ACTA ARITHMETICA
185.4 (2018)

Computing Galois groups of certain families of polynomials

by

Khosro Monsef Shokri, Jafar Shaffaf and Reza Taleb (Tehran)

1. Introduction. Computing the Galois groups of polynomials with integer coefficients is a classical problem in algebra and number theory. Although a probabilistic argument shows that the Galois group of a random irreducible polynomial of degree n is the full symmetric group S_n, there is no algorithm to compute the Galois group of a specific polynomial. In 1897, Hilbert proved the existence of extensions of $\mathbb{Q}$ with Galois group S_n for any positive integer n. In 1930, Schur explicitly constructed such extensions. More precisely, he proved that the Galois group of the splitting field of the truncated exponential polynomial of degree n is the full symmetric group S_n if $n \not\equiv 0 \pmod 4$, and the alternating group A_n otherwise.

There are some classical results for computing the Galois group G_f of the splitting field of an irreducible polynomial $f(x) \in \mathbb{Z}[x]$ of degree n over $\mathbb{Q}$. For instance, if n is prime and $f(x)$ has exactly two imaginary roots then $G_f \simeq S_n$. The idea of these classical results is mainly based on the Dedekind theorem which predicts the existence of a permutation in G_f with a certain type depending on the factorization of $f(x)$ modulo a prime number. For polynomials with small degrees one can easily compute the Galois groups using the Dedekind theorem and also using another method based on the corresponding resolvent polynomials (this method is examined for polynomials up to degree 7 in [11]). But, what if one takes a family of polynomials with no restriction on their degrees?

The first interesting such family is the trinomials $f(x) = x^n + ax^s + b$. Osada ([7], [8]), Cohen, Movahhedi, Salinier (see for example [1], [2], [3], [5], [6]) and others used another approach to this problem. The main idea in this approach is to compute an explicit formula for the discriminant and then find the inertia groups of primes dividing the discriminant. Then by

2010 *Mathematics Subject Classification*: Primary 11R32; Secondary 11R29, 11S15.
Key words and phrases: Galois theory, discriminant, ramification.
Received 14 October 2017; revised 9 January 2018.
Published online 8 October 2018.

DOI: 10.4064/aa171014-26-2

using a theorem of Minkowski, which says that all non-trivial extensions of $\mathbb{Q}$ are ramified, one finds that the subgroup generated by all the inertia groups of primes of the splitting field N of $f(x)$ sitting above the primes dividing the discriminant of N—which is the same as the discriminant of $f(x)$ modulo a perfect square—equals the Galois group G_f. Furthermore, Cohen, Movahhedi and Salinier were the first to notice that primitivity plays an essential role in computing such Galois groups.

Although in the case of trinomials there is an explicit formula for the discriminant by Swan [12], there is no explicit formula for the discriminant of a general quadrinomial. After reviewing some basic lemmas in Section 2, in the first part of Section 3 we first compute an explicit formula for the discriminant of quadrinomials of the form

$$f(x) = x^n + ax^{n-1} + bx^{n-2} + c \in \mathbb{Z}[x]$$

with $a^2 = 4b$.

In the rest of Section 3 we use the factorization of the derivative polynomial $f'(x)$ modulo different primes dividing the discriminant to obtain the corresponding inertia groups, and finally we show that the Galois group G_f of the irreducible polynomial $f(x) = x^n + ax^{n-1} + bx^{n-2} \pm 1 \in \mathbb{Z}[x]$ with $a^2 = 4b$ and $\gcd(n, a) = 1$ equals S_n (Theorem 3.1). It is worth mentioning that determining the irreducibility of polynomials is another problem of independent interest. In Section 3 we also provide an infinite family of irreducible quadrinomials of the form $f(x) = x^n + ax^{n-1} + bx^{n-2} \pm 1 \in \mathbb{Z}[x]$ with $a^2 = 4b$ and $\gcd(n, a) = 1$.

When $n = \ell$ is an odd prime, the Cauchy theorem implies the existence of a cycle of length ℓ in G_f. So it is enough to find a transposition to have the full symmetric group as the Galois group. In the last part of Section 3 we find such a transposition to conclude that the Galois group of any irreducible polynomial of the form $f(x) = x^\ell + ax^{\ell-1} + bx^{\ell-2} + c \in \mathbb{Z}[x]$ with $a^2 = 4b$ is S_ℓ provided that $\gcd(2a(\ell-2), c\ell) = 1$ and $(-1)^{\ell-2}4(a/2)^\ell(\ell-2)^{\ell-2} + \ell^\ell c$ is not a perfect square, e.g. $\ell c \not\equiv 1 \pmod 4$ (see Theorem 3.2). We also provide infinitely many examples of quadrinomials satisfying these hypotheses.

