ADVANCES IN MATHEMATICS **124**, 49–76 (1996)
ARTICLE NO. 0077

Explicit Generators of the Invariants of Finite Groups

David R. Richman*

Department of Mathematics, University of South Carolina,
Columbia, South Carolina 29208

Received January 1, 1990

Let R denote a commutative (and associative) ring with 1 and let A denote a finitely generated commutative R-algebra. Let G denote a finite group of R-algebra automorphisms of A. In the case that R is a field of characteristic 0, Noether constructed a finite set of R-algebra generators of the invariants of G. This paper

INTRODUCTION

Let R, A, and G be as in the abstract. An element which is fixed by every automorphism in G is called an invariant of G, and A^G denotes the set of invariants of G in A. Let $\{a_1, ..., a_m\}$ be a finite set of R-algebra generators of A and let $Y_1, ..., Y_m$ denote commuting indeterminates. Define

$$F(Y_1, ..., Y_m) = \prod_{g \in G} (1 + g(a_1) Y_1 + g(a_2) Y_2 + \cdots + g(a_m) Y_m).$$

Noether [10] proved that

> if the non-zero integers are all invertible in R, then A^G is generated as an R-algebra by the coefficients of $F(Y_1, ..., Y_m)$. (0.1)

Noether's proof is an ingenious application of the theorem (due to Waring [18, p. 13]) that the symmetric polynomials are generated by the elementary symmetric polynomials. A different proof of (0.1) is described in [19, pp. 275–276], but it is not as short or as direct as Noether's original proof.

* Deceased. Please direct all correspondence to Professor Michael Filaseta, Department of Mathematics, University of South Carolina, Columbia, South Carolina 29208.

0001-8708/96 $18.00

This paper generalizes statement (0.1) by proving that

if $|G|!$ is invertible in R, then A^G is generated as an R-algebra by the coefficients of $F(Y_1, ..., Y_m)$. (0.2)

The proofs of statement (0.1) cannot be used to establish (0.2), because they involve dividing by multinomial coefficients which can have arbitrarily large prime factors.

Noether also proved in [7, pp. 9–10; 11] that

if R is Noetherian, then A^G is finitely generated as an R-algebra. (0.3)

As will be shown in this paper, one can deduce easily from (0.3) that

if $|G|$ is invertible in R, then A^G is finitely generated as an R-algebra. (0.4)

Now let $a_1, ..., a_k$ denote elements of A such that

$A = R[a_1, ..., a_k]$ and $g(a_i) \in Ra_1 + \cdots + Ra_k$ for every $g \in G$ and $i \in \{1, ..., k\}$. (0.5)

Such elements $a_1, ..., a_k$ always exist, because if S is any finite set of R-algebra generators of A, then we may take $\{a_1, ..., a_k\}$ to be the union of the sets $\sigma(S)$, as σ varies over the elements of G. Campbell *et al.* [2, 3] strengthened statement (0.4) by showing that

if $|G|$ is invertible in R, then A^G is generated by the elements $\sum_{g \in G} g(a_1^{e_1} \cdots a_k^{e_k})$, where $(e_1, ..., e_k)$ varies over all k-tuples of non-negative integers such that $e_1 + \cdots + e_k \leqslant \max\{|G|, k|G|(|G|-1)/2\}$. (0.6)

This paper proves that

if $|G|$ is invertible in R and G is a solvable group, then A^G is generated by the elements $\sum_{g \in G} g(a_1^{e_1} \cdots a_k^{e_k})$, where $(e_1, ..., e_k)$ varies over all k-tuples of non-negative integers such that $e_1 + \cdots + e_k \leqslant |G|$. (0.7)

Statements (0.2) and (0.7) are the main results of this paper. It would be interesting to determine whether the conclusion of statement (0.7) still holds when $|G|$ is invertible in R and G is not solvable.

Let $d(R, \{a_1, ..., a_k\}, G)$ denote the smallest non-negative number such that the R-module generated by $\{a_1^{e_1} \cdots a_k^{e_k} : e_1 + \cdots + e_k \leqslant d(R, \{a_1, ..., a_k\}, G)\}$ contains a set of R-algebra generators of A^G. Statement (0.3) implies that $d(R, \{a_1, ..., a_k\}, G)$ is finite when R is Noetherian and statement (0.7) implies that $d(R, \{a_1, ..., a_k\}, G) \leqslant |G|$ when $|G|$ is invertible in R and G is solvable. Let F_p denote the finite field of size p. I recently showed [12, Prop. 8] that, for every prime p and every integer b, there is a finitely generated F_p-algebra $A = F_p[a_1, ..., a_k]$ and a group G of automorphisms of A such that $|G| = p$ and $d(F_p, \{a_1, ..., a_k\}, G) > b$. Therefore one cannot remove the assumption in statement (0.7) that $|G|$ is invertible in R.

Smith and Stong [14, Theorem 3.2] proved the following result.

> Suppose that R is a field of characteristic $p > 0$. If $d(R, \{a_1, ..., a_k\}, G) < p$ and p does not divide $|G|$, then A^G is generated by the coefficients of the polynomials $\prod_{h \in \{g(L) : g \in G\}} X - h$, where L varies over the elements of $Ra_1 + \cdots + Ra_k$. (0.8)

Statements (0.2) and (0.8) imply that, if R is a field and $|G|$ is strictly less than the characteristic of R, then A^G is generated by the coefficients of the polynomials mentioned in statement (0.8). Other results about the invariants of G, in the case that R is a field of characteristic $p > 0$, can be found in [1, 2, 4, 8, 9, 13]. This list is not intended to be complete; more references can be found in the cited articles.

Huffman and Sloane [5] have shown that, if G is a primitive group and R is a field of characteristic 0, then the set of generators described in (0.1) is (in some sense) close to being optimal. Methods to efficiently compute generators of the invariants of G, in the case that R is a field of characteristic 0, are described in [6] and [15]. An algorithm for computing generators of the seminvariants of binary forms is described in [16].

Let m and N denote strictly positive integers and let S_N denote the group of permutations of $\{1, ..., N\}$. Let $\{X(i, j) : 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant m\}$ denote a set of commuting indeterminates. For every $\sigma \in S_N$ and $f \in R[X(i, j) : 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant m]$, let $\sigma(f)$ denote the image of f under the R-algebra homomorphism which maps $X(i, j)$ to $X(\sigma(i), j)$ for all i, j. The set of elements $f \in R[X(i, j) : 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant m]$ such that $\sigma(f) = f$ for every $\sigma \in S_N$ is denoted $R[X(i, j) : 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant m]^{S_N}$; such elements f are called vector invariants of S_N. The proof of statement (0.1) found in [19, pp. 275–276] and the proof of statement (0.6) found in [2] both rely on results about the vector invariants of S_N (where $N = |G|$). To prove statement (0.2), this paper also starts by studying the vector invariants of S_N.

This paper is organized as follows. Section 1 contains a proof of statement (0.2). Section 2 contains a proof of statement (0.7). Section 3 describes R-algebra generators of the vector invariants of S_N in the case that R is an arbitrary commutative ring with 1 (Campbell *et al.* [3] have described a different set of generators of these invariants). Section 3 also contains proofs of (0.4) and a result which is similar to (0.6). Sections 1–3 are independent of each other (except for a few place in Section 3, which use observations or notation from Section 1).

1. INVARIANTS OF FINITE GROUPS OVER RINGS IN WHICH $|G|!$ IS INVERTIBLE.

Recall that $\{X(i, j): 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant m\}$ denotes a set of commuting indeterminates.

PROPOSITION 1. *If* $U \subseteq \{1, ..., m\}$, *define* $x(U) = \sum_{h \text{ one–one}} \prod_{u \in U} X(h(u), u)$, *where the sum varies over all one-to-one functions* h *from* U *to* $\{1, ..., N\}$. *Assume that* $(m-1)!$ *is invertible in* R; *then* $\sum_{i=1}^{N} X(i, 1) X(i, 2) \cdots X(i, m)$ *lies in* $R[x(U): U \subseteq \{1, ..., m\}$ *and* $|U| \leqslant N]$.

Proof. Let $T \subseteq \{1, ..., m\}$ and $f: T \to \{1, ..., N\}$. If $B \subseteq \{1, ..., N\}$, let $|f^{-1}(B)|$ denote the number of elements t in T such that $f(t) \in B$. Two functions g, h from T to $\{1, ..., N\}$ are said to be T-equivalent if the sequence $|g^{-1}(\{1\})|, |g^{-1}(\{2\})|, ..., |g^{-1}(\{N\})|$ is a permutation of the sequence $|h^{-1}(\{1\})|, |h^{-1}(\{2\})|, ..., |h^{-1}(\{N\})|$. Let $E(f, T)$ denote the set of functions which are T-equivalent to f. Observe that, if $T = \{1, ..., m\}$ and f is a constant function, then $E(f, T)$ is the set of all constant functions from $\{1, ..., m\}$ to $\{1, ..., N\}$ and $\sum_{h \in E(f, T)} \prod_{t \in T} X(h(t), t)$ equals $\sum_{i=1}^{N} X(i, 1) X(i, 2) \cdots X(i, m)$. Therefore, to finish the proof, it suffices to establish the following claim.

CLAIM. $\sum_{h \in E(f, T)} \prod_{t \in T} X(h(t), t) \in R[x(U): U \subseteq \{1, ..., m\}$ *and* $|U| \leqslant N]$ *for every* $T \subseteq \{1, ..., m\}$ *and* $f: T \to \{1, ..., N\}$.

Proof. The claim will be established by induction on $|T| - |f(T)|$, where $|f(T)|$ denotes the size of the set $\{f(t): t \in T\}$. Suppose at first that $|T| - |f(T)| = 0$; then $E(f, T)$ is the set of all one-to-one functions from T to $\{1, ..., N\}$ and $\sum_{h \in E(f, T)} \prod_{t \in T} X(h(t), t) = x(T)$. Therefore the claim is true.

