ACTA ARITHMETICA
178.4 (2017)

On the solvability of an Eisenstein trinomial of prime degree

by

Chahrazede Bouyacoub (Alger) and Alain Salinier (Limoges)

Since all binomials are solvable, trinomials provide the simplest examples of *affect-free* polynomials, that is, polynomials of degree n with rational coefficients whose Galois group is isomorphic to the symmetric group S_n. For example, it is known [12], [15, p. 52] that the trinomial $X^n - X - 1$ has this property for every integer $n > 1$. The easiness to find affect-free trinomials is linked to the following fact shown by Schinzel [14]: generic trinomials $X^n + T^r X^m + T^s$, with n, m, r, s integers such that $n > m > 0$ and $s(n-m) - rn = 1$, have S_n as Galois group over the field $\mathbb{Q}(T)$ generated by a transcendental indeterminate T. Indeed, Hilbert's irreducibility theorem then entails that trinomials $X^n + t^r X^m + t^s$ are affect-free for an infinite set of values of $t \in \mathbb{Q}^*$. In fact, the present literature suggests that there are only very few examples of irreducible trinomials of prime degree $p \geq 7$ whose Galois group over $\mathbb{Q}$ is a permutation group not containing the alternating group A_p. For example, Angeli [2] showed that if $p \geq 7$ is a fixed prime integer, there are only a finite number of orbits of irreducible solvable trinomials $f(X) = X^p + AX + B$ under the action $f(X) \mapsto k^p f(X/k)$ of the group $\mathbb{Q}^*$.

In the present paper, we are interested precisely in the possibility of finding irreducible solvable trinomials $f_0(X) = AX^p + BX + C$ $(ABC \neq 0)$ with rational coefficients of prime degree $p \geq 7$. For such a trinomial, there exists a $k \in \mathbb{Q}^*$ such that the trinomial $A^{-1}k^p f_0(X/k)$ is of the form

$$f(X) = X^p + ac^{p-2}X + ac^{p-1} \tag{1}$$

for two coprime integers a and c (see Section 5 below). So we limit ourselves to trinomials of the form (1). To ensure the irreducibility of such a trinomial, we assume that it is Eisenstein with respect to the same prime p, which means that $a = pa_1$, where a_1 is an integer coprime to p. (One can think

2010 *Mathematics Subject Classification*: 11R32, 12F10.
Key words and phrases: Galois group, local fields, Eisenstein polynomials, trinomials, Newton polygons.
Received 6 August 2016; revised 30 September 2016.
Published online 26 April 2017.

DOI: 10.4064/aa8581-10-2016

that it is an overly restrictive assumption, but recall that the Galois group of an irreducible trinomial $X^p + aX^s + a$ is not solvable as soon as the prime $p \geq 5$ does not divide a [3, Theorem 3.2]). Moreover, in our proofs we need the additional assumption that c is coprime to $p-1$. Our main result is the following.

THEOREM 1. *Let $p \geq 7$ be a prime number, and a_1, c two rational integers such* $\gcd(a_1, pc) = \gcd(c, p(p-1)) = 1$. *Set $a = pa_1$ and*

$$D_0 = \frac{c}{|c|}(p^{p-1}c + (p-1)^{p-1}a_1).$$

For the Galois group G of the trinomial $f(X)$ of the form (1) *to be solvable, the following conditions are necessary.*

1. *The integer D_0 is a square in $\mathbb{Z}$.*
2. *If $p \equiv 1 \pmod 4$, then the integer $p|c|$ is a quadratic residue modulo any prime divisor of D_0.*
3. *If $p \equiv 3 \pmod 4$, then the integer $(p-1)/2$ is a quadratic residue modulo any prime divisor of D_0.*

A special case of trinomials of Theorem 1, already dealt with in the literature [9, 8], is when $c = 1$, that is, the trinomials $X^p + aX + a$, where a is an integer divisible by p exactly once. We stress that Kölle and Schmid [8] conjectured that the Galois group of $f(X)$ is always S_p when $c = 1$. However, in full generality this has been proved only for $p \leq 5$ so far [7]. Our methods of proof are similar to those used in [8], and we rectify a slight inaccuracy in that paper (see Remark 1). Item 1 of Theorem 1 is proved in [8, pp. 82–83] in the particular case which the authors consider, while items 2 and 3 are new: we deduce them from the Pellet–Stickelberger theorem.

The main idea of our proofs is the local method, that is, the study of the properties of some fields generated by the roots of the trinomial over local fields which are completions of $\mathbb{Q}$ with respect to specific absolute values. Our Lemma 1 can thus be seen as a local study at the infinite prime, namely over the real number field $\mathbb{R}$, while the subsequent lemmas constitute a local study at a finite prime q dividing D_0. In this study, we make use of Ore's theorem linking Newton polygons to the factorization of polynomials [11, 5]. While previous works, with the exception of [8], use exclusively the local study at primes which are ramified in extensions generated by the roots of the trinomial, it is remarkable that such a general study is feasible, because the prime numbers dividing D_0 are not necessarily ramified in such extensions.

