

## The Galois group of $X^p + aX^s + a$

by

B. BENSEBAA, A. MOVAHHEDI and A. SALINIER (Limoges)

**1. Introduction.** Let  $p$  be an odd prime number and  $s < p$  a positive integer. In this paper we study the absolute Galois group  $G$  of a trinomial  $\varphi(X) = X^p + aX^s + a$ ,  $a \in \mathbb{Z}$ , supposed to be irreducible over the field  $\mathbb{Q}$  of rational numbers. This Galois group was previously studied in [8, 9, 11] when  $s = 1$  and the  $p$ -adic valuation  $v_p(a)$  of the integer  $a$  is  $\leq 1$ . When  $s = v_p(a) = 1$ , the Galois group  $G$  is isomorphic either to the symmetric group  $S_p$  or to the affine group  $\text{Aff}(\mathbb{F}_p)$ . When  $s = 1$  and  $v_p(a) = 0$ , then  $G \simeq S_p$  if the discriminant  $D$  of  $\varphi(X)$  is not a square; otherwise,  $G$  is isomorphic either to the alternating group  $A_p$  or to the projective special linear group  $\text{PSL}_2(2^e)$ . The latter is, of course, only possible when  $p - 1$  is a power of 2.

Here we deal with the Galois group of  $\varphi(X)$  under very general circumstances. In fact, the only case we do not cover is where we simultaneously have

$$p \mid a, \quad p \nmid v_p(a), \quad sv_p(a) < p, \quad \gcd(p - 1, sv_p(a)) > 1.$$

With a few minor exceptions, we prove that if the Galois group is not solvable then it is simply  $S_p$  or  $A_p$ .

Let  $N$  be the splitting field of  $\varphi(X)$  over  $\mathbb{Q}$ . By using Newton polygons, we determine the inertia groups of ramified primes in  $N/\mathbb{Q}$ . For a prime  $\ell \neq p$  which ramifies in  $N$ , the inertia group is cyclic of order  $p$ . For  $p > 3$ , the prime  $p$  ramifies in  $N$  precisely when  $p$  divides  $a$ . To determine the inertia group of  $p$ , we argue according to whether  $p$  divides  $v_p(a)$  or not. The ramification of  $p$  in  $N$  is wild if  $p$  does not divide  $v_p(a)$  (Lemma 2.1) where the approach is similar to that of the cases already treated in the literature.

---

2000 *Mathematics Subject Classification*: Primary 11R32, 12F10; Secondary 11S15, 12E10.

*Key words and phrases*: trinomials, inertia groups, Newton polygons, classification of finite simple groups, Galois group.

Assume now that  $v_p(a) = kp$  with an integer  $k \geq 1$ . Then the ramification of  $p$  in  $N$  can be tame or wild. We manage to compute the corresponding inertia group in each case (Proposition 2.5) using the results of a previous paper on the factorization of a polynomial over a local field [4].

Once we know the different inertia groups in  $N/\mathbb{Q}$ , we determine  $G$  using the list of possible Galois groups over  $\mathbb{Q}$  of prime degree trinomials given by Feit [7].

**Acknowledgements.** It is a pleasure to thank Alain Kraus for correspondence concerning the elliptic curve occurring in Section 3.

**2. Inertia groups.** Let  $p$  be an odd prime number and  $\varphi(X) = X^p + aX^s + a$  be a trinomial with  $0 \neq a \in \mathbb{Z}$ ,  $1 \leq s \leq p-1$ , supposed to be irreducible over  $\mathbb{Q}$ . We denote by  $\alpha := \alpha_1, \alpha_2, \dots, \alpha_p$  the different roots of  $\varphi$  in an algebraic closure of  $\mathbb{Q}$ . Let  $K := \mathbb{Q}(\alpha)$  be the field obtained by adjoining the root  $\alpha$  to the field  $\mathbb{Q}$ , and  $N := \mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_p)$  be the normal closure of  $K$  over  $\mathbb{Q}$ . We consider the Galois group  $G$  of  $N$  over  $\mathbb{Q}$  as a transitive group of permutations of the roots of  $\varphi$ . The discriminant  $D$  of  $\varphi$  is [15, Theorem 2]

$$D = (-1)^{(p-1)/2} a^{p-1} [p^p + (p-s)^{p-s} s^s a^s].$$

We set  $\delta := \min(p, sv_p(a))$  and  $b := a/p^{v_p(a)}$ , so that

$$(1) \quad D = (-1)^{(p-1)/2} p^{p-1} p^{(p-1)v_p(a)+\delta} D_0,$$

where

$$(2) \quad D_0 = p^{p-\delta} + (p-s)^{p-s} s^s b^s p^{sv_p(a)-\delta}.$$

**2.1. Inertia above  $p$ .** Here we will determine the inertia group of a  $p$ -adic place  $\wp$  of  $N$ . From the expression of  $D$ , we deduce that if  $p$  does not divide  $a$ , then the place  $\wp$  is unramified over  $p$ . For the rest of this section, we suppose that  $p$  divides  $a$  and we argue according to whether  $p$  divides  $v_p(a)$  or not.

