BULLETIN OF THE POLISH
ACADEMY OF SCIENCES
MATHEMATICS
Vol. 53, No. 3, 2005

ALGEBRA

Reducibility of Symmetric Polynomials

by

A. SCHINZEL

To Donald G. Lewis on his 80th birthday

Summary. A necessary and sufficient condition is given for reducibility of a symmetric polynomial whose number of variables is large in comparison to degree.

Let K be a field and $\tau_i(x_1,\ldots,x_m)$ the ith elementary symmetric polynomial of the variables $x_1,\ldots,x_m$. We shall show

THEOREM 1. *Let $F\in K[y_1,\ldots,y_n]\setminus K$ and $n>\max\{4,\deg F+1\}$, $\tau_i=\tau_i(x_1,\ldots,x_n)$. Then $F(\tau_1,\ldots,\tau_n)$ is reducible in $K[x_1,\ldots,x_n]$ if and only if either F is reducible over K, or*

$$F=cN_{K(\alpha)/K}\Big(\alpha^n+\sum_{j=1}^{n}\alpha^{n-j}y_j\Big),\qquad c\in K^*,\ \alpha \text{ algebraic over } K.$$

THEOREM 2. *Let $F\in K[y_1,\ldots,y_n]\setminus K$ be isobaric with respect to weights $1,\ldots,n$ (y_i of weight i) and $n>\deg F+1$. Then $F(\tau_1,\ldots,\tau_n)$ is reducible over K if and only if either F is reducible over K, or $F=cy_n$, $c\in K^*$, or $n=4$, $\operatorname{char}K\neq 3$, K contains a primitive cubic root of 1 and*

$$F=a(y_2^2-3y_1y_3+12y_4),\qquad a\in K^*.$$

The last part of Theorem 2 shows that the 4 in the formulation of Theorem 1 cannot be replaced by 3. The example given at the end of the paper shows that $\deg F+1$ cannot be replaced by $\deg F$.

For a polynomial $f\in K[x_1,\ldots,x_n]$ and a permutation $\sigma\in\mathfrak{S}_n$ we set

$$f^\sigma=f(x_{\sigma(1)},\ldots,x_{\sigma(n)}).$$

The proof of Theorem 1 is based on three lemmas.

2000 *Mathematics Subject Classification*: Primary 12E05.
Key words and phrases: polynomial, reducibility, symmetric.

Lemma 1. *For $n \geq 5$ the alternating group $\mathfrak{A}_n$ is generated by products $(ab)(cd)$ of two transpositions with a, b, c, d distinct.*

Proof. See [1, p. 342]. ■

Lemma 2. *Assume that $C \in K[x_1, \ldots, x_n]$ is invariant with respect to $\mathfrak{A}_n$, but not symmetric. Then for $n \geq 3$,*

$$\deg_{x_n} C \geq n-1.$$

Proof. By the theorem of P. Samuel (see [2, p. 13])

$$C = A + BD_n$$

where $A, B \in K[x_1, \ldots, x_n]$ are symmetric, $B \neq 0$ and

$$D_n = \frac{1}{2}\Big(\prod_{i<j}(x_i - x_j) + \prod_{i<j}(x_i + x_j)\Big).$$

For $n \geq 3$ we have $\deg_{x_n} D_n \geq n-1$, hence $\deg_{x_n} C \geq n-1$, except possibly when $\deg_{x_n} A = \deg_{x_n} BD_n$. In that case, let $\alpha = \deg_{x_n} A$, $\beta = \deg_{x_n} B$, and let a, b be the leading coefficients of A and B with respect to x_n. The coefficient of $x_n^{\beta+n-1}$ in C equals

$$c = a + bD_{n-1}$$

and since D_{n-1} is not symmetric, $c \neq 0$, thus again

$$\deg_{x_n} C \geq n-1. \ ■$$

Lemma 3. *If $f \in K[x_1, \ldots, x_n] \setminus \bigcup_{i=1}^n K[x_i]$ is irreducible over K and not symmetric, then*

$$\deg_{x_n} \operatorname*{l.c.m.}_{\sigma \in \mathfrak{S}_n} f^\sigma \geq n-1. \tag{1}$$

Proof. Let f depend on exactly r variables, where $1 \leq r < n$. The case $r = 1$ is excluded by the conditions that f irreducible and $f \neq cx_i$. For every subset R of $\{1, \ldots, n\}$ of cardinality r and containing n there exists $\sigma \in \mathfrak{S}_n$ such that f^σ depends on the variables x_i $(i \in R)$ exclusively. For different sets R the forms f^σ are projectively different and hence coprime. For $1 < r < n$ the number of sets R in question is $\binom{n-1}{r-1} \geq n-1$, thus (1) holds.

