Discrete Math. Appl., Vol. 10, No. 5, pp. 455–468 (2000)

Vector invariants of symmetric groups in prime characteristic*

S. A. STEPANOV

Abstract — Let R be a commutative ring with the unit element 1 and S_n be the symmetric group of degree $n \geq 1$. Let $A_{mn}^{S_n}$ denote the subalgebra of invariants of the polynomial algebra

$$A_{mn} = R[x_{11}, \ldots, x_{1n}; \ldots; x_{m1}, \ldots, x_{mn}]$$

with respect to S_n. The classical result of H. Weyl implies that if every non-zero integer is invertible in R, then the algebra $A_{mn}^{S_n}$ is generated by the polarized elementary symmetric polynomials of degree at most n, no matter how large m is. As it was recently shown by D. Richman, this result remains true under the condition that $|S_n| = n!$ is invertible in R. On the other hand, if R is a field of prime characteristic $p \leq n$, D. Richman proved that every system of R-algebra generators of $A_{mn}^{S_n}$ contains a generator whose degree is no less than $\max\{n, (m+p-n)/(p-1)\}$. The last result implies that the above Weyl bound on degrees of generators no longer holds when the characteristic p of R divides $|S_n|$. In general, it is proved that, for an arbitrary commutative ring R, the algebra $A_{mn}^{S_n}$ is generated by the invariants of degree at most $\max\{n, mn(n-1)/2\}$. The purpose of this paper is to give a simple arithmetical proof of the first result of D. Richman and to sharpen his second result, again with the use of new arithmetical arguments. Independently, a similar refinement of Richman's lower bound was given by G. Kemper on the basis of completely different considerations. A recent result of P. Fleischmann shows that the lower bound obtained in the paper is sharp if $m > 1$ and n is a prime power, $n = p^{\alpha}$.

1. INTRODUCTION

Let m, n be positive integers, R be a commutative ring with the unit element 1, and

$$A_{mn} = R[x_{11}, \ldots, x_{m1}; \ldots; x_{1n}, \ldots, x_{mn}]$$

be the algebra of polynomials in mn variables x_{ij} over R. The symmetric group S_n operates on the algebra A_{mn} as a group of R-automorphisms by the rule

$$\sigma(x_{ij}) = x_{i,\sigma(j)}, \qquad \sigma \in S_n.$$

Denote by $A_{mn}^{S_n}$ the subalgebra of invariants of the algebra A_{mn} with respect to the group S_n and define the polarized elementary symmetric polynomials $u_{r_1,\ldots,r_m} \in A_{mn}^{S_n}$ in n vector variables

$$(x_{11}, \ldots, x_{m1}), \ldots, (x_{1n}, \ldots, x_{mn})$$

*UDC 519.4. Originally published in *Diskretnaya Matematika* (2000) **12**, No. 4 (in Russian). Received August 18, 2000. Translated by the author.

by means of the formal identity

$$\prod_{j=1}^{n}(1+x_{1j}z_1+\ldots+x_{mj}z_m)=1+\sum_{1\le r_1+\ldots+r_m\le n} u_{r_1,\ldots,r_m}{z_1}^{r_1}\ldots{z_m}^{r_m}.$$

The elements of $A_{mn}^{S_n}$ are usually called the vector invariants of S_n. If R is Noetherian, then it follows from the Hilbert–Noether finiteness theorem (see [6, 9]) that $A_{mn}^{S_n}$ is a finitely generated commutative R-algebra and A_{mn} is finitely generated as a module over $A_{mn}^{S_n}$. Moreover, if every non-zero integer is invertible in R, then the invariants $u_{r_1,\ldots,r_m}$ form a complete system of generators of $A_{mn}^{S_n}$ over R (see [1], p. 9; [17], p. 37). In other words, every element u of the algebra $A_{mn}^{S_n}$ may be written as a polynomial in

$$u_{r_1,\ldots,r_m}, \qquad 1\le r_1+\ldots+r_m\le n,$$

with coefficients in R. The above system of generating invariants contains $\binom{m+n}{m}-1$ elements connected with each other by different algebraic relations (see [4, p. 68] and [14]). This result was recently generalised by D. Richman [11] as follows.

Theorem 1. *Assume that $|S_n|=n!$ is invertible in R. Then $A_{mn}^{S_n}$ is generated as an R-algebra by the polarized elementary symmetric polynomials*

$$u_{r_1,\ldots,r_m}, \qquad 1\le r_1+\ldots+r_m\le n,$$

of degree at most n.

In particular, if R is a field of prime characteristic $p>n$, then $n!$ is invertible in R, and we arrive at the following result.

Corollary 1. *Let R be a field. If* $\operatorname{char}R=0$ *or* $\operatorname{char}R=p>n$, *then $A_{mn}^{S_n}$ is generated as an R-algebra by the polarized elementary symmetric polynomials*

$$u_{r_1,\ldots,r_m}, \qquad 1\le r_1+\ldots+r_m\le n.$$

In this paper, we give a simple arithmetical proof of Theorem 1 based on polarisation of classical Waring's formulas [16] and closely related to the Weyl original proof [17] in the case where R contains the field of rational numbers $\mathbf{Q}$.