First suppose that  $p$  does not divide  $v_p(a)$ :

**LEMMA 2.1.** *If  $p|a$  and  $p$  does not divide  $v_p(a)$ , then the prime number  $p$  is totally ramified in  $K = \mathbb{Q}(\alpha)$ .*

*Proof.* The  $(\mathbb{Q}_p, X)$ -polygon [4] of  $\varphi(X)$  has a unique side  $S$  joining the point  $(0, 0)$  to  $(p, v_p(a))$ . As  $v_p(a)$  and  $p$  are coprime, we see by [4, Theorem 1.5] that the ramification index of the local extension  $\mathbb{Q}_p(\alpha)/\mathbb{Q}_p$  is equal to  $p$ . ■

**PROPOSITION 2.2.** *Assume  $p|a$  and  $p$  does not divide  $v_p(a)$ . Further assume that  $\gcd(p-1, sv_p(a)) = 1$  if  $sv_p(a) < p$ . Then the inertia group of  $p$  (in fact of a prime of  $N$  above  $p$ ) in  $N/\mathbb{Q}$  is isomorphic to the affine group  $\text{Aff}(\mathbb{F}_p)$ .*

*Proof.* Consider the polynomial

$$\psi(X) = \frac{\varphi(\alpha(X+1))}{\alpha^p X} = X^{p-1} + \sum_{i=1}^{p-1} a_i X^{p-1-i}$$

in  $\mathbb{Q}(\alpha)[X]$  where the coefficient  $a_i$  is given by

$$a_i = \begin{cases} \binom{p}{i} & \text{if } 1 \leq i \leq p-s-1, \\ \binom{p}{i} + \binom{s}{i+s-p} \frac{a}{\alpha^{p-s}} & \text{if } p-s \leq i \leq p-1. \end{cases}$$

Introduce a prime element  $\pi$  of  $\mathbb{Q}_p(\alpha)$ . The  $\pi$ -adic valuations  $v_\pi(a_i)$  of the coefficients  $a_i$  are given by

$$v_\pi(a_i) = \begin{cases} p & \text{if } 1 \leq i \leq p-s-1, \\ \min(p, sv_p(a)) & \text{if } p-s \leq i \leq p-1, \end{cases}$$

since  $v_\pi(\alpha) = v_p(a)$  and  $v_\pi(x) = pv_p(x)$  for any rational  $x$  by Lemma 2.1.

So the  $(\mathbb{Q}_p(\alpha), X)$ -polygon [4] of  $\psi(X)$  has a unique side  $S$  joining  $(0, 0)$  to  $(p-1, \min(p, sv_p(a)))$ . By hypothesis, the integers  $p-1$  and  $\min(p, sv_p(a))$  are coprime. Hence by [4, Theorem 1.5] the ramification index of the local extension  $\mathbb{Q}_p(\alpha, \alpha_2)/\mathbb{Q}_p(\alpha)$  is equal to  $p-1$ . So the inertia group of  $p$  in  $N/\mathbb{Q}_p$  is a transitive solvable permutation group of prime degree  $p$  with order at least  $p(p-1)$ . The proposition follows by [6, Section 3.5]. ■

Assume now that  $p$  divides  $v_p(a) > 0$ : let  $v_p(a) = kp$  for an integer  $k \geq 1$  and  $b := a/p^{kp}$ . Consider in  $\mathbb{Q}[X]$  the polynomial

$$\psi(X) := \frac{\varphi(p^k X)}{p^{kp}} = X^p + bp^{ks} X^s + b.$$

By the Taylor formula, we can write

$$(3) \quad \psi(X) = (X+b)^p + \sum_{i=1}^{p-1} a_i (X+b)^{p-i} + a_p$$

where the coefficient  $a_i$  is given by

$$a_i = \begin{cases} \binom{p}{i} (-b)^i & \text{if } 1 \leq i \leq p-s-1, \\ \binom{p}{i} (-b)^i - \binom{s}{i+s-p} p^{ks} (-b)^{i+s-p+1} & \text{if } p-s \leq i \leq p-1, \\ -b^p + (-1)^s p^{ks} b^{s+1} + b & \text{if } i = p. \end{cases}$$

We discuss several cases according to the  $p$ -adic valuation of  $b^{p-1} - (-1)^s p^{ks} b^s - 1$ .

