THE GALOIS GROUP OF $f(x^r)$

by S. D. COHEN and W. W. STOTHERS

(Received 23 September, 1982)

1. Introduction. Let $f(x)$ be an irreducible polynomial of degree n with coefficients in a field L and r be an integer prime to the characteristic of L. The object of this paper is to describe the galois group $\mathcal{G}$ of $f(x^r)$ over L when the galois group G of $f(x)$ itself over L is either the full symmetric group S_n or the alternating group A_n. We shall call f *standard* if $G = S_n$ or A_n with $|G| \geq 2$.

Denote† by $\mathbf{x} = \{x_1, \ldots, x_n\}$ the zeros of f (in a splitting field) and put $\mathbf{y} = \{y_1, \ldots, y_n\}$, where, for each $i = 1, \ldots, n$, y_i is any solution of $y_i^r = x_i$. Then the splitting field of $f(x^r)$ can be obtained by adjoining to L the set $\mathbf{y}$ along with all rth roots of unity. Henceforth, we assume that L already contains ζ_r, a primitive rth root of unity, so that this splitting field is $L(\mathbf{y})$ itself. Also put

$$\nu = \nu(f) = \frac{(-1)^n f(0)}{\text{leading coefficient of } f} \; (= x_1 \ldots x_n)$$

and note that $L(\mathbf{y})$ always contains $\sqrt[t]{\nu}$.

Let $H(r)$ be the galois group of $f(x^r)$ over $L(\mathbf{x})$. As part of an earlier investigation, the first author [**2**, Lemma 5] showed that, if $G = S_n$, then there are essentially only two possibilities for $H(r)$. In the simplest case (when r is prime) we have either

(I) $H_r = C_r^{n-1} \times C_t$, where

$$t = \begin{cases} 1, & \text{if } \sqrt[t]{\nu} \in L \text{ or if } r = 2 \text{ and } \nu = (\text{discriminant of } f) \quad (\text{square in } L), \\ r, & \text{otherwise,} \end{cases}$$

or

(II) $H(r) = C_r$, which occurs when $L(\mathbf{y}) = L(\mathbf{x}, y_1)$.

We refer to these as type I (the "generic" case) and type II even when r is composite.

In [**2**], no specific occurrence of a polynomial of type II was provided, but, in fact, there is an obvious potential source. Define $\mathcal{S}(r)$ by

$$\mathcal{S}(r) = \{f(x) \in L[x]; f(x) \mid (x^i F_1^r(x) - \alpha F_2^r(x)),$$
$$\text{for some } i \text{ prime to } r, \text{ co-prime polynomials}$$
$$F_1 \text{ and } F_2 \text{ over } L \text{ and } \alpha (\neq 0) \in L\}.$$

(Actually, in this definition, we can assume $i = 1$; see §2.) Here evidently $L(\mathbf{y}) = L(\mathbf{x}, \sqrt[t]{\alpha})$ and so $H(r) \subseteq C_r$.

In §2 we describe $H(r)$ precisely when f is a *standard* polynomial in $\mathcal{S}(r)$ and exhibit examples of arbitrary degree. In particular, $H(r)$ may occasionally be slightly smaller than

† Note that except in two obvious places at the beginning of §2, x and (later) y are indeterminates over L; subscripted symbols x_1, x_i, y_1, etc., are specialisations of them in an algebraic extension of L.

is immediately apparent. An instance occurring when L is the function field $\mathbb{C}(w)$, w an indeterminate, is the polynomial

$$(x-2)^3(x+2)-16w^3(x+1)^3$$

(actually in $\mathcal{S}(3)$) for which $G=A_4$ yet $H(3)$ is trivial.

In general, the reduction into polynomials of types I or II remains valid for all standard polynomials (even those with $G=A_n$); see §3. However, if $G=S_2$, a polynomial of type I with $t=1$ can have formally the same group $H(r)$ as one of type II. Moreover, if $G=A_3$, the basic argument of [**2**] actually breaks down and a third properly distinct possibility for $H(r)$ arises, namely $H(r)=C_r\times C_t$ (when r is prime, $t=1$ or r) although $H(r)$ is then formally indistinguishable from that of either a type I or a type II polynomial (see §5). For the sake of tidiness, we usually exclude these cases and assume that $|G|>3$.

The fact that, normally, a standard polynomial for which $H(r)\subseteq C_r$ must be in $\mathcal{S}(r)$ is the core of the paper (§4). However, there are some interesting exceptions when $n=4$ and $r=2$ and, in general, when $n=4$ and r is even we can prove only that f always belongs to $\mathcal{S}(r/2)$. We illustrate with two examples in which again $L=\mathbb{C}(w)$. The polynomial

$$x(x+2i\sqrt{2})(x+4+i\sqrt{2})^2-27w(\notin\mathcal{S}(2))$$

has $G=S_4$ yet $H(2)=C_2$. Further, the galois group of

$$(x-1)^3(x+3)-16wx(\notin\mathcal{S}(2))$$

is A_4 while $H(2)=C_2$.

In §5, we synthesise the preceding discussion and classify $H(r)$ in general. We summarise the conclusions as follows.

THEOREM 1. *Let r be a positive integer and L a field containing ζ_r whose characteristic is prime to r. Let f be a standard polynomial of degree n over L with $|G|>3$ and suppose that s is the greatest divisor of r for which $f\in\mathcal{S}(s)$. Then there exist integers q, t with $q\mid s$, $t\mid r/s$ for which $H(r)$ is an extension of $C_{r/s}^{n-1}\times C_t$ by C_q. Alternatively, if $n=4$ and r/s is even, $H(r)$ is an extension of $C_{r/(2s)}^3\times C_{t/2}$ by C_{2q}.*

The full significance of the integers q, t will emerge later but certainly, if $f(x)$ divides $x^iF_1^s(x)-\alpha F_2^s(x)$ and $\alpha=\beta^d$ $(\beta\in L)$, then $q\mid s/d$.

Because they were inspired by Riemann surface considerations, the examples constructed generally have $L=\mathbb{C}(w)$. Of course $\mathbb{C}$ could be replaced by any suitable field such as an algebraic number field or even a field of non-zero characteristic. Indeed, by specialising using Hilbert's irreducibility theorem, one could demonstrate the existence of similar examples with L an algebraic number field, often $\mathbb{Q}(\zeta_r)$ itself.

2. The group $H(r)$ when $f\in\mathcal{S}(r)$. Note first that, if $(i,r)=1$ and u and v are integers for which $ui+vr=1$, then

$$x^i\frac{F_1^r(x)}{F_2^r(x)}=\alpha\quad(x\in L,\ xF_2(x)\neq 0)$$

https://doi.org/10.1017/S0017089500005449 Published online by Cambridge University Press

implies that

$$x\left\{\frac{F_1^u(x)}{x^v F_2^u(x)}\right\}^r = \alpha^u$$

and so

$$\mathscr{S}(r) = \{f(x) : f(x) \mid (xF_1^r(x) - \alpha F_2^r(x)),\ \alpha(\neq 0) \in L,\ F_1, F_2 \text{ co-prime}\}. \tag{1}$$

Next, it is obvious that, if $r_1 \mid r$, then $\mathscr{S}(r) \subseteq \mathscr{S}(r_1)$.

LEMMA 2. *If* $(r_1, r_2) = 1$, *then* $\mathscr{S}(r_1) \cap \mathscr{S}(r_2) = \mathscr{S}(r_1 r_2)$.

Proof. Let $ur_1 + vr_2 = 1$. Suppose f divides both $xF_1^{r_1}(x) - \alpha F_2^{r_1}(x)$ and $xG_1^{r_2}(x) - \beta G_2^{r_2}(x)$. Then a zero x of f satisfies

$$x\left\{\left(\frac{F_1}{F_2}\right)^u \left(\frac{G_1}{G_2}\right)^v\right\}^{r_1 r_2}(x) = \alpha^u \beta^v$$

and the result follows.

For a given f let s (as in Theorem 1) be the largest divisor of r for which $f \in \mathscr{S}(s)$. A particular consequence of Lemma 2 is that when $d \mid r$, $f \in \mathscr{S}(d)$ if and only if $d \mid s$.

