

7. The finiteness theorem for the invariants of finite groups

Math. Ann. 77 (1916), pp. 89–92

In what follows, we give an entirely elementary finiteness proof for the invariants of finite groups — based only on the theory of symmetric functions — that also explicitly specifies a complete system; the usual proof, based on Hilbert’s theorem on module bases (Ann. 36), proves only existence.¹¹³

Let the finite group $\mathfrak{H}$ consist of the h linear transformations (of nonzero determinant) $A_1, \dots, A_h$, where A_k denotes the transformation

$$x_1^{(k)} = \sum_{\nu=1}^n a_{1\nu}^{(k)} x_\nu, \dots, x_n^{(k)} = \sum_{\nu=1}^n a_{n\nu}^{(k)} x_\nu,$$

or, briefly, $(x^{(k)}) = A_k(x)$. Thus $\mathfrak{H}$ carries the row (x) with entries $x_1, \dots, x_n$ into the rows $(x^{(k)})$ with entries $x_1^{(k)}, \dots, x_n^{(k)}$. Since $A_1, \dots, A_h$ must include the identity, the rows $(x^{(k)})$ also include (x) . A polynomial (absolute) invariant of the group means a polynomial in $x_1, \dots, x_n$ that remains identically unchanged under $A_1, \dots, A_h$; hence every such invariant $f(x)$ satisfies

$$f(x) = f(x^{(1)}) = \dots = f(x^{(h)}) = \frac{1}{h} \sum_{k=1}^h f(x^{(k)}). \quad (1)$$

1.

Formula (1) says that $f(x)$ is a symmetric polynomial in the rows $(x^{(1)}), \dots, (x^{(h)})$. Since each summand $f(x^{(k)})$ contains only the single row $(x^{(k)})$, this is the simplest case, usually called the *one-row* case. By the familiar theorem on symmetric functions of rows of quantities,¹¹⁴ $f(x)$ can therefore be expressed polynomially in the elementary symmetric functions of these rows, that is, in the coefficients $G_{\alpha\alpha_1\dots\alpha_n}(x)$ of the “Galois resolvent”

$$\begin{aligned} \Phi(z, u) &= \prod_{k=1}^h (z + u_1 x_1^{(k)} + \dots + u_n x_n^{(k)}) \\ &= z^h + \sum G_{\alpha\alpha_1\dots\alpha_n}(x) z^\alpha u_1^{\alpha_1} \dots u_n^{\alpha_n}, \end{aligned} \quad \left(\begin{array}{c} \alpha + \alpha_1 + \dots + \alpha_n = h \\ \alpha \neq h \end{array} \right),$$

where the $G_{\alpha\alpha_1\dots\alpha_n}(x)$ are invariants of degree $\alpha_1 + \dots + \alpha_n$ in the x ’s. We have thus proved:

The coefficients $G_{\alpha\alpha_1\dots\alpha_n}(x)$ of the Galois resolvent form a complete system of invariants of the group: every invariant is a polynomial expression in these finitely many invariants.

2.

Starting from (1), one may give the following still more elementary argument,¹¹⁵ which also leads to a second complete system. Put

$$f(x) = a + b x_1^{\mu_1} \dots x_n^{\mu_n} + \dots + c x_1^{\nu_1} \dots x_n^{\nu_n},$$

where $a, b, \dots, c$ denote constants. Then by (1) one has

$$\begin{aligned} h \cdot f(x) &= h \cdot a + b \sum_{k=1}^h (x_1^{(k)})^{\mu_1} \dots (x_n^{(k)})^{\mu_n} + \dots + c \sum_{k=1}^h (x_1^{(k)})^{\nu_1} \dots (x_n^{(k)})^{\nu_n} \\ &= h \cdot a + b \cdot J_{\mu_1\dots\mu_n} + \dots + c \cdot J_{\nu_1\dots\nu_n}. \end{aligned}$$

Every invariant is therefore a linear combination of the special invariants

$$J_{\mu_1\dots\mu_n} = \sum_{k=1}^h (x_1^{(k)})^{\mu_1} \dots (x_n^{(k)})^{\mu_n},$$

¹¹³See, for example, Weber, *Lehrbuch der Algebra* (2nd ed.), vol. 2, § 57.

¹¹⁴See the note to 2.