LEMMA 2.3. *Assume that  $v_p(b^{p-1} - (-1)^s p^{ks} b^s - 1) = 1$ . Then  $p$  is totally ramified in  $K = \mathbb{Q}(\alpha)$ .*

*Proof.* As  $v_p\left(\binom{p}{i}(-b)^i\right) = 1$  for all  $i = 1, \dots, p-1$ , the  $(\mathbb{Q}_p, X+b)$ -polygon [4] of  $\psi(X)$  has a unique side  $S$  joining  $(0, 0)$  to  $(p, 1)$ . By [4, Theorem 1.5] the ramification index of the local extension  $\mathbb{Q}_p(\alpha)/\mathbb{Q}_p$  is equal to  $p$ . ■

LEMMA 2.4. *Assume that  $v_p(b^{p-1} - (-1)^s p^{ks} b^s - 1) > 1$ . Then the prime decomposition of  $p$  in  $K = \mathbb{Q}(\alpha)$  is  $p = \mathfrak{p}_1^{p-1} \mathfrak{p}_2$  in each of the following two cases:*

- (i)  $k = s = 1$  and  $b \not\equiv -1 \pmod{p}$ ;
- (ii)  $ks > 1$ .

*If neither of the above two conditions holds, then  $p = \mathfrak{p}_1^{p-2} \mathfrak{a}$  in  $K$ , where  $\mathfrak{p}_1$  is a prime ideal of  $K$ .*

*Proof.* The coefficient  $a_{p-1}$  of the Taylor expansion (3) is  $a_{p-1} = p(b^{p-1} - (-1)^s s b^s p^{ks-1})$ . So  $v_p(a_{p-1}) = 1$  precisely when (i) or (ii) holds.

Now, in both cases (i) and (ii), the  $(\mathbb{Q}_p, X+b)$ -polygon [4] of  $\psi(X)$  has two sides:  $S_1$  joining  $(0, 0)$  to  $(p-1, 1)$  and  $S_2$  joining  $(p-1, 1)$  to  $(p, v_p(b^{p-1} - (-1)^s s p^{ks} b^s - 1))$ . The corresponding associated polynomials, being linear, are irreducible. We conclude by [4, Theorem 1.8].

If neither (i) nor (ii) holds, then  $k = s = 1$  and  $v_p(a_{p-1}) > 1$ . As  $s = 1$ , we necessarily have  $v_p(a_{p-2}) = 1$ , so that the  $(\mathbb{Q}_p, X+b)$ -polygon [4] of  $\psi(X)$  has two or three sides, the first of which,  $S_1$ , joins  $(0, 0)$  to  $(p-2, 1)$ . The associated polynomial of  $S_1$  being linear, once again we conclude by [4, Theorem 1.8]. ■

As the following example shows, when  $k = s = 1$ , the  $(\mathbb{Q}_p, X+b)$ -polygon of  $\psi(X)$  may have one, two or three sides according to the choice of  $b$ :

- if  $b = -1 + 2p$ , then  $v_p(b^{p-1} + pb - 1) = 1$ , hence a unique side;
- if  $b = 1 + p$ , then  $v_p(b^{p-1} + pb - 1) \geq 2$  and  $b \not\equiv -1 \pmod{p}$ , hence two sides;
- if  $b = -1 + p - p^2 + \frac{5(p+1)}{2}p^3$  for  $p > 3$ , then  $v_p(b^{p-1} + pb - 1) \geq 4$  and  $v_p(b^{p-2} + 1) = 1$ , hence three sides.

We are now going to look at the inertia at  $p$  in the extension  $N/K$ .

PROPOSITION 2.5. *Assume  $p \mid v_p(a) \geq 1$ . Let  $v_p(a) = kp$  for an integer  $k \geq 1$  and  $b := a/p^{kp}$ .*

- (1) *If  $v_p(b^{p-1} - (-1)^s p^{ks} b^s - 1) = 1$ , then the inertia group of  $p$  (in fact of a prime of  $N$  above  $p$ ) in  $N/\mathbb{Q}$  is isomorphic to  $\text{Aff}(\mathbb{F}_p)$  except when  $k = s = 1$  and  $b \equiv -1 \pmod{p}$ , in which case it is isomorphic to the subgroup of index 2 of  $\text{Aff}(\mathbb{F}_p)$ .*

- (2) If instead  $v_p(b^{p-1} - (-1)^s p^{ks} b^s - 1) > 1$ , then the inertia group of  $p$  in  $N/\mathbb{Q}$  is cyclic; it is generated by a  $(p-1)$ -cycle except when  $k = s = 1$  and  $b \equiv -1 \pmod{p}$ , in which case it is generated either by a  $(p-2)$ -cycle or by a product of a transposition and a disjoint  $(p-2)$ -cycle.