The result of Theorem 1 can be easily extended as follows. Let $A=R[x_1,\ldots,x_m]$ be a finitely generated commutative R-algebra, G be a finite group of R-algebra automorphisms of A, and A^G be the subalgebra of invariants of G. If $z_1,\ldots,z_m$ are commuting indeterminates, then we set

$$F(z_1,\ldots,z_m)=\prod_{\sigma\in G}(1+\sigma(x_1)z_1+\sigma(x_2)z_2+\ldots+\sigma(x_m)z_m).$$

If every non-zero integer is invertible in R, then it follows from the Noether theorem that A^G is generated as an R-algebra by the coefficients of $F(z_1,\ldots,z_m)$. Theorem 1 and the standard arguments based on the use of the Reynolds operator and the Noether map (see [8]; [12], p. 63; [17], p. 275) lead to the following theorem.

Theorem 2. *If $|G|!$ is invertible in R, then A^G is generated as an R-algebra by the coefficients of $F(z_1,\dots,z_m)$. In other words, A^G is generated over R by invariant polynomials in $x_1,\dots,x_m$ of degree at most $|G|$.*

The results of Theorems 1 and 3 provide us with an efficient algorithm to compute a complete system of generating polynomial invariants under the condition that $|G|!$ is invertible in R. There is another constructive proof of Theorem 3 based on different arguments also ascending to Noether ([12], p. 29). The upper bound on the degrees of a set of generating polynomials for the algebra of invariants given by Theorem 3 is known as Noether's bound (see also [12], p. 28, and [13]).

If $|S_n| = n!$ is invertible in R, then the upper bound on degrees of R-algebra generators of $A_{mn}^{S_n}$, stated in Theorem 1, is the best possible. In the case where R is an arbitrary commutative ring, it is proved in [3] that the Weyl algebra $A_{mn}^{S_n}$ is generated over R by polynomials of degree at most $\max\{n, mn(n-1)/2\}$. A similar result was also obtained by Richman (see [11], Prop. 7). On the other hand, this paper gives the following lower bound.

Theorem 3. *Let α be a positive integer, S_n be the symmetric group of degree $n \geq 2$, and R be a field of prime characteristic p. If p^α divides n, then every system of R-algebra generators of $A_{mn}^{S_n}$ contains a generator whose degree is no less than* $\max\{n, m(p^\alpha - 1)\}$.

This result sharpens the above mentioned Richman's lower bound in the case where p is a divisor of n, and shows that Noether's upper bound is false if n is not invertible in R. As it was recently proved by P. Fleischmann [5], the lower bound in Theorem 3 is exact if $n = p^\alpha$ and $m > 1$.

The result of Theorem 3 can be easily extended as follows. Let r be a positive integer that does not exceed n. In that case, the group S_r is a subgroup of S_n and therefore $A_{mn}^{S_n} \subseteq A_{mn}^{S_r}$. This observation and Theorem 3 applying to S_r yield the following result.

Corollary 2. *Let λ and $r \leq n$ be positive integers, S_n be the symmetric group of degree $n \geq 2$, and R be a field of prime characteristic p. If p^λ divides r, then in any system of R-algebra generators of $A_{mn}^{S_n}$ there exists a generator whose degree is no less than* $\max\{n, m(p^\lambda - 1)\}$.

Corollary 3. *Let S_n be the symmetric group of degree $n \geq 2$ and R be a commutative ring with the unit element* 1. *If p is a prime divisor of $n!$ which is not invertible in R, then every system of R-algebra generators of $A_{mn}^{S_n}$ contains a generator whose degree is no less than* $\max\{n, m(p-1)\}$.

If $R = \mathbf{Z}$ is the ring of integers, then we can use the well-known results on the distribution of primes in short intervals to get an universal lower bound in terms of m and n.

Corollary 4. *Let $R = \mathbf{Z}$ be the ring of integers and S_n be the symmetric group of degree $n \geq 2$. Then every system of R-algebra generators of $A_{mn}^{S_n}$ contains a generator whose degree is no less than* $\max\{n, c_n m(n-1)\}$, *where $c_n = 1/2$ for every $n \geq 2$; moreover, $c_n = 5/6$ for every $n \geq 25$, and $c_n \to 1$ as $n \to \infty$. In particular, if n is a prime number, then every*

system of R-algebra generators of $A_{mn}^{S_n}$ contains a generator whose degree is no less than $\max\{n, m(n-1)\}$.

A similar result holds in the case where R is the ring $\mathbf{Z}_K$ of integers of a number field K.

2. GENERATING INVARIANTS OF THE SYMMETRIC GROUP S_n

Let S_n be the symmetric group of degree $n \geq 1$ that operates on the R-algebra

$$A_{mn} = R[x_{11}, \ldots, x_{m1}; \ldots; x_{1n}, \ldots, x_{mn}]$$

as a group of R-automorphisms, $A_{mn}^{S_n}$ be the subalgebra of invariants of the algebra A_{mn}, and

$$u_{r_1,\ldots,r_m}, \qquad 1 \leq r_1 + \ldots + r_m \leq n,$$

be the polarized elementary symmetric polynomials in $A_{mn}^{S_n}$.

Let $v_{s_1,\ldots,s_m}$ be an invariant polynomial in $A_{mn}^{S_n}$ of the form

$$v_{s_1,\ldots,s_m} = \sum_{j=1}^{n} x_{1j}^{s_1} \ldots x_{mj}^{s_m}.$$

If $m = 1$, then according to the well-known Waring formula (see [16], p. 13, and [2], p. 99)

$$v_s = \sum_{j=1}^{n} x_j^s = \sum_{k_1+2k_2+\ldots+nk_n=s} c(k_1, \ldots, k_n) u_1^{k_1} \ldots u_n^{k_n}, \tag{1}$$

where $c_{k_1,\ldots,k_n}$ are integers of the form

$$c(k_1, \ldots, k_n) = (-1)^{k_2+2k_3+\ldots+(n-1)k_n} \frac{(k_1 + \ldots + k_n - 1)!}{k_1! \ldots k_n! s}.$$

The following result can be considered as a generalisation of the Waring formula to the case where $m > 1$ (see also [14], [15]).

