PACIFIC JOURNAL OF MATHEMATICS
Vol. 90, No. 1, 1980

THE GALOIS GROUP OF A POLYNOMIAL WITH TWO INDETERMINATE COEFFICIENTS

S. D. COHEN

Suppose that $f(x) = \sum_{i=0}^{n} \alpha_i X^i (\alpha_0 \alpha_n \neq 0)$ is a polynomial in which two of the coefficients are indeterminates t, u and the remainder belong to a field F. We find the galois group of f over $F(t, u)$. In particular, it is the full symmetric group S_n provided that (as is obviously necessary) $f(X) \neq f_1(X^r)$ for any $r > 1$. The results are always valid if F has characteristic zero and hold under mild conditions involving the characteristic of F otherwise. Work of Uchida [10] and Smith [9] is extended even in the case of trinomials $X^n + tX^a + u$ on which they concentrated.

1. Introduction. Let F be any field and suppose that it has characteristic p, where $p = 0$ or is a prime. In [9], J. H. Smith, extending work of K. Uchida [10], proved that, if n and a are *co-prime* positive integers with $n > a$, then the trinomial $X^n + tX^a + u$, where t and u are independent indeterminates, has galois group S_n over $F(t, u)$, a proviso being that, if $p > 0$, then $p \nmid na(n - a)$. (Note, however, that this conveys no information whenever $p = 2$, for example.) Smith also conjectured that, subject to appropriate restriction involving the characteristic, the following holds. Let I be a subset (including 0) of the set $\{0, 1, \cdots, n - 1\}$ having cardinality at least 2 and such that the members of I together with n are co-prime. Let $T = \{t_i, i \in I\}$ be a set of indeterminates. Then the polynomial $X^n + \sum_{i=0}^{n-1} t_i x^i$ has galois group S_n over $F(T)$.

In this paper, we shall confirm this conjecture under mild conditions involving $p(>0)$, thereby extending even the range of validity of the trinomial theorem. In fact, we also relax the other assumptions. Specifically, we allow some of the t_i to be fixed nonzero members of F and insist only that two members of T be indeterminates. Indeed, even if the co-prime condition is dispensed with, so that the galois group is definitely not S_n, we can still describe what that group actually is. On the other hand, if, in fact, more than two members of T are indeterminates, then the nature of our results ensures that, in general, the relevant galois group is deducible by specialization.

Accordingly, from now on, let I denote a subset of *co-prime* integers from $\{0, 1, \cdots, n\}$ containing 0 and n and having cardinality $\geqq 3$. Write

$$(1)\quad f(X) = \sum_{i\in I} \alpha_i X^i = g(X) + tX^a + uX^b (\alpha_0\alpha_n \neq 0,\ 0 \leqq b < a \leqq n)\ ,$$

say, where two of the coefficients α_a, α_b are indeterminates t, u and the remaining coefficients $\alpha_i (i \neq a, b)$ are fixed nonzero members of f; in particular, g is not identically zero. By the co-prime condition, assuredly f is *separable*, i.e., $f(X) \neq f_1(X^p)$. (We deal with sets of the form I which are not co-prime by equivalently considering $f(X^r)$ with $r > 1$, §4.) Put $G = G(f(X), F(t, u))$, the galois group of f over $F(t, u)$, regarded as a group of permutations of the zeros of f.

THEOREM 1. *Let* $f(x)$ *in* $F[t, u, X]$ *be given by* (1). *Suppose* $G \neq S_n$. *Then* $p > 0$ *and* $g(X)$, X^a *and* X^b *are linearly dependent over* $F(X^p)$. *In particular,* p *divides* $(n-a)(n-b)(a-b)$.

Notes. (i) The polynomials $g(X)$, X^a and X^b are linearly dependent over $F(X^p)$ if and only if either $p \mid (a-b)$ or

$$g(X) = g_1(X^p)X^{a^*} + g_2(X^p)X^{b^*}\ ,$$

where $g_1(X), g_2(X) \in F[X]$ and, for any integer m, m^* denotes the least nonnegative residue of m modulo p.

(ii) For the case in which F is an algebraic number field, Theorem 1 is an easy by-product of Theorem 1 of [4].

If, for example, $p = 2$, then Theorem 1 is vacuous. However, if, additionally, we assume that f is monic (i.e., $a \neq n$) and has indeterminate constant term (i.e., $b = 0$), then we can strengthen Theorem 1 to give useful information even when $p = 2$ (although we retain one restriction, namely, $p \nmid (a, n)$). Before stating the result, we introduce some further notation. Let $c (\leqq a)$ denote the least positive member of I. Further, define

$$e = \begin{cases} a^*\ , & \text{if } p \nmid a\ , \\ n^*\ , & \text{if } p \mid a\ . \end{cases}$$

Finally, let $\gamma(n)$ be the maximal degree of transitivity of a subgroup of S_n that is neither S_n itself nor the alternating group, A_n.

THEOREM 2. *Suppose that* f *is given by* (1) *with* $a \neq n, b = 0$ *and* $p \nmid (a, n)$. *Suppose* $G \neq S_n$. *Then one of the following* (i)-(iii) *holds.*

(i) $a = n - 1$ *and* $c \geqq n - \gamma(n) + 1 (> 1)$

(ii) $a \leqq \gamma(n) - 1 (< n - 1)$ *and* $c = 1$,

(iii) $a = n - 1$ *and* $c = 1$, *necessarily with* $p = 2$ *if* $p \nmid (n - 1)$.