In the next statement, based in part on Theorem 1 and also on [8, 9], we summarize the known results about the Galois group of the trinomial $f(X)$ when $c = 1$.

THEOREM 2. *Let $p \geq 7$ be a prime number and $a_1 \in \mathbb{Z} \setminus p\mathbb{Z}$. Set $a = pa_1$, $f(X) = X^p + aX + a$ and $D_0 = p^{p-1} + (p-1)^{p-1}a_1$. The Galois group over $\mathbb{Q}$ of the trinomial $f(X)$ is either isomorphic to the symmetric group S_p or to the affine group $\mathrm{AGL}(1,p)$, the latter occurring precisely when some splitting field of $f(X)$ over $\mathbb{Q}$ contains a pth primitive root of unity. The trinomial $f(X)$ is affect-free in each of the following cases:*

(a) *D_0 is not a square in $\mathbb{Z}$;*
(b) *a_1 is a square in $\mathbb{Z}$;*
(c) *$a_1 \not\equiv 1 \pmod p$;*
(d) *$a_1 < p$;*
(e) *there exists a prime divisor q of D_0 such that $q \not\equiv \pm 1 \pmod p$;*
(f) *there exists a prime divisor q of D_0 with $q \equiv 1 \pmod p$ such that $-p(p-1)/2$ is not a quadratic residue modulo q;*
(g) *there exists a prime divisor q of D_0 with $q \equiv -1 \pmod p$ such that $-p(p-1)/2$ is a quadratic residue modulo q;*
(h) *a is odd;*
(h′) *$a \equiv 2 \pmod 3$;*
(h″) *$p \equiv 2 \pmod 3$ and $a \equiv 1 \pmod 3$.*

Furthermore, we deduce from the law of quadratic reciprocity and Theorems 1 and 2 the following result, whose main interest is to specify the form of a possible counterexample to the Kölle–Schmid conjecture.

THEOREM 3. *Given a prime number $p \equiv 7 \pmod 8$ such that $\ell = (p-1)/2$ is also prime, and an integer $a_1 \in \mathbb{Z}$ which is coprime to p, for the Eisenstein trinomial*

$$f(X) = X^p + pa_1X + pa_1 \tag{2}$$

to be solvable, it is necessary that there exists an integer $\mu \equiv -4v \pm 2 \pmod p$ such that

$$a_1 = (v + 2^{2\ell-2}\mu)(u + \ell^{2\ell}\mu), \tag{3}$$

where (u,v) is the only ordered pair of natural integers such that $u2^{2\ell-2} - v\ell^{2\ell} = p^\ell$ and $u < \ell^{2\ell}$.

1. Local study. We start with the following well-known statement [6, p. 91].

LEMMA 0. *Any transitive and solvable permutation group of prime degree p is isomorphic to a subgroup of the affine group $\mathrm{AGL}(1,p)$.*

LEMMA 1. *If the trinomial $f(X)$ is solvable, then the integer D_0 is positive.*

Proof. The discriminant of the trinomial $f(X)$ is (see [16])

$$D(f) = (-1)^{(p-1)/2} p^p a_1^{p-1} |c|^{p(p-2)} D_0. \tag{4}$$

As p and $(p-1)a_1$ are coprime, certainly $D_0 \neq 0$, so that the trinomial $f(X)$ is separable. This allows us to define the Galois group G of the trinomial $f(X)$ over $\mathbb{Q}$, which is a permutation group acting on the p roots of this trinomial. By Descartes's rule [13, p. 41], $f(X)$ has at most three real roots. If it has exactly three real roots, then complex conjugation induces in G a permutation of the roots with exactly three fixed points. On the other hand, since $f(X)$ is irreducible (for it is Eisenstein), solvable and of prime degree p, we know from Lemma 0 that its Galois group G is isomorphic to a subgroup of the affine group $\mathrm{AGL}(1,p)$. In $\mathrm{AGL}(1,p)$, there is no permutation having exactly three fixed points [1]. So f cannot have three real roots, therefore it has a single one, so that the number r_2 of pairs of conjugate imaginary roots of $f(X)$ is exactly $(p-1)/2$. As $D(f)(-1)^{r_2} > 0$ [4], we deduce from (4) that D_0 is positive. ∎

For every prime q, we denote by v_q the q-adic valuation on $\mathbb{Q}$ or on its completion $\mathbb{Q}_q$ (the field of q-adic numbers).

Lemma 2. *Let q be a prime divisor of D_0. The Newton $(\mathbb{Q}_q, X+1)$-polygon of the polynomial*

$$f^*(X) = \left(\frac{p-1}{pc}\right)^p f\left(\frac{pc}{p-1}X\right)$$

is composed of two sides: a horizontal side of length $p-2$ and an oblique side (S) joining the points $(p-2,0)$ and $(p, v_q(D_0))$.

