Glasgow Math. J. **63** (2021) 106–120. © The Author(s) 2020. Published by Cambridge University Press on behalf of Glasgow Mathematical Journal Trust.
doi:10.1017/S001708952000004X.

WILD RAMIFICATION IN TRINOMIAL EXTENSIONS AND GALOIS GROUPS

BOUALEM BENSEBAA
Laboratoire LA3C, Faculté de Mathématiques, USTHB, Bab Ezzouar 16111, Algeria
e-mail: b.benseba@usthb.dz

ABBAS MOVAHHEDI and ALAIN SALINIER
XLIM (UMR 7252 CNRS, Université de Limoges), 87060 Limoges Cedex, France
e-mails: abbas.movahhedi@unilim.fr, alain.salinier@unilim.fr

(Received 21 October 2019; revised 27 January 2020, accepted 30 January 2020; first published online 12 March 2020)

Abstract. It is proven that, for a wide range of integers s ($2 < s < p-2$), the existence of a single wildly ramified odd prime $\ell \neq p$ leads to either the alternating group or the full symmetric group as Galois group of any irreducible trinomial $X^p + aX^s + b$ of prime degree p.

2010 *Mathematics Subject Classification*. Primary 11R32, 12F10; Secondary 11S15, 12E10.

1. Introduction. Let $f(X) = X^p + aX^s + b$ be a trinomial of prime degree p, with integral coefficients, and N the splitting field of $f(X)$ over the field $\mathbb{Q}$ of rational numbers. When $a = b$, the prime p is the only prime which can be wildly ramified in the extension $N/\mathbb{Q}$. This fact means in particular that inertia groups at other places $\ell \neq p$ are cyclic and so makes it easier to determine the Galois group of $f(X)$. It is therefore of interest to elucidate whether other wild ramifications can occur in more general circumstances and how this kind of information can be used in order to find the Galois group of $f(X)$. This is the main goal of this paper.

So we are driven to analyse the inertia groups of all the primes which ramify in N. To get precise information concerning the prime p, we suppose that p does not divide the p-adic valuation $v_p(b)$ of the constant term b of our trinomial. We are able to entirely determine the inertia group (even the decomposition group in the case of wild ramification) at p and also the inertia groups at almost all other primes. The only exceptions are the primes dividing $s(p-s)$. Hence, only the primes dividing $ps(p-s)$ can be wildly ramified. This study completes our previous results [**2**] in the case $a = b$. Complementing earlier work of Plans and Vila [**23**], we also give a condition which suffices to ensure wild ramification at a prime $\ell \neq p$ (Proposition 2.8).

Let us note that the determination of the Galois group of an irreducible trinomial with integral coefficients $X^n + aX^s + b$ is far from being entirely established, even though it has been studied since at least the beginning of the twentieth century, as testified by the paper [**16**]. From the seventies on, many authors renewed interest in the topic (see, e.g., [**14**, **22**, **27**]). In the special case of prime degree $n = p$ and $s = 1$, it is conjectured [**5**, **13**] that the Galois group of the Eisenstein trinomial $X^p + aX + a$ is always the full symmetric group, if p divides a exactly once. To date, this is only known for $p \leq 5$ [**11**] . Special cases

https://doi.org/10.1017/S001708952000004X Published online by Cambridge University Press

were known, such as the case where a/p is a perfect square integer [**15**]. In fact, if the prime p divides the integer a exactly once, the Galois group G of the trinomial $X^p + aX + a$ is isomorphic to either S_p or to the affine group $\mathrm{Aff}(\mathbb{F}_p)$ [**19**, Theorem 3.1]. The latter occurs precisely when the splitting field of $f(X)$ contains the p-th roots of unity [**19**, Theorem 2.2]. More generally, if $\gcd(p-1, s) = 1$, then the Galois group of an Eisenstein (with respect to p) trinomial $X^p + aX^s + a$ is once again isomorphic to either S_p or $\mathrm{Aff}(\mathbb{F}_p)$ [**2**, Theorem 3.3]. We stress that the knowledge of inertia and decomposition groups of primes ramified in the splitting field of a trinomial, as determined in this paper, narrows accordingly the area which can be searched for possible examples of Eisenstein-type trinomials with affine group as Galois group.

Our paper is organised as follows.

Section 2 is devoted to the detailed analysis of different inertia groups of the primes ramified in N. Our method is based on Newton polygons which turn out to be efficient for the study of factorisations of polynomials over a local field. We distinguish three kinds of ramification of a prime ℓ according to the sign of the integer $pv_\ell(a) - (p-s)v_\ell(b)$, giving rise to three different types of polygons for $f(X)$. For a prime ℓ such that $pv_\ell(a) - (p-s)v_\ell(b) = 0$ which is ramified in N, its inertia group is generated by a transposition. As far as the prime p is concerned, it is wildly ramified in N if and only if the integer $pv_p(a) - (p-s)v_p(b)$ is positive.

In Section 3, we show how the precise local study in Section 2 can be used for the determination of the Galois group G. This is done with the help of Feit's list of degree p permutation groups that can arise as the Galois group of a degree p trinomial [**10**, Section 4]. We pay special attention to the possibility of wild ramification and prove the following:

THEOREM (Theorem 3.13). *Let p be a prime number and $f(X) = X^p + aX^s + b$ a trinomial of degree p with integer coefficients. If $2 < s < p-2$, the existence of a single wildly ramified odd prime $\ell \neq p$ leads to either the alternating group or the full symmetric group as Galois group of $f(X)$ over $\mathbb{Q}$.*

2. Local study. Let p be an odd prime number, $f(X) = X^p + aX^s + b$ be an irreducible trinomial with a and b two non-zero rational integers, and $1 \leq s \leq p-1$ be a natural number. Denote by $\theta := \theta_1, \theta_2, \ldots, \theta_p$ the different roots of f in an algebraic closure of $\mathbb{Q}$. Let $K := \mathbb{Q}(\theta)$ be the field obtained by adjoining the root θ to the field $\mathbb{Q}$ and $N := \mathbb{Q}(\theta, \theta_2, \ldots, \theta_p)$ be the normal closure of K over $\mathbb{Q}$.

2.1. Local study at a finite prime. Let ℓ be a prime number. In order to get information about the inertia at ℓ, we consider the $(\mathbb{Q}_\ell, X)$-polygon [**8**] of $f(X)$. We are driven to analyse three cases depending on the sign of $(p-s)v_\ell(b) - pv_\ell(a)$, where v_ℓ denotes the ℓ-adic valuation. We use the notations $a_\ell := \frac{a}{\ell^{v_\ell(a)}}$ and $b_\ell := \frac{b}{\ell^{v_\ell(b)}}$.

2.1.1. The case $(p-s)v_\ell(b) < pv_\ell(a)$

In this case, we have two different possible behaviours for the ramification depending on whether the two prime numbers ℓ and p are equal or not. If $\ell \neq p$, the extension $K/\mathbb{Q}$ is indeed tamely ramified at ℓ, as we are going to see.

PROPOSITION 2.1. *Let $\ell \neq p$ be a prime number such that $(p-s)v_\ell(b) < pv_\ell(a)$.*

(i) *If p divides $v_\ell(b)$, then the prime number ℓ is unramified in $N/\mathbb{Q}$.*
(ii) *If p does not divide $v_\ell(b)$, then the prime number ℓ ramifies in $N/\mathbb{Q}$ and the inertia group of an ℓ-adic place of N is cyclic of order p.*

https://doi.org/10.1017/S001708952000004X Published online by Cambridge University Press

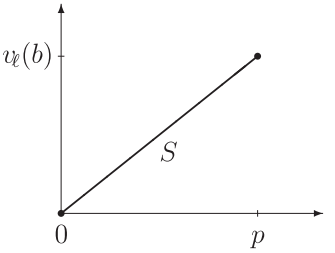


Figure 1. The $(\mathbb{Q}_\ell, X)$-polygon of $f(X)$ when $(p-s)v_\ell(b) < pv_\ell(a)$.