Proposition 1. *Let $s_1, \ldots, s_m$ be non-negative integers,*

$$v_{s_1,\ldots,s_m} = \sum_{j=1}^{n} x_{1j}^{s_1} \ldots x_{mj}^{s_m}$$

be the polynomial in $A_{mn}^{S_n}$ of degree $s = s_1 + \ldots + s_m$, and

$$u_{r_1,\ldots,r_m}, \qquad 1 \leq r_1 + \ldots + r_m \leq n,$$

be the polarized elementary symmetric polynomials of the vectors

$$(x_{1j}, \ldots, x_{mj}), \qquad 1 \leq j \leq n.$$

For non-negative integers $k_1, \ldots, k_n$ *and* $k_{1\nu}, \ldots, k_{m\nu}$ *such that*

$$k_1 + 2k_2 + \ldots + nk_n = s,$$
$$k_{1\nu} + \ldots + k_{m\nu} = \nu k_\nu, \qquad 1 \leq \nu \leq n,$$

let

$$w_{k_{1\nu},\ldots,k_{m\nu}} = \sum_{A_{m,n}} \frac{k_\nu!}{l_{\nu 1}! \ldots l_{\nu k_\nu}!} \prod_{\mu=1}^{k_\nu} u_{r_{1\mu},\ldots,r_{m\mu}}^{l_{\nu\mu}},$$

where the sum is over the set $A_{m,n}$ *of all non-negative integers* $r_{1\mu}, \ldots, r_{m\mu}$ *and* $l_{\nu 1}, \ldots, l_{\nu k_\nu}$ *such that*

$$r_{i1} l_{\nu 1} + \ldots r_{ik_\nu} l_{\nu k_\nu} = k_{i\nu},$$
$$l_{\nu 1} + \ldots + l_{\nu k_\nu} = k_\nu,$$
$$r_{1\mu} + \ldots + r_{m\mu} = \nu$$

for $1 \leq i \leq m$, $1 \leq \mu \leq k_\nu$, $1 \leq \nu \leq n$.

Then

$$v_{s_1,\ldots,s_m} = \frac{s_1! \ldots s_m!}{s!} \sum_{k_1+2k_2+\ldots+nk_n=s} c(k_1, \ldots, k_n) \sum_{B_{m,n}} \prod_{\nu=1}^{n} w_{k_{1\nu},\ldots,k_{m\nu}},$$

where the inner sum is over the set $B_{m,n}$ *of all non-negative integers* $k_{i1}, \ldots, k_{in}$ *satisfying the relations*

$$k_{i1} + \ldots + k_{in} = s_i,$$
$$k_{1\nu} + \ldots + k_{m\nu} = \nu k_\nu$$

for $1 \leq i \leq m$, $1 \leq \nu \leq n$.

Proof. In (1) we set

$$x_j = x_{1j} z_1 + \ldots + x_{mj} z_m, \qquad 1 \leq j \leq n.$$

Since

$$(x_{1j} z_1 + \ldots + x_{mj} z_m)^s = \sum_{s_1+\ldots+s_m=s} \frac{s!}{s_1! \ldots s_m!} x_{1j}^{s_1} \ldots x_{mj}^{s_m} z_1^{s_1} \ldots z_m^{s_m},$$

we have

$$\sum_{j=1}^{n} (x_{1j} z_1 + \ldots + x_{mj} z_m)^s = \sum_{s_1+\ldots+s_m=s} \frac{s!}{s_1! \ldots s_m!} \left(\sum_{j=1}^{n} x_{1j}^{s_1} \ldots x_{mj}^{s_m} \right) z_1^{s_1} \ldots z_m^{s_m}.$$

On the other hand,

$$\sum_{1 \leq j_1 < \ldots < j_\nu \leq n} \prod_{k=1}^{\nu} (x_{1j_k} z_1 + \ldots + x_{mj_k} z_m) = \sum_{r_1+\ldots+r_m=\nu} u_{r_1,\ldots,r_m} z_1^{r_1} \ldots z_m^{r_m}$$

and hence, in view of (1),

$$\sum_{j=1}^{n}(x_{1j}z_1+\ldots+x_{mj}z_m)^s = \sum_{k_1+2k_2+\ldots+nk_n=s} c(k_1,\ldots,k_n)\prod_{\nu=1}^{n}\left(\sum_{r_1+\ldots+r_m=\nu} u_{r_1,\ldots,r_m}z_1^{r_1}\ldots z_m^{r_m}\right)^{k_\nu}$$

As a result we find that

$$\sum_{s_1+\ldots+s_m=s}\frac{s!}{s_1!\ldots s_m!}\left(\sum_{j=1}^{n}x_{1j}^{s_1}\ldots x_{mj}^{s_m}\right)z_1^{s_1}\ldots z_m^{s_m} \sum_{k_1+2k_2+\ldots+nk_n=s} c(k_1,\ldots,k_n)\prod_{\nu=1}^{n}\left(\sum_{r_1+\ldots+r_m=\nu} u_{r_1,\ldots,r_m}z_1^{r_1}\ldots z_m^{r_m}\right)^{k_\nu}$$