Suppose now that $|T| - |f(T)| > 0$. Let $b_1, ..., b_N$ denote the sequence which is obtained from $|f^{-1}(\{1\})|, ..., |f^{-1}(\{N\})|$ by subtracting 1 from every term that is strictly bigger than 0. For example, if the sequence

$|f^{-1}(\{1\})|, ..., |f^{-1}(\{N\})|$ is 3, 1, 0, 2, 2, then $b_1, ..., b_N$ equals 2, 0, 0, 1, 1. If $U \subseteq T$ and $|U| = |f(T)|$, let $E^*(f, U)$ denote the set of functions g from $T-U$ to $\{1, ..., N\}$ such that $|g^{-1}(\{1\})|, ..., |g^{-1}(\{N\})|$ is a permutation of $b_1, ..., b_N$. Suppose that $U_0 \subset T$ and note that

$$\text{if } |U_0| = |f(T)| \text{ and the restriction of } f \text{ to } U_0 \text{ is one-to-one, then the restriction of } f \text{ to } T-U_0 \text{ lies in } E^*(f, U_0). \tag{1.1}$$

Note also that

$$\text{if} \quad g \in E^*(f, U) \quad \text{then} \quad E^*(f, U) = E(g, T-U). \tag{1.2}$$

Define

$$H(f, T) = \sum_{\substack{U \subset T \\ |U| = |f(T)|}} \left(x(U) \sum_{h \in E^*(f, U)} \prod_{t \in T-U} X(h(t), t) \right). \tag{1.3}$$

Let U denote a subset of T such that $|U| = |f(T)|$. Note that, for every map $g\colon T-U \to \{1, ..., N\}$,

$$|T-U| - |g(T-U)| < |T-U| = |T| - |f(T)|,$$

because $T-U$ is non-empty (because $|U| = |f(T)| < |T|$), $|U| = |f(T)|$ and $U \subset T$. This observation and the induction hypothesis for the claim, together with statement (1.2), imply that $\sum_{h \in E^*(f, U)} \prod_{t \in T-U} X(h(t), t)$ is an element of $R[x(U)\colon U \subseteq \{1, ..., m\}$ and $|U| \leqslant N]$. Therefore

$$H(f, T) \in R[x(U)\colon U \subseteq \{1, ..., m\} \text{ and } |U| \leqslant N]. \tag{1.4}$$

One can write

$$H(f, T) = \sum_{\substack{h \\ h\colon T \to \{1, ..., N\}}} a_f(h) \prod_{t \in T} X(h(t), t), \tag{1.5}$$

where $a_f(h) \in R$ for every h. The next goal is to show that $a_f(h)$ is unchanged when h is replaced by a map which is T-equivalent to it. Define $x^*(f, U) = \sum_{h \in E^*(f, U)} \prod_{t \in T-U} X(h(t), t)$ for every subset U of T whose size is $|f(T)|$. Let σ denote a permutation of $\{1, ..., N\}$. Observe that the map $h \to \sigma \circ h$ permutes the one-to-one functions from U to $\{1, ..., N\}$, and it also permutes the elements of $E^*(f, U)$. Therefore both $x(U)$ and

$x^*(f, U)$ are unchanged when $X(i, j)$ is replaced with $X(\sigma(i), j)$ for all i, j. This observation and Eqs (1.3) and (1.5) imply that

$$a_f(h) = a_f(\sigma \circ h) \text{ for every map } h\colon T \to \{1, ..., N\} \text{ and every permutation } \sigma \text{ of } \{1, ..., N\}. \tag{1.6}$$

Let ψ denote a permutation of T and let ψ^* denote the R-algebra automorphism of $R[X(i, j)\colon 1 \leqslant i \leqslant N,\ j \in T]$ such that $\psi^*(X(i, j)) = X(i, \psi(j))$ for all i, j. The substitution $s = \psi(t)$ yields

$$\prod_{t \in T-U} X(h(t), \psi(t)) = \prod_{s \in T - \psi(U)} X(h(\psi^{-1}(s)), s). \tag{1.7}$$

Note that the map $h \to h \circ \psi^{-1}$ gives a one-to-one correspondence from $E^*(f, U)$ to $E^*(f, \psi(U))$. Therefore, by summing both sides of Eq. (1.7) over the elements h in $E^*(f, U)$, one obtains the equation $\psi^*(x^*(f, U)) = x^*(f, \psi(U))$. A similar argument implies that $\psi^*(x(U)) = x(\psi(U))$. Note that by (1.3)

$$\begin{aligned} \psi^*(H(f, T)) &= \sum_{\substack{U \subset T \\ |U| = |f(T)|}} \psi^*(x(U))\, \psi^*(x^*(f, U)) \\ &= \sum_{\substack{U \subset T \\ |U| = |f(T)|}} x(\psi(U))\, x^*(f, \psi(U)) \\ &= H(f, T) \end{aligned}$$

(replace U with $\psi^{-1}(U)$ in the preceding sum and use (1.3)). This equation and Eq. (1.5) imply that

$$a_f(h \circ \psi) = a_f(h) \text{ for every map } h\colon T \to \{1, ..., N\} \text{ and every permutation } \psi \text{ of } T. \tag{1.8}$$

Note that every function which is T-equivalent to h can be express in the form $\sigma \circ h \circ \psi$, where σ is a permutation of $\{1, ..., N\}$ and ψ is a permutation of T. This observation and statements (1.6) and (1.8) imply that

$$a_f(h) = a_f(h') \tag{1.9}$$

for every map h' which is T-equivalent to h.

Suppose now that h is a map from T to $\{1, ..., N\}$ such that $|h(T)| = |f(T)|$ and $a_f(h) \neq 0$. It will be shown that h is T-equivalent to f. Equations (1.3) and (1.5) and the hypothesis that $a_f(h) \neq 0$ imply that there is a subset U of T such that $|U| = |f(T)|$, the restriction of h to U is one-to-one, and the sequence $|h^{-1}(\{1\}) \cap (T-U)|, ..., |h^{-1}(\{N\}) \cap (T-U)|$ is a permutation of $b_1, ..., b_N$. Let τ denote a permutation of

$\{1, ..., N\}$ such that $|h^{-1}(\{j\}) \cap (T-U)| = b_{\tau(j)}$ for every j. Observe that, for every $j \in \{1, ..., N\}$, because the domain of h is T,

$$\begin{aligned} |h^{-1}(\{j\})| &= |h^{-1}(\{j\}) \cap (T-U)| + |h^{-1}(\{j\}) \cap U| \\ &= b_{\tau(j)} + |h^{-1}(\{j\}) \cap U|. \end{aligned} \tag{1.10}$$

Recall that $|h(T)| = |f(T)| = |U|$ and the restriction of h to U is one-to-one. Therefore $|h^{-1}(\{j\}) \cap U| = 1$ if $|h^{-1}(\{j\})| > 0$. This observation and Eq. (1.10) imply that the sequence $|h^{-1}(\{1\})|, ..., |h^{-1}(\{N\})|$ is obtained from $b_{\tau(1)}, ..., b_{\tau(N)}$ by adding 1 to $|h(T)|$ of the terms, in such a way that every non-zero term from $b_{\tau(1)}, ..., b_{\tau(N)}$ is increased. Note also that the sequence $|f^{-1}(\{1\})|, ..., |f^{-1}(\{N\})|$ is obtained from $b_1, ..., b_N$ in a similar manner and recall that $|f(T)| = |h(T)|$; therefore the sequence $|h^{-1}(\{1\})|, ..., |h^{-1}(\{N\})|$ is a permutation of $|f^{-1}(\{1\})|, ..., |f^{-1}(\{N\})|$. This proves that

$$\text{if } |h(T)| = |f(T)| \text{ and } a_f(h) \neq 0, \text{ then } h \text{ is } T\text{-equivalent to } f. \tag{1.11}$$

Equations (1.3) and (1.5) imply that, for every map $h: T \to \{1, ..., N\}$ such that $a_f(h) \neq 0$, there is a subset $U = U_h$ of T such that $|U| = |f(T)|$ and the restriction of h to U is one-to-one. Therefore, if $a_f(h) \neq 0$, then $|f(T)| = |h(U)| \leqslant |h(T)|$. This observation and statement (1.11) imply that

$$\text{if } a_f(h) \neq 0 \text{ and } h \text{ is not } T\text{-equivalent to } f, \text{ then } |h(T)| > |f(T)|. \tag{1.12}$$

Statements (1.5), (1.9), and (1.12) imply that

$$\begin{aligned} &H(f, T) = a_f(f) \sum_{h \in E(f, T)} \prod_{t \in T} X(h(t), t) + \text{a sum of expressions} \\ &\text{of the form } a_f(\phi) \sum_{h \in E(\phi, T)} \prod_{t \in T} X(h(t), t), \text{ where } \phi \text{ varies over} \\ &\text{a set of maps from } T \text{ to } \{1, ..., N\} \text{ such that } |\phi(T)| > |f(T)|. \end{aligned} \tag{1.13}$$

The induction hypothesis for the claim implies that, if ϕ is a map from T to $\{1, ..., N\}$ such that $|\phi(T)| > |f(T)|$, then $\sum_{h \in E(\phi, T)} \prod_{t \in T} X(h(t), t)$ lies in $R[x(U): U \subseteq \{1, ..., m\}$ and $|U| \leqslant N]$. This observation and statements (1.4) and (1.13) imply that

$$a_f(f) \sum_{h \in E(f, T)} \prod_{t \in T} X(h(t), t) \in R[x(U): U \subseteq \{1, ..., m\} \text{ and } |U| \leqslant N]. \tag{1.14}$$

Statements (1.1), (1.3), and (1.5) imply that

$$\begin{aligned} a_f(f) &= \text{the number of subsets } U \text{ of } T \text{ such that } |U| = |f(T)| \\ &\qquad \text{and the restriction of } f \text{ to } U \text{ is one-to-one} \\ &= \prod_{j \in f(T)} |f^{-1}(\{j\})| \end{aligned}$$

because, for every $j \in f(T)$, there are $|f^{-1}(\{j\})|$ possible choices for $U \cap f^{-1}(\{j\})$. Thus

$$a_f(f) = \prod_{j \in f(T)} |f^{-1}(\{j\})|. \tag{1.15}$$

If f is not a constant function or $|T| < m$, then $|f^{-1}(\{j\})| < m$ for every $j \in f(T)$ (because the domain of $f = T \subseteq \{1, ..., m\}$) and hence $|f^{-1}(\{j\})|$ is invertible in R for every $j \in f(T)$ (because of the hypothesis that $(m-1)!$ is invertible in R). This observation and statements (1.14) and (1.15) imply that

$$\begin{gathered} \text{if } f \text{ is not a constant function or } |T| < m, \text{ then} \\ \sum_{h \in E(f,\, T)} \prod_{t \in T} X(h(t), t) \in R[x(U) \colon U \subseteq \{1, ..., m\} \text{ and } |U| \leqslant N]. \end{gathered} \tag{1.16}$$

