

# 1. The Main Theorem of Invariant Theory

Objektyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **20.09.2024**

## **Nutzungsbedingungen**

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern. Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden. Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

## **Haftungsausschluss**

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

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  $\mathcal{R}$  satisfying the mean value property

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

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  $\mathcal{M}$ .  $\mathcal{M}$  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  $x_1, \dots, x_n$  be a coordinate system for  $V$ . Then  $P(v)$  becomes a polynomial which we designate by  $P(x)$ .  $\sigma$  is represented by a matrix which we

again designate by  $\sigma$ . 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  $1 \leq i \leq m$ . Hence the determination of the invariants of  $G$  reduces to the determination of its homogeneous invariants.

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

As a concrete illustration of the above definitions, let  $G$  be the symmetric group  $S_n$  consisting of the linear transformations  $x'_i = x_{\sigma(i)}$ ,  $\sigma$  being any permutation of  $1, \dots, n$ . The invariants of  $S_n$  are the symmetric polynomials in  $x_1, \dots, x_n$ . It is well known ([22], Vol. I, p. 79) that the elementary symmetric polynomials  $I_j(x) = \sum x_{i_1} \dots x_{i_j}$  ( $1 \leq i_1 < \dots < i_j \leq n$ ),  $1 \leq j \leq n$ , 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  $\mathcal{I}$  be the ideal generated by  $I$ . By Hilbert's Basis Theorem ([22], Vol. 2, p. 18),  $\mathcal{I} = (I_1, \dots, I_k)$  where  $I_1, \dots, I_k$  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  $I_1, \dots, I_k$ . Now  $P \in I \Rightarrow P \in \mathcal{I}$ , 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 process. Since  $P(x) = P(\sigma x)$  for all  $\sigma \in G$ , we have

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

where

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

For  $\sigma_1 \in G$

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

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

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

LEMMA 1.1. Let

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

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

*Proof.* For  $n = 1$ , the above states the well known fact that  $\sum_{i=1}^N x_i^a$  is a polynomial in  $\sum_{i=1}^N x_i, \dots, \sum_{i=1}^N x_i^N$  ([22], Vol. 1, p. 81). Suppose that the result holds for  $n - 1, n \geq 2$ . The case  $(a_1, \dots, a_{n-1}, 0)$  is identical with  $(a_1, \dots, a_{n-1})$ . Hence the result holds for  $(a_1, \dots, a_n), a_n = 0$ . Suppose it holds for  $(a_1, \dots, a_n)$ , where  $a_n < m$  ( $n \geq 2$  and  $m \geq 1$ ). We show that it holds for  $a_n = m$  and so, by induction, for all  $(a_1, \dots, a_n)$ . 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  $s_1, \dots, s_l$  be a denumeration of the sums  $\sum_{i=1}^N x_i^a, |a| \leq N$ .

Then

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

where  $F = F(u_1, \dots, u_l)$  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

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

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

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

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

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

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

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

By Lemma 1.1, each  $J_a$  is a polynomial in the  $J_a$ 's with  $|a| \leq |G|$ . It follows from (1.6) that the  $J_a$ 's,  $|a| \leq |G|$ , 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  $\leq |G|$ . 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  $n \rightarrow \infty$ ) homogeneous invariants of degrees  $\leq n!$ , while in actuality there are  $n$  basic homogeneous invariants of degree  $\leq n$ .

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

**THEOREM 1.2.** *Let  $I_1, \dots, I_l$  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  $l \geq n$ .*

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

$$(1.7) \quad p_i(X) = \prod_{\sigma \in G} (X - x_i(\sigma x)) = X^{|G|-1} + a_1 X^{|G|-2} + a_2 X^{|G|-3} + \dots + a_{|G|}$$

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

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

$$(1.8) \quad \text{Tr.deg. } L/k = \text{Tr.deg. } L/K + \text{Tr.deg. } K/k \text{ ([22], Vol. 1, p. 202).}$$

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

## 2. MOLLIEN'S FORMULA

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

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

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