Proof. Under the condition $(p-s)v_\ell(b) < pv_\ell(a)$, the $(\mathbb{Q}_\ell, X)$-polygon of $f(X)$ has a unique side S joining $(0, 0)$ to $(p, v_\ell(b))$ as illustrated in Figure 1. The associated polynomial of the side S is a binomial of the form

$$F(Y) = Y^m + b_\ell,$$

where $m = p$ or 1, depending on whether p divides $v_\ell(b)$ or not. Since $F(Y)$ is separable modulo ℓ, by [**8**, Theorem 1.5], the ramification index of the local extension $\mathbb{Q}_\ell(\theta)/\mathbb{Q}_\ell$ is equal to p/m, an integer coprime to ℓ. So the extension $K/\mathbb{Q}$ is tamely ramified at ℓ if p does not divide $v_\ell(b)$, and otherwise unramified at ℓ. By Abhyankar's Lemma [**21**, p. 236], the extension $\mathbb{Q}_\ell(\theta, \theta_2, \ldots, \theta_p)/\mathbb{Q}_\ell(\theta)$ is unramified so, in this case, the inertia group is either trivial or cyclic of order p depending on whether p divides $v_\ell(b)$ or not. □

In the more intricate case $\ell = p$, we assume that p does not divide $v_p(b)$, so that, as in Proposition 2.1(ii), the prime number p is totally ramified in $K = \mathbb{Q}(\theta)$. The slope of the unique side of the $(\mathbb{Q}_p, X)$-polygon of $f(X)$ is equal to $\frac{v_p(b)}{p}$. Therefore $\pi := \frac{\theta^\alpha}{p^\beta}$ is a prime element of the completion $\mathbb{Q}_p(\theta)$ of K with respect to its p-adic place, where $\alpha \in [1, p-1]$ and $\beta \in [0, v_p(b)]$ are integers defined via the Bézout identity $\alpha v_p(b) - \beta p = 1$. Moreover, we have

$$\frac{\theta^p}{p^{v_p(b)}} = \frac{-a_p p^{v_p(a)}\theta^s - b_p p^{v_p(b)}}{p^{v_p(b)}} = -a_p p^{v_p(a)-v_p(b)}\theta^s - b_p\,.$$

As the π-adic valuation of $p^{v_p(a)-v_p(b)}\theta^s$ is $p(v_p(a) - v_p(b)) + sv_p(b) > 0$, this proves that $\frac{\theta^p}{p^{v_p(b)}}$ is a unit of the local field $\mathbb{Q}_p(\theta)$, with

$$\frac{\theta^p}{p^{v_p(b)}} \equiv -b_p \pmod{\pi}\,. \tag{2.1}$$

Hence $\pi^{v_p(b)} = \frac{\theta^{\alpha v_p(b)}}{p^{\beta v_p(b)}} = \theta\left(\frac{\theta^p}{p^{v_p(b)}}\right)^\beta$, so that we get from (2.1)

$$\theta \equiv \pi^{v_p(b)}(-b_p)^{-\beta} \pmod{\pi^{v_p(b)+1}}\,. \tag{2.2}$$

Similarly $\pi^p = \frac{\theta^{\alpha p}}{p^{\beta p}} = p\left(\frac{\theta^p}{p^{v_p(b)}}\right)^\alpha$ and so, once again by (2.1)

$$p \equiv \pi^p(-b_p)^{-\alpha} \pmod{\pi^{p+1}}\,. \tag{2.3}$$

We will now determine the inertia and the decomposition groups of a p-adic place $\wp$ of N. We recall our notations $a_p = \frac{a}{p^{v_p(a)}}$ and $b_p = \frac{b}{p^{v_p(b)}}$.

https://doi.org/10.1017/S001708952000004X Published online by Cambridge University Press

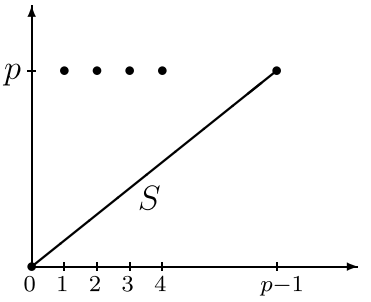


Figure 2. The $(\mathbb{Q}_p(\theta), X)$-polygon of $g(X)$ when $pv_p(a) - (p-s)v_p(b) > p$.

PROPOSITION 2.2. *Assume that $pv_p(a) > (p-s)v_p(b)$ and that p does not divide $v_p(b)$. The inertia group of a prime $\wp$ of N above p in $N/\mathbb{Q}$ is isomorphic to:*

- *the affine group* $\mathrm{Aff}(\mathbb{F}_p)$, *if* $pv_p(a) - (p-s)v_p(b) > p$,
- *the subgroup of the affine group of index* $\gcd(p-1, v_p(ab^{s-1}))$, *if* $0 < pv_p(a) - (p-s)v_p(b) < p$.

The decomposition group of $\wp$ is isomorphic to:

- $\mathrm{Aff}(\mathbb{F}_p)$, *if* $pv_p(a) - (p-s)v_p(b) > p$,
- *the subgroup of* $\mathrm{Aff}(\mathbb{F}_p)$ *of order* $\frac{p(p-1)r}{\gcd(p-1, v_p(ab^{s-1}))}$, *if* $0 < pv_p(a) - (p-s)v_p(b) < p$, *where r is the order of the class of* $(-1)^s s a_p b_p^{s-1}$ *in the factor group* $\mathbb{F}_p^*/\mathbb{F}_p^{*v_p(ab^{s-1})}$.

Proof. Consider the polynomial

$$g(X) = \frac{f(\theta(X+1))}{\theta^p X} = X^{p-1} + \sum_{i=1}^{p-1} c_i X^{p-1-i},$$

in $\mathbb{Q}(\theta)[X]$, where the coefficient c_i is given by

$$c_i = \begin{cases} \binom{p}{i} & \text{if } 1 \le i \le p-s-1 \\ \binom{p}{i} + \binom{s}{i+s-p}\frac{a}{\theta^{p-s}} & \text{if } p-s \le i \le p-1. \end{cases}$$

The π-adic valuations $v_\pi(c_i)$ of the coefficients c_i are given by

$$v_\pi(c_i) = \begin{cases} p & \text{if } 1 \le i \le p-s-1 \\ \min(p, pv_p(a) - (p-s)v_p(b)) & \text{if } p-s \le i \le p-1 \end{cases},$$

since $v_\pi(\theta) = v_p(b)$ and $v_\pi(x) = pv_p(x)$ for any rational x. So, the $(\mathbb{Q}_p(\theta), X)$-polygon [**8**] of $g(X)$ has a unique side S joining the point $(0, 0)$ to the point $(p-1, \min(p, pv_p(a) - (p-s)v_p(b))$.

If $pv_p(a) - (p-s)v_p(b) > p$, then S joins $(0, 0)$ to $(p-1, p)$ as in Figure 2; hence, as the integers $p-1$ and p are coprime, by [**8**, Theorem 1.5] we see that the ramification index of the local extension $\mathbb{Q}_p(\theta, \theta_2)/\mathbb{Q}_p(\theta)$ is equal to $p-1$. Thus, the extension $\mathbb{Q}_p(\theta, \theta_2)/\mathbb{Q}_p$ is totally ramified of degree $p(p-1)$. Moreover, the inertia group of $\wp$ in the extension $N/\mathbb{Q}$ being a transitive solvable permutation group of prime degree p, it is necessarily isomorphic to the affine group $\mathrm{Aff}(\mathbb{F}_p)$. This is also the case for the decomposition group.

https://doi.org/10.1017/S001708952000004X Published online by Cambridge University Press

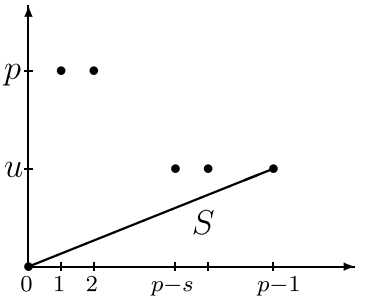


Figure 3. The $(\mathbb{Q}_p(\theta), X)$-polygon of $g(X)$ when $pv_p(a) - (p-s)v_p(b) < p$.

