ACTA ARITHMETICA
LXXXII.1 (1997)

Double transitivity of Galois groups of trinomials

by

S. D. Cohen (Glasgow), A. Movahhedi (Limoges) and
A. Salinier (Limoges)

1. Introduction. In this paper we study the Galois group $G(f)$ of an irreducible trinomial $f(X) = X^n + aX^s + b$ with integral coefficients $(1 \le s \le n-1,\ ab \ne 0)$. Irreducibility has the effect that $G(f)$ is a transitive subgroup of the full symmetric group acting on the zeros of $f(X)$. If n and s are not coprime, then $f(X) = g(X^d)$, say, where $d > 1$ is the greatest common divisor of n and s. Thus $f(X)$ is functionally decomposable over $\mathbb{Q}$ and, easily, $G(f)$ is imprimitive as a permutation group. We shall show that in fairly general circumstances, when n and s are co-prime, $G(f)$ is not only primitive but even doubly transitive. As we shall see, our results extend a theorem of Osada [18] who proved, under stronger conditions, that $G(f)$ is the full symmetric group S_n itself. See also [17] for a related result.

We denote by (u, v) the greatest common divisor of two integers u and v. For any prime p and non-zero integer c, we use $v_p(c)$ to denote the p-adic valuation of c. Our first result is as follows.

Theorem 1.1. *Let $f(X) = X^n + aX^s + b$ be an irreducible trinomial with integral coefficients where $(n, as) = (a(n-s), b) = 1$. Suppose there is a prime divisor p of b such that $(s, v_p(b)) = 1$. Then the Galois group $G(f)$ of $f(X)$ over $\mathbb{Q}$ is doubly transitive.*

A doubly transitive group of degree n which contains a transposition is the full symmetric group S_n. Accordingly, under the hypotheses of Theorem 1.1, for $G(f)$ to be S_n, it suffices to guarantee the existence of a transposition in $G(f)$. In particular, this is the case when there exists a prime p not dividing (b, s) such that $v_p(D_0(f))$ is odd, where

$$D_0(f) = n^n b^{n-s} + (-1)^{n-1} s^s (n-s)^{n-s} a^n.$$

Indeed, the discriminant $D(f)$ of f is given [21] by

$$D(f) = (-1)^{n(n-1)/2} b^{s-1} D_0(f).$$

1991 *Mathematics Subject Classification*: 11R32, 11S15, 12F10.

Thus, the above prime p, not dividing b, divides $D(f)$ to an odd power, which shows that p is ramified in the splitting field L of $f(X)$. Hence, as shown in Lemma 2.1 below, the group $G(f)$ contains a transposition.

We comment on the relationship of Theorem 1.1 to Osada's work. Firstly, there is the minor observation that he allowed the existence of an integer c such that $(a,b) = c^n$ and b/c^n coprime to c, but, then, replacing $f(X)$ by $f(cX)/c^n$ we may suppose that $c = 1$.

Next, Theorem 1.1 significantly extends Theorem 1 of [18]; its statement is similar except that our hypothesis about the existence of a prime divisor p of b such that $(s, v_p(b)) = 1$ is replaced by the stronger condition $(b,s) = 1$ and $v_p(b) = 1$ for a prime p. Moreover, in [18], it was assumed that $|D_0(f)|$ is a non-square integer, which, as remarked above, ensures the existence of a transposition in $G(f)$. Thus, we recover Theorem 1 of [18] under lesser constraints. Furthermore, whereas the weakening of "$v_p(b) = 1$" to "$(s, v_p(b)) = 1$" may not rank as a major improvement, we claim that the omission of the hypothesis $(b,s) = 1$ is of some significance. For, as we shall see, a prime p such that p divides (b,s) and $(s, v_p(b)) = 1$ is wildly ramified in the splitting field L of $f(X)$; whereas, to our knowledge, wild ramification has been excluded in preceding works on this subject. Thus the demonstration that $G(f)$ is doubly transitive, even though several primes are wildly ramified in L, appears to represent significant progress.

Further, it is useful to be able to derive double transitivity without prescribing $|D_0(f)|$ be a non-square, since it is possible to find examples of trinomials satisfying the hypotheses of Theorem 1.1 for which $|D_0(f)|$ is a square (see Example 8 in Section 5).

We remark that, when no prime p satisfies the condition $(s, v_p(b)) = 1$, it is still possible in some circumstances to obtain the primitivity of the Galois group $G(f)$ as in [13].

In Theorem 1.1 although the hypotheses do not preclude wild ramification, we have, however, assumed that $p \nmid n - s$ for every prime p dividing b. The possibility that $p \mid (n-s, b)$ is particularly difficult to treat. Nevertheless, in our other main result (which we now state) we allow this to occur for a single prime p in the case in which $n - s = p^t$ $(t \geq 0)$.

THEOREM 1.2. *Let $f(X) = X^n + aX^s + b$ be an irreducible trinomial with integral coefficients where $(n,s) = 1$. Suppose that there exists a prime divisor p of b, but not of a, such that*

(i) $n = s + p^t$, $t \geq 0$,
(ii) $v_p(f(-a)) = 1$,
(iii) $(s, v_p(b)) = 1$.

Then $G(f)$ is doubly transitive.

Note that when $v_p(b) = 1$, then the condition "$v_p(f(-a)) = 1$" is automatically satisfied if

$$\begin{aligned} a &= +1 \text{ or } -1 \pmod{p^2} && \text{for } p \text{ odd;} \\ a &= -1 \pmod 4 && \text{for } p = 2. \end{aligned}$$

Next, we state some results which are used in the proofs of Theorems 1.1 and 1.2 and also may be employed in conjunction with these theorems to provide yet stronger conclusions.