Suppose now that f is a standard polynomial in $\mathscr{S}(r)$ and that, in fact, $f(x)$ divides $xF_1^r(x) - \alpha F_2^r(x)$. Certainly the splitting field of $f(x^r)$ over L is $L(\mathbf{x}, \sqrt[r]{\alpha})$. Let r^* be the divisor of r such that, as an rth power residue, α is at most an r/r^*th power in L. Then obviously $H(r) \subseteq C_{r^*}$ but the containment may be proper. For this purpose, define $q = q_r(\alpha, L)$ as follows. If $G \neq A_3$ or A_4, q is the least divisor of r for which α can be written in one of the forms $\beta^{r/q}$ or $(\beta\sqrt{D})^{r/q}$, where $\beta \in L$ and D is the discriminant of f (in L). If $G = A_3$ or A_4, f possesses an invariant C in L with the property that $L(\sqrt[3]{C})$ is a cubic extension of L contained in $L(\mathbf{x})$, see e.g. [**5**, §§7,10]. In these cases, define q as the minimal divisor of r for which α can be written in one of the forms

$$\alpha = (\beta\sqrt[3]{(C^i)})^{r/q}, \qquad \beta \in L, \qquad i = 0, 1, 2.$$

It follows that $q = r^*$ unless $G = S_n$ and r^* is even when $q = r^*$ or $r^*/2$, or $G = A_3$ or A_4 and $3 \mid r^*$ when $q = r^*$ or $r^*/3$. Of course, $xF_1^r(x) - \alpha F_2^r(x)$ is not uniquely determined by f and r. However, it follows from our results that $q_r(\alpha, L)$ is and we write $q_r(f)$ for this number.

THEOREM 3. *Suppose* f *is a standard polynomial in* $\mathscr{S}(r)$. *Then* $H(r) = C_q$, *where* $q = q_r(f)$.

Proof. Suppose $f(x)$ divides $xF_1^r(x) - \alpha F_2^r(x)$ so that the splitting field of $f(x^r)$ over L is $L(\mathbf{x}, \sqrt[r]{\alpha})$. By the theorem of natural irrationalities, if $K = L(\mathbf{x}) \cap L(\sqrt[r]{\alpha})$, then $H(r) \cong \text{gal}(L(\sqrt[r]{\alpha})/K)$. Of course, K/L is a cyclic extension of order dividing r^* and

$$G/\text{gal}(L(\mathbf{x})/K) \cong \text{gal}(K/L).$$

Since $G = S_n$ or A_n, this implies that, if $K \neq L$, then either $G = S_n$ and $K = L(\sqrt{D})$ or $G = A_3$ or A_4 and $K = L(\sqrt[3]{C})$ [**4**, §5]. Now, by definition, $\alpha = \gamma^{r/r^*}$, where $\gamma \in L$. If $K = L(\sqrt{D})$, then obviously $\gamma = D \times$(square in L), while, if $K = L(\sqrt[3]{C})$, then $\gamma = C^i \times$(cube in L), $i = 1$ or 2. The result follows.

https://doi.org/10.1017/S0017089500005449 Published online by Cambridge University Press

To indicate the scope of Theorem 3, we show that for any r there are indeed standard polynomials of any degree in $\mathcal{S}(r)$ including some with $q = r^*/2$ or $r^*/3$ as permitted by Theorem 3. We take L to be a function field $L_0(w)$ and consider in the first place polynomials in $\mathcal{S}(r)$ of the form

$$f_w(x) = a(w)(x^i F_1^r(x) - AwF_2^r(x)), \qquad F_2(0) \neq 0,$$

calling then *genus zero* polynomials (because $L(x_1) = L_0(x_1)$, where $f_w(x_1) = 0$, has genus zero over L). For a genus zero polynomial, either $r \mid n$ or $(n, r) = 1$. Of course, if $n \geq 3$ and f is a standard polynomial over L then $f(x)/(x - x_1)$ is a standard polynomial over $L(x_1)$ and thus our construction will establish the existence (for appropriate L) of standard polynomials in $\mathcal{S}(r)$ of any degree. We use the fact [**2**, Lemma 7], that, if L_0 is algebraically closed, then to any $\alpha \in L_0 \cup \{\infty\}$ for which $f_\alpha(x)$ is not square-free, there is an element of G (a permutation of the zeros $x_1, \ldots, x_n$) which corresponds to the factorisation of $f_\alpha(x)$. Indeed, G is generated by such elements if L_0 has characteristic zero.

We remark here that it is a straightforward exercise to show that the genus zero polynomial $f_w(x) \notin \mathcal{S}(r_1)$ for any $r_1 > r$, unless $F_1 = h^{r_1/r}F_2$, say.

EXAMPLE 1. Let $L = \mathbb{C}(w)$. For any $m \geq 1$, put $n = mr$ and

$$f(x) = (x^m + rm - 1)^r - (rm)^r wx.$$

Considering the singularity at $w = \infty$ we see that G contains an $(n-1)$-cycle. Now

$$x^2 \frac{d}{dx}\left(\frac{(x^m + rm - 1)^r}{x}\right) = (rm - 1)(x^m - 1)(x^m + rm - 1)^{r-1},$$

whose zero at any mth root of unity ζ gives rise to a simple singularity at $w = 1/\zeta$. Hence G certainly contains transpositions and so $G = S_n$. Further, the discriminant is $bw^{m(r-1)}(w^r - 1)$ $(b \in \mathbb{Z})$ so that $H(r) = C_r$. Actually, since f is rationally defined we can take $L = \mathbb{Q}(\zeta_r, w)$ and still have $G = S_n$ and $H(r) = C_r$.

EXAMPLE 2. For any m, i with $(i, r) = 1$ put $n = mr + i$ and define

$$f_w(x) = x^i F^r(x) - Aw,$$

where

$$F(x) = \sum_{j=0}^{m} \binom{m}{j} \frac{x^j}{jr + i}$$

and

$$A = (-1)^i F^r(-1) = (-1)^i \left(\frac{r^m m!}{i(i+r)\ldots(i+mr)}\right)^r.$$

We then have

$$f_w'(x) = x^{i-1} F^{r-1}(x)(x+1)^m.$$

In particular, $f_1(x) = (x+1)^{m+1} g(x)$, where g is square-free. Hence G contains an $(m+1)$-cycle. A straightforward, though messy, argument (which works for any F not of the form cx^u) shows that $x^i F^r(x)$ is functionally indecomposable and so by [**3**, Lemma 2] G is

https://doi.org/10.1017/S0017089500005449 Published online by Cambridge University Press

primitive. Thus [**6**, Theorem 13.8] G is certainly $(n-m)$-transitive. Hence, if G is not standard, then by [**1**, p. 150]

$$n-m \leq \tfrac{1}{3}n+1$$

which (for $r \geq 2$) can only happen if $i=1$, $r=2$, $m=1$ and $n=3$ in which case G contains a transposition and so must be S_3. Taking account of the remaining ramification at 0 and ∞, we see that $D = c[w^{r-1}(w-1)]^m$ $(c \in \mathbb{Z})$. Thus, if $L = \mathbb{C}(w)$, then

$$G = \begin{cases} S_n, & \text{if } m \text{ is odd,} \\ A_n, & \text{if } m \text{ is even,} \end{cases}$$

while clearly $H(r) = C_r$. Again f_w is rationally defined and so, if $L = \mathbb{Q}(\zeta_r, w)$, the above still holds at least if m is odd; the only modification when m is even being that $G = S_n$ unless c is a square in $\mathbb{Q}(\zeta_r)$.

Actually, if i is negative (when we are really considering $F^r(x) - Ax^i w$, $(j, r) = 1$, so that $n = \max(mr, j)$), then the above description is still essentially valid; in particular, G possesses an $(m+1)$-cycle and so is $(n-m)$-transitive, whence $G = S_n$ or A_n.