Note that

$$\begin{aligned} \prod_{j=1}^{m} x(\{j\}) &= \prod_{j=1}^{m} (X(1, j) + X(2, j) + \cdots + X(N, j)) \\ &= \sum_{h} X(h(1), 1)\, X(h(2), 2) \cdots X(h(m), m), \end{aligned}$$

where h varies over all maps from $\{1, ..., m\}$ to $\{1, ..., N\}$. Hence,

$$\prod_{j=1}^{m} x(\{j\}) = \sum_{i=1}^{N} X(i, 1)\, X(i, 2) \cdots X(i, m) + \text{a sum of expressions of the form } \sum_{h \in E(g,\, \{1, ..., m\})} \prod_{j=1}^{m} X(h(j), j),$$

where g varies over a set of non-constant maps from $\{1, ..., m\}$ to $\{1, ..., N\}$. This equation and statement (1.16) (with f replaced by g) imply that if $T = \{1, ..., m\}$, then

$$\sum_{i=1}^{N} X(i, 1)\, X(i, 2) \cdots X(i, m) \in R[x(U) \colon U \subseteq \{1, ..., m\} \text{ and } |U| \leqslant N]. \tag{1.17}$$

Note that if $|T|=m$ and f is a constant map from T to $\{1, ..., N\}$, then $E(f, T)$ is the set of constant maps from $\{1, ..., m\}$ to $\{1, ..., N\}$ and

$$\sum_{h \in E(f, T)} \prod_{t \in T} X(h(t), t) = \sum_{i=1}^{N} X(i, 1)\, X(i, 2) \cdots X(i, m)$$
$$\in R[x(U) \colon U \subseteq \{1, ..., m\} \text{ and } |U| \leqslant N],$$

by (1.17). This observation and statement (1.16) establish the claim. ▮

A monomial in $R[X(i, j) \colon 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant m]$ is defined to be an element of the multiplicative monoid generated by $\{X(i, j) : 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant m\}$.

PROPOSITION 2. *Let $Y_1, ..., Y_m$ denote commuting indeterminates and define $F^*(Y_1, ..., Y_m) = \prod_{i=1}^{N} (1 + X(i, 1) Y_1 + X(i, 2) Y_2 + \cdots + X(i, m) Y_m)$. Assume that $N!$ is invertible in R; then $R[X(i, j) \colon 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant m]^{S_N}$ is generated as an R-algebra by the coefficients of $F^*(Y_1, ..., Y_m)$.*

Proof. Suppose that w is a monomial in $R[X(i, j) : 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant m]$ and f is a vector invariant of S_N. Note that, for every $\sigma \in S_N$, the coefficient of w in f equals the coefficient of $\sigma(w)$ in f, because $\sigma(f) = f$. Therefore

every vector invariant f of S_N is an R-linear combination of the expressions $\sum_{v \in \{\sigma(w) : \sigma \in S_N\}} v$, where w varies over the monomials which appear in f. (2.1)

Let A_1 denote the R-algebra generated by the elements $\sum_{v \in \{\sigma(z) : \sigma \in S_N\}} v$, where z varies over the monomials in $R[X(1, j) : 1 \leqslant j \leqslant m]$.

CLAIM 1. *$\sum_{v \in \{\sigma(w) : \sigma \in S_N\}} v \in A_1$ for every monomial w in $R[X(i, j) : 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant m]$.*

Proof of the Claim. Let w denote a monomial in $R[X(i, j) : 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant m]$ and write $w = w_1 w_2 ... w_N$, where each w_i is a monomial in $R[X(i, j) : 1 \leqslant j \leqslant m]$. Let $\gamma(w) = \max\{\deg\ w_i : 1 \leqslant i \leqslant N\}$; the claim will be established by induction on $\deg w - \gamma(w)$. Suppose at first that $\deg w - \gamma(w) = 0$; then there is an element $\tau \in S_N$ such that $\tau(w) \in R[X(1, j) : 1 \leqslant j \leqslant m]$. Observe that

$$\sum_{v \in \{\sigma(w) : \sigma \in S_N\}} v = \sum_{v \in \{\sigma(\tau(w)) : \sigma \in S_N\}} v \in A_1,$$

because $\tau(w)$ is a monomial in $R[X(1, j) : 1 \leqslant j \leqslant m]$. Suppose now that $\deg w - \gamma(w) > 0$ and let u denote an element of $\{1, ..., N\}$ such that $\gamma(w) = \deg w_u$. Define $H_1 = \sum_{v \in \{\sigma(w_u) : \sigma \in S_N\}} v$ and $H_2 = \sum_{v^* \in \{\sigma(w/w_u) : \sigma \in S_N\}} v^*$. The induction hypothesis implies that

$$H_1 \text{ and } H_2 \text{ both lie in } A_1. \tag{2.2}$$

Define, for every $\tau \in G$, P_τ to be the set of pairs (v, v^*) such that $v \in \{\sigma(w_u) : \sigma \in S_N\}$, $v^* \in \{\sigma(w/w_u) : \sigma \in S_N\}$, and $vv^* = \tau(w)$. Let I denote the identity element of S_N and note that the map $(v, v^*) \to (\tau(v), \tau(v^*))$ gives a one-to-one correspondence between P_I and P_τ. Hence $|P_\tau| = |P_I|$ for every $\tau \in S_N$. Note also that $\gamma(vv^*) \geqslant \gamma(w)$ for all $v \in \{\sigma(w_u) : \sigma \in S_N\}$ and $v^* \in \{\sigma(w/w_u) : \sigma \in S_N\}$, with equality if and only if $vv^* \in \{\sigma(w) : \sigma \in S_N\}$. Therefore

$$H_1 H_2 = |P_I| \sum_{v \in \{\sigma(w) : \sigma \in S_N\}} v \ + \ \text{a sum of monomials } y$$
$$\text{such that } \deg y = \deg w \text{ and } \gamma(y) > \gamma(w). \tag{2.3}$$

The elements H_1, H_2 and $\sum_{v \in \{\sigma(w) : \sigma \in S_N\}} v$ are vector invariants of S_N. This observation and statements (2.1) and (2.3) imply that $H_1 H_2 - |P_I| \sum_{v \in \{\sigma(w) : \sigma \in S_N\}} v$ is a sum of expressions of the form $\sum_{v \in \{\sigma(y) : \sigma \in S_N\}} v$, where y varies over a set of monomials satisfying $\deg y = \deg w$ and $\gamma(y) > \gamma(w)$. This observation and the induction hypothesis imply that $H_1 H_2 - |P_I| \sum_{v \in \{\sigma(w) : \sigma \in S_N\}} v \in A_1$. This relation and statement (2.2) imply that $|P_I| \sum_{v \in \{\sigma(w) : \sigma \in S_N\}} v \in A_1$. Note also that $|P_I|$ is invertible in R, because $1 \leqslant |P_I| \leqslant |\{\sigma(w_u) : \sigma \in S_N\}| = N$ and $N!$ is invertible in R (by hypothesis). Therefore $\sum_{v \in \{\sigma(w) : \sigma \in S_N\}} v \in A_1$. This establishes the claim.

Claim 2. *If $j_1, j_2, ..., j_t \in \{1, ..., m\}$, then $\sum_{i=1}^{N} X(i, j_1) X(i, j_2) \cdots X(i, j_t)$ lies in the R-algebra generated by the coefficients of $F^*(Y_1, ..., Y_m)$.*

Proof of the Claim. The proof proceeds by induction on t. Suppose at first that $t \leqslant N+1$. Let h denote the R-algebra homomorphism from $R[X(i, j) : 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant t]$ to $R[X(i, j) : 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant m]$ such that $h(X(i, k)) = X(i, j_k)$ for every $i \in \{1, ..., N\}$ and $k \in \{1, ..., t\}$. Note that

$$\begin{aligned}\sum_{i=1}^{N} & X(i, j_1)\, X(i, j_2) \cdots X(i, j_t) \\ &= h\left(\sum_{i=1}^{N} X(i, 1)\, X(i, 2) \cdots X(i, t)\right) \\ &\in R[h(x(U)) : U \subseteq \{1, ..., t\} \text{ and } |U| \leqslant N],\end{aligned} \tag{2.4}$$

by Proposition 1. Note that the last line of statement (2.4) uses the assumption that $t \leqslant N+1$ and $N!$ is invertible in R. Let $Z_1, ..., Z_m$ denote the elements of the additive group generated by $\{Y_1, ..., Y_t\}$ such that, for every $i \in \{1, ..., N\}$,

$$\begin{aligned} X(i, j_1)\, Y_1 + X(i, j_2)\, Y_2 + \cdots + X(i, j_t)\, Y_t \\ = X(i, 1) Z_1 + X(i, 2) Z_2 + \cdots + X(i, m) Z_m. \end{aligned} \tag{2.5}$$

Let U denote a subset of $\{1, ..., t\}$ such that $|U| \leqslant N$ and observe that

$$\begin{aligned} h(x(U)) &= \text{the coefficient of } \prod_{u \in U} Y_u \text{ in} \\ &\quad \prod_{i=1}^{N} (1 + h(X(i, 1))\, Y_1 + h(X(i, 2))\, Y_2 + \cdots + h(X(i, t))\, Y_t) \\ &= \text{the coefficient of } \prod_{u \in U} Y_u \\ &\quad \text{in } \prod_{i=1}^{N} (1 + X(i, 1) Z_1 + \cdots + X(i, m) Z_m), \end{aligned}$$

by (2.5) and the definition of h. It follows that $h(X(U))$ is

$$\sum_{d_1, ..., d_m} \left(\text{the coefficient of } Y_1^{d_1} \cdots Y_m^{d_m} \text{ in } \prod_{i=1}^{N} (1 + X(i, 1) Y_1 + \cdots + X(i, m) Y_m) \right)$$
$$\times \left(\text{the coefficient of } \prod_{u \in U} Y_u \text{ in } Z_1^{d_1} \cdots Z_m^{d_m} \right),$$

where the sum ranges over all m-tuples $(d_1, ..., d_m)$ of non-negative integers (and if Z_i and d_i are 0, then $Z_i^{d_i}$ is defined to be 1). Thus,

$$h(x(U)) = \text{an } R\text{-linear combination of coefficients of } F^*(Y_1, ..., Y_m)$$

when $U \subseteq \{1, ..., t\}$ and $|U| \leqslant N$. This observation and statement (2.4) establish the claim.

