Discrete Math. Appl., Vol. 9, No. 4, pp. 343–354 (1999)

Polynomial invariants of finite groups over fields of prime characteristics*

S. A. STEPANOV

Abstract — Let R be a commutative ring with the unit element 1, and let $G = S_n$ be the symmetric group of degree $n \geq 1$. Let A_{mn}^G 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 G. A classical result of Noether [6] implies that if every non-zero integer is invertible in R, then A_{mn}^G is generated by polarized elementary symmetric polynomials. As was recently shown by D. Richman, this result remains true under the condition that $n!$ is invertible in R. The purpose of this paper is to give a short proof of Richman's result based on the use of Waring's formula and closely related to Noether's original proof.

The research was supported by Bilkent University, 06533 Bilkent, Ankara, Turkey.

1. INTRODUCTION

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

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

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

$$gx_{ij} = x_{i,g(j)}, \qquad g \in G.$$

Denote by A_{mn}^G the subalgebra of invariants of the algebra A_{mn} with respect to the group G and define polarized elementary symmetric polynomials $u_{r_1,\ldots,r_m} \in A_{mn}^G$ in n vector variables $(x_{11}, \ldots, x_{m1}), \ldots, (x_{1n}, \ldots, x_{mn})$ by means of the formal identity

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

If R is Noetherian, it follows from the Hilbert-Noether finiteness theorem [4, 6] that A_{mn}^G is a finitely generated commutative R-algebra and A_{mn} is finitely generated as a module over A_{mn}^G. Moreover, if every integer is invertible in R, the invariants $u_{r_1,\ldots,r_m}$ form a complete system of generators of A_{mn}^G over R (see [1], p. 9; [2], p. 62; [14], p. 37). In other words, every element u of the algebra A_{mn}^G may be

* UDC 519.4. Originally published in *Diskretnaya Matematika* (1999) **11**, No. 3, 3–14 (in Russian). Received May 25, 1999. Translated by the author.

written as a polynomial in $u_{r_1,\dots,r_m}$, $1 \le r_1 + \dots + r_m \le n$, 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 [3], p. 68, and [12]). This result was recently generalized by D. Richman [8] as follows.

Theorem 1. *Assume that $G = S_n$ and $n!$ is invertible in R. Then A_{mn}^G is generated as an R-algebra by the polarized elementary symmetric polynomials $u_{r_1,\dots,r_m}$, $1 \le r_1 + \dots + r_m \le n$, of degree at most n.*

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

Corollary 1. *Let R be a field and $G = S_n$. If the characteristic of R is zero or $p > n$, then A_{mn}^G is generated as an R-algebra by the polarized elementary symmetric polynomials $u_{r_1,\dots,r_m}$, $1 \le r_1 + \dots + r_m \le n$.*

In this paper we give a short and simple proof of Theorem 1 based on polarization of the classical Waring formula and closely related to one of two Noether's original proofs in the case where R is a field of characteristic 0. Several examples presented in the final section of the paper show that the restriction on R stated in Theorem 1 cannot be removed.

More generally, let $A = R[x_1, \dots, x_m]$ be a finitely generated commutative R-algebra, G be a finite group of the R-algebra automorphisms of A, and let A^G be the subalgebra of invariants of G. If $z_1, \dots, z_m$ are commuting indeterminates, define

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

If every non-zero integer is invertible in R, it follows from the Noether theorem that A^G is generated as an R-algebra by the coefficients of $F(z_1, \dots, z_m)$. The result of Theorem 1 and the standard arguments based on the use of the Reynolds operator and the Noether map (see [6], [10], p. 63, [14], 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 the invariant polynomials in $x_1, \dots, x_m$ of degree at most $|G|$.*

This result provides 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 1 based on different arguments also ascending to Noether (see [9] and [10], p. 29). The upper bound on the degrees of a set of generating polynomials for the algebra of invariants given by Theorem 2 is known as Noether's bound (see also [9], [10], p. 28, and [11]). In the final section of the paper, we show that the conditions of Theorem 2 cannot be removed. In particular, it will be shown that Noether's bound is false if R is a field of characteristic

2 and $G = S_2$. For other results and problems in the theory of polynomial invariants over fields of prime characteristic see [9] and [11].

