Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 7(1): 212–224.
DOI: 10.3934/math.2022013
Received: 05 July 2021
Accepted: 08 October 2021
Published: 11 October 2021

Research article

On the Galois group of three classes of trinomials

Lingfeng Ao, Shuanglin Fei and Shaofang Hong*

Mathematical College, Sichuan University, Chengdu 610064, China

* **Correspondence:** Email: sfhong@scu.edu.cn.

Abstract: Let $n \geq 8$ be an integer and let p be a prime number satisfying $\frac{n}{2} < p < n-2$. In this paper, we prove that the Galois groups of the trinomials

$$T_{n,p,k}(x) := x^n + n^k p^{(n-1-p)k} x^p + n^k p^{nk},$$

$$S_{n,p}(x) := x^n + p^{n(n-1-p)} n^p x^p + n^p p^{n^2}$$

and

$$E_{n,p}(x) := x^n + pnx^{n-p} + pn^2$$

are the full symmetric group S_n under several conditions. This extends the Cohen-Movahhedi-Salinier theorem on the irreducible trinomials $f(x) = x^n + ax^s + b$ with integral coefficients.

Keywords: p-adic Newton polygon; irreducibility criterion; Galois group
Mathematics Subject Classification: Primary 11R09, 11R32, 11C08

1. Introduction

Let $\mathbb{Z}$, $\mathbb{Z}^+$ and $\mathbb{Q}$ be the set of integers, the set of positive integers and the field of rational numbers, respectively. Let $f(x) \in \mathbb{Q}[x]$ be a polynomial of degree n. The Galois group of $f(x)$ over $\mathbb{Q}$ means the Galois group of the splitting field of $f(x)$ over $\mathbb{Q}$, and is denoted by $\mathrm{Gal}_{\mathbb{Q}}(f)$. Let $f(x) = x^n + ax^s + b$ be a trinomial with integral coefficients, where $\gcd(n, s) = 1$. There are lots of results about the Galois group of special trinomials. Uchida [14] and Yamamoto [15] showed that the Galois group of the polynomial $x^n + ax + b \in \mathbb{Z}[x]$ over $\mathbb{Q}$ is S_n under the following conditions:

(1) n is a prime number,

(2) $a(n-1)$ and nb are relatively prime,

(3) $x^n + ax + b$ is irreducible over $\mathbb{Q}$.

Ohta [11] generalized these results under certain conditions. Osada [12] considered the polynomial $f(x) = x^n + a_0 c^n x^l + b_0^l c^n$ and proved that $\mathrm{Gal}_{\mathbb{Q}}(f)$ is S_n if $f(x)$ is irreducible over $\mathbb{Q}$ and $\gcd(a_0 c(n -$

$l), nb_0) = 1$. Cohen, Movahhedi and Salinier [4] extended Osada's result by considering irreducible trinomials $f(x) = x^n + ax^s + b$ with integral coefficients, where $\gcd(nb, as(n-s)) = 1$ and $s \neq n-1$. They proved that if s is a prime number and there is a prime divisor p of b such that $\gcd(s, v_p(b)) = 1$, then $\mathrm{Gal}_{\mathbb{Q}}(f)$ contains A_n. They also determined what $\mathrm{Gal}_{\mathbb{Q}}(f)$ could be if $A_n \not\subseteq \mathrm{Gal}_{\mathbb{Q}}(f)$ under certain conditions.

Another variation of the result of Uchida and Yamamoto is to consider the Galois group of $f(x) = x^p + ax^s + a$, where p is a prime number. These trinomials were investigated by Komatsu in [9] and [10] with a taking special values. Later on, Movahhedi, Cohen, Bensebaa and Salinier also considered the trinomials of the forms $x^p + ax + a$, $x^p + ax^{p-1} + a$ and $x^p + ax^s + a$. The interested readers can consult with [1,2,8].

Let $x^n + ax^s + b$ denote a general trinomial over $\mathbb{Q}$. In this paper, we mainly study three kinds of trinomials. Setting $s = p$, $a = n^k p^{(n-1-p)k}$ and $b = n^k p^{nk}$, we get the first trinomials

$$T_{n,p,k}(x) := x^n + n^k p^{(n-1-p)k} x^p + n^k p^{nk}.$$

The first main result of this paper can be stated as follows:

Theorem 1.1. *Let n and k be positive integers such that $n \geq 8$ and $k < n \log 2/\log n$. Let p be a prime number with $n/2 < p < n-2$. Then $\mathrm{Gal}_{\mathbb{Q}}(T_{n,p,k}) = S_n$.*

Setting $s = p$, $a = p^{n(n-1-p)}$ and $b = n^p p^{n^2}$ gives the second trinomials as follows:

$$S_{n,p}(x) := x^n + p^{n(n-1-p)} n^p x^p + n^p p^{n^2}.$$

We have the second main result of this paper as follows:

Theorem 1.2. *Let n be an integer greater than 8 and let p be a prime number with $n/2 < p < n-2$. Then $\mathrm{Gal}_{\mathbb{Q}}(S_{n,p}) = S_n$.*

Letting $s = n-p$, $a = pn$ and $b = pn^2$ yields the third trinomials as follows:

$$E_{n,p}(x) := x^n + pnx^{n-p} + pn^2.$$

This is an Eisenstein trinomial. The third main result is given in the following:

Theorem 1.3. *Let n be an integer greater than 8 and let p be a prime number with $n/2 < p < n-2$. Then $\mathrm{Gal}_{\mathbb{Q}}(E_{n,p}) = S_n$.*

The existence of the prime number p between $n/2$ and $n-2$ for each $n \geq 8$ is guaranteed by Chebyshev's result in [3]. As one sees clearly that the coefficients a and b of the trinomials $T_{n,p,k}(x)$, $S_{n,p}(x)$ and $E_{n,p}(x)$ are not coprime, our results can be viewed as an extension of Theorem 2 of [4].