Suppose now that $t > N+1$. Let h^* denote the R-algebra homomorphism from $R[X(i, j) : 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant N+1]$ to $R[X(i, j) : 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant m]$ such that

$$h^*(X(i, k)) = X(i, j_k) \qquad \text{for all} \quad i, k \in \{1, ..., N\}$$

and

$$h^*(X(i, N+1)) = X(i, j_{N+1}) X(i, j_{N+2}) \cdots X(i, j_t) \qquad \text{for all} \quad i \in \{1, ..., N\}.$$

Observe that by Proposition 1

$$\sum_{i=1}^{N} X(i, j_1)\, X(i, j_2) \cdots X(i, j_t)$$

$$= h^* \left(\sum_{i=1}^{N} X(i, 1)\, X(i, 2) \cdots X(i, N+1) \right)$$

$$\in R[h^*(x(U)) : U \subseteq \{1, ..., N+1\} \text{ and } |U| \leqslant N]. \tag{2.6}$$

Suppose that $U \subseteq \{1, ..., N+1\}$ and $|U| \leqslant N$. The definitions of h^* and $x(U)$ imply that degree $h^*(x(U)) < t$. Note also that $h^*(x(U))$ is a vector invariant of S_N, because $x(U)$ is a vector invariant of S_N and $h^*(\sigma(f)) = \sigma(h^*(f))$ for every $\sigma \in S_N$ and $f \in R[X(i, j) : 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant N+1]$. These observations and statement (2.1) imply that $h^*(x(U))$ is an R-linear combination of the expressions $\sum_{v \in \{\sigma(w) : \sigma \in S_N\}} v$, where w varies over a set of monomials whose degrees are strictly less then t. This observation and Claim 1, together with the induction hypothesis for Claim 2, imply that $h^*(x(U))$ lies in the R-algebra generated by the coefficients of $F^*(Y_1, ..., Y_m)$. This observation and statement (2.6) establish Claim 2.

Claims 1 and 2 imply that, for every monomial w in $R[X(i, j) : 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant m]$,

$$\sum_{v \in \{\sigma(w) : \sigma \in S_N\}} v \in A_1$$

$$\subseteq \text{the } R\text{-algebra generated by the coefficients of } F^*(Y_1, ..., Y_m).$$

This observation and statement (2.1) imply that every vector invariant of S_N lies in the R-algebra generated by the coefficients of $F^*(Y_1, ..., Y_m)$. Observe also that the coefficients of $F^*(Y_1, ..., Y_m)$ are all vector invariants of S_N; therefore $R[X(i, j) : 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant m]^{S_N}$ equals the R-algebra generated by the coefficients of $F^*(Y_1, ..., Y_m)$. ∎

Remark. Suppose that there is an integer $b > 0$ which is not invertible in R. The following argument proves that if $m > N$ and $b | N$, then $\sum_{i=1}^{N} X(i, 1) X(i, 2) \cdots X(i, m)$ does not lie in the R-algebra generated by the coefficients of $F^*(Y_1, ..., Y_m)$. Therefore the hypotheses on R which are stated in Propositions 1 and 2 cannot be removed.

Assume that $m > N$ and $b | N$. Let M denote the R-module generated by the homogeneous polynomials of degree m in $R[X(i, j) : 1 \leqslant i \leqslant N,$

$1 \leqslant j \leqslant m]$. Let h denote the R-module homomorphism from M to R such that

$$h(X(i_1, j_1) \cdots X(i_m, j_m)) = 0 \qquad \text{if} \quad j_1, ..., j_m \text{ are not distinct,}$$

$$h(X(i_1, 1) X(i_2, 2) \cdots X(i_m, m)) = 0 \qquad \text{if} \quad i_1 \neq 1$$

and

$$h(X(i_1, 1) X(i_2, 2) \cdots X(i_m, m)) = 1 \qquad \text{if} \quad i_1 = 1.$$

Let $c_1, ..., c_t$ denote coefficients of $F^*(Y_1, ..., Y_m)$ such that deg $c_1 c_2 \cdots c_t = m$; the elements $c_1, ..., c_t$ are not required to be distinct.

It will now be shown that $h(c_1 c_2 \cdots c_t)$ is divisible by b. Let $w_1, ..., w_t$ denote monomials in $R[Y_1, ..., Y_m]$ such that c_i is the coefficient of w_i in $F^*(Y_1, ..., Y_m)$ for every i. Note that deg $c_i =$ deg w_i for every i; therefore deg $w_1 \cdots w_t =$ deg $c_1 \cdots c_t = m$. Therefore, if $w_1 \cdots w_t \neq Y_1 Y_2 \cdots Y_m$, then $w_1 \cdots w_t$ is not square-free, so $c_1 \cdots c_t$ is a linear combination of monomials $X(i_1, j_1) \cdots X(i_m, j_m)$ such that $j_1, ..., j_m$ are not distinct. Hence, if $w_1 \cdots w_t \neq Y_1 \cdots Y_m$, then $h(c_1 \cdots c_t) = 0$. Suppose now that $w_1 \cdots w_t = Y_1 \cdots Y_m$. Then there is one and only one subscript $e \in \{1, ..., t\}$ such that w_e is divisible by Y_1. Note that deg $w_e \leqslant N$, because w_e is a monomial (in the indeterminates $Y_1, ..., Y_m$) which appears in $F^*(Y_1, ..., Y_m)$. This observation and the hypothesis that $m > N$ imply that deg $w_e < m =$ deg $w_1 \cdots w_t$. Therefore there is a subscript $r \neq e$ such that deg $w_r > 0$. Observe that

$$c_r \in R[X(i, j) : 1 \leqslant i \leqslant N, 2 \leqslant j \leqslant m], \tag{2.7}$$

because $r \neq e$ and e is the only subscript for which w_e is divisible by Y_1.

If $f \in R[X(i, j) : 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant m]$, let $s(f)$ denote the sum of the coefficients of f, i.e., $s(f)$ is the element of R which is obtained from f by replacing all the indeterminates $X(i, j)$ with ones. Statement (2.7) and the supposition that $w_1 \cdots w_t = Y_1 Y_2 \cdots Y_m$ imply that

$$s(c_r) \text{ divides } h(c_1 c_2 \cdots c_t). \tag{2.8}$$

There are distinct integers $j(1), j(2), ..., j(d)$ such that $w_r = Y_{j(1)} Y_{j(2)} \cdots Y_{j(d)}$, because $w_1 \cdots w_t = Y_1 Y_2 \cdots Y_m$. Note that

$$\begin{aligned} c_r &= \text{the coefficient of } Y_{j(1)} Y_{j(2)} \cdots Y_{j(d)} \text{ in } F^*(Y_1, ..., Y_m) \\ &= x(\{j(1), j(2), ..., j(d)\}), \end{aligned}$$

where $x(U)$ is defined as in Proposition 1. Note also that $s(x(\{j(1), ..., j(d)\})) = N(N-1) \cdots (N-d+1)$; therefore $s(c_r)$ is divisible by N. This observation and the hypothesis that $b|N$ imply that $s(c_r)$ is divisible by b. This observation and statement (2.8) imply that $h(c_1 c_2 \cdots c_t)$ is divisible by b. This proves that $h(f)$ is divisible by b for every $f \in M \cap$ (the R-algebra generated by the coefficients of $F^*(Y_1, ..., Y_m)$). On the other hand, $\sum_{i=1}^{N} X(i, 1) X(i, 2) \cdots X(i, m) \in M$ and $h(\sum_{i=1}^{N} X(i, 1) X(i, 2) \cdots X(i, m)) = 1$, which is not divisible by b (because b is not invertible in R). Therefore $\sum_{i=1}^{N} X(i, 1) X(i, 2) \cdots X(i, m)$ does not lie in the R-algebra generated by the coefficients of $F^*(Y_1, ..., Y_m)$.

Let $\{a_1, ..., a_m\}$ and $F(Y_1, ..., Y_m)$ be defined as in the Introduction.

Proposition 3. *If $|G|!$ is invertible in R, then A^G is generated as an R-algebra by the coefficients of $F(Y_1, ..., Y_m)$.*

Proof. Let $N = |G|$ and let $g_1, ..., g_N$ be a list of the elements of G. Let h denote the R-algebra homomorphism from $R[X(i, j) : 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant m]$ to A such that $h(X(i, j)) = g_i(a_j)$ for all i, j. Note that, for every $f \in A$, there is an element $f^* = f^*(X(1, 1), X(1, 2), ..., X(1, m)) \in R[X(1, j) : 1 \leqslant j \leqslant m]$ such that $h(f^*) = f$, because $\{a_1, ..., a_m\}$ generates A as an R-algebra. Observe that if $f \in A^G$ and N is invertible in R, then

$$\begin{aligned} f &= (1/N) \sum_{g \in G} g(f) \\ &= (1/N) h\left(\sum_{i=1}^{N} f^*(X(i, 1), X(i, 2), ..., X(i, m)) \right) \\ &\in h(R[X(i, j) : 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant m]^{S_N}). \end{aligned} \tag{3.1}$$

Let $F^*(Y_1, ..., Y_m)$ be defined as in Proposition 2 and observe that h maps the coefficients of $F^*(Y_1, ..., Y_m)$ to the coefficients of $F(Y_1, ..., Y_m)$. This observation and Proposition 2 imply that

> if $N!$ is invertible in R, then $h(R[X(i, j) : 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant m]^{S_N})$ is generated as an R-algebra by the coefficients of $F(Y_1, ..., Y_m)$. (3.2)

Suppose that $N!$ is invertible in R. Statement (3.2) and (3.1) imply that A^G is generated as an R-algebra by the coefficients of $F(Y_1, ..., Y_m)$. ▌

Remarks. The argument presented here, showing how Proposition 3 follows from Proposition 2, is similar to the one used in [19, pp. 275–276].

If it is assumed that $\sigma(a_j) \in Ra_1 + \cdots + Ra_m$ for every $\sigma \in G$ and $j \in \{1, ..., m\}$, then one can prove Proposition 3 directly from Proposition 1, without using Proposition 2.

2. INVARIANTS OF FINITE SOLVABLE GROUPS

In this section, $a_1, ..., a_k$ denote elements of A which satisfy condition (0.5).

