JOURNAL OF ALGEBRA **180,** 341–363 (1996)
ARTICLE NO. 0071

Efficient Generation of the Ring of Invariants*

Shou-Jen Hu†

Department of Mathematics, Tamkang University, Tam Shui, Taipei, Taiwan

and

Ming-chang Kang‡

Department of Mathematics, National Taiwan University, Taipei, Taiwan

Communicated by Richard G. Swan

Received April 27, 1994

We shall use the Binet–Minc formula in the theory of permanents to prove David Richman's theorem: Let G be a finite group acting on $A := R[a_1, \dots, a_r]$, where R is any commutative ring with $1/|G|! \in R$. Then the ring of invariants A^G is generated over R by $\sum_{\sigma \in G} \sigma(a_1^{\alpha_1} a_2^{\alpha_2} \cdots a_r^{\alpha_r})$, where $\alpha_1 + \cdots + \alpha_r \le |G|$. Applications of permanents to other problems related to invariants are given also.

1. INTRODUCTION

Let R be any commutative ring, $A = R[a_1, \dots, a_r]$ a finitely generated R-algebra. (Note that it is unnecessary that $a_1, \dots, a_r$ are indeterminates over R.) Suppose that G is a finite group acting on A by R-automorphisms; i.e., the action of G on A is induced by some group homomorphism from G into $\mathrm{Aut}_R(A)$. Denote by A^G the ring of invariants of A under G,

$$A^G := \{a \in A : \sigma(a) = a \text{ for any } \sigma \in G\}.$$

A classical result of Emmy Noether is the following.

*Partially supported by National Science Council of the Republic of China.
† E-mail: sjhu@mail.tku.edu.tw.
‡ E-mail: kang@math.ntu.edu.tw.

0021-8693/96 $18.00

THEOREM 1.1 (E. Noether [8; 9; 7, Theorem 2, p. 9; 15, 1.2 Theorem]).

(i) *If R is a noetherian ring, then A^G is a finitely generated R-algebra.*

(ii) *If $\mathbb{Q} \subset R$, then A^G is generated over R by all the coefficients in $T_1, \dots, T_r$ of the polynomial*

$$F(T_1, \dots, T_r) = \prod_{\sigma \in G} \{1 + \sigma(a_1)T_1 + \sigma(a_2)T_2 + \cdots + \sigma(a_r)T_r\}. \quad (1)$$

It might be interesting to recall some history of this theorem. What Noether considered was the situation of an arbitrary representation of G, i.e., $G \to GL(V)$, where V is a finite-dimensional vector space over a field K, and $A := K[V]$ the symmetric algebra of V over K. When char $K = 0$, the finite generation of A^G was proved by David Hilbert. A simplified proof of this case, together with result (ii) of the above theorem was provided by Noether in 1916 [8]. The finite generation of A^G when char $K = p > 0$ was solved in 1926 [9].

It is not difficult to see that when char $K = 0$ the set consisting of all coefficients of the polynomial (1) generates the same K-algebra as the set consisting of the traces of all the monomials

$$X_1^{\alpha_1} X_2^{\alpha_2} \cdots X_r^{\alpha_r}, \qquad 0 \le \alpha_1 + \alpha_2 + \cdots + \alpha_r \le |G|,$$

where $X_1, \dots, X_r$ is a base of V over K. In fact, the condition that $1/|G|! \in K$ will suffice to guarantee that these two sets of elements will generate the same subalgebra; moreover, merely the condition that $1/|G| \in K$ is insufficient to guarantee the above fact. (See Theorem 4.3. and Examples 4.4–4.6.) Moreover, both David Richman and Barbara J. Schmid were able to improve Noether's theorem. Namely,

THEOREM 1.2 (Richman [10, Propositions 3 and 5]). (i) *If R is any commutative ring with $1/|G|! \in R$, then A^G is generated over R by the coefficients of the polynomial* (1).

(ii) *If R is any commutative ring with $1/|G| \in R$ and G is a solvable group, then A^G is generated over R by*

$$\sum_{\sigma \in G} \sigma(a_1^{\alpha_1} a_2^{\alpha_2} \cdots a_r^{\alpha_r}), \qquad 0 \le \alpha_1 + \alpha_2 + \cdots + \alpha_r \le |G|.$$

THEOREM 1.3 (Schmid [12; 13, 1.7 Theorem]). *Let R be an algebraically closed field with characteristic zero and let G send "the linear part" $\sum_{i=1}^r Ra_i$ into itself. If G is not a cyclic group, then A^G is generated over R by*

$$\sum_{\sigma \in G} \sigma(a_1^{\alpha_1} a_2^{\alpha_2} \cdots a_r^{\alpha_r}), \qquad 0 \le \alpha_1 + \alpha_2 + \cdots + \alpha_r \le |G| - 1.$$

It seems that Theorem 1.2 has not been published, perhaps due to the tragic death of David Richman in the airplane crash in Los Angeles, 1991. The main purpose of this paper is to provide a new proof of Richman's results. Our approach to prove it is to use the theory of permanents. So far as we know, it seems to be the first case of the application of permanents to invariant theory. Once Theorem 1.2 is established, we may generalize Theorem 1.3 to the situation when R is any commutative ring with $1/|G|! \in R$ and G sends "the linear part" $\sum_{i=1}^{r} R \cdot a_i$ into itself.

Standing Notation. All the rings in this paper are commutative with identity elements. It is not assumed that our rings are noetherian rings. If n is a positive integer, we shall abbreviate the fact that n is invertible in R by quoting that $1/n \in R$. A finitely generated R-algebra A is often denoted by $A = R[a_1, \dots, a_2, \dots, a_r]$; note that $a_1, a_2, \dots, a_r$ need not be indeterminates over R. Indeterminates are designated by $X_1, X_2, \dots, X_r$ or $X(i, j)$. Hence $R[X_1, X_2, \dots, X_r]$ and $R[X(i, j)\colon 1 \le i \le n,\ 1 \le j \le r]$ are polynomial rings over R in r and nr variables, respectively. Abusing the terminology, an element $a_1^{\alpha_1} a_2^{\alpha_2} \cdots a_r^{\alpha_r}$ in $A = R[a_1, \dots, a_r]$ is called a "monomial" of degree $|\alpha| := \alpha_1 + \alpha_2 + \cdots + \alpha_r$. The order of a group G is denoted by $|G|$. The symmetric group of degree n is denoted by S_n.

2. PERMANENTS

DEFINITION 2.1. Let B be any $n \times m$ matrix over a ring, $B = (a_{ij})$, $1 \le i \le n$, $1 \le j \le m$ with $n \ge m$. The permanent of B, $\operatorname{per}(B)$, is defined by

$$\operatorname{per}(B) := \sum_{h} a_{h(1),1} a_{h(2),2} \cdots a_{h(m),m},$$

where h runs over all the injective functions from $\{1, 2, \dots, m\}$ into $\{1, 2, \dots, n\}$.

REMARK. In Minc's monograph [5], a permanent is defined for any $n \times m$ matrix with $n \le m$, instead of $n \ge m$. Moreover, the permanent of a square matrix B is denoted by $\operatorname{per}(B)$ while that of a nonsquare matrix B is denoted by $\operatorname{Per}(B)$ by Minc. Because of our applications we make a modification of Minc's notations.

DEFINITION 2.2. Consider an $n \times m$ matrix B with $n \geq m$,

$$B = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{pmatrix}.$$

Let ω be a partition of m, i.e.,

$$m = \omega_1 + \omega_2 + \cdots + \omega_k,$$

where $1 \leq \omega_1 \leq \omega_2 \leq \cdots \leq \omega_k$ for some positive integer k.

