JOURNAL OF NUMBER THEORY 25, 230–238 (1987)

The Galois Groups of the Polynomials $X^n + aX^l + b$

HIROYUKI OSADA

Department of Mathematics, Rikkyo University, Ikebukuro, Tokyo, 171, Japan

Communicated by H. Zassenhaus

Received July 12, 1985; revised November 27, 1985

We give conditions under which the Galois group of the polynomial $X^n + aX^l + b$ over the rational number field Q is isomorphic to the symmetric group S_n of degree n. Using the result, we prove the Williams–Uchiyama conjecture concerning the irreducibility of the polynomial $X^n + X + a$ modulo p.

In his paper (2), Fujisaki gave an interesting example of a quadratic field with the class number 1 which has an unramified extension in the narrow sense with the alternating group A_5 of degree 5 as the Galois group. This is an typical example for our Theorem 1. Later Uchida (10) and Yamamoto (16) generalized the result of Fujisaki. They showed that the Galois group of a polynomial $X^n + aX + b$ (a and b are rational integers) over Q is isomorphic to the symmetric group S_n of degree n under the conditions:

(1) n is a prime number,

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

(3) $X^n + aX + b$ is irreducible over Q.

Further, let D be the discriminant of the polynomial $X^n + aX + b$. Then the splitting field of $X^n + aX + b$ over Q is an unramified extension in the narrow sense of the quadratic field $Q(\sqrt{D})$ with the alternating group A_n of degree n as the Galois group. Ohta (5) also generalized these results under certain conditions. In this paper, we shall generalize the results of Uchida, Yamamoto, and Ohta to arbitrary n. In fact, we shall give some conditions under which the Galois group of a polynomial $X^n + aX^l + b$ is isomorphic to S_n (Theorem 1–5). By Hilbert's irreducibility Theorem (3), for any non-zero integer a, there exist infinitely many integers b such that the Galois group of $X^n + aX + b$ over Q is isomorphic to S_n. But, concrete determination of such integers b is another problem. And we do this for some special cases. As a Corollary, we can show that the Galois group of

0022-314X/87 $3.00

$X^n - X - 1$ over Q is isomorphic to S_n for any integer $n \geqslant 2$ (Corollary 3 of Theorem 1). As another consequence of our results, we also prove the Williams–Uchiyama conjecture concerning the irreducibility of the polynomial $X^n + X + a$ modulo p. In this paper, "unramified" means that any finite prime is unramified.

For a polynomial $f(X)$ of degree n with coefficients in the ring of rational integers, we shall denote by K the splitting field of $f(x)$ over Q. The Galois group of K over Q is denoted by G.

THEOREM 1. *Let $f(X) = X^n + aX^l + b$ be a polynomial of rational integral coefficients, that is, $f(X) \in Z[X]$. Let $a = a_0 c^n$ and $b = b_0^l c^n$. Then the Galois group G is isomorphic to the symmetric group S_n of degree n if the following conditions are satisfied:*

(1) *$f(X)$ is irreducible over Q,*

(2) *$a_0 c(n-l)\,l$ and nb_0 are relatively prime, that is, $(a_0 c(n-l)\,l, nb_0) = 1$.*

To prove Theorem 1, we need some lemmas.

LEMMA 1. *Let p be a prime number and $\mathfrak{p}$ be a prime ideal in K satisfying $\mathfrak{p} \mid p$. If $f(X) \equiv (X-c)^2\, \bar{h}(X)$ (mod p) for some $c \in Z$ and a separable polynomial $\bar{h}(X)$ (mod p) such that $\bar{h}(c) \not\equiv 0$ (mod p), then the inertia group of $\mathfrak{p}$ over Q is either trivial or a group generated by a transposition.*

Proof. Since $f(X) \equiv (X-c)^2\, \bar{h}(X)$ (mod p), Hensel's lemma shows that $f(X) = g(X)\, h(X)$ in the rational p-adic number field Q_p such that $g(X) \equiv (X-c)^2$ (mod p) and $h(X) \equiv \bar{h}(X)$ (mod p). Let $K_\mathfrak{p}$ be the $\mathfrak{p}$-completion of K. $K_\mathfrak{p}$ is obtained from Q_p by adjoining the roots of $f(X)$. The roots of $h(X)$ generate an unramified extension of Q_p. Hence, if $K_\mathfrak{p}$ is ramified over Q_p, then the inertia group of $\mathfrak{p}$ over Q is a group generated by the transposition of the roots of $g(X)$. This completes the proof.

