multiplicities of the zeros equals $2h$ is the exact analog for Maass wave forms of the theorem of Hecke for holomorphic forms mentioned in the introduction. This follows from the result about zeros of Selberg zeta functions mentioned at the beginning of Section 2.

The theorem also gives the surprising result that all other zeros of $Z(s, \pi^+)$ and $Z(s, \pi^-)$ are equal and occur with the same multiplicity. The author has no explanations for this.

References

[1] H. Feldmann, *Über das Verhalten der Modulfunktionen von Primazahlstufe bei beliebigen Modulsubstitution*, Abh. Math. Seminar der Hamburg Univ. 8 (1931), 323–347.

[2] K. Hashimoto, *Representations of the Finite Symplectic Group* SP (4, F_p) in *The Selberg Trace Formula and Related Topics* (edited by D. Hejhal, P. Sarnak and A. Terras), Contemporary Mathematics 53, Amer. Math. Soc., 1986.

[3] E. Hecke, *Mathematische Werke*, Vandenhoeck und Ruprecht, Göttingen 1983.

[4] D. Hejhal, *The Selberg Trace Formula for* PSL (2, R), Vol. II, Lecture Notes in Mathematics 1001, Springer-Verlag, New York 1983.

[5] H. Huber, *Über die Darstellungen der Automorphismengruppe einer Riemannschen fläche in den Eigenräumen des Laplace-operators*, Comment. Math. Helvetici 52 (1977), 177–184.

[6] S. Lang, *Elliptic Functions*, Springer-Verlag, New York.

[7] H. Saito, *On the representation of* SL_2 (F_q) *in the spaces of Hilbert modular forms*, J. Math. Kyoto Univ. 15 (1975), 101–128.

[8] P. Sarnak, *Class numbers of indefinite binary quadratic forms*, J. Number Theory 15 (1982), 229–247.

[9] J. Stopple, *A Functional Equation for some Selberg Zeta Functions*, Thesis, University of California at San Diego, 1986.

[10] — *Some Explicit Cases of the Selberg Trace Formula for Vector Valued Functions*, to appear in Trans. Amer. Math. Soc.

[11] S. Tanaka, *Construction and classification of irreducible representations of special linear group of the second order over a finite field*, Osaka J. Math. 4 (1967), 65–84.

MATHEMATICS DEPARTMENT
UNIVERSITY OF CALIFORNIA
Santa Barbara, CA 93 106
USA

Received on 5.11.1987
and in revised form on 30.5.1988 (1764)

ACTA ARITHMETICA
LIV (1989)

Galois groups of trinomials

by

STEPHEN D. COHEN (Glasgow)

1. Introduction. Let $f(X)$ denote a trinomial of the form

$$f(X) = X^n + aX^r + b, \tag{1}$$

where a and b are rational integers. We always assume that f is irreducible over Q which implies that $G(f) (= G_Q(f))$, the Galois group of f over Q, is a transitive subgroup of the full symmetric group S_n acting on the zeros of f. Various authors, including Uchida [12], Yamamoto [13], Ohta [9] and Nart and Vila [8] have shown that, when $r = 1$, then, under certain specific simple conditions, $G(f) = S_n$ itself. (See also Yamamura [14].)

Recently, H. Osada [10], [10a], in extending these results, has shown that for arbitrary r, necessarily with n, r co-prime, i.e.

$$(n, r) = 1, \tag{2}$$

a similar conclusion can be drawn under conditions which we summarise.

Let $d = (a, b)$ and put $a = da_0$, $b = db_0$. Assume that

$$(a, n) = 1, \tag{3}$$

$$d = c^n \quad \text{for some integer } c, \tag{4}$$

$$d \text{ is a unitary divisor of } b, \text{ i.e. } (d, b_0) = 1, \tag{5}$$

$$(r(n-r), b_0) = 1. \tag{6}$$

Then $G(f) = S_n$ in either of the following two situations.

I. $b_0 = b_1^r$ for some integer b_1 (e.g. $r = 1$) or $r = 2$.

II. For some prime p, $p \| b_0$ (i.e. $p | b_0$ but $p^2 \nmid b_0$) and the integer $|D_0(f)|$ is a non-square, where

$$D_0(f) = n^n b_0^{n-r} + (-1)^{n-1} r^r (n-r)^{n-r} a_0^n d^r$$

is related to the discriminant $D(f)$ of f by

$$D(f) = (-1)^{n(n-1)/2} b_0^{r-1} d^{n-1} D_0(f).$$

(The restriction of r to certain values in [10] was dispensed with in [10a].)