The paper is organized as follows. Section 2 is devoted to some preliminary lemmas. We give the proof of Theorem 1.1 in Section 3. In Section 4, we present the proof of Theorems 1.2 and 1.3.

2. Preliminary lemmas

In this section, we present some definitions and preliminary lemmas.

Definition 2.1. The *p-adic valuation* of an integer m with respect to p, denoted by $v_p(m)$, is defined as

$$v_p(m) = \begin{cases} \max\{k : p^k \mid m\} & \text{if } m \neq 0, \\ \infty & \text{if } m = 0. \end{cases}$$

Obviously, this definition can extend to the rational field $\mathbb{Q}$ and the local field $\mathbb{Q}_p$ naturally. We recall the definition of p-adic Newton polygons.

Definition 2.2. The *p-adic Newton polygon* $NP_p(f)$ of a polynomial $f(x) = \sum_{j=0}^{n} c_j x^j \in \mathbb{Q}[x]$ is the lower convex hull of the set $S_p(f) = \{(j, v_p(c_j)) \mid 0 \leq j \leq n\}$.

Evidently, the p-adic Newton polygon is the highest polygonal line passing on or below the points in $S_p(f)$.

The vertices $(x_0, y_0), (x_1, y_1), \ldots, (x_r, y_r)$, where the slope of the Newton polygon changes are called the *corners* of $NP_p(f)$; their x-coordinates $0 = x_0 < x_1 < ... < x_r = n$ are the *breaks* of $NP_p(f)$; the lines connected two vertices are called the *segments* of $NP_p(f)$. We also need the following result on the p-adic Newton polygon.

Lemma 2.3. [6] (Main theorem of p-adic Newton polygon). *Let $(x_0, y_0), (x_1, y_1), ..., (x_r, y_r)$ denote the successive vertices of $NP_p(f)$. Then there exist polynomials $f_1, ..., f_r$ in $\mathbb{Q}_p[x]$ such that*

(i) $f(x) = f_1(x) f_2(x) \cdots f_r(x)$*;*

(ii) *the degree of f_i is $x_i - x_{i-1}$;*

(iii) *all the roots of f_i in $\overline{\mathbb{Q}_p}$ have p-adic valuations $-\frac{y_i - y_{i-1}}{x_i - x_{i-1}}$.*

The following lemma is a generalization of the well-known Eisenstein irreducibility criterion over $\mathbb{Q}_p$. It provides an upper bound for the number of irreducible factors of a polynomial over $\mathbb{Q}_p$ according to its p-adic Newton polygon.

Lemma 2.4. *Let (x_{i-1}, y_{i-1}) and (x_i, y_i) be two consecutive vertices of $NP_p(f)$, and let $d_i = \gcd(x_i - x_{i-1}, y_i - y_{i-1})$. Then for each i, $f_i(x)$ has at most d_i irreducible factors in $\mathbb{Q}_p$ and the degree of the factors of $f_i(x)$ is a multiple of $\frac{x_i - x_{i-1}}{d_i}$. Particularly, if $d_i = 1$, then $f_i(x)$ is irreducible over $\mathbb{Q}_p$.*

Proof. Let $x_i - x_{i-1} = u_i$ and $y_i - y_{i-1} = v_i$. By Lemma 2.3, we have $\deg f_i = u_i$ and all the roots of $f_i(x)$ in $\overline{\mathbb{Q}_p}$ have p-adic valuations $-\frac{v_i}{u_i}$. Let $h(x) \in \mathbb{Q}_p[x]$ with $\deg h(x) = t$ such that $h(x) \mid f_i(x)$, and $\alpha_1, ..., \alpha_t$ be roots of $h(x)$ in $\overline{\mathbb{Q}_p}$. Since $h(0) \in \mathbb{Q}_p$, we have

$$v_p\Big(\prod_{j=1}^{t} \alpha_j\Big) = v_p((-1)^t h(0)) \in \mathbb{Z}.$$

Noticing that for each i and j, we have $v_p(\alpha_i) = v_p(\alpha_j)$. Therefore we derive that $\frac{-tv_i}{u_i} \in \mathbb{Z}$. Since $\gcd(u_i, v_i) = d_i$, one writes $u_i = u_i' d_i, v_i = v_i' d_i$, where $\gcd(u_i', v_i') = 1$. It follows that $u_i' \mid t$, and one claims that the degree of every factor of $f_i(x)$ is a multiple of u_i'. Since $u_i = u_i' d_i$, it follows that $f_i(x)$ has at most d_i irreducible factors in $\mathbb{Q}_p$.

This finishes the proof of Lemma 2.4. □

For a trinomial and a fixed prime number p, the p-adic Newton polygon of this trinomial has at most three vertices, so one can compute its p-adic Newton polygon easily. The following definition and lemma play an important role in computing the Galois group of a polynomial. Actually, this lemma presents the information of the Galois group of an irreducible polynomial over $\mathbb{Q}$.

Definition 2.5. Given $f \in \mathbb{Q}[x]$, let $\mathcal{N}_f$ be the least common multiple of the denominators (in lowest terms) of all slopes of the p-adic Newton polygon $NP_p(f)$ as p ranges over all primes. Such $\mathcal{N}_f$ is called the *Newton index* of f.

