeta \neq 1$. Let $v' = v + (\zeta - 1)^{-1} p$ and choose $p_1, \ldots, p_{n-1}$ as a basis for π. Then $\sigma p_i = p_i$, $1 \leqslant i \leqslant n-1$, $\sigma v' = \zeta v'$. ζ is a root of 1 in k which is distinct from 1, as σ is of finite order > 1. Thus σ is a reflection iff relative to some basis, the matrix for σ is diagonal, $n-1$ of the diagonal entries equalling 1 and the remaining one equalling a root of 1 in k distinct from 1.

Definition 2.2. G is a finite reflection group acting on $V \Leftrightarrow G$ is a finite group generated by reflections on V.

As an example of a finite reflection group, let $G = S_n$. It is well known that S_n is generated by transpositions. The transposition of the variables x_i, x_j $(i \neq j)$ fixes the hyperplane $x_i - x_j = 0$, so that it is a reflection.

We have the following result

Theorem 2.1 (Chevalley [4]). *Let G be a finite reflection group acting on the n-dimensional vector space V. The invariants of G have a basis consisting of n homogeneous elements which are algebraically independent over k.*

Let $k[x]$ denote the ring of polynomials in $x_i, ..., x_n$ with coefficients in k. We prove the following.

Lemma 2.1. Let $I_1, ..., I_m$ be invariant polynomials of G, $I_1 \notin (I_2, ..., I_m)$ = the ideal in $k[x]$ generated by $I_2, ..., I_m$. Suppose that $P_1 I_1 + ... + P_m I_m = 0$, the P_i's being polynomials with P_1 homogeneous. Then $P_1 \in \mathscr{I}$, where $\mathscr{I}$ is the ideal in $k[x]$ generated by the homogeneous invariants of positive degree.

Proof of Lemma 2.1. The proof proceeds by induction on $\deg P_1$. Suppose $\deg P_1 = 0$, so that $P_1 = c \in k$. If $c \neq 0$, then $I_1 \in (I_2, ..., I_m)$, contrary to assumption. Hence $c = 0 \Rightarrow P_1 \in \mathscr{I}$. Let $\deg P_1 = n > 0$. Let σ be a reflection in G and $L = 0$ the equation of its r.h. (L is a linear homogeneous polynomial). We have $P_1(x) I_1(x) + ... + P_m(x) I_m(x) = 0$, $P_1(\sigma x) I_1(x) + ... + P_m(\sigma x) I_m(x) = 0$. Hence $[P_1(\sigma x) - P_1(x)] I_1(x) + ... + [P_m(\sigma x) - P_m(x)] I_m(x)$. For $L(x) = 0$, $\sigma(x) = x$, so that $P_i(\sigma x) - P_i(x) = 0$ whenever $L(x) = 0, 1 \leqslant i \leqslant m$. Since $L(x)$ is irreducible it follows that

$$\frac{P_i(\sigma x) - P_i(x)}{L(x)}$$

is a polynomial, $1 \leqslant i \leqslant m$. We have

$$\left[\frac{P_1(\sigma x) - P_1(x)}{L(x)}\right] I_1(x) + ... + \left[\frac{P_m(\sigma x) - P_m(x)}{L(x)}\right] I_m(x) = 0 .$$

$$\deg \left[\frac{P_1(\sigma x) - P_1(x)}{L(x)}\right] < \deg P_1(x) ,$$

so that by the induction hypothesis

$$\frac{P_1(\sigma x) - P_1(x)}{L(x)} \equiv 0 \pmod{\mathscr{I}}.$$

Hence $P_1(\sigma x) \equiv P_1(x) \pmod{\mathscr{I}}$. Since the σ's generate G, this congruence holds for $\sigma \in G$. We conclude that

$$P_1(x) \equiv \frac{1}{|G|} \sum_{\sigma \varepsilon G} P_1(\sigma x) \pmod{\mathscr{I}}.$$

The polynomial $\frac{1}{|G|} \sum_{\sigma \varepsilon G} P_1(\sigma x)$ is invariant and homogeneous of degree $n \geqslant 1$. Hence it $\in \mathscr{I}$, so that $P_1 \in \mathscr{I}$.