In this paper we focus on situation II with essentially arbitrary $r\ (>1)$, supposing that $p\|b_0$ for some prime $p\nmid a$ but greatly easing the other constraints. We dispense with (3)–(5) (thus allowing $(a, n) > 1$ or $(a, b) > 1$ to hold in a significant sense). Moreover, (6) (which ensured that much underlying ramification was tame) is weakened to an assumption merely that $p\nmid(n-r)$ or $p = n-r$ (thus permitting $(r, b) > 1$). Typically, for all r with $2 \leqslant r \leqslant n-3$, we can show that $G(f)$ contains the alternating group A_n. Combining these arguments with the well-known fact ([6], Theorem 41) that $G(f) \subseteq A_n$ if and only if $D(f)$ is a square yields useful sufficient conditions for $G(f) = S_n$ to hold. To check these, it is by no means always necessary to calculate $D(f)$ – notably, it is usually enough for r to be even. (Incidentally, if (3), (5) and (6) hold, then $D(f)$ cannot be a square when $|D_0(f)|$ is itself a non-square, in agreement with Osada's findings.)

We state the main theorems. These extend the result sketched above to the case in which $p^k\|b$. Otherwise, they involve notation already introduced.

THEOREM 1. *Let $f(x)$ given by* (1) *and satisfying* (2) *be irreducible over Q and such that $b = p^k b^*$ for some prime $p\nmid ab^*$ and $k \geqslant 1$. Suppose that $2 \leqslant r \leqslant n-3$ with $(r, k) = 1$ and $p\nmid(n-r)$. Then (with possible exceptions when $n = 11, r = 8, p = 2$ or $n = 23, r = 20, p = 2$ or 5) $G(f)$ contains A_n. Further $G(f) = S_n$ provided $D(f)$ is a non-square which certainly is true if any one of the following* (7)–(9) *holds.*

(7) r *is even (provided* $p\nmid r$ *or* $p = 2 = r$);

(8) n *is even, d is a non-square and* $(d, nb_0) = 1$;

(9) $D(f) < 0$ (*e.g.* $n \equiv 3 \pmod 4$ *and a and b are positive*).

THEOREM 2. *Let*

$$f(X) = X^n + aX^{n-p} + p^k b^*, \quad p\nmid nab^*k, \quad p \leqslant n-3,$$

be irreducible over Q. Then $G(f)$ contains A_n. Indeed $G(f) = S_n$ provided $p = 2$ or $D(f)$ is a non-square (which occurs if either (8) *or* (9) *holds).*

Illustrations of the theorems are legion and can readily be written down. For instance, by using Lemma 9 of [10] or Eisenstein's criterion to guarantee irreducibility, we can state unconditionally that $G(f)$ is the full symmetric group for each of the polynomials listed below.

$X^{2m} + X^r + 2$, $(r, m) = 1$, r, m odd;

$X^n + X^2 + 2$, n odd;

$X^n - X^{n-2} + 2$, n odd;

$X^n + X^{2r} + 2$, $(2r, n) = 1$ and $n \equiv 3 \pmod 4$, or

$n \equiv 1 \pmod 4$ and $n/4 < r < (n-1)/2$;

$X^n + 3X^r + 3p$, $(n, r) = 1$, $p\nmid 3(n-r)$, $2 \leqslant r \leqslant n-3$,

$n \equiv 3 \pmod 4$ if $2p|r$,

$n \not\equiv 0, 1, 5$ or $6 \pmod{12}$ if r odd.

Note (inserted at revision). This paper was prepared before the sequel [10a] by Osada to [10] appeared. While there is some overlap between [10a] and the present article, essentially they are complementary. It is suggested that the reader's appreciation of either would be enriched by a study of the other.

2. $G(f)$ is primitive. A special case of a result of Fried and Schinzel ([4], Lemma 1 with $n = 0$) implies that, in our situation, the trinomial f is functionally indecomposable which, as we now see, is equivalent to $G(f)$ being primitive.

LEMMA 3. *Let f be an irreducible trinomial of the form* (1) *satisfying* (2) *over a field K of characteristic zero. Then $G_K(f)$ is primitive (as a permutation of the zeros of f in a splitting field L).*

Proof. As stated above, it suffices to assume that G is imprimitive and deduce that f is functionally decomposable.