The way the derivative $f'(x)$ factors over the rationals is crucial to our arguments. Proceeding backwards, by constructing polynomials from the favorite derivative polynomials, in Section 4 we also extend our arguments to show that the Galois group G_f of any irreducible polynomial with an arbitrary number of terms of the form

$$\begin{aligned} f(x) = x^{n+k+1} - \binom{k}{1}(k+1)x^{n+k} + \binom{k}{2}(k+1)^2x^{n+k-1} - \cdots \\ + (-1)^k\binom{k}{k}(k+1)^kx^{n+1} + c \in \mathbb{Z}[x] \end{aligned}$$

is S_{n+k+1} if either $c = \pm 1$ and $\gcd(n+k+1, nk) = 1$, or $n+k+1$ is prime, $\gcd(c, (k+1)(n+1)k)$ and $(-1)^k(k+1)^{n+k+1}(n+1)^{n+1}k^k + c(n+k+1)^{n+k+1}$ is not a perfect square (Theorems 4.2 and 4.3).

In the last section we consider the general irreducible quadrinomial of the form $f(x) = x^n + ax^{n-1} + bx^{n-2} + c \in \mathbb{Z}[x]$ (not necessarily with $a^2 = 4b$). Although G_f seems to have several possibilities in the case $a^2 \neq 4b$, using the formula for the discriminant we show that if $n = \ell$ is an odd prime of the form $4k+1$ and the coefficients a, b and c are all odd, then $G_f \simeq S_\ell$ (Theorem 5.1). An infinite family of such irreducible quadrinomials is indicated.

2. Some basic lemmas. In this section we gather some tools on permutation and Galois groups. Throughout this section let $f(x)$ be a monic polynomial with integer coefficients of degree n, and let N be the splitting field of $f(x)$ with Galois group G_f over $\mathbb{Q}$. A theorem of Minkowski says that all non-trivial extensions of $\mathbb{Q}$ are ramified, and this implies the following lemma:

LEMMA 2.1. *The Galois group G_f is generated by all inertia groups $I_{\mathfrak{P}/p}$ over prime ideals $\mathfrak{P}$ of N sitting above prime numbers p.*

Therefore, to compute G_f it is enough to compute all inertia groups of primes of N. But we know that these inertia groups are all trivial except for the primes sitting above the ramified ones in N. On the other hand, the ramified primes of $\mathbb{Q}$ in N are exactly the primes dividing the discriminant d_N of the field N, which satisfies the equality

$$\mathrm{disc}(f) = [\mathcal{O}_N : \mathbb{Z}]^2 d_N \tag{2.1}$$

where $\mathrm{disc}(f)$ is the discriminant of the polynomial $f(x)$, and $\mathcal{O}_N$ is the ring of integers of N.

So to compute G_f one needs to determine the inertia groups of primes of N sitting above the primes dividing d_N. The following lemma is fundamental for our purpose:

LEMMA 2.2 ([7, Lemma 1]). *Let p be a prime number and let $\mathfrak{P}$ be a prime ideal of N sitting above p. If $f(x) \equiv (x-c)^2\bar{h}(x) \pmod{p}$ for some $c \in \mathbb{Z}$ and a separable polynomial $\bar{h}(x) \in \mathbb{F}_p[x]$ such that $\bar{h}(c) \not\equiv 0 \pmod{p}$, then the inertia group of $I_{\mathfrak{P}/p}$ is either trivial or a group generated by a transposition.*

Since the Galois group of $f(x)$ as a subgroup of S_n is transitive, we will use the following elementary lemma in the next section:

LEMMA 2.3 ([10, Lemma 4.4.4]). *Any transitive subgroup of S_n which is generated by transpositions is the full group S_n.*

Furthermore, in case $n = \ell$ is prime, we will also use the following elementary lemma:

LEMMA 2.4. *Let ℓ be a prime number. Any permutation subgroup of S_ℓ generated by a transposition and a cycle of length ℓ is the full group S_ℓ.*

