PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 63, Number 2, April 1977

GENERAL TRINOMIALS HAVING SYMMETRIC GALOIS GROUP

JOHN HOWARD SMITH

ABSTRACT. Let a and b be independent transcendentals over a field F and let $n > k$ be integers > 1 with $n, k, n - k$ and the characteristic of F pairwise relatively prime. Then the Galois group of $x^n + ax^k + b$ over $F(a, b)$ is S_n.

It is well known (e.g. p. 175 of [3]) that the Galois group of the general polynomial, $X^n + a_1X^{n-1} + \cdots + a_n$ is the full symmetric group on the roots. Uchida [2] has shown that with suitable conditions on the characteristic the same is true of the polynomial $X^n + aX + b$. In this note we extend Uchida's methods and result to the case $X^n + aX^k + b$, where $(k, n) = 1$ (obviously a necessary condition).

LEMMA 1. *Let a and b be independent variables over a field F. Let $(m, n) = 1$, $m, n \in Z^+$ and let $rm + sn = 1$, $r, s \in Z$. Let $c = b^s a^r$ and let the ring $R = F[a, b, c] = F[a, b] \subset F(a, b)$. Then for any nonzero u, v in F, if P is the principal ideal $(ua^n - vb^m)$ in R, then R/P is the polynomial ring over F in one variable. (In particular P is prime.)*

PROOF. If $\bar{a}, \bar{b}, \bar{c}$ denote the images of a, b, c modulo P then $\bar{b} = (u/v)^r \bar{c}^n$, $\bar{a} = (v/u)^s \bar{c}^m$ so $R/P = F[\bar{c}]$. To see that $\bar{c}$ satisfies no polynomial over F we note that since R has transcendence degree 2 over F, R/P must have transcendence degree (at least) 1.

LEMMA 2. *Let a, b be independent transcendentals over a field F and let $K = F(a, b)$. Then $x^n + aX^k + b$ is irreducible in $K[X]$.*

PROOF. It suffices to show irreducibility for some specialization of the coefficients; in this case let $a = 0$ and apply the Eisenstein criterion.

LEMMA 3. *Let $B = (b_{ij})$ be an $n \times n$ matrix such that $b_{ij} = 0$ unless $j - i \equiv m$ or k (mod n). Suppose further that $(m - k, n) = 1$. Then the only nonzero terms in the determinant are $\prod_i b_{ii+m}$ and $\prod_i b_{ii+k}$ (with appropriate signs).*

PROOF. Elementary.

Received by the editors December 10, 1974 and, in revised form, June 13, 1975 and February 24, 1976.

AMS (MOS) subject classifications (1970). Primary 12A20, 12A55, 12F10.

LEMMA 4. *If* $(k, n) = 1$ *and the polynomial* $X^n + aX^k + b$ *with coefficients in a field* K *is irreducible, then its discriminant is*:

$$(-1)^{n(n-1)/2} b^{k-1} \left[n^n b^{n-k} + (-1)^{(n+1)k} (n-k)^{n-k} k^k a^n \right].$$

(*See Note added in proof.*)

SKETCH OF PROOF. If the roots of $f(X) = 0$ are $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ the discriminant is

$$(-1)^{n(n-1)/2} \Pi_i f'(\alpha_i).$$

Multiplication by $f'(\alpha)$ is a K-linear map of $K[\alpha]$ to itself whose determinant is the norm of $f'(\alpha)$ or $\Pi_i f'(\alpha_i)$.

The determinant is computed with respect to the basis $1, \alpha, \ldots, \alpha^{n-1}$ using Laplace expansion on the first column, elementary row operations, and Lemma 3.

LEMMA 5. *Suppose that the characteristic of* F *is prime to* n, k *and* $n - k$ *and that* $(k, n) = 1$. *Then, if* a, b *are independent over* F, *the Galois group of* $f(X) = X^n + aX^k + b$ *over* $K = F(a, b)$ *contains a transposition.*

PROOF. Since $nf(X) - Xf'(X) = (n-k)aX^k + nb = h(X)$, any common zeros of f and f' are also zeros of h, i.e. kth roots of $-nb/(n-k)a$.

We consider the ring $R = F[a, b, c]$ with c as in Lemma 1 and the ideal (prime by Lemma 1) $P = (n^n b^m + (-1)^{(n+1)k} m^m k^k a^n)$, where $m = n - k$. Let $\bar{R} = R/P$ and let $\bar{K}$ be the field of quotients. The polynomial $\bar{f}(X) = X^n + \bar{a}X^k + \bar{b}$ certainly has a repeated zero, $\bar{\alpha}$, in some extension field of $\bar{K}$ since its discriminant vanishes by Lemma 4. On the other hand, if $\bar{\alpha}$ and $\bar{\beta}$ are repeated zeros of $\bar{f}$ then $\bar{\alpha}^k = \bar{\beta}^k = -n\bar{b}/(n-k)\bar{a}$ and $\bar{\alpha}^n = \bar{\beta}^n = -k\bar{b}/(n-k)$, hence, since $(n, k) = 1$, $\bar{\alpha} = \bar{\beta}$. Further a triple zero of $\bar{f}$ would be a double zero of $\bar{h}$, but the latter has distinct roots by our assumption on the characteristic.