Let the zeros of f be $\alpha_1, \ldots, \alpha_n$. Suppose that G is imprimitive and that $A = \{\alpha_1, \ldots, \alpha_s\}$ (say), where $s|n$ and $1 < s < n$, is a subset of imprimitivity. Put $G_A = \{\sigma \in G_K(f)\colon \sigma(A) = A\}$. Then the fixed field L_A of G_A is a proper subfield of $K(\alpha_1)$ ([11], Prop. 3.4) and hence $L_A = K(\beta_1)$, say, where $\beta_1 = h(\alpha_1)$ for some polynomial $h(X)$ in $K[X]$ which can be assumed to be monic. Since $G(f)$ is transitive it contains $\sigma_1, \ldots, \sigma_s$, such that $\sigma_i(\alpha_1) = \alpha_i$, $i = 1, \ldots, s$. Indeed, by the nature of A, $\sigma_i \in G_A$ and $h(\alpha_i) = \sigma_i(\beta_1) = \beta_1 = h(\alpha_1)$ for each $i = 1, \ldots, s$.

Now apply $G(f)$ to the polynomial $h(X) - \beta_1$ to produce in all $t = n/s$ conjugates $h(X) - \beta_j$ each of whose zeros comprise s of the zeros of f. Moreover, their product is invariant under $G(f)$ and therefore has coefficients in K. Clearly

$$f(X) = \prod_{j=1}^{t} (h(X) - \beta_j) = g(h(X)),$$

where $g(x) = (X - \beta_1) \ldots (X - \beta_t)$ has coefficients in K by the construction of $\beta_1, \ldots, \beta_t$. Thus f is decomposable and the proof is complete.

3. Cycles and transitivity. Within the proof of Theorem 3 of [10], Osada showed that in the circumstances, for r prime, $G(f)$ contained a permutation acting as an r-cycle (by which is meant a cycle of length r) on the zeros of f. Our key is a significant extension of this idea based on a study of the ramification of p working in the p-adic field Q_p and its extensions. For this, we refer, for example, to [7], Chapter 6.

LEMMA 4. *Let $f(X)$ be the trinomial* (1) *with $b = p^k b^*$, where $k \geqslant 1$ and $p \nmid ab^*$. Suppose that f, irreducible over Q, has a zero α in a splitting field. Then, over Q_p, $f(X)$ factorises as*

$$f(X) = g(X)h(X), \tag{10}$$

where $\deg g = r$, $g(X) \equiv X^r$ *and* $h(X) \equiv X^{n-r}+a \pmod p$. *Corresponding to this factorisation the prinicipal ideal (p) in $Q(\alpha)$ splits as a product*

$$(p) = \mathfrak{a}\mathfrak{b} \tag{11}$$

of relatively prime ideals such that $\mathfrak{p}|\alpha$ for any prime ideal $\mathfrak{p}$ dividing $\mathfrak{a}$ and $\mathfrak{p}|\alpha^{n-r}+a$ if $\mathfrak{p}|\mathfrak{b}$. More precisely,

(i) *if $(r, k) = 1$, then g is irreducible over Q_p and $\mathfrak{a} = \mathfrak{p}^r$ for some prime ideal $\mathfrak{p}$;*

(ii) *if $n-r = p^t m$ and $p \nmid km$ (when $t > 0$) then any irreducible factor of h has degree divisible by p^t and $\mathfrak{b} = \mathfrak{b}_1^{p^t}$ for some square-free ideal $\mathfrak{b}_1$.*

Proof. The factorisations (10) and (11) can be deduced by Hensel's lemma from

$$f(X) \equiv X^r(X^{n-r}+a) \pmod p.$$

To add to this description consider the normal extension $K = Q(\gamma, \zeta)$, where $\gamma^m = -a$ and ζ is a primitive mth root of unity, a field in which p is unramified. Let $\mathfrak{P}$ be a prime ideal of K dividing p and $K_{\mathfrak{P}}$ the corresponding completion. Once more by Hensel's lemma, we have a factorisation

$$h(X) = h_1(X) \ldots h_m(X)$$

over $K_{\mathfrak{P}}$, where

$$h_i(X) \equiv X - \zeta^{i-1}\gamma \pmod{\mathfrak{P}}, \quad i = 1, \ldots, m.$$

This yields, in the first place, the result of (ii) when $t = 0$.

Now let $\mathfrak{p}$ be any prime ideal dividing p in $L = Q(\alpha)$ with completion $L_{\mathfrak{p}}$. With reference to (i) and (ii), we consider two cases.