In the case where $u := pv_p(a) - (p-s)v_p(b) < p$, the side S joins $(0, 0)$ to $(p-1, u)$ as in Figure 3; by [**8**, Theorem 1.5, (i)] the ramification index of the local extension $\mathbb{Q}_p(\theta, \theta_2)/\mathbb{Q}_p(\theta)$ is divisible by $(p-1)/\gcd(p-1, u)$. The unique side S of the $(\mathbb{Q}_p(\theta), X)$-polygon contains as only points of the form $(i, v_\pi(c_i))$ the two points $(0, 0)$ and $(p-1, u)$. Therefore, to compute the associated polynomial $F(Y)$ [**8**, Definition 1.4] of the side S, we only need to consider the leading term X^{p-1} and the constant coefficient

$$c_{p-1} = \pi^u \left(\frac{p}{\pi^u} + \frac{as\theta^s}{\theta^p \pi^u} \right) = \pi^u \left(\frac{p}{\pi^u} - \frac{as}{b\pi^u \theta^{-s} + a\pi^u} \right)$$

$$= \pi^u \left(\frac{p}{\pi^u} - \frac{a_p s}{b_p \pi^u p^{v_p(b)-v_p(a)} \theta^{-s} + a_p \pi^u} \right),$$

of the polynomial $g(X)$. Thus,

$$F(Y) = Y^\epsilon - \left(\frac{a_p s}{b_p \pi^u p^{v_p(b)-v_p(a)} \theta^{-s} + a_p \pi^u} - \frac{p}{\pi^u} \right),$$

with $\epsilon = \gcd(p-1, u) = \gcd(p-1, v_p(ab^{s-1}))$.

We have by (2.2) and (2.3) the congruence

$$\pi^u p^{v_p(b)-v_p(a)} \theta^{-s} \equiv (-b_p)^{\alpha(v_p(a)-v_p(b))+\beta s} \pmod{\pi}.$$

As $v_\pi\left(\frac{p}{\pi^u}\right) = p - u > 0$, and $v_\pi(a_p \pi^u) = u > 0$, we have verified the congruence

$$F(Y) \equiv Y^\epsilon + s a_p (-b_p)^{-\alpha v_p(a)+\alpha v_p(\beta)-\beta s-1} \bmod \pi \mathbb{Z}_p[\pi][Y].$$

As ϵ divides $p-1$, we see that the associated polynomial $F(Y)$ is separable modulo p. From [**8**, Theorem 1.5, (ii)], we conclude that the ramification index of the local extension $\mathbb{Q}_p(\theta, \theta_2)/\mathbb{Q}_p(\theta)$ is precisely $(p-1)/\epsilon$. Since every finite extension of the local field $\mathbb{Q}_p$ is solvable, and as $f(X)$ is irreducible over $\mathbb{Q}_p$, the decomposition group of $\wp$ in the extension $N/\mathbb{Q}$ is a transitive solvable group of degree p, hence isomorphic to a subgroup of $\mathrm{Aff}(\mathbb{F}_p)$. As the identity is the only permutation in $\mathrm{Aff}(\mathbb{F}_p)$ keeping two elements fixed, we have $\mathbb{Q}_p(\theta, \theta_2, \ldots, \theta_p) = \mathbb{Q}_p(\theta, \theta_2)$. Accordingly, the ramification index of the local extension $\mathbb{Q}_p(\theta, \theta_2, \ldots, \theta_p)/\mathbb{Q}_p$ is precisely $\frac{p(p-1)}{\epsilon}$. So the inertia group of $\wp$ in $N/\mathbb{Q}$ is in this case a transitive solvable permutation group of degree p and order $\frac{p(p-1)}{\epsilon}$.

In order to get the decomposition group, we have to factorise the reduction $\overline{F}(Y)$ modulo π of the associated polynomial $F(Y)$ over the residue field $\mathbb{F}_p$ of the local field $\mathbb{Q}_p(\theta)$. As

$$-\alpha v_p(a) + \alpha v_p(b) - \beta s - 1 = -\alpha v_p(ab^{s-1}) + s(\alpha v_p(b) - \beta p) + s\beta(p-1) - 1$$

https://doi.org/10.1017/S001708952000004X Published online by Cambridge University Press

satisfies the congruence

$$-\alpha v_p(a) + \alpha v_p(b) - \beta s - 1 \equiv s - 1 \pmod{\epsilon},$$

the number and the degrees of irreducible factors of $\overline{F}(Y)$ are the same as those of the polynomial

$$\overline{F_1}(Y) = Y^{\epsilon} - (-1)^s \overline{s a_p b_p^{s-1}}\,.$$

By Kummer Theory [4, Remarque, p. A V.87], the factorisation of $\overline{F_1}(Y)$ into irreducible factors over $\mathbb{F}_p$ is given precisely by

$$\overline{F_1}(Y) \equiv \prod (Y^r - \zeta)\,,$$

where the product is taken over the set of elements ζ of $\mathbb{F}_p$, such that $\zeta^{\frac{\epsilon}{r}} = \overline{(-1)^s s a_p b_p^{s-1}}$.

From this factorisation, we deduce that the local extension $\mathbb{Q}_p(\theta, \theta_2)/\mathbb{Q}_p(\theta)$ is of degree $\frac{(p-1)r}{\epsilon}$. As $\mathbb{Q}_p(\theta, \theta_2, \ldots, \theta_p) = \mathbb{Q}_p(\theta, \theta_2)$, this shows that the decomposition group of $\wp$ is isomorphic to the subgroup of $\mathrm{Aff}(\mathbb{F}_p)$ of index $\frac{\epsilon}{r}$ [8, Theorem 1.5, (i)]. This concludes the proof. □

The following corollary in the particular case of an Eisenstein trinomial is worth being mentioned.

COROLLARY 2.3. *Suppose $v_p(a) \geq v_p(b) = 1$. Then :*
the inertia group of a prime $\wp$ of N above p in $N/\mathbb{Q}$ is isomorphic to:

- *the affine group* $\mathrm{Aff}(\mathbb{F}_p)$ *if* $v_p(a) > 1$,
- *the subgroup of the affine group of index* $\gcd(p-1, s)$ *if* $v_p(a) = 1$ *;*

and the decomposition group of $\wp$ is isomorphic to:

- $\mathrm{Aff}(\mathbb{F}_p)$ *if* $v_p(a) > 1$,
- *the subgroup of* $\mathrm{Aff}(\mathbb{F}_p)$ *of order* $\frac{p(p-1)r}{\gcd(p-1,s)}$ *if* $v_p(a) = 1$, *where r is the order of the class of* $\frac{a_p s}{b_p}$ *in the factor group* $\mathbb{F}_p^*/\mathbb{F}_p^{*s}$.

