MATHEMATICA, 65 (88), N° 1, 2023, pp. 115–121

# THE GALOIS GROUP OF $X^{p^2} + aX + a$

SOUFYANE MOKHTARI and BOUALEM BENSEBA

**Abstract.** Let $p$ be an odd prime number, and $a$ be an integer divisible by $p$ exactly once. We prove that the Galois group $G$ of the trinomial $X^{p^2} + aX + a$ over the field $\mathbb{Q}$ of rational number, is either the full symmetric group $S_{p^2}$, or $\mathrm{AGL}(1, p^2) \leq G \leq \mathrm{AGL}(2, p)$. And we show that $G \simeq S_{p^2}$, except possibly when $p \equiv 1 \pmod 8$, and each prime divisor $q$ of $p+1$ satisfies $q \not\equiv -1 \pmod 4$, and $p$ divides the $\ell$-adic valuation $v_\ell(a)$ of $a$ for each prime divisor $\ell$ of $a/p$.

**MSC 2020.** Primary 11R32, 12F10; Secondary 11S15, 12E10.

**Key words.** Trinomials, ramification, Newton polygons, classification of finite simple groups, Galois group.

## 1. INTRODUCTION

Let $p$ an odd prime number and

$$f(X) = X^{p^2} + aX + a \in \mathbb{Z}[X]$$

be an Eisenstein trinomial with respect to $p$ and $N$ be the splitting field of $f(X)$ over $\mathbb{Q}$. The principal aim of this article is to determine the Galois group of $f$. While the study of the Galois group of trinomial goes back to the beginning of the twentieth century [12], his determination is far from established. From the seventies on, many authors renewed interest in the topic, see for example [2, 5, 6, 9, 10, 14, 18, 19].

In [10] and [11], K. Komatsu investigated the Galois group of trinomial $g(X) = X^p + aX + a$. In [11], it is shown, in particular when $p$ divides $a$ exactly once and $b = \frac{a}{p}$ is a square, that the Galois group of $g(X)$ is the full symmetric group $S_p$. In [14], A. Movahhedi has shown that the Galois group of such an Eisenstein trinomial, with respect to $p$, is either the group $\mathrm{Aff}(\mathbb{F}_p)$, or the full symmetric group $S_p$ which occurs when $b < 0$ or $b \not\equiv 1 \pmod p$, which improving the result of [10]. Later, in [2] and [3] the authors generalized to a wide family of trinomials the results given in [14].

Note that, knowing the inertia groups of the primes ramified in $N$, reduces the area of possible realizations of a permutation group as the Galois group of $f(X)$. So we are driven to analyse the inertia groups of all primes which ramifies in $N$.

Corresponding author: Soufyane Mokhtari.

DOI: 10.24193/mathcluj.2023.1.12

Section 2 is devoted to the detailed analysis of different inertia groups of primes ramified in $N$. Our method is based on Newton polygon which turns out to be efficient for the study of factorisations of polynomials over local field.

In Section 3, the precise local study in Section 2 combined with the classification of the multiply transitive groups [1] allow us to show that the Galois group $G$ of the trinomial $f(X)$ is either the full symmetric group $S_{p^2}$, or $\mathrm{AGL}(1,p^2) \leq G \leq \mathrm{AGL}(2,p)$, where $\mathrm{AGL}(1,p^2)$ is the affine group of dimension 1 over $\mathbb{F}_{p^2}$, and $\mathrm{AGL}(2,p)$ the affine group of dimension 2 over $\mathbb{F}_p$. Furthermore, we shall see that $G \simeq S_{p^2}$ in each of the following cases:

(*i*) $p \not\equiv 1 \pmod 8$.
(*ii*) $p \equiv 1 \pmod 8$, and there exists a prime divisor $q$ of $p+1$ such that $q \equiv -1 \pmod 4$.
(*iii*) there exists a prime divisor $\ell$ of $a/p$, such that $\gcd(v_\ell(a), p) \neq 1$.

## 2. INERTIA GROUPS

Let $p$ be an odd prime number and $a$ be a rational integer divisible by $p$ exactly once. Denote by $\alpha = \alpha_1, \alpha_2, ..., \alpha_{p^2}$ the different roots of the Eisenstein trinomial $f(X) = X^{p^2} + aX + a$ in a fixed 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 let $N = \mathbb{Q}(\alpha, \alpha_2, ..., \alpha_{p^2})$ be the splitting field of $f(X)$ over $\mathbb{Q}$. The Galois group $G$ of $N$ over $\mathbb{Q}$ is a transitive group of permutations of the roots of $f$. The discriminant $D$ of $f$ is

$$D = p^{p^2} b^{p^2-1} D_0,$$

where $b = a/p$ and $D_0 = p^{2p^2-1} + b(p^2-1)^{p^2-1}$.