PROPOSITION 4. *Assume that $|G|$ is a prime and is invertible in R. Then A^G is generated as an R-algebra by $\{\sum_{g \in G} g(a_1^{e_1} a_2^{e_2} \cdots a_k^{e_k}) : e_1 + \cdots + e_k \leqslant |G|\}$.*

Proof. Let $\sigma \in G - \{1\}$; observe that σ generates G as a group, because $|G|$ is a prime. Let $p = |G|$ and assume at first that there is an element θ in R such that $1 + \theta + \theta^2 + \cdots + \theta^{p-1} = 0$. The first goal is to show that A is generated as an R-algebra by a finite set of elements L in $Ra_1 + \cdots + Ra_k$ such that $\sigma(L) = (\text{a power of } \theta) L$. Define, for every integer j and every $a \in A$,

$$h_j(a) = (1/p)(a + \theta^{-j}\sigma(a) + \theta^{-2j}\sigma^2(a) + \cdots + \theta^{-(p-1)j}\sigma^{p-1}(a)).$$

Note that

$$\sigma(h_j(a)) = \theta^j h_j(a) \qquad \text{for every } j \text{ and } a, \tag{4.1}$$

because σ^p is the identity map and $\theta^p = 1$. If $t \in \{1, ..., p-1\}$, then the sequence $1, \theta^{-t}, \theta^{-2t}, ..., \theta^{-(p-1)t}$ is a permutation of $1, \theta, \theta^2, ..., \theta^{p-1}$ (because p is a prime and $\theta^p = 1$), so $1 + \theta^{-t} + \cdots + \theta^{-(p-1)t} = 1 + \theta + \cdots + \theta^{p-1} = 0$. Therefore

$$h_0(a) + h_1(a) + \cdots + h_{p-1}(a) = a \qquad \text{for every} \quad a \in A. \tag{4.2}$$

Define $V_j = \{h_j(a_1), h_j(a_2), ..., h_j(a_k)\}$ for every integer j. Equation (4.1) implies that

$$\sigma(L) = \theta^j L \qquad \text{for every} \quad L \in V_j. \tag{4.3}$$

Statement (4.2) implies that a_i is a sum of elements in $V_0 \cup V_1 \cup \cdots \cup V_{p-1}$ for every i; therefore

$$A \text{ is generated as an } R\text{-algebra by } V_0 \cup V_1 \cup \cdots \cup V_{p-1}. \tag{4.4}$$

Let M denote the multiplicative monoid generated by $V_0 \cup V_1 \cup \cdots \cup V_{p-1}$. Statement (4.3) implies that, for every element $z \in M$, there is a number $e(z) \in \{0, 1, ..., p-1\}$ such that $\sigma(z) = \theta^{e(z)} z$. Note also that, by statement (4.4), every element of A is an R-linear combination of elements of M. Therefore, for every $a \in A$, there exist elements $b_0 = b_0(a), ..., b_{p-1} = b_{p-1}(a)$ in A such that

$$a = b_0 + b_1 + \cdots + b_{p-1} \text{ and, for each } i,\ b_i \text{ is an } R\text{-linear combination of elements } z \text{ in } M \text{ satisfying } \sigma(z) = \theta^i z. \tag{4.5}$$

Note that $\sigma(b_i) = \theta^i b_i$ for every i. Therefore, if $i \in \{1, 2, ..., p-1\}$, then $(1 + \sigma + \cdots + \sigma^{p-1})(b_i) = (1 + \theta^i + \cdots + \theta^{(p-1)i}) b_i = 0$. This observation and statement (4.5) imply that $(1 + \sigma + \cdots + \sigma^{p-1})(a) = pb_0$. Therefore, if $\sigma(a) = a$, then $a = b_0$, so a is an R-linear combination of elements in $M \cap A^G$. Hence

$$\text{every element of } A^G \text{ is an } R\text{-linear combination of elements of } M \cap A^G \tag{4.6}$$

Let M^* denote the set of elements of $M \cap A^G$ which are products of p or fewer elements of $V_0 \cup V_1 \cup \cdots \cup V_{p-1}$ (these elements are not required to be distinct). Suppose that $z \in M \cap A^G - \{1\}$ and write $z = w_1 w_2 \cdots w_t$, where each w_i lies in $V_0 \cup V_1 \cup \cdots \cup V_{p-1}$. It will be shown by induction on t that z is a product of elements of M^*. If $t \leqslant p$ then $z \in M^*$. Suppose now that $t > p$. Statement (4.3) implies that for every $i \in \{1, ..., t\}$, there is an integer $e(i)$ such that $\sigma(w_1 w_2 \cdots w_i) = \theta^{e(i)} w_1 w_2 \cdots w_i$. If the elements $\theta^{e(1)}, \theta^{e(2)}, ..., \theta^{e(p)}$ are distinct, then $\theta^{e(1)}, \theta^{e(2)}, ..., \theta^{e(p)}$ must be a permutation of $1, \theta, ..., \theta^{p-1}$ (because $\theta^p = 1$), so there is a number $j \in \{1, ..., p\}$ such that $\theta^{e(j)} = 1$. In this case define $z^* = w_1 w_2 \cdots w_j$. If the elements $\theta^{e(1)}, \theta^{e(2)}, ..., \theta^{e(p)}$ are not distinct, then there are numbers $i, j \in \{1, ..., p\}$ such that $i < j$ and $\theta^{e(i)} = \theta^{e(j)}$; in this case define $z^* = w_{i+1} w_{i+2} \cdots w_j$. Observe that, in all cases, $z^* \in M^*$, and the induction hypothesis implies that z/z^* is a product of elements of M^*. Therefore z is a product of elements of M^*. This proves that every element of $M \cap A^G - \{1\}$ is a product of elements of M^*. This observation and statement (4.6) imply that M^* generates A^G as an R-algebra.

Let $S = \{a_1^{e_1} a_2^{e_2} \cdots a_k^{e_k} : e_1 + \cdots + e_k \leqslant p\}$. Note that M^* is contained in the R-module generated by S, because $V_0 \cup V_1 \cup \cdots \cup V_{p-1}$ is contained in $Ra_1 + \cdots + Ra_k$. If $z^* \in M^*$, then

$$\begin{aligned} z^* &= (1/p)(z^* + \sigma(z^*) + \cdots + \sigma^{p-1}(z^*)) \\ &\in \text{ the } R\text{-module generated by } \left\{ \sum_{g \in G} g(s) : s \in S \right\}, \end{aligned}$$

because $M^* \subseteq A^G$, $G = \{1, \sigma, ..., \sigma^{p-1}\}$ and M^* is contained in the R-module generated by S.

Thus M^* is contained in the R-module generated by $\{\sum_{g\in G} g(s) : s\in S\}$. This observation and the fact that M^* generates A^G as an R-algebra imply that the set $\{\sum_{g\in G} g(s) : s\in S\}$ generates A^G as an R-algebra.

In the case that R does not contain a solution to $1+\theta+\cdots+\theta^{p-1}=0$, one can reduce to the case considered earlier by the "extension of constants" [7, pp. 7–9] and thereby establish the proposition. To keep the exposition self-contained, the details of this argument are presented here. Let T denote an indeterminate and let θ denote the natural image of T in $A[T]/(1+T+T^2+\cdots+T^{p-1})$. Observe that σ extends to an R-algebra automorphism of $A[T]$ which fixes T; this extended automorphism maps the ideal $(1+T+\cdots+T^{p-1})$ into itself. Therefore σ extends to an $R[\theta]$-algebra automorphism σ^* of $A[\theta]$. Let $A[\theta]^G$ denote the set of elements in $A[\theta]$ which are fixed by σ^*. Note that $A[\theta]$ is generated as an $R[\theta]$-algebra by the set $\{a_1, ..., a_k\}$ and $(\sigma^*)^p$ is the identity map on $A[\theta]$. Therefore the first part of the proof implies that

$$A[\theta]^G \text{ is generated as an } R[\theta]\text{-algebra by } \left\{\sum_{g\in G} g(s) : s\in S\right\}. \tag{4.7}$$

Let β denote the A-module homomorphism from $A[\theta]$ to A such that $\beta(a_0+a_1\theta+\cdots+a_{p-2}\theta^{p-2})=a_0$ for all $a_0, a_1, ..., a_{p-2}\in A$. If $f\in A^G$, then

$$f=\beta(f),$$

because β fixes every element of A. By (4.7),

$$\begin{aligned} f &\in \beta\left(\text{the } R[\theta]\text{-algebra generated by } \left\{\sum_{g\in G} g(s) : s\in S\right\}\right) \\ &= \text{the } R\text{-algebra generated by } \left\{\sum_{g\in G} g(s) : s\in S\right\}. \end{aligned}$$

This proves that A^G is contained in the R-algebra generated by $\{\sum_{g\in G} g(s) : s\in S\}$. This observation and the fact that $\sum_{g\in G} g(a)\in A^G$ for every $a\in A$ imply that the set $\{\sum_{g\in G} g(s) : s\in S\}$ generates A^G as an R-algebra. ▌

Remark. The expressions $h_j(a)$ used in the preceding proof are special types of Lagrange resolvents. Lagrange resolvents were introduced independently by Vandermonde and Lagrange in the 1770's as tools to express the roots of certain polynomials in terms of radicals [17, pp. 77–81].

PROPOSITION 5. *Assume that G is solvable and $|G|$ is invertible in R; then A^G is generated as an R-algebra by the set $\{\sum_{g\in G} g(a_1^{e_1}a_2^{e_2}\cdots a_k^{e_k}) : e_1+\cdots+e_k\leqslant|G|\}$.*

Proof. Proceed by induction on $|G|$. If $|G|=1$, then $A^G=A=R[a_1, ..., a_k]$ (by (0.5)), so the proposition is true. Suppose now that $|G|>1$. Since G is solvable, there is a normal subgroup H of G such that the index of H in G is a prime p. Let $f_1, ..., f_t$ be a list of the elements of $\{\sum_{h\in H} h(a_1^{e_1}a_2^{e_2}\cdots a_k^{e_k}) : e_1+\cdots+e_k\leqslant |H|\}$. The induction hypothesis implies that

$$A^H \text{ is generated as an } R\text{-algebra by } \{f_1, ..., f_t\}. \tag{5.1}$$

If $\tau\in G$ and $x\in A$, then

$$\begin{aligned}\tau\left(\sum_{h\in H} h(x)\right) &= \sum_{h\in H} \tau h\tau^{-1}(\tau(x))\\ &= \sum_{h\in H} h(\tau(x)),\end{aligned}$$

because the map $h\to\tau h\tau^{-1}$ permutes the elements of H (because H is a normal subgroup of G).

This equation and condition (0.5) imply that

$$\tau(f_i)\in Rf_1+Rf_2+\cdots+Rf_t \text{ for every } \tau\in G \text{ and } i\in\{1, ..., t\}. \tag{5.2}$$

Statements (5.1) and (5.2) imply that every element of G maps A^H into itself. Let $r(G/H)$ denote the group of automorphisms of A^H obtained by restricting the elements of G to A^H. Note that $r(G/H)$ is a homomorphic image of G/H; therefore $|r(G/H)|$ divides $|G/H|$. Thus $|r(G/H)|$ divides p, so $|r(G/H)|=p$ or 1 (because p is prime).