For a subset (e.g. a subgroup) H of $G(f)$ we denote by $\operatorname{supp} H$ (the support of H) the set of roots α of $f(X)$ such that $\sigma(\alpha) \neq \alpha$ for some $\sigma \in H$. Our results assert that, under appropriate conditions, there are subgroups H of $G(f)$ transitive on $\operatorname{supp} H$.

THEOREM 1.3. *Let $f(X) = X^n + aX^s + b$ be an irreducible trinomial with integral coefficients with $(n, s) = 1$. Suppose there exists a prime p dividing b but not $a(n - s)$ such that $(s, v_p(b)) = 1$. Then $G(f)$ contains a subgroup H acting transitively on s roots of $f(X)$ and fixing each of the other roots. Furthermore, if $p \nmid s$, then the subgroup H is generated by an s-cycle.*

THEOREM 1.4. *Let $f(X) = X^n + aX^s + b$ be an irreducible trinomial with integral coefficients with $(n, s) = 1$. Suppose there exists a prime p dividing b, but not a, such that*

(i) $n - s = p^t,\ t \geq 1$,
(ii) $v_p(f(-a)) = 1$.

Then $G(f)$ contains a subgroup H acting transitively on p^t roots of $f(X)$ and fixing each of the other roots.

Theorems 1.3 and 1.4 may sometimes be used together. For example, for a trinomial satisfying the hypotheses of Theorem 1.2, Theorem 1.4 always applies, but for the same trinomial there may exist another prime p' such that $(s, v_{p'}(b)) = 1$ and then the conclusion of Theorem 1.3 is also valid. More generally, by combining the conclusions of Theorems 1.1 and 1.2 with such facts as Theorems 1.3 and 1.4 and the classification of doubly transitive groups [2], we can show that in most of the cases described in Theorems 1.1 and 1.2 (without assuming that $|D_0(f)|$ or $D(f)$ is a non-square), $G(f) = A_n$ or S_n (see Theorems 4.3 and 4.4). We leave the details of this procedure to a further paper but give some examples which illustrate our result in Section 5.

Finally, we comment briefly on some of the literature on the Galois groups of trinomials other than that which climaxed in Osada's papers. In [13] it is proved that $G(f)$ is primitive in certain cases under conditions like those of Theorem 1.1 except that b is assumed to be coprime to s but, on the other hand, $(v_p(b), s)$ may be greater than 1 for each prime p.

Usually, if $d = (a, b) > 1$, ramification of a prime divisor of d is of a rather different nature than that considered here and in [13]. Thus, for example, Komatsu [6–8] and Movahhedi [12] have studied trinomials of the form $X^n + aX + a$.

An interesting example of Trinks [22] with $(n, a) > 1$ is $G(X^7 - 7X + 3) = \mathrm{PSL}_2(7)$, where $\mathrm{PSL}_2(7)$ is the projective special linear group of degree 2 over the finite field of 7 elements. But generally not many trinomials for which $A_n \not\subseteq G(f)$ are known; perhaps the results of the paper and its sequel may help to narrow the search for such examples to a smaller area. The paper [4] contains serious errors (e.g. the claim to establish primitivity in Lemma 3 is false); therefore the examples given there are not justified. The present paper establishes modified results in a similar direction. The main difference in the proof is that, instead of concentrating on the ramification of a single prime p dividing b as there, in Theorem 1.1 all ramification is taken into account. The only effect of these additional considerations in the hypotheses of Theorem 1.1 is the inclusion of the assumption that $(a, b) = 1$.

2. Inertia groups. Let $f(X) = X^n + aX^s + b$ be an irreducible trinomial with integral coefficients $(1 \le s \le n - 1, ab \ne 0)$. Let $\alpha := \alpha_1, \alpha_2, \dots, \alpha_n$ be the different roots of $f(X)$ in an algebraic closure of $\mathbb{Q}$. We denote by $K = \mathbb{Q}(\alpha)$ the field obtained by adjoining the root α to the field $\mathbb{Q}$, and by $L := \mathbb{Q}(\alpha, \alpha_2, \dots, \alpha_n)$ the splitting field of $f(X)$.

For a given prime p, we choose a fixed prime ideal $\mathfrak{p}$ of L dividing p and denote by $L_\mathfrak{p}$ the corresponding completion with respect to the $\mathfrak{p}$-adic valuation. Write $I_\mathfrak{p}$ for the inertia group of $\mathfrak{p}$ and L_I the inertia field of $\mathfrak{p}$: we have $I_\mathfrak{p} = \mathrm{Gal}(L_\mathfrak{p}/L_I)$.

In this section we first describe the factorization of $f(X)$ in the p-adic field $\mathbb{Q}_p$ and in some of the sub-extensions of $L_\mathfrak{p}$, and then prove Theorems 1.3 and 1.4.

LEMMA 2.1. *Suppose $(n, as) = 1$. Let p be a prime which does not divide b but is ramified in K. Then the inertia group $I_\mathfrak{p}$ is generated by a transposition.*

Proof. We necessarily have $p \mid D_0(f)$ and $p \nmid a$. So, by Theorem 2 of [11], the prime p divides the absolute discriminant of the field $K = \mathbb{Q}(\alpha)$ exactly once. The rest of the proof is similar to that of Lemma 5 of [13]. ∎

Next, let p be a prime divisor of b but not of a. By Hensel's Lemma,

$$f(X) = g(X)h(X) \quad \text{over } \mathbb{Z}_p,$$

where

$$g(X) \equiv X^s \pmod p \quad \text{and} \quad h(X) \equiv X^{n-s} + a \pmod p.$$

Throughout the rest of the paper, this notation will be retained for the factors of $f(X)$ over $\mathbb{Z}_p$.