Now since

$$\left(\sum_{r_1+\ldots+r_m=\nu} u_{r_1,\ldots,r_m}z_1^{r_1}\ldots z_m^{r_m}\right)^{k_\nu} = \sum_{k_{1\nu}+\ldots+k_{m\nu}=\nu k_\nu} w_{k_{1\nu},\ldots,k_{m\nu}}z_1^{k_{1\nu}}\ldots z_m^{k_{m\nu}},$$

where

$$w_{k_{1\nu},\ldots,k_{m\nu}} = \sum_{C_{m,\nu}}\frac{k_\nu!}{l_{\nu 1}!\ldots l_{\nu k_\nu}!}\prod_{\mu=1}^{k_\nu}u_{r_{1\mu},\ldots,r_{m\mu}}^{l_{\nu\mu}},$$

and the summation is over the set $C_{m,\nu}$ of all non-negative integers $r_{1\mu},\ldots,r_{m\mu}$ and $l_{\nu 1},\ldots,l_{\nu k_\nu}$ such that

$$\begin{aligned} r_{i1}l_{\nu 1}+\ldots+r_{is_\nu}l_{\nu k_\nu} &= k_{i\nu}, \qquad 1\le i\le m,\\ r_{1\mu}+\ldots+r_{m\mu} &= \nu, \qquad 1\le \mu\le k_\nu,\\ l_{\nu 1}+\ldots+l_{\nu k_\nu} &= k_\nu, \end{aligned}$$

we find that

$$\sum_{s_1+\ldots+s_m=s}\frac{s!}{s_1!\ldots s_m!}\left(\sum_{j=1}^{n}x_{1j}^{s_1}\ldots x_{mj}^{s_m}\right)z_1^{s_1}\ldots z_m^{s_m} = \sum_{s_1+\ldots+s_m=s}\left(\sum_{k_1+2k_2+\ldots+nk_n=s} c(k_1,\ldots,k_n)\sum_{B_{m,n}}\prod_{\nu=1}^{n}w_{k_{1\nu},\ldots,k_{m\nu}}\right)z_1^{s_1}\ldots z_m^{s_m},$$

where the summation in the last sum is over the set $B_{m,n}$ of all non-negative integers $k_{i1},\ldots,k_{iv}$, $i=1,\ldots,m$ such that

$$\begin{aligned} k_{i1}+\ldots+k_{iv} &= s_i,\\ k_{1\nu}+\ldots+k_{m\nu} &= \nu k_\nu, \end{aligned}$$

for $1 \le i \le m$, $1 \le v \le n$.

Thus we arrive at the relation

$$\sum_{j=1}^{n} x_{1j}^{s_1} \dots x_{mj}^{s_m} = \frac{s_1! \dots s_m!}{s!} \sum_{k_1+2k_2+\dots+nk_n=s} c(k_1, \dots, k_n) \sum_{B_{m,n}} \prod_{v=1}^{n} w_{k_{1v},\dots,k_{mv}},$$

which proves the proposition.

If $s = s_1 + \dots + s_m \le n+1$, then

$$v_{s_1,\dots,s_m} = \frac{s_1! \dots s_m!}{s!} \sum_{k_1+2k_2+\dots+nk_n=s} c(k_1, \dots, k_n) \sum_{B_{m,n}} \prod_{v=1}^{n} w_{k_{1v},\dots,k_{mv}}$$

is a polynomial in $u_{r_1,\dots,r_m}$, $1 \le r_1 + \dots + r_m \le n$, with rational coefficients whose denominators are not divisible by any prime $p \ge n+1$. As a consequence of this observations we get the following result.

Corollary 5. *If $n!$ is invertible in R and $s = s_1 + \dots + s_m \le n+1$, then*

$$v_{s_1,\dots,s_m} = \sum_{j=1}^{n} x_{1j}^{s_1} \dots x_{mj}^{s_m}$$

is a polynomial over R in $u_{r_1,\dots,r_m}$, $1 \le r_1 + \dots + r_m \le n$, of degree at most n.

Now we show that if $n!$ is invertible in R, then any vector invariant in $A_{mn}^{S_n}$ can be represented as a polynomial over R in the invariants $v_{s_1,\dots,s_m}$.

Proposition 2. *Let f be a monomial in A_{mn} and*

$$v = \sum_{u \in \{\sigma(f) | \sigma \in S_n\}} u.$$

If $n!$ is invertible in R, then v is a polynomial over R in the invariants

$$v_{s_1,\dots,s_m} = \sum_{j=1}^{n} x_{1j}^{s_1} \dots x_{mj}^{s_m},$$

where $s_1, \dots, s_m$ are non-negative integers satisfying the condition

$$0 \le s_1 + \dots + s_m \le \deg f.$$

Proof. We represent f in the form $f = f_1 \dots f_n$, where each f_j is a monomial in $R[x_{1j}, \dots, x_{mj}]$. We set

$$d(f) = \max_{1 \le j \le n} (\deg f_j)$$

and prove the assertion by induction on $\delta(f) = \deg f - d(f)$. Suppose at first that $\delta(f) = 0$. Then $f = f_j = x_{1j}^{s_1} \dots x_{mj}^{s_m}$, where $j \in \{1, 2, \dots, n\}$ and $s_1, \dots, s_m$ are non-negative integers with the condition $s_1 + \dots + s_m = \deg f$, and

$$v = \sum_{u \in \{\sigma(f) | \sigma \in S_n\}} u = \sum_{j=1}^{n} x_{1j}^{s_1} \dots x_{mj}^{s_m}.$$