Proof of Theorem 2.1. We choose $I_1, \ldots, I_r$ to be homogeneous invariants of positive degree forming a minimal basis for $\mathscr{I}$. Hilbert's proof of Theorem 1.1 shows that $I_1, \ldots, I_r$ form a basis for the invariants of G. We show that $I_1, \ldots, I_r$ are algebraically independent, so that $r = n$.

Suppose, to the contrary, that $I_1, \ldots, I_r$ are algebraically dependent. Choose $H(y_1, \ldots, y_r)$ to be a polynomial of minimal positive degree so that $H(I_1(x), \ldots, I_r(x)) = 0$. Let x-degree of any monomial $y_1^{a_1} \ldots y_r^{a_r}$ be $d_1 a_1 + \ldots + d_r a_r$, where $d_i = \deg I_i$. We may assume that all x-degrees of the monomials appearing in H are the same. Let

$$H_i(x) = \frac{\partial H}{\partial y_i}(I_1(x), \ldots, I_r(x)), \; 1 \leqslant i \leqslant r.$$

The H_i's are invariant homogeneous polynomials, as all monomials in H have equal x-degree. Since $H(y_1, \ldots, y_n)$ is of positive degree, some $\frac{\partial H}{\partial y_i} \neq 0$, It follows that the corresponding $H_i(x) \neq 0$, as H was chosen to be of minimal degree; i.e. not all H_i's $= 0$. We relabel indices so that $H_1, \ldots, H_s$, $1 \leqslant s \leqslant r$, are ideally independent (i.e. none of the H_i's is in the ideal generated by the others) and $H_{s+j} \in (H_1, \ldots, H_s)$. $1 \leqslant j \leqslant r - s$. Thus $H_{s+j} = \sum_{i=1}^{s} V_{ji} H_i$, $1 \leqslant j \leqslant r - s$, where each V_{ji} is a homogeneous polynomial of degree $d_i - d_{s+j}$ (V_{ji} is interpreted to be 0 if this degree is negative). Differentiating the relation $H(I_1(x), \ldots, I_r(x)) = 0$ with respect to x_k, we obtain

$$\text{(2.1)} \qquad \sum_{i=1}^{r} H_i \frac{\partial I_i}{\partial x_k} = \sum_{i=1}^{s} H_i \frac{\partial I_i}{\partial x_k} + \sum_{l=1}^{r-s} H_{s+l} \frac{\partial I_{s+l}}{\partial x_k}$$
$$= \sum_{i=1}^{s} H_i \left[\frac{\partial I_i}{\partial x_k} + \sum_{l=1}^{r-s} V_{li} \frac{\partial I_{s+l}}{\partial x_k}\right] = 0.$$

Since

$$\frac{\partial I_i}{\partial x_k} + \sum_{l=1}^{r-s} V_{li} \frac{\partial I_{s+l}}{\partial x_k}$$

is homogeneous of degree $d_i - 1$, we conclude from Lemma 2.1 that

$$\frac{\partial I_i}{\partial x_k} + \sum_{l=1}^{r-s} V_{li} \frac{\partial I_{s+l}}{\partial x_k} = \sum_{j=1}^{r} B_j I_j, \ 1 \leqslant i \leqslant s \,, \tag{2.2}$$

where the B_j's are homogeneous and each term in (2.2) is homogeneous of degree $d_i - 1$. This forces $B_i = 0$. Multiply both sides of (2.2) by x_k and sum over k. We conclude, by Euler's identity for homogeneous polynomials,

$$d_i I_i + \sum_{l=1}^{r-s} V_{li} \, d_{s+l} I_{s+l} = \sum_{j=1}^{r} A_j I_j \,, \tag{2.3}$$

the A_j's being homogeneous with $A_i = 0$.

(2.3) shows that $I_i \in (I_1, ..., I_{i-1}, I_{i+1}, ..., I_r)$, contradicting the minimality of the basis $I_1, ..., I_r$. Hence $I_1, ..., I_r$ are algebraically independent and $r = n$.