LEMMA 2. *If $f(X)$ is irreducible over Q, then the Galois group G is transitive (see van der Wearden [13, Chap. 7, Sect. 50]).*

By $D(f)$ we shall denote the discriminant of a polynomial $f(X)$. Hence if $f(X) = X^n + aX^l + b$, $a = a_0 c^n$, $b = b_0^l c^n$, and $(n, l) = 1$, then $D(f) = (-1)^{n(n-1)/2}\, b_0^{l(l-1)} c^{n(n-1)} D_0(f)$ where $D_0(f) = n^n b_0^{(n-l)\,l} + (-1)^{n-1} l^l (n-l)^{n-l} a_0^n c^{nl}$.

LEMMA 3. *Let p be a prime number and $\mathfrak{p}$ be a prime ideal in K satisfying $\mathfrak{p} \mid p$. If $(a_0 c(n-l)\,l, nb_0) = 1$ and if $p \mid D_0(f)$, then the inertia group of $\mathfrak{p}$ over Q is either trivial or a group generated by a transposition.*

Proof. Since $p \mid D_0(f)$, $p \nmid a(n-l)\,lb$. So $f'(X) \equiv X^{l-1}(nX^{n-l}+al)$ $(\bmod p)$ has no multiple root other than $X=0$. Clearly, $X=0$ is not a root of $f(X) \equiv 0 \pmod p$. Hence every irreducible factors of $f(X)$ have multiplicity at most two.

Let β be a multiple root of $f(X) \pmod p$ in an algebraic closure of Z/pZ. We get

$$\beta^{n-l} = -al/n \qquad \text{and} \qquad \beta^{l} = -b/(a+\beta^{n-l}) = -nb/(a(n-l)).$$

Since $(n-l, l)=1$, this shows that $\beta \in Z/pZ$. If γ is another multiple root of $f(X) \pmod p$, from $(n-l, l)=1$ and $(\gamma/\beta)^{n-l} = (\gamma/\beta)^{l} = 1$, we get $\beta = \gamma$. Hence $f(X) \equiv (X-\beta)^2\,\bar{h}(X) \pmod p$ where $\bar{h}(X) \pmod p$ is a separable polynomial such that $\bar{h}(\beta) \not\equiv 0 \pmod p$. It is now easy to see that Lemma 3 is a consequence of Lemma 1.

LEMMA 4. *Let $a = a_0 c^n$ and $b = b_0^l c^n$ (or $b_0 c^n$) be rational integers. Further let $(a_0 c(n-l)\,l, nb_0) = 1$. If $f(X)$ is irreducible over Q, then all the prime divisors of b (resp. c) are unramified in K (see Llorente, Nart, and Vila [6]).*

LEMMA 5. *Let G be a permutation group of the set $\Omega = \{1, 2, ..., n\}$ generated by transpositions. If G is transitive on Ω, then it is the symmetric group S_n.*