Proof. As pc and $(p-1)a_1$ are coprime, the divisor q of D_0 does not divide $p(p-1)c$. By Taylor's formula applied to f^* in the neighborhood of -1, we have

$$f^*(X) = \sum_{k=0}^{p} \frac{f^{*(k)}(-1)}{k!}(X+1)^k.$$

For $k=0$, $k=1$, and $2 \leq k \leq p$, we have respectively

$$f^*(-1) = \frac{-D_0}{|c|p^{p-1}}, \quad (f^*)'(-1) = \frac{D_0}{|c|p^{p-2}}, \quad \frac{f^{*(k)}(-1)}{k!} = \binom{p}{k}(-1)^{p-k}.$$

Hence

$$f^*(X) = \sum_{j=0}^{p-2} \binom{p}{j}(-1)^j (X+1)^{p-j} + \frac{D_0}{|c|p^{p-2}}(X+1) - \frac{D_0}{|c|p^{p-1}}. \tag{5}$$

From this expansion in powers of $X+1$, we construct Newton's cloud consisting of the following $p+1$ points: $(0,0)$, $\left(j, v_q\left(\binom{p}{j}\right)\right)$ for every integer j between 1 and $p-2$, $(p-1, v_q(D_0))$ and $(p, v_q(D_0))$. In particular, since the

integers q and $p(p-1)$ are coprime, the point $(p-2,0)$ belongs to this cloud. All the points of this cloud are above the horizontal axis, and the axis passes through at least two of these points, $(0,0)$ and $(p-2,0)$, which proves that the segment joining these points is a side of the Newton polygon. Likewise, all points in the cloud are above the line of equation $y = \frac{v_q(D_0)}{2}(x-(p-2))$ passing through the points $(p-2,0)$ and $(p, v_q(D_0))$. Thus the segment (S) joining them is a side of the Newton polygon. ∎

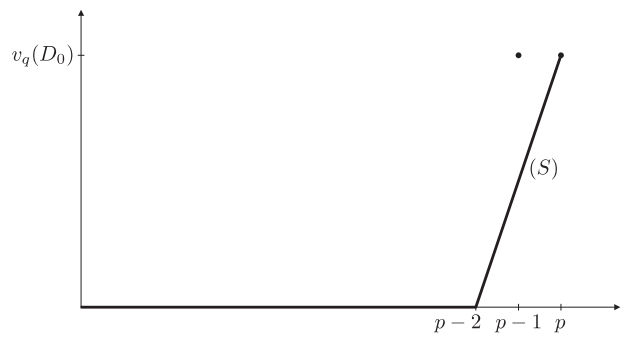

Fig. 1. Newton $(\mathbb{Q}_q, X+1)$-polygon.

LEMMA 3. *If $g(X) = X^p + aX + b$ $(ab \neq 0)$ is a trinomial with coefficients in a field K of characteristic not equal to p, then the greatest common divisor of $g(X)$ and of its derivative $g'(X)$ has degree at most* 1.

Proof. Indeed, $g'(X) = pX^{p-1} + a$ and $g(X) = g'(X)\frac{X}{p} + \frac{p-1}{p}aX + b$. Consequently, the gcd of $g(X)$ and $g'(X)$ must divide the nonzero polynomial $\frac{p-1}{p}aX + b$. ∎

LEMMA 4. *For every prime divisor q of D_0, the trinomial $f^*(X)$ of Lemma* 2 *factorizes in the ring $\mathbb{Z}_q[X]$ as*

$$f^*(X) = f_{p-2}(X)f_2(X), \tag{6}$$

where $f_{p-2}(X)$ is a monic polynomial of degree $p-2$ having as reduction modulo q a polynomial without multiple roots, and $f_2(X)$ is a monic polynomial of degree 2 *whose Newton $(\mathbb{Q}_q, X+1)$-polygon is a translate of the oblique side (S). Every splitting field of $f_{p-2}(X)$ over $\mathbb{Q}_q$ is an unramified extension of $\mathbb{Q}_q$.*

Proof. The factorization (6) results immediately from Lemma 2 and Ore's theorem [5]. From (6), we obtain the factorization

$$\overline{f^*}(X) = \overline{f_{p-2}}(X)(X+1)^2 \tag{7}$$

in the ring $\mathbb{F}_q[X]$ where $\overline{g}(X)$ denotes the reduction modulo q of $g(X) \in \mathbb{Z}_q[X]$. Since q and p are coprime, it follows from (7) and from Lemma 3

that $\overline{f_{p-2}}(X)$ is separable over $\mathbb{F}_q$. Using [10, Lemma 5.24, p. 222] we deduce that, for each root α of $f_{p-2}(X)$, the extension $\mathbb{Q}_q(\alpha)/\mathbb{Q}_q$ is unramified. Consequently, every splitting field F of $f_{p-2}(X)$ over $\mathbb{Q}_q$ is an unramified extension of $\mathbb{Q}_q$. ∎