2. GENERATING INVARIANTS OF THE SYMMETRIC GROUP

Let $G = S_n$ 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}^G be the subalgebra of invariants of G in A_{mn}, and $u_{r_1,\ldots,r_m}$, $1 \leq r_1 + \ldots + r_m \leq n$, be the polarized elementary symmetric polynomials in A_{mn}^G.

Let $v_{\sigma_1,\ldots,\sigma_m}$ be an invariant polynomial in A_{mn}^G of the form

$$v_{\sigma_1,\ldots,\sigma_m} = \sum_{j=1}^{n} x_{1j}^{\sigma_1} \ldots x_{mj}^{\sigma_m}.$$

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

$$v_\sigma = \sum_{j=1}^{n} x_j^\sigma = \sum_{s_1+2s_2+\ldots+ns_n=\sigma} c(s_1, \ldots, s_n) u_1^{s_1} \ldots u_n^{s_n}, \tag{2}$$

where $c_{s_1,\ldots,c_n}$ are integers of the form

$$c(s_1, \ldots, s_n) = (-1)^{s_2+2s_3+\ldots+(n-1)s_n} \frac{\sigma(s_1 + \ldots + s_n - 1)!}{s_1! \ldots s_n!}.$$

The following result can be considered as a generalization of the Waring formula to the case where $m > 1$ (see also [12]).

Proposition 1. *Let $\sigma_1, \ldots, \sigma_m$ be non-negative integers, $v_{\sigma_1,\ldots,\sigma_m} = \sum_{j=1}^{n} x_{1j}^{\sigma_1} \ldots x_{mj}^{\sigma_m}$ be the polynomial in A_{mn}^G of degree $\sigma = \sigma_1 + \ldots + \sigma_m$, and let $u_{r_1,\ldots,r_m}$, $1 \leq r_1 + \ldots + r_m \leq n$, be the polarized elementary symmetric polynomials of vectors $(x_{1j}, \ldots, x_{mj})$, $1 \leq j \leq n$. For non-negative integers $s_1, \ldots, s_n$ and $s_{1\nu}, \ldots, s_{m\nu}$ satisfying the conditions*

$$s_1 + 2s_2 + \ldots + ns_n = \sigma, \quad s_{1\nu} + \ldots + s_{m\nu} = \nu s_\nu, \quad 1 \leq \nu \leq n,$$

let

$$w_{s_{1\nu},\ldots,s_{m\nu}} = \sum_R \frac{s_\nu!}{\sigma_{\nu 1}! \ldots \sigma_{\nu s_\nu}!} \prod_{\tau=1}^{s_\nu} u_{r_{1\tau},\ldots,r_{m\tau}}^{\sigma_{\nu\tau}},$$

where the sum is over the set R of all non-negative integers $r_{1\tau}, \ldots, r_{ms_\nu}$ and $\sigma_{\nu 1}, \ldots, \sigma_{\nu s_\nu}$ such that

$$\begin{aligned} r_{\mu 1}\sigma_{\nu 1} + \ldots + r_{ms_\nu}\sigma_{\nu s_\nu} &= s_{\mu\nu}, \\ \sigma_{\nu 1} + \ldots + \sigma_{\nu s_\nu} &= s_\nu, \\ r_{1\tau} + \ldots + r_{m\tau} &= \nu, \quad 1 \leq \mu \leq m, \quad 1 \leq \nu \leq n, \quad 1 \leq \tau \leq s_\nu. \end{aligned}$$