Proof. We shall show that G is doubly transitive. Let $\tau = (i, j)$ be a transposition contained in G and k be any letter in Ω. Since G is generated by transpositions and is transitive, there exists a series of transpositions connecting j and k. Hence there exist transpositions (j, i_1) (i_1, i_2),..., (i_{r-1}, i_r), and (i_r, k) all contained in the set of generators of G. Without loss of generality, we can assume that i_s are mutually different $(s = 1, 2, ..., r)$. First, assume that i_s are different from i too. Since G contains the element $\sigma = (j, i_1)(i_1, i_2) \cdots (i_r, k)$, G also contains $\sigma\tau\sigma^{-1} = (i, k)$. Next, assume that $i_t = i$ for some t. Then G contains $\sigma = (i_t, i_{t+1})$ $(i_{t+1}, i_{t+2}) \cdots (i_r, k)$. Hence G contains $\sigma\tau\sigma^{-1} = (j, k)$ and also contains $\tau(\sigma\tau\sigma^{-1})\tau^{-1} = (i, k)$. So G is the symmetric group S_n.

LEMMA 6. *Let $f(X)$ be an irreducible polynomial in $Z[X]$. If the inertia group of any prime in K is either trivial or a group generated by a transposition, then the Galois group G is isomorphic to S_n.*

Proof. Let H be the subgroup of G generated by all inertia groups. Minkowski's theorem shows that there exists no unramified extension of the field Q. Hence H is equal to the whole group G. Since $f(X)$ is irreducible over Q, G is transitive by Lemma 2. So the Galois group G is isomorphic to S_n by Lemma 5.

Proof of Theorem 1. Let $\mathfrak{p}$ be any prime ideal in K. Since $(a_0c(n-l)\,l, nb_0)=1$ and $f(X)$ is irreducible over Q, $\mathfrak{p}$ is unramified in K if $\mathfrak{p} \mid b$ (Lemma 4). Also if $\mathfrak{p} \mid D_0(f)$, then the inertia group of $\mathfrak{p}$ over Q is either trivial or a group generated by a transposition (Lemma 3). Hence the Galois group G is isomorphic to S_n (Lemma 6). This completes the proof.

COROLLARY 1. *$K/Q(\sqrt{D(f)})$ is unramified.*

Proof. The inertia group T of any prime in K is either trivial or a group generated by a transposition. Hence the intersection of the groups A_n and T is trivial. So $K/Q(\sqrt{D(f)})$ is unramified.

Putting $l=1$ in Theorem 1, we get

COROLLARY 2. *Let $f(X)=X^n+aX+b$ be a polynomial in $Z[X]$, where $a=a_0c^n$ and $b=b_0c^n$ for some integer c. Then the Galois group G is isomorphic to S_n if the following conditions are satisfied:*

(1) *$f(X)$ is irreducible over Q,*

(2) $(a_0c(n-1), nb_0)=1$.

Besides $K/Q(\sqrt{D(f)})$ is unramified.

We were informed by Nart that Corollary 2 was already proved in their paper [7] in 1979.

LEMMA 7. The polynomial X^n-X-1 is irreducible over Q for all $n \geqslant 2$. The polynomial X^n+X+1 is irreducible over Q for $n \not\equiv 2 \pmod 3$ (see Selmer [8]).

Hence, by Corollary 2 of Theorem 1 and Lemma 7, we get

COROLLARY 3. *The Galois group of X^n-X-1 over Q is isomorphic to S_n for all $n \geqslant 2$.*

Let p be a prime number and $n \geqslant 2$ a positive integer. We shall denote by $a_n(p)$ the least positive integral value of a which makes the polynomial $X^n+X+a \pmod p$ irreducible. Williams [15] conjectured that all $n \geqslant 2$ one has

$$\liminf_{P \to \infty} a_n(p)=1. \tag{1}$$

The case of $n=2$ and 3 was shown by himself. But, since the polynomial

X^n+X+1 has the factor X^2+X+1 for $n\equiv 2 \pmod 3$, Uchiyama [11] modified the conjecture as follows (the Williams–Uchiyama conjecture):

(1) for $n=2$ or $n\not\equiv 2 \pmod 3$

$$\liminf_{p\to\infty} a_n(p)=1,$$

(2) for all even $n>2$ such that $n\equiv 2 \pmod 3$ (*)

$$\liminf_{p\to\infty} a_n(p)=2,$$

(3) for all odd n such that $n\equiv 2 \pmod 3$

$$\liminf_{p\to\infty} a_n(p)=3.$$

He showed that (*) is true for $n=4$, 6, 9 and any odd prime. Moreover Mortimer, Williams, and others showed that (*) is true for $n\leqslant 20$ and for some other values of n. Now applying Corollary 2 of Theorem 1, we shall show that (*) is true for all $n\geqslant 2$ (see Mortimer and Williams [4], Uchida [10], and Uchiyama and Hitotumatu [12]).