LEMMA 2.2. *Suppose $(n,s)=1$ and p is a prime dividing b but not $a(n-s)$. Then $h(X)$ splits completely over the inertia field L_I and the support of the inertia group $I_{\mathfrak{p}}$ has at most s elements.*

P r o o f. Let α be a root of $h(X)$ having $h_1(X)$ as minimal polynomial over $\mathbb{Q}_p$. The reduction $\overline{h}_1(X)$ of $h_1(X)$ modulo p is, by Hensel's Lemma, a power of an irreducible polynomial. On the other hand, since by hypothesis $p\nmid a(n-s)$, $\overline{h}(X)$, the reduction of $h(X)$ modulo p, has no multiple root. So the same is true of $\overline{h}_1(X)$. Thus $\overline{h}_1(X)$ is irreducible, showing that the local extension $\mathbb{Q}_p(\alpha)/\mathbb{Q}_p$ is unramified. Hence the splitting field of $h(X)$ is an unramified extension of $\mathbb{Q}_p$ which therefore must be contained in the maximal unramified extension L_I. ∎

LEMMA 2.3. *Let p be a prime divisor of b but not of a such that $(s, v_p(b))=1$. Then, for each root α of $g(X)$, the extension $\mathbb{Q}_p(\alpha)/\mathbb{Q}_p$ is totally ramified. Furthermore, $g(X)$ is irreducible over the inertia field L_I.*

P r o o f. Let w be the normalized valuation of the local field $\mathbb{Q}_p(\alpha)$. Then $w(p)=e$, where e is the ramification index of the extension $\mathbb{Q}_p(\alpha)/\mathbb{Q}_p$. Since $g(X)\equiv X^s \pmod p$, we have $w(\alpha)>0$ and, since $f(\alpha)=\alpha^n+a\alpha^s+b=0$, we necessarily have

$$sw(\alpha)=w(b)=ev_p(b).$$

Now, since $(s,v_p(b))=1$ by hypothesis, s must divide e. As

$$e\le[\mathbb{Q}_p(\alpha):\mathbb{Q}_p]\le s=\text{degree of } g(X),$$

we obtain simultaneously that the extension $\mathbb{Q}_p(\alpha)/\mathbb{Q}_p$ is totally ramified and the polynomial $g(X)$ is irreducible over $\mathbb{Q}_p$. The unramified extension L_I being linearly disjoint over $\mathbb{Q}_p$ with the totally ramified extension $\mathbb{Q}_p(\alpha)$, the polynomial $g(X)$ remains irreducible over L_I. ∎

P r o o f o f T h e o r e m 1.3. By the preceding two lemmas, over the field L_I, $g(X)$ is irreducible while $h(X)$ splits completely. Hence $I_{\mathfrak{p}}=\mathrm{Gal}(L_{\mathfrak{p}}/L_I)$ is transitive on its support which consists of the roots of $g(X)$. This proves the first part of Theorem 1.3. If, additionally, we suppose that $p\nmid s$, then $L_{\mathfrak{p}}=L_I(\alpha)$ for any root α of $g(X)$. Indeed, let β be another root of $g(X)$. Then by Lemma 2.3, and Abhyankar's lemma [14, Chapter 5, Corollary 4 to Theorem 5.11] the extension $L_I(\alpha,\beta)/L_I(\alpha)$ is unramified. Since $L_{\mathfrak{p}}/L_I$ is totally ramified, we must have $L_I(\alpha,\beta)=L_I(\alpha)$. Thus $L_{\mathfrak{p}}/L_I$ is a totally and tamely ramified extension of degree s. So its Galois group $I_{\mathfrak{p}}$ is cyclic [3, Chapter I, Section 8, Proposition 1] of order s acting transitively on the s roots of $g(X)$, and as such must necessarily be generated by an s-cycle. ∎

Proof of Theorem 1.4. Let $g_0(X) = g(X-a), h_0(X) = h(X-a)$. Then

$$h_0(X) \equiv X^{p^t} + (-a)^{p^t} + a \equiv X^{p^t} \pmod{p},$$

and $1 = v_p(f(-a)) = v_p(h_0(0)g_0(0))$. Hence $v_p(h_0(0)) = 1$ and so h_0 is an Eisenstein polynomial of degree p^t with respect to p. Thus the polynomial $h(X)$ is irreducible of degree p^t over $\mathbb{Q}_p$ and the field $\mathbb{Q}_p(\gamma)$, obtained by adjunction of a root γ of $h(X)$ to $\mathbb{Q}_p$, is a totally and wildly ramified extension of $\mathbb{Q}_p$. Hence $\mathbb{Q}_p(\gamma)$ is linearly disjoint over $\mathbb{Q}_p$ with the maximal tamely ramified extension L_T of $\mathbb{Q}_p$ contained in $L_{\mathfrak{p}}$. This proves that the polynomial $h(X)$ is irreducible over L_T.