Consider now the case $r = n$ and let

$$\mathcal{G} = \{\sigma \in \mathfrak{S}_n : f^\sigma/f \in K\}, \quad \mathcal{H} = \{\sigma \in \mathfrak{S}_n : f^\sigma = f\}.$$

By Bertrand's theorem (see [1, pp. 348–352]) we have either $\mathcal{G} = \mathfrak{S}_n$ or $\mathcal{G} = \mathfrak{A}_n$ or $[\mathfrak{S}_n : \mathcal{G}] \geq n$. In the first case, if $f^\tau = f$ for each transposition τ, then $f^\sigma = f$ for all $\sigma \in \mathfrak{S}_n$, since $\mathfrak{S}_n$ is generated by transpositions, thus f is symmetric, contrary to assumption. Therefore, there exists a transposition $\tau = (ij)$, $i \neq j$, such that

$$f^\tau = cf, \quad c \neq 1.$$

Since $\tau^2 = \mathrm{id}$, we have $c^2 = 1$, thus $\mathrm{char}\, K \neq 2$, $c = -1$, and $x_i = x_j$ implies $f = 0$. Since f is irreducible,

$$f = a(x_i - x_j), \qquad a \in K,$$

and it is easy to see that

$$\deg_{x_n} \operatorname*{l.c.m.}_{\sigma \in \mathfrak{S}_n} f^\sigma \geq n - 1.$$

Consider now the case $\mathcal{G} = \mathfrak{A}_n$. By Lemma 1, $\mathfrak{A}_n$ is generated by the products $\pi = (ab)(cd)$, where a, b, c, d are distinct. Since $\pi^2 = \mathrm{id}$, we have $f^\pi = cf$, where $c^2 = 1$. It follows that $(f^2)^\sigma = f^2$ for all $\sigma \in \mathfrak{A}_n$. On the other hand, $\mathcal{H} < \mathcal{G}$ gives either $\mathcal{H} = \mathfrak{A}_n$ or $[\mathfrak{S}_n : \mathcal{H}] \geq n$.

If $\mathcal{H} = \mathfrak{A}_n$, then by Lemma 2, $\deg_{x_n} f \geq n - 1$, hence (1) holds. If $[\mathfrak{S}_n : \mathcal{H}] \geq n$, then f^2 cannot be symmetric, hence by Lemma 2,

$$\deg_{x_n} f^2 \geq n - 1,$$

thus

$$\deg_{x_n} f \geq \left\lceil \frac{n-1}{2} \right\rceil.$$

Now, by the definition of $\mathcal{G}$ it follows that for $\tau = (12)$ we have $f^\tau / f \notin K$, hence $(f^\tau, f) = 1$, thus

$$\deg_{x_n} [f, f^\tau] \geq 2 \left\lceil \frac{n-1}{2} \right\rceil \geq n - 1,$$

and (1) holds.

It remains to consider the case $[\mathfrak{S}_n : \mathcal{G}] \geq n$. Then among the polynomials f^σ there are at least n projectively distinct, hence coprime. Since each of them is of degree at least 1 in x_n, (1) follows. ∎

Proof of Theorem 1. Necessity. If $F(\tau_1, \ldots, \tau_n)$ is reducible over K, then

$$F(\tau_1, \ldots, \tau_n) = f_1 f_2, \tag{2}$$

where $f_\nu \in K[x_1, \ldots, x_n] \setminus K$ $(\nu = 1, 2)$ and f_1 is irreducible over K.