Suppose now that $\delta(f) > 0$ and let $j \in \{1, 2, \ldots, n\}$ be such that

$$d(f) = \deg f_j < \deg f.$$

we define v_j and v'_j, setting

$$v_j = \sum_{u \in \{\sigma(f_j) | \sigma \in S_n\}} u, \qquad v'_j = \sum_{u' \in \{\sigma(f/f_j) | \sigma \in S_n\}} u'.$$

The induction hypothesis implies that v_j and v'_j are polynomials in

$$v_{s_1, \ldots, s_m}, \qquad 0 \le s_1 + \ldots + s_m \le \deg f.$$

For every $\tau \in S_n$, we define U_τ to be the set of all pairs (u, u') such that

$$u \in \{\sigma(f_j) \mid \sigma \in S_n\}, \quad u' \in \{\sigma(f/f_j) \mid \sigma \in S_n\}, \quad uu' = \tau(f)$$

and note that the map

$$U_{id} \to U_\tau, \qquad (u, u') \to (\tau(u), \tau(u'))$$

is a bijection. Thus $|U_\tau| = |U_{id}|$ for all $\tau \in S_n$. Note also that $d(uu') \ge d(f)$ for all $u \in \{\sigma(f_j) \mid \sigma \in S_n\}$ and $u' \in \{\sigma(f/f_j) \mid \sigma \in S_n\}$, where the equality is attained if and only if $uu' \in \{\sigma(f) \mid \sigma \in S_n\}$. Therefore,

$$v_j v'_j = |U_{id}| \sum_{u \in \{\sigma(f) | \sigma \in S_n\}} u + \sum_{f' :\ \deg f' = \deg f, d(f') > d(f)} \ \sum_{u \in \{\sigma(f') | \sigma \in S_n\}} u.$$

By the induction hypothesis, the invariant

$$v_j v'_j - |U_{id}| \sum_{u \in \{\sigma(f) | \sigma \in S_n\}} u = \sum_{f' :\ \deg f' = \deg f, d(f') > d(f)} \ \sum_{u \in \{\sigma(f') | \sigma \in S_n\}} u$$

is a polynomial over R in $v_{s_1, \ldots, s_m}$, $0 \le s_1 + \ldots + s_m \le \deg f$. The cardinality of U_{id} does not exceed the cardinality of $\{\sigma(f_j) \mid \sigma \in S_n\}$ and the last cardinality does not exceed the cardinality of $\{x_{1j}^{s_1} \ldots x_{mj}^{s_m} \mid 1 \le j \le n\}$, therefore $1 \le |U_{id}| \le n$. Since $n!$ is invertible in R, we conclude that

$$\sum_{u \in \{\sigma(f) | \sigma \in S_n\}} u$$

is a polynomial over R in $v_{s_1, \ldots, s_m}$, $0 \le \sigma_1 + \ldots + \sigma_m \le \deg f$. This completes the proof.

Let S_n be the symmetric group of degree $n \ge 2$ and

$$v_{s_1, \ldots, s_m} = \sum_{j=1}^{n} x_{1j}^{s_1} \ldots x_{mj}^{s_m}$$

be a homogeneous polynomial in $A_{mn}^{S_n}$ of degree $s_1 + \ldots + s_m \ge 1$. Let R be a field of prime characteristic p dividing n. The following result shows that Weyl's bound fails to be correct over R for $m > n \ge 2$.

Proposition 3. *Let R be a field of prime characteristic p and S_n be the symmetric group of degree $n \geq 2$. If p divides n, and $m > n$, then the element $v_{11\ldots11} \in A_{mn}^{S_n}$ cannot be expressed as a polynomial over R in the invariants*

$$u_{r_1,\ldots,r_m}, \qquad 1 \leq r_1 + \ldots + r_m \leq n.$$

Proof. Assume, for a contradiction, that $v_{11\ldots11}$ is expressible as a polynomial over R in $u_{r_1,\ldots,r_m}$, $1 \leq r_1 + \ldots + r_m \leq n$, and write $v_{11\ldots11}$ in the form

$$v_{11\ldots11} = \sum_{s_1+2s_2+\ldots+ns_n=m} a_{s_1,\ldots,s_n} \sum_{R_m(s_1,\ldots,s_n)} \prod_{\nu=1}^{n} \prod_{\sigma_\nu=1}^{s_\nu} u_{r_{1\sigma_\nu},\ldots,r_{m\sigma_\nu}}$$

with some $a_{s_1,\ldots,s_n} \in R$, where $R_m(s_1,\ldots,s_n)$ is the set of all non-negative integers $r_i j$, $i = 1,\ldots,m$, $j = 1,\ldots,s_\nu$, $\nu = 1,\ldots,n$ such that

$$r_{1\sigma_\nu} + \ldots + r_{m\sigma_\nu} = \nu, \quad 1 \leq \sigma_\nu \leq s_\nu, \quad 1 \leq \nu \leq n,$$
$$r_{i\sigma_1} + \ldots + r_{i\sigma_n} = 1, \qquad 1 \leq i \leq m.$$

Without loss of generality we may assume that if $k \leq n$ is the smallest positive integer such that $s_k \geq 1$, then

$$r_{1\sigma_k} = \begin{cases} 1 & \text{if } \sigma_k = 1, \\ 0 & \text{if } 2 \leq \sigma_k \leq s_k. \end{cases}$$