Now we apply results of Ore (see the Appendix below) to find the prime decomposition of p in K. The factorization of $f(X) \bmod p$ is

$$f(X) \equiv X^s(X+a)^{p^t} \pmod{p}.$$

The principal part of the (p, X)-polygon of $f(X)$ is made up of a unique side S which joins the point $(n-s, 0)$ to the point $(n, v_p(b))$, and the associated polynomial of it is

$$F_S(Y) = Y^r + bp^{-v_p(b)}a_1,$$

where $r := (s, v_p(b))$ and a_1 is an integer such that $aa_1 \equiv 1 \pmod{p}$. Likewise, since $v_p(f(-a)) = 1$ and $f(X) \equiv X^s(X+a)^{p^t} \pmod{p}$, the principal part of the $(p, X+a)$-polygon of $f(X)$ is made up of a unique side S_a joining the point $(s, 0)$ to the point $(n, 1)$, hence with a linear associated polynomial $F_{S_a}(Y)$. Now by Theorem A.2, it follows that

$$p = \mathcal{A}_1^q \mathcal{A}_2^{p^t},$$

where $q := s/r$ and $\mathcal{A}_1, \mathcal{A}_2$ are two integral ideals of K which are relatively prime and which have absolute norms

$$N_K(\mathcal{A}_1) = p^r, \qquad N_K(\mathcal{A}_2) = p.$$

Moreover, since the polynomials $F_S(Y)$ and $F_{S_a}(Y)$ are separable modulo p, Theorem A.2 also yields

$$\mathcal{A}_1 = \mathcal{P}_1\mathcal{P}_2 \dots \mathcal{P}_m,$$

where the $\mathcal{P}_i$'s are distinct prime ideals of K, and $\mathcal{A}_2$ is a prime ideal $\mathcal{Q}$. Hence the exact prime decomposition of p in K is the following

$$p = \mathcal{Q}^{p^t}\mathcal{P}_1^q\mathcal{P}_2^q \dots \mathcal{P}_m^q.$$

To each prime ideal $\mathcal{P}_i$ corresponds an irreducible factor $g_i(X)$ which is the minimal polynomial of α in the tamely ramified extension $K_{\mathcal{P}_i}/\mathbb{Q}_p$, where $K_{\mathcal{P}_i}$ is the completion of K with respect to the $\mathcal{P}_i$-adic valuation. The product $\prod_{i=1}^n g_i(X)$ is necessarily $g(X)$ since each $g_i(X)$ is different from the irreducible polynomial $h(X)$. This implies that $g(X)$ splits completely

over L_T. Now, in this situation, the first ramification group $G(L_\mathfrak{p}/L_T)$ acts transitively on the p^t roots of $h(X)$ and fixes the roots of $g(X)$. ∎

When $(s, v_p(b)) = 1$, the preceding proof can be carried out without using Ore's result as it follows from Lemma 2.3 that $g(X)$ splits completely over L_T.

A doubly transitive group with a subgroup like those described in Theorems 1.3 and 1.4 has been called a *Jordan group*, and these have been classified (see [15]). This is the starting point for our sequel.

3. Primitivity of $G(f)$. The crucial part of our method is to show that, in the situation of Theorems 1.1 and 1.2, $G(f)$ is primitive. We assume the notation of the previous sections.

LEMMA 3.1. *Let $f(X) = X^n + aX^s + b$ be an irreducible trinomial with integral coefficients such that $(n, as) = (a(n-s), b) = 1$. Suppose there is a prime divisor p of b such that $(s, v_p(b)) = 1$. Then $G(f)$ is primitive.*

Proof. Suppose $G(f)$ is imprimitive. Let $A_1, \dots, A_l$ be a system of imprimitivity of $G(f)$ with $k := n/l$ the cardinality of each of the blocks A_i. By Theorem 1.3 there exists a subgroup H of $G(f)$ which acts transitively on a set S consisting of s roots of $f(X)$ and fixes each of the other roots. Since $(k, s) = 1$, we see that S is not a union of some of the blocks. Hence there is a block A_1 such that A_1 has a non-empty intersection with S but is not contained in S. Because it contains a point fixed by H, the block A_1 is fixed by H. On the other hand, since A_1 contains a point of S and H is transitive on S, we see that A_1 must actually (strictly) contain S. Hence $s < k$.

Since $G(f)$ is transitive, and, crucially, generated by all inertia groups, there exists a prime ideal $\mathfrak{p}$ of L such that for an element $\sigma \in I_\mathfrak{p}$ we have $\sigma(A_1) \neq A_1$. In particular, $|\operatorname{supp} I_\mathfrak{p}| \geq |A_1 \cup \sigma(A_1)| = 2k \geq 4$. This clearly implies that σ cannot be a transposition and so by Lemma 2.1, necessarily $p \mid b$. Therefore, by Lemma 2.2,

$$|\operatorname{supp} I_\mathfrak{p}| \leq s.$$

Thus $2k \leq s < k$, which is impossible. ∎

LEMMA 3.2. *Let $f(X)$ be an irreducible trinomial satisfying all the conditions of Theorem* 1.2. *Then $G(f)$ is primitive.*

Proof. Suppose $G(f)$ is imprimitive. Let $A_1, \dots, A_l$ be a system of imprimitivity of $G(f)$ with $k := n/l$ the cardinality of each of the blocks A_i. We consider two cases.

First suppose that $t \geq 1$. Let $f(X) = g(X)h(X)$ be the factorization of $f(X)$ in $\mathbb{Q}_p$ and $\mathfrak{p}$ a prime ideal of L dividing p as in Section 2. As shown

in the proof of Theorem 1.4, there exists a subgroup H of $G(f)$ which acts transitively on the set R_h of the p^t roots of $h(X)$ and fixes each of the other roots. Since $p \nmid k$, the set R_h is not a union of blocks and so the set R_g of the s roots of $g(X)$ also cannot be a union of blocks.