Let $\Lambda(\omega)$ be the set of all permutations ρ in S_m such that ρ is the product of disjoint cycles with lengths $\omega_1, \omega_2, \ldots,$ and ω_k modulo relations of the following type

$$(1\ 2\ 3) \sim (1\ 3\ 2)$$
$$(1\ 2\ 3\ 4) \sim (1\ 3\ 2\ 4) \sim (1\ 2\ 4\ 3) \sim \cdots.$$

For example,

$$\begin{aligned} \Lambda(2,2) &= \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}, \\ \Lambda(1,4) &= \{(1)(2\ 3\ 4\ 5), (2)(1\ 3\ 4\ 5), (3)(1\ 2\ 4\ 5), \\ &\qquad (4)(1\ 2\ 3\ 5), (5)(1\ 2\ 3\ 4)\}. \end{aligned}$$

If ω is the partition

$$m = \omega_1 + \omega_2 + \cdots + \omega_k$$

as above and $\rho \in \Lambda(\omega)$ is the "standard" permutation

$$\begin{aligned} \rho &:= (1\ 2\ 3\ \cdots\ \omega_1)(\omega_1 + 1, \omega_1 + 2, \ldots, \omega_1 + \omega_2) \cdots \\ &\quad (\omega_1 + \omega_2 + \cdots + \omega_{k-1} + 1, \ldots, \omega_1 + \omega_2 + \cdots + \omega_k), \end{aligned}$$

we define $r(\rho)$ by

$$\begin{aligned} r(\rho) &= \left\{ \sum_{i=1}^{n} a_{i1} a_{i2} \cdots a_{i\omega_1} \right\} \left\{ \sum_{i=1}^{n} a_{i,\omega_1+1} \cdots a_{i,\omega_1+\omega_2} \right\} \cdots \\ &\quad \times \left\{ \sum_{i=1}^{n} a_{i,\omega_1+\cdots+\omega_{k-1}+1} \cdots a_{i,m} \right\}. \end{aligned}$$

The reader can imagine how to define $r(\rho)$ for any $\rho \in \Lambda(\omega)$. Note that $r(\rho)$ is denoted in a different way in [5, pp. 119–120].

Define $S(\omega) = S(\omega_1, \omega_2, \dots, \omega_k)$ by

$$S(\omega) = S(\omega_1, \omega_2, \dots, \omega_k) := \sum_{\rho \in \Lambda(\omega)} r(\rho).$$

Finally, we define the coefficient $c(\omega)$ for ω by

$$c(\omega) := (-1)^{m+k} \prod_{i=1}^{k} (\omega_i - 1)!.$$

Now we can state the Binet–Minc formula.

THEOREM 2.3 (Binet-Minc formula [5, Theorem 1.2, pp. 120–121; 6]). *Let B be an $n \times m$ matrix with $n \geq m \geq 2$. Then*

$$\mathrm{per}(B) = \sum_{\omega} c(\omega) S(\omega),$$

where ω runs over all partitions of the integer m.

To illustrate applications of Theorem 2.3, we shall prove some properties of symmetric polynomials. We begin with the following definition first.

DEFINITION 2.4. Let R be any commutative ring and let the symmetric group S_n act on the polynomial ring $R[X_1, \dots, X_n]$ by

$$\sigma(X_i) := X_{\sigma(i)}$$

for any $\sigma \in S_n$ and any $1 \leq i \leq n$. For any positive integers $d_1, d_2, \dots, d_k$ with $1 \leq k \leq n$, $\langle d_1, d_2, \dots, d_k \rangle$ is defined to be the sum of all monomials in the orbit containing $X_1^{d_1} X_2^{d_2} \cdots X_k^{d_k}$. $\langle d_1, d_2, \dots, d_k \rangle$ is called a monomial symmetric polynomial of degree $d := d_1 + \cdots + d_k$.

It is easy to see that $\langle 1, 1, \dots, 1 \rangle$ is the elementary symmetric polynomial, while $\langle d \rangle$ is the symmetric sum of degree d.

THEOREM 2.5 (Mead [4]). *Let $M(1), M(2), \dots, M(n)$ be monomial symmetric polynomials with* $\deg M(1) \leq \deg M(2) \leq \cdots \leq \deg M(n)$. *If* $1/n! \in R$, *then* $R[X_1, \dots, X_n]^{S_n} = R[M(1), M(2), \dots, M(n)]$ *if and only if* $\deg M(i) = i$ *for* $1 \leq i \leq n$.

Proof. Let $f_1 := \langle 1 \rangle$, $f_2 := \langle 1, 1 \rangle, \dots, f_n := \langle 1, \dots, 1 \rangle$ be the elementary symmetric polynomials of degree $1, 2, \dots, n$, respectively.

For the "only if" part, just compare the Hilbert series of $R[M(1), \dots, M(n)]$ and $R[f_1, f_2, \dots, f_n]$, where the Hilbert series of a graded algebra is defined by the same way as in [15, p. 479] with $\dim_k \Lambda_m$ being interpreted as the rank of the grade m part as a free R-module.

If remains to prove the ‘‘if’’ part.

For a monomial symmetric polynomial $\langle d_1, \dots, d_k \rangle$, consider the following matrix:

$$B := \begin{pmatrix} X_1^{d_1} & X_1^{d_2} & \cdots & X_1^{d_k} \\ X_2^{d_1} & X_2^{d_2} & \cdots & X_2^{d_k} \\ \cdots & \cdots & \cdots & \cdots \\ X_n^{d_1} & X_n^{d_2} & \cdots & X_n^{d_k} \end{pmatrix}.$$

We may regard $d_1 + d_2 + \cdots + d_k$ as a partition of $d := d_1 + d_2 + \cdots + d_k$ with k summands and represent it as

$$(1^{e_1} 2^{e_2} \cdots d^{e_d}),$$

where e_i is the number of i appearing in this partition. By Definition 2.1, we find that

$$\operatorname{per}(B) = e_1! \cdots e_d! \langle d_1, \dots, d_k \rangle.$$

On the other hand, we may apply Theorem 2.3 to evaluate $\operatorname{per}(B)$ also. Hence we get

$$e_1! e_2! \cdots e_d! \langle d_1, \dots, d_k \rangle = (-1)^{k+1}(k-1)! \langle d \rangle + \sum_{\omega} c(\omega) S(\omega), \quad (2)$$

where ω in the right-hand side runs over all partitions of k with at least two nonzero summands. Note that $S(\omega) \in R[\langle 1 \rangle, \langle 2 \rangle, \dots, \langle d-1 \rangle]$ for these $S(\omega)$.

Now the proof of the ‘‘if’’ part.

Suppose that $1 \le i \le n-1$ and we have proved that $R[M(1), M(2), \dots, M(i)] = R[\langle 1 \rangle, \langle 2 \rangle, \dots, \langle i \rangle]$. We find that

$$\begin{aligned} R[M(1), \dots, M(i+1)] &= R[\langle 1 \rangle, \dots, \langle i \rangle, M(i+1)] \\ &= R[\langle 1 \rangle, \dots, \langle i+1 \rangle] \end{aligned}$$

because of formula (2) and the assumption that $1/(i+1)! \in R$. Thus we obtain that $R[M(1), M(2), \dots, M(n)] = R[\langle 1 \rangle, \langle 2 \rangle, \dots, \langle n \rangle]$ by induction.

The above argument shows, in particular, that $R[f_1, \dots, f_n] = R[\langle 1 \rangle, \langle 2 \rangle, \dots, \langle n \rangle]$. It follows that

$$\begin{aligned} R[X_1, \dots, X_n]^{S_n} &= R[f_1, \dots, f_n] \\ &= R[\langle 1 \rangle, \langle 2 \rangle, \dots, \langle n \rangle] \\ &= R[M(1), M(2), \dots, M(n)]. \end{aligned}$$

Using formula (2) and similar tricks, it is not difficult to prove the following theorem whose proof is thus omitted. (Note that we may as well deduce Theorem 2.6 from Theorem 2.7.)

THEOREM 2.6. *Let R be any commutative ring for which $n!$ is not invertible. If $f_1, \dots, f_n$ are the elementary symmetric polynomials of degree $1, 2, \dots, n$, respectively, in the polynomial ring $R[X_1, \dots, X_n]$, then $R[\langle 1\rangle, \langle 2\rangle, \dots, \langle n\rangle] \subsetneqq R[f_1, \dots, f_n]$.*

THEOREM 2.7. *Let K be a field, let $K[X_1, \dots, X_n]$ be the polynomial ring over K, and let $f_1, \dots, f_n$ be the elementary symmetric polynomials of degree $1, 2, \dots, n$, respectively, and let $\langle m\rangle := X_1^m + \cdots + X_n^m$ be the symmetric sum of degree m. Then the following four statements are equivalent*:

(1) *$n!$ is invertible in K;*

(2) *$K[\langle m\rangle : m \in \mathbb{N}] = K[X_1, \dots, X_n]^{S_n}$;*

(3) *$K[\langle m\rangle : m \in \mathbb{N}] = K[\langle 1\rangle, \langle 2\rangle, \dots, \langle n\rangle]$;*

(4) *$K[\langle m\rangle : m \in \mathbb{N}]$ is finitely generated over K.*

Proof. It is easy to see that "(1) $\Rightarrow$ (2) $\Rightarrow$ (4)" and "(1) $\Rightarrow$ (3) $\Rightarrow$ (4)."