2.1.2. The case $(p-s)v_\ell(b) = pv_\ell(a)$

PROPOSITION 2.4. *Let $\ell \neq p$ be a prime number such that $(p-s)v_\ell(b) = pv_\ell(a)$. Then the prime number ℓ is ramified in the extension $N/\mathbb{Q}$ precisely when $v_\ell(p^p b_\ell^{p-1} + s^s(p-s)^{p-s} a_\ell^p b_\ell^{s-1}) = v_\ell(p^p b_\ell^{p-s} + s^s(p-s)^{p-s} a_\ell^p)$ is odd. In the case of ramification, the inertia group of an ℓ-adic place of N is generated by a transposition.*

Proof. As p must divide $v_\ell(b)$, we put $k = \frac{v_\ell(b)}{p}$ and we replace our trinomial $f(X)$ by $\frac{f(\ell^k X)}{\ell^{kp}} = X^p + a_\ell X^s + b_\ell$, whose discriminant is given by

$$(-1)^{\frac{p-1}{2}}[p^p b_\ell^{p-1} + s^s(p-s)^{p-s} a_\ell^p b_\ell^{s-1}].$$

As ℓ does not divide $a_\ell b_\ell$, by [17, Theorem 2] or [18, Theorem 1], the ℓ-adic valuation of the absolute discriminant d_K of the field $K = \mathbb{Q}(\theta)$ is either 0 or 1 according to the parity of the ℓ-adic valuation of the discriminant of $\frac{f(\ell^k X)}{\ell^{kp}}$ (or of $f(X)$). The rest of the proof is similar to that of Lemma 5 of [20]. Namely, in the case of ramification, as $v_\ell(d_K) = 1$, the prime number ℓ admits a factorisation such as $\ell = \mathfrak{l}_1^2 \mathfrak{l}_2 \cdots \mathfrak{l}_g$, where the $\mathfrak{l}_i$s are distinct

https://doi.org/10.1017/S001708952000004X Published online by Cambridge University Press

prime ideals in K and the residue class field of $\mathfrak{l}_1$ is isomorphic to $\mathbb{F}_\ell$. Thus, the factorisation of $f(X)$ as product of distinct irreducible elements of $\mathbb{Q}_\ell[X]$ is of the form

$$f(X) = f_1(X)f_2(X)\cdots f_g(X),$$

where the roots of $f_1(X)$ generate a ramified extension of $\mathbb{Q}_\ell$ of degree 2 and the roots of the other factors $f_j(X)$ $(j \geq 2)$ generate unramified extensions of $\mathbb{Q}_\ell$. Then, the inertia group of a place of N above $\mathfrak{l}_1$ is the group of order 2 generated by the transposition which exchanges the two roots of $f_1(X)$. □

When $\ell = p$, replacing once again $f(X)$ by $\frac{f(p^kX)}{p^{kp}} = X^p + a_pX^s + b_p$, leads to a prime-to-$p$ discriminant $(-1)^{\frac{p-1}{2}}[p^pb_p^{p-1} + s^s(p-s)^{p-s}a_p^pb_p^{s-1}]$. Hence, under the hypothesis $(p-s)v_p(b) = pv_p(a)$, the prime p does not ramify in $N/\mathbb{Q}$.

2.1.3. The case $(p-s)v_\ell(b) > pv_\ell(a)$

It remains for us to deal with the case where $(p-s)v_\ell(b) > pv_\ell(a)$. This case is more involved, as the $(\mathbb{Q}_\ell, X)$-polygon of the trinomial $f(X)$ has two sides (Figure 4), namely a side S_1 joining the points $(0, 0)$ and $(p-s, v_\ell(a))$ and a side S_2 joining the point $(p-s, v_\ell(a))$ to $(p, v_\ell(b))$.

Changing $f(X)$ to $\ell^p f\left(\frac{X}{\ell}\right)$ if $v_\ell(a) = 0$, we can suppose that the $(\mathbb{Q}_\ell, X)$-polygon of $f(X)$ has no horizontal part. The associated polynomials [**8**, Definition 1.4] of S_1 and S_2 are, respectively, $F_1(Y) = Y^{\varepsilon_1} + a_\ell$ and $F_2(Y) = Y^{\varepsilon_2} + \frac{b_\ell}{a_\ell}$, where $\varepsilon_1 = \gcd(p-s, v_\ell(a))$ and $\varepsilon_2 = \gcd(s, v_\ell(b) - v_\ell(a))$.

Let us first recall the following well-known result, which is an immediate consequence of [**9**, Theorem 1.6.A(i)].

LEMMA 2.5. *Let I be a cyclic normal subgroup of order e of a transitive permutation group D. Then I is generated by a product of disjoint cycles of equal length e.*

PROPOSITION 2.6. *(to be compared with [**20**, Theorem 2]). Let ℓ be a prime number coprime to $s(p-s)$, such that $(p-s)v_\ell(b) > pv_\ell(a)$. Then $N/\mathbb{Q}$ is not wildly ramified at ℓ. More precisely, the ramification index of an ℓ-adic place $\mathfrak{L}$ of N is $\frac{(p-s)s}{\varepsilon_1\varepsilon_2}$, where $\varepsilon_1 = \gcd(p-s, v_\ell(a))$ and $\varepsilon_2 = \gcd(s, v_\ell(b) - v_\ell(a))$. The corresponding cyclic inertia group is generated by a permutation which is the product of ε_1 disjoint cycles of equal length $\frac{p-s}{\varepsilon_1}$ and of ε_2 disjoint cycles of equal length $\frac{s}{\varepsilon_2}$.*

Proof. We use the factorisations of the two reductions $\overline{F_i}(Y)$ $(1 \leq i \leq 2)$ modulo ℓ of the associated polynomials $F_i(Y)$ in product of irreducible polynomials of $\mathbb{F}_\ell[Y]$. These factorisations are of the form

$$\overline{F_i}(Y) = \prod_{j=1}^{t_i} \bar{F}_j^{(i)}(Y) \qquad (1 \leq i \leq 2).$$

From this, we deduce by [**8**, Theorem 1.5] the following factorisation

$$f(X) = \prod_{i=1}^{2}\prod_{j=1}^{t_i} \Phi_j^{(i)}(X),$$

where, for each j, the polynomial $\Phi_j^{(i)}(X)$ is irreducible over $\mathbb{Q}_\ell$ of degree $e_i \deg_Y\left(\bar{F}_j^{(i)}\right)$, with $e_1 := \frac{p-s}{\varepsilon_1}$ and $e_2 := \frac{s}{\varepsilon_2}$. Furthermore, by [**8**, Theorem 1.5, (ii)], as the associated

https://doi.org/10.1017/S001708952000004X Published online by Cambridge University Press

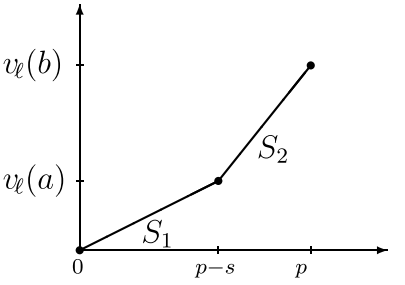


Figure 4. The $(\mathbb{Q}_\ell, X)$-polygon of $f(X)$ when $(p-s)v_\ell(b) > pv_\ell(a)$.

polynomials are separable modulo ℓ, the ramification index of the extension $\mathbb{Q}_\ell(\theta_j^{(i)})/\mathbb{Q}_\ell$ is precisely e_i for every root $\theta_j^{(i)}$ of $\Phi_j^{(i)}(X)$. As ℓ does not divide $s(p-s)$, these extensions are tamely ramified. By Abhyankar's Lemma, the ramification index of the splitting field of $f_i(X) := \prod_{j=1}^{t_i} \Phi_j^{(i)}(X)$ over $\mathbb{Q}_\ell$ is e_i, for each $i = 1, 2$. So the ramification index of the splitting field of $f(X) = f_1(X)f_2(X)$ over $\mathbb{Q}_\ell$ is precisely $e_1e_2 = \frac{s(p-s)}{\varepsilon_1\varepsilon_2}$. As the prime $\mathfrak{L}$ is tamely ramified above ℓ, its inertia group $I_\mathfrak{L}$ is cyclic. Let σ be a generator of $I_\mathfrak{L}$. Introduce the splitting fields $L_j^{(i)}$ of the factors $\Phi_j^{(i)}(X)$ over $\mathbb{Q}_\ell$. Lemma 2.5, applied to the action of the Galois group of the extension $L_j^{(i)}/\mathbb{Q}_\ell$ on the set of the roots of the factor $\Phi_j^{(i)}(X)$ and to its normal subgroup $I_j^{(i)}$ (the restriction of $I_\mathfrak{L}$ to $L_j^{(i)}$), shows that σ must act on the roots of $\Phi_j^{(i)}(X)$ as a product of disjoint cycles of equal length e_i. This completes the proof. □