Differentiating the above equality with respect to x_{11} and taking into account that

$$\frac{\partial u_{r_1,\ldots,r_m}}{\partial x_{11}} = \begin{cases} 0 & \text{if } r_1 = 0, \\ u_{0,r_2,\ldots,r_m}^{(1,0,\ldots,0)} & \text{if } r_1 = 1, \end{cases}$$

where $u_{0,r_2,\ldots,r_m}^{(1,0,\ldots,0)}$ is the corresponding elementary symmetric polynomial of vectors $(x_{2j},\ldots,x_{mj})$, $1 \leq j \leq n$, we obtain

$$x_{21}\ldots x_{m1} = \sum_{s_1+2s_2+\ldots+ns_n=m} a_{s_1,\ldots,s_n} \sum_{j=1}^{n} \Psi_{s_1,\ldots,s_n}^{(j)}, \tag{2}$$

where

$$\Psi_{s_1,\ldots,s_n}^{(j)} = \sum_{R_m(s_1,\ldots,s_n)} u_{0,r_{2\sigma_k},\ldots,r_{m\sigma_k}}^{(1,0,\ldots,0)} \prod_{\sigma_k=2}^{s_k} u_{0,r_{2\sigma_k},\ldots,r_{m\sigma_k}} \prod_{\nu=1,\nu\neq k}^{n} \prod_{\sigma_\nu=1}^{s_\nu} u_{0,r_{2\sigma_\nu}\ldots,r_{m\sigma_\nu}}.$$

We denote by $\omega_{0,r_2,\ldots,r_m}$ the value of $u_{0,r_2,\ldots,r_m}$ at the point

$$(x_{11},\ldots,x_{m1};\ldots;x_{1n},\ldots,x_{mn}) = (1,\ldots,1;\ldots;1\ldots,1).$$

Since $m > n \geq 2$, each binary sequence $(0,r_2,\ldots,r_m)$ encountered in the last equality contains l non-zero elements for some $1 \leq l \leq n$. In that case

$$\omega_{0,r_2,\ldots,r_m} = n(n-1)\ldots(n-l+1),$$

and setting

$$x_{11} = \ldots = x_{m1} = \ldots = x_{1n} = \ldots = x_{mn} = 1$$

in (2), we arrive at the relation

$$1 = n \sum_{s_1+2s_2+\ldots+ns_n=m} b_{s_1,\ldots,s_n},$$

which is impossible in R for any prime p dividing n. This completes the proof.

3. PROOF OF THEOREM 1

Let S_n be the symmetric group of degree n. Suppose that f is a monomial in A_{mn} and $w \in A_{mn}^{S_n}$ is a polynomial invariant of S_n. Since $\sigma(w) = w$ for any $\sigma \in S_n$, the polynomials w and $\sigma(w)$ have equal coefficients. This shows that every polynomial invariant of S_n is an R-linear combination of the invariants

$$v = \sum_{u \in \{\sigma(f) | \sigma \in S_n\}} u,$$

where f varies over the monomials which appear in w.

Let $(i_1, i_2, \ldots, i_\mu)$ be a sequence of elements $i_1, i_2, \ldots, i_\mu \in \{1,2,\ldots,n\}$. At first we prove that every invariant w_μ of the form

$$w_\mu = \sum_{j=1}^{n} x_{i_1,j} \ldots x_{i_\mu,j}$$

is a polynomial over R in polarized elementary symmetric polynomials

$$u_{r_1,\ldots,r_m}, \qquad 1 \le r_1 + \ldots + r_m \le n.$$

If $\mu \le n+1$, then the assertion of Theorem 1 follows from Proposition 1. Assume now that $\mu > n+1$ and proceed the proof by induction on μ. Let

$$\tilde{x}_{i_s,j} = \begin{cases} x_{i_s,j} & \text{if } s \le n, \\ x_{i_{n+1},j} x_{i_{n+2},j} \ldots x_{i_{\mu+1},j} & \text{if } s = n+1 \end{cases}$$

for $j = 1,2,\ldots,n$, and write

$$w_{\mu+1} = \sum_{j=1}^{n} \tilde{x}_{i_1,j} \ldots \tilde{x}_{i_n,j} \tilde{x}_{i_{n+1},j}.$$

Let

$$\tilde{A}_{mn} = R[\tilde{x}_{11}, \ldots, \tilde{x}_{m1}; \ldots; \tilde{x}_{1n}, \ldots, \tilde{x}_{mn}]$$

and let $\tilde{A}_{mn}^{S_n}$ be the subalgebra of invariants of $\tilde{A}_{mn}$. It follows from Corollary 5 that $w_{\mu+1}$ is a polynomial over R in the polarized elementary symmetric polynomials

$$\tilde{u}_{r_1,\ldots,r_m} \in \tilde{A}_{mn}, \quad 1 \le r_1 + \ldots + r_m \le n.$$

Since every such polynomial $\tilde{u}_{r_1,\ldots,r_m}$ has the form

$$\tilde{u}_{r_1,\ldots,r_m} = \sum_{\bar{u}\in\{\tau(\tilde{f})|\tau\in G\}} \bar{u},$$

for some monomial $\tilde{f} \in \tilde{A}_{mn}$ of degree at most n, by Proposition 1 it can be written as a polynomial over R in the invariants

$$\tilde{v}_{s_1,\ldots,s_m} = \sum_{j=1}^{n} \tilde{x}_{1j}^{s_1} \ldots \tilde{x}_{mj}^{s_m}$$

of degree at most n. Moreover, each $\tilde{v}_{s_1,\ldots,s_m}$ has the form

$$\tilde{v}_{s_1,\ldots,s_m} = \sum_{j=1}^{n} x_{1j}^{t_1} \cdots x_{mj}^{t_j},$$

where $1 \leq t_1 + \ldots + t_m \leq \mu$. The induction hypothesis implies that every invariant $\tilde{v}_{s_1,\ldots,s_m}$ is a polynomial over R in

$$u_{r_1,\ldots,r_m}, \qquad 1 \leq r_1 + \ldots + r_m \leq n,$$

therefore $w_{\mu+1}$ is also a polynomial over R in the polarized elementary symmetric polynomials $u_{r_1,\ldots,r_m}$, $1 \leq r_1 + \ldots + r_m \leq n$.