We shall now look at the inertia group of the different places of $N$ in the extension $N/\mathbb{Q}$.

Proposition 2.1. *The inertia group $I_{\mathfrak{P}}$ (defined up to conjugation of $p$) in $N/\mathbb{Q}$ is isomorphic to* $\mathrm{AGL}(1,p^2)$*, the* 1*- dimensional affine group over the finite field $\mathbb{F}_{p^2}$.*

*Proof.* We fix a prime ideal $\mathfrak{P}$ of $N$ dividing $p$. Let $\mathfrak{p} = \mathfrak{P} \cap K$. We denote by $N_{\mathfrak{P}}$ the completion of $N$ at $\mathfrak{P}$ and by $K_{\mathfrak{p}}$ the closure of $K$ in $N_{\mathfrak{P}}$. Since the trinomial $f$ is of Eisenstein over $\mathbb{Q}_p$, by [16, Theorem 5.27] the extension $K_{\mathfrak{p}}/\mathbb{Q}_p$ is fully ramified.

Consider the polynomial

$$\varphi(X) = \frac{f(\alpha X + \alpha)}{\alpha^{p^2} X} = X^{p^2-1} + \sum_{i=1}^{p^2-1} a_i X^{p^2-i-1} \in \mathbb{Q}(\alpha)[X],$$

where the coefficients $a_i$ are given by

$$a_i = \begin{cases} \binom{p^2}{i} & \text{if } 1 \leq i \leq p^2-2 \\ (p^2 + a\alpha^{1-p^2}) & \text{if } i = p^2-1. \end{cases}$$

Let $\pi$ be a uniformizer of $K_{\mathfrak{p}}$, and $\upsilon_\pi$ be the normalized valuation $\pi$-adic of $K_{\mathfrak{p}}$, so $\upsilon_\pi(\alpha)=\upsilon_p(a)=1$ and $\upsilon_\pi(\lambda)=p^2\upsilon_p(\lambda)$ for all $\lambda\in\mathbb{Q}_p$, since $K_{\mathfrak{p}}/\mathbb{Q}_p$ is totally ramified. Then we have $\upsilon_\pi(a_i)\geq p^2$ if $1\leq i\leq p^2-2$ and $\upsilon_\pi\left(a_{p^2-1}\right)=1$.

So the $(K_{\mathfrak{p}},X)$-Newton polygon of $\varphi$ consists of one segment joining the points $(0,0)$ and $(p^2-1,1)$. Hence by [7, Theorem 1.5], the ramification index of the local extension $K_{\mathfrak{p}}(\alpha_2)/K_{\mathfrak{p}}$ is equal to $p^2-1$.

Write $I_{\mathfrak{P}}$ for the inertia group of $N_{\mathfrak{P}}/\mathbb{Q}_p$, and

$$I_{\mathfrak{P}}^{'}=I_{\mathfrak{P}}\cap \mathrm{Gal}(N_{\mathfrak{P}}/K_{\mathfrak{p}})$$

for the inertia group of $N_{\mathfrak{P}}/K_{\mathfrak{p}}$ , it is a point stabilizer of $I_{\mathfrak{P}}$. By the Abhyankar's Lemma [16, p. 229], the extension $N_{\mathfrak{P}}/K_{\mathfrak{p}}$ is tamely ramified, so in this case $I_{\mathfrak{P}}^{'}$ is cyclic generated by a $\left(p^2-1\right)$-cycle. Introduce the inertia field $L_0$ in $N_{\mathfrak{P}}/\mathbb{Q}_p$, then the totally ramified extension $K_{\mathfrak{p}}/\mathbb{Q}_p$ is linearly disjoint from the unramified extension $L_0/\mathbb{Q}_p$, so $f(X)$ remains irreducible over $L_0$ which implies that $I_{\mathfrak{P}}$ act transitively on the roots of $f(X)$. On the other hand the totally ramified extension $K_{\mathfrak{p}}(\alpha_2)/K_{\mathfrak{p}}$ is linearly disjoint from the unramified extension $L_0(\alpha)/K_{\mathfrak{p}}$, so $\varphi(X)$ remains irreducible over $L_0(\alpha)$. which implies that $I_{\mathfrak{P}}^{'}$ is regular. Hence $I_{\mathfrak{P}}$ is sharply doubly transitive group [1, 15] of degree $p^2$ with order $p^2(p^2-1)$ whose point stabilizers are abelian. The proposition follows by [8, Corollary 7.6A (ii), p. 239]. □

