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 I GENERAL THEORY
DOI: https://doi.org/10.5169/seals-49704

of $\sum_{i=1}^{n} \frac{\partial^2 f}{\partial x_i^2} = 0$ and $\sum_{i=1}^{n} x_i^2$ is the basic invariant for the orthogonal group $O(n)$ ([23] p. 53). We use Steinberg's result to describe the solution space S_y of continuous functions on $\mathscr{R}$ satisfying the mean value property

$$2) \qquad f(x) = \frac{1}{|G|} \sum_{\sigma \in G} f(x + t\sigma y), \; x \in \mathscr{R}$$

and $0 < t < \varepsilon_x$, y denoting a fixed vector $\neq 0$. Observe that 2) is again an analog of the familiar mean value property characterizing harmonic functions ([15] p. 224). Flatto and Wiener [10] have shown that the solution spaces to 1) and 2) are identical, provided the degrees d_i are distinct and y does not belong to a certain algebraic manifold $\mathscr{M}$. $\mathscr{M}$ can be described by equations, the latter yielding an explicit integrity basis for the invariants of G.

I have tried to keep the present paper self-contained, defining and explaining most of the notions and results needed in it. Occasionally, I quote some well known results of algebra, most of which can be found in [22]. In Chapter IV we require some standard results on harmonic functions, which may be found in [15]. In Chapter III, we require Coxeter's classification of the irreducible finite reflection groups acting on R^n. It would have taken us too far afield to present this matter in detail. I present a brief exposition, without proof, of the main points of this theory which are required in the present paper. For a quick and readable account of the details, the reader is referred to [1].

CHAPTER I

GENERAL THEORY

1. The Main Theorem of Invariant Theory

We present in this chapter some basic notions and results of invariant theory. We assume throughout that G is a finite group of linear transformations acting on the finite dimensional vector space V over a given field k of characteristic 0. n designates the dimension of V.

Definition 1.1. Let $P(v)$ be a polynomial function on V. $P(v)$ is invariant of $G \Leftrightarrow P(\sigma v) = P(v)$ for $\sigma \in G$, $v \in V$.

Let $x_1, \ldots, x_n$ be a coordinate system for V. Then $P(v)$ becomes a polynomial which we designate by $P(x)$. σ is represented by a matrix which we

again designate by σ. For this coordinate system, the above definition takes the form $P(\sigma x) = P(x)$, $\sigma \in G$ and x arbitrary. Let $P(x) = \sum_{i=0}^{m} P_i(x)$, where $m = \deg P$ and $P_i(x)$ is homogeneous of degree i. Then $P(\sigma x) = \sum_{i=0}^{m} P_i(\sigma x)$. Since $P_i(\sigma x)$ is also homogeneous of degree i, we conclude that $P(x)$ is invariant under G iff $P_i(x)$ is invariant under G for $1 \leqslant i \leqslant m$. Hence the determination of the invariants of G reduces to the determination of its homogeneous invariants.

DEFINITION 1.2. Let $I_1(x), \ldots, I_k(x)$ be invariants of G. $I_1(x), \ldots, I_k(x)$ form an integrity basis for the invariants of $G \Leftrightarrow$ any polynomial invariant under G is a polynomial in $I_1, \ldots, I_k$.

As a concrete illustration of the above definitions, let G be the symmetric group S_n consisting of the linear transformations $x_i' = x_{\sigma(i)}$, σ being any permutation of $1, \ldots, n$. The invariants of S_n are the symmetric polynomials in $x_1, \ldots, x_n$. It is well known ([22], Vol. I, p. 79) that the elementary symmetric polynomials $I_j(x) = \sum x_{i_1} \ldots x_{i_j}$ $(1 \leqslant i_1 < \ldots < i_j \leqslant n)$, $1 \leqslant j \leqslant n$, form an integrity basis for all symmetric polynomials.

In the sequel, we shall use the term basis to mean integrity basis. The following result, due to Hilbert, is the main theorem of invariant theory.

THEOREM 1.1. *The invariants of G have a finite basis.*

We present two proofs of this theorem, due respectively to Hilbert [14] and Noether [17].