Now let A_1 be a block that has a non-empty intersection with R_h but is not contained in R_h. Because A_1 contains a point fixed by H (a root of $g(X)$), the block A_1 is fixed by H. Further, because it contains a point of R_h and H is transitive on R_h, the block A_1 strictly contains R_h. Let $\beta_1 \in A_1 \backslash R_h$ and $\beta_2 \notin A_1$ be two roots of $g(X)$. By Lemma 2.3 we know that $g(X)$ remains irreducible over the inertia field L_I, so that there exists σ in the inertia group $I_{\mathfrak{p}}$ for which $\sigma(\beta_1) = \beta_2$. But this is impossible, since $\sigma(R_h) = R_h$ and consequently $\sigma(A_1) = A_1$.

Suppose finally that $t = 0$. In that case, using Theorem 1.3, we see that $G(f)$ is not only primitive but even doubly transitive. ∎

N o t e. If $s < n/2$, a contradiction is already reached in the above proof at the point where it is shown that $R_h \subset A_1$. Thus, in this situation, Lemma 2.3, and so the assumption that $(s, v_p(b)) = 1$, are not needed.

4. Double transitivity. We quote the following theorem of Jordan ([5] or explicitly in [23, Theorem 13.1]).

LEMMA 4.1. *Let G be a primitive group of degree n such that the stabilizer of some set of m points (where $1 \le m \le n-2$) is transitive on the remaining $n-m$ points. Then G is doubly transitive.*

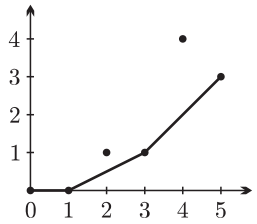
P r o o f o f T h e o r e m 1.1. When $s = 1$, Lemmas 2.1 and 2.2 show that the Galois group $G(f)$ is generated by transpositions, so $G(f)$ is not only doubly transitive but the full symmetric group S_n [19, Lemma 4.4.4, p. 40]. For $s > 1$, the proof follows by applying Lemma 4.1 to the Galois group $G(f)$ (which is primitive by Lemma 3.1) and the subgroup H with $|\operatorname{supp} H| = s$ whose existence was shown in Theorem 1.3. ∎

P r o o f o f T h e o r e m 1.2. When $t = 0$, the double transitivity of $G(f)$ is a consequence of Theorem 1.3. When $t \ge 1$, the proof follows by applying Lemma 4.1 to the Galois group $G(f)$ (which is primitive by Lemma 3.2) and the subgroup H of Theorem 1.4. ∎

N o t e s. 1. By the note following Lemma 3.2, in Theorem 1.2 as an alternative to (iii), it suffices to assume that $s < n/2$.

2. As the following example shows, if the hypothesis (ii) of Theorem 1.2 is dropped, then we no longer get the double transitivity of $G(f)$ in general. Take $f(X) = X^5 - 5X + 12$ and $p = 2$. The hypotheses of Theorem 1.2 are satisfied except that $v_2(f(5)) = 3$. According to [20, Table II], $G(f)$ is the dihedral group D_5 of order 10. For this example the polynomial

$h(X) = f(X)/g(X)$ is not irreducible over $\mathbb{Q}_2$ (as was the case in the proof of Theorem 1.4). Indeed, the Newton polygon of $f(X+5)$ with respect to $p = 2$ has three sides (see diagram).



Therefore $f(X)$ has at least three factors over $\mathbb{Q}_2$.

As we have already observed, the main difference between the proofs of Theorems 1.1 and 1.2 is that, for the former, inertia groups corresponding to all ramified primes have to be taken into account to establish primitivity, whereas for the latter only those relating to a single prime divisor of b need be considered. In fact, by imposing a suitable condition on a, we can show that, even if the conditions $(a, n) = (a(n-s), b) = 1$ are not met but there does exist a prime divisor p of b (with $p \nmid a(n-s)$) such that $(s, v_p(b)) = 1$, then $G(f)$ is doubly transitive. We illustrate this with one kind of condition on a.

THEOREM 4.2. *Let $f(X) = X^n + aX^s + b$ be an irreducible trinomial with integral coefficients where $(n, s) = 1$. Suppose there exists a prime divisor p of b such that*

(i) $p \nmid a(n-s)$,
(ii) $(s, v_p(b)) = 1$,
(iii) *$X^{n-s} + a$ is irreducible modulo p.*

Then $G(f)$ is doubly transitive.

P r o o f. With $\mathfrak{p}$ a prime divisor of p in L, consider, as in Section 2, the factorization $f(X) = g(X)\,h(X)$ in $\mathbb{Z}_p$. The case $s = 1$ is straightforward, since by hypothesis (iii), the polynomial $h(X)$ is irreducible over $\mathbb{Q}_p$ and, the stabilizer in $\mathrm{Gal}(L_\mathfrak{p}/\mathbb{Q}_p)$ of the root of $g(X)$ acts transitively on the roots of $h(X)$. Now assume that $s > 1$. By Lemma 2.3, the polynomial $g(X)$ is irreducible over the inertia field L_I, whereas the polynomial $h(X)$ splits completely over L_I by Lemma 2.2. We may apply a similar argument to the proof of Lemma 3.2 with $\mathrm{Gal}(L_\mathfrak{p}/\mathbb{Q}_p)$ and $I_\mathfrak{p}$ in place of $I_\mathfrak{p}$ and $\mathrm{Gal}(L_\mathfrak{p}/L_T)$, respectively, and the roles of $g(X)$ and $h(X)$ interchanged to yield a contradiction to the supposition that $G(f)$ is imprimitive. Finally, applying Lemma 4.1 with $I_\mathfrak{p}$, we obtain the double transitivity of $G(f)$. ∎

N o t e s. 1. If $s > n/2$, a contradiction is already reached in the above proof on showing that R_g is contained in a block of imprimitivity. Hence, in the statement of Theorem 4.2, it suffices to assume $s > n/2$ in place of the condition (iii).