(4) $\Rightarrow$ (1). If $n!$ is not invertible in K, then $\operatorname{char} K = p > 0$ and $p \le n$. If $K[\langle m\rangle : m \in \mathbb{N}]$ is finitely generated over K, by letting $X_{p+1} = X_{p+2} = \cdots = X_n = 0$, it follows that $K[X_1^m + X_2^m + \cdots + X_p^m : m \in \mathbb{N}]$ is a finitely generated K-subalgebra of $K[X_1, \dots, X_p]$. In other words, we may assume that $\operatorname{char} K = p = n \ge 2$ without loss of generality.

It is clear that $K[\langle m\rangle : 1 \le m \le p] = K[f_1, f_2, \dots, f_{p-1}]$. We claim that, for $1 \le i \le p-1$, for any positive integer l, $K[\langle m\rangle : 1 \le m \le lp + i]$ is generated over K by the following set of generators

$$
\begin{gathered}
f_1, f_2, \dots, f_{p-1}, \\
f_1 f_p, f_1 f_p^2, \dots, f_1 f_p^l, \\
f_2 f_p, f_2 f_p^2, \dots, f_2 f_p^l, \\
\cdots \\
f_i f_p, f_i f_p^2, \dots, f_i f_p^l, \\
f_{i+1} f_p, f_{i+1} f_p^2, \dots, f_{i+1} f_p^{l-1}, \\
\cdots \\
f_{p-1} f_p, f_{p-1} f_p^2, \dots, f_{p-1} f_p^{l-1}.
\end{gathered}
$$

Induction on l and i.

For the case of $\langle lp + i\rangle$, consider the $p \times p$ matrix

$$B := \begin{pmatrix} X_1^{(l-1)p+i+1} & X_1 & X_1 & \cdots & X_1 \\ X_2^{(l-1)p+i+1} & X_2 & X_2 & \cdots & X_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ X_p^{(l-1)p+i+1} & X_p & X_p & \cdots & X_p \end{pmatrix}.$$

Evaluate per(B) by definition and also by Theorem 2.3 as in the proof of Theorem 2.5. Hence we finish the proof of the above claim.

It follows that

$$K[\langle m\rangle : m \in \mathbb{N}] = K\left[f_1, \dots, f_{p-1}, f_i f_p^j : 1 \le i \le p-1, j \in \mathbb{N}\right]$$

is not finitely generated over K, since $f_1, \dots, f_p$ are algebraically independent over K.

2.8 A final remark about permanents. There is another formula of expanding a permanent, the Ryser formula [11, Corollary 4.2, p. 27]. By using the Ryser formula, we may obtain a proof of [13, 1.2 Lemma, p. 38]. A similar argument works for the dth symmetric sum for $1 \le d \le n$, provided that $d!$ is invertible. The verification is left to the reader.

3. THE SYMMETRIC PRODUCTS

Throughout this section, we shall denote by R any commutative ring, and A is defined by

$$A := R[X(i,j) : 1 \le i \le n, 1 \le j \le m],$$

the polynomial ring of nm variables over R.

The symmetric group S_n acts on A by

$$\sigma(X(i,j)) = X(\sigma(i), j)$$
$$\sigma(a) = a$$

for any $\sigma \in S_n$, $a \in R$, $1 \le i \le n$, $1 \le j \le m$.

Similar to the polynomial (1) defined in Theorem 1.1, we define

$$F(T_1, \dots, T_m) = \prod_{1 \le i \le n} \{1 + X(i,1)T_1 + X(i,2)T_2 + \cdots + X(i,m)T_m\}. \tag{3}$$

DEFINITION 3.1. Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_m)$ be an m-tuple of nonnegative integers. Define

$$T^\alpha := T_1^{\alpha_1} T_2^{\alpha_2} \cdots T_m^{\alpha_m},$$
$$|\alpha| := \alpha_1 + \alpha_2 + \cdots + \alpha_m.$$

DEFINITION 3.2. Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_m)$ be an m-tuple of nonnegative integers and let M be a monomial defined by

$$M := X(1,1)^{\alpha_1} X(1,2)^{\alpha_2} \cdots X(1,m)^{\alpha_m};$$

we define the Spur (Spur: the German for "trace") of M, denoted by Sp(M), by

$$\operatorname{Sp}(M) := \sum_{1 \le i \le n} X(i,1)^{\alpha_1} X(i,2)^{\alpha_2} \cdots X(i,m)^{\alpha_m}.$$

DEFINITION 3.3. Let A_1 be the R-subalgebra of A generated by all the coefficients of the polynomial in (3), and let A_2 be the R-subalgebra of A generated by

$$\operatorname{Sp}\left(\prod_{j=1}^{m} X(1,j)^{\alpha_j}\right),$$

where $\alpha := (\alpha_1, \ldots, \alpha_m)$ runs over all m-tuples of nonnegative integers with $|\alpha| \le n$.

The main purpose of this section is to study the relationship among A^{S_n}, A_1, and A_2. When $R \supset \mathbb{Q}$, it is well known that $A^{S_n} = A_1$ [16, pp. 36–39; 1, Exercise 5, pp. A.IV. 98–99]. If we write the polynomial in (3) as

$$F(T_1, \ldots, T_m) = \sum_\alpha b(\alpha) T_1^{\alpha_1} \cdots T_m^{\alpha_m},$$

then it is routine to verify that

$$\operatorname{per}(B(\alpha)) = b(\alpha) \cdot \alpha_1! \alpha_2! \cdots \alpha_m!,$$

where $B(\alpha)$ is the $n \times |\alpha|$ matrix defined by

$$B(\alpha) := \begin{pmatrix} \underbrace{\begin{matrix} X(1,1) \cdots X(1,1) \\ X(2,1) \cdots X(2,1) \\ \cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots \\ X(n,1) \cdots X(n,1) \end{matrix}}_{\alpha_1 \text{ columns}} & \underbrace{\begin{matrix} X(1,2) \cdots X(1,2) \\ X(2,2) \cdots X(2,2) \\ \cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots \\ X(n,2) \cdots X(n,2) \end{matrix}}_{\alpha_2 \text{ columns}} & \begin{matrix} \cdots \\ \cdots \\ \cdots \\ \cdots \\ \cdots \end{matrix} & \underbrace{\begin{matrix} X(1,m) \cdots X(1,m) \\ X(2,m) \cdots X(2,m) \\ \cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots \\ X(n,m) \cdots X(n,m) \end{matrix}}_{\alpha_m \text{ columns}} \end{pmatrix}.$$

LEMMA 3.4. *Let R be any commutative ring.*

(i) *If $1/(n-1)! \in R$, then $A_2 \subset A_1$. On the other hand, if $1/n! \in R$, then $A_1 = A_2$.*

(ii) *Assume that $1/(n-1)! \in R$. Then the R-subalgebra of A generated by all the coefficients of $T_1^{\alpha_1} \cdots T_m^{\alpha_m}$ in the polynomial* (3), *where $T_1^{\alpha_1} \cdots T_m^{\alpha_m}$ runs over all square-free monomials* (*i.e.*, $\alpha_j = 0$ *or* 1) *equals that generated by*

$$\operatorname{Sp}(X(1,i_1)X(1,i_2)\cdots X(1,i_k)),$$

where $1 \le i_1 < i_2 < \cdots < i_k \le m$ runs over all k-subsets of $\{1,2,\dots,m\}$ with $1 \le k \le n$.

Proof. (i) Assume that $n!$ is invertible in R. Evaluate $\operatorname{per}(B(\alpha))$ by Theorem 2.3, where $B(\alpha)$ is the matrix defined in Definition 3.3. Note that $\alpha_1!\alpha_2!\cdots\alpha_m!$ is invertible in R because so is $n!$. Thus we find that $A_1 \subset A_2$.

Suppose that $(n-1)!$ is invertible in R. To prove that $A_2 \subset A_1$, we shall show that

$$\operatorname{Sp}\left(\prod_{j=1}^{m} X(1,j)^{\alpha_j}\right) \in A_1$$

by induction on $|\alpha|$.