Then

$$v_{\sigma_1,\dots,\sigma_m} = \frac{\sigma_1!\dots\sigma_m!}{\sigma!} \sum_{s_1+2s_2+\dots+ns_n=\sigma} c(s_1,\dots,s_n) \sum_S \prod_{i=1}^{n} v_{s_{1\nu_i},\dots,s_{m\nu_i}}, \tag{3}$$

where the inner sum is over the set S of all non-negative integers $s_{\mu\nu_1},\dots,s_{\mu\nu_n}$ *satisfying the relations*

$$s_{\mu\nu_1}+\dots+s_{\mu\nu_n} = \sigma_\mu,$$
$$s_{1\nu_i}+\dots+s_{m\nu_i} = is_i, \quad 1\le\mu\le m, \quad 1\le i\le n.$$

Proof. In (2) we set

$$x_j = x_{1j}z_1+\dots+x_{mj}z_m, \qquad 1\le j\le m.$$

Since

$$(x_{1j}z_1+\dots+x_{mj}z_m)^\sigma = \sum_{\sigma_1+\dots+\sigma_m=\sigma} \frac{\sigma!}{\sigma_1!\dots\sigma_m!} x_{1j}^{\sigma_1}\dots x_{mj}^{\sigma_m} z_1^{\sigma_1}\dots z_m^{\sigma_m},$$

we have

$$\sum_{j=1}^{n}(x_{1j}z_1+\dots+x_{mj}z_m)^\sigma = \sum_{\sigma_1+\dots+\sigma_m=\sigma} \frac{\sigma!}{\sigma_1!\dots\sigma_m!} \left(\sum_{j=1}^{n} x_{1j}^{\sigma_1}\dots x_{mj}^{\sigma_m}\right) z_1^{\sigma_1}\dots z_m^{\sigma_m}.$$

On the other hand,

$$\sum_{1\le j_1<\dots<j_\nu\le n} \prod_{s=1}^{\nu}(x_{1j_s}z_1+\dots+x_{mj_s}z_m) = \sum_{r_1+\dots+r_m=\nu} u_{r_1,\dots,r_m} z_1^{r_1}\dots z_m^{r_m},$$

and hence, in view of (2),

$$\sum_{j=1}^{n}(x_{1j}z_1+\dots+x_{mj}z_m)^\sigma = \sum_{s_1+2s_2+\dots+ns_n=\sigma} c(s_1,\dots,s_n) \prod_{\nu=1}^{n} \left(\sum_{r_1+\dots+r_m=\nu} u_{r_1,\dots,r_m} z_1^{r_1}\dots z_m^{r_m}\right)^{s_\nu}.$$

As a result we find that

$$\sum_{\sigma_1+\dots+\sigma_m=\sigma} \frac{\sigma!}{\sigma_1!\dots\sigma_m!} \left(\sum_{j=1}^{n} x_{1j}^{\sigma_1}\dots x_{mj}^{\sigma_m}\right) z_1^{\sigma_1}\dots z_m^{\sigma_m} = \sum_{s_1+sl_2+\dots+ns_n=\sigma} c(s_1,\dots,s_n) \prod_{\nu=1}^{n} \left(\sum_{r_1+\dots+rm=\nu} u_{r_1,\dots,r_m} z_1^{r_1}\dots z_m^{r_m}\right)^{s_\nu}.$$

Note that

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

where

$$w_{s_{1\nu},\ldots,s_{m\nu}} = \sum_R \frac{s_\nu!}{\sigma_{\nu 1}!\ldots\sigma_{\nu s_\nu}!} \prod_{\tau=1}^{s_\nu} u_{r_{1\tau},\ldots,r_{m\tau}}^{\sigma_{\nu\tau}},$$

and the set R is defined in the statement of the proposition, therefore we find that