2. The hypothesis "$X^{n-s} + a$ is irreducible modulo p" in Theorem 4.2 can be replaced by the three following:

- $4 \nmid (p+1, n-s)$,
- $\left(\frac{p-1}{r}, n-s\right) = 1$, where r is the order of $-a$ modulo p,
- each prime divisor of $n-s$ divides r,

which are its equivalent because p does not divide a [10, Theorem 3.75].

Another modification to Theorem 1.1 is to assume that $p \nmid s$ for at least one prime p such that $(s, v_p(b)) = 1$. Then, by Theorem 1.3, $G(f)$ contains an s-cycle and so, since it is primitive, provided $s \geq 2$ we have that $G(f)$ is $(n-s+1)$-transitive by Marggraff's theorem ([1] or [9]). In particular, if $2 \leq s \leq n-3$, then $G(f)$ is at least 4-transitive and so, if $A_n \not\subseteq G(f)$, then using the classification of finite simple groups (see [2]), $G(f)$ must be one of the Mathieu groups M_n, $n = 11, 12, 23, 24$ with $s = n-3$ or $n-4$. Since M_{11} and M_{23} are not 5-transitive, the only possibilities for this (having in mind that n and s are coprime) are $(n, s) = (11, 8)$ or $(23, 20)$. But the Mathieu groups M_{11} and M_{23} consisting of even permutations do not possess cycles of length 8 and 20 respectively. Thus, granted the classification of finite simple groups, we have the following consequence of Theorem 1.1 (note that when $s = 1$, by Lemmas 2.1 and 2.2, $G(f)$ is generated by transpositions and $G(f) = S_n$ [19, Lemma 4.4.4, p. 40]).

THEOREM 4.3. *Let $f(X) = X^n + aX^s + b$ be an irreducible trinomial with integral coefficients where $(n, as) = (a(n-s), b) = 1$ and $s \leq n-3$. Suppose there is a prime divisor p of b but not of s such that $(s, v_p(b)) = 1$. Then $G(f)$ is either A_n or S_n.*

It is not hard to see that for $s \leq n-3$, the preceding theorem improves Theorem 1 of [18].

There is a similar consequence of Theorem 1.2 (or Lemma 3.2) when $t = 1$.

THEOREM 4.4. *Let $f(X) = X^n + aX^s + b$ be an irreducible trinomial with integral coefficients with $(n, s) = 1$. Suppose that $n - s = p$ is a prime satisfying $p \mid b$, $p \nmid a$, $v_p(f(-a)) = 1$ and $(s, v_p(b)) = 1$. If $s \geq 3$ then $G(f)$ contains A_n.*

P r o o f. Follows from Lemma 3.2, Theorem 1.4 and Theorem 13.9 of [23]. ∎

5. Examples

1. If $(n,s)=1$, we see from Lemma 9 of [17] that the trinomial $X^n \pm X^s \pm p$ is irreducible for a prime p, unless $p=2$ and $X \pm 1$ is a factor (this fact is also used in Examples 3 and 8 below). Except in this last situation, it follows from our results that $G(X^n \pm X^s \pm p)$ is doubly transitive provided the two following conditions are satisfied:

- $(n,s)=1$,
- $p \nmid n-s$ or $n = s + p^t$.

In particular, if n is odd, then $X^n + X^2 + 2$ is irreducible and $G(X^n + X^2 + 2)$ is the full symmetric group since it contains a transposition by Theorem 1.3. Similarly, if n is odd, $G(X^n - X^{n-2} + 2) = S_n$.

Actually, when $(n,s)=1$ and $X \pm 1$ is not a factor of $X^n \pm X^s \pm p$ for $p=2$, the Galois group $G(X^n \pm X^s \pm p)$ contains A_n in each of the following cases:

(a) $s \leq n-3$, $p \nmid s(n-s)$,
(b) $s \leq n-3$ and $p = s$,
(c) $s \geq 3$ and $p = n-s$.

It is easy to see that (a) follows from Theorem 4.3; (b) follows from Theorem 13.9 of [23] and Theorem 1.3 which guarantees the existence of a cycle of length p in the Galois group (take any element of order p in the subgroup H occurring in Theorem 1.3); and (c) follows from Theorem 4.4.

2. Let $(n,s)=1$ and $s \leq n-3$. Take two distinct prime numbers p and q such that

$$(p,s) = (pq, n-s) = 1.$$

If $f(X) = X^n \pm X^s \pm pq$ is irreducible over $\mathbb{Q}$, then $G(f) = A_n$ or S_n by Theorem 4.3.

3. If $p \nmid s$, then the trinomial

$$X^{p^t+s} - X^s + p$$

is irreducible over $\mathbb{Q}$, and its Galois group is doubly transitive by Theorem 1.2.

4. Let p and q be two distinct primes. Then by Theorem 1.2 the Galois group $G(X^{p^t+q^r} - X^{q^r} + pq)$ is doubly transitive provided the polynomial is irreducible. Indeed, by Theorems 1.3 and 1.4, the Galois group contains subgroups H_1 and H_2 transitive on their supports which have sizes q^r, p^t. By using the classification of doubly transitive groups and the nature of these groups, it can be shown that such subgroups H_1 and H_2 cannot exist simultaneously unless the Galois group is A_n or S_n. We leave the details

of this, as such group theoretical arguments will form the substance of our ensuing paper.