2. The Theorem of Shephard and Todd

We obtain in this section a converse to Chevalley's Theorem, thereby obtaining an invariant theoretical characterization of finite reflection groups. We first prove several preliminary results.

Lemma 2.2. Let H be a finite group of linear transformations acting on the n-dimensional space V and fixing the $n - 1$ dimensional hyperplane π. The elements of H have a common eigenvector $v \in V - \pi$. Let $\sigma(v) = \zeta(\sigma) v$, $\sigma \in H$. $\zeta(\sigma)$ is an isomorphism from H into the multiplicative group of the roots of unity in k. It follows that H is a cyclic group.

Remark. The above lemma is a consequence of Maschke's Theorem proven in section 2.3. We provide another proof below.

Proof. Let $\sigma_1 \in H$, $\sigma_1 \neq e$ (the identity of H). By the remark following Definition 2.1, there exists $v \in V - \pi$ such that $\sigma_1(v) = \zeta_1 v$, ζ_1 being a root of unity $\neq 1$. For $\sigma \in H$, let $\sigma(v) = \zeta(\sigma) v + p(\sigma)$, $\zeta(\sigma) \in k$ and $p(\sigma) \in \pi$. Let $\sigma^* = \sigma_1^{-1} \sigma^{-1} \sigma_1 \sigma$. Then $\sigma^*(v) = v + (1 - \zeta_1) p(\sigma)$. Since σ^* is of finite order, $(1 - \zeta_1) p(\sigma) = 0 \Rightarrow p(\sigma) = 0$. Hence $\sigma(v) = \zeta(\sigma) v$. $\zeta(\sigma)$ is clearly an isomorphism from H into U, the multiplicative group of the roots of unity in k. U is known to be cyclic ([22], Vol. 1, p. 112). It follows that $\zeta(H)$, a subgroup of U, is cyclic and so H is cyclic.

THEOREM 2.2. *Let G be a finite group acting on the n-dimensional space V. Let $I_1, \dots, I_n$ be homogeneous polynomials forming a basis for the invariants of G. Let $d_1, \dots, d_n$ be the respective degrees of $I_1, \dots, I_n$. Then*

$$\prod_{i=1}^{n} d_i = |G|, \quad \sum_{i=1}^{n} (d_i - 1) = r \tag{2.4}$$

where r = number of reflections in G.

Proof. By Theorem 1.2, $I_1, \dots, I_n$ are algebraically independent. Let $I(x)$ be a homogeneous invariant of degree m. Then I is a linear combination of the monomials $I_1^{a_1} \dots I_n^{a_n}$ where $a_1 d_1 + \dots a_n d_n = m$. Furthermore, these monomials are linearly independent over k, as $I_1, \dots, I_n$ are algebraically independent over k. It follows that the dimension δ_m of homogeneous invariants of degree m = number of non-negative integer solutions to $a_1 d_1 + \dots + a_n d_n = m$. Hence

$$\sum_{m=0}^{\infty} \delta_m t^m = \frac{1}{(1-t^{d_1}) \dots (1-t^{d_n})} . \tag{2.5}$$

(1.9) and (2.5) yield

$$\frac{1}{|G|} \sum_{\sigma \varepsilon G} \frac{1}{(1-\omega_1(\sigma)t) \dots (1-\omega_n(\sigma)t)} = \frac{1}{(1-t^{d_1}) \dots (1-t^{d_n})} \tag{2.6}$$