$$\sum_{\sigma_1+\ldots+\sigma_m=\sigma}\left(\sum_{j=1}^n x_{1j}^{\sigma_1}\ldots x_{mj}^{\sigma_m}\right) z_1^{\sigma_1}\ldots z_m^{\sigma_m}$$
$$= \sum_{\sigma_1+\ldots+\sigma_m=\sigma}\left(\sum_{s_1+2s_2+\ldots+ns_n=\sigma} c(s_1,\ldots,s_n)\sum_S\prod_{i=1}^n w_{s_{1\nu_i},\ldots,s_{m\nu_i}}\right) z_1^{\sigma_1}\ldots z_m^{\sigma_m},$$

where the set S is defined in the statement of the theorem. Thus, we arrive at the relation

$$\sum_{j=1}^n x_{1j}^{\sigma_1}\ldots x_{mj}^{\sigma_m} = \frac{\sigma_1!\ldots\sigma_m!}{\sigma!}\sum_{s_1+2s_2+\ldots+ns_n=\sigma} c(s_1,\ldots,s_n)\sum_S\prod_{i=1}^n w_{s_{1\nu_i},\ldots,s_{m\nu_i}},$$

which proves the theorem.

If $\sigma=\sigma_1+\ldots+\sigma_m\le n+1$, then

$$v_{\sigma_1,\ldots,\sigma_m} = \frac{\sigma_1!\ldots\sigma_m!}{\sigma!}\sum_{s_1+2s_2+\ldots+n\sigma_n=\sigma} c(s_1,\ldots,\sigma_m)\prod_{i=1}^n v_{s_{1\nu_i},\ldots,m_{\nu_i}}$$

involves only the polarized elementary symmetric polynomials $u_{r_1,\ldots,r_m}$, $1\le r_1+\ldots+r_m\le n$. Moreover, the coefficients of $v_{\sigma_1,\ldots,\sigma_m}$ are rational numbers whose denominators are not divisible by any prime $p>\sigma$. As a consequence of this observations we get the following result.

Corollary 2. *If $n!$ is invertible in R and $\sigma=\sigma_1+\ldots+\sigma_m\le n+1$, then*

$$v_{\sigma_1,\ldots,\sigma_m} = \sum_{j=1}^n x_{1j}^{\sigma_1}\ldots x_{mj}^{\sigma_m}$$

is a polynomial over R in the polarized elementary symmetric polynomials $u_{r_1,\ldots,r_m}$, $1\le r_1+\ldots+r_m\le n$, of degree at most n.

Now we show that any invariant in A_{mn}^G can be represented as a polynomial over R in $v_{\sigma_1,\ldots,\sigma_m}$.

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

$$v = \sum_{u \in \{\tau(f) | \tau \in G\}} u.$$

Then v is a polynomial over R in the invariants

$$v_{\sigma_1,\dots,\sigma_m} = \sum_{j=1}^{n} x_{1j}^{\sigma_1} \dots x_{mj}^{\sigma_m},$$

where $\sigma_1, \dots, \sigma_m$ are non-negative integers such that $0 \le \sigma_1 + \dots + \sigma_m \le \deg f$.

Proof. We write 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 first that $\delta(f) = 0$. Then $f = f_j = x_{1j}^{\alpha_1} \dots x_{mj}^{\alpha_m}$ for some $j \in \{1, 2, \dots, n\}$ and $(\alpha_1, \dots, \alpha_m)$, $0 \le \alpha_1 + \dots + \alpha_m \le \deg f$, therefore

$$v = \sum_{u \in \{\tau(f) | \tau \in G\}} u = \sum_{j=1}^{n} x_{1j}^{\alpha_1} \dots x_{mj}^{\alpha_m}.$$

Suppose now that $\delta(f) > 0$ and let $j \in \{1, 2, \dots, n\}$ satisfy the condition $d(f) = \deg f_j < \deg f$. Define v_j and v'_j, setting

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

The induction hypothesis implies that v_j and v'_j are polynomials in $v_{\sigma_1,\dots,\sigma_m}$, $0 \le \sigma_1 + \dots + \sigma_m \le \deg f$. For every $\rho \in G$, we define U_ρ as the set of all pairs (u, u') such that

