TOKYO J. MATH.
VOL. 15, NO. 2, 1992

# On the Galois Group of $x^p+p^tb(x+1)=0$

Kenzo KOMATSU

*Keio University*

**1.** In [3] we discussed the Galois group of

$$x^p+ax+a=0$$

over the rational number field $\boldsymbol{Q}$, where $p$ is a prime number, and $a\in\boldsymbol{Z}$, $(p, a)=1$. The situation becomes much more complicated when $a$ is divisible by $p$. In this paper we deal with three special cases:

1. $a=p^tb$, $0<t<p$, $(p, b)=1$, $|(p-1)^{p-1}b+p^{p-t}|$ is not a square;
2. $a=pk^2$, $(p, k)=1$;
3. $a=p^{2m}b$, $0<2m<p$, $(p, b)=1$.

We begin by proving the following theorem (cf. [3]).

THEOREM 1. *Let $a_0, a_1, \cdots, a_{n-1}$ be rational integers such that*

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$$

*is irreducible over the rational number field $\boldsymbol{Q}$. Let $\alpha$ be a root of $f(x)=0$, and let*

$$\delta=f'(\alpha), \qquad D=\operatorname{norm}\delta \ (in\ \boldsymbol{Q}(\alpha)),$$

$$D/\delta=x_0+x_1\alpha+\cdots+x_{n-1}\alpha^{n-1}, \qquad x_i\in\boldsymbol{Z}.$$

*Let $D_1$ and $D_2$ denote any rational integers which satisfy the following conditions:*

$$D=D_1D_2, \tag{1.1}$$

$$(D_1, D_2)=1, \tag{1.2}$$

$$(D_2, x_0, x_1, \cdots, x_{n-1})=1. \tag{1.3}$$

*Let $G$ denote the Galois group of $f(x)=0$ over $\boldsymbol{Q}$; $G$ is a transitive permutation group on the set $\{1, 2, \cdots, n\}$. Then we have:*

I. *If $|D_2|$ is not a square, $G$ contains a transposition.*

II. *If $|D_2|$ is a square, $D_1$ is divisible by the discriminant of $\boldsymbol{Q}(\alpha)$.*

PROOF. Suppose first that $|D_2|$ is not a square. Then there exists a prime number

Received September 6, 1991

$q$ such that $(D_2)_q$ is odd, where the symbol $(D_2)_q$ means the largest integer $M$ such that $D_2$ is divisible by $q^M$ (cf. [1]). Since $D_2$ is divisible by $q$, it follows from (1.3) that $q \nmid x_i$ for some $i$. Clearly, $(D)_q$ is also odd. Hence, by Theorem 1 of [1], we see that the discriminant $d$ of $Q(\alpha)$ is exactly divisible by $q$. Therefore $G$ contains a transposition ([4]). Suppose next that $|D_2|$ is a square. Let $q$ denote a prime factor of $D_2$. Then, by (1.3), we see that $q \nmid x_i$ for some $i$. Since $(D)_q=(D_2)_q$ is even, it follows from Theorem 1 of [1] that $d$ is not divisible by $q$. Hence we obtain $(d, D_2)=1$. Since $D$ is divisible by $d$, we see that $D_1$ is divisible by $d$.

**2.** Now we prove the following theorem.

THEOREM 2. *Let $p$ denote an odd prime, and let $t$ and $b$ denote rational integers such that $0<t<p$, $(p, b)=1$. Suppose that $|(p-1)^{p-1}b+p^{p-t}|$ is not a square. Then the Galois group of*

$$x^p+p^t b(x+1)=0$$

*over $Q$ is the symmetric group $S_p$.*

PROOF. Since $0<t<p$, $t$ is not divisible by $p$. It is easily seen that

$$f(x)=x^p+p^t b(x+1)$$

is irreducible over $Q$ ([2], Lemma 1). Let $\alpha$ be a root of $f(x)=0$, and let $\delta=f'(\alpha)$, $D=\operatorname{norm}\delta$ (in $Q(\alpha)$). Then ([1], Theorem 2)

$$\begin{aligned} D&=(p-1)^{p-1}(p^t b)^p+p^p(p^t b)^{p-1} \\ &=p^{tp}b^{p-1}\{(p-1)^{p-1}b+p^{p-t}\}. \end{aligned} \tag{2.1}$$