Expand both sides of (2.6) in powers of $(1-t)$. Let $\mathcal{R}$ = set of reflections in G and $\zeta(\sigma)$ = eigenvalue of the reflection σ which $\neq 1$. We have

$$\frac{1}{|G|} \sum_{\sigma \varepsilon G} \frac{1}{(1-\omega_1)(\sigma)t) \dots (1-\omega_n(\sigma)t)} \tag{2.7}$$

$$= \frac{1}{|G|} \frac{1}{(1-t)^n} + \frac{1}{|G|} \sum_{\sigma \varepsilon \mathcal{R}} \frac{1}{1-\zeta(\sigma)} \frac{1}{(1-t)^{n-1}} + \dots$$

$$\frac{1}{(1-t^{d_1}) \dots (1-t^{d_n})} = \prod_{i=1}^{n} \frac{1}{d_i(1-t) - \binom{d_i}{2}(1-t)^2 + \dots \pm (1-t)^{d_i}} \tag{2.8}$$

$$= \frac{1}{\prod_{i=1}^{n} d_i} \frac{1}{(1-t)^n} + \frac{\frac{1}{2} \sum_{i=1}^{n} (d_i - 1)}{\prod_{i=1}^{n} d_i} \frac{1}{(1-t)^{n-1}} + \dots$$

Equating coefficients of (2.7), (2.8), we get

$$\prod_{i=1}^{n} d_i = |G|, \quad \sum_{i=1}^{n} (d_i - 1) = 2 \sum_{\sigma \varepsilon \mathcal{R}} \frac{1}{1 - \zeta(\sigma)}. \tag{2.9}$$

We evaluate the sum

$$\sum_{\sigma \varepsilon \mathcal{R}} \frac{1}{1 - \zeta(\sigma)}:$$

Let π be any r.h. Let $H_\pi = \{\sigma \mid \sigma \in G \text{ and } \sigma \text{ fixes } \pi\}$. Thus H_π is the subgroup of G consisting of the identity and those reflections in G with r.h. π. Applying Lemma 2.2 to H_π, we conclude that there exists $v \notin \pi$ such that $\sigma(v) = \zeta(\sigma)\, v$ for $\sigma \in H_\pi$. Let $H_\pi' = H_\pi - \{e\}$. Since $\zeta(\sigma^{-1}) = (\zeta(\sigma))^{-1}$, we obtain

$$\sum_{\sigma \varepsilon H_\pi'} \frac{1}{1 - \zeta(\sigma)} = \sum_{\sigma \varepsilon H_\pi'} \frac{1}{1 - \zeta(\sigma^{-1})} \tag{2.10}$$

$$= \sum_{\sigma \varepsilon H_\pi'} \left(1 - \frac{1}{1 - \zeta(\sigma)}\right) = |H_\pi'| - \sum_{\sigma \varepsilon H_\pi'} \frac{1}{1 - \zeta(\sigma)}.$$

Hence

$$\sum_{\sigma \varepsilon H_\pi'} \frac{1}{1 - \zeta(\sigma)} = \frac{|H_\pi'|}{2}. \tag{2.11}$$

Summing both sides of (2.11) over all r.h. π, we get

$$\sum_{\sigma \varepsilon \mathcal{R}} \frac{1}{1 - \zeta(\sigma)} = \frac{r}{2}. \tag{2.12}$$

(2.9), (2.12) yield Theorem 2.2.

THEOREM 2.3. *Let* $f_1, \ldots, f_n$ *be polynomials in the variables* $x_1, \ldots, x_n$. $f_1, \ldots, f_n$ *are algebraically independent over* $k \Leftrightarrow$

$$\frac{\partial(f_1, \ldots, f_n)}{\partial(x_1, \ldots, x_n)} \neq 0.$$

Proof. Suppose that $f_1, \ldots, f_n$ are algebraically independent. Then $G(f_1, \ldots, f_n) = 0$ for some polynomial $G = G(y_1, \ldots, y_n)$. Assume that $G(y_1, \ldots, y_n)$ is of minimal positive degree. Differentiating this relation with respect to x_j, we get

$$(2.13) \qquad \sum_{i=1}^{n} \frac{\partial G}{\partial y_i}(f_1, \ldots, f_n) \frac{\partial f_i}{\partial x_j} = 0, \ 1 \leqslant j \leqslant n .$$