To complete the proof, we note now that every element $v \in A_{mn}^{S_n}$ can be written, in view of Proposition 2, as a polynomial over R in the invariants w_μ.

4. PROOF OF THEOREM 3

The arguments which we shall use are the same as in the proof of Proposition 3. Let S_n be the symmetric group of degree $n \geq 2$, and suppose that p is a prime divisor of n. Let R be a field of characteristic p and $A_{mn}^{S_n}$ be the algebra of vector invariants over R with respect to S_n. Let

$$v_{s_1,\ldots,s_m}, \qquad s_1 + \ldots + s_m \geq 1,$$

denote a polynomial in $A_{mn}^{S_n}$ of the form

$$v_{s_1,\ldots,s_m} = \sum_{j=1}^{n} x_{1j}^{s_1} \ldots x_{mj}^{s_m}.$$

Recall that every vector invariant $v \in A_{mn}^{S_n}$ is an R-linear combination of the invariants

$$w = \sum_{u\in\{\sigma(f)|\sigma\in S_n\}} u,$$

where f varies over the monomials in A_{mn} which appear in v.

To prove Theorem 3, it is sufficient to show that if $p^\alpha \mid n$, then every system of R-algebra generators of $A_{mn}^{S_n}$ contains at least one generator v of degree $m(p^\alpha - 1)$. The crucial point is that the invariant $v_{p^\alpha-1,\ldots,p^\alpha-1}$ of degree $m(p^\alpha - 1)$ cannot be presented as a polynomial over R in vector invariants of smaller degree.

We denote by $W_{mn}^{S_n}$ the set of R-algebra generators of $A_{mn}^{S_n}$ of the form

$$w = \sum_{u \in \{\sigma(f) | \sigma \in S_n\}} u,$$

where f is a monomial in A_{mn} of degree less than $m(p^\alpha - 1)$. Since every vector invariant $v \in A_{mn}^{S_n}$ whose degree is less than $m(p^\alpha - 1)$ can be written as an R-linear combination of elements $w \in W_{mn}^{S_n}$, it suffices to prove that the invariant $v_{p^\alpha - 1, \dots, p^\alpha - 1}$ is not representable as a polynomial over R in the elements $w \in W_{mn}^{S_n}$. Let l denote the cardinality of $W_{mn}^{S_n}$. We enumerate the elements of $W_{mn}^{S_n}$ by the numbers $1, 2, \dots, l$ and assume, for the contradiction, that the invariant $v_{p^\alpha - 1, \dots, p^\alpha - 1}$ is a polynomial over R in $w_1, \dots, w_l$, that is,

$$v_{p^\alpha - 1, \dots, p^\alpha - 1} = \sum_M a_{\mu_1, \dots, \mu_l} w_1^{\mu_1} \dots w_l^{\mu_l}, \qquad a_{\mu_1, \dots, \mu_l} \in R, \tag{3}$$

where M is the set of all non-negative integers $\mu_1, \dots, \mu_l$ such that

$$0 \le \mu_1 + \dots + \mu_l \le m(p^\alpha - 1),$$
$$\mu_1 \deg w_1 + \dots + \mu_l \deg w_l = m(p^\alpha - 1).$$

Comparing the degrees of the monomials which appear in both sides of the last identity (with respect to each of the variables $x_{11}, \dots, x_{m1}; \dots; x_{1n}, \dots, x_{mn}$), we find that $\mu_k \in \{0, 1, \dots, p^\alpha - 1\}$, $1 \le k \le l$, and $\mu_1 + \dots + \mu_l > 1$; moreover, every invariant

$$w_k = \sum_{u \in \{\sigma(f_k) | \sigma \in S_n\}} u,$$

which appears in the right-hand side with a non-zero coefficient, is generated by a monomial $f_k \in A_{mn}$ of the form

$$f_k = (x_{1 j_{11}^{(k)}} \dots x_{1 j_{1\nu_1}^{(k)}}) \dots (x_{m j_{m1}^{(k)}} \dots x_{m j_{m\nu_m}^{(k)}}),$$

where $1 \le j_{i j_{i1}}^{(k)} \le \dots \le j_{i \nu_i^{(k)}} \le n$ and $j_{i \nu_i^{(k)}} \le p^\alpha - 1$ at least for one i, $i = 1, 2, \dots, m$.

