ELECTRONIC RESEARCH ANNOUNCEMENTS
OF THE AMERICAN MATHEMATICAL SOCIETY
Volume 7, Pages 5–7 (March 16, 2001)
S 1079-6762(01)00088-9

ON NOETHER'S BOUND FOR POLYNOMIAL INVARIANTS OF A FINITE GROUP

JOHN FOGARTY

(Communicated by Efim Zelmanov)

ABSTRACT. E. Noether's a priori bound, viz., the group order g, for the degrees of generating polynomial invariants of a finite group, is extended from characteristic 0 to characteristic prime to g.

1. Introduction

The present paper contains an extension to characteristic p—prime to the order g of the finite group G—of Emmy Noether's *a priori* bound (viz., g) for the degrees of generators for rings of polynomial invariants of G (see [3], p. 275). Although Noether's original estimate was in characteristic zero, it turns out that her method, viz., embedding the quotient variety in a Chow variety, remains valid under the assumption that $g!$ is prime to the characteristic. The question as to whether the number $g!$ can be replaced with g apparently has remained open since the publication of [1] in 1916.

Dave Benson has apprised the author that the same result has been obtained in work of Fleischmann. Benson has also accomplished a compression of the original matrix proof in the ratio of 6:1!

In [1], Noether used the Chow coordinates of the orbits of G, regarded as 0-cycles of degree g, as generators of the ring of polynomial invariants. If the characteristic divides g, there are examples where the Chow coordinates do not generate the ring of invariants. We do not use Chow varieties to establish Noether's bound, and the important question as to whether the canonical map of the orbit space to the Chow variety parametrizing 0-cycles of degree g in affine space is an embedding remains open in the coprime case. If the characteristic divides the group order, this map is almost always *radiciel*.

Up to the present, almost all the results on invariants of finite linearly reductive groups can be made to follow from the complete reducibility of representations together with either general results on noetherian rings or explicit calculations in polynomial rings. The reasoning in the present proof is more elementary—in a sense, it is a variation on the theme $(1-1)^g = 0$ (see (2) below).

Received by the editors October 25, 1999.
2000 *Mathematics Subject Classification.* Primary 13A50.

2. Calculations

Let A be a commutative ring. Let G be a finite group of automorphisms of A, of order g. Let $\underline{m}$ be a G-stable ideal in A. Let J be the ideal in A generated by all G-invariants in $\underline{m}$. Then

$$g\underline{m}^g \subset J. \tag{1}$$

If g is invertible in A, then $\underline{m}^g \subset J$ and it is from this that the *a priori* bound follows. (1) follows from an explicit syzygy (in the 19th century sense—see (3) below). We apply (1) in the case where k is a field in which g is invertible, E is the space of a representation of G over k, $\underline{m}$ is the ideal of forms of positive degree in the polynomial ring $A = k[E]$ and J is the ideal of nullforms in $k[E]$, i.e., the ideal generated by invariants of positive degree. Then $\underline{m}^g \subset J$ implies that J is generated by forms $f_1, \ldots, f_r$ of degree $\leq g$, for J contains all forms of degree $\geq g$ and hence is generated by a basis of forms of degree g $\underline{\text{plus}}$ some forms of degree $< g$. Then there exist invariant forms $u_1, \ldots, u_n$ and forms h_{ij} such that

$$f_i = \sum_j h_{ij} u_i, \quad h_{ij} \in k[E],\ 1 \leq i \leq r.$$

We may assume that every u appears in at least one such equation with a nonzero coefficient. The u's evidently generate J, and since $\deg f_i = (\deg h_{ij})(\deg u_j)$, we see that $\deg u_j \leq g$. Since g is prime to the characteristic, an ideal basis $u_1, \ldots, u_r$ of J consisting of invariants will also be a set of generators for the algebra $k[E]^G$, for $J = \underline{m}^G k[E]$ so that every element of $\underline{m}^G$ is of the form

$$g_1 u_1 + \cdots + g_r u_r,$$

with g_j in $k[E]$. Averaging over G shows that we can replace each g_j with an invariant. Thus $\underline{m}^G$ has an ideal basis of invariants of degree $\leq g$. Since $k[E]^G$ is a graded algebra, such an ideal basis will generate $k[E]^G$ as algebra.

Before beginning, a word where the proof came from! If f is an element of A, we denote the norm polynomial

$$\prod_{\gamma \in G} (t - \gamma(f))$$

by $\Phi(t, f)$. The identity $\Phi(f, f) = 0$ shows that f^g is in J because the nonleading coefficients of Φ are the elementary symmetric functions of the G-conjugates of f. We seek then a "polarized" version of the identity which can be applied to the product of g elements instead of a gth power. (Straightforward polarization will not do, as it introduces coefficients which may be divisible by the characteristic.) For example, take $g = 3$ and let

$$X = \begin{pmatrix} X & Y & Z \\ U & V & W \\ R & S & T \end{pmatrix}$$

be a matrix of indeterminates with the alternating group $G = A_3$ acting by permuting the columns cyclically. Then by a stroke of good fortune,

$$\begin{aligned} 3XUR = {} & XU(R + S + T) + UR(X + Y + Z) + XR(U + V + W) \\ & - X(US + VT + WR) - U(RY + SZ + TX) - R(XV + YW + ZU) \\ & + XVT + YWR + ZUS. \end{aligned}$$

It was this example, with its solitary nonunit coefficient, which hinted at the possibility of reducing $g!$ to g.

Let $\{f_\gamma\}$ be g elements of $\underline{m}$ indexed by the elements γ of G, which may or may not be distinct. Then

$$\sum_{\sigma \in G} \prod_{\gamma \in G} (f_\gamma - \sigma^{-1}\gamma f_\gamma) = 0, \tag{2}$$

because at least one term in each product is 0. If S is a subset of G and we set

$$\Psi_S = \sum_{\sigma \in G} \left(\prod_{\gamma \notin S} f_\gamma \right) \left(\sigma^{-1} \prod_{\gamma \in S} (\gamma f_\gamma) \right),$$

then on expanding the products in (2) and collecting terms by subsets of G, we obtain the identity

$$\sum_{\text{all } S \subset G} (-1)^{|S|} \Psi_S = 0. \tag{3}$$

If S is nonempty, then Ψ_S lies in J. Also, as empty products in A are 1, we see that, for $S = \emptyset$,

$$\Psi_\emptyset = g \prod_{\gamma \in G} f_\gamma .$$

This shows that $g\underline{m}^g \subset J$, as required.

Our argument covers both the coprime case and the characteristic 0 case and establishes Noether's bound without recourse to Chow coordinates.

References

[1] E. Noether, *Der Endlichkeitsatz der Invarianten endlicher Gruppen*, Mathematische Annalen **77** (1916), 89.

[2] L. Smith, *Polynomial invariants of finite groups*, Bull. Amer. Math. Soc. (N.S.) **34** (1997), 211–250. MR **98i**:13009

[3] H. Weyl, *The classical groups*, Princeton, 1939. MR **1**:42c

Department of Mathematics and Statistics, University of Massachusetts, Amherst, MA 01003-4515

E-mail address: `jfoga9786@aol.com`