Moreover, there exist $g_1(X)$, $g_2(X)$ *in* $F[X]$ *such that*

$$(2)\qquad g(X) = g_1(X^p)X^e + g_2(X^p)\ ,$$

except possibly when $c = 1$ and $a = n - 1$, the latter being divisible by p.

REMARKS. (a) I cannot quite prove (2) in the excluded case (see §3). On the other hand, if $p \mid a$ then, aside from this case ((iii)), the proof actually implies that

$$g(X) = \alpha X^n + g_2(X^p)\ , \quad \alpha \neq 0\ . \tag{3}$$

(b) Some estimates for $\gamma(n)$ are

$$\gamma(n) \leqq \frac{1}{3}n + 1 \quad \text{(see [1, p. 150])}\ ; \tag{4}$$

$$\gamma(n) \leqq 3\sqrt{n} - 2,\ n > 12 \ \text{([7], [1, p. 150])}\ ; \tag{5}$$

$$\gamma(n) < 3 \log n,\ n \to \infty \ \text{([11])}\ .$$

(c) It is an open question whether in (i) we must have $a = c = n - 1$, i.e., $f(X) = X^n + tX^{n-1} + u$ and in (ii) we must have $a = c = 1$. In any event, the trinomials $X^n + tX + u$ considered by Uchida emerge as the most likely type of polynomial for which $G = S_n$ may be false. Indeed, he demonstrated that sometimes in this case G is definitely not S_n.

(d) In fact, in the cases excluded by the hypotheses of Theorem 2 (namely, $p \mid (a, n)$, $b \neq 0$, etc.), I have obtained partial results in the direction of Theorem 2 but the details are too cumbersome to present here. However, although it is difficult to state a comprehensive result, the methods used presently will often enable G to be determined for a given specific f.

From Theorem 2, we derive immediately the following improvement of Smith's theorem.

COROLLARY 3. *Let $f(X) = X^n + tX^a + u$, where $(a, n) = 1$, $(n > a > 0)$. Then $G = S_n$ unless $p(>0)$ divides $n(n - 1)$ and $a = 1$ or $n - 1$.*

The galois group of $f(X^r)(r > 1)$ over $F(t, u)$ is described in §4.

2. Preliminary results. Clearly, if Theorems 1 and 2 hold when F is algebraically closed, then they are valid for arbitrary F. Hence we assume throughout §§2–3 that F is algebraically closed. In particular, F is infinite. As usual, the phrase "for almost all members of F" means "for all but finitely many members of F".

A simplification arises from the use of the following lemma established by Uchida [10] in a special case. (Suprisingly, Smith failed to use the corresponding result in his paper, [9].)

LEMMA 4. *Suppose that f is given by* (1). *Then G is doubly transitive.*

Proof. Obviously f is irreducible over $F(t, u)$ and hence G is transitive. Let x be a zero of f in a suitable extension of $F(t, u)$. Then $x \neq 0$ and $u = -(g(x) + tx^a)/x^b$ so that $F(t, u, x) = F(t, x)$, x being transcendental over F. Thus

$$x^b f(X) = x^b g(X) - g(x)X^b + t(x^b X^a - x^a X^b) . \tag{6}$$

Of course, $X - x$ is a factor of (6). But since (6) is linear in t and separable, then $f(X)/(X - x)$ can be reducible as polynomial in X only if for some $\xi(\neq x)$ in an extension of $F(x)$ we have

$$x^b g(\xi) = \xi^b g(x) \quad \text{and} \quad \xi^a x^b = \xi^b x^a . \tag{7}$$

Now, $g(0) \neq 0$ or $b = 0$. In either case, (7) implies that $\xi \neq 0$ and that, in fact, $\xi = \zeta x$, where ζ is an $(a - b)$th root of unity $(\neq 1)$ in F (so that $a - b > 1$). Hence, we have

$$g(\zeta X) = \zeta^b g(X) , \tag{8}$$

identically. If $b = 0$, deduce from (8) that $g(X) \in F[X^a]$, where $a > 1$, which yields the contradiction that $f(X) \in F[t, u, X^a]$. Otherwise, if $b > 0$, then $g(0) \neq 0$ and so, by (8), $\zeta^b = 1$. Accordingly, ζ must be a primitive dth root of unity for some $d(>1)$ dividing $(a, a - b) = (a, b)$ and, therefore, $f(X) \in F[t, u, X^d]$, again a contradiction and the lemma is proved.