Clearly

$$\deg_{x_n} \operatorname*{l.c.m.}_{\sigma \in \mathfrak{S}_n} f_1^\sigma \leq \deg F < n - 1.$$

If f_1 is not symmetric and $f_1 \notin K[x_i]$ $(1 \leq i \leq n)$, this contradicts Lemma 3, thus either

$$f_1 \text{ is symmetric} \tag{3}$$

or

$$f_1 \in K[x_i] \quad \text{for some } i. \tag{4}$$

In the case (3), $f_\nu = F_\nu(\tau_1, \dots, \tau_n)$, $\nu = 1, 2$, where $F_\nu \in K[y_1, \dots, y_n] \setminus K$, and it follows from (2) that

$$F(\tau_1, \dots, \tau_n) = \prod_{\nu=1}^{2} F_\nu(\tau_1, \dots, \tau_n).$$

By the algebraic independence of $\tau_1, \dots, \tau_n$ over K,

$$F = F_1 F_2,$$

thus F is reducible over K.

In the case (4), since f_1 is irreducible over K, we have

$$f_1 = c_1 N_{L/K}(\alpha + x_i), \quad \text{where } L = K(\alpha),\ \alpha \text{ algebraic over } K,\ c_1 \in K.$$

Since $F(\tau_1, \dots, \tau_n)$ is symmetric, we have

$$f_1(x_j) \mid F(\tau_1, \dots, \tau_n) \quad (1 \le j \le n),$$

thus

$$\prod_{j=1}^{n} f_1(x_j) \,\Big|\, F(\tau_1, \dots, \tau_n).$$

However,

$$\prod_{j=1}^{n} f_1(x_j) = c_1^n \prod_{j=1}^{n} N_{L/K}(\alpha + x_j) = c_1^n N_{L/K}\Big(\alpha^n + \sum_{j=1}^{n} \alpha^{n-j}\tau_j\Big),$$

hence

$$N_{L/K}\Big(\alpha^n + \sum_{j=1}^{n} \alpha^{n-j}\tau_j\Big) \,\Big|\, F(\tau_1, \dots, \tau_n)$$

and by the algebraic independence of $\tau_1, \dots, \tau_n$,

$$N_{L/K}\Big(\alpha^n + \sum_{j=1}^{n} \alpha^{n-j} y_j\Big) \,\Big|\, F.$$

Therefore, either F is reducible over K or

$$F = c N_{L/K}\Big(\alpha^n + \sum_{j=1}^{n} \alpha^{n-j} y_j\Big), \quad c \in K^*.$$

Sufficiency. If $F = F_1 F_2$, where $F_i \in K[y_1, \dots, y_n] \setminus K$, then

$$F(\tau_1, \dots, \tau_n) = \prod_{\nu=1}^{2} F_\nu(\tau_1, \dots, \tau_n),$$

and since $\tau_1, \dots, \tau_n$ are algebraically independent,

$$F_\nu(\tau_1, \dots, \tau_n) \notin K,$$

thus $F(\tau_1, \dots, \tau_n)$ is reducible over K.

If $F = cN_{K(\alpha)/K}(\alpha^n + \sum_{j=1}^{n} \alpha^{n-j} y_j)$, then

$$F(\tau_1, \ldots, \tau_n) = cN_{K(\alpha)/K}\Big(\prod_{i=1}^{n}(\alpha + x_i)\Big) = c\prod_{i=1}^{n} N_{K(\alpha)/K}(\alpha + x_i),$$

and since $n > 1$, $F(\tau_1, \ldots, \tau_n)$ is reducible over K.

The proof of Theorem 2 is based on two lemmas.

LEMMA 4. *For* $n = 3$, $\tau_1^2 + a\tau_2$ *is reducible over* K *only if either* $a = 0$, *or* $a = -3$, $\operatorname{char} K \neq 3$ *and* K *contains a primitive cubic root* ϱ *of* 1. *In the latter case*

$$\tau_1^2 + a\tau_2 = (x_1 + \varrho x_2 + \varrho^2 x_3)(x_1 + \varrho^2 x_2 + \varrho x_3). \tag{5}$$

Proof. Assuming reducibility we have

$$\tau_1^2 + a\tau_2 = (x_1 + \alpha x_2 + \beta x_3)(x_1 + \beta x_2 + \alpha x_3), \qquad \alpha, \beta \in K,$$

which gives

$$\alpha\beta = 1, \qquad \alpha + \beta = a + 2, \qquad \alpha^2 + \beta^2 = a + 2.$$