(2.13) is a system of linear equations (with coefficients in $k(x_1, \ldots, x_n)$) in the unknowns $H_i(x) = \frac{\partial G}{\partial y_i}(f_1, \ldots, f_n)$, $1 \leqslant i \leqslant n$. $\frac{\partial G}{\partial y_i} \neq 0$ for some i, as G is not constant, and $\deg \frac{\partial G}{\partial y_i} < \deg G$. It follows that the corresponding $H_i(x) \neq 0$. Thus the linear system (2.13) has a non-zero solution, so that its determinant

$$\frac{\partial (f_1, \ldots, f_n)}{\partial (x_1, \ldots, x_n)} \neq 0 .$$

Conversely, let $f_1, \ldots, f_n$ be algebraically independent. For each i, $x_i, f_1, \ldots, f_n$ are algebraically dependent. Hence there exists a polynomial $G_i(x_i, y_1, \ldots, y_n)$ of minimal positive degree in x_i such that $G_i(x_i, f_1, \ldots, f_n) = 0$. Differentiating these relations with respect to x_k, we get

$$(2.14) \qquad \sum_{j=1}^{n} \frac{\partial G_i}{\partial y_j}(x_i, f_1, \ldots, f_n) \frac{\partial f_j}{\partial x_k} + \frac{\partial G_i}{\partial x_k}(x_i, f_1, \ldots, f_n)\, \delta_{ik}, \ 1 \leqslant k \leqslant n ,$$

δ_{ik} denoting the Kronecker symbol. (2.14) may be rewritten in matrix notation as

$$(2.15) \qquad \left(\frac{\partial G_i}{\partial y_j}\right) \cdot \left(\frac{\partial f_i}{\partial x_j}\right) = D$$

where the entries of D are

$$- \delta_{ij} \frac{\partial G_i}{\partial x_j} .$$

$\det D \neq 0$, as x_i − degree of $\frac{\partial G_i}{\partial x_i} < x_i$ − degree of G_i, $1 \leqslant i \leqslant n$.

It follows from (2.15) that $\frac{\partial (f_1, \ldots, f_n)}{\partial (x_1, \ldots, x_n)} \neq 0$.

THEOREM 2.4. (Shephard and Todd [19]). *Let G be a finite group acting on the n-dimensional space V. Suppose there exists a basis of n homogeneous polynomials for the invariants of G. Then G is a finite reflection group.*

Proof. Let H be the subgroup of G generated by the reflections in G. By assumption G has n basic homogeneous invariants which, by Theorem 1.2, are algebraically independent. Since H is a finite reflection group, we conclude from Chevalley's Theorem that H has n basic homogeneous invariants $J_1, \ldots, J_n$ which are algebraically independent. Each I_i is invariant under H so that $I_i = I_i(J_1, \ldots, J_n)$, the latter quantity denoting a polynomial in the J_i's. We may assume that $I_i(J_1, \ldots, J_n)$ is a linear combination of monomials $J_1^{a_1} \ldots J_n^{a_n}$ whose x-degree $= \deg I_i$. We have

$$\frac{\partial(I_1, \ldots, I_n)}{\partial(x_1, \ldots, x_n)} = \frac{\partial(I_1, \ldots, I_n)}{\partial(J_1, \ldots, J_n)} \cdot \frac{\partial(J_1, \ldots, J_n)}{\partial(x_1, \ldots, x_n)} \tag{2.16}$$

By Theorem 2.3,

$$\frac{\partial(I_1, \ldots, I_n)}{\partial(x_1, \ldots, x_n)} \neq 0$$

and (2.16) then shows that

$$\frac{\partial(I_1, \ldots, I_n)}{\partial(J_1, \ldots, J_n)} \neq 0 .$$

It follows that there is a rearrangement $k_1, \ldots, k_n$ of $1, \ldots, n$ so that

$$\frac{\partial I_{k_1}}{\partial J_1} \cdots \frac{\partial I_{k_n}}{\partial J_n} \neq 0 .$$

Hence $I_{k_i}(J_1, \ldots, J_n)$ is of positive degree in J_i and $\deg I_{k_i} \geqslant \deg J_i$, $1 \leqslant i \leqslant n$. Applying Theorem 2.2 both to G and H, we obtain

$$\prod_{i=1}^{n} \deg J_i = |H|, \quad \prod_{i=1}^{n} \deg I_i = |G| \tag{2.17}$$

$$\sum_{i=1}^{n} (\deg J_i - 1) = \sum_{i=1}^{n} (\deg I_i - 1) = r \tag{2.18}$$

where r = number of reflections in G = number of reflections in H.