We denote by ω_k the value of w_k at the point

$$(x_{11}, \dots, x_{m1}; \dots; x_{1n}, \dots, x_{mn}) = (1, \dots, 1; \dots; 1, \dots, 1)$$

and observe that $\omega_k = |\mathrm{orb}(f_k)|$, where

$$\mathrm{orb}(f_k) = \{\sigma(f_k) \mid \sigma \in S_n\}$$

is the orbit of f_k under S_n. If

$$S_n(f_k) = \{\sigma \in S_n \mid \sigma(f_k) = f_k\}$$

is the isotropy group of f_k, then

$$|\mathrm{orb}(f_k)| = \frac{|S_n|}{|S_n(f_k)|} = \frac{n!}{|S_n(f_k)|}.$$

Since $j_{iv_i^{(k)}} \leq p^\alpha - 1$ for every $k = 1,2,\ldots,l$ and at least for one i, $i = 1,2,\ldots,m$, the exponent of p in the prime factorisation of every $|S_n(f_k)|$ is less than the exponent of p in the prime factorisation of $n!$. This implies that $|\mathrm{orb}(f_k)|$ is divisible by p, therfore $\omega_k = 0$ in R for all $k = 1,2,\ldots,l$. Differentiating now identity (3) with respect to x_{11}, setting

$$x_{11} = \ldots = x_{m1} = \ldots = x_{1n} = \ldots = x_{mn} = 1$$

in the resulting identity, and taking into account that every product

$$w_1^{\mu_1} \ldots w_l^{\mu_l}$$

in the right-hand side of (3) involves at least two factors, say w_k and $w_{k'}$, with $1 \leq k \leq k' \leq l$, we arrive at the relation $p - 1 = 0$, which is impossible in R.

Since the invariant $v_{p^\alpha - 1,\ldots,p^\alpha - 1}$ cannot be written as a polynomial over R in vector invariants of smaller degree, every system of R-algebra generators of $A_{mn}^{S_n}$ has to contain at least one generator of degree $m(p^\alpha - 1)$. Observing now that every system of R-algebra generators of $A_{mn}^{S_n}$ contains a generator of degree n (for example, the invariant $w = x_{11}\ldots x_{1n}$), we find that it has to contain a generator v whose degree is no less than $\max\{n, m(p^\alpha - 1)\}$.

5. PROOF OF COROLLARY 3

Let R be a commutative ring with the unit element 1, let p be a prime divisor of $n!$, and $\mathfrak{m}$ be a maximal ideal in R that contains p. Then $F = R/\mathfrak{m}$ is a field of characteristic p. Consider the reduction homomorphism

$$\varphi\colon R[x_{11},\ldots,x_{m1};\ldots;x_{n1},\ldots,x_{mn}] \to F[x_{11},\ldots,x_{m1};\ldots;x_{n1},\ldots,x_{mn}],$$

which leaves fixed all the variables x_{ij}, $1 \leq i \leq m, 1 \leq j \leq n$. This homomorphism induces a surjective homomorphism

$$\psi\colon R[x_{11},\ldots,x_{m1};\ldots;x_{n1},\ldots,x_{mn}]^{S_n} \to F[x_{11},\ldots,x_{m1};\ldots;x_{1n},\ldots,x_{mn}]^{S_n}.$$

Therefore ψ maps every set of generators of $R[x_{11},\ldots,x_{m1};\ldots;x_{1n},\ldots,x_{mn}]^{S_n}$ to a set of generators of $F[x_{11},\ldots,x_{m1};\ldots;x_{1n},\ldots,x_{mn}]^{S_n}$. This fact and Corollary 2 imply that every system of R-algebra generators of $R[x_{11},\ldots,x_{m1};\ldots;x_{1n},\ldots,x_{mn}]^{S_n}$ contains a generator of degree at least $\max\{n, m(p-1)\}$. In particular, if $n = p$ is a prime number, we conclude that it contains a generator whose degree is no less than $\max\{n, m(n-1)\}$.

REFERENCES

1. D. J. Benson, *Polynomial Invariants of Finite Groups.* Cambridge Univ. Press, Cambridge, 1993.
2. N. Bourbaki, *Elements of Mathematics, Algebra II.* Springer, Berlin, 1990.
3. H. E. A. Campbell, I. Hughes, and R. D. Pollack, Vector invariants of symmetric groups, *Canad. Math. Bull.* (1990) **33**, 391–397.
4. J. A. Dieudonne and J. B. Carrel, *Invariant Theory, Old and New.* Academic Press, New York, 1971.

5. P. Fleischmann, A new degree bound for vector invariants of symmetric groups. *Trans. Amer. Math. Soc.* (1998) **350**, 1703–1712.
6. D Hilbert, Über die vollen Invariantensystem. *Math. Ann.* (1893) **42**, 313–373.
7. G. Kemper, Lower degree bounds for modular invariants and a question of I. Hughes. *Transformation Groups* (1998) **3**, 135–144.
8. E. Noether, Der Endlichkeitssatz der Invarianten endlicher Gruppen. *Math. Ann.* (1916) **77**, 89–92.
9. E. Noether, Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik *p*. *Nachr. Ges. Wiss. Göttingen* (1926), 28–35.
10. D. R. Richman, Invariants of finite groups over fields of characteristic *p*. *Adv. Math.* (1996) **124**, 25–48.
11. D. R. Richman, Explicit generators of the invariants of finite groups. *Adv. Math.* (1996) **124**, 49–76.
12. L. Smith, *Polynomial Invariants of Finite Groups.* A K Peters, Wellesley, MA, 1995.
13. L. Smith, Polynomial invariants of finite groups. A survey of recent developments. *Bull. Amer. Math. Soc.* (1997) **34**, 211–250.
14. S. A. Stepanov, Transcendence bases of the algebra of vector invariants for a symmetric group. *Proc. Intern. Conf. Number Theory*, Berlin, 1999, 487–501.
15. S. A. Stepanov, Polynomial invariants of finite groups in prime characteristic. *Discrete Math. Appl.* (1999) **9**, 343–354.
16. E. Waring, *Meditationes Algebraicae.* Cambridge Univ. Press, Cambridge, 1782.
17. H. Weyl, *The Classical Groups, their Invariants and Representations.* New Jersey, 1939.