Hence

$$a + 2 = \alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha\beta = (a + 2)^2 - 2 = a^2 + 4a + 2,$$

so that $a(a + 3) = 0$, thus either $a = 0$, or $a = -3$ and $\operatorname{char} K \neq 3$. In the latter case $(x - \alpha)(x - \beta) = x^2 + x + 1$, hence α and β are two primitive cubic roots of 1. The identity (5) is easily verified. ∎

LEMMA 5. *For* $n = 3$, $\tau_2^2 + a\tau_1\tau_3$ *is reducible over* K *if and only if either* $a = 0$, *or* $a = -3$, $\operatorname{char} K \neq 3$ *and* K *contains a primitive cubic root* ϱ *of* 1. *In the latter case*

$$\tau_2^2 + a\tau_1\tau_3 = (x_2x_3 + \varrho x_1x_3 + \varrho^2 x_1x_2)(x_2x_3 + \varrho^2 x_1x_3 + \varrho x_1x_2). \tag{6}$$

Proof. We have

$$\tau_1^2 + a\tau_2 = \tau_3^2(\tau_2(x_1^{-1}, x_2^{-1}, x_3^{-1})^2 + a\tau_1(x_1^{-1}, x_2^{-1}, x_3^{-1})\tau_3(x_1^{-1}, x_2^{-1}, x_3^{-1})).$$

Therefore, if

$$\tau_2^2 + a\tau_1\tau_3 = f_1f_2, \qquad f_\nu \in K[x_1, x_2, x_3] \setminus K \qquad (\nu = 1, 2),$$

we obtain

$$\tau_1^2 + a\tau_2 = \tau_3 f_1(x_1^{-1}, x_2^{-1}, x_3^{-1})\tau_3 f_2(x_1^{-1}, x_2^{-1}, x_3^{-1}),$$

where $\tau_3 f_\nu(x_1^{-1}, x_2^{-1}, x_3^{-1}) \in K[x_1, x_2, x_3] \setminus K$, hence by Lemma 4 either $a = 0$, or $a = -3$, $\operatorname{char} K \neq 3$ and K contains a primitive cubic root ϱ of 1. The identity (6) is easily verified. ∎

Proof of Theorem 2. Necessity. If $\deg F = 1$, then since F is isobaric, $F = cy_i$, $c \in K^*$, $i \leq n$. If $c\tau_i$ is reducible in $K[x_1, \ldots, x_n]$, then $i = n$. If

$n \geq 5$, then Theorem 1 applies and either F is reducible or

$$F = cN_{K(\alpha)/K}\Big(\alpha^n + \sum_{j=1}^{n} \alpha^{n-j} y_j\Big), \qquad c \in K^*. \tag{7}$$

Since F is isobaric, we have $\alpha = 0$ and $F = cy_n$.

It remains to consider the case $2 \leq \deg F < n-1 \leq 3$, hence $n = 4$ and $\deg F = 2$. We distinguish the following subcases:

$$\begin{aligned}
&F = y_1^2 + ay_2 =: F_1, && a \neq 0,\\
&F = y_1y_2 + ay_3 =: F_2, && a \neq 0,\\
&F = ay_2^2 + by_1y_3 + cy_4 =: F_3, && ab \neq 0, \text{ or } ac \neq 0, \text{ or } bc \neq 0,\\
&F = y_2y_3 + ay_1y_4 =: F_4, && a \neq 0,\\
&F = y_3^2 + ay_2y_4 =: F_5, && a \neq 0.
\end{aligned}$$

We have $F_1(\tau_1, \tau_2) = x_4^2 + (a+2)\tau_1' + (\tau_1'^2 + a\tau_2')$, where $\tau_i' = \tau_i(x_1, x_2, x_3)$. If $F_1(\tau_1, \tau_2) = (x_4 + g)(x_4 + h)$, where g, h are linear forms over K in x_1, x_2, x_3, then $gh = \tau_1'^2 + a\tau_2'$, hence by Lemma 4, $a = -3$, $\operatorname{char} K \neq 3$ and without loss of generality

$$g = b(x_1 + \varrho x_2 + \varrho^2 x_3), \qquad h = b^{-1}(x_1 + \varrho^2 x_2 + \varrho x_3), \qquad b \in K^*.$$