Since $\deg I_{k_i} \geqslant \deg J_i$, $1 \leqslant i \leqslant n$, we conclude from (2.18) that $\deg I_{k_i} = \deg J_i$, $1 \leqslant i \leqslant n$. Hence $\prod_{i=1}^{n} \deg I_i = \prod_{i=1}^{n} \deg J_i$, and we conclude from (2.17) that $|G| = |H|$. Thus $G = H$ and G is a finite reflection group.

3. A Formula for $\dfrac{\partial (I_1, \ldots, I_n)}{\partial (x_1, \ldots, x_n)}$

We obtain a formula which shall be used in Chapter III.

THEOREM 2.5. *Let* G *be a finite reflection group acting on the* n-*dimensional space* V. *Let* $I_1, \ldots, I_n$ *be a basic set of homogeneous invariants for* G. *Let* x *be a coordinate system for* V *and* $L_i(x) = 0$, $1 \leqslant i \leqslant r$, *the r.h.'s for* G, *each* L_i *being linear and homogeneous. Then*

$$\frac{\partial (I_1, \ldots, I_n)}{\partial (x_1, \ldots, x_n)} = c \prod_{i=1}^{r} L_i(x) \tag{2.19}$$

c being a constant $\neq 0$.

Proof. Let J the left hand side of (2.19). We observe that J is a non-zero homogeneous polynomial of degree $\sum_{i=1}^{n} (d_i - 1)$. By Theorem 2.2, $\sum_{i=1}^{n} (d_i - 1) = r$, so that $\deg J = r$. If k is the real field R, we have the following simple proof of (2.19). $I_i = I_i(x_1, \ldots, x_n)$, $1 \leqslant i \leqslant n$, is a mapping from x-space to I-space. This mapping is not $1 - 1$ in any neighborhood of a point x lying in the r.h. $L_i(x) = 0$, as any point and its reflection get mapped into the same point I. It follows from the Implicit Function Theorem that $J(x) = 0$. whenever $L_i(x) = 0$. Thus $L_i \mid J$, $1 \leqslant i \leqslant r$, and so $\prod_{i=1}^{r} L_i \mid J$. Since J, $\prod_{i=1}^{r} L_i$ have the same degree r, we have $J = c \prod_{i=1}^{r} L_i$, $c \neq 0$.

For an arbitrary field k, the theorem is proven as follows. Let π be an r.h. with equation $L(x) = 0$ and H the subgroup of h elements in G fixing π. Thus there are $h - 1$ reflections in G with r.h. π. We show that $L^{h-1} \mid J$. By Lemma 2.2, H is a cyclic group generated by an element σ. Furthermore there exists $v \notin \pi$ and a primitive h-th root of 1 such that $\sigma(v) = \zeta v$. Choose a coordinate system $y = (y_1, \ldots, y_n)$ in V so that π has the equation $y_n = 0$ and $v = (0, \ldots, 0, 1)$ σ then becomes the transformation $(y_1, \ldots, y_{n-1}, y_n) \to (y_1, \ldots, y_{n-1}, \zeta y_n)$. Let $x = \tau y$ and $J_i(y) = I_i(\tau y)$, $1 \leqslant i \leqslant n$. We have

$$J_i(y_1, \ldots, y_{n-1}, \zeta y_n) = J_i(y_1, \ldots, y_{n-1}, y_n), \; 1 \leqslant i \leqslant n \tag{2.20}$$