When $|\alpha| = 1$, $\operatorname{Sp}(X(1,j))$ is simply the coefficient of T_j in (3).

In general, let $\alpha = (\alpha_1,\dots,\alpha_m)$ with $|\alpha| \le n$. Consider the matrix $B(\alpha)$ in Definition 3.3 again. Thanks to Theorem 2.3, we have

$$b(\alpha)\alpha_1!\cdots\alpha_m! = (-1)^{|\alpha|+1}(|\alpha|-1)!\operatorname{Sp}\left(\prod_{j=1}^{m} X(1,j)^{\alpha_j}\right) + \sum_{\omega} c(\omega)S(\omega),$$

where ω in the right-hand side runs over all partitions of $|\alpha|$ with at least two nonzero summands. By induction hypothesis, these $S(\omega)$ are in A_1. Hence $\operatorname{Sp}(\prod_{j=1}^{m} X(1,j)^{\alpha_j})$ is in A_1 also because $(|\alpha|-1)!$ is invertible in R.

(ii) The proof is almost the same and is omitted.

EXAMPLE 3.5. If K is a field with $\operatorname{char} K = p > 0$, and S_p acts on $K[X_1,\dots,X_p]$ in the usual way, then the proof of Theorem 2.7 shows that $X_1X_2\cdots X_p \notin K[\sum_{i=1}^{p} X_i^m : m \in \mathbb{N}]$. This provides an example with $A_1 \not\subset A_2$ and $p! = 0$.

On the other hand, if K is a field with $\operatorname{char} K = 3$ and $m = 2$, $n \geq 4$, then $A_2 \not\subset A_1$, because $\operatorname{Sp}(X(1,1)^2 X(1,2)^2) \notin K[M(i,j) : 0 \leq i, j \leq n$ and $1 \leq i + j \leq n]$ by [1, Exercise 5(d), p. A.IV. 99], where $M(i,j)$ is the sum of all monomials in the orbit containing $\{\prod_{1 \leq \lambda \leq i} X(\lambda, 1)\}\{\prod_{1 \leq \rho \leq j} X(i + \rho, 2)\}$. Note that, for each $M(i,j)$, there is a $c(i,j) \in \mathbf{Z}$ such that $c(i,j)M(i,j)$ is the coefficient of $T_1^i T_2^j$ in the polynomial of (3) with $m = 2$. ($c(i,j)$ may become zero in the commutative ring R.)

EXAMPLE 3.6. For any positive integers n and m with $n \geq m \geq 3$, if $\operatorname{char} R = m - 1$, then $A_2 \not\subset A_1$. Moreover, both A_1 and A_2 are not equal to A^{S_n}. The proof will be given in 4.7.

THEOREM 3.7 (Richman [10, Proposition 2]). *If R is any commutative ring with $1/n! \in R$, then $A^{S_n} = A_1 = A_2$.*

Proof. By Part (i) of Lemma 3.4, it suffices to show that $f \in A_2$ for any $f \in A^{S_n}$.

STEP 1. Without loss of generality, we may assume that f is a homogeneous polynomial. Write

$$f = \sum_k c_k N_k,$$

where $c_k \in R$ and N_k is a monomial in $X(i,j)$, $1 \leq i \leq n$, $1 \leq j \leq m$. Since

$$f = \frac{1}{n!} \sum_{\sigma \in S_n} \sigma(f) = \frac{1}{n!} \sum_k c_k \sum_{\sigma \in S_n} \sigma(N_k),$$

we may as well assume that f is of the form

$$\sum_{\sigma \in S_n} \sigma(N),$$

where N is a monomial in $X(i,j)$.

STEP 2. We shall prove that $f := \sum_{\sigma \in S_n} \sigma(N)$ belongs to $R[\operatorname{Sp}(\prod_{j=1}^m X(1,j)^{\alpha_j}) : \alpha$ is any m-tuple of nonnegative integers]. Write

$$N = N_1 N_2 \cdots N_n,$$

where

$$N_i = \prod_{j=1}^m X(i,j)^{\beta_{ij}} \qquad \text{for } 1 \leq i \leq n.$$

Define $M_1, M_2, \ldots, M_n$ by

$$M_i := \prod_{j=1}^{m} X(1, j)^{\beta_{ij}} \qquad \text{for } 1 \le i \le n.$$

Let H be the subgroup of S_n defined by

$$H := \{\sigma \in S_n : \sigma(1) = 1\}.$$

Define $\sigma_1 = \mathrm{id}, \sigma_2, \ldots, \sigma_n$ by

$$\sigma_i = (1 \;\; i) \qquad \text{for } 2 \le i \le n.$$

Consider the square matrix B defined by

$$B := \begin{pmatrix} \sigma_1(M_1) & \sigma_1(M_2) & \cdots & \sigma_1(M_n) \\ \sigma_2(M_1) & \sigma_2(M_2) & \cdots & \sigma_2(M_n) \\ \cdots & \cdots & \cdots & \cdots \\ \sigma_n(M_1) & \sigma_n(M_2) & \cdots & \sigma_n(M_n) \end{pmatrix}.$$

Hence we find that

$$\begin{aligned} \sum_{\sigma \in S_n} \sigma(N) &= \sum_{\sigma \in S_n} \sigma\left(\sigma_1(M_1)\sigma_2(M_2) \cdots \sigma_n(M_n)\right) \\ &= \sum_{\sigma \in S_n} \prod_{i=1}^{n} \sigma\sigma_i(M_i) \\ &= \sum_{h} \sigma_{h(1)}(M_1)\sigma_{h(2)}(M_2) \cdots \sigma_{h(n)}(M_n), \end{aligned}$$

where h runs over all the injective functions from $\{1, 2, \ldots, n\}$ into itself. But the last expression is just $\mathrm{per}(B)$!

By Theorem 2.3, $\mathrm{per}(B) = \sum c(\omega) S(\omega)$. Clearly each $S(\omega)$ belongs to the subalgebra defined before. Hence the result.

STEP 3. Because of Step 2, it suffices to show that $\mathrm{Sp}(\prod_{j=1}^{m} X(1, j)^{\alpha_j}) \in A_2$, where $\alpha := (\alpha_1, \ldots, \alpha_m)$ is any m-tuple of nonnegative integers.

If $|\alpha| \le n$, there is nothing to prove. Hence we may assume that $|\alpha| \ge n + 1$. We shall prove by induction on $|\alpha|$.

Let $\tilde{A} := R[Y(i, k) : 1 \le i \le n, 1 \le k \le n + 1]$ be the polynomial ring of $n(n + 1)$ variables over R. Define an R-algebra homomorphism Φ: $\tilde{A} \to A$ satisfying the following conditions:

(a) for $1 \leq k \leq n+1$, $\Phi(Y(1,k))$ is a monomial, $\Phi(Y(1,k)) \neq 1$, and

$$\prod_{k=1}^{n+1} \Phi(Y(1,k)) = \prod_{j=1}^{m} X(1,j)^{\alpha_j};$$

(b) for $2 \leq i \leq n$, $1 \leq k \leq n+1$, $\Phi(Y(i,k))$ is defined by

$$\Phi(Y(i,k)) \coloneqq \sigma_i(\Phi(Y(1,k)))$$

where $\sigma_i \coloneqq (1\ \ i) \in S_n$.