LEMMA 5. *Assume that the Galois group G of $f(X)$ over $\mathbb{Q}$ is solvable. If q is a prime divisor of D_0, then the integer $v_q(D_0)$ is even.*

Proof. Suppose on the contrary that $v_q(D_0)$ is odd. By Lemma 2, the length of the horizontal projection of the oblique side (S) is $\ell = 2$, and the length of its vertical projection is $h = v_q(D_0)$. As the lengths ℓ and h are coprime in this case, it follows from [5, Theorem 1.5] that, denoting by β one root of $f_2(X)$, the ramification index of the extension $\mathbb{Q}_q(\beta)/\mathbb{Q}_q$ is even. Because the polynomial $f_2(X)$ has degree 2, we see that the extension $\mathbb{Q}_q(\beta)/\mathbb{Q}_q$, which is a splitting field of $f_2(X)$ over $\mathbb{Q}_q$, is totally ramified of degree 2.

Let N_q be a splitting field of $f(X)$ (or of $f^*(X)$) over $\mathbb{Q}_q$, β a root of $f_2(X)$ in N_q, and $E/\mathbb{Q}_q$ the subextension of $N_q/\mathbb{Q}_q$ generated by the roots of $f_{p-2}(X)$. According to (6), N_q is the compositum of the fields E and $\mathbb{Q}_q(\beta)$. Since the extension $E/\mathbb{Q}_q$ is unramified, it follows from Abhyankar's Lemma [10, Corollary 4, p. 229] that the ramification index of $N_q/\mathbb{Q}_q$ is 2.

Let N be the subfield of N_q generated by the roots of $f(X)$ (or of $f^*(X)$). It is readily seen that N is a splitting field of $f(X)$ over $\mathbb{Q}$, so that the Galois group G can be identified with the group of automorphisms of N. It follows from the above that the inertia group I of the place of N induced by the maximal ideal of N_q is of order 2, and that its generator fixes the roots of $f_{p-2}(X)$. Consequently, the group I is generated by a transposition. As the affine group $\mathrm{AGL}(1,p)$ has no transposition, we conclude that G is not isomorphic to a subgroup of $\mathrm{AGL}(1,p)$. Thus, from Lemma 0, we conclude that G is not solvable. ∎

LEMMA 6. *If the Galois group G of the trinomial $f(X)$ is solvable, and $f_2(X)$ and $f_{p-2}(X)$ are as in Lemma 4, then, for every prime divisor q of D_0, we have:*

(a) *the field $\mathbb{Q}_q(\sqrt{-p(p-1)|c|/2})$ is a splitting field of $f_2(X)$ over $\mathbb{Q}_q$;*
(b) *every irreducible factor of $f^*(X)$ over $\mathbb{Q}_q$ is of degree at most 2, and the number r of irreducible factors of $f_{p-2}(X)$ over $\mathbb{Q}_q$ is given by*

$$r = \begin{cases} p-2 & \text{if } -p(p-1)|c|/2 \text{ is a quadratic residue modulo } q, \\ (p-1)/2 & \text{if not.} \end{cases} \tag{8}$$

Proof. From Lemma 5, we know that $v_q(D_0)$ is even. In this case, the length of the horizontal projection of the side (S) is $\ell = 2$, and the length of its vertical projection is $h = v_q(D_0)$, which is an even number. To find the associated polynomial of (S), we can apply [5, Proposition 3.4]: the slope of

(S) being the integer $\rho = v_q(D_0)/2$, we introduce on $\mathbb{Q}_q(X)$ the valuation w such that, for every polynomial $Q(X) \in \mathbb{Q}_q[X]$,

$$w(Q) = \min\left\{ v_q\left(\frac{Q^{(k)}(-1)}{k!}\right) + k\frac{v_q(D_0)}{2} : k \in \mathbb{N}\right\}.$$

We set $g(X) = f^*(X)/q^{v_q(D_0)}$ and we consider its residue class $G(Y)$ in the residual field of w; this residue class is a polynomial (with coefficients from the residue field of $\mathbb{Q}_q$) in the residue class Y of $\frac{X+1}{q^{v_q(D_0)/2}}$ [5, Proposition 2.4]. By (5), we get

$$g(X) = \sum_{j=0}^{p-2} \binom{p}{j}(-1)^j(X+1)^{p-j}q^{-v_q(D_0)} + \frac{D_0^*}{|c|p^{p-2}}(X+1) - \frac{D_0^*}{|c|p^{p-1}}. \tag{9}$$

where $D_0^* = D_0 q^{-v_q(D_0)}$ is the greatest divisor of D_0 which is coprime to q. In (9), the terms $\binom{p}{j}(-1)^j(X+1)^{p-j}q^{-v_q(D_0)}$ have a positive w-valuation for all $0 \le j < p-2$. Similarly the w-valuation of $\frac{D_0^*}{|c|p^{p-2}}(X+1)$ is $v_q(D_0)/2 > 0$. So $G(Y)$ is the residue class of $-\binom{p}{p-2}(X+1)^2q^{-v_q(D_0)} - \frac{D_0^*}{|c|p^{p-1}}$. Hence, denoting by $\overline{x}$ the residue class of the integer x modulo the prime q, we conclude that

$$G(Y) = -\frac{\overline{p}(\overline{p}-\overline{1})}{\overline{2}}Y^2 - \frac{\overline{D_0^*}}{\overline{|c|}\,\overline{p}^{p-1}}.$$