REMARK 2.7. According to the above propositions, every prime coprime to $ps(p-s)$ which ramifies in K is tamely ramified. We note that the prime p is wildly ramified in N as soon as the trinomial $f(X)$ is Eisenstein with respect to p. For the prime p to be wildly ramified in N, it is necessary, by the last paragraph in Subsection 2.1.2 and Proposition 2.6, that $pv_p(a) > (p-s)v_p(b)$. The next proposition complements results of Plans and Vila [**23**] concerning sufficient conditions for the wild ramification of a prime in the splitting field of a trinomial over the rationals.

PROPOSITION 2.8. *(to be compared with [**6**, Theorem 1.3]). Let ℓ be a prime number such that $(p-s)v_\ell(b) > pv_\ell(a)$. Then the index of ramification of an ℓ-adic place in $N/\mathbb{Q}$ is divisible by $\frac{(p-s)s}{\varepsilon_1\varepsilon_2}$, where $\varepsilon_1 = \gcd(p-s, v_\ell(a))$ and $\varepsilon_2 = \gcd(s, v_\ell(b) - v_\ell(a))$. If, moreover, ℓ is wildly ramified in $N/\mathbb{Q}$, then there exists in the corresponding inertia group a permutation of order ℓ which fixes $p-s$ or s roots according to whether ℓ divides s or $p-s$. In particular, ℓ is wildly ramified in $N/\mathbb{Q}$, if $v_\ell(s) > v_\ell(v_\ell(\frac{b}{a}))$ or if $v_\ell(p-s) > v_\ell(v_\ell(a))$.*

Proof. By [**8**, Theorem 1.5], from the factorisations

$$\overline{F_i}(Y) = \prod_{j=1}^{t_i} \bar{F}_j^{(i)}(Y)^{a_j^{(i)}} \qquad (i = 1, 2),$$

of the reductions modulo ℓ of the associated polynomials $F_i(Y)$ into irreducible factors in $\mathbb{F}_\ell[Y]$, we deduce in $\mathbb{Q}_\ell[X]$ the following factorisation

$$f(X) = \prod_{i=1}^{2} \prod_{j=1}^{t_i} \Phi_j^{(i)}(X),$$

https://doi.org/10.1017/S001708952000004X Published online by Cambridge University Press

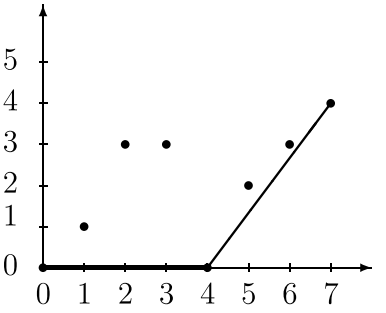


Figure 5. The $(X-6, \mathbb{Q}_3)$-polygon of X^7+7X^3-378.

where, for each j, the polynomial $\Phi_j^{(i)}(X)$ is of degree $\lambda_i a_j^{(i)} \deg_Y(\bar{F}_j^{(i)})$, with $\lambda_1 := \frac{p-s}{\varepsilon_1}$ and $\lambda_2 := \frac{s}{\varepsilon_2}$. Furthermore, the extension generated over $\mathbb{Q}_\ell$ by a root of the polynomial $\Phi_j^{(i)}(X)$ has a ramification index divisible by λ_i. As the integers λ_1 and λ_2 are coprime, the ramification index of the splitting field of $f(X)$ over $\mathbb{Q}_\ell$ is divisible by $\lambda_1\lambda_2 = \frac{(p-s)s}{\varepsilon_1\varepsilon_2}$.

Let us denote, for $i \in \{1, 2\}$, by $f_i(X)$ the factor of $f(X)$ given by

$$f_i(X) = \prod_{j=1}^{t_i} \Phi_j^{(i)}(X)\,.$$

If a prime ℓ is wildly ramified in $N/\mathbb{Q}$, then we know by Remark 2.7 that ℓ divides s or $p-s$. If ℓ divides s (resp. $p-s$), then ℓ does not divide $p-s$ (resp. s), so that the associated polynomial $F_1(Y)$ (resp. $F_2(Y)$) is separable over $\mathbb{F}_\ell$, hence we have $a_j^{(1)} = 1$ (resp. $a_j^{(2)} = 1$) for every index $j \in \{1, \ldots, t_1\}$ (resp. $j \in \{1, \ldots, t_2\}$). By [**8**, Theorem 1.5, (ii)], the ramification index of the extension of $\mathbb{Q}_\ell$ generated by a root of the polynomial $f_1(X)$ (resp. $f_2(X)$) is precisely λ_1 (resp. λ_2). Thus, this extension is tamely ramified. Accordingly, the ℓ-Sylow subgroup of the inertia group leaves fixed any of the $p-s$ (resp. s) roots of $f_1(X)$ (resp. $f_2(X)$). As ℓ is supposed to be wildly ramified in $N/\mathbb{Q}$, this ℓ-Sylow subgroup contains a permutation of order ℓ.

The condition $v_\ell(s) > v_\ell(v_\ell(\frac{b}{a}))$ (resp. $v_\ell(p-s) > v_\ell(v_\ell(a))$) is equivalent to the divisibility by ℓ of λ_2 (resp. λ_1). Hence, under each of these conditions, the prime ℓ is wildly ramified in $N/\mathbb{Q}$. □

Suppose that ℓ is a prime divisor of s and that $(p-s)v_\ell(b) > pv_\ell(a)$. When the inequality $v_\ell(s) > v_\ell\,(v_\ell(b/a))$ is not satisfied, then the ramification at ℓ could be either wild or tame as the following two examples (with $p = 7$ and $s = \ell = 3$) show.

EXAMPLES 2.9. (i) If $f(X) = X^7 + 7X^3 - 378$, let us show that the prime 3 is wildly ramified. By Taylor's formula, we have

$$X^7+7X^3-378 = (X-6)^7+42(X-6)^6+756(X-6)^5+7560(X-6)^4+$$
$$45367(X-6)^3+163422(X-6)^2+327348(X-6)+281070.$$

Hence, Figure 5 represents the $(X-6, \mathbb{Q}_3)$-polygon of our trinomial. We observe that this polygon has a side of slope $4/3$ and of horizontal length 3 : by Ore's Theorem [**8**, Theorem 1.5], we conclude that the ramification index over $\mathbb{Q}_3$ of the splitting field of the trinomial X^7+7X^3-378 is divisible by 3. So the prime 3 is wildly ramified in the splitting field of this trinomial.

https://doi.org/10.1017/S001708952000004X Published online by Cambridge University Press

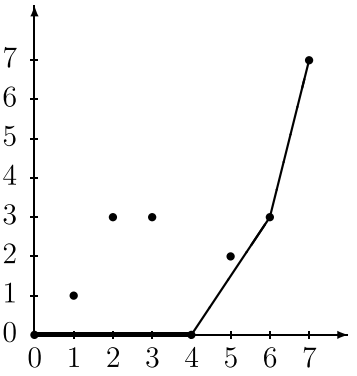


Figure 6. The $(X-3, \mathbb{Q}_3)$-polygon of X^7+7X^3-189.

