2. The Theorem of Shephard and Todd

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **24 (1978)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **27.04.2024**

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 $I_i \in (I_1, \ldots, I_{i-1}, I_{i+1}, \ldots, I_r)$, contradicting the minimality of the basis $I_1, \ldots, I_r$. Hence $I_1, \ldots, I_r$ 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 $I_1, \ldots, I_n$ be homogeneous polynomials forming a basis for the invariants of G. Let $d_1, \ldots, d_n$ be the respective degrees of $I_1, \ldots, I_n$. Then*

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

where r = number of reflections in G.

Proof. By Theorem 1.2, $I_1, \ldots, I_n$ are algebraically independent. Let $I(x)$ be a homogeneous invariant of degree m. Then I is a linear combination of the monomials $I_1^{a_1} \ldots I_n^{a_n}$ where $a_1 d_1 + \ldots a_n d_n = m$. Furthermore, these monomials are linearly independent over k, as $I_1, \ldots, I_n$ 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 $a_1 d_1 + \ldots + a_n d_n = m$. Hence

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

(1.9) and (2.5) yield

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

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

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

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

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

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

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

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

Proof. Suppose that $f_1, ..., f_n$ are algebraically independent. Then $G(f_1, ..., f_n) = 0$ for some polynomial $G = G(y_1, ..., y_n)$. Assume that $G(y_1, ..., y_n)$ 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 $H_i(x) = \dfrac{\partial G}{\partial y_i}(f_1, \ldots, f_n)$, $1 \leqslant i \leqslant n$. $\dfrac{\partial G}{\partial y_i} \neq 0$ for some i, as G is not constant, and $\deg \dfrac{\partial G}{\partial y_i} < \deg G$. 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 $\dfrac{\partial G_i}{\partial x_i} < x_i -$ degree of G_i, $1 \leqslant i \leqslant n$.

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

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

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

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

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

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

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.