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

and note that the map

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

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

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

By the induction hypothesis, the invariant

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

is a polynomial over R in $v_{\sigma_1,\ldots,\sigma_m}$, $0 \leq \sigma_1 + \ldots + \sigma_m \leq \deg f$. The cardinality of U_{id} does not exceed the cardinality of $\{\tau(f_j) \mid \tau \in G\}$, and the last cardinality does not exceed the cardinality of $\{x_{1j}^{\sigma_1} \ldots x_{mj}^{\sigma_m} \mid 1 \leq j \leq n\}$, therefore $1 \leq |U_{id}| \leq n$. Since $n!$ is invertible in R, we conclude that

$$\sum_{u \in \{\tau(f) | \tau \in G\}} u$$

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

3. PROOF OF THEOREM 1

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

$$v = \sum_{u \in \{\tau(f) | \tau \in G\}} u,$$

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 the polarized elementary symmetric polynomials $u_{r_1,\ldots,r_m}$, $1 \leq r_1 + \ldots + r_m \leq n$. If $\mu \leq n+1$, the assertion follows from Proposition 4. Assume now that $\mu > n+1$ and proceed the proof by induction on μ. We set

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

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 $\tilde{A}_{mn}^G$ be the subalgebra of invariants of $\tilde{A}_{mn}$. It follows from Corollary 2 that $w_{\mu+1}$ is a polynomial over R in the polarized elementary symmetric polynomials $\tilde{u}_{r_1,\ldots,r_m} \in \tilde{A}_{mn}$, $1 \leq r_1 + \ldots + r_m \leq n$. Since every such polynomial $\tilde{u}_{r_1,\ldots,r_m}$ has the form

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

for some monomial $\tilde{f} \in \tilde{A}_{mn}$ of degree at most n, by Proposition 2 it can be written as a polynomial over R in invariants

$$\tilde{v}_{\sigma_1,\ldots,\sigma_m} = \sum_{j=1}^{n} \tilde{x}_{1j}^{\sigma_1} \ldots \tilde{x}_{mj}^{\sigma_m}$$

of degree at most n. Therefore,

$$\tilde{v}_{\sigma_1,\ldots,\sigma_m} = \sum_{j=1}^{n} x_{1j}^{s_1} \ldots x_{mj}^{s_j}$$

with $1 \leq s_1 + \ldots + s_m \leq \mu$. The induction hypothesis implies that every invariant $\tilde{v}_{\sigma_1,\ldots,\sigma_m}$ is a polynomial over R in $u_{r_1,\ldots,r_m}$, $1 \leq r_1 + \ldots + r_m \leq n$, so $w_{\mu+1}$ is also a polynomial over R in these polarized elementary symmetric polynomials.

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

4. EXAMPLES

Example 1. Let $m = 3$ and $n = 2$. Let us show that the cubic

$$v_{111} = x_{11}x_{21}x_{31} + x_{12}x_{22}x_{32},$$

which is invariant with respect to $G = S_2$, cannot be written as a polynomial in the invariants u_{100}, u_{010}, u_{001}, u_{200}, u_{110}, u_{101}, u_{020}, u_{011}, u_{002} over F_2, the prime finite field of characteristic 2. By Proposition 1, we have

$$2v_{111} = 2u_{100}u_{010}u_{001} - (u_{100}u_{011} + u_{010}u_{101} + u_{001}u_{110}),$$

and since the generating elements u_{100}, u_{010}, u_{001}, u_{110}, u_{101}, u_{011} of the algebra $\mathbf{Q}[x_{11}, x_{21}, x_{31}; x_{12}, x_{22}, x_{32}]^G$ are algebraically independent over $\mathbf{Q}$, this decomposition is unique. Hence it follows that v_{111} cannot be expressed over F_2 as a polynomial in u_{100}, u_{010}, u_{001}, u_{200}, u_{110}, u_{101}, u_{020}, u_{011}, u_{002}. Thus, the Noether bound is false in characteristic 2. Therefore, the conditions of Theorem 1 and Theorem 2 cannot be removed. Moreover, we see that u_{100}, u_{010}, u_{001}, u_{011}, u_{101}, u_{110} are algebraically dependent over F_2.