Suppose at first that $|r(G/H)|=p$. Note that p is invertible in R, because p divides $|G|$ and $|G|$ is invertible in R. Therefore statements (5.1) and (5.2) and Proposition 4 (with A, G, and $\{a_1, ..., a_k\}$ replaced by A^H, $r(G/H)$, and $\{f_1, ..., f_t\}$, respectively) imply that

$$(A^H)^{r(G/H)} \text{ is generated as an } R\text{-algebra by}$$
$$\left\{\sum_{\sigma\in r(G/H)} \sigma(f_1^{d_1}\cdots f_t^{d_t}) : d_1+\cdots+d_t\leqslant p\right\}. \tag{5.3}$$

If $|r(G/H)|=1$, then statement (5.3) follows from statement (5.1); thus statement (5.3) holds in all cases.

Define $S=\{a_1^{e_1}a_2^{e_2}\cdots a_k^{e_k} : e_1+\cdots+e_k\leqslant |G|\}$ and let M denote the R-module generated by S. Condition (0.5) and the definition of the elements $f_1, ..., f_t$ (together with the fact that $|H|p=|G|$) imply that $\sum_{\sigma\in r(G/H)}\sigma(f_1^{d_1}\cdots f_t^{d_t})\in M$ when $d_1+\cdots+d_t\leqslant p$. Note also that $(A^H)^{r(G/H)}$ equals A^G, by the definition of $r(G/H)$. These observations and statement (5.3) imply that

$$A^G \text{ is generated as an } R\text{-algebra by elements in } M\cap A^G. \tag{5.4}$$

Note that $M \cap A^G$ is contained in the R-module generated by the set $\{\sum_{g \in G} g(s) : s \in S\}$, because $f = (1/|G|) \sum_{g \in G} g(f)$ for every $f \in A^G$ and M is the R-module generated by S. This observation and statement (5.4) imply that A^G is generated as an R-algebra by $\{\sum_{g \in G} g(s) : s \in S\}$. ▮

Remark. Using Proposition 3 and an argument similar to the one used to prove Proposition 5, one can establish the following result (here G is not necessarily solvable).

> Let u denote the maximum of the sizes of the composition factors of G. If $u!$ is invertible in R, then A^G is generated as an R-algebra by the set mentioned in Proposition 5. (5.5)

3. VECTOR INVARIANTS OF S_N OVER ARBITRARY RINGS

Notation. If $a \in A$, let $d(a)$ denote the number of elements in the set $\{g(a) : g \in G\}$ and let $E_1(a)$, $E_2(a)$, ..., $E_{d(a)}(a)$ denote the elements of A such that

$$\prod_{h \in \{g(a) : g \in G\}} (Y + h) = Y^{d(a)} + E_1(a) Y^{d(a)-1} + E_2(a) Y^{d(a)-2} + \cdots + E_{d(a)}(a); \tag{6.0}$$

here Y denotes an indeterminate. Thus $E_i(a)$ is the ith elementary symmetric function in the elements of $\{g(a) : g \in G\}$.

Recall that $\{a_1, ..., a_m\}$ denotes a finite set of R-algebra generators of A.

PROPOSITION 6. *Assume that $a_1, ..., a_m$ are algebraically independent over R and $\sigma(a_j) \in \{a_1, ..., a_m\}$ for every $\sigma \in G$ and $j \in \{1, ..., m\}$. Let M denote the R-module generated by $\{a_1^{e_1} \cdots a_m^{e_m} : 0 \leqslant e_j < d(a_j)$ for every $j\}$; then A^G equals the $R[E_i(a_j) : 1 \leqslant j \leqslant m, 1 \leqslant i \leqslant d(a_j)]$- module generated by $M \cap A^G$.*

Proof. Define $d(j) = d(a_j)$ for every $j \in \{1, ..., m\}$. If a is replaced by a_j and Y is replaced by $-a_j$ in Eq. (6.0), then one obtains

$$a_j^{d(j)} = E_1(a_j) a_j^{d(j)-1} - E_2(a_j) a_j^{d(j)-2} + \cdots + (-1)^{d(j)-1} E_{d(j)}(a_j).$$

Therefore

$$a_j^e = E_1(a_j) a_j^{e-1} - E_2(a_j) a_j^{e-2} + \cdots + (-1)^{d(j)-1} E_{d(j)}(a_j) a_j^{e-d(j)} \tag{6.1}$$

for every $j \in \{1, ..., m\}$ and every integer $e \geqslant d(j)$. By repeatedly applying Eq. (6.1), one can express every element of A as an element of the $R[E_i(a_j) : 1 \leqslant j \leqslant m, 1 \leqslant i \leqslant d(j)]$-module generated by $\{a_1^{e_1} \cdots a_m^{e_m} : 1 \leqslant e_j < d(j)$ for every $j\}$. Therefore every $h \in A$ can be expressed as

$$h = \sum_w \mu_w(h) w, \tag{6.2}$$

where the sum varies over the elements w in the multiplicative monoid generated by $\{E_i(a_j) : 1 \leqslant j \leqslant m, 1 \leqslant i \leqslant d(j)\}$ and $\mu_w(h) \in M$ for every w.

If $h \in A^G$, then $\sum_w \mu_w(h) w = \sum_w \sigma(\mu_w(h)) w$ for every $\sigma \in G$, so one might guess (by "equating coefficients") that $\mu_w(h) \in A^G$ for every w. If this guess were indeed true, then every element of A^G would lie in the $R[E_i(a_j) : 1 \leqslant j \leqslant m, 1 \leqslant i \leqslant d(j)]$-module generated by $A^G \cap M$ (by (6.2)) and the proposition would be established. A problem with this approach is that there is often more than one way to write an element of A^G as in Eq. (6.2); for example, if $d(j) > 1$ and $1 \leqslant i \leqslant d(j)$, then $E_i(a_j) \in M$. Thus the elements $\mu_w(h)$ are not well defined by Eq. (6.2). The rest of the proof describes how to overcome this problem by a more precise definition of the elements $\mu_w(h)$.

If $j \in \{1, ..., m\}$, let $Ga_j = \{\sigma(a_j) : \sigma \in G\}$. Let $\{Y(i, Ga_j) : 1 \leqslant j \leqslant m, 1 \leqslant i \leqslant d(j)\}$ denote a set of commuting indeterminates (where $Y(i, Ga_j) = Y(i, Ga_t)$ if $Ga_j = Ga_t$) and let $\mathrm{Mon}(Y)$ denote the multiplicative monoid generated by this set. Let $A^* = A[Y(i, Ga_j) : 1 \leqslant j \leqslant m, 1 \leqslant i \leqslant d(j)]$. Let θ denote the R-module homomorphism from A^* to A^* such that

$$\begin{aligned} \theta(a_j^e) &= a_j^e \qquad \text{if } 0 \leqslant e < d(j) \text{ and } j \in \{1, ..., m\}, \\ \theta(a_j^e) &= a_j^{e-1} Y(1, Ga_j) - a_j^{e-2} Y(2, Ga_j) + \cdots \\ &\qquad + (-1)^{d(j)-1} a_j^{e-d(j)} Y(d(j), Ga_j) \end{aligned}$$

if $e \geqslant d(j)$ and $j \in \{1, ..., m\}$, and

$$\theta\left(y \prod_{j=1}^m a_j^{e_j}\right) = y \prod_{j=1}^m \theta(a_j^{e_j})$$

for all $y \in \mathrm{Mon}(Y)$ and all non-negative integers $e_1, ..., e_m$.

Note that such a homomorphism θ exists because $a_1, ..., a_m$ are algebraically independent over R and hence over $R[Y(i, Ga_j) : 1 \leqslant j \leqslant m, 1 \leqslant i \leqslant d(j)]$.

Let M^* denote the $R[Y(i, Ga_j) : 1 \leqslant j \leqslant m, 1 \leqslant i \leqslant d(j)]$-module generated by M and suppose that $h \in A^*$. The definition of θ implies that the set $\{h, \theta(h), \theta(\theta(h)), \ldots\}$ contains an element of M^*. Note also that every element of M^* is fixed by θ. Therefore the set $\{h, \theta(h), \theta(\theta(h)), \ldots\}$ contains exactly one element of M^*; let $\theta^*(h)$ denote this element. Write

$$\theta^*(h) = \sum_{y \in \mathrm{Mon}(Y)} \mu_y(h) y, \text{ where } \mu_y(h) \in M \text{ for every } y \in \mathrm{Mon}(Y). \tag{6.3}$$

Suppose that $\sigma \in G$. Extend σ to an R-algebra automorphism of A^* by defining $\sigma(Y(i, Ga_j)) = Y(i, Ga_j)$ for every i and j. The definition of θ and the assumption that $\sigma(a_j) \in \{a_1, ..., a_m\}$ for every j imply that $\sigma \circ \theta = \theta \circ \sigma$. Therefore $\sigma \circ \theta^* = \theta^* \circ \sigma$. This observation and Eq. (6.3) imply that

$$\sigma(\mu_y(h)) = \mu_y(\sigma(h)) \qquad \text{for every } \sigma \in G,\ y \in \mathrm{Mon}(Y) \text{ and } h \in A^*. \tag{6.4}$$

Let ψ denote the A-algebra homomorphism from A^* to A such that $\psi(Y(i, Ga_j)) = E_i(a_j)$ for all i, j; note that ψ is well defined because $E_i(a_j) = E_i(a_t)$ when $Ga_j = Ga_t$. Equation (6.1) and the definition of θ imply that $\psi(\theta(h)) = \psi(h)$ for every $h \in A^*$. Therefore $\psi \circ \theta^* = \psi$. If $h \in A$, then we use that ψ fixes every element of A, $\psi \circ \theta^* = \psi$, and (6.3) to obtain

$$h = \psi(h) = \psi(\theta^*(h)) = \sum_{y \in \mathrm{Mon}(Y)} \mu_y(h) \psi(y).$$

Therefore,

$$\text{if } h \in A, \text{ then } h \text{ lies in the } R[E_i(a_j) : 1 \leqslant j \leqslant m, 1 \leqslant i \leqslant d(j)]\text{-module generated by } \{\mu_y(h) : y \in \mathrm{Mon}(Y)\}. \tag{6.5}$$