3. Galois groups of $x^n + ax^{n-1} + bx^{n-2} + c$ with $a^2 = 4b$. In this section we first compute the discriminant of any polynomial of the form

$$f(x) = x^n + ax^{n-1} + bx^{n-2} + c \in \mathbb{Q}[x]$$

with $a^2 = 4b$. Its derivative

$$f'(x) = x^{n-3}(nx^2 + a(n-1)x + b(n-2))$$

has the following rational roots:

$$x_1 = \cdots = x_{n-3} = 0, \qquad x_{n-2} = -a/2, \qquad x_{n-1} = -a/2 + a/n.$$

To do this we first take the product of the values of $f(x)$ over all roots of $f'(x)$:

$$\begin{aligned} \operatorname{disc}(f) &= (-1)^{n(n-1)/2} \operatorname{Res}(f, f') \\ &= (-1)^{n(n-1)/2} n^n f(0)^{n-3} f(-a/2) f(-a/2 + a/n) \\ &= (-1)^{n(n-1)/2} n^n c^{n-3} c(a^n(1/n - 1/2)^{n-2}(1/n)^2 + c) \\ &= (-1)^{n(n-1)/2} n^n c^{n-2} \biggl((-1)^{n-2} 4\biggl(\frac{a}{2n}\biggr)^n (n-2)^{n-2} + c\biggr). \end{aligned}$$

Therefore,

$$\operatorname{disc}(f) = (-1)^{n(n-1)/2} c^{n-2} \bigl((-1)^{n-2} 4(a/2)^n (n-2)^{n-2} + n^n c\bigr). \tag{3.1}$$

Let $f(x) = x^n + ax^{n-1} + bx^{n-2} + c \in \mathbb{Z}[x]$ be a quadrinomial such that $a^2 = 4b$. As already mentioned, its derivative has three distinct rational roots $\{0, -a/2, -a/2 + a/n\}$ where $f(-a/2) = f(0) = c$. Let p be a prime number with $p \nmid nc$ and

$$p \mid \operatorname{disc}(f) = (-1)^{n(n-1)/2} c^{n-2} \bigl((-1)^{n-2} 4(a/2)^n (n-2)^{n-2} + n^n c\bigr).$$

Hence $f(x)$ has a multiple root α modulo p. Since this root has to be a root of $f'(x)$ modulo p as well, one has

$$\alpha \in \{0, -a/2, -a/2 + a/n\}.$$

But, since $p \nmid c$, we have $f(0) = f(-a/2) = c \neq 0$ modulo p. Therefore, the only multiple root of $f(x)$ modulo p is $\alpha = -a/2 + a/n$ whose order is two. Therefore,

$$f(x) \equiv (x - \alpha)^2 \bar{h}(x) \pmod{p}$$

with a separable polynomial $\bar{h} \in \mathbb{F}_p[x]$. Now if $c = \pm 1$ and $\gcd(n, a) = 1$, using the discriminant formula we see that $p \nmid nc$ for any prime p dividing $\operatorname{disc}(f)$. Hence by Lemma 2.2 we obtain the following theorem:

Theorem 3.1. *For any irreducible polynomial of the form*

$$f(x) = x^n + ax^{n-1} + bx^{n-2} \pm 1 \in \mathbb{Z}[x]$$

with $a^2 = 4b$ *and* $\gcd(n, a) = 1$, *the Galois group* G_f *is* S_n.

Let us now show the existence of an infinite family of quadrinomials satisfying the hypothesis of Theorem 3.1. By a result of Heath-Brown [4] there exists an odd prime p such that p is a primitive root modulo ℓ for infinitely many odd primes ℓ. For such a pair (p, ℓ), if b is relatively prime to ℓ and divisible by p, then any quadrinomial of the form $f(x) = x^\ell + ax^{\ell-1} + bx^{\ell-2} - 1$ is irreducible and so $G_f \simeq S_\ell$. To see the irreducibility, it is enough to consider $f(x) \equiv (x-1)(x^{\ell-1} + x^{\ell-2} + \cdots + 1)$ modulo p and note that $x^{\ell-1} + x^{\ell-2} + \cdots + 1$ is irreducible in $\mathbb{F}_p[x]$ if p is a primitive root modulo ℓ by Dedekind's theorem together with [13, Theorem 2.13].