(i) $L_{\mathfrak{p}} = Q_p(\alpha)$, where $g(\alpha) = 0$, and $(r, k) = 1$. Clearly $\mathfrak{p}|\alpha$ and $\deg [L_{\mathfrak{p}}: Q_p] \leqslant r$. Let $v_{\mathfrak{p}}$ denote the (additive) $\mathfrak{p}$-adic valuation on $L_{\mathfrak{p}}$. Then $v_{\mathfrak{p}}(\alpha^{n-r}+a) = 0$ since $p \nmid a$ and

$$rv_{\mathfrak{p}}(\alpha) = v_{\mathfrak{p}}(\alpha^r(\alpha^{n-r}+a)) = v_{\mathfrak{p}}(-p^k b^*) = kv_{\mathfrak{p}}(p) \leqslant kr;$$

indeed equality holds here because $(k, r) = 1$. Hence g is irreducible over $Q_{\mathfrak{p}}$ and (i) follows.

(ii) $L_{\mathfrak{p}} = Q_p(\alpha)$, where $h(\alpha) = 0$, and $p \nmid k$. Let $\bar{\mathfrak{p}}$ in $L(K)$ divide both $\mathfrak{P}$ and $\mathfrak{p}$ and $L_{\bar{\mathfrak{p}}}$ be the corresponding completion. Clearly

$$kv_{\bar{\mathfrak{p}}}(p) = v_{\bar{\mathfrak{p}}}(-p^k b^*) = v_{\bar{\mathfrak{p}}}(\alpha^r(\alpha^{n-r}+a)) = p^t w,$$

where $w = v_{\bar{\mathfrak{p}}}(\alpha - \zeta^i\gamma)$ with $\alpha \equiv \zeta^i\gamma \pmod{\bar{\mathfrak{p}}}$. Since $p \nmid k$, then $p^t | v_{\bar{\mathfrak{p}}}(p) = v_{\mathfrak{p}}(p)$ because p is unramified in K. This completes the proof.

Write $G^{(m)}(f)$ for the stabiliser of m of the zeros of f regarded as a permutation of the remaining $n-m$ zeros.

COROLLARY 5. *Suppose that f is an irreducible trinomial as in Lemma 4.*

(i) *If $(k, r) = 1$ and $p \nmid n-r$, then $G^{(n-r)}(f)$ is transitive. Indeed $G(f)$ contains an r-cycle if $p \nmid r$ or $p = r$.*

(ii) *If $p \nmid kn$ and $r = n-p$, then $G(f)$ contains a p-cycle.*

Proof. Let $\mathfrak{p}$ be a prime ideal of the splitting field L of f dividing p with corresponding completion $L_{\mathfrak{p}}$. Naturally, $\mathrm{Gal}(L_{\mathfrak{p}}/Q_p)$ can be regarded as a subgroup of $G_Q(f)$. We also have a tower of extensions

$$Q_p \subseteq L_D \subseteq L_I \subseteq L_T \subseteq L_{\mathfrak{p}},$$

wherein L_D and L_I are the decomposition and inertia fields of $\mathfrak{p}$ and L_T is the maximal tamely ramified extension of Q_p in $L_{\mathfrak{p}}$, itself a normal extension of L_I. Then, in particular, $\mathrm{Gal}(L_T/L_I)$ is cyclic of order prime to p and $\mathrm{Gal}(L_{\mathfrak{p}}/L_T)$ is a p-group (see [7], § 6.2). Some implications of this for the factorisation (10) are as follows.

(a) Suppose that $p \nmid (n-r)$ and $(k, r) = 1$. Then, over L_D, g is irreducible (of degree r) and remains so over L_I and h splits completely. Thus $\mathrm{Gal}(L_{\mathfrak{p}}/L_I)$ $(\subseteq G^{(n-r)}(f))$ is transitive and indeed cyclic of order r if $p \nmid r$.

(b) Suppose that $p = r \nmid kn$. Then, over L_D, h splits completely while g is irreducible of degree p, remaining thus over L_T. In this simple case, the p-group $\mathrm{Gal}(L_{\mathfrak{p}}/L_T)$ must be cyclic, a generator yielding a p-cycle in $G(f)$.

(c) Suppose that $p = n-r \nmid kn$. Here g (irreducible over L_D) splits completely in L_T. On the other hand h is irreducible of degree p over L_T. We therefore obtain a p-cycle as in (b).