*Proof.* (1) We fix a  $p$ -adic prime  $\wp$  of  $N$ . Let  $\mathfrak{p} = \wp \cap K$ . We denote by  $N_\wp$  the completion of  $N$  at  $\wp$  and by  $K_{\mathfrak{p}}$  the closure of  $K$  in  $N_\wp$ . By Lemma 2.3, we know that  $p = \mathfrak{p}^p$ .

We let  $\mathcal{D}(M/N)$  be the different of a local extension  $M/N$ . By the transitivity of the different, we have

$$\mathcal{D}(N_\wp/\mathbb{Q}_p) = \mathcal{D}(N_\wp/K_{\mathfrak{p}}) \cdot \mathcal{D}(K_{\mathfrak{p}}/\mathbb{Q}_p).$$

The discriminant of the polynomial  $\psi(X)$  is given by

$$D(\psi) = (-1)^{(p-1)/2} b^{s-1} [p^p b^{p-s} + s^s (p-s)^{p-s} b^p p^{ksp}],$$

so the  $p$ -adic valuation of  $D(\psi)$  is equal to  $p$  except when  $k = s = 1$  and  $b \equiv -1 \pmod{p}$ .

We first treat the case where  $v_p(D(\psi)) = p$ . Since  $p$  is wildly ramified in  $K$  by Lemma 2.3, so is the  $p$ -adic valuation of the discriminant of  $K$ :  $v_p(D_K) = p$ . Thus we also have  $v_p(\mathcal{D}(K_{\mathfrak{p}}/\mathbb{Q}_p)) = p$  and

$$\mathcal{D}(K_{\mathfrak{p}}/\mathbb{Q}_p) = (\wp^{e/p})^p = \wp^e$$

where the integer  $e$  is the ramification index of the extension  $N_\wp/\mathbb{Q}_p$ . On the other hand, since  $N_\wp/K_{\mathfrak{p}}$  is tamely ramified,

$$\mathcal{D}(N_\wp/K_{\mathfrak{p}}) = \wp^{e/p-1}.$$

Now let  $(G_i)_{i \geq 0}$  denote the ramification groups of the Galois extension  $N_\wp/\mathbb{Q}_p$ . We then have [14, chapitre IV, §2]

$$\mathcal{D}(N_\wp/\mathbb{Q}_p) = \wp^{\sum_{i \geq 0} (\text{Card}(G_i) - 1)} = \wp^{e-1+\lambda(p-1)}$$

where  $G_\lambda$  is the last non-trivial ramification group.

Taking all these equalities into account, we obtain  $e = \lambda p(p-1)$ . As any maximal solvable transitive permutation group of degree  $p$  is isomorphic to  $\text{Aff}(\mathbb{F}_p)$ , we necessarily have  $\lambda = 1$  and  $e = p(p-1)$ .

Suppose now that  $k = s = 1$  and  $b \equiv -1 \pmod{p}$ . Then

$$\psi(X) = \frac{\varphi(pX)}{p^p} = X^p + bpX + b.$$

Let  $\beta = \alpha/p$  be a root of  $\psi(X)$ . As noticed in the proof of Lemma 2.3, the polynomial  $\psi(X - b)$  is Eisenstein with respect to the prime  $p$ : in particular its root  $\beta + b$  is a prime element of the local field  $K_{\mathfrak{p}} = \mathbb{Q}_p(\alpha)$ . Since  $p$  divides  $b + 1$ , the same holds for  $\beta - 1 = (\beta + b) - (b + 1)$ . Now if we rewrite

the equality  $\psi(\beta) = 0$  as

$$\beta^{p-1} + b = \frac{b}{\beta} [(\beta - 1) - p\beta],$$

we see that ( $\beta$  being a unit of  $K_{\mathfrak{p}}$  since its norm  $b$  is a unit of  $\mathbb{Q}_p$ )

$$v_{\mathfrak{p}}(\beta^{p-1} + b) = 1.$$

So the  $(K_{\mathfrak{p}}, X - \beta)$ -polygon [4] of

$$\frac{\psi(X)}{X - \beta} = (X - \beta)^{p-1} + p\beta(X - \beta)^{p-2} + \dots + \frac{p(p-1)}{2}\beta^{p-2}(X - \beta) + p(\beta^{p-1} + b)$$