Now we show that any polynomial $f_{\sigma_1\sigma_2\sigma_3}$ of the form

$$f_{\sigma_1\sigma_2\sigma_3} = x_{11}^{\sigma_1}x_{21}^{\sigma_2}x_{31}^{\sigma_{31}} + x_{12}^{\sigma_1}x_{22}^{\sigma_2}x_{32}^{\sigma_3}$$

can be expressed as a polynomial in $u_{001}, u_{010}, u_{100}, u_{002}, u_{011}, u_{020}, u_{101}, u_{110}, u_{200}$, and v_{111} with integer coefficients.

At first we show that any polynomial

$$f_{\sigma_1\sigma_2} = x_{11}^{\sigma_1}x_{21}^{\sigma_2} + x_{12}^{\sigma_2}x_{22}^{\sigma_2}$$

is a polynomial in $u_{01}, u_{10}, u_{02}, u_{11}, u_{20}$ over $\mathbf{Z}$. Indeed, we have

$$x_{11} + x_{12} = u_{10}, \qquad x_{21} + x_{22} = u_{01}$$

and

$$x_{11}^2 + x_{12}^2 = u_{10}^2 - 2u_{20}, \quad x_{11}x_{21} + x_{12}x_{22} = u_{01}u_{10} - u_{11}, \quad x_{21}^2 + x_{22}^2 = u_{01}^2 - 2u_{02}.$$

If $\sigma = \sigma_1 + \sigma_2 > 2$, we can assume without loss of generality that $\sigma_2 \geq 2$. In that case,

$$\begin{aligned} f_{\sigma_1\sigma_2} &= (x_{21} + x_{22})f_{\sigma_1\sigma_2 - 1} - (x_{11}^{\sigma_{11}}x_{21}^{\sigma_2 - 1}x_{22} + x_{21}^{\sigma_1}x_{22}^{\sigma_2 - 1}x_{21}) \\ &= (x_{21} + x_{22})f_{\sigma_1\sigma_2 - 1} - x_{21}x_{22}f_{\sigma_1,\sigma_2 - 2} = u_{01}f_{\sigma_1\sigma_2 - 1} - u_{02}f_{\sigma_1\sigma_2 - 2}, \end{aligned}$$

and we can use the double induction on m and σ.

Similarly, if $\sigma = \sigma_1 + \sigma_2 + \sigma_3 > 3$, we can assume without loss of generality that $\sigma_3 \geq 2$. In that case,

$$\begin{aligned} f_{\sigma_1\sigma_2\sigma_3} &= (x_{31} + x_{32})f_{\sigma_1\sigma_2\sigma_3 - 1} - (x_{11}^{\sigma_1}x_{21}^{\sigma_2}x_{31}^{\sigma_3 - 1}x_{32} + x_{21}^{\sigma_1}x_{22}^{\sigma_2}x_{32}^{\sigma_3 - 1}x_{31}) \\ &= u_{001}f_{\sigma_1,\sigma_2,\sigma_3 - 1} - u_{002}f_{\sigma_1\sigma_2\sigma_3 - 2}, \end{aligned}$$

and the assertion follows with the use of the double induction on m and σ.