As another variation, consider $f_{w^r+1}(x)$ over $\mathbb{C}(w)$ with m odd and r even. The discriminant becomes $c[(w^r+1)^{r-1}w^r]^m$ and still $G = S_n$ but now $q_r(f) = r/2$ since $w^r + 1 = (\beta\sqrt{D})^2$, where

$$\beta = c_1 \frac{(w^r+1)^{\frac{1}{2}[1-(r-1)m]}}{w^{\frac{1}{2}rm}}, \quad c_1 \in \mathbb{C}.$$

Hence $H(r) = C_{r/2}$. A genus zero occurrence of this phenomenon with $r=2$ is provided in the next example.

EXAMPLE 3. For any $m \geq 2$ and appropriate $A(\neq 0) \in \mathbb{C}$ put $n = 2m$ and

$$f(x) = x(x+1)^{2m-2} - w(x+A)^{2m}$$

over $\mathbb{C}(w)$. There is, of course, ramification at $w=0$ and $w=\infty$. The remaining ramification arises from the zeros of $x^2 + (2m-1)(1-A)x - A$. Choose A so that this quadratic is a square, e.g. put

$$A = 1 - \frac{2+4\sqrt{(m-m^2)}}{(2m-1)^2}.$$

If B is the corresponding value of w, the ramification at $w=B$ indicates that G possesses a 3-cycle (and so $A_n \subseteq G$) while $D = cw^{2m-3}(w-B)^2$. Thus, in fact, $G = S_n$ yet $H(2)$ is trivial.

EXAMPLE 4. With $n=4$ and $r=3$ put

$$f_w(x) = x(x+4)^3 - 16w(x+1)^3.$$

Then $D = -3[48w(w-1)]^2$. Solving explicitly, one finds that $G = A_4$ over $\mathbb{Q}(\zeta_r, w) = \mathbb{Q}(\sqrt{(-3)}, w)$ with a splitting field containing $\sqrt[3]{(4w(w-1))}$. Thus $H(3) = C_3$. On the other hand, if $g = f_{w^3+1}$, then still $G = A_4$ but $q_3(g) = 1$ and so $H(3)$ is trivial. This provides an example of a standard polynomial in Theorem 2 with $q = r^*/3$. In an alternative form,

https://doi.org/10.1017/S0017089500005449 Published online by Cambridge University Press

noted in the introduction, namely

$$f_{w^3+1}(x) = (x-2)^3(x+2) - 16w^3(x+1)^3$$

the triviality of $H(3)$ is particularly well-disguised.

3. The basic result. In this section we examine and modify the argument of Lemma 5 of [**2**].

Let f be a standard polynomial over L such that $f(x^r)$ has splitting field $L(\mathbf{y})$ as described in §1. It was noted there that certainly $\sqrt[r]{\nu} \in L(\mathbf{y})$. Further, given r, define u as the least divisor of r for which $L(\mathbf{y}^u) = L(\mathbf{x}, y_1^u)$, where $\mathbf{y}^u = \{y_1^u, \ldots, y_n^u\}$. (Since G is transitive any y_i, $1 \le i \le n$, can take the place of y_1.) Then certainly $H(r/u) \subseteq C_{r/u}$.

LEMMA 4. *Suppose that f is a standard polynomial with $G \neq A_3$. Then*

$$\mathrm{gal}(f(x^r), L(\mathbf{y}^u, \sqrt[r]{\nu})) = C_u^{n-1}.$$

Proof. Obviously, we can assume $u > 1$. Fix m as the largest integer with $0 \le m \le n-1$ such that

$$\mathrm{gal}(L(\mathbf{y}^u, y_1, \ldots, y_m)/L(\mathbf{y}^u)) = C_u^m.$$

It suffices to prove that $m = n-1$ so assume that $0 \le m \le n-2$. For some divisor d of u with $d < u$, we have

$$y_{m+1}^d \in L(\mathbf{y}^u, y_1, \ldots, y_m).$$

The argument now proceeds as in [**2**]. If $m \ge 1$, the monomials

$$\mathbf{Y}^{\mathbf{j}} = y_1^{j_1} \ldots y_m^{j_m} (0 \le j_i \le u-1, 1 \le i \le m)$$

form a basis of $L(\mathbf{y}^u, y_1, \ldots, y_m)$ over $L(\mathbf{y}^u)$. Thus y_{m+1}^d has a unique expansion in the form

$$y_{m+1}^d = \sum_{\mathbf{j}} a_{\mathbf{j}} \mathbf{Y}^{\mathbf{j}}, \qquad a_{\mathbf{j}} \in L(\mathbf{y}^u).$$

Suppose that $a_{\mathbf{j}}$ and $a_{\mathbf{j}'}$ are both non-zero, where $\mathbf{j} \neq \mathbf{j}'$, say with $j_1 \neq j_1'$. By the definition of m, there exist $\sigma \in G = \mathrm{gal}(L(\mathbf{y})/L)$ and a primitive uth root of unity ζ such that $\sigma(y_1) = \zeta y_1$, $\sigma(y_i) = y_i$ $(1 < i \le m)$ while $\sigma(y_i^u) = y_i^u$, $1 \le i \le n$. Thus $\sigma(y_{m+1}) = \zeta^e y_{m+1}$, say. The identity

$$\sigma(y_{m+1}^d) - \zeta^{de} y_{m+1} = 0$$

now leads to a contradiction of the basis property of the $\mathbf{Y}$ as in [**2**]. Thus

$$y_{m+1}^d = a y_1^{j_1} \ldots y_m^{j_m} \ (a \in L(\mathbf{y}^u), 0 \le j_i \le u-1, i = 1, \ldots, m).$$

We rewrite this as

$$y_1^{d_1} \ldots y_n^{d_n} \in L(\mathbf{y}^u), \qquad (0 \le d_i \le u-1, i = 1, \ldots, n), \tag{2}$$

where the d_i are not all equal (since $m < n-1$, $d_{m+1} > 0$ and $d_n = 0$). Further, this remains valid even if $m = 0$.

https://doi.org/10.1017/S0017089500005449 Published online by Cambridge University Press

The following section of the argument applies to all standard f with $n \geq 4$. A simpler treatment using only transpositions, works for $G = S_n$ $(n \geq 2)$ and is omitted; see [**2**].

Suppose that the d_i's in (2) are pairwise distinct. Then the integers $2d_i$, $i = 2, 3, 4$ are not all congruent (mod u) and so $2(d_1 + d_i) \not\equiv d_1 + d_2 + d_3 + d_4 \pmod{u}$ for some $i = 2, 3, 4$. Renumbering if necessary, we may assume that $d_1 + d_2 \not\equiv d_3 + d_4 \pmod{u}$. Let τ be any extension to $\mathcal{G}$ of the element (12) (34) of G, where the action is on the subscripts of $x_1, \ldots, x_n$. Then certainly τ is an automorphism of $L(\mathbf{y}^u)$. Applying τ to (2) we see that

$$y_2^{d_1} y_1^{d_2} y_4^{d_3} y_3^{d_4} y_5^{d_5} \ldots y_n^{d_n} \in L(\mathbf{y}^u)$$

and hence

$$y_1^{d_1+d_2} y_2^{d_1+d_2} y_3^{d_3+d_4} y_4^{d_3+d_4} y_5^{2d_5} \ldots y_n^{2d_n} \in L(\mathbf{y}^u) \tag{3}$$

Now since $d_1 + d_2 \not\equiv d_3 + d_4 \pmod{u}$, on reducing the indices in (3) modulo u and renumbering, we see that, in any case, we can assume (2) holds with $d_1 \neq d_2 = d_3$. Now, to (2) apply an extension of $(123)(\in G)$ to $\mathcal{G}$ and conclude that

$$y_2^{d_1} y_3^{d_2} y_1^{d_2} y_4^{d_4} \ldots y_n^{d_n} \in L(\mathbf{y}^u).$$

Along with (2) itself, this yields

$$\left(\frac{y_2}{y_1}\right)^{d_1 - d_2} \in L(\mathbf{y}^u) = L(\mathbf{x}, y_1^u),$$

where $0 < |d_1 - d_2| < u$. Put $u^* = (d_1 - d_2, u)$ so that $u^* \mid u$ but $u^* < u$. Then certainly $y_2^{u^*} \in L(\mathbf{x}, y_1^{u^*})$. Since G is at least 2-transitive, this implies that $L(\mathbf{y}^{u^*}) = L(\mathbf{x}, y_1^{u^*})$ which contradicts the definition of u. Thus $m = n - 1$ and the result is proved.