Statement (6.4) and the definition of μ_y imply that, if $h \in A^G$, then $\mu_y(h) \in A^G \cap M$ for every $y \in$ Mon(Y). This observation and statement (6.5) imply that A^G is contained in the $R[E_i(a_j) : 1 \leqslant j \leqslant m, 1 \leqslant i \leqslant d(j)]$-module generated by $A^G \cap M$. Note also that $E_i(a_j) \in A^G$ for every i and j; therefore A^G equals the $R[E_i(a_j) : 1 \leqslant j \leqslant m, 1 \leqslant i \leqslant d(j)]$-module generated by $A^G \cap M$. ▮

Suppose that $y \in$ Mon(Y) and z lies in the multiplicative monoid generated by $\{a_1, ..., a_m\}$. The definition of μ_y implies that $\mu_y(z)$ is an R-linear combination of the divisors of z. Therefore μ_y $(\sum_{v \in \{g(z) : g \in G\}} v)$ is an R-linear combination of the divisors of the elements in $\{g(z) : g \in G\}$. Note also that $\mu_y(h) \in A^G \cap M$ for every $h \in A^G$, by statement (6.4) and the definition of μ_y. These observations and statement (6.5) (with $h = \sum_{v \in \{g(z) : g \in G\}} v$) imply that

$$\sum_{v \in \{g(z) : g \in G\}} v \text{ lies in the } R[E_i(a_j) : 1 \leqslant j \leqslant m, 1 \leqslant i \leqslant d(j)]\text{-}$$ module generated by $A^G \cap M \cap$ (the R-module generated by the divisors of the elements in $\{g(z) : g \in G\}$), assuming that $\{a_1, ..., a_m\}$ and G satisfy the conditions of Proposition 6. (6.6)

Notation. If $f \in R[X(i, j) : 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant m]$ and $i \in \{1, ..., N\}$, let $E_i(f)$ denote the ith elementary symmetric function in the elements of $\{\sigma(f) : \sigma \in S_N\}$.

PROPOSITION 7. *The set* $\{X(1, j)\, X(2, j) \cdots X(N, j), E_i(w) : 1 \leqslant i \leqslant N-1, 1 \leqslant j \leqslant m,$ *w divides* $\prod_{j=1}^{m} X(1, j)^{N-1}\}$ *generates* $R[X(i, j) : 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant m]^{S_N}$ *as an R-algebra.*

Proof. Suppose that z is a monomial in $R[X(i, j) : 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant m]$. Let $F_1(z), F_2(z), ..., F_N(z)$ denote the monomials such that

$$F_e(z) \in R[X(e, j) : 1 \leqslant j \leqslant m] \qquad \text{for every } e \in \{1, ..., N\}$$
$$\text{and } z = F_1(z) F_2(z) \cdots F_N(z). \tag{7.1}$$

Define $\gamma(z) = \max\{\deg\ F_e(z) : 1 \leqslant e \leqslant N\}$. Let B denote the R-algebra generated by the set mentioned in the proposition, and let w denote a monomial in $R[X(i, j) : 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant m]$. It will be shown, by induction on $\deg w - \gamma(w)$, that $\sum_{v \in \{\sigma(w) : \sigma \in S_N\}} v \in B$. Let u denote an element of $\{1, ..., N\}$ such that $\deg F_u(w) = \gamma(w)$ and let U denote the set of subscripts i such that $F_i(w) \in \{\sigma(F_u(w)) : \sigma \in S_N\}$. Note that $u \in U$. Define $w' = \prod_{i \in U} F_i\,(w)$.

CLAIM 1. $\sum_{v \in \{\sigma(w') : \sigma \in S_N\}} v \in B$.

Proof of the Claim. Suppose at first that $F_u(w)$ divides $\prod_{j=1}^{m} X(u, j)^{N-1}$. Let τ denote an element of S_N such that $\tau(u) = 1$ and note that $\tau(F_u(w))$ divides $\prod_{j=1}^{m} X(1, j)^{N-1}$. Let $|U|$ denote the size of U and observe that

$$\begin{aligned}\sum_{v \in \{\sigma(w') : \sigma \in S_N\}} v &= E_{|U|}(F_u(w)) \\ &= E_{|U|}(\tau(F_u(w))),\end{aligned} \tag{7.2}$$

by the definitions of w' and U. If $|U| < N$, then $E_{|U|}(\tau(F_u(w))) \in B$, because $\tau(F_u(w))$ divides $\prod_{j=1}^{m} X(1, j)^{N-1}$. If $|U| = N$, then $E_{|U|}(\tau(F_u(w)))$ is a product of elements in $\{X(1, j)\, X(2, j) \cdots X(N, j) : 1 \leqslant j \leqslant m\}$, so it lies in B. Thus $E_{|U|}(\tau(F_u(w)))$ lies in B in all cases. This observation and Eq. (7.2) establish the claim.

Suppose now that $F_u(w)$ does not divide $\prod_{j=1}^{m} X(u, j)^{N-1}$. Let M denote the R-module generated by the divisors of $\prod_{i=1}^{N} \prod_{j=1}^{m} X(i, j)^{N-1}$. Statement (6.6) (with $z = w'$, $G = S_N$, and $\{a_1, ..., a_m\} = \{X(i, j) : 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant m\}$) implies that

$$\sum_{v \in \{\sigma(w') : \sigma \in S_N\}} v \text{ lies in the } B\text{-module generated by (the invariants of } S_N) \cap M \cap (\text{the } R\text{-module generated by the divisors of the elements in } \{\sigma(w') : \sigma \in S_N\}). \tag{7.3}$$

The definition of U and the supposition that $F_u(w)$ does not divide $\prod_{j=1}^{m} X(u, j)^{N-1}$ imply that

$$F_i(w) \text{ does not divide } \prod_{j=1}^{m} X(i, j)^{N-1} \text{ when } i \in U. \tag{7.4}$$

Let z denote a divisor of w' which lies in M. Note that $F_i(z)$ divides $F_i(w)$ when $i \in U$, because z divides w' and $w' = \prod_{i \in U} F_i(w)$. Note also that $F_i(z)$ divides $\prod_{j=1}^{m} X(i, j)^{N-1}$ for every i, because $z \in M$. These observations and statement (7.4) imply that $\deg F_i(z) < \deg F_i(w)$ for every $i \in U$. Note that, since $z | w' = \prod_{i \in U} F_i(w)$, $\deg F_i(z) = 0$ when i does not lie in U. Therefore there is an element $u' \in U$ such that $\deg F_{u'}(z) = \gamma(z)$. Suppose that $|U| > 1$ and observe that

$$\deg z - \gamma(z) = \sum_{i \in U - \{u'\}} \deg F_i(z),$$

by (7.1), the definition of u', and the fact that $\deg F_i\ (z) = 0$ when i does not lie in U. Thus

$$\deg z - \gamma(z) < \sum_{i \in U - \{u'\}} \deg F_i(z),$$

because $\deg F_i(z) < \deg F_i(w)$ for every $i \in U$ (and because $|U| > 1$). Hence

$$\deg z - \gamma(z) < \deg w - \gamma(w),$$

because $w = F_1(w) \cdots F_N(w)$ and $\deg F_{u'}(w) = \gamma(w)$ (because $\deg F_i(w) = \gamma(w)$ for every $i \in U$). Thus $\deg z - \gamma(z) < \deg w - \gamma(w)$ (when $|U| > 1$). This inequality and the induction hypothesis (for the assertion that $\sum_{v \in \{\sigma(w)\,:\,\sigma \in S_N\}} v \in B$) imply that, when $|U| > 1$, $\sum_{v \in \{\sigma(z)\,:\,\sigma \in S_N\}} v \in B$. Note also that, if $|U| = 1$, then z divides $\prod_{j=1}^{m} X(u, j)^{N-1}$ (because z divides w', $w' = F_u(w)$, and $z \in M$) and hence $\sum_{v \in \{\sigma(z)\,:\,\sigma \in S_N\}} v = E_1(z) \in B$. Thus $\sum_{v \in \{\sigma(z)\,:\,\sigma \in S_N\}} v \in B$ in all cases, i.e., for all divisors z of w' which lie in M. This observation and statement (2.1) imply that

> (the invariants of S_N) $\cap\, M \,\cap$ (the R-module generated by the divisors of the elements in $\{\sigma(w') : \sigma \in S_N\}$) is contained in B.

This containment and statement (7.3) establish the claim.

Claim 1 implies that, if $w = w'$, then $\sum_{v \in \{\sigma(w)\,:\,\sigma \in S_N\}} v \in B$. Assume now that $w \neq w'$. Observe that

$$\begin{aligned} \deg w - \gamma(w) &\geqslant \deg(w/w'), \qquad \text{because } \gamma(w) = \deg F_u(w) \leqslant \deg w' \\ &> \deg(w/w') - \gamma(w/w'), \qquad \text{because } w \neq w'. \end{aligned}$$

This inequality and the induction hypothesis (for the assertion that $\sum_{v \in \{\sigma(w)\,:\,\sigma \in S_N\}} v \in B$) imply that

$$\sum_{v \in \{\sigma(w/w')\,:\,\sigma \in S_N\}} v \in B. \tag{7.5}$$

If v is a monomial in $R[X(i, j) : 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant m]$, let $J(v)$ denote the set of subscripts j such that $\deg F_j(v) > 0$. Note that $J(w/w')$ is non-empty, because $w \neq w'$. Define

$$H_1 = \sum_{v \in \{\sigma(w')\,:\,\sigma \in S_N\}} \; \sum_{\substack{v^* \in \{\sigma(w/w')\,:\,\sigma \in S_N\} \\ J(v) \cap J(v^*) \text{ is empty}}} vv^*$$

and

$$H_2 = \sum_{v \in \{\sigma(w')\,:\,\sigma \in S_N\}} \; \sum_{\substack{v^* \in \{\sigma(w/w')\,:\,\sigma \in S_N\} \\ J(v) \cap j(v^*) \text{ is non-empty}}} vv^*.$$

Observe that

$$H_1 + H_2 = \Bigg(\sum_{v \in \{\sigma(w')\,:\,\sigma \in S_N\}} v\Bigg)\Bigg(\sum_{v^* \in \{\sigma(w/w')\,:\,\sigma \in S_N\}} v^*\Bigg) \in B, \tag{7.6}$$

by Claim 1 and (7.5).

CLAIM 2. $H_1 = \sum_{v \in \{\sigma(w) : \sigma \in S_N\}} v$.