It follows that

$$\mathrm{Sp}\left(\sum_{j=1}^{m} X(1,j)^{\alpha_j}\right) = \Phi\left(\mathrm{Sp}\left(\sum_{k=1}^{n+1} Y(1,k)\right)\right). \tag{4}$$

Consider the following $(n+1) \times (n+1)$ matrix:

$$C \coloneqq \begin{pmatrix} Y(1,1) & Y(1,2) & \cdots & Y(1,n+1) \\ Y(2,1) & Y(2,2) & \cdots & Y(2,n+1) \\ \cdots & \cdots & \cdots & \cdots \\ Y(n,1) & Y(n,2) & \cdots & Y(n,n+1) \\ 1 & 1 & \cdots & 1 \end{pmatrix}.$$

By definition, $\mathrm{per}(C)$ is the sum of coefficients of all square-free monomials of degree n of the following polynomial:

$$\prod_{i=1}^{n} \{1 + Y(i,1)T_1 + Y(i,2)T_2 + \cdots + Y(i,n+1)T_{n+1}\},$$

i.e., $m = n+1$ in (3). By Part (ii) of Lemma 3.4. These coefficients lie in the R-subalgebra generated by

$$\mathrm{Sp}(Y(1,i_1)Y(1,i_2)\cdots Y(1,i_k)),$$

where $1 \leq i_1 < i_2 < \cdots < i_k \leq n+1$ runs over all k-subsets of $\{1, 2, \ldots, n+1\}$ with $1 \leq k \leq n$. The images under Φ of these $\mathrm{Sp}(Y(1,i_1)Y(1,i_2)\cdots Y(1,i_k))$ is of the form $\mathrm{Sp}(\prod_{j=1}^{m} X(1,j)^{\beta_j})$ with $|\beta| < |\alpha|$ because of condition (a) in our construction of Φ. Thus these images are in A_2 by the induction hypothesis. It follows that $\Phi(\mathrm{per}(C)) \in A_2$ also.

On the other hand, applying Theorem 2.3 to evaluate $\mathrm{per}(C)$, we get

$$\mathrm{per}(C) = (-1)^n n!\left(\mathrm{Sp}\left(\prod_{k=1}^{n+1} Y(1,k)\right) + 1\right) + \sum_{\omega} c(\omega)S(\omega),$$

where ω in the right-hand side runs over all partitions of $n+1$ with at least two nonzero summands. Again by the induction hypothesis, $\Phi(S(\omega)) \in A_2$.

It follows from (4) that $\mathrm{Sp}(\prod_{j=1}^m X(1,j)^{\alpha_j}) \in A_2$.

REMARK. The Molien series of A^{S_n} when R is a field with char $R = 0$ is discussed in [15, 5.3 Example, pp. 492–493]. When R is a field, the quotient field of A^{S_n} is purely transcendental over R [3, Example 1]. The following example provides a transcendental basis with a peculiar property.

EXAMPLE 3.8. Let K be any field, $A := K[X(i,j): 1 \le i \le n,\ 1 \le j \le m]$ with $m \ge 2$. Define $f_{1,1}, \dots, f_{n,1}$ to be the elementary symmetric polynomials of degree $1, 2, \dots, n$ respectively in $K[X(i,1): 1 \le i \le n]$. For $1 \le i \le n$, $2 \le j \le m$, define $f_{i,j}$ to be the sum of monomials of the orbit of S_n containing $X(1,1)X(2,1) \cdots X(i-1,1)X(i,j)$.

We claim that

(a) A^{S_n} and $K(f_{i,j}: 1 \le i \le n, 1 \le j \le m)$ have the same quotient field, and

(b) A^{S_n} is not finitely generated as a module over $B := K[f_{ij}: 1 \le i \le n, 1 \le j \le m]$.

Since $K(f_{ij}: 1 \le i \le n,\ 1 \le j \le m)(X(i,1): 1 \le i \le n) = K(X(i,j): 1 \le i \le n,\ 1 \le j \le m)$, it follows that the vector space degree of $K(X(i,j): 1 \le i \le n,\ 1 \le j \le m)$ over $K(f_{ij}: 1 \le i \le n,\ 1 \le j \le m)$ is $\le n!$. Hence (a) is established.

As for (b), since B is a polynomial ring because of (a), B is integrally closed. If A^{S_n} were a finitely generated B-module, then A^{S_n} would be finite over B and therefore $A^{S_n} = B$. It follows that A^{S_n} is a polynomial ring. However, since $m \ge 2$, the action of S_n on $\oplus_{i,j} K \cdot X(i,j)$ is not a pseudo-reflection group; thus A^{S_n} is never a polynomial ring by [14].

EXAMPLE 3.9. Let K be a field of char $K = p > 0$, let m and n be any positive integers with $n \ge p$, and let $A := K[X(i,j): 1 \le i \le n,\ 1 \le j \le m]$. Let A_3 be the K-subalgebra of A generated by

$$\mathrm{Sp}\big(X(1,1)^{\alpha_1} X(1,2)^{\alpha_2} \cdots X(1,m)^{\alpha_m}\big),$$

where $\alpha := (\alpha_1, \dots, \alpha_m)$ runs over all m-tuples of nonnegative integers (without restriction on $|\alpha|$).

Then A_3 is not finitely generated over K and $A_3 \ne A^{S_n}$. (Reason: When $m = 1$ and $n = p$, use Theorem 2.7. The general case may be reduced to this special case by letting $X(i,j) = 1$ for any $p+1 \le i \le n$ and $2 \le j \le m$.)

When R is any commutative ring, a generating system of $R[X(i,j): 1 \le i \le n,\ 1 \le j \le m]^{S_n}$ is listed in [2; 10, Proposition 7]. It is not surprising that this set is very big.

4. FINITE GROUP ACTIONS

In this section, we shall denote by R any commutative ring, by $A = R[a_1, \dots, a_r]$ a finitely generated R-algebra, and by G a finite group acting on A by R-automorphisms. The reader should not be confused with the same notations A, A_1, A_2 in this section and the preceding section.

DEFINITION 4.1. Let A_1 be the R-subalgebra of A generated by all the coefficients of the polynomial

$$F(T_1, \dots, T_r) = \prod_{\sigma \in G} \{1 + \sigma(a_1)T_1 + \sigma(a_2)T_2 + \cdots + \sigma(a_r)T_r\}. \quad (5)$$

Let A_2 be the R-subalgebra of A generated by

$$\sum_{\sigma \in G} \sigma\left(a_1^{\alpha_1} a_2^{\alpha_2} \cdots a_r^{\alpha_r}\right),$$

where $\alpha := (\alpha_1, \dots, \alpha_r)$ runs over all r-tuples of nonnegative integers with $|\alpha| \le |G|$.

LEMMA 4.2. *Suppose that G sends "the linear part" $\sum_{i=1}^r R \cdot a_i$ into itself, i.e. $\sigma(a_i) \in \sum_{1 \le j \le r} Ra_j$ for any $\sigma \in G$, any $1 \le i \le r$. If $1/|G| \in R$, then $A_1 \subset A_2$.*

REMARK. The condition $\sigma(a_i) \in \sum_{1 \le j \le r} Ra_j$ is not a very restricted condition in practical computation, because we may extend the generators $a_1, \dots, a_r$ to include $\sigma(a_i)$ for all $\sigma \in G$, $1 \le i \le r$.

Proof. Let b be any coefficient of the polynomial in (5). By the assumption, b can be written as

$$b = \sum_{|\alpha| = l} c_\alpha \prod_{i,j} \sigma_i(a_j)^{\alpha_{ij}} = \sum_{|\beta| = l} c'_\beta a_1^{\beta_1} \cdots a_r^{\beta_r},$$

where $c_\alpha, c'_\beta \in R$ and l is an integer with $0 \le l \le |G|$. Then

$$b = \frac{1}{|G|} \sum_{\sigma \in G} \sigma(b) = \frac{1}{|G|} \sum_{|\beta| = l} c'_\beta \sum_{\sigma \in G} \sigma\left(a_1^{\beta_1} \cdots a_r^{\beta_r}\right) \in A_2.$$

THEOREM 4.3 (Richman [10, Proposition 3]). *Suppose that $1/|G|! \in R$. Then $A^G = A_1 = A_2$.*

Proof. Let $|G| = n$ and $G = \{\sigma_1, \sigma_2, \dots, \sigma_n\}$.
If $f \in A^G$, we shall prove that $f \in A_1 \cap A_2$.

Write f as

$$f = \sum c_\beta a_1^{\beta_1} a_2^{\beta_2} \cdots a_r^{\beta_r},$$

where $c_\beta \in R$. Then

$$f = \frac{1}{n} \sum_{i=1}^{n} \sigma_i(f) = \frac{1}{n} \sum_{\beta} c_\beta \sum_{i=1}^{n} \sigma_i\left(a_1^{\beta_1} \cdots a_r^{\beta_r}\right).$$

Hence we may assume that f is of the form

$$\sum_{i=1}^{n} \sigma_i\left(a_1^{\beta_1} \cdots a_r^{\beta_r}\right)$$

for some $\beta = (\beta_1, \dots, \beta_r)$.