Therefore,

$$b + b^{-1} = -1, \qquad b\varrho + b^{-1}\varrho^2 = -1, \qquad b\varrho^2 + b^{-1}\varrho = -1.$$

The first equation gives $b = \varrho$ or $b = \varrho^2$, thus either $b\varrho^2 + b^{-1}\varrho \neq -1$ or $b\varrho + b^{-1}\varrho^2 \neq -1$, a contradiction. Therefore $F_1(\tau_1, \tau_2)$ is irreducible over K. Since

$$F_1(\tau_1, \tau_2) = \tau_4^2 F_5(\tau_2(x_1^{-1}, \ldots, x_4^{-1}),\ \tau_3(x_1^{-1}, \ldots, x_4^{-1}),\ \tau_4(x_1^{-1}, \ldots, x_4^{-1})),$$

the same applies to $F_5(\tau_2, \tau_3, \tau_4)$ (cf. proof of Lemma 5).

We have further

$$F_2(\tau_1, \tau_2, \tau_3) = \tau_1' x_4^2 + (\tau_1'^2 + (a+1)\tau_2')x_4 + (\tau_1'\tau_2' + a\tau_3'),$$

hence, if $F_2(\tau_1, \tau_2, \tau_3)$ is reducible over K then

$$F_2(\tau_1, \tau_2, \tau_3) = (\tau_1' x_4 + b\tau_1'^2 + c\tau_2')(x_4 + d\tau_1'), \qquad b, c, d \in K,$$

and

$$\tau_1'\tau_2' + a\tau_3' = bd\tau_1'^3 + cd\tau_1'\tau_2'.$$

Since $\tau_1', \tau_2', \tau_3'$ are algebraically independent, it follows that $a = 0$, a contradiction. Therefore $F_2(\tau_1, \tau_2, \tau_3)$ is irreducible over K. Since

$$F_2(\tau_1, \tau_2, \tau_3) = \tau_4^2 F_4(\tau_1(x_1^{-1}, \ldots, x_4^{-1}), \ldots, \tau_4(x_1^{-1}, \ldots, x_4^{-1}))$$

the same applies to $F_4(\tau_1, \ldots, \tau_4)$ (cf. proof of Lemma 5).

It remains to consider F_3. We have

$$F_3(\tau_1,\dots,\tau_4) = a(\tau_1'x_4+\tau_2')^2 + b(x_4+\tau_1')(\tau_2'x_4+\tau_3') + c\tau_3'x_4$$
$$= (a\tau_1'^2+b\tau_2')x_4^2 + ((2a+b)\tau_1'\tau_2' + (b+c)\tau_3')x_4 + (a\tau_2'^2+b\tau_1'\tau_3').$$

If $a\tau_1'^2+b\tau_2'$ were the leading coefficient with respect to x_4 of a proper factor over K of $F_3(\tau_1,\dots,\tau_4)$, then since it does not divide $a\tau_2'^2+b\tau_1'\tau_3'$, the complementary factor of $F_3(\tau_1,\dots,\tau_4)$ would be $x_4+d\tau_1'$, $d\in K^*$, which implies $a=0$, $b\tau_1'\tau_2'+(b+c)\tau_3' = bd\tau_1'\tau_2'+(b/d)\tau_3'$, $d=1$, $c=0$, a contradiction.

If $a\tau_1'^2+b\tau_2'$ is not the leading coefficient of any proper factor of $F_3(\tau_1,\dots,\tau_4)$ and the latter polynomial is reducible over K, then $a\tau_1'^2+b\tau_2'$ is reducible over K, hence, by Lemma 4, either $b=0$, or $b=-3a$, $\operatorname{char} K\neq 3$ and K contains a primitive cubic root ϱ of 1. In the former case

$$F_3(\tau_1,\dots,\tau_4) = a(\tau_1'x_4+d_1\tau_1'^2+e_1\tau_2')(\tau_1'x_4+d_2\tau_1'^2+e_2\tau_2');$$
$$a(d_1\tau_1'^2+e_1\tau_2')(d_2\tau_1'^2+e_2\tau_2') = a\tau_2'^2;\qquad d_1=d_2=0,$$
$$(ae_1+ae_2)\tau_1'\tau_2' = 2a\tau_1'\tau_2'+c\tau_3',\qquad c=0,\qquad \text{a contradiction.}$$