Lemma 2.6. [7] *For any irreducible polynomial $f \in \mathbb{Q}[x]$ of degree n, $\mathcal{N}_f$ divides the order of* $\mathrm{Gal}_{\mathbb{Q}}(f)$*. Moreover, if $\mathcal{N}_f$ has a prime divisor p in the range $\frac{n}{2} < p < n-2$, then* $\mathrm{Gal}_{\mathbb{Q}}(f)$ *contains the alternating group A_n.*

To determine whether the Galois group of a polynomial is A_n or S_n, we need the results on the discriminant of polynomials. First of all, we present some facts about the discriminant in general. Let $f(x) \in F[x]$ be a given monic polynomial of degree n, and let $\alpha_1, ..., \alpha_n$ be all the roots of $f(x)$ over the field F. Then

$$\mathrm{Disc}_F(f) := \prod_{1\le i<j\le n} (\alpha_i - \alpha_j)^2$$

is called the *discriminant* of $f(x)$ over F.

Lemma 2.7. [5] *Let $f(x) \in F[x]$ be a polynomial of degree n. Then each of the following holds:*
(i) $\mathrm{Gal}_F(f)$ *is transitive if and only if $f(x)$ is irreducible over F.*
(ii) *If* $\mathrm{char}(F) \neq 2$*, then* $\mathrm{Gal}_F(f) \subseteq A_n$ *if and only if* $\mathrm{Disc}_F(f)$ *is a square in F.*

The following formula about the discriminant of an arbitrary trinomial over $\mathbb{Q}$ is due to Swan.

Lemma 2.8. [13] *Let $n > s > 0$ and $d = \gcd(n, s)$. Write $n = n_1 d$, $s = s_1 d$, where* $\gcd(n_1, s_1) = 1$*. For any $a, b \in \mathbb{Q}$, we have*

$$\mathrm{Disc}_{\mathbb{Q}}(x^n + ax^s + b) = (-1)^{\frac{n(n-1)}{2}} b^{s-1}(n^{n_1} b^{n_1-s_1} + (-1)^{n_1+1}(n-s)^{n_1-s_1} s^{s_1} a^{n_1})^d.$$

Lemma 2.8 gives an explicit formula for the discriminant of a trinomial. Making the use of this formula, we will show that the discriminants of $T_{n,p,k}(x)$, $S_{n,p}(x)$ and $E_{n,p}(x)$ are non-square, which are the following lemmas.

Lemma 2.9. *Let $n \ge 8$ be a positive integer. Let p be an arbitrary prime number satisfying $n/2 < p < n-2$. For any positive integer k, the discriminant* $\mathrm{Disc}_{\mathbb{Q}}(T_{n,p,k})$ *is not a square.*

Proof. By Lemma 2.8 and the definition of $T_{n,p,k}(x)$, we have

$$\begin{aligned}\mathrm{Disc}_{\mathbb{Q}}(T_{n,p,k}) =&(-1)^{\frac{n(n-1)}{2}} n^{k(p-1)} p^{nk(p-1)}(n^{n+k(n-p)} p^{nk(n-p)} \\ &+ (-1)^{n+1}(n-p)^{n-p} n^{nk} p^{nk(n-p)+p-nk}).\end{aligned}$$

Since p is an odd prime, it follows that $n^{k(p-1)}p^{nk(p-1)}$ is a square. To show that $\mathrm{Disc}_{\mathbb{Q}}(T_{n,p,k})$ is not a square, it is sufficient to show that

$$D := (-1)^{\frac{n(n-1)}{2}}(n^{n+k(n-p)} p^{nk(n-p)} + (-1)^{n+1}(n-p)^{n-p} n^{nk} p^{nk(n-p)+p-nk}) \tag{2.1}$$

is not a square. Since $p - nk < 0$, by the isosceles triangle principle, we have

$$v_p(D) = \min\{nk(n-p), nk(n-p) + p - nk\} = (n-1-p)nk + p. \tag{2.2}$$

Noticing that p is an odd prime, by (2.2), one knows that if nk is even, then $v_p(D)$ is odd. Hence D is not a square if either n or k is even. In the following, we assume that both of n and k are odd. We consider the following cases.

Case 1. n is not a square. It follows that there exists a prime number l dividing n such that $v_l(n)$ is odd. Noticing that $n - pk < 0$, by (2.1) and the isosceles triangle principle, one has

$$v_l(D) = \min\{(n-p)k + n, nk\}v_l(n) = ((n-p)k + n)v_l(n).$$

Because $n - p$ is even and both of n and $v_l(n)$ are odd, we have that $v_l(D)$ is odd. Therefore D is not a square in this case.

Case 2. n is a square. Then $n \equiv 1 \pmod 4$. By (2.1), we have

$$D = n^{nk} p^{nk(n-p)} (n^{n-kp} + (n-p)^{n-p} p^{p-nk}).$$

Since n is a square and $n - p$ is even, it follows that $n^{nk} p^{nk(n-p)}$ is a square. So it is sufficient to show that

$$D_k := n^{n-kp} + (n-p)^{n-p} p^{p-nk} \tag{2.3}$$

is not a square.