5. Let n be odd and p a prime $\equiv 3 \pmod 4$. By Theorem 4.2 the Galois group of the trinomial $X^n + X^{n-2} + 2p$ is doubly transitive provided it is irreducible.

6. Let $n = s + 2^t$ (s odd, $t \geq 1$) and p, q be distinct primes with $p \equiv 1 \pmod 4$ and q a quadratic non-residue (mod p). By Theorem 4.2 and the Eisenstein criterion, $G(X^n - qX^s + qp)$ is doubly transitive. For example, $G(X^{143} - qX^{15} + 5q)$, $q = 2$ or 13, is doubly transitive.

7. Let p be a prime and a a rational integer such that $p \nmid a$. Then by Theorem 4.2 the Galois group of $X^n + aX^{n-1} + ap$ is doubly transitive provided it is irreducible. For instance, $G(X^n + qX^{n-1} + qp)$ is doubly transitive if p and q are two distinct primes.

8. Let $f(X) = X^8 + X^7 + p$ where $p := 246767749$ is a prime. By Theorem 1.1 its Galois group G is doubly transitive. In fact, $G = A_8$, since $D_0(f)$ is a square and the factorization of $f(X)$ modulo 19 shows that G contains a 3-cycle.

6. Appendix on Ore's theorem. This section has been added at the suggestion of the referee. Since a careful reading of [16] is required to extract the precise version of the theorem of Ore needed in the proof of Theorem 1.4, we give here a formulation of the appropriate result.

Let p be a fixed prime number and let $\varphi(X) \in \mathbb{Z}[X]$ be a monic polynomial of degree $m \geq 1$ such that $\varphi \bmod p$ is irreducible. Given a monic polynomial $f(X) \in \mathbb{Q}_p[X]$, by Euclidean division we expand $f(X)$ according to powers of $\varphi(X)$; that is, we write

$$f(X) = \sum_{j=0}^{t} p^{\alpha_j} Q_j(X) \varphi(X)^{t-j} \tag{1}$$

with polynomials $Q_j(X) \in \mathbb{Z}_p[X]$ and degree $Q_j < m$ for each j. In this equality (1), p does not divide all the coefficients of Q_j, except when $Q_j \equiv 0$, in which case we omit the corresponding term. Since f and φ are monic, the polynomial Q_0 is monic and $\alpha_0 = 0$. The integer t is the largest integer $\leq n/m$, where $n = \deg(f)$. This expansion will be called the *canonical decomposition* of $f(X)$.

Definition A.1. The (p, φ)-*polygon* of $f(X)$ is the boundary of the upper convex envelope of the set of points (j, α_j) minus the two vertical sides. The (p, φ)-polygon, minus the (possible) horizontal part, is, by definition, the *principal part* of it.

Let $S_1, \ldots, S_k$ be the sides of the principal part of the (p,φ)-polygon of $f(X)$ with increasing slopes. Define

$$\begin{aligned} l_0 &:= \text{the length of the horizontal side;} \\ l_i &:= \text{the length of the projection of } S_i \text{ to the } x\text{-axis;} \\ h_i &:= \text{the length of the projection of } S_i \text{ to the } y\text{-axis.} \end{aligned}$$

Set

$$\varepsilon_i := (l_i, h_i), \quad \lambda_i := l_i/\varepsilon_i \quad \text{and} \quad \kappa_i := h_i/\varepsilon_i.$$

We fix a side S_i of the (p,φ)-polygon of $f(X)$. In the canonical decomposition of $f(X)$, consider the sum of the terms $p^{\alpha_j} Q_j(X)\varphi(X)^{t-j}$ corresponding to the points $(j,\alpha_j) \in S_i$. In this sum, we separate

$$\varphi(X)^{t-l_0-\ldots-l_i} p^{h_1+\ldots+h_{i-1}},$$

thus making apparent a factor

$$\begin{aligned} R_{i,0}(X)\varphi(X)^{l_i} + R_{i,1}(X)p^{\kappa_i}\varphi(X)^{l_i-\lambda_i} \\ + R_{i,2}(X)p^{2\kappa_i}\varphi(X)^{l_i-2\lambda_i} + \ldots + R_{i,\varepsilon_i}(X)p^{h_i}, \end{aligned}$$

where the polynomials $R_{i,0}(X), \ldots, R_{i,\varepsilon_i}(X)$ are of degree $< m$. In particular $R_{i,0}$ and $\varphi(X)$ (considered as polynomials of $\mathbb{F}_p[X]$) are co-prime. So there exists $A_i(X) \in \mathbb{Z}[X]$ such that

$$R_{i,0}(X)A_i(X) \equiv 1 \bmod (p, \varphi(X)).$$

Define

$$S_{i,j}(X) := A_i(X)R_{i,j}(X).$$

The *associated polynomial* of the ith side is by definition

$$F_i(X,Y) = Y^{\varepsilon_i} + S_{i,1}(X)Y^{\varepsilon_i-1} + \ldots + S_{i,\varepsilon_i}(X).$$

$F_i(X,Y)$ depends on the choice of A_i, but its class modulo the ideal $(p,\varphi(X))$ does not.

Theorem 5, Chapter 2 of [16] and the paragraph following this theorem can now be stated as follows.