A consequence of Lemma 4 is that, provided $G \neq S_2$, then type II polynomials are characterised by $H(r) \subseteq C_r$ without specifying that necessarily $L(\mathbf{y}) = L(\mathbf{x}, y_1)$.

COROLLARY 5. *Suppose that f is a standard polynomial with $|G| > 3$ and such that $H(r) \subseteq C_r$. Then $L(\mathbf{y}) = L(\mathbf{x}, y_1)$.*

Proof. The group C_u^{n-1} in Lemma 4 is a subgroup of $H(r)$ and, since $n - 1 > 1$, cannot be cyclic unless $u = 1$.

4. Type II polynomials. We begin with a weak version of Theorem 3 for general polynomials of type II. For any f, define r^* to be the degree of the cyclic extension $L(y_1)/L(x_1)$. This is consistent with the usage in §2 for $f\mathcal{S}(r)$. Of course $r^* \mid r$.

LEMMA 6. *Let f be a standard polynomial with $|G| > 3$ and suppose that $H(r) \subseteq C_r$. Then*

(i) *either* (a) $H(r) = C_{r^*}$, *or* (b) $G = S_n$, r^* *is even and* $H(r) = C_{r^*/2}$, *or* (c) $n = 4$ *or* 5, $G = A_n$, $3 \mid r^*$ *and* $H(r) = C_{r^*/3}$;

(ii) $y_2/y_1 \in L(\mathbf{x})$.

Proof. (i) Observe first that $\mathrm{gal}(L(\mathbf{x})/L(x_1)) = S_{n-1}$ or A_{n-1}. By Corollary 5 $L(\mathbf{y}) = L(\mathbf{x}, y_1)$. Hence, since $L(\mathbf{y})$ is normal over $L(x_1)$, the theorem of natural irrationalities

https://doi.org/10.1017/S0017089500005449 Published online by Cambridge University Press

implies that

$$H(r) \cong \mathrm{gal}(L(y_1)/L(y_1) \cap L(\mathbf{x})) \subseteq C_{r^*}.$$

Of course, if $L(y_1) \cap L(\mathbf{x}) = L(x_1)$, then $H(r) = C_{r^*}$. On the other hand, if $L(\mathbf{x}) \subseteq L(y_1)$, then $L(\mathbf{y}) = L(y_1)$ and

$$C_{r^*}/H(r) \cong \mathrm{gal}(L(\mathbf{x})/L(x_1)) = S_{n-1} \text{ or } A_{n-1}$$

from which it follows that either $G = S_3$ and $H(r) = C_{r^*/2}$ (r^* even) or $G = A_4$ and $H(r) = C_{r^*/3}$ ($3 \mid r^*$). The remaining possibility is that $\mathrm{gal}(L(\mathbf{x})/L(x_1))/\mathrm{gal}(L(\mathbf{x})/L(\mathbf{x}) \cap L(y_1))$ is a non-trivial cyclic quotient of S_{n-1} or A_{n-1} which (cf. Proof of Theorem 3) forces $G = S_n$ and $H(r) = C_{r^*/2}$ or $G = A_5$ and $H(r) = C_{r^*/3}$.

(ii) Let $H(r) = C_q$, where $q \mid r$. Actually, by (i), $q = r^*$, $r^*/2$ or $r^*/3$. By Corollary 5, $\{1, y_1, \ldots, y_1^{q-1}\}$ is a basis for $L(\mathbf{y})$ over $L(\mathbf{x})$. Thus y_2 has a unique expansion in the form

$$y_2 = \sum_{i=0}^{q-1} a_i(\mathbf{x}) y_1^i, \; a_i(\mathbf{x}) \in L(\mathbf{x}).$$

A simpler version of the argument used in Lemma 4 now implies that, for some m with $(m, q) = 1$

$$y_2 = a(\mathbf{x}) y_1^m, \qquad a(\mathbf{x}) \in L(\mathbf{x}).$$

Consequently,

$$x_2 = a^r(\mathbf{x}) x_1^m, \qquad (m, q) = 1. \tag{4}$$

Certainly G is doubly transitive and $n \geq 3$. It follows that we may apply to (4) any member of G which fixes x_1 and maps x_2 onto x_3 to obtain

$$x_3 = b^r(\mathbf{x}) x_1^m, \qquad b(\mathbf{x}) \in L(\mathbf{x}),$$

whence

$$x_3 = \left(\frac{a(\mathbf{x})}{b(\mathbf{x})}\right)^r x_2.$$

Again using the fact that G is doubly transitive, we deduce (ii).

It is easy to see that Lemma 6(ii) can be reformulated as "$\mathcal{G}$ is a central extension of $H(r)$" (i.e. $H(r)$ is contained in the centre of $\mathcal{G}$). This feature characterises type II polynomials. What follows is an attempt to show that, in general, a standard type II polynomial is actually in $\mathcal{S}(r)$. This would be equivalent to the group-theoretical fact that the above central extension splits with complement S_n or A_n. Relevant here is the Schur multiplier or multiplicator of S_n or A_n which is known (see [**4**, §25]) and which indicates by how much an abstract extension $\mathcal{G}$ by S_n or A_n may fail to split. Indeed, this approach does throw some light on the nature of our results. However, we do not pursue it here because, in our specialised situation, it turns out that the worst does not usually occur and it seems one makes only partial progress towards a classification using group theory alone. Suffice it to remark that, if $G = S_3$, then the Schur multiplier of G is trivial and so the extension splits. An elementary proof of this is incorporated in the discussion which follows.

We concentrate now on the relationship between type II polynomials and those in $\mathcal{S}(r)$. As a final preliminary, we consider two easy special cases.

LEMMA 7. *Suppose $n = 3$ or 4 and f is a polynomial with $G = S_3$ or A_4 and $(n, r) = 1$. Suppose also that $H(r) \subseteq C_r$. Then $f \in \mathcal{S}(r)$.*

Proof. Both cases go the same way. We therefore illustrate by considering only $G = A_4$. Let $\sigma = (234) \in G$. Then σ generates the stabiliser of x_1. By Lemma 6(ii), $x_2 = a^r x_1$, where $a \in L(\mathbf{x})$ and hence

$$\nu = x_1 x_2 x_3 x_4 = b^r x_1^4,$$

where $b = a\sigma(a)\sigma^2(a)$ is fixed by σ and so $b = b(x_1) \in L(x_1)$. Accordingly, x_1 satisfies an equation of the form

$$b^r(x)x^4 = \nu, \tag{5}$$

where $\nu \in L$. Since r is odd, (5) cannot be an identity and so by (1) the result holds.

THEOREM 8.† *Suppose that f is a standard polynomial with $|G| > 3$ and $H(r) \subseteq C_r$. Then either $f \in \mathcal{S}(r)$ or $n = 4$, r is even and $f \in \mathcal{S}(r/2)$.*

Proof. By Lemma 6(ii), x_2/x_1 is an rth power in $L(\mathbf{x})$. We consider two cases.

Case (a). x_2/x_1 is an rth power in $L(x_1, x_2)$.

Observe that, if $G = S_3$ or A_4, then $L(\mathbf{x}) = L(x_1, x_2)$ and so case (a) always applies. Actually, by Lemmas 2 and 7, we may even assume that

$$\begin{cases} \text{if} \quad G = S_3, & \text{then } r \text{ is a power of 3,} \\ \text{if} \quad G = A_4, & \text{then } r \text{ is a power of 2.} \end{cases} \tag{6}$$

We return to the general case. Pick any rth root of x_2/x_1 and denote it by $\omega(2) \in L(x_1, x_2)$. Then $L(x_1, \omega(2)) = L(x_1, x_2)$, a field having degree $n-1$ over $L(x_1)$ (because $\text{gal}(L(\mathbf{x})/L(x_1)) = S_{n-1} (n \geq 3)$ or $A_{n-1} (n \geq 4)$) with conjugate fields $L(x_1, x_j)$, $j = 3, \ldots, n$, over $L(x_1)$. The element $\omega(2)$ has conjugates $\omega(3), \ldots, \omega(n)$, say, over $L(x_1)$ with the property that $\omega^r(j) = x_j/x_1$, $j = 3, \ldots, n$.