Define $\tilde{A} := R[X(i,j) : 1 \le i \le n,\ 1 \le j \le r]$, the polynomial ring of nr variables over R. Define an R-algebra homomorphism $\Phi\colon \tilde{A} \to A$ by $\Phi(X(i,j)) = \sigma_i(a_j)$ for $1 \le i \le n$, $1 \le j \le r$. Define $\tilde{f} \in \tilde{A}$ by

$$\tilde{f} := \sum_{i=1}^{n} X(i,1)^{\beta_1} X(i,2)^{\beta_2} \cdots X(i,r)^{\beta_r}.$$

It follows that $\Phi(\mathrm{Sp}(X(1,1)^{\beta_1} \cdots X(1,r)^{\beta_r})) = \Phi(\tilde{f}) = f$.

Since $1/n! \in R$, we may apply Theorem 3.7. It follows that $\mathrm{Sp}(X(1,1)^{\beta_1} \cdots X(1,r)^{\beta_r}) \in \tilde{A}^{S_n} = \tilde{A}_1 = \tilde{A}_2$, where $\tilde{A}_1$ is the R-subalgebra of $\tilde{A}$ generated by the coefficients of the polynomial

$$\prod_{i=1}^{n} \{1 + X(i,1)T_1 + X(i,2)T_2 + \cdots + X(i,r)T_r\},$$

and $\tilde{A}_2$ is the R-subalgebra of $\tilde{A}$ generated by

$$\mathrm{Sp}\left(X(1,1)^{\alpha_1} X(1,2)^{\alpha_2} \cdots X(1,r)^{\alpha_r}\right),$$

where α runs over all r-tuples of nonnegative integers with $|\alpha| \le n$.

Since $\Phi(\tilde{A}_1) = A_1$ and $\Phi(\tilde{A}_2) = A_2$, it follows that $f \in A_1 \cap A_2$.

Example 4.4. Let K be a field of characteristic 2 containing a primitive seventh root of unity ζ. Define a K-automorphism $\sigma : A = K[X_1, X_2, X_3] \to K[X_1, X_2, X_3]$ by $\sigma(X_1) = \zeta X_1$, $\sigma(X_2) = \zeta^2 X_2$, $\sigma(X_3) = \zeta^4 X_3$. Then the nonzero coefficients of the polynomial

$$F(T) = \prod_{i=0}^{6} \left\{1 + \sigma^i(X_1)T_1 + \sigma^i(X_2)T_2 + \sigma^i(X_3)T_3\right\}$$

are of degrees 4, 6, or 7 in X_1, X_2, X_3. In particular, $X_1X_2X_3 \in A_2$, but $X_1X_2X_3 \notin A_1$. Note that $\frac{1}{7} \in K$, but $7! = 0$ in K.

EXAMPLE 4.5. Let n and m be any integers with $n \geq m \geq 3$ and g.c.d. $\{n, m-1\} = 1$. Let R be any commutative ring of characteristic $m-1$ containing a primitive nth root of unity ζ, and $A \coloneqq R[X_1, \dots, X_m]$ the polynomial ring of m variables over R.

Define an R-automorphism σ on A by $\sigma(X_i) = \zeta X_i$ for $1 \leq i \leq m-1$ and $\sigma(X_m) = \zeta^{n-m+1}X_m$. Then it is routine to verify that

(a) $X_1X_2 \cdots X_m \in A^{\langle\sigma\rangle}$, and

(b) Any square-free monomial $\neq 1$ or $X_1X_2 \cdots X_m$ is not in $A^{\langle\sigma\rangle}$.

Consider

$$F(T) \coloneqq \prod_{i=0}^{n-1} \left\{1 + \sigma^i(X_1)T_1 + \sigma^i(X_2)T_2 + \cdots + \sigma^i(X_m)T_m\right\}.$$

The coefficient of $T_1^{\alpha_1}T_2^{\alpha_2} \cdots T_m^{\alpha_m}$ in $F(T)$ is $X_1^{\alpha_1}X_2^{\alpha_2} \cdots X_m^{\alpha_m}$ multiplied by some element in R. By (b), all the coefficients of nontrivial square-free monomials $\neq T_1T_2 \cdots T_m$ are zero. On the other hand, the coefficient of $T_1T_2 \cdots T_m$ is per(B) where B is the following matrix:

$$B \coloneqq \begin{pmatrix} X_1 & X_2 & \cdots & X_{m-1} & X_m \\ \zeta X_1 & \zeta X_2 & \cdots & \zeta X_{m-1} & \zeta^{n-m+1}X_m \\ \zeta^2 X_1 & \zeta^2 X_2 & \cdots & \zeta^2 X_{m-1} & \zeta^{2(n-m+1)}X_m \\ \vdots & \vdots & & \vdots & \vdots \\ \zeta^{n-1}X_1 & \zeta^{n-1}X_2 & \cdots & \zeta^{n-1}X_{m-1} & \zeta^{(n-1)(n-m+1)}X_m \end{pmatrix}.$$

Apply Theorem 2.3 to evaluate per(B).

Let ω_0 be the partition of m consisting of one summand only. Then $c(\omega_0) = (-1)^{m+1}(m-1)! = 0$.

If ω is any partition of m other than ω_0, then $r(\rho) = 0$ for any $\rho \in \Lambda(\omega)$ because $1 + \zeta^i + \zeta^{2i} + \cdots + \zeta^{(n-1)i} = 0$ for any $\zeta^i \neq 1$.

Therefore, per$(B) = 0$.

We conclude that no nontrivial square-free monomial in $X_1, \dots, X_m$ will be a nonzero coefficient of $F(T)$. Hence $X_1X_2 \cdots X_m$ does not belong to A_1, the subalgebra generated by all the coefficients of $F(T)$, while $X_1X_2 \cdots X_m \in A_2$.

EXAMPLE 4.6. Let n, m, R be the same as in Example 4.5. For any positive integer r, let

$$A \coloneqq R[X(i,j) : 1 \leq i \leq m, 1 \leq j \leq r]$$

the polynomial ring of rm variables over R. Let $G = \langle \sigma_1 \rangle \times \langle \sigma_2 \rangle \times \cdots \times \langle \sigma_r \rangle$ be the abelian group of order rn, where each σ_j is defined by

$$\begin{aligned} \sigma_j(X(i,k)) &= X(i,k), && \text{if } k \neq j; \\ \sigma_j(X(i,j)) &= \zeta X(i,j), && \text{if } 1 \leq i \leq m-1; \\ \sigma_j(X(m,j)) &= \zeta^{n-m+1} X(m,j). \end{aligned}$$

Define

$$F(T) := \prod_{\tau \in G} \left\{ 1 + \sum_{i,j} \tau(X(i,j)) T(i,j) \right\}.$$

Consider

$$\begin{aligned} G(S_0, S_1, \dots, S_m) := \prod_{k=0}^{n-1} \{ S_0 + \sigma_1^k(X(1,1)) S_1 + \sigma_1^k(X(2,1)) S_2 \\ + \cdots + \sigma_1^k(X(m,1)) S_m \}. \end{aligned}$$

Define

$$H(T) := G\left(1 + \sum_{\substack{1 \leq i \leq m \\ 2 \leq j \leq r}} X(i,j) T(i,j), T(1,1), T(2,1), \dots, T(m,1) \right).$$

By Example 4.5, regarding $H(T)$ as a polynomial in $T(i,1)$, where $1 \leq i \leq m$, all the nontrivial square-free monomials in $H(T)$ will have zero coefficients.

It is not difficult to check that

$$\begin{aligned} F(T) &= \prod_{r \in \langle \sigma_2 \rangle \times \cdots \times \langle \sigma_r \rangle} \tau(H(T)) \\ &= \prod_{\tau \in \langle \sigma_2 \rangle \times \cdots \times \langle \sigma_r \rangle} G\left(1 + \sum_{\substack{1 \leq i \leq m \\ 2 \leq j \leq r}} \tau(X(i,j)) T(i,j), T(1,1), \right. \\ &\qquad \left. T(2,1), \dots, T(m,1) \right). \end{aligned}$$

Thus all the nontrivial square-free monomials in $F(T)$, regarding $F(T)$ as a polynomial in $T(i,1)$, where $1 \leq i \leq m$, will have zero coefficients.

It follows that $T(1,1)T(2,1)\cdots T(m,1)$ does not belong to A_1, the subalgebra generated by all the coefficients of $F(T)$, while it is in A_2!