(ii) If $f(X)=X^7+7X^3-189$, then the prime 3 is tamely ramified. Indeed, Taylor's formula gives

$$X^7+7X^3-189=(X-3)^7+21(X-3)^6+189(X-3)^5+945(X-3)^4$$
$$+2842(X-3)^3+5166(X-3)^2+5292(X-3)+2187.$$

Therefore, Figure 6 represents the $(X-3, \mathbb{Q}_3)$-polygon of X^7+7X^3-189. It has two non-horizontal sides: the first is of slope $3/2$ and of horizontal length 2, the second is of slope 4 and of horizontal length 1. By Hensel's Lemma and Ore's Theorem [**8**, Theorem 1.5], we conclude that, in the ring $\mathbb{Z}_3[X]$, the trinomial X^7+7X^3-189 is the product $f_4(X)f_2(X)f_1(X)$ of a polynomial $f_4(X)\in\mathbb{Z}_3[X]$ of degree 4 such that

$$f_4(X)\equiv X^4+7 \pmod{3\mathbb{Z}_3[X]}$$

by two irreducible polynomials $f_2(X)$ and $f_1(X)$ of degrees, respectively, 2 and 1. As the polynomial X^4+7 has no repeated root modulo the prime 3, the roots of the factor $f_4(X)$ lie in an unramified extension of $\mathbb{Q}_3$. As the roots of $f_2(X)$ have a 3-adic valuation $3/2$, the splitting field of $f_2(X)$ is a totally ramified extension of $\mathbb{Q}_3$ of degree 2. Finally, the unique root of $f_1(X)$ is in $\mathbb{Q}_3$. Thus, we see that the ramification index of the splitting field of our trinomial over $\mathbb{Q}_3$ is 2. So the prime 3 is tamely ramified in the splitting field of X^7+7X^3-189.

Likewise, for a divisor ℓ of $p-s$ such that $(p-s)v_\ell(b)>pv_\ell(a)$, when the inequality $v_\ell(p-s)>v_\ell(v_\ell(a))$ is not satisfied, we can verify in an analogous way that the ramification at ℓ can be either wild or tame. Namely, with $p=5$ and $\ell=3$, the ramification at 3 is wild for the Eisenstein trinomial $f(X)=X^5+5X^2+15$; but it is tame for $f(X)=X^5-5X^2+15$.

2.2. Local study at the infinite prime. By Descartes' rule of signs, it is known that our trinomial $f(X)$ has one or three real roots. On the other hand, the discriminant D of $f(X)$ has the same sign as $(-1)^{r_2}$, where $2r_2$ is the number of complex embeddings of K. Accordingly, the inertia group I_∞ above the infinite prime is generated by a product of $\frac{p-1}{2}$ transpositions if $(-1)^{\frac{p-1}{2}}D>0$ and by the product of $\frac{p-3}{2}$ transpositions if $(-1)^{\frac{p-1}{2}}D<0$.

https://doi.org/10.1017/S001708952000004X Published online by Cambridge University Press

3. Galois group. As a consequence of the classification of finite simple groups, Feit [10] drew up the list of possible non-solvable Galois groups of prime degree trinomials over the field $\mathbb{Q}$ of rational numbers:

1. the symmetric group S_p or the alternating group A_p;
2. the projective linear group $\mathrm{PSL}_3(2)$ of degree 7;
3. the groups $\mathrm{PSL}_2(11)$ or M_{11} (Mathieu group) of degree 11;
4. the projective semi-linear groups G between $PSL_2(2^e)$ and $P\Gamma L_2(2^e)$ of prime degree $p = 1 + 2^e > 5$.

We are going to apply our local study to determine the Galois group of trinomials $f(X) = X^p + aX^s + b$ with integral coefficients. The discriminant D of f is [26, Theorem 2]

$$D = (-1)^{(p-1)/2}[p^p b^{p-1} + (p-s)^{p-s} s^s a^p b^{s-1}]. \tag{3.1}$$

Let $\delta := \min(pv_p(a), (p-s)v_p(b) + p)$, so that

$$D = (-1)^{(p-1)/2} b_p^{s-1} p^{\delta+(s-1)v_p(b)} \left[p^{(p-s)v_p(b)+p-\delta} b_p^{p-s} + s^s (p-s)^{p-s} p^{pv_p(a)-\delta} a_p^p \right],$$

where we recall that $a_p = \frac{a}{p^{v_p(a)}}$, $b_p = \frac{b}{p^{v_p(b)}}$.

THEOREM 3.1. *Let $f(X) = X^p + aX^s + b$, with $0 < s < p$, be an irreducible trinomial such that p does not divide $v_p(b)$. Suppose either $pv_p(a) - (p-s)v_p(b) > p$ or $v_p(ab^{s-1})$ is odd. Then the Galois group G of $f(X)$ over $\mathbb{Q}$ is either solvable or the symmetric group S_p.*

Proof. If $pv_p(a) - (p-s)v_p(b) > p$, then the p-adic valuation of the discriminant D is the odd integer $(p-1)v_p(b) + p$. If $v_p(ab^{s-1})$ is odd and $pv_p(a) - (p-s)v_p(b) < p$, then $\delta = pv_p(a)$ and $v_p(D) = pv_p(a) + (s-1)v_p(b) = v_p(ab^{s-1}) + (p-1)v_p(a)$ is again odd. Hence under either of the above two conditions, the discriminant is not a square in $\mathbb{Q}$ and the Galois group G is an odd permutation group. Apart from the full symmetric group S_p, all the non-solvable Galois groups appearing in Feit's list are even permutation groups (for the projective semi-linear group $P\Gamma L_2(2^e)$, see [7, Lemma 3.1]). Therefore, the theorem follows. □

COROLLARY 3.2. *Let $f(X) = X^p + aX^s + b$ be a trinomial of Eisenstein type with respect to a prime number p, with $0 < s < p$. Suppose either $v_p(a) > 1$ or s is odd. Then the Galois group G of $f(X)$ over $\mathbb{Q}$ is either solvable or the symmetric group S_p.*

REMARK 3.3. By Proposition 2.2, if the Galois group in the above Theorem 3.1 is solvable, it can only be the affine group $\mathrm{Aff}(\mathbb{F}_p)$ in each of the following two cases:

(1) $v_p(ab^{s-1})$ and $p-1$ are coprime;
(2) $pv_p(a) - (p-s)v_p(b) > p$.

REMARK 3.4. To our knowledge, no example of an irreducible solvable trinomial $X^p + aX^s + b$ of prime degree $p \geq 7$ is known, though degree 8 irreducible trinomials can be solvable: it is well known that the Galois group of $X^8 - 5X - 5$ is the wreath product $S_4 \wr S_2$ of order $1152 = 2^7 \cdot 3^2$. For $p = 5$, there exist explicit parametrisations for general solvable trinomials $X^5 + aX + b$, dating at least back to Weber [28, p. 704] (see also [24, 25] and [12, chapter 2]). In view of Corollary 2.3, such an irreducible solvable trinomial cannot have a cyclic or dihedral Galois group if it is Eisenstein with respect to 5. An example of a solvable Eisenstein trinomial is provided for $p = 5$ by $X^5 - 5^2 \cdot 41^3 X + 5 \cdot 2^2 \cdot 3^2 \cdot 7 \cdot 41^4$, whose Galois group is the affine group $\mathrm{Aff}(\mathbb{F}_5)$.