An immediate consequence of Lemma 4 is that, if G is known to contain a transposition, then necessarily $G = S_n$. The next lemma will enable us to generate members of G with identifiable cycle patterns. First, we connect such a permutation cycle pattern with the "cycle pattern" of a polynomial $h(X)$ of degree n in $F[X]$ (recalling that F is assumed to be algebraically closed). To define this concept, suppose that in the factorization of $h(X)$ into a product of linear factors there are precisely μ_i distinct factors of multiplicity i, $i = 1, 2, \cdots$. Thus $\sum i\mu_i = n$. We shall then say that h has *cycle pattern* $\mu(h) = (1^{(\mu_1)}, 2^{(\mu_2)}, \cdots)$, where the ith term is omitted if $\mu_i = 0$. For a given n, we extend this definition to apply to all nonzero h of degree $d < n$ by formally adjoining ∞ to F and defining $\mu(h)$ to be the cycle pattern of $(X - \infty)^{n-d}h(X)$. Such a cycle pattern is identified with a cycle pattern of a permutation in S_n in the obvious way. The proof of the lemma we now state represents a simplification of the first part of Lemma 7 of [4] and is not restricted to "tame" polynomials.

LEMMA 5. *Let F be algebraically closed and $h_1(X)$, $h_2(X)$ be nonzero co-prime polynomials in $F[X]$ not both in $F[X^p]$ and such that $n = \max(\deg h_1, \deg h_2)$. Suppose that $(\beta_1, \beta_2)(\neq(0, 0)) \in F^2$ and put $\mu = \mu(\beta_1 h_1 + \beta_2 h_2)$. Let t be an indeterminate. Then $G(h_1 + th_2, F(t))$ contains an element with cycle pattern μ.*

Proof. Evidently, $h_1 + th_2$ and $th_1 + h_2$ have the same galois group over $F(t)$. Hence, we may assume, without loss of generality, that $\beta_1 \neq 0$. Put $\beta = -\beta_2/\beta_1$ and write h for $h_1 + th_2$. We now make some transformations which, while not essential, make the argument easier to visualise. First, replacing h_1 by $h_1 + \beta h_2$ and t by $t + \beta$, we can suppose that $\beta = 0$. If then $\deg h_1 < n$, we may take $(cX + d)^n h_1(L(X))$ for h_1 and $(cX + d)^n h_2(L(X))$ for h_2, where $L(X)$ is a nonsingular linear transformation with denominator $cX + d$, in such a way that $\deg h_1 = n$. Obviously, the hypotheses remain valid and h has a galois group isomorphic to the original one.

Now, let x be a zero of h. Then $t = -h_1(x)/h_2(x)$ and $F(t, x) = F(x)$, x being transcendental over F. The function field extension $F(x)/F(t)$ has degree n and genus 0. In particular, if $P(x)$ is a (linear) irreducible factor of $h_1(x)$, then the $P(x)$-adic valuation on $F(x)$ is an extension of the t-adic valuation on $F(t)$. Indeed, in the extension to $F(x)$ of the local ring of integers of $F(t)$ corresponding to the t-adic valuation, the cycle pattern μ provides a description of the ramification of t in the sense that there are precisely μ_i primes with ramification index i, $i = 1, 2, \cdots$, in its prime decomposition. It follows [2, Ch. 2] that, in the prime decomposition of $h(X)$ over $F\{t\}$, the t-adic completion of $F(t)$, there are precisely μ_i distinct irreducible factors of degree i, $i = 1, 2, \cdots$. Hence $G(h, F\{t\})$ (which is cyclic [2, Ch. 1]) clearly has as a generator a permutation with cycle pattern μ. However, $G(h, F\{t\})$ can be considered as a subgroup of $G(h, F(t))$ and the proof is complete.

COROLLARY 6. *Let F be algebraically closed and $h_1(X)$, $h_2(X)$, $h_3(X)$ be co-prime polynomials in $F[X]$, not all in $F[X^p]$, linearly independent over F and such that $\max_i \deg h_i = n$. Suppose that $(\beta_1, \beta_2, \beta_3)(\neq(0, 0, 0)) \in F^3$ and put $\mu = \mu(\beta_1 h_1 + \beta_2 h_2 + \beta_3 h_3)$. Let t, u be indeterminates. Then $G(h_1 + th_2 + uh_3, F(t, u))$ contains an element with cycle pattern μ.*

Proof. We may suppose that $\beta_1 \neq 0$. Note that the h_i's and the polynomial $B := \beta_1 h_1 + \beta_2 h_2 + \beta_3 h_3$ are nonzero. By our assumptions and the fact that F is infinite. We can choose γ_2 and γ_3 in F such that $h_1^*: = \beta_1 h_1 + \gamma_2 h_2 + \gamma_3 h_3$ is not in $F[X^p]$ and $(h_1^*, B) = 1$. (For example, if the latter assertion were false, B would have a nontrivial factor which divides h_1^* for infinitely many values of each of γ_2 and γ_3 and so divides (h_1, h_2, h_3) contrary to hypothesis.) With this choice of γ_2 and γ_3, put $h_2^* = (\beta_2 - \gamma_2)h_2 + (\beta_3 - \gamma_3)h_3$. Then h_1^* and h_2^* satisfy the conditions of Lemma 5. Consequently, $G(h_1^* + th_2^* F(t))$, $(\subseteq G(h_1 + th_2 + uh_3, F(t, u)))$ contains an element of cycle pattern μ, as required.

3. When is the galois group S_n? We shall use $R'(X)$ to denote the formal derivative of rational function R (usually a polynomial) in $F(X)$. Of course, all members of $F(X^p)$ are constants with respect to this differentiation process. Moreover, if $(X - \theta)^k \| h'(X)$ (exactly), where h is a polynomial and $k \geqq 1$, then $(X - \theta)^j \| (h(X) - h(\theta))$, where $j = k + 1$ or k, the latter being possible if $p \mid k$.