4.7. *Proof of Example* 3.6. Recall the definitions of A_1 and A_2 in Definition 3.3. We shall prove $A_2 \not\subset A_1$. Consider the case $n = m$ first.

Since char $R = m - 1 = n - 1$, we may adjoin a primitive nth root of unity ζ, to R if $\zeta \notin R$. Let σ be the $R[\zeta]$-automorphism of $R[\zeta][X_1, \dots, X_m]$ in Example 4.5 with $n = m$.

Define an R-algebra homomorphism Φ by

$$\Phi : A \to R[\zeta][X_1, \dots, X_m]$$
$$X(i,j) \mapsto \sigma^i(X_j)$$

for $1 \le i, j \le m = n$. Note that $X_1 X_2 \cdots X_m = nX_1 X_2 \cdots X_m = \Phi(\mathrm{Sp}(X(1,1)X(1,2)\cdots X(1,m)))$.

If $A_2 \subset A_1$, then $\mathrm{Sp}(X(1,1)\cdots X(1,m)) \in A_2 \subset A_1$. Hence $X_1 X_2 \cdots X_m = \Phi(\mathrm{Sp}(X(1,1)\cdots X(1,m)))$ can be expressed in terms of elements of $\Phi(A_1)$. However, $\Phi(A_1)$ is generated over R by the coefficients of the polynomial

$$\Phi\left(\prod_{i=0}^{n-1}\{1 + X(i,1)T_1 + \cdots + X(i,m)T_m\}\right)$$
$$= \prod_{i=0}^{n-1}\left\{1 + \sigma^i(X_1)T_1 + \cdots + \sigma^i(X_m)T_m\right\}.$$

Thus we find a contradiction with Example 4.5.

The case when $n > m$ may be reduced to the case $n = m$ by letting $X(i,j) = 1$ for all (i,j) with $m + 1 \le i \le n$ and $1 \le j \le m$.

It remains to show that $A_2 \ne A^{S_n}$.

By Theorem 2.6, find $f \in R[X(i,1) : 1 \le i \le n]^{S_n}$, but $f \notin R[\mathrm{Sp}(X(1,1)), \mathrm{Sp}(X(1,1)^2), \dots, \mathrm{Sp}(X(1,1)^n)]$.

If $f \in A_2$, by letting $X(i,j) = 1$ for all (i,j) with $1 \le i \le n$ and $2 \le j \le m$, we find a contradiction. Thus $f \notin A_2$.

THEOREM 4.8 (Richman [10, Proposition 5]). *Suppose that G sends "the linear part" $\sum_{i=1}^r R \cdot a_i$ into itself. If $1/|G| \in R$ and G is a solvable group, then $A^G = A_2$.*

Proof. *Step* 1. By induction on $|G|$, it suffices to prove the theorem for the case $G = \langle \sigma \rangle$ is a cyclic group of prime order p, because G is solvable.

Step 2. We shall lift the action of $G = \langle \sigma \rangle$ to a direct sum of regular representations. Define $\tilde{A} = R[X(i,j) : 1 \le i \le p,\ 1 \le j \le r]$ and define an R-algebra homomorphism Φ: $\tilde{A} \to A$ by $\Phi(X(i,j)) = \sigma^i(a_j)$. The action of G on A can be lifted to $\tilde{A}$ by defining $\sigma^k(X(i,j)) = X(i+k,j)$, where $i+k$ is taken modulo p.

Since $1/p \in R$, it follows that $A^{\langle\sigma\rangle} = \Phi(\tilde{A}^{\langle\sigma\rangle})$. Moreover, Φ sends "the linear part" of $\tilde{A}$ into that of A. Hence it suffices to prove the theorem for the case of $\tilde{A}$.

Step 3. Assume that R contains a primitive pth root of unity ζ. Since $1/p \in R$ and σ permutes the variables $X(i,j)$, the action of σ on $\sum_{i,j} R \cdot X(i,j)$ can be diagonalized (by taking $\sum_{i=1}^{p} \zeta^{ik} X(i,j)$, $0 \le k \le p-1$, $1 \le j \le r$). Thus, there exist $Y_1, \dots, Y_{rp}$ such that $\tilde{A} = R[X(i,j): 1 \le i \le p, 1 \le j \le r] = R[Y_1, \dots, Y_{rp}]$ with $\sigma(Y_l) = \zeta^{\lambda_l} Y_l$ for all $1 \le l \le rp$. By [13, Section 2], $R[Y_1, \dots, Y_{rp}]^{\langle\sigma\rangle}$ is generated over R by $Y_1^{\alpha_1} \cdots Y_{rp}^{\alpha_{rp}}$, where $\alpha_1 + \alpha_2 + \cdots + \alpha_{rp} \le p$ and $\lambda_1\alpha_1 + \cdots + \lambda_{rp}\alpha_{rp} = 0 \pmod p$. Since each Y_l is a linear combination of $X(i,j)$, it follows that these $Y_1^{\alpha_1} \cdots Y_{rp}^{\alpha_{rp}}$ can be expressed in terms of $\sum_{k=0}^{p-1} \sigma^k(\prod_{i,j} X(i,j)^{\beta_{ij}})$, where $\sum_{i,j} \beta_{ij} \le p$.

Step 4. Assume that R does not contain a primitive pth root of unity. Consider $R[T]/\Phi_p(T)$, where $\Phi_p(T)$ is a pth cyclotomic polynomial. We shall write $R[T]/\Phi_p(T) = R[\zeta]$, where ζ is the image of T in $R[T]/\Phi_p(T)$. Note that $R[\zeta]$ is a free R-module with basis $\{1, \zeta, \dots, \zeta^{p-1}\}$.

If $f \in \tilde{A}^{S_n}$, by Step 3 we may write

$$f = \sum_{\alpha} c_\alpha M_\alpha,$$

where $c_\alpha \in R[\zeta]$ and M_α is of the form $\sum_{i=0}^{p-1} \sigma^i(\Pi_{i,j} X(i,j)^{\alpha_{ij}})$ with $\sum_{i,j} \alpha_{ij} \le p$.

Write $c_\alpha = \sum_{i=0}^{p-1} c_{\alpha l} \zeta^l$ with $c_{\alpha l} \in R$. It follows that $f = \sum_\alpha c_{\alpha o} M_\alpha$ as desired.

THEOREM 4.9. *Let R be any commutative ring, $A := R[a_1, \dots, a_r]$ a finitely generated R-algebra, G a finite group acting on A by R-automorphisms. Suppose that H is a subgroup of G such that*

(a) *$G = \bigcup_{i=1}^{n} \sigma_i H$ is a coset decomposition, and*

(b) *$A^H = R[b_1, b_2, \dots, b_m]$.*

Assume that either of the following conditions is valid:

(i) $1/n! \in R$, *or*

(ii) $1/n \in R$, *H is normal in G, G/H is a solvable group, and G/H sends "the linear part" $\sum_{j=1}^{m} R \cdot b_j$ into itself.*

Then A^G is generated as an R-algebra by the elements

$$\sum_{i=1}^{n} \sigma_i\left(b_1^{\alpha_1} b_2^{\alpha_2} \cdots b_m^{\alpha_m}\right),$$

where $\alpha = (\alpha_1, \dots, \alpha_m)$ *runs over all* m*-tuples of nonnegative integers with* $|\alpha| \le n$.

Proof. In general there is no guarantee that $\sigma_i(b_j)$ should belong to A^H, except for the case H being normal in G.

Assume that Condition (ii) is valid. Then G/H acts on A^H and $A^G = (A^H)^{G/H}$. Apply Theorem 4.8.

Now we assume that Condition (i) is valid.