THEOREM A.2 (Ore). *Let $f(X) = X^n + a_1X^{n-1} + \ldots + a_n \in \mathbb{Z}[X]$ be an irreducible polynomial, and let θ be a root of $f(X)$ in a fixed algebraic closure of $\mathbb{Q}$. Assume that $f(X) \equiv \varphi_1(X)^{a_1} \ldots \varphi_s(X)^{a_s} \bmod p$, where each $\varphi_\nu(X) \in \mathbb{Z}[X]$, is the factorization of $f(X)$ modulo p. Denote by m_ν the degree of $\varphi_\nu(X)$. Then*

$$p = \mathfrak{a}_1 \ldots \mathfrak{a}_s$$

where $\mathfrak{a}_\nu$ are coprime integer ideals of $K := \mathbb{Q}(\theta)$, with $N_K(\mathfrak{a}_\nu) = p^{a_\nu m_\nu}$ (N_K stands for the absolute norm of the number field K).

In order to factorize each ideal $\mathfrak{a} := \mathfrak{a}_\nu$, corresponding to the irreducible factor $\varphi := \varphi_\nu$, we construct the (p,φ)-polygon of $f(X)$. For each side S_i

of the principal part of this polygon, we consider the factorization modulo (p, φ) *of the associated polynomial* $F_i(X, Y)$:

$$F_i(X,Y) \equiv F_1^{(i)}(X,Y)^{a_1^{(i)}} \dots F_{t_i}^{(i)}(X,Y)^{a_{t_i}^{(i)}} \bmod (p,\varphi).$$

Then $\mathfrak{a} = \prod_{i=1}^{k} \prod_{j=1}^{t_i} [\mathfrak{c}_j^{(i)}]^{\lambda_i}$, *where* $\lambda_i := l_i/(l_i, h_i)$ *is the parameter defined above and where the* $\mathfrak{c}_j^{(i)}$ *are coprime integer ideals of* $K = \mathbb{Q}(\theta)$. *Moreover,*

$$N_K(\mathfrak{c}_j^{(i)}) = p^{m\, m_j^{(i)} a_j^{(i)}}, \quad m_j^{(i)} := \mathrm{degree}_Y F_j^{(i)}(X,Y).$$

Furthermore, if $a_j^{(i)} = 1$, *then the ideal* $\mathfrak{c}_j^{(i)}$ *is prime.*

Acknowledgements. The authors are indebted to the referee for his careful reading of the manuscript and valuable suggestions.

References

[1] M. D. Atkinson, *Doubly transitive but not doubly primitive permutation groups II*, J. London Math. Soc. (2) 10 (1975), 53–60.

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

[3] J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory*, Academic Press, 1967.

[4] S. D. Cohen, *Galois groups of trinomials*, Acta Arith. 54 (1989), 43–49.

[5] C. Jordan, *Théorèmes sur les groupes primitifs*, J. Math. Pures Appl. (2) 16 (1871), 383–408 = Œuvres, Tome 1, Gauthier-Villars, Paris, 1961, 313–338.

[6] K. Komatsu, *Square free discriminants and affect-free equations*, Tokyo J. Math. 14 (1991), 57–60.

[7] —, *On the Galois group of* $x^p + ax + a = 0$, ibid. 14 (1991), 227–229.

[8] —, *On the Galois group of* $x^p + p^t b(x+1) = 0$, ibid. 15 (1992), 351–356.

[9] R. Levingston and D. E. Taylor, *The theorem of Marggraff on primitive permutation groups which contain a cycle*, Bull. Austral. Math. Soc. 15 (1976), 125–128.

[10] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, Mass., 1983. (Now distributed by Cambridge University Press.)

[11] P. Llorente, E. Nart and N. Vila, *Discriminants of number fields defined by trinomials*, Acta Arith. 43 (1984), 367–373.

[12] A. Movahhedi, *Galois group of* $x^p + ax + a$, J. Algebra 180 (1996), 966–975.

[13] A. Movahhedi and A. Salinier, *The primitivity of the Galois group of a trinomial*, J. London Math. Soc. (2) 53 (1996), 433–440.

[14] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 2nd ed., Springer, Berlin, and PWN–Polish Scientific Publ., Warszawa, 1990.

[15] P. M. Neumann, *Some primitive permutation groups*, Proc. London Math. Soc. 50 (1985), 265–281.

[16] O. Ore, *Newtonsche Polygone in der Theorie der algebraischen Körper*, Math. Ann. 99 (1928), 84–117.

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

[18] H. Osada, *The Galois groups of the polynomials $x^n + ax^s + b$. II*, Tôhoku Math. J. 39 (1987), 437–445.
[19] J.-P. Serre, *Topics in Galois Theory*, Res. Notes Math., Vol. 1, Jones and Bartlett, Boston, 1992.
[20] L. Soicher and J. McKay, *Computing Galois groups over the rationals*, J. Number Theory 20 (1985), 273–281.
[21] R. G. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math. 12 (1962), 1099–1106.
[22] W. Trinks, *Arithmetisch ähnliche Zahlkörper*, Diplomarbeit, Math. Fak. Univ. Karlsruhe (TH), 1969.
[23] H. Wielandt, *Finite Permutation Groups*, Academic Press, 1964.

Department of Mathematics
University of Glasgow
Glasgow G12 8QW, Scotland
E-mail: sdc@maths.gla.ac.uk

UPRES A 6090 CNRS
Faculté des Sciences
123 Avenue Albert Thomas
87060 Limoges Cedex, France
E-mail: mova@cict.fr
salinier@cict.fr

Received on 19.12.1994
and in revised form on 30.4.1997 (2716)