1. Chevalley's Theorem

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **28.04.2024**

(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

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

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

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

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 $p_1, \dots, p_{n-1}$ 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 $x_i, \ldots, x_n$ with coefficients in k. We prove the following.

LEMMA 2.1. Let $I_1, \ldots, I_m$ be invariant polynomials of G, $I_1 \notin (I_2, \ldots, I_m)$ = the ideal in $k[x]$ generated by $I_2, \ldots, I_m$. Suppose that $P_1 I_1 + \ldots + P_m I_m = 0$, the P_i's being polynomials with P_1 homogeneous. Then $P_1 \in \mathcal{I}$, where $\mathcal{I}$ 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 $I_1 \in (I_2, \ldots, I_m)$, contrary to assumption. Hence $c = 0 \Rightarrow P_1 \in \mathcal{I}$. 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 $P_1(x) I_1(x) + \ldots + P_m(x) I_m(x) = 0$, $P_1(\sigma x) I_1(x) + \ldots + P_m(\sigma x) I_m(x) = 0$. Hence $[P_1(\sigma x) - P_1(x)] I_1(x) + \ldots + [P_m(\sigma x) - P_m(x)] I_m(x)$. 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

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

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

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

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

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

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

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