Theorem 1 is immediate from the next lemma together with the remark subsequent to Lemma 4 and Corollary 6. Recall that we are assuming that F is algebraically closed.

LEMMA 7. *Suppose that f is given by* (1) *and that $g(X)$, X^a and X^b are linearly independent over $F(X^p)$. Then there exists $(\beta_1, \beta_2, \beta_3)$ in F^3 with $\beta_3 \neq 0$ (and $\beta_2 \neq 0$ if $a = n$) such that*

$$(\mu(B) =)\mu(\beta_1 g(X) + \beta_2 X^a + \beta_3 X^b) = (1^{(n-2)}, 2^{(1)}) .$$

Proof. Suppose $a < n$ so that $\deg g = n$ and put $\beta_1 = 1$. (Otherwise, if $a = n$, put $\beta_2 = 1$ and proceed in like manner.) The assertion which follows is established by the argument of Lemma 5 of [3] as expressed in the more general context of Lemma 9 of [4] (yet without the restriction $p > n$ assumed there). Note that the hypothesis "$p \nmid 2(n - m)$" and the tameness assumption implicit in the statement of Lemma 5 of [3] are not relevant here and not necessary for the proof. The conclusion is that for almost all β_2 in F, $\mu(B) = (1^{(n)})$ or $(1^{(n-2)}, 2^{(1)})$ for every β_3 in F. We show that the latter must occur for some pair $(\beta_2, \beta_3)(\beta_3 \neq 0)$ in F^2.

To do this, consider the polynomial equation

$$bg(X) - Xg'(X) + (b - a)\beta_2 X^a = 0 . \tag{9}$$

Now, for almost all β_2, the left side of (9) is a polynomial in $F[X]$ not of the form $\delta_1 X^a (\delta_1 \in F)$. (Otherwise, since $p \nmid (a - b)$ and F is infinite, we would have identically

$$\frac{bX^{b-1}g(X) - X^b g'(X)}{X^{2b}} = \delta_2 X^{a-b-1} \quad (\delta_2 \in F) ,$$

which implies that $g(X)/X^b = \delta_3 X^{a-b} + \phi(X^p)$, for some rational function ϕ. But this would mean that

$$g(X) = \delta_3 X^a + \phi(X^p)X^b ,$$

contrary to hypothesis.) It follows that, for almost all β_2, we can pick a nonzero solution $X = \xi(=\xi(\beta_2))$ of (9). Obviously, as β_2 varies, $\xi(\beta_2)$ must take infinitely many distinct values (because $p \nmid (b - a)$). Next, we claim that, for almost all β_2, $g(\xi) + \beta_2\xi^a \neq 0$. For, if this were false, then we could conclude from (9) that infinitely many ξ would satisfy $ag(\xi) - \xi g'(\xi) = 0$ which would imply that $g(X) = \phi_1(X^p)X^a$, say, a contradiction. Put $\beta_3 = -(g(\xi) + \beta_2\xi^a)/\xi^b$. Then $(X - \xi)^2 | B$. Hence, for almost all β_2, $\beta_3 \neq 0$ and $\mu(B) = (1^{(n-2)}, 2^{(1)})$. This completes the proof.

We now move towards the proof of Theorem 2 and can assume $p > 0$. Take $b = 0$, $a \neq n$ and define c as in Theorem 2. However, in the meantime, we continue to allow the possibility $p | (a, n)$.

LEMMA 8. *There exist $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ in G with cycle patterns as follows*

$$\mu(\sigma_1) = (n^{(1)}),\ \mu(\sigma_2) = ((n - a)^{(1)}, a^{(1)}) ,$$
$$\mu(\sigma_3) = ((n - a)^{(1)}, (p^q)^{(a_1)}) ,\quad \mu(\sigma_4) = (c^{(1)}, (p^r)^{(s)}) ,$$

where $a = p^q a_1 (q \geqq 0, p \nmid a_1)$ *and* $n - c = p^r s (r \geqq 0, (p^r, c) = 1)$.

Note. Of course, if $a = n/2$, then σ_2 is really $(a^{(2)})$, etc.

Proof. We use Corollary 6. Write $\mu(\beta_1, \beta_2, \beta_3)$ for $\mu(\beta_1 g(X) + \beta_2 X^a + \beta_3)$.

Since $\mu(0, 0, 1) = (n^{(1)})$, the existence of σ_1 is clear. Similarly, σ_2 is present because $\mu(0, 1, 0) = ((n - a)^{(1)}, a^{(1)})$. Next, $\mu(0, 1, -1) = ((n - a)^{(1)}, (p^q)^{(a_1)})$ which yields σ_3. For σ_4, we consider $\mu(1, \beta, 0)$ for an appropriate nonzero value of β and distinguish two cases.

(i) $p | a$. We show that here we can pick β such that the part $g(X) + \beta X^a$ that is prime to X is actually square-free. This would give the existence of σ_4 with $r = 0$. For any β in F, the repeated roots of $g(X) + \beta X^a = 0$ satisfy $g'(X) = 0$. Now, $g'(X)$ is not identically zero for otherwise $g(X) \in F[X^p]$ which would mean that $f(X) \in F[t, u, X^p]$. Thus $g'(\theta) = 0$ for at most $n - 1$ nonzero values of θ. Choose any nonzero β which is not equal to $-g(\theta)/\theta^a$ for any such θ and we are through.