Dividing $G(Y)$ by its leading coefficient, we obtain the residue class of the associated polynomial of (S) modulo the ideal $(q, X+1)$. So we conclude that the associated polynomial of the side (S) modulo $(q, X+1)$ is

$$F(Y) \equiv Y^2 + \frac{2D_0^*}{|c|p^p(p-1)} \pmod{(q, X+1)}. \tag{10}$$

From Lemma 4, the trinomial $f^*(X)$ factorizes as (6), where $f_{p-2}(X) \in \mathbb{Z}_q[X]$ is a polynomial of degree $p-2$, whose splitting fields over $\mathbb{Q}_q$ are unramified extensions of $\mathbb{Q}_q$. As q is odd (since it does not divide $p(p-1)$), the polynomial $F(Y)$ is separable modulo q. Thus, by [5, Theorem 1.5], a splitting field of $f_2(X)$ over $\mathbb{Q}_q$ is an unramified extension of $\mathbb{Q}_q$. Moreover it can be deduced from [5, Theorem 1.5] that the factorization of $f_2(X)$ in $\mathbb{Q}_q[X]$ is of the same form as that of the reduction $\overline{F}(Y)$ modulo q of the associated polynomial $F(Y)$ in $\mathbb{F}_q[Y]$. As D_0^* is a square in $\mathbb{Z}$ by Lemmas 1 and 4, equation (10) shows that the factorization of $\overline{F}(Y)$ depends only upon the quadratic character of $-p(p-1)|c|/2$ modulo q. Hence the degree of a splitting field over $\mathbb{Q}_q$ of $f_2(X)$ is 1 or 2 depending on whether the integer $-p(p-1)|c|/2$ is a quadratic residue modulo q or not. As q is coprime to $p(p-1)$, the field $\mathbb{Q}_q(\sqrt{-p(p-1)|c|/2})$ is an unramified extension of $\mathbb{Q}_q$ having the same degree as a splitting field over $\mathbb{Q}_q$ of the polynomial $f_2(X)$;

as two unramified extensions of $\mathbb{Q}_q$ with the same degree are isomorphic, this proves our first assertion (a).

Let N_q be a splitting field of $f^*(X)$ over $\mathbb{Q}_q$. Since every root of $f^*(X)$ generates an unramified extension of $\mathbb{Q}_q$, the field N_q is an unramified extension of $\mathbb{Q}_q$. Thus the decomposition group, that is, the Galois group of $f^*(X)$ over $\mathbb{Q}_q$, is cyclic. Now we distinguish two cases.

Case 1: *The integer $-p(p-1)|c|/2$ is a quadratic residue modulo q.* Then the reduction $\overline{F}(Y)$ modulo q of the associated polynomial $F(Y)$ factorizes into two polynomials of degree 1 in $\mathbb{F}_q[Y]$. Consequently, $f_2(X)$ factorizes into two factors of degree 1 in $\mathbb{Q}_q[X]$, so all permutations in the Galois group of $f(X)$ over $\mathbb{Q}_q$ have to fix the two roots of $f_2(X)$. As G is supposed to be solvable, and as the only permutation of $\mathrm{AGL}(1,p)$ which fixes two points is the identity, we see by Lemma 0 that $f_{p-2}(X)$ splits over $\mathbb{Q}_q$, and so has $p-2$ irreducible factors in $\mathbb{Q}_q[X]$.

Case 2: *$-p(p-1)|c|/2$ is not a quadratic residue modulo q.* Then the reduction $\overline{F}(Y)$ of $F(Y)$ modulo q is irreducible in $\mathbb{F}_q[Y]$, so that $f_2(X)$ is irreducible over $\mathbb{Q}_q$. One generator of the Galois group G_q of $f^*(X)$ over $\mathbb{Q}_q$ then acts by exchanging the two roots of $f_2(X)$, and thus is of even order. As by Lemma 0 the group G, and hence also G_q, is isomorphic to a subgroup of $\mathrm{AGL}(1,p)$, we conclude that this generator of G_q has only one fixed point, which is necessarily a root of $f_{p-2}(X)$. By examining the permutations included in $\mathrm{AGL}(1,p)$, we see that the only permutations in this group which have exactly one fixed point and a cycle of length 2 are products of $(p-1)/2$ disjoint transpositions. Consequently, $f_{p-2}(X)$ factorizes over $\mathbb{Q}_q$ into $(p-1)/2$ irreducible factors: one of degree 1 and $(p-3)/2$ of degree 2.