Lemma 2.2. *Let $q\neq p$ be a prime divisor of $a$.*

(1) *If $p^2$ divides $\upsilon_q(a)$, then the prime number $q$ is unramified in $K$.*
(2) *If $\gcd(p^2;\upsilon_q(a))\leq p$, then the prime number $q$ is tamely ramified in $K$. Moreover, when $\gcd(p^2;\upsilon_q(a))=1$ then the prime $q$ is totally ramified in $K$.*

*Proof.* The Newton's polygon of $f(X)$ relative to the prime $q$ consists of a single side joining the points $(0;0)$ and $(p^2;\upsilon_q(a))$, and its associated polynomial is a binomial of the form

$$G(Y)=Y^m+a_q,$$

where $a_q=a/q^{\upsilon_q(a)}$ and $m=\gcd(p^2,\upsilon_q(a))$. Then from [17, Sect. 2, Theorem 5], it follows that $q=\mathfrak{A}^{p^2/m}$, where $\mathfrak{A}$ is an integral ideal of $K$.

Furthermore, since $G(Y)$ is separable modulo $q$, so $\mathfrak{A}$ is a product of distinct prime ideals of $K$ [17, Sect. 2, Theorem 6]. □

By combining the last lemma and the Abhyankar's Lemma [16, p.229], we obtain immediately:

Proposition 2.3. *Let $q\neq p$ be a prime divisor of $a$, ramified in $N$, then the inertia group (defined up to conjugation) of $q$ in $N/\mathbb{Q}$ is a cyclic group of order either $p^2$ or $p$ according to whether $\gcd\left(p^2,\upsilon_q(a)\right)=1$ or $p$.*

### 3. GALOIS GROUPS

Note that, if $\mid D_0 \mid$ is not a square, then the Galois group $G$ of the trinomial $f$ is the symmetric group $S_{p^2}$. Indeed, if a prime number $\ell$ divides $\mid D_0 \mid$ to an odd power, then $\ell$ divides the absolute discriminant of the number field $K$ exactly once [13, Theorem 2]. This implies that the Galois group $G$ contains a transposition [10, Lemma 1]. Now $G$ is a doubly transitive permutation group (see Proposition 2.1) and contains a transposition, then by [8, Theorem 3.3A, p. 77] $G$ is the full symmetric group.

Now, the question which springs to mind is: for which values of $p$, is the absolute value of $D_0$ not a square?

LEMMA 3.1. *Let $p$ be an odd prime number, and*

$$f(X) = X^{p^2} + aX + a \in \mathbb{Z}[X]$$

*be an Eisenstein trinomial with respect to $p$. Then the integer $|D_0|$ is not a square in each of the following two cases:*

(i) $p \not\equiv 1 \pmod 8$
(ii) $p \equiv 1 \pmod 8$*, and there exists a prime divisor $q$ of $p+1$ such that* $q \equiv -1 \pmod 4$.

*Proof.* Suppose that $|D_0| = k^2$ for somme rational integer $k$, then we have $D_0 \equiv p^{2p^2-1} \equiv p \equiv \pm k^2 \pmod 8$.

If $p \not\equiv 1 \pmod 8$, then $p \equiv -1 \pmod 8$ and $D_0 = -k^2$. So $\dfrac{p-1}{2} \equiv -1 \pmod 4$ and there exists is a prime divisor $q$ of $\dfrac{p-1}{2}$ such that $q \equiv -1 \pmod 4$. Knowing that $p \equiv 1 \pmod q$, then $-k^2 \equiv p^{2p^2-1} \equiv 1 \pmod q$, so $-1$ is a quadratic residue modulo $q$ which is a contradiction since $q \equiv -1 \pmod 4$.

If $(ii)$ holds, then $D_0 \equiv p^{2p^2-1} \equiv p \equiv 1 \pmod 8$ and the equality $D_0 = -k^2$ is impossible. So $D_0 = k^2$ and then $k^2 \equiv p^{2p^2-1} \equiv p \equiv -1 \pmod q$ which implies that $-1$ is a quadratic residue modulo $q$; which is a contradiction since $q \equiv -1 \pmod 4$. Therefore, the integer $|D_0|$ is not a square. □

The above discussion and Lemma 3.1 immediately yields the following result.