If $k = 1$, multiple the square number p^{n-p} to D_1, we have

$$\begin{aligned}
(n^{\frac{n-p}{2}} p^{\frac{n-p}{2}})^2 &< (n^{\frac{n-p}{2}} p^{\frac{n-p}{2}})^2 + (n-p)^{n-p} = n^{n-p} p^{n-p} + (n-p)^{n-p} = D_1 \\
&< (n^{\frac{n-p}{2}} p^{\frac{n-p}{2}})^2 + n^{\frac{n-p}{2}} p^{\frac{n-p}{2}} \\
&< (n^{\frac{n-p}{2}} p^{\frac{n-p}{2}})^2 + 2n^{\frac{n-p}{2}} p^{\frac{n-p}{2}} + 1 = (n^{\frac{n-q}{2}} p^{\frac{n-p}{2}} + 1)^2.
\end{aligned}$$

This implies that D_1 lies strictly between the squares of two consecutive integer. It follows that D_k is not a square for $k = 1$.

Now we may let $k > 1$. Then $n - pk < 0$ and $p - nk < 0$. Noticing that k, n, p are odd numbers, it follows that $n - pk$, $p - nk$ are even numbers and $n^{pk-n} p^{nk-p}$ is a square. Multiplying $n^{pk-n} p^{nk-p}$ to D_k, it is sufficient to show that

$$p^{nk-p} + (n-p)^{n-p} n^{n-kp}$$

is not a square. Suppose that there exists a positive integer z satisfying that

$$p^{nk-p} + (n-p)^{n-p} n^{n-kp} = z^2.$$

Since n, k and p are odd, we may let $p^{nk-p} = a_0^2$ and $(n-p)^{n-p} n^{n-kp} = b_0^2$. Thus $a_0^2 + b_0^2 = z^2$ and so $a_0^2 = (z + b_0)(z - b_0)$. Since $\gcd(p, n) = 1$, one has $\gcd(a_0, b_0) = \gcd(a_0, z) = \gcd(b_0, z) = 1$. Noticing that $z + b_0$ is odd, one has

$$\gcd(z + b_0, z - b_0) = \gcd(z + b_0, 2z) = \gcd(z + b_0, z) = \gcd(b_0, z) = 1.$$

But $a_0 = p^{\frac{nk-p}{2}}$ is a power of p, by unique factorization, it follows that $z + b_0 = a_0^2$ and $z - b_0 = 1$. This implies that $a_0^2 = 2b_0 + 1$, i.e. we have

$$p^{nk-p} = 2(n-p)^{\frac{n-p}{2}} n^{\frac{pk-n}{2}} + 1. \tag{2.4}$$

Clearly, one has

$$1 < 2(n-p)^{\frac{n-p}{2}} n^{\frac{pk-n}{2}} + 1 < 4(n-p)^{\frac{n-p}{2}} n^{\frac{pk-n}{2}}.$$

Hence

$$\begin{aligned}\log\left(2(n-p)^{\frac{n-p}{2}} n^{\frac{pk-n}{2}} + 1\right) &< \log\left(4(n-p)^{\frac{n-p}{2}} n^{\frac{pk-n}{2}}\right)\\ &= 2\log 2 + \frac{n-p}{2}\log(n-p) + \frac{pk-n}{2}\log n.\end{aligned} \tag{2.5}$$

Since n is an integer greater than 8 and $n/2 < p$, it follows that $p \geq 5$. Noticing the condition that $n < 2p$, $2 < n-p < p$ and the fact that $\log 2x \leq 2\log x$ for any $x \geq 2$, we have

$$2\log 2 < \log 5 < \frac{n-p}{2}\log p.$$

By (2.5), we derive that

$$\begin{aligned}\log\left(2(n-p)^{\frac{n-p}{2}} n^{\frac{pk-n}{2}} + 1\right) &< 2\log 2 + \frac{n-p}{2}\log(n-p) + \frac{pk-n}{2}\log n\\ &< 2\log 2 + \frac{n-p}{2}\log p + \frac{pk-n}{2}\log 2p\\ &< (n-p)\log p + (pk-n)\log p = (pk-p)\log p\\ &< (nk-p)\log p.\end{aligned}$$

This implies that

$$2(n-p)^{\frac{n-p}{2}} n^{\frac{pk-n}{2}} + 1 < p^{nk-p},$$

which contradicts to (2.4) Therefore D_k is not a square in this case.

Combining all the cases, we complete the proof of Lemma 2.9. □

Lemma 2.10. *Let n be a positive integer greater than* 8. *Let p be a prime satisfying* $n/2 < p < n-2$. *The discriminant* $\mathrm{Disc}_{\mathbb{Q}}(S_{n,p})$ *is not a square.*

Proof. By Lemma 2.8 and the definition of $S_{n,p}(x)$, we have

$$\begin{aligned}\mathrm{Disc}_{\mathbb{Q}}(S_{n,p}) =& (-1)^{\frac{n(n-1)}{2}} n^{p(p-1)} p^{n^2(p-1)} \big(n^{pn-p^2+n} p^{n^3-pn^2}\\ &+ (-1)^{n+1}(n-p)^{n-p} n^{np} p^{p+n^3-pn^2-n^2}\big).\end{aligned}$$

Since p is an odd prime, it follows that $n^{p(p-1)}p^{n^2(p-1)}$ is a square. To show that $\mathrm{Disc}_{\mathbb{Q}}(S_{n,k})$ is not a square, it is sufficient to show that

$$D := (-1)^{\frac{n(n-1)}{2}} \left(n^{pn-p^2+n} p^{n^3-pn^2} + (-1)^{n+1}(n-p)^{n-p} n^{np} p^{p+n^3-pn^2-n^2}\right) \tag{2.6}$$

is not a square.