If $n = \ell$ is an odd prime, there exists an ℓ-cycle in G_f by the Cauchy theorem. So to show that G_f is S_ℓ, by Lemma 2.4 it is enough to find a transposition in G_f. To do so, assume that

$$\gcd(2a(\ell-2), \ell c) = 1$$

and $g(\ell) := (-1)^{\ell-2}4(a/2)^\ell(\ell-2)^{\ell-2} + \ell^\ell c$ is not a perfect square, e.g. $\ell c \not\equiv 1 \pmod 4$. Then c and $g(\ell)$ are relatively prime, and there is a prime number p dividing $g(\ell)$ to an odd power. Hence, using the discriminant formula (3.1) and equality (2.1), one has $p \mid d_N$ and $p \nmid \ell c$ where N is the splitting field of $f(x)$. Now we repeat the same argument as above to conclude that the corresponding inertia group of p is either trivial or generated by a transposition. But, since $p \mid d_N$, the prime p is ramified, and so the inertia group is not trivial. This completes the proof of the following theorem:

Theorem 3.2. *Let* ℓ *be a prime number, and assume* $\gcd(2a(\ell-2), \ell c) = 1$ *and* $(-1)^{\ell-2}4(a/2)^\ell(\ell-2)^{\ell-2} + \ell^\ell c$ *is not a perfect square. Then, for any irreducible polynomial of the form*

$$f(x) = x^\ell + ax^{\ell-1} + bx^{\ell-2} + c \in \mathbb{Z}[x]$$

with $a^2 = 4b$, *the Galois group* G_f *is* S_ℓ.

We finally mention an infinite family of polynomials satisfying the hypotheses of Theorem 3.2. Let $f(x) = x^\ell + ax^{\ell-1} + bx^{\ell-2} + c \in \mathbb{Z}[x]$ be a quadrinomial with ℓ prime, $\ell \nmid a$ and $a^2 = 4b$. Assume that c is a prime greater than $\max\{1 + |a| + |b|, 2a(\ell-2)\}$. This implies that $f(x)$ is irreducible by [7, Lemma 9]. If we also suppose that $\ell c \not\equiv 1 \pmod 4$, then all hypotheses of Theorem 3.2 hold and hence $G_f \simeq S_\ell$.

4. The Galois groups of a family with an arbitrary number of terms.

In this section, we generalize the argument of Theorem 3.1 to compute the Galois group of a family of polynomials with an arbitrary number of terms. The strategy is to construct a polynomial $f(x)$ whose derivative is of a certain form.

Remark 4.1. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ be an irreducible polynomial whose derivative factors in $\mathbb{C}[x]$ as follows:

$$f'(x) = nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1 = n(x-\alpha_1)\cdots(x-\alpha_{n-1}).$$

By integrating, the coefficients of $f(x)$ have the following form in terms of its roots:

$$f(x) = x^n - \frac{n\sum\alpha_i}{n-1}x^{n-1} + \frac{n\sum\alpha_i\alpha_j}{n-2}x^{n-2} + \cdots + (-1)^n\alpha_{i_1}\cdots\alpha_{i_{n-1}}x + a_0.$$

So to have integer coefficients, it is enough to have, for all $1 \le l \le n-1$,

$$n - l \,\Big|\, \sum_{1\le i_1,\dots,i_{i-1}\le n} \alpha_{i_1}\cdots\alpha_{i_l}.$$

We are now looking for a polynomial $f(x) = x^{n+k+1} + a_{n+k}x^{n+k} + \cdots + a_0 \in \mathbb{Z}[x]$ whose derivative has the form

$$f'(x) = x^n(x-a)^{k-1}\big((n+a)x - (n+1)a\big).$$

Hence the coefficients of $f(x)$ are of the form

$$\begin{aligned}\pm a_{n+k-l} &= (k+1)\binom{k-1}{l}a^l + (k+1)\binom{k-1}{l-1}a^{l-1}(a-k)\\ &= (k+1)a^{l-1}(a-k)\binom{k}{l}.\end{aligned}$$

Letting $a := k+1$ yields

$$\begin{aligned}f(x) = x^{n+k+1} &- \binom{k}{1}(k+1)x^{n+k} + \binom{k}{2}(k+1)^2x^{n+k-1} - \cdots\\ &+ (-1)^k\binom{k}{k}(k+1)^kx^{n+1} + c = x^{n+1}(x-k-1)^k + c.\end{aligned}$$