The next step fails if $G = A_4$ so we exclude this case meantime. (But note that $G = S_3$ is included; in which case some of the details are unnecessary.) For each $j, k \geq 3$, there exists $\sigma_{jk} \in G$ fixing x_1 and x_2 and such that $\sigma_{jk}(x_j) = x_k$. It follows that $\omega(3), \ldots, \omega(n)$ are conjugate over $L(x_1, x_2)$. Hence $\omega(3)/\omega(2), \ldots, \omega(n)/\omega(2)$ are conjugate over $L(x_1, x_2)$ and so *a fortiori* conjugate over $L(x_2)$. Now,

$$\left(\frac{\omega(3)}{\omega(2)}\right)^r = \frac{x_3}{x_2} \quad \text{and so} \quad L\left(x_2, \frac{\omega(3)}{\omega(2)}\right) = L(x_2, x_3)$$

a field having degree $n-1$ over $L(x_2)$. Clearly, the missing conjugate of $\omega(3)/\omega(2)$ must be an rth root of x_1/x_2 and so has the form $\zeta^{(2)}/\omega(2)$, where $\zeta^{(2)}$ is an rth root of unity.

† In corrections to earlier work, essential use of Theorem 8 (and Lemma 4) has been made by Cohen on p. 485 of Pacific Journal of Mathematics **97** (1981), 482–486.

https://doi.org/10.1017/S0017089500005449 Published online by Cambridge University Press

Similarly, for each $j = 2, \ldots, n$, there are rth roots of unity $\zeta^{(j)}$ such that

$$\left\{\frac{\omega(k)}{\omega(j)}, 2 \le k(\ne j) \le n\right\} \cup \left\{\frac{\zeta^{(j)}}{\omega(j)}\right\} \quad \text{is a set of conjugates over } L(x_j). \tag{7}$$

Since $\omega(2), \ldots, \omega(n)$ is a full set of conjugates over $L(x_1)$ and evidently $L(\mathbf{x}) = L(x_1, \omega(2), \ldots, \omega(n))$, then the group $\mathrm{gal}(L(\mathbf{x})/L(x_1))$ also acts as S_{n-1} or A_{n-1} when represented on $\omega(2), \ldots, \omega(n)$ and, as such, is certainly doubly transitive (recall that $G \ne A_4$). Consequently, for any $2 \le j < k \le n$ there exists σ in G fixing x_1 for which $\omega(j) \leftrightarrow \omega(k)$ and, automatically, $x_j \leftrightarrow x_k$. Because $\omega(k)/\omega(j)$ and $\zeta^{(j)}/\omega(j)$ are conjugate over $L(x_j)$, by applying σ we see that $\omega(j)/\omega(k)$ and $\zeta^{(j)}/\omega(k)$ are conjugate over $L(x_k)$. But, by (7), the unique rth root of x_1/x_k which is conjugate over $L(x_k)$ to $\omega(j)/\omega(k)$ is $\zeta^{(k)}/\omega(k)$. Hence $\zeta^{(j)} = \zeta^{(k)}$. We conclude that, for all j, $2 \le j \le n$, $\zeta^{(j)}$ takes the same value ζ, say.

Now pick any rth root of x_1 and call it y_1 but fix $y_2, \ldots, y_n$ by defining

$$y_j = \zeta^{-1} y_1 \omega(j), \qquad j = 2, \ldots, n.$$

Then the import of the preceding discussion is that, for each $j = 1, \ldots, n$, the polynomial $\prod_{\substack{k=1 \\ k \ne j}}^{n} (y - y_k)$ is fixed by any member of $\mathrm{gal}(L(\mathbf{y})/L(y_j))$. Hence, if $g(y) = (y - y_1) \ldots (y - y_n)$, then $g(y) \in K[y]$, where $K = \bigcap_{j=1}^{n} L(y_j)$. Thus $g(y)$ is divisible by the minimal polynomial of y_1 over K. Hence $[L(y_1) : K] = d$, say, where clearly $d \mid n$. The next step is to prove that, in fact, $d = n$.

The splitting field $L(\mathbf{y})$ of $g(y)$ over K is an extension of degree less than or equal to $(d!)^{n/d}$ while

$$[K : L] = \frac{[L(y_1) : L]}{[L(y_1) : K]} = \frac{nr^*}{d},$$

where, as before, $r^* = [L(y_1) : L(x_1)]$, a divisor of r. We deduce that

$$|\mathcal{G}| = [L(\mathbf{y}) : L] \le \frac{(d!)^{n/d} n r^*}{d}.$$

But $[L(\mathbf{x}) : L] = |G| = n!$ or $n!/2$ and, by Lemma 6(i), $|H(r)| = [L(\mathbf{y}) : L(\mathbf{x})] = r^*/k$, where $k = 1, 2$ or 3 as indicated there. Hence, certainly,

$$\frac{r^* n!}{6} \le \frac{(d!)^{n/d} n r^*}{d},$$

which yields

$$\frac{n!}{(d!)^{n/d}} \le \frac{6n}{d}. \tag{8}$$

Suppose $d < n$. Then (8) implies that $n \le 4$. However, if $G = S_4$, then $|H(r)|$ is at least

https://doi.org/10.1017/S0017089500005449 Published online by Cambridge University Press

$r^*/2$ and we can replace (8) by the stronger inequality

$$\frac{4!}{(d!)^{4/d}} \leq \frac{8}{d}, \tag{9}$$

which is false as $d < n = 4$. Moreover, if $G = S_3$, then by assumption (6), we must have $|H(r)| = r^*$ so that (8) can be improved to yield

$$\frac{3!}{(d!)^{3/d}} \leq \frac{3}{d},$$

which fails since d must be 1.

(For later use, we give a partial result for $G = A_4$. If it happens that $[L(y_1) : K] = d \leq 4$ then, by (6), we have $|H(r)| = r^*$ so that (9) holds. Then $d = 4$.)

Summarising, we have shown that, if $G \neq A_4$, then $[L(y_1) : K] = n$ so that $[K : L] = r^* = [L(y_1) : L(x_1)]$. Now the theorem of natural irrationalities implies that, anyway, $\mathrm{gal}(L(y_1)/L(x_1))$ is a subgroup of $\mathrm{gal}(K/L)$ from which it follows that K/L is a cyclic extension of degree r^*. Since $L(\zeta_r) = L$, a standard result [**5**, Theorem 34] shows that $K = L(\theta)$, where $\theta^{r^*} = \gamma \in L$. Now, $L(y_1) = L(x_1, \theta)$ and so we have a unique representation

$$y_1 = \sum_{i=0}^{r^*-1} a_i(x_1)\theta^i, \qquad a_i(x_1) \in L(x_1).$$

Apply to this a generator of $\mathrm{gal}(L(y_1)/L(x_1))$. This sends y_1 to ζy_1, say, where ζ is a primitive r^*th root of unity, and, for some k, θ to $\zeta^k\theta$. As in Lemmas 4 or 6, we conclude that, in fact,

$$y_1 = a(x_1)\theta^j, \qquad (j, r^*) = 1;$$

whence

$$x_1 = a^r(x_1)\gamma^{jr/r^*}, \qquad a(x_1) \in L(x_1).$$

The desired conclusion, namely that $f(x) \in \mathcal{S}(r)$, now follows at last.