Hilbert's Proof: Let I denote the set of all homogeneous invariants of positive degree. Let $\mathscr{I}$ be the ideal generated by I. By Hilbert's Basis Theorem ([22], Vol. 2, p. 18), $\mathscr{I} = (I_1, \ldots, I_k)$ where $I_1, \ldots, I_k$ are homogeneous invariants of positive degree. Since every invariant polynomial is a sum of homogeneous invariants, it suffices to show that every P in I is a polynomial in $I_1, \ldots, I_k$. Now $P \in I \Rightarrow P \in \mathscr{I}$, so that $P(x) = \sum_{j=1}^{m} Q_j(x) I_j(x)$.

Since P and the I_j's are homogeneous, the Q_j's may be chosen homogeneous. We show that the Q_j's may be chosen invariant by the following group averaging processs. Since $P(x) = P(\sigma x)$ for all $\sigma \in G$, we have

$$P(x) = \frac{1}{|G|} \sum_{\sigma \in G} P(\sigma x) = \sum_{j=1}^{k} M_j(x) I_j(x), \tag{1.1}$$

where

$$M_j(x) = \frac{1}{|G|} \sum_{\sigma \varepsilon G} Q_j(\sigma x) . \tag{1.2}$$

For $\sigma_1 \in G$

$$M_j(\sigma_1 x) = \frac{1}{|G|} \sum_{\sigma \varepsilon G} Q_j(\sigma \sigma_1 x) = \frac{1}{|G|} \sum_{\sigma \varepsilon G} Q_j(\sigma x) = M_j(x) . \tag{1.3}$$

Thus $M_j(x)$ is a homogeneous invariant, $1 \leqslant j \leqslant k$. Since deg M_j + deg I_j = deg P and deg $I_j > 0$, we have deg $M_j <$ deg P, $1 \leqslant j \leqslant k$ The proof of Theorem 1.1 now follows by induction. It obviously holds for deg $P = 0$ and suppose that it holds for deg $P \leqslant m - 1$. Let deg $P = m$. M_j is a polynomial in $I_1, ..., I_k$ for $1 \leqslant j \leqslant k$. It follows from (1.1) that P is a polynomial in $I_1, ..., I_k$.

Noether's Proof: We prove first a preliminary lemma. For any n-tuple $a = (a_1, ..., a_n)$ of non-negative integers, let $|a| = a_1 + ... + a_n$.

LEMMA 1.1. Let

$$x_i = (x_{i1}, ..., x_{in}),\ x_i^a = x_{i1}^{a_1} ... x_{in}^{a_n},\ 1 \leqslant i \leqslant N,\ a = (a_1, ..., a_n)$$

being an arbitrary n-tuple of non-negative integers. $\sum_{i=1}^{N} x_i^a$ is a polynomial in the sums $\sum_{i=1}^{N} x_i^a$, $|a| \leqslant N$

Proof. For $n = 1$, the above states the well known fact that $\sum_{i=1}^{N} x_i^a$ is a polynomial in $\sum_{i=1}^{N} x_i, ..., \sum_{i=1}^{N} x_i^N$ ([22], Vol. 1, p. 81). Suppose that the result holds for $n - 1$, $n \geqslant 2$. The case $(a_1, ..., a_{n-1}, 0)$ is identical with $(a_1, ..., a_{n-1})$. Hence the result holds for $(a_1, ..., a_n)$, $a_n = 0$. Suppose it holds for $(a_1, ..., a_n)$, where $a_n < m$ ($n \geqslant 2$ and $m \geqslant 1$). We show that it holds for $a_n = m$ and so, by induction, for all $(a_1, ..., a_n)$. Increase a_{n-1} by 1, decrease a_n by 1, keeping the other a_i's fixed, and call the new n-tuple b. Let $s_1, ..., s_l$ be a denumeration of the sums $\sum_{i=1}^{N} x_i^a$, $|a| \leqslant N$. Then

$$\sum_{i=1}^{N} x_i^b = F(s_1, ..., s_l) \tag{1.4}$$

where $F = F(u_1, ..., u_l)$ is a polynomial in the u_i's. Differentiate both sides of (1.4) with respect to $x_{j,n-1}$ and multiply by x_{jn}. We obtain

$$(1.5) \qquad (a_{n-1}+1)\, x_j^a = \sum_{k=1}^{l} \frac{\partial F}{\partial u_k}(s_1, \ldots, s_l) \frac{\partial s_k}{\partial x_{j,n-1}} x_{jn}$$

If $s_k = \sum_{i=1}^{N} x_i^c$, $c = (c_1, \ldots, c_n)$, then

$$\frac{\partial s_k}{\partial x_{j,n-1}} x_{jn} = c_{n-1}\, x_j^d, \; d = (c_1, \ldots, c_{n-2}, c_{n-1}-1, c_n+1)\,.$$

It follows by summing both sides of (1.5) over j, $1 \leqslant j \leqslant N$, that $\sum_{i=1}^{N} x_i^a$ is a polynomial in $s_1, \ldots, s_l$.