Remark 1. Equation (10) expressing the associated polynomial $F(Y)$ of the side (S) indicates that the similar computation contained in [8, p. 82, line -1] is erroneous. This explains why, if we have $c=1$ as in [8], our discussion depends on the quadratic character of $-p(p-1)/2$, and not on that of $-p/(p-1)$.

2. Proof of Theorem 1. Suppose G is solvable. Lemmas 1 and 5 show that the integer D_0 is a square in $\mathbb{Z}$.

By (4) and (6), there is a nonzero element x of $\mathbb{Q}_q$ such that

$$D(f_{p-2})D(f_2) = (-1)^{(p-1)/2}p|c|x^2, \tag{11}$$

where $D(f_{p-2})$ and $D(f_2)$ are the respective discriminants of the polynomials in the factorization (6). Since, by Lemma 6, $\mathbb{Q}_q(\sqrt{-p(p-1)|c|/2})$ is a splitting field of $f_2(X)$ over $\mathbb{Q}_q$, we have $-\frac{p(p-1)|c|}{2}D(f_2) \in \mathbb{Q}_q^{*2}$, and (11) implies that $D(f_{p-2}) \in (-1)^{(p+1)/2}\frac{p-1}{2}\mathbb{Q}_q^{*2}$.

Denote by r the number of irreducible factors of $f_{p-2}(X)$ in $\mathbb{Q}_q[X]$. By the Pellet–Stickelberger theorem [16, Theorem 1, p. 1100], and since by Lemma 4 the reduction $\overline{f_{p-2}}(X)$ of $f_{p-2}(X)$ modulo q is separable, we have

$$r \text{ is odd} \Leftrightarrow D(f_{p-2}) \text{ is a square in } \mathbb{Q}_q. \tag{12}$$

Suppose first that $p \equiv 1 \pmod 4$, so that $D(f_{p-2})$ belongs to $-\frac{p-1}{2}\mathbb{Q}_q^{*2}$. Lemma 6 shows that the number r of irreducible factors of $f_{p-2}(X)$ in $\mathbb{Q}_q[X]$ is odd when $-p(p-1)|c|/2$ is a quadratic residue modulo q, and is even otherwise. Using the Pellet–Stickelberger theorem, we see that $-(p-1)/2$ is a square in $\mathbb{Q}_q^*$ if and only if $-p(p-1)|c|/2$ is. Therefore, the product of these two invertible elements of $\mathbb{Z}_q$ is always a square in $\mathbb{Q}_q^*$. So $p|c|$ is always a square in $\mathbb{Q}_q^*$, that is, the integer $p|c|$ is a quadratic residue modulo q.

Now we assume $p \equiv 3 \pmod 4$. We have seen that then $D(f_{p-2}) \in \frac{p-1}{2}\mathbb{Q}_q^{*2}$, and Lemma 6 now shows that the number r of irreducible factors of $f_{p-2}(X)$ in $\mathbb{Q}_q[X]$ is odd, regardless of the quadratic character of $-p(p-1)|c|/2$ modulo q. We then deduce by the Pellet–Stickelberger theorem that $(p-1)/2$ is a quadratic residue modulo q.

3. Proof of Theorem 2. Denote by G the Galois group of $f(X) = X^p + aX + a$ over $\mathbb{Q}$. We suppose that $a = pa_1$, with $a_1 \in \mathbb{Z}$ coprime to p. For the proof of Theorem 2, we rely upon known results. We observe first that Movahhedi has shown that G is either S_p or $\mathrm{AGL}(1,p)$ [9, Theorem 3.1]. The equivalence between the solvability of $f(X)$ and the fact that a pth primitive root of unity belongs to a splitting field of $f(X)$ over $\mathbb{Q}$ results from classical work of Wegener and Hasse, quoted in [8]. Movahhedi has reproved this result in a more readable form [9, Theorem 2.2].

Item (a) of Theorem 2 is simply item 1 of Theorem 1, and (c) is a result of Movahhedi [9, Theorem 4.3].

To justify (b), one can argue as follows. Suppose that $a_1 = h^2$ is the square of an integer h and that $f(X)$ is not affect-free. Then, by Theorem 1, $D_0 = p^{p-1} + (p-1)^{p-1}h^2$ has to be the square of an integer. By using the fact that h and p are coprime, it is readily seen that we must have $p^{p-1} = 2(p-1)^{(p-1)/2}h + 1$, showing that $\pm 2h + 1 \equiv 0 \pmod p$. But by (c) we have $h \equiv \pm 1 \pmod p$. So $\pm 2 + 1$ is divisible by p, which is not the case.

For (d), one can distinguish three cases: the case $a_1 < 0$ is dealt with by Movahhedi [9, Theorem 4.5], the case $a_1 = 1$ is a particular instance of (b), and the case $1 < a_1 < p$ is implied by (c).