Now an irreducible factor of f cannot have a double root since the hypotheses imply that the characteristic is not 2. If two irreducible factors have a root in common they are both linear.

Hence $\bar{f} = \bar{f}_1 \ldots \bar{f}_m$ where the $\bar{f}_i$ are monic and pairwise relatively prime in $\bar{K}[X]$, $\bar{f}_1(X) = (X - \bar{\alpha})^2$ and $\bar{f}_2, \ldots, \bar{f}_m$ are irreducible. Since $\bar{R}$ is integrally closed in $\bar{K}$ by Lemma 1 the factorization can be carried out over $\bar{R}$.

By Hensel's Lemma we may then factor over the completion K_P of K with respect to the prime ideal P into $f = f_1 \ldots f_m$ with each f_i having coefficients in the completion R_P and reducing to $\bar{f}_i$ modulo P.

Since the $\bar{f}_i$ are irreducible for $i \geqslant 2$ and have the same degrees as the f_i, the extensions generated over K_P by roots of the latter are unramified. However since $P = (\Pi_{i<j}(\alpha_i - \alpha_j))^2, P$ ramifies if we adjoin all the roots of f, it must

ramify if we adjoin a root of f_1; in particular the latter is irreducible over K_P. Hence the inertia group of the splitting field of f over K_P leaves the roots of f_i fixed for $i \geqslant 2$ and interchanges those of f_1. This completes the proof.

LEMMA 6. *Let G be a transitive permutation group on $A = \{\alpha_1, \ldots, \alpha_n\}$. Suppose G includes σ, which permutes $\{\alpha_1, \ldots, \alpha_k\} = A'$ cyclicly, and τ, which permutes $\{\alpha_{k+1}, \ldots, \alpha_n\} = A''$ cyclicly. (This says nothing about how σ acts on A'' or τ on A'.) Then if $(k, n) = 1$, G is primitive.*

PROOF. Suppose there is a system of imprimitivity. For each block B let $B' = A' \cap B$, $B'' = A'' \cap B$. Neither is empty, for if, for example, $B'' = \varphi$, i.e. $B \subset A'$ then the blocks contained in A' would be a system of imprimitivity for the action of H, the subgroup generated by σ, on A'. Hence the order of B, a divisor of n, would also divide k.

Now H permutes the B' cyclicly, hence permutes the B cyclicly. Hence, the number of blocks (a divisor of n), divides k. This is impossible since there is more than one block.

To apply Lemma 6 to our equation we look for σ, τ in the decomposition groups of appropriate valuations. For the sake of symmetry it will be convenient to work temporarily with $\alpha X^n + \beta X^k + \gamma$, which clearly has the same Galois group as the original. We first prove a form of Hensel's Lemma.

LEMMA 7. *Let F be a field, let α, β, γ be independent transcendentals over F and let $A = F(\beta)[[\alpha, \gamma]]$ (power series in α, γ with coefficients in $F(\beta)$). Let $B = A/(\alpha\gamma)$ and for any $g(X) \in A[X]$ let $\bar{g}(X) \in B[X]$ denote the reduction. Suppose $k < n - k$. Then $f(X) = \alpha X^n + \beta X^k + \gamma$ can be factored $f(X) = f_1(X)f_2(X)$, with $f_1(X), f_2(X) \in A[X]$, $\bar{f}_1(X) = X^k + \overline{\gamma/\beta}$, $\bar{f}_2(X) = \bar{\alpha}X^{n-k} + \bar{\beta}$.*

PROOF. We apply Bourbaki's form of Hensel's Lemma (p.215 of [1]). A is a complete linearly topologized ring under the topology given by total order in α and γ, $M = (\alpha\gamma)$ is an ideal whose elements are topologically nilpotent. Further, $\bar{f}(X) = \bar{f}_1(X)\bar{f}_2(X)$ where $\bar{f}_1(X) = X^k + \overline{\gamma/\beta}$, $\bar{f}_2(X) = \bar{\alpha}X^{n-k} + \bar{\beta}$ and these are strongly relatively prime since the ideal they generate in $B[X]$ contains $\overline{\alpha\beta}X^k + \overline{\alpha\gamma} = \overline{\alpha\beta}X^k$, hence $\bar{\alpha}X^k$, hence $\bar{\alpha}X^{n-k}$, hence $\bar{\beta}$, a unit. The existence of the desired $f_1(X), f_2(X)$ follows.