Example 2. Let $m = 4$ and $n = 2$. Let us show that the quartic

$$v_{1111} = x_{11}x_{21}x_{31}x_{41} + x_{12}x_{22}x_{32}x_{42},$$

which is invariant with respect to $G = S_2$, cannot be expressed over F_2 as a polynomial in u_{r_1,r_2,r_3,r_4}, $1 \leq r_1 + r_2 + r_3 + r_4 \leq 4$. Assume, for a contradiction, that

$$\begin{aligned} v_{1111} = {} & a u_{1000}u_{0100}u_{0010}u_{0001} \\ & + b(u_{1000}u_{0100}u_{0011} + u_{1000}u_{0010}u_{0101} + u_{1000}u_{0001}u_{0110}) \\ & + b(u_{0100}u_{0001}u_{1010} + u_{0100}u_{0010}u_{1001} + u_{0010}u_{0001}u_{1100}) \\ & + c(u_{1100}u_{0011} + u_{1010}u_{0101} + u_{1001}u_{0110}) \end{aligned}$$

with some $a, b, c \in F_2$, and observe that

$$u_{1000} = x_{11} + x_{21}, \quad u_{0100} = x_{21} + x_{22},$$
$$u_{0010} = x_{31} + x_{32}, \quad x_{0001} = x_{41} + x_{42}$$

and

$$u_{1100} = x_{11}x_{22} + x_{12}x_{12}, \quad u_{1010} = x_{11}x_{32} + x_{12}x_{31}, \quad u_{1001} = x_{11}x_{42} + x_{12}x_{41},$$
$$u_{0110} = x_{21}x_{32} + x_{22}x_{31}, \quad u_{0101} = x_{21}x_{42} + x_{22}x_{41}, \quad u_{0011} = x_{31}x_{42} + x_{32}x_{41}.$$

Differentiating the both sides of this equality with respect to x_{11} and taking into account that

$$\frac{\partial u_{1000}}{\partial x_{11}} = 1, \quad \frac{\partial u_{0100}}{\partial x_{11}} = 0, \quad \frac{\partial u_{0010}}{\partial x_{11}} = 0, \quad \frac{\partial u_{0001}}{\partial x_{11}} = 0$$

and

$$\frac{\partial u_{1100}}{\partial x_{11}} = x_{22}, \quad \frac{\partial u_{1010}}{\partial x_{11}} = x_{32}, \quad \frac{\partial u_{1001}}{\partial x_{11}} = x_{42},$$
$$\frac{\partial u_{0110}}{\partial x_{11}} = 0, \quad \frac{\partial u_{0101}}{\partial x_{11}} = 0, \quad \frac{\partial u_{0011}}{\partial x_{11}} = 0,$$

we obtain

$$\begin{aligned} x_{21}x_{31}x_{41} = {} & a u_{0100}u_{0010}u_{0001} + b(u_{0100}u_{0011} + u_{0010}u_{0101} + u_{0001}u_{0110}) \\ & + b(u_{0100}u_{0001}x_{32} + u_{0100}u_{0010}x_{42} + u_{0010}u_{0001}x_{22}) \\ & + c(u_{0011}x_{22} + u_{0101}x_{32} + u_{0110}x_{42}). \end{aligned}$$

Setting now $x_{21} = x_{31} = x_{41} = x_{12} = x_{22} = x_{32} = x_{42} = 1$ in the last equality, we arrive at the relation $1 = 8a + 24b + 6c$, which is impossible in F_2.

Finally, it follows from Proposition 2 that

$$\begin{aligned} 6v_{1111} = {} & 6u_{1000}u_{0100}u_{0010}u_{0001} \\ & - 2(u_{1000}u_{0100}u_{0011} + u_{1000}u_{0010}u_{0101} + u_{1000}u_{0001}u_{0110}) \\ & - 2(u_{0100}u_{0001}u_{1010} + u_{0100}u_{0010}u_{1001} + u_{0010}u_{0001}u_{1100}) \\ & + (u_{1100}u_{0011} + u_{1010}u_{0101} + u_{1001}u_{0110}), \end{aligned}$$

so the polynomials $u_{1100}, u_{1010}, u_{1001}, u_{0110}, u_{0101}, u_{0011}$ are algebraically dependent over F_2. On the other hand, they are algebraically independent over $\mathbf{Q}$.