We can now provide Noether's proof. Let $P(x)$ be a homogeneous invariant of degree m. Thus $P(x) = \sum_{|a|=m} c_a x^a$, the c_a's being elements of k. We have

$$(1.6) \qquad P(x) = \frac{1}{|G|} \sum P(\sigma x) = \sum_{|a|=m} \frac{c_a}{|G|} J_a(x)$$

where $J_a(x) = \sum_{\sigma \varepsilon G} (\sigma x)^a$

By Lemma 1.1, each J_a is a polynomial in the J_a's with $|a| \leqslant |G|$. It follows from (1.6) that the J_a's, $|a| \leqslant |G|$, form a basis for the invariants of G.

Comparing the two methods of proof, Noether's has the advantage of producing an explicit basis. It is however a proof of "finite type" which can not be generalized to continuous groups. Hilbert's proof goes through directly for continuous compact groups acting on the Euclidean space R^n, as we then have the notion of Haar measure and the group averaging process can be carried out.

We observe that the basis produced by Noether's method consists of $\binom{|G|+n}{n}$ elements of degree $\leqslant |G|$. The main interest in these bounds is their universality. In individual cases, they may prove to be very poor. Consider, for instance, the case $G = S_n$. Noether's method yields a basis of $\binom{n!+n}{n} \sim (n!)^{n-1}$ (as $n \to \infty$) homogeneous invariants of degrees $\leqslant n!$, while in actuality there are n basic homogeneous invariants of degree $\leqslant n$.

We obtain the following lower bound for the number of elements in a basis.

THEOREM 1.2. *Let* $I_1, \ldots, I_l$ *form a basis for the invariants of* G. *We may choose from the* I_j's n *elements which are algebraically independent over* k. *Thus* $l \geqslant n$.

Proof. Let $k(x_1, \ldots, x_n)$ be the field of rational functions in the indeterminates $x_1, \ldots, x_n$ with coefficients in k, a similar meaning being attached to $k(I_1, \ldots, I_l)$. We show that $k(x_1, \ldots, x_n)$ is a finite extension of $k(I_1, \ldots, I_l)$. Let $x_i(x) = x_i$ and set

$$(1.7) \qquad p_i(X) = \prod_{\sigma \in G} (X - x_i(\sigma x)) = X^{|G|-1} + a_1 X^{|G|-1} + a_1 X^{|G|-1} + \ldots + a_{|G|}$$

It is readily checked that the coefficients a_j are polynomials which are invariant under G. Thus each $a_j \in k(I_1, \ldots, I_l)$. Since $p_i(x_i) = 0$, we conclude that $x_i, \ldots, x_n$ are algebraic over $k(I_1, \ldots, I_l)$. Hence $k(x_1, \ldots, x_n)$ is a finite extension of $k(I_i, \ldots, I_l)$.

Let $K = k(\alpha_1, \ldots, \alpha_s)$ be the field obtained by adjoining $\alpha_1, \ldots, \alpha_s$ to k. We may define the transcendence degree of K over k to be the maximum number of α_i's which are algebraically independent over k ([22], Vol. 1, p. 201). We denote this degree by Tr.deg. K/k. If we have three fields $k \subset K \subset L$, then it is known that

(1.8) Tr.deg. L/k = Tr.deg. L/K + Tr.deg. K/k ([22], Vol. 1, p. 202).

Apply (1.8) with $L = k(x_1, \ldots, x_n)$, $K = k(I_1, \ldots, I_l)$. Then Tr.deg. $L/k = n$ and the finiteness of L over K means that Tr.deg. $L/K = 0$. Hence Tr.deg. $K/k = n$, which means that we may choose n I_j's which are algebraically independent over k.