Let $J_i = \sum A_m y_n^m$, the A_m's being polynomials in $y_1, \ldots, y_{n-1}$. (2.20) implies that $A_m = 0$ whenever $h \nmid m$, so that $A_m = 0, 0 \leqslant m \leqslant h - 1$. Since

$$\frac{\partial J_i}{\partial y_m} = \Sigma_m A_m y_n^{m-1},$$

we conclude

$$y_n^{h-1} \left| \frac{\partial J_i}{\partial y_n}, \quad 1 \leqslant i \leqslant n \right. .$$

Hence

$$\text{(2.21)} \qquad y_n^{h-1} \left| \frac{\partial (J_1, \ldots, J_n)}{\partial (y_1, \ldots, y_n)} \right. ,$$

Since

$$\frac{\partial (J_1, \ldots, J_n)}{\partial (y_1, \ldots, y_n)} = J(x) \cdot \det \tau,$$

(2.21) is equivalent to $L^{h-1}(x) \mid J(x)$. It follows that if $L_i(x) = 0$, $1 \leqslant i \leqslant r$, are the r.h.'s for G, then $\prod_{i=1}^{r} L_i \mid J$. But J, $\prod_{i=1}^{r} L_i$ have the same degree r, so that $J = c \prod_{i=1}^{r} L_i \; c \neq 0$.

4. Decomposition of Finite Reflection Groups

We shall decompose every finite reflection group into a direct product of irreducible ones and show that it suffices to study the invariant theory of the irreducible groups.

Definition 2.3. Let the group G act on V. G is said to be reducible iff there exists a proper subspace W invariant under G; i.e. $\sigma w \in W$ for $\sigma \in G$, $w \in W$. G is said to be completely reducible iff $V = V_1 \oplus V_2$, V_1 and V_2 being proper invariant subspaces. G is said to be irreducible iff it is not reducible.

Theorem 2.6. (Maschke [22], Vol. 2, p. 179). *Let G be a finite group acting on the vector space V. If G is reducible, then it is completely reducible.*

Proof. Let V_1 be a proper invariant subspace of V. Let V_2 be a complementary subspace. Thus for $v \in V$, we have a unique decomposition

$v = v_1 + v_2, v_i \in V_i \ (i=1, 2)$. Let $\eta v = v_2$ and set $\tau = \frac{1}{|G|} \sum_{\sigma \varepsilon G} \sigma \eta \sigma^{-1}$.

τ satisfies the following:

i) $\tau \sigma = \sigma \tau, \sigma \in G$. For $\sigma \tau = \frac{1}{|G|} \sum_{\sigma_1 \varepsilon G} \sigma \sigma_1 \eta (\sigma\sigma_1)^{-1} \sigma = \tau \sigma$

ii) $\tau v_1 = 0, v_1 \in V_1$. For $\sigma^{-1} v_1 \in V_1, \sigma \in G$, so that $\eta \sigma^{-1} v_1 = 0$ $\Rightarrow \tau v_1 = 0$

iii) $(1-\tau) v \in V_1, v \in V$, 1 denoting the identity of G. For $(1-\eta) v \in V_1$, so that $(1-\eta) \sigma^{-1} v \in V_1 \Rightarrow \sigma (1-\eta) \sigma^{-1} v \in V_1, \sigma \in G$. It follows that $(1-\tau) v = \frac{1}{|G|} \sum_{\sigma \varepsilon G} \sigma (1-\eta)\sigma^{-1} v \in V_1$.

Let $V_2' = \tau V$. V_2' is invariant under G as $\sigma (\tau v) = \tau (\sigma v)$. For any v, $v = \tau v + (1-\tau) v$. It follows from iii) that $V = V_1 + V_2'$. ii), iii) imply $\tau (1-\tau) = 0 \Leftrightarrow \tau = \tau^2$. Hence $\tau v_2' = v_2'$ for $v_2' \in V_2'$. Let $v_1 + v_2' = 0$, where $v_1 \in V_1, v_2' \in V_2'$. Applying τ to both sides, we get $v_2' = 0$ and so $v_1 = 0$. Hence $V = V_1 \oplus V_2'$.