Consider the p-adic valuation of D, by the isosceles triangle principle, we have

$$v_p(D) = \min\{n^3 - pn^2, n^3 - pn^2 - n^2 + p\}.$$

Noticing that $p < n$, we have $v_p(D) = n^3 - pn^2 - n^2 + p$. If n is even, then $n^3 - pn^2 - n^2 + p$ is odd. Thus $v_p(D)$ is odd and D is not a square in this case. In the following, we always assume that n is odd. We consider the following two cases:

Case 1. n is not a square. Then there exists a prime divisor l dividing n such that $v_l(n)$ is odd. So

$$v_l(D) = \min\{pn - p^2 + n, np\}v_l(n) = (pn - p^2 + n)v_l(n).$$

Since $v_l(n)$ and $pn - p^2 + n$ are both odd, $v_l(D)$ is odd in this case.

Case 2. n is a square. Thus $n \equiv 1 \pmod 4$. By (2.6), we have

$$D = n^{pn-p^2+n}p^{n^3-pn^2} + (n-p)^{n-p}n^{np}p^{p+n^3-pn^2-n^2}.$$

Noticing that $p^{n^3-pn^2}$ and n^{pn} are squares, to show that D is not a square, it is sufficient to show that

$$D_0 = n^{n-p^2} + (n-p)^{n-p}p^{p-n^2}$$

is not a square. Multiplying the square number $n^{p^2-n}p^{n^2-p}$ to D_0, it suffices to show that

$$p^{n^2-p} + (n-p)^{n-p}n^{p^2-n}$$

is not a square. Suppose that there exists a positive integer z such that

$$p^{n^2-p} + (n-p)^{n-p}n^{p^2-n} = z^2.$$

Noticing that p^{n^2-p} and $(n-p)^{n-p}n^{p^2-n}$ are squares, letting $a_1^2 = p^{n^2-p}$ and $b_1^2 = (n-p)^{n-p}n^{p^2-n}$ gives $a_1^2 + b_1^2 = z^2$. It follows that $a_1^2 = (z+b_1)(z-b_1)$. One can check that a_1, b_1 and z are pairwise relatively prime and a_1 is a power of p. Thus $z + b_1 = a_1^2$ and $z - b_1 = 1$. It follows that

$$2(n-p)^{\frac{n-p}{2}}n^{\frac{p^2-n}{2}} + 1 = p^{n^2-p}. \tag{2.7}$$

By the same argument as in the proof of Lemma 2.9, we have

$$\begin{aligned}\log\left(2(n-p)^{\frac{n-p}{2}}n^{\frac{p^2-n}{2}} + 1\right) &< 2\log 2 + \frac{n-p}{2}\log(n-p) + \frac{p^2-n}{2}\log n\\ &< 2\log 2 + \frac{n-p}{2}\log p + \frac{p^2-n}{2}\log 2p\\ &< (n-p)\log p + (p^2-n)\log p = (p^2-p)\log p\\ &< (n^2-p)\log p.\end{aligned}$$

This implies that (2.7) cannot hold. Hence D is not a square in this case.

Combing all the cases, we complete the proof of Lemma 2.10. □

Lemma 2.11. *Let $n \geq 8$ be a positive integer. Let p be a prime number satisfying $n/2 < p < n-2$. The discriminant $\mathrm{Disc}_{\mathbb{Q}}(E_{n,p})$ is not a square.*

Proof. By Lemma 2.8 and the definition of $E_{n,p}(x)$, we have

$$\mathrm{Disc}_{\mathbb{Q}}(E_{n,p}) = (-1)^{\frac{n(n-1)}{2}} p^{n-1}(n^{n+2p} + (-1)^{n+1} p^n (n-p)^{n-p} n^n).$$

Let $D = \mathrm{Disc}_{\mathbb{Q}}(E_{n,p})$. If n is even, then $v_p(D) = n-1$ is odd. It implies that D is not a square. In the following, we assume that n is odd. If n is not a square, then exists a prime number l dividing n such that $v_l(n)$ is odd. Hence one derives that $v_l(D) = nv_l(n)$ is odd. This infers that D is not a square again.

Now let n be an odd square. Then $n \equiv 1 \pmod 4$ and it follows that $(-1)^{\frac{n(n-1)}{2}} = 1$. Since n^n and p^{n-1} are square numbers, to show that D is not a square, it is enough to show that $n^{2p} + p^n(n-p)^{n-p}$ is not a square.

Suppose that there exists a positive integer z such that

$$n^{2p} + p^n(n-p)^{n-p} = z^2.$$

It follows that

$$(z + n^p)(z - n^p) = p^n(n-p)^{n-p}.$$

Since $\gcd(n, p(n-p)) = 1$, we have $\gcd(n^p, z) = 1$. Hence

$$\gcd(z + n^p, z - n^p) = \gcd(2z, 2n^p) = 2\gcd(z, n^p) = 2.$$

Since $p > n - p$ and $n > n - p$, we have $p^n > (n-p)^{n-p}$. Noticing that $z + n^p > z - n^p$ and $\gcd(z + n^p, z - n^p) = 2$, we have $2p^n | z + n^p$ which implies that

$$z + n^p \geq 2p^n$$

and

$$z - n^p \leq \frac{1}{2}(n-p)^{n-p}.$$

Hence

$$2n^p \geq 2p^n - \frac{1}{2}(n-p)^{n-p}. \tag{2.8}$$

On the other hand, for fixed $n \geq 9$, we define an auxiliary function F_n as follows:

$$F_n(x) := \log 2 + x \log n - n \log x,$$

where $n/2 < x < n-2$. Noticing that $n \geq 9$ and $n/x < 2$, we have

$$F_n'(x) = \log n - n/x > 2\log 3 - 2 = 0.197... > 0.$$

This shows that the function $F_n(x)$ is a monotone increasing function in the interval $[n/2, n-2]$. Therefore

$$\begin{aligned} F_n(x) < F_n(n-2) &= \log 2 + (n-2)\log n - n\log(n-2) \\ &= \log 2 + (n-2)\log n - (n-2)\log(n-2) - 2\log(n-2) \\ &= \log 2 + (n-2)\log(1 + \frac{1}{n-2}) - 2\log(n-2). \end{aligned}$$