has a unique side  $S$  joining  $(0, 0)$  to  $(p-1, p+1)$ . As the associated polynomial of  $S$  is a binomial of degree  $2 = \gcd(p-1, p+1)$ , it is separable modulo  $p$ . Accordingly, by [4, Theorem 1.5], the ramification index of  $\mathbb{Q}_p(\alpha, \alpha_2)/\mathbb{Q}_p(\alpha)$  is  $(p-1)/2$ . Since  $\varphi$  remains irreducible over  $\mathbb{Q}_p$ , the decomposition group of  $p$  in  $N/\mathbb{Q}$  is a subgroup of  $\text{Aff}(\mathbb{F}_p)$ . As a non-trivial element of  $\text{Aff}(\mathbb{F}_p)$  does not fix two points [1, §15], we have  $N_{\varphi} = \mathbb{Q}_p(\alpha, \alpha_2)$ . Hence the inertia group of  $p$  in  $N/\mathbb{Q}$  is of order  $p(p-1)/2$ . It is therefore isomorphic to the unique subgroup of  $\text{Aff}(\mathbb{F}_p)$  of index 2.

(2) By Lemma 2.4, the ramification of  $p$  in  $K/\mathbb{Q}$  is tame, more precisely,  $p = \mathfrak{p}^{p-1}\mathfrak{p}'$  or  $p = \mathfrak{p}^{p-2}\mathfrak{a}$ . Thus the ramification of  $p$  in  $N/\mathbb{Q}$  is tame, so that the inertia group is cyclic. This decomposition of  $p$  corresponds to a factorization of the polynomial  $\varphi(X)$  over  $\mathbb{Q}_p$ :

$$\varphi(X) = g(X)h(X)$$

with  $g(X)$  being irreducible over  $\mathbb{Q}_p$  of degree  $\deg g = p-1$  in the first case and  $\deg g = p-2$  in the second. The first case occurs precisely when (i) or (ii) of Lemma 2.4 holds. The local field  $K_{\mathfrak{p}}$  is obtained by adjoining a root of  $g(X)$  to  $\mathbb{Q}_p$ ; it is a totally ramified extension of  $\mathbb{Q}_p$ . Write  $I_{\varphi}$  for the inertia group of  $\varphi|_{\mathfrak{p}}$  in  $N/\mathbb{Q}$ . Introduce the inertia field  $M$  in  $N_{\varphi}/\mathbb{Q}_p$ . The totally ramified extension  $K_{\mathfrak{p}}/\mathbb{Q}_p$  is linearly disjoint from the unramified extension  $M/\mathbb{Q}_p$ , so  $g(X)$  remains irreducible over  $M$ . Hence  $I_{\varphi} = G(N_{\varphi}/M)$  acts transitively on the roots of  $g(X)$ . As  $I_{\varphi}$  is cyclic, it contains a cycle of order  $p-1$  or  $p-2$  according to the degree of  $g(X)$ .

Now if  $\deg g = p-1$ , and  $\alpha'$  is another root of  $\varphi(X)$ , the ramification index of  $\mathbb{Q}_p(\alpha')/\mathbb{Q}_p$  is  $p-1$  or 1, according to whether  $\alpha'$  is a root of  $g(X)$  or  $h(X)$ . By Abhyankar's lemma [13, p. 236], the extension  $N_{\varphi}/K_{\mathfrak{p}}$  is unramified, so in this case  $I_{\varphi}$  is cyclic generated by a  $(p-1)$ -cycle.

If instead  $\deg g = p-2$ , consider a root  $\alpha'$  of  $h(X)$ . If  $\mathbb{Q}_p(\alpha')/\mathbb{Q}_p$  is unramified, arguing as in the preceding case we see that  $I_{\varphi}$  is cyclic generated by a  $(p-2)$ -cycle. If  $\mathbb{Q}_p(\alpha')/\mathbb{Q}_p$  is ramified, then its ramification index is  $2 = \deg h(X)$ , in particular the quadratic polynomial  $h(X)$  is irreducible over  $\mathbb{Q}_p$  (hence also over the inertia field  $M$ ). In this last case, again by

Abhyankar's lemma, the ramification index of  $N_\varphi/\mathbb{Q}_p$  is  $2(p-2)$ . As  $I_\varphi$  also acts transitively on the roots of  $h(X)$ , we conclude that it is generated by a product of a transposition and a disjoint  $(p-2)$ -cycle. ■

**2.2. Inertia at non- $p$ -adic primes.** Let  $\ell \neq p$  be a prime divisor of  $a$ .

LEMMA 2.6.