Proof of the Claim. The definition of w' and Eq. (7.1) (with z replaced by w) imply that

$$w' = \prod_{i \in U} F_i(w) \qquad \text{and} \qquad w/w' = \prod_{i \in \{1, ..., N\} - U} F_i(w). \tag{7.7}$$

Let α and β denote elements of S_N such that $J(\alpha(w')) \cap J(\beta(w/w'))$ is empty. Then $\alpha(J(w')) \cap \beta(J(w/w'))$ is empty. Note also that $J(w') \cap J(w/w')$ is empty, by statement (7.7); therefore there is an element $\sigma \in S_N$ such that the restriction of σ to $J(w')$ equals the restriction of α to $J(w')$ and the restriction of σ to $J(w/w')$ equals the restriction of β to $J(w/w')$. Therefore $\sigma(w') = \alpha(w')$ and $\sigma(w/w') = \beta(w/w')$, so $\sigma(w) = \alpha(w')\beta(w/w')$. This proves that

$$\begin{gathered}\text{if } J(\alpha(w')) \cap J(\beta(w/w')) \text{ is empty, then} \\ \alpha(w')\beta(w/w') \in \{\sigma(w) : \sigma \in S_N\}.\end{gathered} \tag{7.8}$$

Suppose now that α and τ are elements of S_N such that $\alpha(w')$ divides $\tau(w)$. Let $\Lambda = \{\sigma(F_u(w)) : \sigma \in S_N\}$. Note that U equals the set of subscripts i such that $F_i(w)$ is divisible by an element of Λ, because of the maximality of deg $F_u(w)$ and the definition of U. Therefore

$$\begin{aligned}\tau(U) = {} & \text{the set of subscripts } i \text{ such that } F_i(\tau(w)) \\ & \text{is divisible by an element of } \Lambda \\ \supseteq {} & \alpha(U), \text{ because } F_i(\tau(w)) \text{ is divisible by } F_i(\alpha(w')) \\ & \text{for every } i \text{ and } F_i(\alpha(w')) \in \Lambda \text{ for every } i \in \alpha(U).\end{aligned}$$

Thus $\tau(U) \supseteq \alpha(U)$. Hence $\tau(U) = \alpha(U)$ (because τ and α are one-to-one and U is finite), so $\tau(w') = \alpha(w')$. This proves that, given $\tau \in S_N$, there is one and only one element of $\{\sigma(w') : \sigma \in S_N\}$ which divides $\tau(w)$, namely $\tau(w')$. Therefore there is one and only one pair (v, v^*) such that $v \in \{\sigma(w') : \sigma \in S_N\}$, $v^* \in \{\sigma(w/w') : \sigma \in S_N\}$, and $vv^* = \tau(w)$, namely, $v = \tau(w')$ and $v^* = \tau(w/w')$. Note also that $J(\tau(w')) \cap J(\tau(w/w'))$ is empty for every $\tau \in S_N$, by (7.7). These observations, together with statement (7.8) and the definition of H_1, imply that $H_1 = \sum_{v \in \{\sigma(w) : \sigma \in S_N\}} v$. This establishes the claim.

CLAIM 3. $H_2 \in B$.

Proof of the Claim. The definitions of U and w' imply that deg $F_i(\sigma(w')) = \gamma(w)$ for every $\sigma \in S_N$ and $i \in J(\sigma(w'))$. This observation and the definition of H_2 imply that, if z is a monomial which appears in H_2, then $\gamma(z) > \gamma(w)$ and $\deg z = \deg w$. This observation and the induction hypothesis (for the assertion that $\sum_{v \in \{\sigma(w) : \sigma \in S_N\}} v$ lies in B) imply that

$$\sum_{v \in \{\sigma(z) : \sigma \in S_N\}} v \in B \qquad \text{for every monomial } z \text{ which appears in } H_2. \quad (7.9)$$

Claim 2 and the first part of statement (7.6) imply that $\sigma(H_2) = H_2$ for every $\sigma \in S_N$. This observation and statement (2.1) (with $f = H_2$) imply that H_2 is an R-linear combination of the expressions $\sum_{v \in \{\sigma(z) : \sigma \in S_N\}} v$, where z varies over the monomials which appear in H_2. This observation and statement (7.9) imply that $H_2 \in B$. This establishes the claim.

Statement (7.6) and Claim 3 imply that $H_1 \in B$. This observation and Claim 2 imply that $\sum_{v \in \{\sigma(w) : \sigma \in S_N\}} v \in B$. Thus, $\sum_{v \in \{\sigma(w) : \sigma \in S_N\}} v \in B$ for every monomial w. This observation and statement (2.1) imply that $R[X(i, j) \ : 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant m]^{S_N} \subseteq B$. Note also that every element of B is a vector invariant of S_N; therefore $R[X(i, j) : 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant m]^{S_N} = B$. ▮

The following is a proof of statement (0.4), using (0.3). Let S denote a finite set of R-algebra generators of A and let R' denote the additive subgroup of R generated by 1. Note that R' is a Noetherian ring, because it is a homomorphic image of the integers, and every element of G maps $R'[\sigma(s) : \sigma \in G, s \in S]$ into itself. Therefore statement (0.3) (with $A = R'[\sigma(s) : \sigma \in G, s \in S]$) implies that

$$R'[\sigma(s) : \sigma \in G, s \in S]^G \text{ is finitely generated as an } R'\text{-algebra.} \quad (8.0)$$

Assume that $|G|$ is invertible in R and let $f \in A^G$. Note that, since $f \in A^G$,

$$\begin{aligned} f &= (1/|G|) \sum_{\sigma \in G} \sigma(f) \\ &= \text{an } R\text{-linear combination of the elements } \sum_{\sigma \in G} \sigma(w), \end{aligned}$$

where w varies over the multiplicative monoid generated by S (because $f \in A$ and A is generated as an R-algebra by S). Thus,

$$f = \text{an } R\text{-linear combination of the elements of } R'[\sigma(s) : \sigma \in G, s \in S]^G.$$

Therefore A^G is contained in the R-module generated by $R'[\sigma(s) : \sigma \in G, s \in S]^G$. Hence every set of R'-algebra generators of $R'[\sigma(s) : \sigma \in G, s \in S]^G$ will generate A^G as an R-algebra. This observation and statement (8.0) imply that A^G is finitely generated as an R-algebra. This establishes statement (0.4).

PROPOSITION 8. *If $|G|$ is invertible in R, then A^G is generated as an R-algebra by the coefficients of the polynomials $\prod_{g \in G} (1 + g(a_1^{e_1} a_2^{e_2} \cdots a_m^{e_m}) Y)$, where $e_1, ..., e_m$ vary independently over the elements of* $\{0, 1, ..., \max\{1, |G| - 1\}\}$.

Proof. Assume that $|G|$ is invertible in R, and let A' denote the R-algebra generated by the coefficients mentioned in the proposition. Let $N = |G|$ and define h as in the proof of Proposition 3. Observe that if $f \in A^G$, then by (3.1) and Proposition 7

$$\begin{aligned} &f \in h(R[X(i, j) : 1 \leqslant i \leqslant N, 1 \leqslant j \leqslant m]^{S_N}) \\ &\quad = R[h(X(1, j) X(2, j) \cdots X(N, j)), h(E_i(w)) : 1 \leqslant i \leqslant N - 1 \leqslant j \leqslant m, \\ &\qquad w \text{ divides } (X(1, 1) X(1, 2) \cdots X(1, m))^{N-1}] \\ &\quad \subseteq A'. \end{aligned}$$

Therefore $A^G \subseteq A'$. Note also that, for every $a \in A$, the coefficients of $\prod_{g \in G} (1 + g(a) Y)$ are invariants of G; therefore $A' \subseteq A^G$. Hence $A' = A^G$. ▮

REFERENCES

1. N. Bourbaki, "Groupes et Algèbres de Lie," Chaps. 4–6, Hermann, Paris, 1968.
2. H. E. A. Campbell, I. Hughes, and R. D. Pollack, Rings of invariants and p-Sylow subgroups, *Canad. Math. Bull.* **34** (1991), 42–47.
3. H. E. A. Campbell, I. Hughes, and R. D. Pollack, Vector invariants of the symmetric groups, *Canad. Math. Bull.* **33** (1990), 391–397.
4. A. Clark and J. Ewing, The realization of the polynomial algebras as cohomology rings, *Pacific J. Math.* **50** (1974), 425–434.
5. W. C. Huffman and N. J. A. Sloane, Most primitive groups have messy invariants, *Adv. in Math.* **32** (1979), 118–127.
6. G. Kempf, Computing invariants, *in* "Invariant Theory" (S. S. Koh, Ed.), Springer Lecture Notes, Vol. 1278, Springer-Verlag, Heidelberg, 1987.
7. M. Nagata, "Lectures on the Fourteenth Problem of Hilbert," Lecture Notes, Vol. 31, Tata Institute, Bombay, 1965.
8. H. Nakajima, Modular representations of finite abelian groups with regular rings of invariants, *Nagoya Math. J.* **86** (1982), 229–248.
9. H. Nakajima, Regular rings of invariants of unipotent groups, *J. Algebra* **85** (1983), 253–286.
10. E. Noether, Der Endlichkeitssatz der Invarianten endlicher Gruppen, *Math. Ann.* **77** (1916), 89–92.
11. E. Noether, Der Endlichkeitssatz der Invarianten endlich linearer Gruppen der Charakteristik p, *Nachr. Akad. Wiss. Göttingen* (1926), 28–35.
12. D. Richman, On vector invariants over finite fields, *Adv. in Math.* **81** (1990), 30–65.

13. D. E. Rutherford, "Modular Invariants," Cambridge Univ. Press, London, 1932.

14. L. Smith and R. Stong, On the invariant theory of finite groups: orbit polynomials and splitting principles, *J. Algebra* **110** (1987), 134–157.

15. B. Sturmfels and N. White, "Computing Combinatorial Decompositions of Rings," RISC-LINZ Tech. Rep. 88-51.0, Johannes Kepler Univ., Linz, 1988.

16. L. Tan, An algorithm for explicit generators of the invariants of the basic G_a-actions, *Comm. Algebra* **17** (1989), 565-572.

17. B. L. van der Waerden, "A History of Algebra," Springer-Verlag, New York, 1985.

18. E. Waring, "Meditationes Algebraicae," 3rd ed., Cambridge Univ. Press, Cambridge, 1782.

19. H. Weyl, "The Classical Groups," 2nd ed., Princeton Univ. Press, Princeton, NJ, 1946.