LEMMA 8. *Let $f(X)$ be a polynomial of degree n in $Z[X]$. If the Galois group of $f(X)$ over Q contains a cycle of length n, then there exist infinitely many primes p for which $f(X)$ $(\mathrm{mod}\, p)$ is irreducible (This is a simple consequence of the Density Theorem. See Čebotarev [1] or Takagi [9, Chap. 16, pp. 239–241]).*

In order to prove the Williams–Uchiyama conjecture, we need the following lemma. We owe the proof to Dr. Funakura.

LEMMA 9. *Let $f(X)=X^n+a_1X^{n-1}+\cdots+a_{n-1}X\pm p$ be a polynomial in $Z[X]$, where p is a prime number. Then $f(X)$ is irreducible over Q if one of the following conditions is satisfied:*

(1) $1+|a_1|+|a_2|+\cdots+|a_{n-1}|<p$, *or*

(2) $1+|a_1|+|a_2|+\cdots+|a_{n-1}|=p$ *and $f(X)$ has no roots of unity.*

Proof. If $f(X)$ is decomposable, then $f(X)=g(X)\,h(X)$, where $g(X)$ and $h(X)$ are polynomials in $Z[X]$. Since p is a prime number, the constant term of $g(X)$ (or $h(X)$) is equal to ± 1. Hence $g(X)$ (resp. $h(X)$) must have at least one root α whose absolute value is not greater than 1. Then, from $f(\alpha)=0$ we get

$$p=|\alpha^n+a_1\alpha^{n-1}+\cdots+a_{n-1}|\leqslant 1+|a_1|+\cdots+|a_{n-1}|.$$

This contradicts the condition. Thus the lemma is proved.

Proof of the Williams–Uchiyama Conjecture. By Corollary 2 of Theorem 1 and Lemma 7, the Galois group of X^n+X+1 over Q is isomorphic to S_n for $n \not\equiv 2 \pmod 3$. So we get (1) by Lemma 8. By Corollary 2 of Theorem 1 and Lemma 9, the Galois group of X^n+X+2 over Q is isomorphic to S_n for all even $n \geqslant 2$ and the Galois group of X^n+X+3 over Q is isomorphic to S_n for all $n \geqslant 2$. So we get (2) and (3) by Lemma 8. This completes the proof.

We can also show the following Theorem 2. The proof is similar to that of Theorem 1.

THEOREM 2. *Let $f(X)=X^n+aX^2+b$ be a polynomial in $Z[X]$, where $a=a_0c^n$ and $b=b_0c^n$ for some integer c. Then the Galois group G is isomorphic to S_n if the following conditions are satisfied:*

(1) *$f(X)$ is irreducible over Q,*

(2) $(a_0c(n-2)\,2, nb_0)=1.$

Further $K/Q(\sqrt{D(f)})$ is unramified.

EXAMPLE. Put $f(X)=X^5+2X^2+1$. Then $f(X) \pmod 5$ is irreducible. Hence by Theorem 1 or by Theorem 2, the Galois group of $f(X)$ over Q is isomorphic to S_5. $K/Q(\sqrt{D(f)})$ is unramified, where $D(f)=6581$. On the other hand, the class number of $Q(\sqrt{6581})$ is equal to 1 and the norm of the fundamental unit of $Q(\sqrt{6581})$ is equal to -1 (see [14]). So there is no abelian extension of $Q(\sqrt{6581})$ which is unramified at all finite primes of $Q(\sqrt{6581})$ (for other examples, see [2, 5, 16, 17]).