1. If  $p$  does not divide  $v_\ell(a)$ , then the prime number  $\ell$  is totally ramified in  $K = \mathbb{Q}(\alpha)$ .
2. If  $p$  divides  $v_\ell(a)$ , then  $\ell$  is unramified in  $K = \mathbb{Q}(\alpha)$ .

*Proof.* The  $(\mathbb{Q}_\ell, X)$ -polygon [4] of  $\varphi(X)$  has a unique side  $S$  joining  $(0, 0)$  to  $(p, v_\ell(a))$ . The associated polynomial of  $S$  is a binomial of the form

$$F(Y) = Y^m + \frac{a}{\ell^{v_\ell(a)}}$$

where  $m = p$  or  $1$ , according to whether  $p$  divides  $v_\ell(a)$  or not. Furthermore,  $F(Y)$  is separable modulo  $\ell$ . Thus, by [4, Theorem 1.5], the ramification index of  $\mathbb{Q}_\ell(\alpha)/\mathbb{Q}_\ell$  is equal to  $p/m$ . ■

This lemma together with Abhyankar's lemma immediately yields:

PROPOSITION 2.7. *Let  $\ell \neq p$  be a prime divisor of  $a$ . The inertia group (defined up to conjugation) of  $\ell$  in  $N/\mathbb{Q}$  is trivial or cyclic of order  $p$  according to whether  $p$  divides  $v_\ell(a)$  or not.*

Let  $\ell \neq p$  be a prime divisor of the number  $D_0$  given by (2).

PROPOSITION 2.8. *The prime  $\ell \mid D_0$  ( $\ell \neq p$ ) is ramified in  $K$  precisely when  $v_\ell(D_0)$  is odd, in which case the corresponding inertia group is generated by a transposition.*

*Proof.* Since  $\ell$  does not divide  $a$ , by [10, Theorem 2] the  $\ell$ -adic valuation of the absolute discriminant of  $K = \mathbb{Q}(\alpha)$  is either 0 or 1 according to the parity of the  $\ell$ -adic valuation of  $D_0$ . The rest of the proof is similar to that of Lemma 5 of [12]. ■

**3. Galois group.** It is known that every transitive solvable permutation group of prime degree  $p$  is isomorphic to a subgroup of the affine group  $\text{Aff}(\mathbb{F}_p)$ . Suppose that the Galois group  $G$  of the irreducible trinomial  $\varphi(X) = X^p + aX^s + a$  is solvable. Then, in view of Propositions 2.2 and 2.5,  $G$  is either  $\text{Aff}(\mathbb{F}_p)$  or its unique subgroup of index 2, except possibly when we simultaneously have  $(p-1, sv_p(a)) > 1$  and  $sv_p(a) < p$ .

Using the classification of finite simple groups, W. Feit [7, Section 4] drew up the list of possible non-solvable Galois groups of prime degree trinomials over  $\mathbb{Q}$ :

1. the projective linear group  $\mathrm{PSL}_3(2)$  of degree 7;
2. the groups  $\mathrm{PSL}_2(11)$  or  $M_{11}$  (Mathieu group) of degree 11;
3. the projective linear groups  $G$  between  $\mathrm{PSL}_2(2^e)$  and  $\mathrm{P}\Gamma\mathrm{L}_2(2^e)$  of degree  $p = 1 + 2^e > 5$ ;
4. the symmetric group  $S_p$  or the alternating group  $A_p$ .

When  $p = 7$ , by (1) and (2), the discriminant  $D$  of  $\varphi(X)$  is

$$D = -a^6[7^7 + (7 - s)^{7-s}s^s a^s].$$

For  $s \in \{1, 3, 4, 6\}$ ,  $D/a^6 \equiv -1 \pmod{3}$ , while for  $s = 2$  or  $s = 5$ ,  $D/a^6 \equiv 2 \pmod{5}$ , so that  $D$  is never a square. Hence the first case above does not hold.