Now let

$$D_1=p^{tp}b^{p-1}, \qquad D_2=(p-1)^{p-1}b+p^{p-t}.$$

Then

$$D=D_1D_2, \qquad (D_1, D_2)=1.$$

By Theorem 2 of [1] we see that the condition (1.3) of Theorem 1 is also satisfied. Since $p$ is a prime, the Galois group of $f(x)=0$ is primitive. Theorem 1 implies that the Galois group is the symmetric group $S_p$ ([5], Theorem 13.3).

**3.** Consider now the case

$$a=pk^2, \qquad (p, k)=1.$$

From Theorem 2 we obtain

THEOREM 3. *Let $p$ denote a prime number, and $k$ a rational integer such that $(p, k)=1$. Then the Galois group of*

$$x^p+pk^2(x+1)=0 \tag{3.1}$$

*over $Q$ is the symmetric group $S_p$.*

PROOF. We may assume that $p>2$, $k>0$. When $p=3$, the Galois group of (3.1) is the symmetric group $S_3$, since the discriminant of (3.1) is negative. So we may assume that

$$p>3, \quad k>0. \tag{3.2}$$

Now suppose that

$$(p-1)^{p-1}k^2+p^{p-1}=c^2, \quad c\in Z, \quad c>0.$$

Then we have

$$\begin{aligned} p^{p-1}&=c^2-(p-1)^{p-1}k^2 \\ &=\{c-(p-1)^{(p-1)/2}k\}\{c+(p-1)^{(p-1)/2}k\}. \end{aligned} \tag{3.3}$$

Clearly,

$$c+(p-1)^{(p-1)/2}k$$

is positive, and prime to

$$c-(p-1)^{(p-1)/2}k.$$

Hence

$$c+(p-1)^{(p-1)/2}k=p^{p-1}, \quad c-(p-1)^{(p-1)/2}k=1.$$

Therefore

$$p^{p-1}-1=2k(p-1)^{(p-1)/2},$$

and so

$$k=\frac{p^{p-1}-1}{2(p-1)^{(p-1)/2}}. \tag{3.4}$$

Now let

$$\frac{p-1}{2}=B,$$

so that

$$p-1=2B, \quad p=2B+1.$$

Then (3.4) becomes

$$k=\frac{(2B+1)^{2B}-1}{2(2B)^{B}}. \tag{3.5}$$

Since $p>3$, we have $B\geq 2$. When $B=2$, (3.5) gives

$$k=\frac{5^4-1}{2\cdot 4^2},$$

which is not an integer. So we may assume that $B\geq 3$. Then, by (3.5) we see that

$$\frac{(2B+1)^{2B}-1}{(2B)^3}$$

is an integer. On the other hand,

$$\begin{aligned}(2B+1)^{2B}-1&=(2B)^{2B}+\cdots+\frac{(2B)(2B-1)}{2}(2B)^2+(2B)(2B)\\&\equiv(2B)^2(2B^2-B+1)\qquad(\mathrm{mod}(2B)^3).\end{aligned}$$

Hence $(2B+1)^{2B}-1$ is not divisible by $(2B)^3$.

A contradiction shows that

$$(p-1)^{p-1}k^2+p^{p-1}$$

is not a square. By Theorem 2 we see that the Galois group of (3.1) over $Q$ is the symmetric group $S_p$.

As a special case $(k=1)$ of Theorem 3, we obtain

THEOREM 4. *For any prime number p, the Galois group of*

$$x^p+px+p=0$$

*over $Q$ is the symmetric group $S_p$.*

4. Now we discuss the case

$$a=p^{2m}b, \qquad 0<2m<p, \quad (p,b)=1.$$

THEOREM 5. *Let $p$ $(p>3)$ denote a prime number and let $b$ and $m$ denote rational integers such that $0<2m<p$, $(p,b)=1$. Let $G$ denote the Galois group of the equation*

$$x^p+p^{2m}b(x+1)=0$$

*over $Q$.*

1. *If $p\equiv 3$ or 5 or 7 (mod 8), then $G$ is the symmetric group $S_p$.*

2. *Suppose that* $p \equiv 1 \pmod 8$. *Then* $G=S_p$ *if and only if* $(p-1)^{p-1}b+p^{p-2m}$ *is not a square. If* $(p-1)^{p-1}b+p^{p-2m}$ *is a square, then G is contained in the alternating group* $A_p$, *where G is regarded as a permutation group on* $\{1, 2, \cdots, p\}$.