4. Synthesis. We draw together our previous conclusions and apply them to the situations of Theorems 1 and 2. For convenience, simultaneously denote r in Theorem 1 and p in Theorem 2 by m so that certainly $2 \leqslant m \leqslant n-3$. By Marggraff's theorem (see [1], § 160), because $G^{(n-m)}(f)$ is transitive, then $G(f)$ is $n-m+1$ transitive; a separate consequence when $m = 2$ or m is even and $p \nmid m$ being that $G(f) \nsubseteq A_n$. The classification theorem of finite simple groups now implies (see [2], Corollary 5.4) that either $A_n \subseteq G(f)$ or $n-m+1 \leqslant 5$, i.e. $m \geqslant n-4$. The only 4 or 5 transitive groups, however, are the Mathieu groups M_n $(n = 11, 12, 23, 24)$ which are contained in A_n and yet (as was known to Frobenius [5]) possess no cycles of length $n-3$ or $n-4$. Accordingly, the theorems fail only if $m \geqslant n-2$ which was excluded (along with $m = 1$). Both theorems are therefore proved.

5. Extension. Once more assume that f is an irreducible trinomial of the form (1) where $b = p^k b^*$, $p \nmid ab^*$ and $k \geqslant 1$ but finally drop the basic assumption (2) and suppose that $(n, r) = s$. For $s > 1$, of course, $G(f)$ is no longer primitive and evidently $G(f) \neq S_n$. Nevertheless, provided $p \nmid s$ and $(s, k) = 1$, it is possible to give a description of $G(f)$ which, while wishing to keep the present study simple and not extend it unduly, we reckon is worth briefly recording here.

Write $F(x) = X^{n^*} + aX^{r^*} + b$, where $n = sn^*$, $r = sr^*$ and note that the splitting field of f contains $M = Q(\beta, \zeta)$, where $\beta^s = (-1)^{n^*} b$ and ζ is an sth root of unity.

THEOREM 6. *With f an irreducible trinomial as above with $p \nmid s = (n, r)$ and $(s, k) = 1$, suppose that $G_Q(F)$ contains A_{n^*}.*

Then $G_M(f)$ is an extension of $C_s^{n^*-1}$ by $G_M(F)$ $(= A_{n^*}$ or $S_{n^*})$, where C_s is a cyclic group of order s.

Theorem 6 is well-suited to apply in harness with Theorems 1 and 2 or the results of [10] and [10a]. Its proof combines ideas from [3] with modifications of Lemma 4 and Corollary 5 (from which the demand (2) was absent). We leave the details just now.

References

[1] W. Burnside, *Theory of groups of finite order*, Dover Publications, 1955.

[2] P. J. Cameron, *Finite permutation groups and finite simple groups*, Bull. London Math. Soc. 13 (1981), 1–22.

[3] S. D. Cohen and W. W. Stothers, *The Galois group of $f(x^r)$*, Glasgow Math. J. 25 (1984), 75–91.

[4] M. Fried and A. Schinzel, *Reducibility of quadrinomials*, Acta Arith. 21 (1972), 153–171.

[5] G. Frobenius, *Über die Charaktere der mehrfach transitiven Gruppen*, S. B. Akad. Berlin 1904, 558–571.

[6] I. Kaplansky, *Fields and Rings*, Chicago 1969.

[7] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, PWN, Warsaw 1974.

[8] E. Nart and N. Vila, *Equations of the type $X^n + aX + b$ with absolute Galois groups S_n*, Rev. Univ. Santander. 2(11) (1979), 821–825.

[9] K. Ohta, *On unramified Galois extensions of quadratic number fields* (Japanese), Sûgaku 24 (1972), 119–120.

[10] H. Osada, *The Galois groups of the polynomials $x^n + ax^l + b$*, J. Number Theory 25 (1987), 230–238.

[10a] — *The Galois groups of the polynomials $x^n + ax^s + b$, II*, Tôhoku Math. J. 39 (1987), 437–445.

[11] D. S. Passman, *Permutation groups*, Benjamin, New York 1968.

[12] K. Uchida, *Unramified extensions of quadratic number fields II*, Tôhoku Math. J. 22 (1970), 220–224.

[13] Y. Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka J. Math. 7 (1970), 57–76.

[14] K. Yamamura, *On unramified Galois extensions of real quadratic fields*, ibid. 23 (1986), 471–478.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF GLASGOW
Glasgow G12 8QW
Scotland

Received on 27.11.1987
and in revised form on 30.5.1988 (1770)