¹¹⁵This amounts to a proof of the theorem on symmetric functions of rows of quantities in the one-row case just mentioned.

and it therefore suffices to prove the assertion for these special invariants. Apart from a numerical factor, however, $J_{\mu_1 \dots \mu_n}$ is the coefficient of $u_1^{\mu_1} \dots u_n^{\mu_n}$ in the expression

$$S_\mu = \sum_{k=1}^h (u_1 x_1^{(k)} + \dots + u_n x_n^{(k)})^\mu,$$

where $\mu = \mu_1 + \dots + \mu_n$; this is the μ th power sum of the h linear forms

$$\xi_1 = u_1 x_1^{(1)} + \dots + u_n x_n^{(1)}, \dots, \xi_h = u_1 x_1^{(h)} + \dots + u_n x_n^{(h)}.$$

It is well known that the infinitely many power sums S_μ are polynomial expressions in

$$S_1, S_2, \dots, S_h,$$

whose coefficients are the invariants

$$J_{\mu_1 \dots \mu_n} \quad (\mu_1 + \dots + \mu_n \leq h).$$

Thus we obtain a second complete system:

A complete system of invariants of the group is given by all invariants $J_{\mu_1 \dots \mu_n}$ for which $\mu_1 + \dots + \mu_n \leq h$, where h is the order of the group.

The connection with 1 is obtained by observing that the power sums $S_1, \dots, S_h$ can be replaced by the elementary symmetric functions of $\xi_1, \dots, \xi_h$, which leads to the complete system of the $G_{\alpha\alpha_1 \dots \alpha_n}(x)$ given there. Both results show that every invariant is a polynomial expression in invariants whose degree in the x 's does not exceed the order h of the group.

3.

The result just proved has consequences for rational representation. Every rational absolute invariant can be represented — as follows immediately by multiplying its numerator and denominator by the conjugates of the denominator under the group — as the quotient of two polynomial absolute invariants, which need not be relatively prime. Hence every rational absolute invariant can be expressed rationally in the coefficients $G_{\alpha\alpha_1 \dots \alpha_n}(x)$ of the Galois resolvent $\Phi(z, u)$. This theorem can also be proved easily in several ways without using the finiteness theorem; it is already stated in Weber II, § 58.¹¹⁶

4.

Finally, the results derived here are implicitly contained in my paper “Fields and Systems of Rational Functions”.¹¹⁷ the complete system given in 1 appears in Theorems VI and VII, while Theorem III gives a proof of rational representation independent of the present finiteness theorem.¹¹⁸ In the present special case, however, both the argument and the result simplify considerably compared with the general theory. Conversations with E. Fischer led me to apply the general investigations to the invariants of finite groups; the substance of the proof in 2 — in the general case, the complete system occurring there cannot be defined rationally — and the note to 3 are also due to him.

Erlangen, May 1915.

¹¹⁶The proof given there, however, is not valid. It shows only that the function $\Psi(t)$ in formula (7) has invariants as coefficients, not that these invariants can be expressed rationally in the coefficients of $\Phi(t)$. This gap is avoided by using a familiar differentiation procedure, instead of Lagrange's interpolation formula, to express the $x_i^{(k)}$ in terms of ξ_k . Differentiating the identity $\Phi(-\xi_k, u) = 0$ with respect to all the u gives

$$\left[\frac{\partial \Phi}{\partial u_i} - x_i^{(k)} \frac{\partial \Phi}{\partial z} \right]_{z=-\xi_k} = 0.$$

Accordingly, for every rational function $\omega(x)$, the following formula must replace Weber's formulas (7) and (8):

$$\omega(x_1^{(k)}, \dots, x_n^{(k)}) = \omega \left(\frac{\partial \Phi / \partial u_1}{\partial \Phi / \partial z}, \dots, \frac{\partial \Phi / \partial u_n}{\partial \Phi / \partial z} \right) \Big|_{z=-\xi_k},$$

This contains only coefficients of $\Phi(z, u)$, and summing it over all k gives the desired representation when $\omega(x)$ is invariant.

¹¹⁷Math. Ann. 76, p. 161 (1915).

¹¹⁸For relative invariants, Theorems VIII and IX contain a finiteness proof that likewise rests on a different foundation from the usual proof, but again establishes only existence; this is because the relative invariants do not form a field.