It is a well-known fact that $\log(1+x) < x$ for any $x > 0$. Hence

$$\begin{aligned}&\log 2 + (n-2)\log(1+\frac{1}{n-2}) - 2\log(n-2)\\ &< \log 2 + 1 - 2\log(n-2)\\ &\leq \log 2 + 1 - 2\log 7 = -2.198... < 0,\end{aligned}$$

which implies that $F_n(x) < 0$ for all x with $n/2 < x < n-2$. Noticing that

$$\frac{2n^x}{x^n} = \exp(F_n(x)),$$

it follows that $2n^x < x^n$ for all x with $n/2 < x < n-2$ when $n \geq 9$. Since $p^n > (n-p)^{n-p}$, one has

$$2n^p < p^n + p^n - (n-p)^{n-p} < 2p^n - \frac{1}{2}(n-p)^{n-p},$$

which contradicts to (2.8). Such z does not exist and this completes the proof of Lemma 2.11. □

3. Proof of Theorem 1.1

In this section, we provide the proof of Theorem 1.1.

Proof of Theorem 1.1. Since $k < \frac{n\log 2}{\log n}$ and $n \geq 8$, we have $k < \frac{n\log 2}{\log 8} = \frac{n}{3}$. Noticing that $\frac{n}{2} < p < n-2$, we have $k < p$ that implies that $\gcd(k,p) = 1$.

We first prove that $T_{n,p,k}(x)$ is irreducible over $\mathbb{Q}$. Consider the p-adic Newton polygon of $T_{n,p,k}(x)$. Since $n-1-p < n-p$, the point $(p,(n-1-p)k)$ lies below the segment connecting the points $(0,nk)$ and $(n,0)$. Hence the p-adic Newton polygon of $T_{n,p,k}(x)$ has vertices as follows:

$$(0,nk),\ (p,(n-1-p)k),\ (n,0).$$

The first segment of the p-adic Newton polygon of $T_{n,p,k}(x)$ has slope

$$\frac{nk-(n-1-p)k}{0-p} = -\frac{nk-(n-1-p)k}{p} = -k - \frac{k}{p}.$$

The second segment of the p-adic Newton polygon of $T_{n,p,k}(x)$ has slope

$$\frac{(n-1-p)k-0}{p-n} = -\frac{(n-1-p)k}{n-p} = -k + \frac{k}{n-p}.$$

By Lemma 2.3 (i), we have $T_{n,p,k}(x) = F_1(x)F_2(x)$ in $\mathbb{Q}_p$, where $\deg F_1(x) = p$ and $\deg F_2(x) = n-p$. Since $\gcd(k,p) = 1$, by Lemma 2.4, it follows that $F_1(x)$ is irreducible over $\mathbb{Q}_p$. Let $\gcd(k,n-p) = d_0$, by Lemma 2.4, $F_2(x)$ has at most d_0 prime factors in $\mathbb{Q}_p$. If $T_{n,p,k}(x)$ is reducible over $\mathbb{Q}$, then $T_{n,p,k}(x)$ is reducible over $\mathbb{Z}$. Let

$$T_{n,p,k}(x) = F(x)G(x),$$

where $\deg F(x) \leq n/2$ and $\deg G(x) \geq n/2$. By the local-global principle, $F(x)$ and $G(x)$ can also be seen as polynomials over $\mathbb{Q}_p$. But we already have proved that $T_{n,p,k}(x) = F_1(x)F_2(x)$ in $\mathbb{Q}_p$, where

$\deg F_1(x) = p$. Hence we derives that $\deg G(x) \geq p$ and $\deg F(x) \leq n - p$. By Lemma 2.4 again, we have

$$\deg F(x) = \frac{(n-p)t}{d_0},$$

where $1 \leq t \leq d_0$.

For any prime number l dividing n, we consider the l-adic Newton polygon of $T_{n,p,k}(x)$. The l-adic Newton polygon of $T_{n,p,k}(x)$ has the vertices as follows:

$$(0, kv_l(n)),\ (n, 0).$$

By Lemma 2.3 (iii), each root of $T_{n,p,k}(x)$ in $\mathbb{Q}_l$ has l-adic valuation

$$-\frac{kv_l(n) - 0}{0 - n} = \frac{kv_l(n)}{n}.$$

Since $F(x)$ is a prime factor of $T_{n,p,k}(x)$ in $\mathbb{Q}$, it is also a prime factor of $T_{n,p,k}(x)$ in $\mathbb{Q}_l$ by the local-global principle. Noticing that $F(0) \in \mathbb{Z}$, we have $v_l(F(0))$ is a nonnegative integer. Moreover, by Vieta's Theorem and $(n-p)tkv_l(n) > 0$, we have

$$v_l(F(0)) = \deg F(x) \cdot \frac{kv_l(n)}{n} = \frac{(n-p)tkv_l(n)}{d_0 n} \in \mathbb{Z}^+. \tag{3.1}$$