PROOF. We have

$$p^{p-2m} \equiv p \pmod 8 . \tag{4.1}$$

Also, for every prime factor $q$ of $p-1$,

$$p^{p-2m} \equiv 1 \pmod q . \tag{4.2}$$

If $p \equiv 3$ or 5 or 7 (mod 8), then

$$|(p-1)^{p-1}b+p^{p-2m}|$$

is not a square ([3], the proof of Theorem 1), and so $G=S_p$ (Theorem 2).

Now suppose that $p \equiv 1 \pmod 8$. It follows from (4.1) that $-\{(p-1)^{p-1}b+p^{p-2m}\}$ is not a square. Hence, if $(p-1)^{p-1}b+p^{p-2m}$ is not a square, then $G=S_p$ (Theorem 2). Suppose further that $(p-1)^{p-1}b+p^{p-2m}$ is a square. Let $\alpha_1, \alpha_2, \cdots, \alpha_p$ denote the roots of

$$f(x)=x^p+p^{2m}b(x+1)=0 ,$$

and let $\delta=f'(\alpha_1)$, $D=\operatorname{norm}\delta$ (in $Q(\alpha_1)$). Then, by (2.1) we see that $D$ is also a square. Now let $A$ denote the following matrix:

$$A=(a_{ij}) , \qquad a_{ij}=\alpha_i^{j-1} \ (1 \leq i \leq p \ ; \ 1 \leq j \leq p) .$$

Then we have

$$(\det A)^2=(-1)^{p(p-1)/2}D=D .$$

Hence $\det A$ is a rational integer. If $g \in G$ is an odd permutation, then

$$(\det A)^g=-(\det A) ,$$

which is impossible. Hence $G$ is contained in $A_p$.

Finally we prove

THEOREM 6. *For any prime number* $p \equiv 1 \pmod 8$ *and any rational integer m with* $0<2m<p$, *there exist infinitely many rational integers b satisfying the following conditions*:

1. $(p, b)=1$;
2. $(p-1)^{p-1}b+p^{p-2m}$ *is a square.*

PROOF. The congruence

$$x^2 \equiv p^{p-2m} \pmod{(p-1)^{p-1}} \tag{4.3}$$

has a solution $x$ ((4.1), (4.2)). We may assume that $x$ is not divisible by $p$, since

$x+(p-1)^{p-1}$ is also a solution of (4.3). Now let

$$x^2-p^{p-2m}=y(p-1)^{p-1}.$$

Then $y$ is not divisible by $p$. For every $n\in \boldsymbol{Z}$,

$$b=y+2xnp+n^2p^2(p-1)^{p-1}$$

satisfies the conditions of Theorem 6, since

$$(p-1)^{p-1}b+p^{p-2m}=(x+np(p-1)^{p-1})^2.$$

## References

[1] K. KOMATSU, Integral bases in algebraic number fields, J. Reine Angew. Math., **278/279** (1975), 137–144.

[2] K. KOMATSU, On certain homogeneous Diophantine equations of degree $n(n-1)$, Tokyo J. Math., **12** (1989), 231–234.

[3] K. KOMATSU, On the Galois group of $x^p+ax+a=0$, Tokyo J. Math., **14** (1991), 227–229.

[4] B. L. VAN DER WAERDEN, Die Zerlegungs- und Trägheitsgruppe als Permutationsgruppen, Math. Ann., **111** (1935), 731–733.

[5] H. WIELANDT, *Finite Permutation Groups*, Academic Press, 1964.

*Present Address*:
DEPARTMENT OF MATHEMATICS, FACULTY OF SCIENCE AND TECHNOLOGY, KEIO UNIVERSITY
HIYOSHI, KOHOKU-KU, YOKOHAMA 223, JAPAN