2. MOLIEN'S FORMULA

For each integer $m \geqslant 0$, the homogeneous invariants of degree m form a finite dimensional vector space over k of dimension δ_m. We derive an interesting and useful formula for the δ_m's.

THEOREM 1.3. (Molien's Formula [16]). *Let* $\omega_1(\sigma), \ldots, \omega_n(\sigma)$ *be the eigenvalues of* σ. *Then*

$$(1.9) \qquad \sum_{m=0}^{\infty} \delta_m t^m = \frac{1}{|G|} \sum_{\sigma \in G} \frac{1}{(1-\omega_1(\sigma)t) \ldots (1-\omega_n(\sigma)t)}$$

REMARK. (1.9) is to be interpreted as an identity between two formal power series. I.e. if the right side is expanded as a formal power series, then its coefficients are identical with the δ_m's.

We require the following

LEMMA 1.2. Let W be the subspace fixed by G.

Then $\dim W = \frac{1}{|G|} \sum_{\sigma \in G} \mathrm{Tr}\,(\sigma)$.

Proof. Let $\{v_1, \ldots, v_r\}$ be a basis for W and augment this to a basis $\{v_1, \ldots, v_n\}$ for V. For $\sigma_1 \in G$ and $v \in V$, we have

$$\sigma_1 \Big(\sum_{\sigma \in G} \sigma v \Big) = \sum_{\sigma \in G} (\sigma_1 \sigma) v = \sum_{\sigma \in G} \sigma v ,$$

so that $\sum_{\sigma \in G} \sigma v \in W$. It follows that

$$\frac{1}{|G|} \sum_{\sigma \in G} \sigma v_i = v_i, \quad 1 \leqslant i \leqslant r ,$$

and

$$\frac{1}{|G|} \sum_{\sigma \in G} \sigma v_i = \sum_{j=1}^{r} a_{ij} v_j, \quad r+1 \leqslant i \leqslant n ,$$

the a_{ij}'s $\in k$. Hence

$$\frac{1}{|G|} \sum_{\sigma \in G} Tr\, \sigma = TR \left(\frac{1}{|G|} \sum_{\sigma \in G} \sigma \right) = r = \dim W .$$

Proof of Theorem 1.3. Let $\tilde{k}$ = algebraic closure of k. For any $\sigma \in G$, we can find a matrix τ with entries in $\tilde{k}$ so that $\tau\, \sigma\, \tau^{-1} = d$, d being diagonal and the diagonal entries being the eigenvalues of σ. Let R_m, $\tilde{R}_m$ denote respectively the space of homogeneous polynomials with coefficients from k, $\tilde{k}$. Let $(\mathrm{Tr}\,\sigma)_m$ = trace of σ as a transformation on R_m = trace of σ as a tranformation on $\tilde{R}_m$. Let $(\mathrm{Tr}\, d)_m$ = trace of d as a transformation on $\tilde{R}_m$. We have $d\,(P\,(x)) = P\,(d^{-1}x)$ for any polynomial $P(x)$. In particular, for any monomial x^a, we have $d\,(x^a) = \omega^a\,(\sigma^{-1})$, where $\omega\,(\sigma) = (\omega_1\,(\sigma), \ldots, \omega_n\,(\sigma))$. The monomials x^a form a basis for R_m and $\tilde{R}_m$. We conclude that

$$(Tr\,\sigma)_m = (Tr\, d)_m = \sum_{|a| = m} \omega^a\,(\sigma^{-1}) . \tag{1.10}$$

(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

$$\begin{aligned}\sum_{m=0}^{\infty}\delta_m t^m &= \frac{1}{|G|}\sum_{m=0}^{\infty}\sum_{\sigma\varepsilon G}\sum_{|a|=m}\omega^a(\sigma)\,t^m\\ &= \frac{1}{|G|}\sum_{\sigma\varepsilon G}\{\sum_{m=0}^{\infty}\omega_1^m(\sigma)\,t^m \ldots \sum_{m=0}^{\infty}\omega_n^m(\sigma)\,t^m\}\\ &= \frac{1}{|G|}\sum_{\sigma\varepsilon G}\frac{1}{(1-\omega_1(\sigma)\,t)\ldots(1-\omega_n(\sigma)\,t)}\end{aligned}$$

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.