We now apply the argument of Theorem 3.1 to this polynomial in the case $c = \pm1$ under the hypothesis $\gcd(n+k+1, nk) = 1$, which guarantees that $f'(x)$ is not the zero polynomial modulo p: the roots of $f'(x)$ are

$$0, \quad k+1, \quad \alpha := \frac{(n+1)(k+1)}{n+k+1}.$$

Since $f(0) = f(k+1) = \pm1$, the only multiple root of $f(x)$ modulo a prime p is α, of order two. Therefore, for any prime number p dividing $\operatorname{disc}(f)$, we have $f(x) \equiv (x-\alpha)^2\bar{h}(x) \pmod{p}$ for a separable polynomial $\bar{h}(x) \in \mathbb{F}_p[x]$. Lemma 2.2 now implies that the inertia group of a prime of the splitting field of $f(x)$ sitting above p is either trivial or generated by a transposition. Combining this with Lemma 2.3 finally gives the main theorem of this section:

Theorem 4.2. *The Galois group G_f of any irreducible polynomial*

$$f(x) = x^{n+k+1} - \binom{k}{1}(k+1)x^{n+k} + \binom{k}{2}(k+1)^2x^{n+k-1} - \cdots \pm x^n \pm 1 \in \mathbb{Z}[x]$$

with $\gcd(n+k+1, nk) = 1$ *is* S_{n+k+1}.

For $f(x) = x^{n+1}(x-k-1)^k + c$ with $n+k+1$ prime, let

$$A := \big((-1)^k(k+1)^{n+k+1}(n+1)^{n+1}k^k + c(n+k+1)^{n+k+1}\big).$$

Then

$$\begin{aligned}\operatorname{disc}(f) &= (n+k+1)^{n+k+1}f(0)^n f(k+1)^{k-1} f\bigg(\frac{(n+1)(k+1)}{n+k+1}\bigg)\\ &= c^{n+k-1}A.\end{aligned}$$

Hence, we obtain the following theorem similar to Theorem 3.2:

Theorem 4.3. *Let $n+k+1$ be a prime number, and assume that* $\gcd(c, (k+1)(n+1)k) = 1$ *and A is not a perfect square. Then, for any irreducible polynomial of the form*

$$\begin{aligned}f(x) = x^{n+k+1} - \binom{k}{1}(k+1)x^{n+k} + \binom{k}{2}(k+1)^2x^{n+k-1} - \cdots\\ + (-1)^k\binom{k}{k}(k+1)^kx^{n+1} + c \in \mathbb{Z}[x],\end{aligned}$$

the Galois group G_f is S_{n+k+1}.

5. Galois groups of $x^n + ax^{n-1} + bx^{n-2} + c$ with $a^2 \neq 4b$. The explicit classification of the Galois groups of the quadrinomials $f(x) = x^n + ax^{n-1} + bx^{n-2} + c \in \mathbb{Z}[x]$ with $a^2 \neq 4b$ seems to be hard due to different possibilities which can occur for the non-zero roots of $f'(x) = 0$ modulo a prime p and their lifts to $\mathbb{Q}_p$. However, assuming that the coefficients a, b and c satisfy a certain congruence modulo 4 and $n = \ell$ is prime, we are able to show that G_f is again S_ℓ. The argument is as follows:

Let ℓ be a prime with $\ell \equiv 1 \pmod 4$ and $f(x) = x^\ell + ax^{\ell-1} + bx^{\ell-2} + c$. Then $f'(x) = x^{\ell-3}(\ell x^2 + a(\ell-1)x + b(\ell-2))$ has three roots $\{0, \delta_1, \delta_2\}$, and

$$\begin{aligned}\operatorname{disc}(f) &= \ell^\ell f(0)^{\ell-3} f(\delta_1)f(\delta_2)\\ &= \ell^\ell c^{\ell-3}(\delta_1^\ell + a\delta_1^{\ell-1} + b\delta_1^{\ell-2} + c)(\delta_2^\ell + a\delta_2^{\ell-1} + b\delta_2^{\ell-2} + c)\\ &= \ell^\ell c^{\ell-3}\big((\delta_1\delta_2)^\ell + a(\delta_1\delta_2)^{\ell-1}(\delta_1+\delta_2) + b(\delta_1\delta_2)^{\ell-2}(\delta_1^2+\delta_2^2)\\ &\qquad + c(\delta_1^\ell + \delta_2^\ell) + a^2(\delta_1\delta_2)^{\ell-1} + b^2(\delta_1\delta_2)^{\ell-2} + c^2\\ &\qquad + ab(\delta_1\delta_2)^{\ell-2}(\delta_1+\delta_2) + ac(\delta_1^{\ell-1} + \delta_2^{\ell-1}) + bc(\delta_1^{\ell-2} + \delta_2^{\ell-2})\big).\end{aligned}$$