It has been shown by Kölle and Schmid [8, p. 83] that if G is the affine group and q divides D_0, then $q \equiv 1 \pmod p$ if the decomposition group in q is trivial, and $q \equiv -1 \pmod p$ if not. This justifies (e) of Theorem 2. When one takes Lemma 6 into account, one also gets (f) and (g).

Items (h), (h′), (h″) are observations of Kölle and Schmid [8, p. 83].

4. Proof of Theorem 3. Let $p \geq 7$ be a prime number and set $\ell = (p-1)/2$. If the trinomial $f(X) = X^p + pa_1X + pa_1$ is solvable, where p does not divide a_1, then Lemmas 1 and 5 show the existence of $y \in \mathbb{Z}$ such that

$$D_0 = p^{2\ell} + (2\ell)^{2\ell}a_1 = y^2. \tag{13}$$

Replacing y by its negative if necessary, we can suppose that y is positive. Obviously, y must be odd, so that $w = (y + p^\ell)/2$ and $w' = (y - p^\ell)/2$ are integers. As p does not divide a_1, these integers are coprime. According to (13), we also have $ww' = 2^{2\ell-2}\ell^{2\ell}a_1$, so that $2^{2\ell-2}$ must divide one and only one of w and w'. We set accordingly

$$\frac{y + \epsilon p^\ell}{2} = 2^{2\ell-2}x, \tag{14}$$

where $\epsilon \in \{-1, 1\}$ and $x \in \mathbb{Z}$. Then $(y - \epsilon p^\ell)/2 = 2^{2\ell-2}x - \epsilon p^\ell$, hence $ww' = 2^{2\ell-2}x(2^{2\ell-2}x - \epsilon p^\ell) = 2^{2\ell-2}\ell^{2\ell}a_1$, which leads to

$$x(2^{2\ell-2}x - \epsilon p^\ell) = \ell^{2\ell}a_1. \tag{15}$$

Supposing now that ℓ is prime and $p \equiv 7 \pmod 8$, and recalling that G is solvable, we want to show that ℓ does not divide x. Assume otherwise. Since ℓ is coprime to $p = 2\ell + 1$, it is coprime to $2^{2\ell-2}x - \epsilon p^\ell$, so that (15) shows the existence of $\mu \in \mathbb{Z}$ such that

$$x = \ell^{2\ell}\mu. \tag{16}$$

From (14) and (16),

$$y = 2^{2\ell-1}\ell^{2\ell}\mu - \epsilon p^\ell. \tag{17}$$

As the exponent $2\ell - 1 \geq 5$ and ℓ are odd, we have $y \equiv \epsilon \pmod 4$. Furthermore, since $f(X)$ is assumed to be solvable, item 3 of Theorem 1 shows that ℓ is a quadratic residue modulo every prime dividing y; hence the Jacobi symbol $\left(\frac{\ell}{y}\right)$ is 1. Then the law of quadratic reciprocity and the congruence $\ell \equiv 3 \pmod 4$ yield

$$\left(\frac{y}{\ell}\right) = (-1)^{(y-1)/2} = (-1)^{(\epsilon-1)/2}. \tag{18}$$

Now, according to (17), and as $p \equiv 1 \pmod \ell$, we have $\left(\frac{y}{\ell}\right) = \left(\frac{-\epsilon}{\ell}\right) = (-1)^{\frac{\ell-1}{2}\cdot\frac{\epsilon+1}{2}} = (-1)^{\frac{\epsilon+1}{2}}$. Consequently, $\frac{\epsilon-1}{2} \equiv \frac{\epsilon+1}{2} \pmod 2$, a contradiction.

Since the prime integer ℓ does not divide x, (15) shows that $\ell^{2\ell}$ must divide the integer $2^{2\ell-2}x - \epsilon p^\ell$, so that we can write

$$2^{2\ell-2}x - \epsilon p^\ell = \ell^{2\ell}\lambda \quad (\lambda \in \mathbb{Z}). \tag{19}$$

Consider the unique integer $u \in]0, \ell^{2\ell}[$ such that $u2^{2\ell-2} \equiv p^\ell \pmod{\ell^{2\ell}}$. By setting $v = (u2^{2\ell-2} - p^\ell)/\ell^{2\ell}$, we obtain an integer $v \in]0, 2^{2\ell-2}[$ such that $u2^{2\ell-2} - v\ell^{2\ell} = p^\ell$. Substituting this expression for p^ℓ in (19), we obtain

$2^{2\ell-2}(x-u\epsilon) = \ell^{2\ell}(\lambda - v\epsilon)$, which proves the existence of $\mu \in \mathbb{Z}$ such that $x - u\epsilon = \ell^{2\ell}\mu$ and $\lambda = v\epsilon + 2^{2\ell-2}\mu$. By substituting this expression of λ in (19), then applying (15), we find after simplification

$$a_1 = (v\epsilon + 2^{2\ell-2}\mu)(u\epsilon + \ell^{2\ell}\mu),$$

which is exactly (3) if $\epsilon = 1$. When $\epsilon = -1$, the procedure leads to the same equation (3) after replacing the parameter μ by its negative.