Similarly when  $p = 11$ , we are going to check that

$$D = -a^{10}[11^{11} + (11 - s)^{11-s}s^s a^s]$$

is not a square. First observe that  $D/a^{10}$  is not a square modulo 8, except when  $s = 2$  or  $s = 9$ . When  $s = 2$ , the discriminant is not a square since it is negative. When  $s = 9$ , assume that  $D$  is a square: there exists an integer  $y$  such that  $y^2 = -11^{11} - 4 \cdot 9^9 a^9$ . Setting  $x := (-9a)^3$ , this would imply that the elliptic curve  $(E)$  of equation

$$y^2 = 4x^3 - 11^{11}$$

has a rational non-trivial point. By the change of coordinates defined by  $y = 2 \cdot 11^3 Y + 11^3$  and  $x = 11^2 X$ , one sees that  $(E)$  is isomorphic to the elliptic curve  $(E')$  defined by the equation

$$Y^2 + Y = X^3 - 40263,$$

which is the curve 1089b1 in Cremona's tables of elliptic curves [5]. In particular, it is of conductor 1089. By Table One of [5],  $(E')$  has rational rank 0 and trivial torsion. So there is no non-trivial rational point in  $(E')$ , hence none in  $(E)$ . This completes the proof.

Therefore when the Galois group  $G$  is not solvable, either it contains  $A_p$  or we have  $\mathrm{PSL}_2(2^e) \leq G \leq \mathrm{P}\Gamma\mathrm{L}_2(2^e)$ . Of course the latter happens in the very special case where  $p$  is a Fermat prime  $p = 1 + 2^e$  with  $e > 2$ . Further, since the projective semilinear group  $\mathrm{P}\Gamma\mathrm{L}_2(2^e)$  consists of even permutations [3, Lemma 3.1] the last case does not occur when  $D$  is not a square.

The above discussion immediately yields the following result.

**PROPOSITION 3.1.** *If the Galois group  $G$  of  $\varphi(X) = X^p + aX^s + a$  is not solvable, then it is the full symmetric group  $S_p$  as soon as one of the following conditions holds:*

- (i)  $sv_p(a) > p$ ;
- (ii)  $sv_p(a) < p$  and  $sv_p(a)$  is odd.



*Proof.* In both cases,  $v_p(D)$  is odd. ■

**THEOREM 3.2.** *Let  $a$  be an integer, and  $p$  a prime number not dividing  $a$ . Let  $\varphi(X) = X^p + aX^s + a$  be irreducible over  $\mathbb{Q}$  and  $G$  its Galois group over  $\mathbb{Q}$ . Then*

- (i)  $G \simeq S_p$  if the discriminant of  $\varphi(X)$  is not a square;
- (ii)  $G \simeq A_p$  or  $\mathrm{PSL}_2(2^e)$  if the discriminant of  $\varphi(X)$  is a square. The latter is only possible when  $p$  is a Fermat prime.

*Proof.* We can assume that  $p > 3$ . Suppose that  $G$  is not isomorphic to  $S_p$ . By Proposition 2.8, the number  $D_0 = p^p + (p-s)^{p-s} s^s a^s$  given by (2) is a square and only the prime divisors of  $a$  may ramify in  $K = \mathbb{Q}(\alpha)$ . The inertia group of such a ramified prime  $\ell \mid a$  in  $N/\mathbb{Q}$  is cyclic of order  $p$  (Proposition 2.7). Hence  $G$  is generated by elements of order  $p$ . On the other hand, the extension  $K/\mathbb{Q}$  is not normal since the trinomial  $\varphi(X)$  has at most three real roots. Therefore  $G$  is not solvable. As all the elements of order  $p$  of  $\mathrm{P}\Gamma\mathrm{L}_2(2^e)$  lie in  $\mathrm{PSL}_2(2^e)$ , the proof is complete. ■

We keep the notations already introduced. Combining the above Proposition 3.1 with Proposition 2.2, we obtain:

**THEOREM 3.3.** *Let  $a$  be an integer such that  $p \mid a$  and  $p$  does not divide  $v_p(a)$ . Further assume that  $\gcd(p-1, sv_p(a)) = 1$  if  $sv_p(a) < p$ . Then the Galois group  $G$  of  $\varphi(X)$  is either  $S_p$  or  $\mathrm{Aff}(\mathbb{F}_p)$ .*

There remains the case where  $v_p(a) = kp$  with an integer  $k \geq 1$ . Let  $p = 1 + 2^e > 17$  be a Fermat prime. We first notice that  $\mathrm{P}\Gamma\mathrm{L}_2(2^e)$  does not contain any subgroup isomorphic to the subgroup of index 2 of  $\mathrm{Aff}(\mathbb{F}_p)$ . In fact, the latter contains an element of order  $(p-1)/2$ , and this is not even the case of the semilinear group  $\Gamma\mathrm{L}_2(2^e)$ . Let, indeed,  $u$  be a semilinear transformation of the vector space  $\mathbb{F}_{2^e}^2$  relative to an automorphism  $\sigma$  of  $\mathbb{F}_{2^e}$  and suppose that  $u$  is of order  $(p-1)/2 = 2^{e-1}$ . Since  $\sigma^e$  is the identity of  $\mathbb{F}_{2^e}$ , we see that  $u^e$  is a linear map. On the other hand, the general linear group  $\mathrm{GL}_2(2^e)$  being of order