Letting $k = ud_0$, by (3.1) we have

$$\frac{(n-p)tkv_l(n)}{d_0 n} = \frac{(n-p)tuv_l(n)}{n} \in \mathbb{Z}^+.$$

Since $\gcd(n, n-p) = \gcd(n, p) = 1$, one has

$$tuv_l(n) \in n\mathbb{Z}^+. \tag{3.2}$$

Since $tu \leq k$ and

$$v_l(n) \leq \frac{\log n}{\log l} \leq \frac{\log n}{\log 2},$$

we have

$$tu\frac{v_l(n)}{n} \leq k\frac{\log n}{n \log 2}.$$

By the condition that $k < \frac{n \log 2}{\log n}$, one has $tu\frac{v_l(n)}{n} < 1$ which contradicts to (3.2). Therefore the irreducibility of $T_{n,p,k}(x)$ over $\mathbb{Q}$ is proved.

Since $\gcd(k, p) = 1$, the first segment of the p-adic Newton polygon of $T_{n,p,k}$ indicates that $p | \mathcal{N}_{T_{n,p,k}}$. By Lemma 2.6, we have $A_n \subseteq \mathrm{Gal}_{\mathbb{Q}}(T_{n,p,k})$. It is a well-known fact that the Galois group of a polynomial of degree n is a subgroup of S_n. So

$$A_n \subseteq \mathrm{Gal}_{\mathbb{Q}}(T_{n,p,k}) \subseteq S_n.$$

By Lemma 2.9, the discriminant $\mathrm{Disc}_{\mathbb{Q}}(T_{n,p,k})$ is not a square. By Lemma 2.7, we have $\mathrm{Gal}_{\mathbb{Q}}(T_{n,p,k}) \nsubseteq A_n$. It then follows that $\mathrm{Gal}_{\mathbb{Q}}(T_{n,p,k}) = S_n$.

This completes the proof of Theorem 1.1. $\square$

4. Proofs of Theorems 1.2 and 1.3

In this section, we give the proofs of Theorems 1.2 and 1.3.

Proof of Theorem 1.2. We first prove the irreducibility of $S_{n,p}(x)$. Consider the p-adic Newton polygon of $S_{n,p}(x)$ which holds the following vertices:

$$(0, n^2), (p, n(n-1-p)), (n, 0).$$

The slope of the first segment of p-adic Newton polygon of $S_{n,p}(x)$ is

$$\frac{n(n-1-p)-n^2}{p-0} = -\frac{n+np}{p}.$$

The slope of the second segment of p-adic Newton polygon of $S_{n,p}(x)$ is

$$\frac{0-n(n-1-p)}{n-p} = \frac{np+n-n^2}{n-p}.$$

Noticing that $\gcd(n, n-p) = 1$ and $\gcd(n^2-n-np, n-p) = \gcd(n, n-p) = 1$, by Lemma 2.4 we have $S_{n,p}(x) = F_1(x)F_2(x)$ in $\mathbb{Q}_p$, where $F_1(x)$ and $F_2(x)$ are both irreducible over $\mathbb{Q}_p$ with $\deg F_1(x) = p$ and $\deg F_2(x) = n-p$. By the local-global principle, one knows that if $S_{n,p}(x)$ is reducible over $\mathbb{Q}$, then $S_{n,p}(x) = f_1(x)f_2(x)$ with $\deg f_1(x) = p$ and $\deg f_2(x) = n-p$.

Let l be an arbitrary prime divisor of n. Now let us consider the l-adic Newton polygon of $S_{n,p}(x)$. Then it has the vertices $(0, pv_l(n))$, $(n, 0)$. By Lemma 2.3 (iii), every root of $S_{n,p}(x)$ in $\mathbb{Q}_l$ has l-adic valuation

$$-\frac{0-pv_l(n)}{n-0} = \frac{pv_l(n)}{n}.$$

Noticing that $v_l(f_1(0)) \in \mathbb{Z}$, we have $p^2v_l(n) \in n\mathbb{Z}$. Since $\gcd(n, p) = 1$ and $v_l(n) < n$, we have

$$p^2v_l(n) \notin n\mathbb{Z}.$$

We arrive at a contradiction and this proves the irreducibility of $S_{n,p}(x)$. The slope of the first segment of the p-adic Newton polygon of $S_{n,p}(x)$ indicates that $p|\mathcal{N}_{S_{n,p}}$, by Lemma 2.6, we have $A_n \subseteq \mathrm{Gal}_{\mathbb{Q}}(S_{n,p})$. By Lemma 2.10 and Lemma 2.7, we have $\mathrm{Gal}_{\mathbb{Q}}(S_{n,p}) \nsubseteq A_n$. By the fact that $A_n \subseteq \mathrm{Gal}_{\mathbb{Q}}(S_{n,p}) \subseteq S_n$, we have $\mathrm{Gal}_{\mathbb{Q}}(S_{n,p}) = S_n$.