From Feit's result and equation (3.1), we obtain the following result.

https://doi.org/10.1017/S001708952000004X Published online by Cambridge University Press

THEOREM 3.5. *Let $f(X) = X^p + aX^s + b$ be an irreducible trinomial of prime degree p, with $0 < s < p$ and $ab^{s-1} > 0$, and suppose that its Galois group G over $\mathbb{Q}$ is not solvable.*

1. *If the discriminant of $f(X)$ is not a square, then the Galois group G is the symmetric group S_p.*
2. *If the discriminant of $f(X)$ is a square, then G is either the alternating group A_p, or a projective semi-linear group between $PSL_2(2^e)$ and $P\Gamma L_2(2^e)$. The projective semi-linear groups can only occur when $p = 2^e + 1$ is a Fermat prime.*

By combination of Corollary 3.2 and Theorem 3.5, we can get the following interesting statement.

PROPOSITION 3.6. *If p is not a Fermat prime, and if $ab > 0$, then the Galois group of an Eisenstein-type trinomial $f(X) = X^p + aX^s + b$ is either solvable or contains the alternating group A_p.*

THEOREM 3.7. *Let $f(X) = X^p + aX^s + b$ be an irreducible trinomial of prime degree p, with $0 < s < p - 2$. Suppose that there exists an odd prime number ℓ dividing s which is wildly ramified in K (or equivalently in N). Then the Galois group G of $f(X)$ over $\mathbb{Q}$ is either the symmetric group S_p or the alternating group A_p.*

Proof. By Propositions 2.1 and 2.4, the prime $\ell \notin \{2, p\}$ being wildly ramified, we know that $(p - s)v_\ell(b) > pv_\ell(a)$. By Proposition 2.8, there exists in G a permutation of order ℓ which fixes $p - s$ roots. As $s < p - 1$, this permutation stabilises at least two roots of $f(X)$. Now the two-point stabiliser in $\mathrm{Aff}(\mathbb{F}_p)$ is trivial, therefore G is not solvable. As $s < p - 2$, we have in G a permutation of order ℓ fixing at least three roots of $f(X)$. On the other hand, the group $P\Gamma L(2, 2^e)$ is a triply transitive group of order $(2^e + 1)2^e(2^e - 1)e$ [**1**, p. 20], so that the three-point stabiliser in $\mathrm{P\Gamma L}(2, 2^e)$ is of order e, which is a power of 2. As ℓ is odd, this proves that G is not a projective semi-linear group contained in $P\Gamma L(2, 2^e)$. As the three-point stabiliser in the Mathieu group M_{11} is of order 8, the group M_{11} and its subgroup $\mathrm{PSL}_2(11)$ are excluded by an analogous argument. Lastly, any permutation in $\mathrm{PSL}_3(2)$ fixing three points has an order dividing 2, so $\mathrm{PSL}_3(2)$ is also not a possible Galois group. So the theorem follows from Feit's list. □

COROLLARY 3.8. *Let $f(X) = X^p + aX^s + b$ be an irreducible trinomial of prime degree p, with $0 < s < p - 2$. Suppose that there exists an odd prime number ℓ such that $(p - s)v_\ell(b) > pv_\ell(a)$ and $v_\ell(s) > v_\ell(v_\ell(b/a))$ (in particular ℓ is a divisor of s). Then the Galois group G of $f(X)$ over $\mathbb{Q}$ is either the symmetric group S_p or the alternating group A_p.*

The conclusion of Theorem 3.7 stands also when $s = p - 2$, once our trinomial is of Eisenstein type with respect to p. Indeed, Corollary 3.2 shows that the Galois group is isomorphic to S_p in this case. For $s = p - 1$, when $pv_p(a) - (p - s)v_p(b) > p$, Theorem 3.1 shows that the Galois group is either S_p or $\mathrm{Aff}(\mathbb{F}_p)$. In the special case where $s = p - 1$ and $pv_p(a) - (p - s)v_p(b) = p - 1 < p$, we have the following result.

THEOREM 3.9. *Let $f(X) = X^p + aX^{p-1} + b \in \mathbb{Z}[X]$ be an irreducible trinomial of prime degree $p \neq 2$, such that b divides a^p and $v_p(a^p/b) = p - 1$, and G be its Galois group over $\mathbb{Q}$.*

(i) *If the discriminant of $f(X)$ is not a square, then $G \simeq S_p$;*
(ii) *If the discriminant of $f(X)$ is a square, then $p \equiv 1 \bmod 8$ and $G \simeq A_p$ or $PSL_2(2^e)$.*

The latter is only possible when p is a Fermat prime.

https://doi.org/10.1017/S001708952000004X Published online by Cambridge University Press

Proof. By the formula (3.1), the discriminant D of $f(X)$ is

$$D = (-1)^{\frac{p-1}{2}} b^{p-1} \left[p^p + (p-1)^{p-1}(a^p/b)\right].$$

For $p \equiv \pm 3 \pmod 8$, we obtain the congruence $D/b^{p-1} \equiv (-1)^{\frac{p-1}{2}} p \pmod 8$ which shows that D cannot be a square. Similarly, if $p \equiv 7 \pmod 8$, then $p-1$ has a prime divisor $\ell \equiv 3 \pmod 4$ and we get the congruence $D/b^{p-1} \equiv -p^p \equiv -1 \pmod \ell$. As -1 is not a quadratic residue modulo ℓ, this shows that D cannot be a square.

As b divides a^p, for every prime ℓ, we have the inequality $v_\ell(b) \leq p v_\ell(a)$. As $v_p(ab^{s-1}) = v_p(ab^{p-2}) = v_p(a^p/b) + (p-1)v_p(b/a) \equiv 0 \pmod{p-1}$, we know by Proposition 2.2 that the inertia group above p is cyclic of order p. By Propositions 2.1 and 2.4, the inertia group above $\ell \neq p$ is either generated by a cycle of order p or by a transposition. If G contains a transposition, we have $G \simeq S_p$. Accordingly, we can reduce the proof to the case where all inertia groups are cyclic of order p. If G were solvable then G would be cyclic of order p, which is excluded for $p > 3$ by the local study at the infinite prime. So G is not solvable if $p > 3$.

When $p = 7$ or $p = 11$, we have just seen that D is not a square; hence, G cannot be isomorphic to $\mathrm{PSL}_3(2)$, M_{11} or $\mathrm{PSL}_2(11)$.

Finally, if $p = 1 + 2^e$ is a Fermat prime number, then the factor group $\mathrm{P\Gamma L}_2(2^e)/\mathrm{PSL}_2(2^e)$ having an order coprime to p, all elements of order p in $\mathrm{P\Gamma L}_2(2^e)$ lie in $\mathrm{PSL}_2(2^e)$. Hence, if the Galois group G is a group between $\mathrm{PSL}_2(2^e)$ and $\mathrm{P\Gamma L}_2(2^e)$, it can only be $\mathrm{PSL}_2(2^e)$. □

Theorem 3.9 can be applied for the trinomial $f(X) = X^p + aX^{p-1} + a$ of Eisenstein type with respect to p. This case was dealt with in [**3**]. Namely, for any rational integer a, the Galois group of the trinomial $X^p + aX^{p-1} + a$ is the full symmetric group, as soon as this trinomial is irreducible.