$$(2^{2e} - 1)(2^{2e} - 2^e),$$

its 2-Sylow subgroups are of order  $2^e$ . Considering the subgroup

$$\left\{ \left( \begin{array}{cc} 1 & \lambda \\ 0 & 1 \end{array} \right) : \lambda \in \mathbb{F}_{2^e} \right\},$$

we see that these 2-Sylow subgroups are elementary abelian. Consequently,  $u^{2^e} = \mathrm{Id}_{\mathbb{F}_{2^e}^2}$ , and  $2^{e-1}$  divides  $2e$ . This contradicts the inequality  $2^e > 16$ . Now the above discussion together with Proposition 2.5 yields:

**THEOREM 3.4.** *Let  $p \neq 17$  be a prime number and  $a$  be an integer such that  $v_p(a) = kp$  for an integer  $k \geq 1$ . Assume that the trinomial  $\varphi(X) = X^p + aX^s + a$  is irreducible over  $\mathbb{Q}$  and denote by  $G$  its Galois group over  $\mathbb{Q}$ . Then*

- (i)  $G$  is  $\text{Aff}(\mathbb{F}_p)$  or  $S_p$  if the discriminant of  $\varphi(X)$  is not a square;
- (ii)  $G \simeq A_p$  or the subgroup of index 2 of  $\text{Aff}(\mathbb{F}_p)$  if the discriminant of  $\varphi(X)$  is a square.

Notice that the discriminant of  $\varphi(X)$  in the above theorem can be a square only when we simultaneously have  $ks = 1$  and  $b := a/p^{kp} \equiv -1 \pmod{p}$ . Further, by Proposition 2.5 the hypothesis  $p \neq 17$  can be removed when either  $ks > 1$  or  $b \not\equiv -1 \pmod{17}$ . Finally, observe that once we fix the prime  $p$ , then for only finitely many integers  $a$  can the above Galois group  $G$  be contained in  $\text{Aff}(\mathbb{F}_p)$  [2].

## 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] S. D. Cohen, A. Movahhedi and A. Salinier, *Galois groups of trinomials*, J. Algebra 222 (1999), 561–573.
- [4] —, —, —, *Factorization over local fields and the irreducibility of generalized difference polynomials*, Mathematika 47 (2000), 173–196.
- [5] J. E. Cremona, *Elliptic Curve Data*, <http://www.maths.nott.ac.uk/personal/jec/ftp/data/>, Univ. of Nottingham, updated 2006-09-24 (with minor corrections on 2006-12-15, 2007-01-05).
- [6] J. D. Dixon and B. Mortimer, *Permutation Groups*, Grad. Texts in Math. 163, Springer, 1996.
- [7] W. Feit, *Some consequences of the classification of finite simple groups*, in: Proc. Sympos. Pure Math. 37, Amer. Math. Soc., 1980, 175–181.
- [8] K. Komatsu, *On the Galois group of  $x^p + ax + a = 0$* , Tokyo J. Math. 14 (1991), 227–229.
- [9] —, *On the Galois group of  $x^p + p^t b(x + 1) = 0$* , *ibid.* 15 (1992), 351–356.
- [10] P. Llorente, E. Nart and N. Vila, *Discriminants of number fields defined by trinomials*, Acta Arith. 43 (1984), 367–373.
- [11] A. Movahhedi, *Galois group of  $X^p + aX + a$* , J. Algebra 180 (1996), 966–975.
- [12] A. Movahhedi and A. Salinier, *The primitivity of the Galois group of a trinomial*, J. London Math. Soc. (2) 53 (1996), 433–440.
- [13] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 2nd ed., Springer, Berlin, and PWN-Polish Sci. Publ., Warszawa 1990.
- [14] J.-P. Serre, *Corps locaux*, Act. Sci. Indust. 1296, Hermann, Paris, 1962.

- [15] R. G. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math. 12 (1962), 1099–1106.

XLIM UMR 6172 CNRS  
Mathématiques et Informatique  
Université de Limoges  
123 Avenue Albert Thomas  
87060 Limoges Cedex, France  
E-mail: bensebaboua@yahoo.fr  
abbas.movahhedi@unilim.fr  
alain.salinier@unilim.fr

*Received on 7.9.2007  
and in revised form on 16.11.2007*

(5516)