Also note that $\delta_1+\delta_2=-a(\ell-1)/\ell\equiv 0 \pmod 4$, $\delta_1\delta_2=b(\ell-2)/\ell\equiv -b \pmod 4$, and

$$\delta_1^m+\delta_2^m\equiv\begin{cases}0 \pmod 4 & \text{if } m \text{ is odd},\\ -2b^{m/2} \pmod 4 & \text{if } m \text{ is even}.\end{cases}$$

For the last congruence it is enough to use the following recursive relation:

$$(\delta_1^m+\delta_2^m)+(\delta_1\delta_2)(\delta_1^{m-2}+\delta_2^{m-2})=(\delta_1+\delta_2)(\delta_1^{m-1}+\delta_2^{m-1}).$$

Therefore,

$$\operatorname{disc}(f)\equiv c^{\ell-3}(a^2b^{\ell-1}+c^2-2acb^{(\ell-1)/2)}) \pmod 4.$$

Hence $\operatorname{disc}(f)\equiv 0 \pmod 4$ whenever a, b and c are all odd.

From now on we assume that $a+b+c\equiv 1 \pmod 4$. So 2 divides $f(-1)$ exactly once, and the $(\mathbb{Q}_2,x+1)$-polygon (see [2, appendix]) of $f(x)$ has two sides: one horizontal side joining the point $(0,0)$ to $(0,\ell-2)$, and another side joining $(0,\ell-2)$ to $(1,\ell)$. The polynomial corresponding to the latter side is of degree 1, and so is irreducible. Therefore, $2=\mathfrak{p}^2\mathfrak{b}$ in the ring of integers of $\mathbb{Q}(\alpha)$, where α is a root of f and $\mathfrak{p}$ is a prime ideal. As a result, $p=2$ is ramified in the splitting field of f. On the other hand, $f(x)\equiv(x-1)^2\bar{h}(x) \pmod 2$ for a separable $\bar{h}(x)\in\mathbb{F}_p[x]$ with $\bar{h}(1)\not\equiv 0 \pmod 2$. Hence by Lemma 2.2 the inertia group of the prime ideal in the splitting field of $f(x)$ sitting above the prime 2 is a transposition. Finally, since by the Cauchy theorem the Galois group G_f contains a cycle of length ℓ, we obtain the following result:

Theorem 5.1. *The Galois group of any irreducible quadrinomial of the form*

$$x^\ell+ax^{\ell-1}+bx^{\ell-2}+c\in\mathbb{Z}[x]$$

with $\ell\equiv 1 \pmod 4$ *an odd prime is* S_ℓ *if the coefficients* a, b *and* c *are all odd integers and* $a+b+c\equiv 1 \pmod 4$.

It is worth mentioning that if $a>b+c+1$, then by a result of Perron [9] the quadrinomial $x^\ell+ax^{\ell-1}+bx^{\ell-2}+c\in\mathbb{Z}[x]$ is irreducible. Hence assuming that a, b and c are all odd integers with $a>b+c+1$ and $a+b+c\equiv 1 \pmod 4$, and that $\ell\equiv 1 \pmod 4$ is prime, we see that the Galois group of $x^\ell+ax^{\ell-1}+bx^{\ell-2}+c\in\mathbb{Z}[x]$ is S_ℓ.

Acknowledgments. The authors would like to thank the referee for comments and corrections.

References

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

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

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

[4] D. R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford 37 (1986), 27–38.

[5] A. Movahhedi, *Sur une classe d'extensions non ramifiées*, Acta Arith. 59 (1991), 91–95.

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

[7] H. Osada, *The Galois groups of the polynomials* $x^n + ax^s + b$, J. Number Theory 25 (1987), 230–238.

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

[9] O. Perron, *Neue Kriterien für die Irreduzibilität algebraischer Gleichungen*, J. Reine Angew. Math. 132 (1907), 288–307.

[10] J.-P. Serre, *Topics in Galois Theory*, 2nd ed., A K Peters/CRC Press, 2007.

[11] L. Soicher and J. McKay, *Computing Galois groups over the rationals*, J. Number Theory 20 (1985), 273–281.

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

[13] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, New York, 1997.

Khosro Monsef Shokri, Jafar Shaffaf, Reza Taleb
Department of Mathematical Sciences
Shahid Beheshti University
P.O. Box 19839-63113, Tehran, Iran
E-mail: k_shokri@sbu.ac.ir
shaffaf@gmail.com
r_taleb@sbu.ac.ir