Examples 3.10. In the situation of Theorem 3.9, the case (*ii*) actually occurs for $p \equiv 1 \bmod 8$. Indeed, when $v_p(a) = v_p(b) = 1$, the discriminant of our trinomial is $D = b^{p-1}p^{p-1}D_0$ with

$$D_0 = p + (p-1)^{p-1}(a_p^p/b_p),$$

where we recall that $a_p = a/p$ and $b_p = b/p$. Obviously, $p \equiv 1 \bmod \ell$ for every odd prime divisor ℓ of $p-1$. As we also suppose $p \equiv 1 \bmod 8$, the residue class of p is a square in the ring $\mathbb{Z}/(p-1)^{p-1}\mathbb{Z}$. So, there exist infinitely many rational integers c such that $p + (p-1)^{p-1}c$ is the square of an integer y. Adding if necessary $(p-1)^{p-1}$ to y, we can suppose that p does not divide c. Now any choice of the two integers a and b such that $a_p^p = b_p c$ yields a square discriminant D. Numerically we can take $p = 17$, denote by q_1, q_2 the prime numbers $q_1 = 727892351$ and $q_2 = 863207903$, and set $c = 2^3 \cdot q_1 \cdot q_2$, $a = 17 \cdot 2 \cdot q_1 \cdot q_2$ and $b = 17 \cdot 2^{14} \cdot q_1^{16} \cdot q_2^{16}$, for which the discriminant of the trinomial $f(X) = X^{17} + aX^{16} + b$ is a square, and we are in the case (*ii*) of Theorem 3.9. For this particular trinomial, it is readily seen that its Galois group is the alternating group A_{17}.

Arguing in a similar way, we get the following statements, analogous to Theorem 3.7 and Corollary 3.8:

Theorem 3.11. *Let $f(X) = X^p + aX^s + b$ be an irreducible trinomial of prime degree p, with $2 < s < p$. Suppose that there exists an odd prime number ℓ dividing $p - s$ which is wildly ramified in K (or equivalently in N). Then, the Galois group G of $f(X)$ over $\mathbb{Q}$ is either the symmetric group S_p or the alternating group A_p.*

https://doi.org/10.1017/S001708952000004X Published online by Cambridge University Press

COROLLARY 3.12. *Let $f(X) = X^p + aX^s + b$ be an irreducible trinomial of prime degree p, with $2 < s < p$. Suppose that there exists an odd prime number ℓ such that $(p-s)v_\ell(b) > pv_\ell(a)$ and $v_\ell(p-s) > v_\ell(v_\ell(a))$ (in particular ℓ is a divisor of $p-s$). Then, the Galois group G of $f(X)$ over $\mathbb{Q}$ is either the symmetric group S_p or the alternating group A_p.*

Combining Remark 2.7 with Theorems 3.7 and 3.11 yields the following statement.

THEOREM 3.13. *Let p be a prime number and $f(X) = X^p + aX^s + b$ a trinomial of degree p with integer coefficients. If $2 < s < p-2$, the existence of a single wildly ramified odd prime $\ell \neq p$ leads to either the alternating group or the full symmetric group as Galois group of $f(X)$ over $\mathbb{Q}$.*

Arguing similarly to the case of wild ramification, it is also possible to get results in some situations when there is a prime number ℓ not dividing $s(p-s)$ such that $(p-s)v_\ell(b) > pv_\ell(a)$. This is illustrated by the next statement.

PROPOSITION 3.14. *Suppose $3 \leq s \leq p-2$, and let G be the Galois group of the irreducible trinomial $f(X) = X^p + aX^s + b$. If a prime number ℓ not dividing $s(p-s)$ is such that $(p-s)v_\ell(b) > pv_\ell(a)$ and $\gcd(v_\ell(a), p-s) = 1$, then the group G contains the alternating group A_p. Moreover, for s odd, the permutation group G is the symmetric group.*

Proof. By Proposition 2.6, we know that the prime ℓ ramifies in N, and that its inertia subgroup is generated by the product of a cycle of length $p-s$ with a disjoint permutation of order dividing s. By taking the s-th power of this generator, we find in G a cycle of length $p-s \geq 2$. By Margraff's Second Theorem [**1**], we conclude that the group G is $(s+1)$-transitive.

As $s \geq 3$, then $s+1 \geq 4$, and this excludes all groups in Feit's list except A_p, S_p and the Mathieu group M_{11}. But M_{11} is also excluded because it does not contain any cycle of order < 11. Moreover, when s is odd, a cycle of length $p-s$ is an odd permutation, so that G cannot be alternating. □

REFERENCES

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

2. B. Bensebaa, A. Movahhedi and A. Salinier, The Galois group of $X^p + aX^s + a$, *Acta Arith.* **134**(1) (2008), 55–65.

3. B. Bensebaa, A. Movahhedi and A. Salinier, The Galois group of $X^p + aX^{p-1} + a$, *J. Number Theory* **129**(4) (2009), 824–830.

4. N. Bourbaki, *Eléments de Mathématique, Algèbre, Chapitres 4 à 7* (Masson, Paris, 1981).

5. C. Bouyacoub and A. Salinier, On the solvability of an Eisenstein trinomial of prime degree, *Acta Arith.* **178**(4) (2017), 385–396.

6. S. D. Cohen, A. Movahhedi and A. Salinier, Double transitivity of Galois groups of trinomials, *Acta Arith.* **82**(1997), 1–15.

7. S. D. Cohen, A. Movahhedi and A. Salinier, Galois groups of trinomials, *J. Alg.* **222**(1999), 561–573.

8. S. D. Cohen, A. Movahhedi and A. Salinier, Factorization over local fields and the irreducibility of generalized difference polynomials, *Mathematika* **47**(2000), 173–196.

9. J. D. Dixon and B. Mortimer, *Permutation Groups*, Graduate Texts in Mathematics, vol. 163 (Springer-Verlag, New-York, 1996).

10. W. Feit, Some consequences of the classification of finite simple groups, *Proc. Sympos. Pure Math.* **37** (1980), 175–181.

https://doi.org/10.1017/S001708952000004X Published online by Cambridge University Press

11. L. Gauckler, The Galois group of the Eisenstein polynomial $X^5 + aX + a$, *Arch. Math.* **90** (2008), 136–139.

12. C. U. Jensen, A. Ledet and N. Yui *Generic polynomials. Constructive aspects of the inverse Galois problem*, Mathematical Sciences Research Institute Publications, vol. 45 (Cambridge University Press, Cambridge, 2002).

13. M. Kölle and P. Schmid, Computing Galois groups by means of Newton polygons, *Acta Arith.* **115** (2004), 71–84.

14. K. Komatsu, Discriminants of certain algebraic number fields, *J. Reine Angew. Math.* **285** (1976), 114–125.

15. K. Komatsu, *On the Galois group of* $x^p + p^l b(x + 1) = 0$, *Tokyo J. Math.* **15** (1992), 351–356.

16. T. Lalesco, Sur le groupe des équations trinômes, *Bulletin de la Société Mathématique de France* **35** (1907), 75–76.

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

18. P. Llorente, E. Nart and N. Vila, Decomposition of primes in number fields defined by trinomials, *Sém. Théor. Nombres Bordeaux* (2) **3**(1) (1991), 27–41.

19. A. Movahhedi, Galois group of $X^p + aX + a$, *J. Alg.* **180**(3) (1996), 966–975.

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

21. W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, 2nd edition (Springer-Verlag, Berlin; PWN-Polish Scientific Publishers, Warsaw, 1990).

22. H. Osada, The Galois groups of the polynomials $x^n + ax^s + b$. II, *Tohoku Math J.* (2) **39** (1987), 437–445.

23. B. Plans and N. Vila, Trinomial extensions of $\mathbb{Q}$ with ramification conditions, *J. Number Theory* **105** (2004), 387–400.

24. G. Roland, N. Yui and D. Zagier, A parametric family of quintic polynomials with Galois group D_5, *J. Number Theory* **15**(1982), 137–142.

25. B. K. Spearman and K. S. Williams, On solvable quintics $X^5 + aX + b$ and $X^5 + aX^2 + b$, *Rocky Mountain J. Math.* **26**(2) (1996), 753–772.

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

27. K. Uchida, Unramified extensions of quadratic number fields. II, *Tôhoku Math. J.* (2) **22** (1970), 220–224.

28. H. Weber, *Lehrbuch der Algebra* (Braunschweig Druck und Verlag von Friedrich Vieweg und Sohn, 1898).

https://doi.org/10.1017/S001708952000004X Published online by Cambridge University Press