THEOREM 3.2. *Let $p$ be an odd prime number, and*

$$f(X) = X^{p^2} + aX + a \in \mathbb{Z}[X]$$

*be an Eisenstein trinomial with respect to $p$. Then the Galois group $G$ of the trinomial $f(X)$ is the full symmetric group $S_{p^2}$ in each of the following two cases:*

(i) $p \not\equiv 1 \pmod 8$

(ii) $p \equiv 1 \pmod 8$, *and there exists a prime divisor* $q$ *of* $p+1$ *such that* $q \equiv -1 \pmod 4$.

From [8, Theorem 4.1B] we see that the socle of a finite doubly transitive group is either a regular elementary abelian $p$-group, or a nonregular nonabelian simple group. The doubly transitive groups with nonabelian socle are listed in [1, CTT p. 20, and weak CDT p. 21]. Those lists and [8, Theorem 4.7A], allows us to give the following list of possible realizations of the Galois group $G$ of the trinomial $f$:

(1) $G \simeq S_{p^2}$; or
(2) $G \simeq A_{p^2}$; or
(3) $(Z_p)^2 \leq G \leq \mathrm{AGL}(2,p)$ , where $(Z_p)$ is the cyclic group of order $p$; or
(4) $\mathrm{PSL}(m,q) \leq G \leq P\Gamma L(m,q)$ for an integer $m>1$ and a prime power $q$ such that $(q^m-1)/(q-1) = p^2$.

THEOREM 3.3. *Let*

$$f(X) = X^{p^2} + aX + a$$

*be an Eisenstein trinomial with respect to* $p$. *Then the absolute Galois group* $G$ *of* $f(X)$ *is either the full symmetric group* $S_{p^2}$, *or* $\mathrm{AGL}(1,p^2) \leq G \leq \mathrm{AGL}(2,p)$.

*Proof.* We first notice that $D$ is not a square, so $G$ is not contained in the alternating group $A_{p^2}$. Now suppose $\mathrm{PSL}(m,q) \leq G \leq P\Gamma L(m,q)$. For some integer $m>1$ and a prime power $q$ we have

$$p^2 = \frac{q^m-1}{q-1} = q^{m-1} + q^{m-2} + \ldots + q + 1.$$

If $q$ is odd, then $m$ must be an odd number, which implies that $G$ does not contain an involution fixing at most three points [6, Proposition 2.4]; this contradicts the assumption that $G$ is a Galois group of trinomial.

If $q$ is even, using [1, Numerical Lemma, p 23] and [6, Proposition 2.4], the only renaming case is $(m,q) = (2,8)$ and $(n,p) = (2,3)$ which is impossible by (Theorem 3.2). Knowing by Proposition 2.1 that the affine linear group $\mathrm{AGL}(1,p^2) \leq G$, this completes the proof. □

Now, we shall assume that the prime number $p \equiv 1 \pmod 8$ such that each prime divisor $q$ of $p+1$ satisfies $q \not\equiv -1 \pmod 4$. It Should be noted that the expression $D_0$ is a square for infinitely many rational integers $b$. Indeed, we have $p^{2p^2-1} \equiv 1 \pmod 8$, and for every odd prime divisors $\ell$ of $p-1$ and $q$ of $p+1$ we have $p^{2p^2-1} \equiv 1 \pmod \ell$ and $p^{2p^2-1} \equiv -1 \pmod q$. Knowing that $q \equiv 1 \pmod 4$, then $p^{2p^2-1}$ is a quadratic residue modulo $q$. So the congruence

$$X^2 \equiv p^{2p^2-1} \bmod \left(p^2-1\right)^{p^2-1}$$

is solvable. Now let $\alpha$ be a solution of the above congruence and we may assume that $\alpha$ is not divisible by $p$, since $\alpha + (p^2-1)^{p^2-1}$ is also a solution of this

congruence. So there exists an integer $\beta$ which is not divisible by $p$ such that $\alpha^2-p^{2p^2-1}=\beta(p^2-1)^{p^2-1}$. For every $r\in\mathbb{Z}$, let $b=\beta+2rp\alpha+r^2p^2(p^2-1)^{p^2-1}$; then $D_0$ is a square.