Let k be a finite extension of Q and O_k be the ring of integers of k. Further let α be a primitive element of the ring O_k. By $i(\alpha)$ we shall denote the index of the subring $Z[\alpha]$ of the ring O_k. Then, $i(\alpha)$ is called the index of α.

LEMMA 10. *Let $a=a_0c^n$ and $b=b_0c^n$ be rational integers. Further let $(a_0c(n-l)\,l, nb_0)=1$. Let $k=Q(\alpha)$, where α is a root of an irreducible polynomial $f(X)=X^n+aX^l+b$ in $Z[X]$. If $q \parallel b_0$ for some prime number q, then $q \nmid i(\alpha)$ (see Llorente, Nart, and Vila [6]).*

THEOREM 3. *Let $f(X)=X^n+aX^l+b$ be a polynomial in $Z[X]$, where $a=a_0c^n$ and $b=b_0c^n$ for some integer c. Let l $(\geqslant 3)$ be a prime number. Then the Galois group G is isomorphic to S_n if the following conditions are satisfied:*

(1) *$f(X)$ is irreducible over Q,*

(2) $(a_0c(n-l)\,l, nb_0)=1,$

(3) $|D_0(f)|$ *is not square,*

(4) $q \parallel b_0$ *for some prime number* q,

where $D_0(f) = n^n b_0^{n-l} + (-1)^{n-1} l^l (n-l)^{n-l} a_0^n c^{nl}$.

Proof. Let $\mathfrak{p}$ be any prime ideal in K. If $\mathfrak{p} \mid b_0$, then $f(X) \equiv X^l(X^{n-l} + a)$ (mod $\mathfrak{p}$). Since $\mathfrak{p} \nmid (n-l)\, a$, the inertia group of $\mathfrak{p}$ over Q is isomorphic to a subgroup of the symmetric group S_l of degree l. Let α be a root of $f(X)$ and q be a prime number such that $q \parallel b_0$. By Lemma 10, we have $q \nmid i(\alpha)$, where $i(\alpha)$ is the index of α. Hence if $\mathfrak{p}$ is a prime ideal in K satisfying $\mathfrak{p} \mid q$, the order of the inertia group T of $\mathfrak{p}$ over Q is divisible by l. Since l is a prime number, this means that T contains a cycle of length l. If $\mathfrak{p} \mid cD_0(f)$, then by Lemmas 3 and 4, the inertia group of $\mathfrak{p}$ over Q is either trivial or a group generated by a transposition. Since $|D_0(f)|$ is not square, there exists at least one inertia group generated by a transposition. Hence we can show in the same way as in the proof of Theorem 1 that the Galois group G is generated by transpositions. So the group G is isomorphic to S_n by Lemma 5. This completes the proof.

Remark. In the case $l = 3$, we do not require the condition (4).

In the same way as in the proof of Theorem 3, we can show the following, Theorems 4 and 5.

THEOREM 4. *Let* $f(X) = X^n + aX^l + b$ *be a polynomial in* $Z[X]$, *where* $a = a_0 c^n$ *and* $b = b_0 c^n$ *for some integer* c. *Let* $l = 2p$ *where* p *is a prime number. Then the Galois group* G *is isomorphic to* S_n *if the following conditions are satisfied:*

(1) $f(X)$ *is irreducible over* Q,

(2) $(a_0 c(n-l)\, l, nb_0) = 1$,

(3) $|D_0(f)|$ *is not square,*

(4) $q \parallel b_0$ *for some prime number* q.

Remark. In the case $l = 4$ and 6, we do not require the condition (4).