(ii) $p \nmid a$. By Theorem 1 we may assume that g has the form

$$g(X) = g_1(X^p)X^{a^*} + g_2(X^p),\ a^* \equiv a (\mathrm{mod}\ p) ,$$

where g_1 and g_2 are polynomials not both zero. Clearly, a repeated zero θ of $g(X) + \beta X^a$ for any given β must satisfy

$$g_1(\theta^p)\theta^{a^*} + \beta\theta^a = 0 . \tag{10}$$

Suppose g_2 is not identically zero. We can evidently choose $\beta(\neq 0)$ such that $g_1(X^p)X^{a^*} + \beta X^a$ and $g_2(X^p)$ have highest common factor X^c. Then $g(\theta) + \beta\theta^a \neq 0$ for any nonzero θ satisfying (10) and so $\mu(1, \beta, 0) = (1^{(n-c)}, c^{(1)})$.

Accordingly, suppose g_2 is identically zero. Then $c \equiv a \not\equiv 0 (\bmod p)$. By way of illustration, take $c = a$; the remaining possibilities submit to an analogous treatment. We have

$$g(X) + \beta X^a = (h(X) + \beta_1)^{p^r} X^a ,$$

say, where $r \geqq 1$, $\beta_1^{p^r} = \beta$ and $h(X) \notin F[X^p]$. By definition, h' is not identically zero and so we can easily select $\beta_1(\neq 0)$ such that $\beta_1 \neq -h(\theta)$ for any θ for which $h'(\theta) = 0$. Put $\beta = \beta_1^{p^r}$ and we find that $\mu(1, \beta, 0) = (a^{(1)}, (p^r)^{(s)})$, where here $a = c$ is not divisible by p. The result is then clear.

All future references to $\sigma_1, \cdots, \sigma_4$ will be to those permutations constructed in Lemma 8.

LEMMA 9. $G \nsubseteq A_n$.

Proof. If n is even, then σ_1 is an odd permutation. If n is odd, then σ_2 is an odd permutation whether a is even or odd.

Note. In the cases $b \neq 0$ or $a = n$ omitted from the present discussion, similar considerations show that Lemma 9 remains true except possibly when n is even and a and b are both odd or when $a = n$ is odd, $b = 0$ and both c and the degree of g are even.

Before proceeding with the proof of Theorem 2, we state a lemma which is based on some classical (but nontrivial) results on permutation groups. We let G (temporarily) be any doubly transitive subgroup of S_n. For any σ in G, let $\lambda(\sigma)$ denote the number of symbols actually moved by σ and define λ, the *minimum degree* of G to be $\min_{\sigma\neq 1} \lambda(\sigma)$.

LEMMA 10. (i) *Suppose that G contains a d-cycle, where $1 < d < n$. Then G is $(n - d + 1)$-ply transitive.*

(ii) *Suppose that $G \neq A_n$ or S_n but is $(d + 1)$-ply transitive where $d > 1$. Then $\lambda \geqq 2d$ with strict inequality unless $d = 2$ and $n = 6$ or 8 or $d = 3$ and $n = 11$ or $d = 4$ and $n = 12$.*

Proof. (i) Since G is certainly primitive, this follows from

Theorem 13.8 in [12]. (For a proof and comments on its authorship and history see [5] and the review of [5] in Mathematical Reviews.)

(ii) If $d > 1$, the inequality $\lambda \geqq 2d$ is standard (see [1, p. 150]). There may well be a direct proof of the strict inequality but I extract it from previous work. We may suppose $\lambda = 2d$. Using the table of lower bounds for λ given in Theorem 15.1 of [12] (due to W. A. Manning), we may easily check that, if $d \leqq 6$, then $n \leqq 20$. Suppose $d \geqq 7$ and $n > 12$. Then, again by [12, Theorem 15.1] and also (5)

$$\frac{2}{3}n \leqq 2d \leqq 6\sqrt{n} - 6 ,$$

which implies that $n \leqq 63$. However, if $n \leqq 63$ we cannot have $d \geqq 7$[1, p. 164]. Hence $d \leqq 6$ and $n \leqq 20$. Therefore, either $d = 2$ or $d = 3$ and G is the Mathieu group M_{11} or $d = 4$ and $G = M_{12}$. Finally, if $d = 2$ and $\lambda = 4$, it follows from G. A. Miller's list [6] of primitive groups with minimal degree 4 that G can be triply transitive only if $n = 6$ or $n = 8$. This completes the proof.

Proof of Theorem 2. We can take g to be monic. Suppose that $G \neq S_n$. By Lemma 9, $G \neq A_n$ either. (This holds, in fact, even if $p \mid (a, n)$ as does the next deduction.) With reference to σ_4, since $r = 0$ or $p \nmid c$, then $\sigma_4^{p^r}$ is a c-cycle and so, if $c > 1$, Lemma 10(i) implies that G is $(n - c + 1)$-ply transitive.