Summarizing, we have established:

THEOREM 3.4. *Let $p$ be a prime number and*

$$f(X)=X^{p^2}+aX+a\in\mathbb{Z}[X]$$

*be an Eisenstein trinomial with respect to $p$. If there is a prime divisor $\ell\neq p$ of $a$ such that $\gcd(v_\ell(a),p)=1$, then the absolute Galois group $G$ of $f$ is the full symmetric group $S_{p^2}$.*

*Proof.* We may assume that $|D_0|$ is a square, since otherwise $G$ would be the symmetric group $S_{p^2}$. We fix a prime ideal $\mathfrak{Q}$ of $N$ lying above $q$. Let $\mathfrak{q}=\mathfrak{Q}\cap K$. We denote by $N_{\mathfrak{Q}}$ the completion of $N$ at $\mathfrak{Q}$ and by $K_{\mathfrak{q}}$ the closure of $K$ in $N_{\mathfrak{q}}$, the local field $K_{\mathfrak{q}}$ is obtained by adjoining a root $\alpha$ of $f$ to $\mathbb{Q}_q$; it is a totally ramified extension of $\mathbb{Q}_q$ (Lemma 3.1).Write $I_{\mathfrak{Q}}$ for the inertia group of $\mathfrak{Q}$ in $N/\mathbb{Q}$. We introduce the maximal unramified extension $L_0$ in $N_{\mathfrak{Q}}/\mathbb{Q}_q$; it is linearly disjoint from the totally ramified extension $K_{\mathfrak{q}}/\mathbb{Q}_q$, so $f(X)$ remains irreducible over $L_0$. Hence $I_{\mathfrak{Q}}$ acts transitively on the roots of $f(X)$. As $I_{\mathfrak{Q}}$ is cyclic of order $p^2$ (Proposition 2.3). By [4, Proposition 1.1], and Theorem 3.3 we conclude that the group $G$ is $S_{p^2}$. □

## REFERENCES


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

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

[3] B. Bensebaa, A. Movahhedi and A. Salinier, *Wild ramification in trinomial extensions and Galois groups*, Glasg. Math. J., **63** (2021), 106–120.

[4] L. Cai Heng , *Permutation groups with a cyclic regular subgroup and arc transitive circulants*, J. Algebraic Combin., **21** (2005), 131–136.

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

[6] S. D. Cohen, A. Movahhedi and A. Salinier, *Galois groups of trinomials*, J. Algebra, **222** (1999), 561–573.

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

[8] J. D. Dixon and B. Mortimer, *Permutation Groups*, Graduate Texts in Mathematics, Vol. 163, Springer, 1996.

[9] K. Komatsu, *Discriminant of certain algebraic number fields*, J. Reine Angew. Math., **285** (1976), 114–125.

[10] K. Komatsu, *On the Galois group of $X^p+aX+a=0$*, Tokyo J. Math., **14** (1991), 227–229.

[11] K. Komatsu, *On the Galois group of $X^p+p^tb(X+1)=0$*, Tokyo J. Math., **15** (1992), 351–356.

[12] T. Lalesco, *Sur le groupe des équations trinômes*, Bull. Soc. Math. France, **35** (1907), 75–76.

[13] P. Llorente, E. Nart and N. Vila, *Discriminants of number fields defined by trinomials*, Acta Arith., **43** (1984), 367–373.
[14] A. Movahhedi, *Galois Group of $X^p + ax + a$*, J. Algebra, **180** (1996), 966–975.
[15] A. Movahhedi and A. Salinier, *The primitivity of the Galois Group of a trinomial*, J. Lond. Math. Soc. (2), **53** (1996), 433–440.
[16] W. Narkiewich, *Elementary and analytic theory of algebraic numbers*, 3rd edition, Springer-Verlag, 2004.
[17] O. Ore,*Newtonsche Polygone in der Theorie der algebraischen Körper*, Math. Ann., **99** (1928), 84–117.
[18] H. Osada, *The Galois group of the polynomials $x^n + ax^s + b$. II*, Tohoku Math. J. (2), **39** (1987), 437-445.
[19] K. Uchida, *Unramified fields II*, Tohoku Math. J., **22** (1970), 220–224.

Received October 29, 2021
Accepted February 28, 2022

*University of Sciences and Technology*
*Houari Boumediene*
*LA3C, Faculty of Mathematics*
*Algiers, Algeria*
*E-mail:* smoukhtari@usthb.dz
https://orcid.org/0000-0002-4416-0765
*E-mail:* b.benseba@usthb.dz
https://orcid.org/0000-0002-5760-8100