Repeated application of Maschke's Theorem yields the

Corollary. *Let G be a finite group acting on the finite-dimensional vector space V. Then $V = V_1 \oplus \ldots \oplus V_s$, the V_i's being invariant subspaces of V and G acting irreducibly on each V_i.*

For finite reflection groups, we have

Theorem 2.7. *Let G be a finite reflection group acting on V. There exists a decomposition $V = V_1 \oplus \ldots \oplus V_s$ into invariant subspaces such that:*

1) *Let $G_i = G|_{V_i}$ = group of restrictions of elements of G to V_i. Then G is isomorphic to $G_1 \times \ldots \times G_s$*

2) *Each G_i, $1 \leqslant i \leqslant s$, is a reflection group acting irreducibly on V_i.*

Proof. By the corollary to Theorem 2.6, there exists a decomposition $V = V_1 \oplus \ldots \oplus V_s$, the V_i's being invariant subspaces and G_i irreducible for $1 \leqslant i \leqslant s$. We label the V_i's so that $V_1, \ldots, V_r$ are 1-dimensional and $G|_{V_i}$ = identity.

By the remark following Definition 2.1, for each reflection σ there exists an eigenvector $v \in V - \pi$, π being the r.h. for σ. Call v a root of G. We have

(2.22) $$\dim (V_i + \pi) + \dim (V_i \cap \pi) = \dim V_i + \dim \pi .$$

If $V_i \not\subset \pi$, then $V_i + \pi = V$ and we conclude from (2.22) that $\dim V_i = \dim (V_i \cap \pi) + 1$. I.e. $V_i \cap \pi$ is a hyperplane in V_i and $\sigma|_{V_i}$ a reflection on V_i. Choose $u \in V_i - \pi$ so that u is an eigenvector of σ. u is a multiple of the root v, so that $v \in V_i$. Thus $\sigma|_{V_i}$ is a reflection of V_i if $v \in V_i$, and the identity if $v \notin V_i$. Furthermore, each root v is in some V_i, $r + 1 \leqslant i \leqslant s$, otherwise the corresponding reflection σ would have been the identity.

Let $\tilde{G}_i$ = subgroup generated by those reflections whose roots are in V_i, $1 \leqslant i \leqslant s$. It is readily checked that $G = \tilde{G}_1 \times \ldots \times \tilde{G}_s$, $G_i = \tilde{G}_i|_{V_i}$. If $\sigma \in \tilde{G}_i$ and $\sigma|_{V_i}$ = identity then σ = identity. The mapping $\sigma \to \sigma|_{V_i}$ is thus an isomorphism from $\tilde{G}_i$ onto G_i.

THEOREM 2.8. *Let G be a finite reflection group acting on V and decompose V as in Theorem 2.7. Every polynomial invariant under G is a polynomial in the invariant polynomials of $G_1, \ldots, G_s$.*

Proof. For each $v \in V$, write $v = v_1 + \ldots + v_s$, $v_i \in V_i$. By Theorem 2.7, for each $\sigma \in G$, we may write $\sigma v = \sigma_1 v_1 + \ldots + \sigma_s v_s$, $\sigma_i \in G_i$. For any polynomial function $p(v)$ on V, we have $p(v) = \sum_{i=1}^{N} p_{i1}(v_1) \ldots p_{is}(v_s)$ where $p_{ij}(v_j)$ is a polynomial function on V_j. If $p(v)$ is invariant under G, then

$$(2.23) \qquad p(v) = \frac{1}{|G|} \sum_{\sigma \varepsilon G} p(\sigma v) = \sum_{i=1}^{N} I_{i1}(v_1) \ldots I_{is}(v_s)$$

where

$$(2.24) \qquad I_{ij}(v_j) = \frac{1}{|G_j|} \sum_{\sigma_j \varepsilon G_j} p_{ij}(\sigma_j v_j)$$

is an invariant of G_j.

CHAPTER III

THE DEGREES OF THE BASIC INVARIANTS

We determine the degrees of the basic homogeneous invariants in case G is a finite reflection group. We present two different methods. The first one (Theorem 3.8), restricts itself to the case where k is the real field and has the advantage of providing an effective method for computing the