We finish case (a) with a discussion of the situation in which $G = A_4$. Let $\sigma_1 = (234)$, $\sigma_2 = (134) \in G$, where, as usual, the action is on the subscripts of $x_1, \ldots, x_4$. As before, let $\omega(2)$ be an rth root of x_2/x_1, then its conjugates $\omega(3)$ and $\omega(4)$ over $L(x_1)$ are

$$\omega(3) = \sigma_1(\omega(2)), \qquad \omega(4) = \sigma_1(\omega(3)).$$

Clearly, for some rth roots of unity ζ, ζ', σ_2 acts on $\omega(3)/\omega(2)$ (producing a set of conjugates over $L(x_2)$) by

$$\sigma_2 : \frac{\omega(3)}{\omega(2)} \to \frac{\zeta\omega(4)}{\omega(2)} \to \frac{\zeta'}{\omega(2)} \to \frac{\omega(3)}{\omega(2)}. \tag{10}$$

However, $\sigma_1\sigma_2 = (14)(23)$ has order 2 and so, by considering the identity

$$(\sigma_1\sigma_2)^2(\omega(2)) = \omega(2),$$

we obtain $\zeta^2 = 1$. Application of σ_1 and σ_1^2 to the members of (10) yields (since

https://doi.org/10.1017/S0017089500005449 Published online by Cambridge University Press

$\zeta = \zeta^{-1} = \pm 1$)

$$\frac{\omega(4)}{\omega(3)}, \frac{\zeta\omega(2)}{\omega(3)}, \frac{\zeta'}{\omega(3)} \text{ are conjugate over } L(x_3);$$

$$\frac{\omega(2)}{\omega(4)}, \frac{\zeta\omega(3)}{\omega(4)}, \frac{\zeta'}{\omega(4)} \text{ are conjugate over } L(x_4).$$

If $\zeta = 1$, complete the proof that $f \in \mathcal{S}(r)$ as before; in particular, recall the remark concerning A_4 following (9). If $\zeta = -1$, then squaring each of the above quantities and arguing as before, we get $f \in \mathcal{S}(r/2)$.

This completes the discussion of case (a).

Case (b). x_2/x_1 is not an rth power in $L(x_1, x_2)$.

Here $|G| \geq 24$. Also, if $(\omega(2))^r = x_2/x_1 \in L(x_1, x_2)$, then $L(x_1, x_2, \omega(2))/L(x_1, x_2)$ is cyclic of order r', say, where $r' \mid r$, yet $r' > 1$. Moreover,

$$\text{gal}(L(\mathbf{x})/L(x_1, x_2))/\text{gal}(L(\mathbf{x})/L(x_1, x_2, \omega(2)) \cong C_{r'}.$$

But $\text{gal}(L(\mathbf{x})/L(x_1, x_2)) = S_{n-2}$ or A_{n-2}. Accordingly, a familiar argument now yields that either $r' = 2$ and $G = S_n$ or $r' = 3$ and $G = A_5$ or A_6.

Suppose first that $r' = 2$ and $G = S_n$ $(n \geq 4)$. Necessarily, $\delta\omega(2) \in L(x_1, x_2)$, where $\delta^2 = D$. This follows since D is the discriminant of $f(x)/(x - x_1)(x - x_2)$ multiplied by a square in $L(x_1, x_2)$.

Now, of course, $L(x_1, x_2) = L(x_1, \delta\omega(2))$ and so $\delta\omega(2)$ has altogether $n - 1$ conjugates over $L(x_1)$ (including itself). Define them by putting

$$\delta\omega(j) = \sigma_1^{j-2}(\delta\omega(2)), \qquad j = 2, \ldots, n,$$

where $\sigma_1 = (23 \ldots n)$. Since r is even $\omega^r(j) = x_j/x_1$, $j = 1, \ldots n$.

Suppose now $n \geq 5$ and put $\sigma = (45)$. Since σ fixes x_1, then σ permutes the $\delta\omega(j)$, $j = 2, \ldots, n$. Also, since σ is odd, then $\sigma(\delta) = -\delta$. Further, σ fixes x_1, x_2 and x_3 and so fixes $\delta\omega(2)$ and $\delta\omega(3)$. Hence

$$\sigma(\omega(2)) = -\omega(2), \qquad \sigma(\omega(3)) = -\omega(3).$$

Obtain a contradiction as follows. On the one hand, since

$$\left(\frac{\omega(3)}{\omega(2)}\right)^r = \frac{x_3}{x_2}, \quad \text{then} \quad \frac{\delta\omega(3)}{\omega(2)} \in L(x_2, x_3)$$

and so is fixed by σ. On the other hand

$$\sigma\left(\frac{\delta\omega(3)}{\omega(2)}\right) = \frac{\sigma(\delta)\sigma(\omega(3))}{\sigma(\omega(2))} = -\frac{\delta\omega(3)}{\omega(2)}.$$

Next, suppose $G = S_4$ necessarily with r even. Then $\omega^2(2) \in L(x_1, x_2)$. Replacing r by $r/2$ and $\omega(2)$ by $\omega^2(2)$ we obtain $f \in \mathcal{S}(r/2)$, by case (a).

It remains to consider $G = A_5$ or A_6 with r divisible by 3. Here $L(\mathbf{x})$ possesses a normal cubic subfield over $L(x_1, x_2)$ and, by a familiar type of argument, $\varepsilon\omega(2) \in L(x_1, x_2)$, where $\varepsilon^3 \in L(x_1, x_2)$.

https://doi.org/10.1017/S0017089500005449 Published online by Cambridge University Press

Let $\sigma = (12)(34) \in G$. Then, of course, $\sigma(\varepsilon\omega(2)) \in L(x_1, x_2)$. However, $\sigma(\varepsilon) = \zeta_1\varepsilon$, where ζ_1 is a cube root of unity and, since

$$\omega^r(2) = \frac{x_2}{x_1}, \quad \text{then} \quad \sigma(\omega(2)) = \frac{\zeta_2}{\omega(2)},$$

where ζ_2 is an rth root of unity. It follows that $\sigma(\varepsilon\omega(2)) = \zeta\varepsilon/\omega(2)$, where $\zeta = \zeta_1\zeta_2$, an rth root of unity. Accordingly, $\varepsilon/\omega(2) \in L(x_1, x_2)$ as well as $\varepsilon\omega(2) \in L(x_1, x_2)$. Thus ε^2 and so $\varepsilon \in L(x_1, x_2)$, a contradiction.

This completes the account of case (b) and so the theorem is proved.

We illustrate below the fact that $n = 4$ is necessarily exceptional in Theorem 8 by providing examples with $r = 2$ in which $H(2)$ is C_2 without $f \in \mathcal{S}(2)$.

While we lack a criterion for distinguishing this exceptional possibility ($f \notin \mathcal{S}(r)$) when $n = 4$, we do pursue it a little further here showing, in particular, that $H(r)$ cannot, in fact, be trivial.

COROLLARY 9. *Suppose that f is a standard quartic polynomial and r is even with $H(r) \subseteq C_r$ yet $f \notin \mathcal{S}(r)$. Then*

$$|H(r)| = 2\left|H\left(\frac{r}{2}\right)\right|.$$

Proof. Suppose the result is false. Then, since $L(\mathbf{y})(=L(\mathbf{x}, y_1)) = L(\mathbf{y}^2)(y_1)$ is at most a quadratic extension of $L(\mathbf{y}^2)$, we have $H(r) = H(r/2)$ and hence

$$(L(\mathbf{y}) =) L(\mathbf{x}, y_1) = L(\mathbf{x}, y_1^2)(= L(\mathbf{y}^2)). \tag{11}$$

Now the maximal subfield of $L(\mathbf{x}, y_1)$ whose degree over $L(\mathbf{x})$ is a power of 2 (call it its 2-*field over* $L(\mathbf{x})$) is $L(\mathbf{x}, y_1^{r_1})$, where r_1 is the odd part of r. By (11), this must be the same as the 2-field of $L(\mathbf{x}, y_1^2)$ over $L(\mathbf{x})$, namely, $L(\mathbf{x}, y_1^{2r_1})$. Replacing $\mathbf{y}$ by $\mathbf{y}^{r_1}$, we may assume that r is a power of 2 and (11) still holds.

