TOKYO J. MATH.
VOL. 14, NO. 1, 1991

On the Galois Group of $x^p+ax+a=0$

Kenzo KOMATSU

Keio University

§1. Introduction.

Let p ($p>3$) be a prime number, and let a be a rational integer with $(p, a)=1$ such that

$$f(x)=x^p+ax+a$$

is irreducible over the rational number field $\boldsymbol{Q}$. In the present paper we discuss the following problem: Is the Galois group of $f(x)=0$ over $\boldsymbol{Q}$ the symmetric group S_p? Our results will be stated in Theorem 1 and Theorem 2.

We require the following lemma of van der Waerden:

LEMMA 1 ([4]). *Let K be an algebraic number field of degree n, and let $\bar{K}$ denote the Galois closure of K over $\boldsymbol{Q}$. If the discriminant d of K is exactly divisible by a prime number q (i.e. $q \mid d$, $q^2 \nmid d$), then the Galois group of $\bar{K}/\boldsymbol{Q}$ contains a transposition (as a permutation group on $\{1, 2, \cdots, n\}$).*

§2. The case $p\equiv 3$ or 5 or 7 (mod 8).

THEOREM 1. *Let a denote a rational integer, and let p denote a prime number with the following properties:*

1. $p\equiv 3$ *or* 5 *or* $7 \pmod 8$, $p\neq 3$;
2. $(p, a)=1$;
3. $f(x)=x^p+ax+a$ *is irreducible over* $\boldsymbol{Q}$.

Then the Galois group of $f(x)=0$ over $\boldsymbol{Q}$ is the symmetric group S_p.

PROOF. Let α be a root of $f(x)=0$, and let $K=\boldsymbol{Q}(\alpha)$, $\delta=f'(\alpha)$, $D=\text{norm } \delta$ (in K). Then ([1], Theorem 2)

$$D=a^{p-1}\{(p-1)^{p-1}a+p^p\}\,.$$

Received October 13, 1990

Now let

$$D_0=(p-1)^{p-1}a+p^p .$$

Then $|D_0|$ cannot be a square. In fact, if $|D_0|=m^2$ with an integer m, then

$$D_0\equiv p^p\equiv p\equiv \pm m^2 \pmod 8 .$$

This implies that $p\equiv 7 \pmod 8$, and $D_0=-m^2$. Since

$$\frac{p-1}{2}\equiv 3 \pmod 4 ,$$

there is at least one prime factor p_0 of $(p-1)/2$ such that $p_0\equiv 3 \pmod 4$. Now

$$-m^2=D_0\equiv p^p\equiv 1 \pmod{p_0} ,$$

since $p\equiv 1 \pmod{p_0}$. We see that -1 is a quadratic residue mod p_0. However, this is impossible, since $p_0\equiv 3 \pmod 4$. A contradiction shows that $|D_0|$ is not a square. Hence there exists a prime number q such that $(D_0)q$ is an odd integer, where the symbol $(D_0)q$ means the largest integer M such that D_0 is divisible by q^M (cf. [1]). Since $(p, a)=1$, we have

$$q\neq p , \quad (q, a)=1 , \quad (q, p-1)=1 .$$

Let d denote the discriminant of K. Then d is exactly divisible by q ([1], Theorem 2), since D_q is odd. It follows from Lemma 1 that the Galois group G of $f(x)=0$ over $\boldsymbol{Q}$ contains a transposition. Since p is a prime, G is primitive. Hence $G=S_p$ ([5], Theorem 13.3).

REMARK. If $p=3$, the Galois group of $x^p+ax+a=0$ is not always symmetric. For example, the Galois group of

$$x^3-7x-7=0$$

is cyclic, since its discriminant is

$$-4(-7)^3-27(-7)^2=7^2 .$$

§3. The case $p\equiv 1 \pmod 8$.

THEOREM 2. *Let $p\equiv 1 \pmod 8$ be a prime number and let a be a rational integer with $(p, a)=1$ such that*

$$f(x)=x^p+ax+a$$

is irreducible over $\boldsymbol{Q}$. Then the Galois group G of $f(x)=0$ over $\boldsymbol{Q}$ is the symmetric group S_p if and only if $(p-1)^{p-1}a+p^p$ is not a square. If $(p-1)^{p-1}a+p^p$ is a square, then G

is a non-cyclic simple group, and the minimal splitting field of $f(x)=0$ *is unramified (with respect to the finite prime spots) over* $\boldsymbol{Q}(\alpha)$, *where* α *denotes an arbitrary root of* $f(x)=0$.

PROOF. Since $p^p \equiv p \equiv 1 \pmod 8$, $(p-1)^{p-1}a+p^p=-m^2$ is impossible. Hence, if $(p-1)^{p-1}a+p^p$ is not a square, there exists a prime number q such that the discriminant d of $K=\boldsymbol{Q}(\alpha)$ is exactly divisible by q, and so $G=S_p$ (See the proof of Theorem 1). The second half of Theorem 2 is proved in [2] (pp. 123–125; $(p, d)=1$, and every prime factor of d is completely ramified in K).

REMARK. We proved in [2] (Theorem 5 and its proof) that, for every prime number $p \equiv 1 \pmod 8$, there exist infinitely many integers a with the following properties:

1. $f(x)=x^p+ax+a$ is irreducible over $\boldsymbol{Q}$;
2. $(p, a)=1$;
3. $(p-1)^{p-1}a+p^p$ is a square.

References

[1] K. KOMATSU, Integral bases in algebraic number fields, J. Reine Angew. Math., **278/279** (1975), 137–144.
[2] K. KOMATSU, Discriminants of certain algebraic number fields, J. Reine Angew. Math., **285** (1976), 114–125.
[3] K. KOMATSU, Square-free discriminants and affect-free equations, Tokyo J. Math., **14** (1991), 57–60.
[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