From now on suppose that $p \nmid (a, n)$ as in the hypothesis of the theorem. Then σ_3^{pq} is an $(n - a)$-cycle. Accordingly, if $a < n - 1$, then G is $(a + 1)$-ply transitive.

It follows from the above and (4) that, if both $a < n - 1$ and $c > 1$, then $2n/3 \leqq c \leqq a \leqq n/3$, a glaring contradiction. Hence, either $a = n - 1$ or $c = 1$ and, in fact, one of (i)-(iii) in Theorem 2 must hold. In particular, since we know already that f must have the form (2) when $p \nmid a$ (by Theorem 1), then, if $p \nmid a = n - 1$ and $c = 1$, necessarily $p = 2$.

It suffices, therefore, to show that, if $p \mid a$ (but $p \nmid n$), then unless f has the form (3), (i) and (ii) lead to a contradiction. We consider the two cases separately.

We begin with (ii). Thus, suppose

$$f(X) = g(X) + tX^a + u, \; p \mid a, \; a < n - 1, \; c = 1 .$$

Then actually (3) is impossible (since $c = 1$) and so $g'(X) = 0$ has a nonzero root θ. For a nonzero value of β to be chosen, set $u = -g(\theta) - \beta\theta^a$. Thus

$$f(X) = g(X) - g(\theta) + \beta(X^a - \theta^a) , \tag{11}$$

where $(X-\theta)^j \| (g(X)-g(\theta))$, say, for some $j \geqq 2$. Put $a = p^q a_1$. If $j \neq p^q$, then $(X-\theta)^k \| f(X)$, where $2 \leqq k = \min(j, p^q) \leqq p^q$. Even if $j = p^q$ this remains true for almost all β. Of course, it is possible that $f(X)$ (given by (11)) has another multiple factor, a power of $(X-\rho)$, say, where $\rho \neq \theta$ and $g'(\rho) = 0$. By (11), for almost all β, $g(\rho) = g(\theta)$ and $\rho^a = \theta^a$ which, in particular, implies that $\rho^{a_1} = \theta^{a_1}$. Hence there are at most $a_1 - 1$ candidates for ρ. Moreover, as for $X-\theta$, the exact power of any such $X-\rho$ dividing $f(X)$ does not exceed p^q for almost all β. Consequently, we can choose β so that the part of $f(X)$ comprising its factors of multiplicity exceeding 1 has degree δ, say, where $2 \leqq \delta \leqq p^q a_1 = a$. Apply Corollary 6 to this polynomial to derive the existence of σ in G with $\lambda(\sigma) = \delta$. Hence G has minimal degree $\lambda \leqq \delta \leqq a$. But G is $(a+1)$-ply transitive and so Lemma 10(ii) supplies a contradiction.

Finally, suppose that (i) holds that but f does not have form (3). Then

$$f(X) = g(X) + tX^{n-1} + u,\ p \mid n-1,\ c > 1\ ,$$

where $g(X) = X^c h(X)$, say, with $h(0) \neq 0$ and $\deg h = n - c$. By our assumptions, $g'(X) = 0$ has at least one and at most $n - c$ nonzero roots. As before, for a β in F to be chosen put $u = -g(\theta) - \beta\theta^{n-1}$. Then $X - \theta$ is a multiple factor of

$$f(X) = g(X) - g(\theta) + \beta(X^{n-1} - \theta^{n-1})\ . \tag{12}$$

Put $n - 1 = p^s n_1 (s \geqq 1,\ p \nmid n_1)$. For almost all β, if $(X-\rho)(\rho \neq \theta)$ is also a multiple factor of (12), then

$$g'(\rho) = 0,\ g(\rho) = g(\theta) \quad \text{and} \quad \rho^{n_1} = \theta^{n_1}\ , \tag{13}$$

which certainly forces $n_1 > 1$. Let $Q(X)$ be that part of $g(X) - g(\theta)$ involving $X - \theta$ and any $X - \rho$ for which ρ satisfies (13). If $n_1 > 1$, even if we take a pessimistic view, we can safely conclude that Q has degree at most $2(n-c)$, equality being possible if $g'(X)/X^{c-1}$ is square-free. On the other hand, if $n_1 = 1$, then $\deg Q \leqq n - c + 1$, equality occuring only if $g'(X) = X^{c-1}(X-\theta)^{n-c}$. Choosing a nonzero β outside a finite subset of F in the usual way, we can exhibit, using Corollary 6, a nonidentical member σ of G for which $\lambda(\sigma) \leqq 2(n-c)$ with $\lambda(\sigma) \leqq n - c + 1$, in fact, if $n_1 = 1$. Hence G is $(n - c + 1)$-ply transitive with $\lambda \leqq 2(n-c)$ which contradicts Lemma 10(ii) (since $c \leqq n - 2$) unless $c = n - 2$ and $n = 6$ or 8 or $c = n - 3$ and $n = 11$ or $c = n - 4$ and $n = 12$. However, if $n = 6, 8$ or 12, then because $n - 1$ is prime, necessarily $n - 1 = p$. Hence $n_1 = 1$ and $\lambda \leqq n - c + 1$ which now is incompatible with Lemma 10(ii). Suppose finally that $n = 11$ and $c = 8$. Then either $p = 2$ which means that $X^8 | g'(X)$ forcing $\lambda \leqq 4$ or $p = 5$ which implies that $n_1 = 2$, deg $Q \leqq 5$ so again $\lambda \leqq 5$. This yields a contradiction either way. (Alternatively, use the fact that $M_{11} \subseteqq A_{11}$.) This completes the proof.