LEMMA 8. *Let $F, \alpha, \beta, \gamma, f$ be as in Lemma 7. Suppose the characteristic of F is prime to k and $n - k$ and that $n \neq 2k$. Then the roots of f may be so numbered that there are σ, τ in the Galois group of f over $F(\alpha, \beta, \gamma)$ permuting $\alpha_1, \ldots, \alpha_k$ and $\alpha_{k+1}, \ldots, \alpha_n$, respectively, cyclicly.*

PROOF. Assume $k < n - k$. (The case $k > n - k$ is similar.) Let A be as in Lemma 7, $L = F(\beta)\{\{\alpha, \gamma\}\}$ its field of quotients (formal Laurent series in α

and γ over $F(\beta)$), $C = F(\beta)\{\{\alpha\}\}[[\gamma]]$, $D = F(\beta)\{\{\gamma\}\}[[\alpha]]$. Let I be the ideal of C generated by γ and J the ideal of D generated by α.

The Galois group of f over L is a subgroup (as a group of permutations on the roots) of its group over $F(\alpha, \beta, \gamma)$.

Factor $f(X)$ into $f_1(X)f_2(X)$ over A as in Lemma 7 and let $\alpha_1, \ldots, \alpha_k$ be the roots of $f_1(X)$, $\alpha_{k+1}, \ldots, \alpha_n$ those of $f_2(X)$. We regard $f_2(X)$ as a polynomial in $C[X]$ and reduce modulo I, getting a polynomial with distinct roots $\bar{f}_2(X) = \bar{\alpha}X^{n-k} + \bar{\beta}$ by the assumption on the characteristic. The group of this polynomial has an element which permutes the roots cyclicly, hence so does the group of $f_2(X)$ by the theorem of p. 190 of [3]. (Although $f_2(X)$ is not monic, its leading coefficient is a unit in C so it may be treated as monic.)

Now we replace X by $1/Y$ in $f_1(X)$ and multiply by Y^k to get $g_1(Y) \in A[Y]$, $g_1(Y) \equiv 1 + (\gamma/\beta)Y^k \pmod{\alpha\gamma}$ whose roots are the reciprocals of those of $f_1(X)$. Regarding $g_1(Y)$ as an element of $D[Y]$ and reducing modulo J we get a polynomial with distinct roots whose Galois group has an element which permutes them cyclicly. Hence the same is true for $g_1(Y)$, hence for $f_1(X)$. This completes the proof.

REMARK. By dividing by α to get $X^n + (\beta/\alpha)X^k + (\gamma/\alpha)$ we see that we may apply Lemma 8 to the equation, $X^n + aX^k + b$, where a and b are independent transcendentals.

We now state precisely and prove the main result.

THEOREM. *Let the characteristic of the field F be prime to k, n and $n - k$, and suppose $(n, k) = 1$. Let a, b be independent over F. Then the Galois group of $f(X) = X^n + aX^k + b$ over $K = F(a, b)$ is the full symmetric group on the roots.*

PROOF. The group is transitive by Lemma 2 and hence primitive by Lemmas 6 and 8. Since it contains a transposition by Lemma 5 it is S_n by Theorem 13.3 of [4].

The above leads to the conjecture that, subject to appropriate restrictions on the characteristic of F, the Galois group of $F(X) = X^n + \sum_I a_i X^i$ over $K = F(a_i, i \in I)$ is the full symmetric group, where I is any subset of $\{0, \ldots, n-1\}$ containing 0 and such that g.c.d.$(n, i, i \in I) = 1$, and the a_i are independent over F. By taking specializations one can use the above theorem to show that this is the case if some $i \in I$ is prime to n; the smallest uncovered case is thus $f(X) = X^6 + aX^3 + bX^2 + c$.

NOTE ADDED IN PROOF. See also P. Lefton, *On the Galois groups of cubics and trinomials*, Bull. Amer. Math. Soc. **82** (1976), 754–755, and the references cited there.

REFERENCES

1. N. Bourbaki, *Elements of mathematics. Commutative algebra*, Hermann, Paris; Addison-Wesley, Reading, Mass., 1972. MR **50** #12997.

2. K. Uchida, *Galois group of an equation* $X^n - aX + b = 0$, Tôhoku Math. J. (2) **22** (1970), 670–678. MR **43** #3238.

3. B. L. van der Waerden, *Modern algebra*, Vol. 1, Springer-Verlag, Berlin, 1937; rev. English transl., Ungar, New York, 1953. MR **2**, 120; **10**, 587.

4. H. Wielandt, *Finite permutation groups*, Lectures, Univ. of Tübingen, 1954/55; English transl., Academic Press,New York, 1964. MR **32** #1252.

DEPARTMENT OF MATHEMATICS, BOSTON COLLEGE, CHESTNUT HILL, MASSACHUSETTS 02167