In addition, item 1 of Theorem 1 and Theorem 2(e) entail that $D_0 \equiv 1 \pmod p$. As $D_0 \equiv a_1 \pmod p$, we choose the integer μ such that $(v + 2^{2\ell-2}\mu)(u + \ell^{2\ell}\mu) \equiv 1 \pmod p$. The residue class $\overline{\mu}$ of μ modulo the prime integer p is then a root of a quadratic equation, and it is easy to check directly that the two classes of integers $-4v \pm 2$ are two different solutions in the field $\mathbb{Z}/p\mathbb{Z}$, so these are the only solutions, which shows that $\mu \equiv -4v \pm 2 \pmod p$.

Example. When $p = 7$, we have $\ell = 3$ and $(u, v) = (67, 1)$. We conclude that if the Galois group of the trinomial $X^7 + 7a_1X + 7a_1$ is solvable, then there exists a rational integer μ such that $a_1 = 67 + 1801\mu + 2^4 \cdot 3^6 \cdot \mu^2$. Furthermore, it is necessary that $\mu \equiv -4 \pm 2 \pmod 7$, that is, the parameter μ is congruent to 1 or -2 modulo 7.

5. A remark about classification of trinomials. The goal of this section is to justify an assertion made in the Introduction: if $f_0(X) = AX^n + BX + C$ $(ABC \neq 0)$ is a trinomial with rational coefficients of degree $n > 1$, then there exists $k \in \mathbb{Q}^*$ such that $A^{-1}k^n f_0(X/k)$ is of the form $f(X) = X^n + ac^{n-2}X + ac^{n-1}$ for two coprime integers a and c. Indeed, simply write the rational number $AC^{n-1}/B^n \neq 0$ as the quotient c/a of two coprime integers, and set $k = \frac{aAC^{n-2}}{B^{n-1}}$. The assertion then results from a direct computation.

Acknowledgements. We are indebted to an anonymous referee for his comments and suggestions.

References

[1] S. S. Abhyankar, *Galois theory on the line in nonzero characteristic*, Bull. Amer. Math. Soc. 27 (1992), 68–133.

[2] J. Angeli, *Trinômes irréductibles résolubles sur un corps de nombres*, Acta Arith. 127 (2007), 169–178.

[3] B. Bensebaa, A. Movahhedi and A. Salinier, *The Galois group of $X^p + aX^s + a$*, Acta Arith. 134 (2008), 55–65.

[4] A. Brill, *Ueber die Discriminante*, Math. Ann. 12 (1877), 87–89.

[5] S. D. Cohen, A. Movahhedi and A. Salinier, *Factorization over local fields and the irreducibility of generalized difference polynomials*, Mathematika 14 (2000), 173–196.

[6] J. D. Dixon and B. Mortimer, *Permutation Groups*, Grad. Texts in Math. 163, Springer, Berlin, 1996.
[7] L. Gauckler, *The Galois group of the Eisenstein polynomial* $X^5 + aX + a$, Arch. Math. (Basel) 90 (2008), 136–139.
[8] M. Kölle and P. Schmid, *Computing Galois groups by means of Newton polygons*, Acta Arith. 115 (2004), 71–84.
[9] A. Movahhedi, *Galois group of* $X^p + aX + a$, J. Algebra 180 (1996), 966–975.
[10] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 3rd ed., Springer Monogr. Math., Springer, Berlin, 2004.
[11] O. Ore, *Newtonsche Polygone in der Theorie der algebraischen Körper*, Math. Ann. 99 (1928), 84–117.
[12] H. Osada, *The Galois groups of the polynomials* $x^n + ax^s + b$, J. Number Theory 25(1987), 230–238.
[13] G. Pólya and G. Szegö, *Problems and Theorems in Analysis, Volume 2*, Springer, New York, 1976.
[14] A. Schinzel, *On reducible trinomials*, Dissertationes Math. 329 (1993), 83 pp.
[15] J.-P. Serre, *Topics in Galois Theory*, Res. Notes in Math. 1, Jones and Barlett, Boston, MA, 1992.
[16] R. G. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math. 12 (1962), 1099–1106.

Chahrazede Bouyacoub
Laboratoire d'Arithmétique, Codage,
Combinatoire et Calcul formel
LA3C, USTHB
BP 32, El Alia, Bab Ezzouar 16111
Alger, Algeria
E-mail: cbouyacoub@yahoo.fr

Alain Salinier
Pôle de Mathématiques et Informatique
Laboratoire XLIM (UMR CNRS 7252)
Université de Limoges
123, avenue Albert Thomas
87060 Limoges Cedex, France
E-mail: alain.salinier@unilim.fr