This finishes the proof of Theorem 1.2. □

Proof of Theorem 1.3. Since $E_{n,p}(x)$ is an Eisenstein polynomial, $E_{n,p}(x)$ is irreducible over $\mathbb{Q}$. Let q be a prime divisor of n. Consider the q-adic Newton polygon of $E_{n,p}(x)$ that has the vertices as follows:

$$(0, 2v_q(n)),\ (n-p, v_q(n)),\ (n, 0).$$

Consider the segment connected the vertices $(n-p, v_q(n))$ and $(n, 0)$. The slope of this segment is

$$\frac{0-v_q(n)}{n-(n-p)} = -\frac{v_q(n)}{p}.$$

Noticing that

$$v_q(n) \le \frac{\log n}{\log q} \le \frac{\log n}{\log 2} \le \frac{n}{2} < p,$$

it follows that $\gcd(v_q(n), p) = 1$. Thus $p|\mathcal{N}_{E_{n,p}}$. By Lemma 2.6, we have $A_n \subseteq \mathrm{Gal}_{\mathbb{Q}}(E_{n,p})$. By Lemmas 2.11 and 2.7, we have $\mathrm{Gal}_{\mathbb{Q}}(E_{n,p}) \nsubseteq A_n$. It then follows that $\mathrm{Gal}_{\mathbb{Q}}(S_{n,p}) = S_n$.

This concludes the proof of Theorem 1.3. □

5. Conclusions

Uchida [14] and Yamamoto [15] proved that the Galois group of the polynomial $x^n + ax + b \in \mathbb{Z}[x]$ over $\mathbb{Q}$ is S_n under certain conditions. Cohen, Movahhedi and Salinier [4] showed that if the trinomials $f(x) = x^n + ax^s + b$ with integral coefficients is irreducible, where $\gcd(nb, as(n-s)) = 1$ with s being a prime number such that $s \neq n-1$ and there is a prime divisor p of b such that $\gcd(s, v_p(b)) = 1$, then $\mathrm{Gal}_{\mathbb{Q}}(f)$ contains A_n. They also determined what $\mathrm{Gal}_{\mathbb{Q}}(f)$ could be if $A_n \nsubseteq \mathrm{Gal}_{\mathbb{Q}}(f)$ under certain conditions. In this paper, we mainly discussed the Galois group of the following three special class of trinomials:

$$T_{n,p,k}(x) := x^n + n^k p^{(n-1-p)k} x^p + n^k p^{nk},$$

$$S_{n,p}(x) := x^n + p^{n(n-1-p)} n^p x^p + n^p p^{n^2}$$

and

$$E_{n,p}(x) := x^n + pnx^{n-p} + pn^2.$$

By using the p-adic Newton polygon, we showed that all these trinomials are irreducible over $\mathbb{Q}$ and have the Galois group S_n. Our results strengthen and extend the theorem of Cohen, Movahhedi and Salinier.

Acknowledgements

S. F. Hong is the corresponding author and was supported partially by National Science Foundation of China Grant #11771304.

The authors would like to thank the anonymous referees for their careful reading and helpful suggestions that improve the presentation of the paper.

Conflict of interest

We declare that we have no conflict of interest.

References

1. B. Bensebaa, A. Movahhedi, A. Salinier, The Galois group of $X^p + aX^s + a = 0$, *Acta Arith.*, **134** (2008), 55–65. doi: 10.4064/aa134-1-4.
2. B. Bensebaa, A. Movahhedi, A. Salinier, The Galois group of $X^p + aX^{p-1} + a = 0$, *J. Number Theory*, **129** (2009), 824–830. doi: 10.1016/j.jnt.2008.09.017.

3. P. I. Chebyshev, Sur la fonction qui détermine la totalité des nombres premiers inférieurs à une limite donnée, *J. Math. Pures Appl.*, **17** (1852), 341–365.

4. S. D. Cohen, A. Movahhedi, A. Salinier, Galois group of trinomials, *J. Algebra*, **222** (1999), 561–573. doi: 10.1006/jabr.1999.8033.

5. P. A. Grillet, *Abstract algebra*, Vol. 242, New York: Springer, 2007.

6. F. Hajir, Algebraic properties of a family of generalized Laguerre polynomials, *Can. J. Math.*, **61** (2009), 583–603. doi: 10.4153/CJM-2009-031-6.

7. F. Hajir, On the Galois group of generalized Laguerre polynomials, *J. Théorie Nombres Bordeaux*, **17** (2005), 517–525.

8. A. Movahhedi, Galois group of $X^p + aX + a = 0$, *J. Algebra*, **180** (1996), 966–975. doi: 10.1006/jabr.1996.0104.

9. K. Komatsu, On the Galois group of $x^p + ax + a = 0$, *Tokyo J. Math*, **14** (1991), 227–229. doi: 10.3836/tjm/1270130502.

10. K. Komatsu, On the Galois group of $x^p + p^t b(x + 1) = 0$, *Tokyo J. Math*, **15** (1992), 351–356. doi: 10.3836/tjm/1270129460.

11. K. Ohta, On unramified Galois extensions of quadratic number fields (in Japanese), *Sügaku*, **24** (1972), 119–120.

12. H. Osada, The Galois group of the polynomials $x^n + ax^l + b$, *J. Number Theory*, **25** (1987), 230–238. doi: 10.1016/0022-314X(87)90029-1.

13. R. G. Swan, Factorization of polynomials over finite fields, *Pacific J. Math.*, **12** (1962), 1099–1106. doi: 10.2140/pjm.1962.12.1099.

14. K. Uchida, Unramified extentions of quadratic number fields II, *Tohoku. Math. J.*, **22** (1970), 220–224. doi: 10.2748/tmj/1178242816.

15. Y. Yamamoto, On unramified Galois extensions of quadratic number fields, *Osaka J. Math.*, **7** (1970), 57–76.

AIMS Press