Next, (11) is equivalent to

$$(L(x_1, x_2, \sqrt{D}, y_1) =) L(\sqrt{D}, y_1, x_2) = L(\sqrt{D}, y_1^2, x_2)(= L(x_1, x_2, \sqrt{D}, y_1^2). \tag{12}$$

Since $L(\sqrt{D}, y_1^i, x_2)/L(\sqrt{D}, y_1^i)$, $i = 1, 2$, is a cubic extension, equating 2-fields over L in (12), we obtain

$$L(\sqrt{D}, y_1) = L(\sqrt{D}, y_1^2)$$

which implies that

$$L(y_1^2) \subseteq L(y_1) \subseteq L(y_1^2, \sqrt{D}).$$

Suppose, in fact, that $L(y_1) = L(y_1^2)$ (which necessarily occurs if $G = A_4$). Since, by Theorem 8, $f \in \mathcal{S}(r/2)$ and so $L(y_1^2) = L(x_1, \theta)$, where $\theta^r \in L$, a familiar argument yields

$$y_1 = a(x_1)\theta^k, \qquad a(x_1) \in L(x_1),$$

whence $f \in \mathcal{S}(r)$, a contradiction.

The remaining possibility is that $G = S_4$ and

$$(L(y_1) =) L(y_1^2)(y_1) = L(y_1^2)(\sqrt{D}),$$

https://doi.org/10.1017/S0017089500005449 Published online by Cambridge University Press

a quadratic extension of $L(y_1^2)$. Applying an $L(y_1^2)$-automorphism sending $\sqrt{D}$ to $-\sqrt{D}$ to this, we obtain in a routine fashion

$$y_1 = a(y_1^2)\sqrt{D}$$

But, as before, $L(y_1^2) = L(x_1, \theta)$, where $\theta^r \in L$ and hence

$$y_1 = p(\theta)\sqrt{D},$$

where p is a polynomial with coefficients in $L(x_1)$ of degree less than $b = [L(x_1, \theta) : L(x_1)]$. If $b > 1$, apply an $L(x_1)$-automorphism σ which sends θ to $\zeta_b\theta$, where ζ_b is a primitive bth root of unity. Of course, $\sigma(y_1) = \zeta_1 y_1$, where $\zeta_1^r = 1$, and $\sigma(\sqrt{D}) = \varepsilon\sqrt{D}$, where $\varepsilon = \pm 1$. This yields

$$0 = p(\theta) - \zeta p(\zeta_b\theta), \qquad \zeta = \zeta_1^{-1}\varepsilon.$$

However, $1, \theta, \ldots, \theta^{b-1}$ are linearly independent over $L(x_1)$ and so, for some k,

$$y_1 = c(x_1)\theta^k\sqrt{D}, \quad c(x_1) \in L(x_1),$$

which is valid even if $b = 1$. It follows that

$$x_1 = c^r(x_1)\gamma^k D^{r/2},$$

where $\gamma = \theta^r \in L$ and $D^{r/2} \in L$, since r is even, and so $f \in \mathcal{S}(r)$, a contradiction as before.

EXAMPLE 5. Let $L = \mathbb{C}(w)$ and put

$$f(x) = x(x + 2i\sqrt{2})(x + 4 + i\sqrt{2})^2 - 27w.$$

There is the obvious ramification at $w = 0$ indicating that G contains a transposition. There is a 4-cycle in G corresponding to $w = \infty$. The only other ramification occurs at $w = 1$, where

$$f(x) = (x + 1 + i\sqrt{2})^3(x + 5 + i\sqrt{2});$$

thus G contains a 3-cycle. Hence, certainly $G = S_4$ while, as remarked in §2, $f \notin \mathcal{S}(2)$. Less obvious is the fact that here $H(2) = C_2$. We do not have a simple direct proof of this. The following proof depends on the apparent coincidence that $L(\mathbf{x}) = \mathbb{C}(w, \mathbf{x})$ turns out to have genus 0.

We therefore calculate the genus of $L(\mathbf{x})$. This field must contain 12 primes of ramification index 2 lying over w, 8 primes with index 3 lying over $w - 1$ and 6 primes with index 4 lying over the infinite prime. The genus formula ("$g = 2N - 2 - \Sigma(e_i - 1)$") now implies that $L(x)$ indeed does have genus 0. We conclude that $L(\mathbf{x}) = \mathbb{C}(u)$ for some $u \in \mathbb{C}(w, \mathbf{x})$. In particular, there is a complex rational function $R = R_1/R_2$, where R_1 and R_2 are co-prime polynomials for which $x_1 = R(u)$.

Now, the discriminant of f is $c_1 w(w-1)^2$ ($c_1 \in \mathbb{C}$) and so $\sqrt{w} \in L(\mathbf{x})$, whence $w = S^2(u)$ for some complex rational function $S = S_1/S_2$. Putting $a = 2i\sqrt{2}$ and $b = 4 + i\sqrt{2}$, we have, identically in $\mathbb{C}(u)$,

$$R_1(R_1 + aR_2)(R_1 + bR_2)^2 = R_2^4 S^2.$$

Since R_1 and $R_1 + aR_2$ are co-prime, we deduce that R_1 is a square in $\mathbb{C}(u)$ and $R_2^2 = c_2 S_2$,

https://doi.org/10.1017/S0017089500005449 Published online by Cambridge University Press

where $c_2 \in \mathbb{C}$. Similarly, $x_2 = R_1'(u)/R_2'(u)$, where R_1' is a square in $\mathbb{C}(u)$ and $R_2'^2 = c_2' S_2$. Thus, in particular $R_2 = cR_2'$, where $c \in \mathbb{C}$. Hence $x_2/x_1 = cR_1'/R_1$ is a square in $\mathbb{C}(u) = L(\mathbf{x})$ and consequently $H(2) \subseteq C_2$. We can confirm directly that $H(2)$ is not trivial here. For, by considering $f(x^2)$ at $w = \infty$, we see that $\mathcal{G}$ contains an 8-cycle τ on the zeros $\{\pm y_j, j = 1, 2, 3, 4\}$ of $f(x^2)$ where $\tau^4 \in H(2)$ so that necessarily $\tau^4(y_j) = -y_j$, $j = 1, \ldots, 4$. Hence $H(2) = C_2$.

EXAMPLE 6. This example is related to Example 4. Let $L = \mathbb{Q}(\sqrt{(-3)}, w)$ and put

$$\begin{aligned} f(x) &= (x-1)^3(x+3) - 16wx \\ &= x^4 - 6x^2 + 8(1-2w)x - 3. \end{aligned}$$

The discriminant is $-3[48w(w-1)]^2$ and clearly $G = A_4$. Let ε be a cube root of $4w(w-1)$ and η a primitive cube root of unity (in $\mathbb{Q}(\sqrt{(-3)})$). Solving explicitly, we find that two zeros of f can be expressed in the form

$$\begin{aligned} x_1 &= \sqrt{(1+\varepsilon)} + \sqrt{(1+\eta\varepsilon)} + \sqrt{(1+\eta^2\varepsilon)}, \\ x_2 &= \sqrt{(1+\varepsilon)} - \sqrt{(1+\eta\varepsilon)} - \sqrt{(1+\eta^2\varepsilon)}, \end{aligned}$$

where the square roots are chosen in such a way that

$$\sqrt{(1+\varepsilon)}\sqrt{(1+\eta\varepsilon)}\sqrt{(1+\eta^2\varepsilon)} = 8(2w-1).$$

From this, we derive

$$\begin{aligned} x_1 x_2 &= 2\varepsilon - 1 - 2\sqrt{(1-\varepsilon+\varepsilon^2)} \\ &= \left\{-\sqrt{3}\left(\frac{\sqrt{(1+\eta\varepsilon)}}{1-\eta} + \frac{\sqrt{(1+\eta^2\varepsilon)}}{1-\eta^2}\right)\right\}^2. \end{aligned}$$

Hence $H(2) = C_2$.

Observe also that, if $L = \mathbb{Q}(w)$, then this f gives $G = S_4$ and $H(2) = C_2$.