REMARKS. When $p | n-1$, I can show that (2) holds in the excluded case (iii) unless the roots of $g'(X) = 0$ can be arranged in s nonsingleton bunches, where $1 < s \leqq n_1$, the members of each bunch giving rise to identical values of g and n_1th powers (without however $g'(X)$ being of the form $g_1(X^{n_1})$). Loosely, call any g which satisfies a condition like this *awkward*. In fact, for large n, (2) holds unless $s = 2$. Similarly, if $p | a$, we can reach beyond (2) in a description of g. Further, even if $p | (a, n)$ or $b \neq 0$, etc., we can obtain information on G and g by analogous arguments. However, the results are too fragmentary to record in detail. Nevertheless, if a specific f not covered by Theorems 1 and 2 is given, an examination of its multiple points may well yield $G = S_n$. We conclude this section by beginning the treatment of one case in which $p | (a, n)$.

Suppose $p | (a, n)$, where $a = p^q a_1 (q \geqq 1, p \nmid a_1)$ but $(n - a) \nmid p^q$ (for example, whenever $a < n/2$); in particular $a < n - 1$. Then $1 < \lambda(\sigma_3^{p^q}) \leqq n - a$. Thus, $\lambda \leqq n - a$. If, additionally, $c > 1$, then G is $(n - c + 1)$-ply transitive and Lemma 10(ii) provides a contradiction. Thus we must have $c = 1$.

4. Polynomials in $X^r > 1$. Let f be given by (1) as before. For any $r > 1$, we wish to find $G_r := G(f(X^r), F(t, u))$. Obviously, if $p > 0$, we may assume that $p \nmid r$. Note that we no longer assume throughout that F is algebraically closed; nevertheless, we appeal to the results of §§2-3 when appropriate. Some devices used in [4] come to the fore.

Let $x_1, \cdots, x_n$ be the zeros of $f(X)$ and define

$$H_r = G(f(X^r)\,, \quad F(t, u, x_1, \cdots, x_n))\,.$$

Then $H_r \cong G_r/G$. For each x_j, $j = 1, \cdots, n$, let y_j be an rth root of x_j. G_r and H_r are groups of permutations of $\{\zeta^i y_j, i = 0, \cdots, r - 1, j = 1, \cdots, n\}$, where ζ is a primitive rth root of unity. With reference to (1), let $\delta(=\delta(F))$ be the least positive divisor of r for which $(-1)^n \alpha_0/\alpha_n$ is an (r/δ)th power in $F(\alpha_0, \alpha_n)$. Evidently, if either $a = n$ or $b = 0$, then $\delta = r$. Put $\eta = ((-1)^n \alpha_0/\alpha_n)^{\delta/r}$. We know that usually $G = S_n$. The following lemma [4, Lemma 5] then narrows down the possibilites for H_r. In it, D denotes the discriminant of f and so is a polynomial in $F[t, u]$ and C_m is a cyclic group of order m.

LEMMA 11. *Suppose that $F = F(\zeta)$ and that $G = S_n$. Then either*

(14) $$H_r = C_r^{n-1} \times C_\varepsilon ,$$

where

$$\varepsilon = \begin{cases} \delta/2 , & \textit{if } \delta \textit{ is even and } \eta D \textit{ is a square in } F(t, u) , \\ \delta , & \textit{otherwise} ; \end{cases}$$

or, for some prime q dividing r,

(15) $$H_q < C_q .$$

In fact we are able to eliminate the possibility that (15) holds[1] and obtain our final theorem which is certainly applicable whenever f is one of the polynomials shown to have $G = S_n$ by either Theorem 1 or Theorem 2.

THEOREM 12. *Suppose f given by (1) is such that $G = S_n$. Let $r > 1$. Then*

$$H_r \cong C_r^{n-1} \times C_\varepsilon \times \Phi ,$$

where $\varepsilon = \delta$ or $\delta/2$, $\delta = \delta(F(\zeta))$ and Φ is the galois group of the cyclotomic extension $F(\zeta)/F$. In fact, $\varepsilon = \delta$ unless $p > 0$, δ is even and $g(X)$, X^a and X^b are linearly dependent over $F(X^p)$.

Note. Of course δ is odd whenever r is odd. Although more investigation would further limit the possibilities in which $\varepsilon = \delta/2$ could happen, some restriction is necessary, particularly for awkward g (see below).

Proof. The result is derived from Lemma 11 in a manner based on Lemma 6 of [4] to which reference is made. By symmetry, we may assume that, if $a = n$, then $b = 0$.

We note first that, if $g(X)$, X^a and X^b are linearly independent over $F(X^p)$, then the care we took in Lemma 7 to ensure that $\beta_3 \neq 0$ (and $\beta_2 \neq 0$, if $a = n$) now repays us with the conclusion that the part of the discriminant D which is prime to u (and t) has a nontrivial irreducible factor of multiplicity 1. Hence ηD cannot be a square in $F(t, u)$ and hence, granted (14) holds, we must have $\varepsilon = \delta$.