Example 3. The above examples can be generalized as follows. Let $m > n \geq 2$ be an integer and p be a prime divisor of n. Let F_p be a prime finite field of characteristic $p > 0$ and

$$v_{11\ldots11} = \sum_{j=1}^{n} x_{1j} \ldots x_{mj}$$

be the homogeneous polynomial of degree m. Let us show that the polynomial $v_{11\ldots11}$ cannot be expressed as a polynomial in the invariants $u_{r_1,\ldots,u_m}$, $1 \leq r_1 + \ldots r_m \leq n$, over F_p.

Assume, for a contradiction, that

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

where $a_{s_1,\ldots,s_n} \in F_p$ and the summation in the second sum is over the set $R(s_1,\ldots,s_n)$ of all non-negative integers $r_{1\sigma_\nu},\ldots,r_{m\sigma_\nu}$, $1 \leq \nu \leq m$, such that

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

We may assume without loss of generality 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 both sides of the above equality with respect to x_{11} and taking into account that

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

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

$$x_{21}\ldots x_{m1} = \sum_{s_1+2s_2+\ldots+ns_n=m} a_{s_1,\ldots,s_n} \sum_{j=1}^{n} \Psi^{(j)}_{s_1,\ldots,s_n}, \tag{4}$$

where

$$\Psi^{(j)}_{s_1,\ldots,s_n} = \sum_{R(s_1,\ldots,s_n)} u^{(1,0,\ldots,0)}_{0,r_{2\sigma_k},\ldots,r_{m\sigma_k}} \prod_{\sigma_k=2}^{s_k} u_{0,r_{2\sigma_k},\ldots,r_{m\sigma_k}} \prod_{\substack{\nu=1 \\ \nu\neq k}}^{n} \prod_{\sigma_\nu=1}^{s_\nu} u_{0,r_{2\sigma_\nu}\ldots,r_{m\sigma_\nu}},$$

where the set $R(s_1,\ldots,s_n)$ is defined above. 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 (4), 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 F_p for any prime p dividing n.

REFERENCES

1. D. J. Benson, *Polynomial Invariants of Finite Groups.* Cambr. Univ. Press, Cambridge, 1993.
2. N. Bourbaki, *Elements of Mathematics, Algebra II.* Springer, Berlin, 1990.
3. J. A. Dieudonne and J. B. Carrel, *Invariant Theory, Old and New.* Academic Press, New York, 1971.
4. D. Hilbert, Über die vollen Invariantensystem. *Math. Ann.* (1893) **42**, 313–373.
5. D. Mumford, *Geometric Invariant Theory.* Springer-Verlag, Berlin, 1993.
6. E. Noether, Der Endlichkeitssatz der Invarianten endlicher Gruppen. *Math. Ann.* (1916) **77**, 89–92.
7. E. Noether, Der Endlichkeitssatz der Invarianten endlicher linear Gruppen der Characteristik *p*. *Nachr. v. d. Ges. d. Wiss. zu Göttingen* (1926), 28–35.
8. D. R. Richman, Explicit generators of the invariants of finite groups. *Adv. Math.* (1996) **124**, 49–76.
9. B. J. Schmid, Finite groups and invariant theory. *Lect. Notes Math.* (1991) **1478**.
10. L. Smith, *Polynomial Invariants of Finite Groups.* A. K. Peters, Wellesley, MA, 1995.
11. L. Smith, Polynomial invariants of finite groups; A survey of recent developments. *Bull. Amer. Math. Soc.* (1997) **34**, 211–250.
12. S. A. Stepanov, On vector invariants of the symmetric group. *Discrete Math. Appl.* (1996) **6**, 135–147.
13. E. Waring, *Meditationes Algebraicae.* Cambr. Univ. Press., Cambridge, 1782.
14. H. Weyl, *The Classical Groups, their Invariants and Representations.* Inst. Advanced Study, Princeton, 1946.