THEOREM 5. *Let* $f(X) = X^n + aX^l + b$ *be a polynomial in* $Z[X]$, *where* $a = a_0 c^n$ *and* $b = b_0 c^n$ *for some integer* c. *Then the Galois group* G *is isomorphic to* S_n *if the following conditions are satisfied:*

(1) $f(X)$ *is irreducible over* Q,

(2) $(a_0 c(n-l)\, l, nb_0) = 1$,

(3) $|D_0(f)$ *is not square,*

(4) *$q \| b_0$ for some prime number q,*

(5) *there exists some prime number p such that $p \mid l$ and $p > k$, for any positive integer k such that $k \mid n$ and $l/2 > k$.*

LEMMA 11. *If a monic polynomial $f(X)$ is irreducible over Q and if $D(f)$ is square free, then the inertia group of any prime in K is either trivial or a group generated by a transposition (see Yamamura [17]).*

Hence, by Lemmas 6 and 11, we get

THEOREM 6. *If a monic polynomial $f(X)$ is irreducible over Q and if $D(f)$ is square free, then the Galois group G is isomorphic to S_n and $K/Q(\sqrt{D(f)})$ is unramified.*

EXAMPLE. Put $f(X) = X^5 + 2X^4 - X^3 + 1$. Then $f(X) \pmod 2$ is irreducible and $D(f) = 28401 = 3 \cdot 9467$ is square free. Hence by Theorem 6, the Galois group of $f(X)$ over Q is isomorphic to S_5 and $K/Q(\sqrt{28401})$ is unramified. It is known that the class number of $Q(\sqrt{28401})$ is equal to 1 (see [14]).

REFERENCES

1. N. ČEBOTAREV, Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gagebenen Substitutionsklasse gehören., *Math. Ann.* **95** (1926), 191–228.
2. G. FUJISAKI, On an example of an unramified Galois extension, *Sûgaku* **9** (1957), 97–99. [Japanese]
3. D. HILBERT, Ueber die irreduzibilität genzen rationalen Funktionen mit ganzzahligen Koeffizienten., *J. Reine Angew. Math.* **110** (1982), 104–129.
4. B. C. MORTIMER AND K. S. WILLIAMS, Note on a paper of S. Uchiyama, *Canad. Math. Bull.* **17** (1974), 289–293.
5. K. OHTA, On unramified Galois extensions of quadratic number fields, *Sûgaku* **24** (1972), 119–120. [Japanese]
6. P. LLORENTE, E. NART, AND N. VILA, Discriminants of number fields defined by trinomials, *Acta Arith.* **43** (1984), 367–373.
7. E. NART AND N. VILA, Equations of the type $X^n + aX + b$ with absolute Galois group S_n, *Rev. Univ. Santander. 2* **II** (1979), 821–825.
8. E. S. SELMER, On the irreducibility of certain trinomials, *Math. Scand.* **4** (1956), 287–302.
9. T. TAKAGI, "Algebraic Number Theory," Iwanami Shoten, 1971. [Japanese]
10. K. UCHIDA, Unramified extensions of quadratic number fields II, *Tôhoku. Math. J.* **22** (1970), 220–224.
11. S. UCHIYAMA, On a conjecture of K. S. Williams, *Proc. Japan Acad.* **46** (1970), 755–757.
12. S. UCHIYAMA AND S. HITOTUMATU, On the irreducibility of certain polynomials, R.I.M.S. Kokyuroku. **155** (1972), 14–30. [Japanese]

13. B. L. VAN DER WEARDEN, "Moderne Algebra," Vol. I, Ungar, New York, 1949.
14. H. WADA, A table of ideal class numbers of real quadratic fields, *Sophia Kokyuroku Math.* **10** (1981). [Japanese]
15. K. S. WILLIAMS, On two conjectures of Chowla, *Canad. Math. Bull.* **12** (1969), 545–565.
16. Y. YAMAMOTO, On unramified Galois extensions of quadratic number fields, *Osaka J. Math.* **7** (1970), 57–76.
17. K. YAMAMURA, On unramified Galois extensions of real quadratic number fields, *Osaka J. Math.* **23** (1986), 471–478.