Accordingly, it suffices to assume that $F = F(\zeta)$ and show that (15) is impossible. Suppose, to the contrary, that q is a prime divisor of r for which (15) holds. Replacing F by its algebraic closure does not affect this property, so we may assume that, in fact, F is

[1] There are occurrences of (15) with f not of the form (1); these have been classified by the author and W. W. Stothers.

algebraically closed. Actually, (15) can be interpreted to say that any member of H_q has cycle pattern $(1^{(nq)})$ or $(q^{(n)})$. We distinguish two cases.

(i) $b \neq 0$. Put $a - b = p^k d (k \geqq 0, p \nmid d)$. Then $\mu(X^a - X^b) = ((n-a)^{(1)}, (p^k)^{(d)}, b^{(1)}) = \mu$, say, while, as a cycle pattern of degree qn we have

$$\mu(X^{q^a} - X^{q^b}) = ((q(n-a))^{(1)}, (p^k)^{(dq)}, (bq)^{(1)}) = \mu_r ,$$

say. Thus (cf. [4, Lemma 6]), by Corollary 6, there exists σ in G_q with $\mu(\sigma) = \mu_r$ whose restriction in G has $\mu(\sigma) = \mu$. Let $m = $ l.c.m. $\{p^k, n-a, b\}$. Since $q \neq p$, q does not divide both m/b and $m/(n-a)$. Accordingly, σ^m is in H_q while $\mu(\sigma^m) = (1^{(q(n-j))}, q^{(j)})$, where $1 \leqq \min(b, n-a) \leqq j \leqq n - a + b \leqq n - 1$, a contradiction.

(ii) $b = 0$. Since $g(X)/X^a$ is certainly not a constant we can always express $g(X)/X^a$ as $h^{p^i}(X)$, where $i \geqq 0$ and $h(X)$ is a rational function not in $F(X^p)$. Accordingly, $h'(X)$ is not identically zero and we can pick $\beta \in F$ such that $\beta \neq -h(\theta)$ for any nonzero θ for which $h'(\theta) = 0$. Now with c as in Theorem 2, put $n - c = p^k d (k \geqq 0, p \nmid d)$. Then, as in case (i),

$$\mu(g(X) + \beta X^a) = ((p^k)^{(d)}, c^{(i)}) = \mu ,$$
$$\mu(g(X^q) + \beta X^{aq}) = ((p^k)^{(dq)}, (cq)^{(1)}) = \mu_r ,$$

say. Thus there exists σ in G_r with $\mu(\sigma) = \mu_r$ whose restriction in G has cycle pattern μ. Put $m = p^k c$. Then $\sigma^m \in H_r$ and $\mu(\sigma^m) = (1^{(q(n-c))}, q^{(c)})$, $1 \leqq c < n$; again a contradiction. This completes the proof.

We conclude with an example for which $\varepsilon = \delta/2$ in (14) with f not even of the shape (2). Let $p = 5$, $r = 2$ and F be algebraically closed. Put

$$f(X) = X^8 - X^6 + 2X^4 + tX^5 + u .$$

Then $G = S_8$ but $D = \alpha u^3(t^2 - (u+2)^2)^2 (\alpha \in F)$ so that uD is a square in $F(t, u)$. Hence $\varepsilon = 1 = \delta/2$ in this case!

References

1. R. Carmichael, *Introduction to the theory of Groups of Finite Order*, Dover, 1956.
2. J. W. S. Cassels and A. Frohlich (Editors), *Algebraic Number Theory*, Academic Press, New York and London, 1967.
3. S. D. Cohen, *Uniform distribution of polynomials over finite fields*, J. London Math. Soc., (2), **6** (1972), 93-102.
4. ———, *The distribution of the galois groups of integral polynomials*, Illinois J. Math., **23** (1979), 135-152.

5. R. Levingston and D. E. Taylor, *The theorem of Marggraff on primitive permutation groups which contain a cycle*, Bull. Austral. Math. Soc., **15** (1974), 125-128; MR **54** (1977), #12, 870.
6. G. A. Miller, *On the primitive groups of class* 4, Amer. Math. Monthly, **9** (1902), 63-66.
7. ———, *Limits of the degree of transitivity of substitution groups*, Bull. Amer. Math. Soc., **22** (1915), 68-71.
8. E. T. Parker, *On quadruply transitive groups*, Pacific J. Math., **9** (1959), 829-836.
9. J. H. Smith, *General trinomials having symmetric Galois group*, Proc. Amer. Math. Soc., **63** (1977), 208-212.
10. K. Uchida, *Galois group of an equation* $X^n-aX+b=0$, Tohoku Math. J., **22** (1970), 670-678.
11. H. Wielandt, *Abschätzungen für den Grad einer Permutationsgruppe von vorgeschriebenem Transitivitätsgrad*, Schr. Math. Sem. Inst. angew. Math. Univ. Berlin, **2** (1934), 151-174.
12. ———, *Finite Permutation Groups*, Academic Press, New York and London, 1964.

Received May 9, 1979.

UNIVERSITY OF ILLINOIS
URBANA, IL 61801
Permanent address:
UNIVERSITY OF GLASGOW
GLASGOW G12 8QW
SCOTLAND