Consider $\tilde{A}$, the polynomial ring of nm variables over R, defined by

$$\tilde{A} := R[X(i,j) : 1 \le i \le n, 1 \le j \le m].$$

Define an R-algebra homomorphism Φ: $\tilde{A} \to A$ by $\Phi(X(i,j)) = \sigma_i(b_j)$. Suppose that $f \in A^G$. Since $A^G \subset A^H$, we may write

$$f = \sum_\alpha r_\alpha b^\alpha,$$

where $b^\alpha = b_1^{\alpha_1} b_2^{\alpha_2} \cdots b_m^{\alpha_m}$. Define $\tilde{f} \in \tilde{A}$ by

$$\tilde{f} = \frac{1}{n} \sum_\alpha r_\alpha \sum_{i=1}^n X(i,1)^{\alpha_1} X(i,2)^{\alpha_2} \cdots X(i,m)^{\alpha_m}.$$

It follows that

$$\begin{aligned}
\Phi(\tilde{f}) &= \frac{1}{n} \sum_\alpha r_\alpha \sum_{i=1}^n \sigma_i\left(b_1^{\alpha_1} b_2^{\alpha_2} \cdots b_m^{\alpha_m}\right) \\
&= \frac{1}{n} \sum_{i=1}^n \sigma_i\left(\sum_\alpha r_\alpha b^\alpha\right) \\
&= \frac{1}{n} \sum_{i=1}^n \sigma_i(f) \\
&= f.
\end{aligned}$$

Note that $\tilde{f}$ is nothing but

$$\frac{1}{n} \sum_\alpha r_\alpha \operatorname{Sp}\left(X(1,1)^{\alpha_1} X(1,2)^{\alpha_2} \cdots X(1,m)^{\alpha_m}\right).$$

By Theorem 3.7, $\tilde{f}$ can be expressed in terms of

$$\operatorname{Sp}\left(\prod_{j=1}^m X(1,j)^{\alpha_j}\right) = \sum_{i=1}^n \prod_{j=1}^m X(i,j)^{\alpha_j}, \qquad \text{where } |\alpha| \le n.$$

Hence $f = \Phi(\tilde{f})$ is of the desired form.

THEOREM 4.10. *Let R be any commutative ring, let $A := R[a_1, \ldots, a_r]$ be a finitely generated R-algebra, and let G be a finite group acting on A by R-automorphisms. Assume that G sends "the linear part" $\sum_{i=1}^{r} R \cdot a_i$ into itself and that either of the following conditions is valid*:

(i) $1/|G|! \in R$ *and G is not a cyclic group*; *or*

(ii) $1/|G| \in R$ *and G is a solvable group but not a cyclic group.*

Then A^G is generated as an R-algebra by the elements

$$\sum_{\sigma \in G} \sigma\left(a_1^{\alpha_1} a_2^{\alpha_2} \cdots a_r^{\alpha_r}\right),$$

where $\alpha = (\alpha_1, \ldots, \alpha_r)$ runs over all r-tuples of nonnegative integers with $|\alpha| \le |G| - 1$.

Proof. Consider Case (i) first.

Step 1. Lift the action of G to the regular representation of G; i.e., if $|G| = n$, $G = \{\sigma_1 = \mathrm{id}, \ldots, \sigma_n\}$, define $\tilde{A} := R[X(i,j): 1 \le i \le n,\ 1 \le j \le r]$, Φ: $\tilde{A} \to A$ by $\Phi(X(i,j)) = \sigma_i(a_j)$, $\sigma_k(X(i,j)) = X(l,j)$ if $\sigma_k \sigma_i = \sigma_l$.

Step 2. If $f \in A^G$, write

$$f = \sum_{\alpha} c_\alpha a_1^{\alpha_1} \cdots a_r^{\alpha_r}.$$

Define $\tilde{f}, \tilde{g} \in \tilde{A}$ by

$$\tilde{g} := \sum_{\alpha} c_\alpha X(1,1)^{\alpha_1} \cdots X(1,r)^{\alpha_r}$$

$$\tilde{f} := \frac{1}{n} \mathrm{Sp}(\tilde{g}) \in \tilde{A}^{S_n}.$$

Then $\Phi(\tilde{f}) = f$.

Step 3. By Theorem 3.7, $\tilde{f}$ can be expressed in terms of $\mathrm{Sp}(X(1,1)^{\beta_1} \cdots X(1,r)^{\beta_r})$ with $|\beta| \le n$.

Step 4. Define $A_0 := \mathbf{Z}[1/n!][X(i,j): 1 \le i \le n,\ 1 \le j \le r]$, Φ_0: $A_0 \to \tilde{A}$ the natural homomorphism.

Those elements $\mathrm{Sp}(X(1,1)^{\beta_1} \cdots X(1,r)^{\beta_r})$ with $|\beta| \le n$ in Step 3 can be lifted to A_0. Apply Schmid's theorem [13] to the action of G on A_0. (We may consider $A_0[\zeta]$, where ζ is a primitive $n!$th root of unity, and then descend as in Step 4 of the proof of Theorem 4.8. Note that all the arguments of Schmid's proof [13] can be adapted to the case of $\mathbf{Z}[1/n!][\zeta][X(i,j): 1 \le i \le n,\ 1 \le j \le r]$; use Theorem 4.9 when necessary.) Hence these $\mathrm{Sp}(X(1,1)^{\beta_1} \cdots X(1,r)^{\beta_r})$ can be expressed in terms of elements of the form

$$h := \sum_{k=1}^{m} \sigma_k\Bigl(\prod_{i,j} X(i,j)^{\gamma_{ij}}\Bigr) \in A_0^G$$

with $\sum_{i,j}\gamma_{ij} \leq n-1$. This finishes the proof.

Now consider Case (ii). Steps 1 and 2 are the same as in Case (i), while Step 3 needs to be modified. In this situation, use Theorem 4.8 and express $\tilde{f}$ in terms of $\sum_{i=1}^{n}\sigma_k(\prod_{i,j}X(i,j)^{\beta_{ij}})$ with $\sum_{i,j}\beta_{ij} \leq n$. Then apply Schmid's theorem to these elements $\sum_{k=1}^{n}\sigma_k(\prod_{i,j}X(i,j)^{\beta_{ij}})$ in $\mathbf{Z}[1/n][X(i,j): 1 \leq i \leq n,\ 1 \leq j \leq r]$ as in Step 4 of Case (i).

REFERENCES

1. N. Bourbaki, "Algebra II," translated by P. M. Cohn and J. Howie, Springer-Verlag, Berlin, 1990.
2. H. E. A. Campbell, I. Hughes, and R. D. Pollack, Vector invariants of symmetric groups, *Canad. Math. Bull.* **33** (1990), 391–397.
3. M. Hajja and M. Kang, Some actions of symmetric groups, *J. Algebra*, **177** (1995), 511–535.
4. D. G. Mead, Generators for the algebra of symmetric polynomials, *Amer. Math. Monthly* **100** (1993), 386–388.
5. H. Minc, "Permanents," Encyclopedia Math. and Its Appl., Vol. 6, Addison–Wesley, Reading, MA, 1978.
6. H. Minc, Evaluation of permanents, *Proc. Edinburgh Math. Soc.* **22** (1979), 27–32.
7. M. Nagata, "Lectures on the Fourteenth Problem of Hilbert," Tata Institute of Fundamental Research, Bombay, 1965.
8. E. Noether, Der Endlichkeitssatz der Invarianten endlicher Gruppen, *Math. Ann.* **77** (1916), 89–92; *in* "Collected Papers," pp. 181–184, Springer-Verlag, Berlin, 1983.
9. E. Noether, Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p, *Nachr. Ges. Wiss. Göttingen* (1926), 28–35; *in* "Collected Papers," pp. 485–492, Springer-Verlag, Berlin, 1983.
10. D. Richman, Explicit generators of the invariants of finite groups, *Adv. Math.*, to appear.
11. H. J. Ryser, Combinatorial mathematics, Carus Math. Monographs, Vol. 14, Math. Assoc. Amer., Washington, DC, 1963.
12. B. J. Schmid, Generating invariants of finite groups, *C. R. Acad. Sci. Paris* **308** (1989), 1–6.
13. B. J. Schmid, Finite groups and invariant theory, *in* "Topics in Invariants Theory: Séminaire d'algèbre P. Dubreil et M.-P. Malliavin 1989–1990 (40ème Année)" (M.-P. Malliavin, Ed.), Lect. Notes. in Math., Vol. 1478, Springer-Verlag, Berlin, 1991.
14. J. P. Serre, Groupes finis d'automorphismes d'anneaux locaux réguliers, *in* "Colloq. d'Algèbre," Ecole Normale Sup. Jeunes Filles, Paris, 1967.
15. R. P. Stanley, Invariants of finite groups and their applications to combinatorics, *Bull. Amer. Math. Soc.* **1** (1979), 475–511.
16. H. Weyl, "The Classical Groups," 2nd ed., Princeton Univ. Press, Princeton, NJ, 1953.