We state without proof one further genus zero polynomial f over $\mathbb{C}(w)$ not in $\mathcal{S}(2)$ for which $G = A_4$ and $H(2) = C_2$. It is $(x+\alpha)^3(x+\beta) - w$, where α, β $(\neq 0)$ satisfy $\alpha^2 - 4\alpha\beta + 7\beta^2 = 0$.

It may be that the above examples essentially exhaust the genus zero standard quartic polynomials with $H(2) = C_2$. We do not know of any standard quartics for which $H(r) \subseteq C_r$ but $f \in \mathcal{S}(r/2) \setminus \mathcal{S}(r)$ with $r > 2$. An interesting possibility permitted by group theory has $r = 6$, $G = A_4 \cong \mathrm{PSL}(2, 3)$ and $H(6) = C_2$. G would be the non-split extension of C_2 by A_4 (namely SL(2, 3)) as in Example 6. In fact, we have been able neither to realise this possibility for some f (necessarily in $\mathcal{S}(3)$) nor to discount it.

5. Conclusions. We bring together the results of §§2–4. Let s be as in Theorem 1 and u as in §3.

By Lemma 4, $H(r)$ is an extension of $C_u^{n-1} \times C_t$ by $H(r/u)$, where t is $\deg[L(\mathbf{y}^u, \sqrt[t]{\nu}) : L(\mathbf{y}^u)]$. Since $\sqrt[t]{(\nu^u)} \in L(\mathbf{y}^u)$, then certainly $t \mid u$.

The crucial consequence of Theorem 8 is that usually (indeed, inevitably, if $n \geq 5$), we have $u = r/s$. Moreover, suppose that, in fact, $f(x)$ divides $x^i F_1^s(x) - \alpha F_2^s(x)$. Then, by

https://doi.org/10.1017/S0017089500005449 Published online by Cambridge University Press

Theorem 3, when $u = r/s$, t is given in the notation of §2 by $q_r(\nu, L(\sqrt[s]{\alpha}))$ and $H(s) = C_q$, where $q = q_s(f)$.

Exceptionally, when $n = 4$, it is possible, by Theorem 8 and Corollary 9, that $u = r/2s$ and $H(r/u) = C_{2q}$ where $q = q_s(f)$. This completes the detailed explanation of Theorem 1.

Finally, we give a brief survey of the excluded cases $G = S_2$ or A_3, observing that here the assumptions on f are too weak to have very meaningful consequences for $H(r)$.

If $G = S_2$, then Lemma 4 still applies and we derive the fact that $H(r)$ is an extension of $C_u^{n-1} \times C_t$ by $H(s^*)$, where $t \mid u$ and $s^* = r/u$. For simplicity in describing the possibilities for $H(s^*)$, suppose s^* is prime. By (4),

$$x_2 = a^{s^*}(x_1)x_1^m, \qquad 1 \leq m \leq s^* - 1,$$

and hence

$$\nu = x_1 x_2 = a^{s^*}(x_1)x_1^{m+1}$$

If $m \neq 1$ or $s^* - 1$, then, as in Lemma 7, $f \in \mathcal{S}(s^*)$ so that $s = s^*$. If $m = s^* - 1$, then $\nu = b^{s^*}(b \in L)$ and f is of type I. If $m = 1$ and s^* is odd, then $f \in \mathcal{S}(s^*)$ (and $s = s^*$) as in Lemma 7, while if $s^* = 2$, then, of course, f is of type I as before.

Turning to the case in which $G = A_3$, we observe that here even Lemma 4 fails because A_3 is not doubly transitive. In fact, the extension $\mathcal{G}$ by G may fail to be central in yet another way. We content ourselves by exhibiting an example of a polynomial $f \notin \mathcal{S}(7)$ for which $G = A_3$ and $H(7) = C_7$.

Start with the polynomial

$$g(u) = u^7 - u + w,$$

where w is an indeterminate. Then $\mathrm{gal}(g, \mathbb{C}(w))$ is generated by transpositions and so is S_7. Since $g \in \mathbb{C}[w]$, is monic and has no singularities with $w = 0$, each of the seven zeros of g can be expressed as a power series of the form $\sum_{i=0}^{\infty} c_i w^i (c_i \in \mathbb{C})$ (in

$$\mathbb{C}\{w\} = \left\{ \sum_{i=M}^{\infty} c_i w^i, c_i \in \mathbb{C}, M \in \mathbb{Z} \right\},$$

the w-adic completion of $\mathbb{C}(w)$). Indeed, since $g(u) \equiv u^7 - u \pmod{w}$, then one zero ($u_1$, say) has zero constant term, while the remaining 6 zeros $u_2, \ldots, u_7$ have constant terms $\eta_2, \ldots, \eta_7$ (respectively) equal to the six 6th roots of unity. Further, $u_1 \equiv 0 \pmod{w}$ and $u_1^7 \equiv u_1 - w \pmod{w^2}$ implies that actually $u_1 \equiv w \pmod{w^2}$.

Put $L = \mathbb{C}(w, \sqrt{D}, u_4, u_5, u_6, u_7)$, where D is the discriminant of g. Let $u = \{u_1, u_2, u_3\}$. Then $\mathrm{gal}(L(\mathbf{u})/L) = A_3$. Write $\mathbf{x} = \{x_1, x_2, x_3\}$, where

$$x_1 = u_1 u_2^2 u_3^4,$$

$$x_2 = u_2 u_3^2 u_1^4,$$

$$x_3 = u_3 u_1^2 u_2^4.$$

https://doi.org/10.1017/S0017089500005449 Published online by Cambridge University Press

Then x_1, x_2 and x_3 are conjugate over L and *distinct*. Thus $L(\mathbf{x}) = L(\mathbf{u})$. Define

$$f(x) = (x - x_1)(x - x_2)(x - x_3).$$

Then $\text{gal}(f, L) = A_3$.

Now

$$\frac{x_2^2}{x_1} = u_1^7,$$

a 7th power in $L(\mathbf{x})$ and so $H(7) \subseteq C_7$. Suppose that, in fact, $H(7)$ is trivial. Then x_1 is a 7th power in $L(\mathbf{x})$ and so certainly a 7th power in $\mathbb{C}\{w\}$. But recall that, in $\mathbb{C}\{w\}$, u_2 and u_3 are units congruent (mod w) to η_2 and η_3, respectively, while $u_1 \equiv w \pmod{w^2}$. Hence

$$x_1 = \eta_2^2 \eta_3^4 w + c_2 w^2 + c_3 w^3 + \ldots \ (\eta_2^2 \eta_3^4 \neq 0),$$

which cannot be a 7th power in $\mathbb{C}\{w\}$, a contradiction. Thus $H(7) = C_7$.

Finally, if $f \in \mathcal{S}(7)$, then x_2/x_1 is a 7th power in $L(\mathbf{x})$ and so certainly in $\mathbb{C}\{w\}$. Now, in $\mathbb{C}\{w\}$, we have, for example,

$$\frac{1}{u_2} = \frac{1}{\eta_2} + d_1 w + d_2 w^2 + \ldots$$

and so

$$\frac{x_2}{x_1} = \frac{u_1^3}{u_2 u_3^2} = \frac{1}{\eta_2 \eta_3^2} w^3 + e_4 w^4 + \ldots,$$

which again is not a 7th power in $\mathbb{C}\{w\}$. Thus $f \notin \mathcal{S}(7)$ (although f is related to $g(u + w)$ in $\mathcal{S}(7)$).

REFERENCES

1. R. Carmichael, *Introduction to the theory of groups of finite order* (Dover, 1956).

2. S. D. Cohen, The distribution of the galois groups of integral polynomials, *Illinois J. Math.* **23** (1979), 135–152.

3. M. Fried, On a conjecture of Schur, *Michigan Math. J.* **17** (1970), 41–55.

4. B. Huppert, *Endliche Gruppen I* (Springer-Verlag, 1967).

5. I. Kaplansky, *Fields and rings* (Chicago, 1969).

6. H. Wielandt, *Finite permutation groups* (Academic Press, 1964).

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF GLASGOW
GLASGOW G12 8QW
SCOTLAND