In the latter case, by Lemmas 4 and 5, either

$$F_3(\tau_1,\dots,\tau_4) = a((x_1+\varrho x_2+\varrho^2x_3)x_4 + d(x_2x_3+\varrho x_1x_3+\varrho^2x_1x_2))$$
$$\times((x_1+\varrho^2x_2+\varrho x_3)x_4 + d^{-1}(x_2x_3+\varrho^2x_1x_3+\varrho x_1x_2))$$

or

$$F_3(\tau_1,\dots,\tau_4) = a((x_1+\varrho^2x_2+\varrho x_3)x_4 + d(x_2x_3+\varrho^2x_1x_3+\varrho x_1x_2))$$
$$\times((x_1+\varrho^2x_2+\varrho x_3)x_4 + d^{-1}(x_2x_3+\varrho x_1x_3+\varrho^2x_1x_2)).$$

In the first subcase

$$d(x_2x_3+\varrho x_1x_3+\varrho^2x_1x_2)(x_1+\varrho^2x_2+\varrho x_3)$$
$$+ d^{-1}(x_2x_3+\varrho^2x_1x_3+\varrho x_1x_2)(x_1+\varrho x_2+\varrho^2x_3)$$
$$= -\tau_1'\tau_2'+(c/a-3)\tau_3',$$

in the second subcase

$$d(x_2x_3+\varrho^2x_1x_3+\varrho x_1x_2)(x_1+\varrho^2x_2+\varrho x_3)$$
$$+ d^{-1}(x_2x_3+\varrho x_1x_3+\varrho^2x_1x_2)(x_1+\varrho x_2+\varrho^2x_3)$$
$$= -\tau_1'\tau_2'+(c/a-3)\tau_3'.$$

In both subcases, the right-hand side is invariant with respect to the conjugation $\varrho\mapsto\varrho^2$ and to any permutation $\sigma\in\mathfrak{S}_3$. The first condition implies $d=\pm1,\pm\varrho,\pm\varrho^2$, the second condition eliminates the second subcase and in the first subcase restricts d to ±1. Thus we obtain

$$d(6x_1x_2x_3 - x_1^2x_2 - x_2^2x_3 - x_3^2x_1 - x_1x_2^2 - x_2x_3^2 - x_3x_1^2)$$
$$= -\tau_1'\tau_2'+(c/a-3)\tau_3',$$

$$d(9\tau_3' - \tau_1'\tau_2') = -\tau_1'\tau_2' + (c/a - 3)\tau_3', \quad d = 1, \quad c = 12a.$$

Sufficiency. In view of Theorem 1 it suffices to consider $n = 4$ and $F = y_2^2 - 3y_1y_3 + 12y_4$. Then

$$F(\tau_1, \ldots, \tau_4) = (x_1x_4 + x_2x_3 + \varrho(x_2x_4 + x_1x_3) + \varrho^2(x_3x_4 + x_1x_2)) \times (x_1x_4 + x_2x_3 + \varrho^2(x_2x_4 + x_1x_3) + \varrho(x_3x_4 + x_1x_2)).$$

EXAMPLE. Take $F = \sum_{i=2}^{n}(-1)^i x_1^{n-i}x_i$. We have $\deg F = n - 1$ and

$$F(\tau_1, \ldots, \tau_n) = \prod_{i=1}^{n}(\tau_1 - x_i).$$

This example also shows that the estimate in Lemma 3 cannot be improved.

References

[1] R. Fricke, *Lehrbuch der Algebra*, Vieweg, Braunschweig, 1924.
[2] L. Smith, *Polynomial Invariants of Finite Groups*, A K Peters, Wellesley, MA, 1995.

A. Schinzel
Institute of Mathematics
Polish Academy of Sciences
P.O. Box 21
00-956 Warszawa, Poland
E-mail: schinzel@impan.gov.pl

Received December 13, 2005 (7494)