Tôhoku Math. Journ.
22(1970), 220-224.

UNRAMIFIED EXTENSIONS OF QUADRATIC NUMBER FIELDS, II

KÔJI UCHIDA

(Received December 25, 1969)

We have studied equations of type $X^n - aX + b = 0$, and have obtained some results on unramified extensions of quadratic number fields [3]. In this paper we have further results which include almost all of [3]. We do not refer to [3] in the following, though the techniques of proofs are almost equal to those of [3]. Theorems proved here are the following.[1] Notice that "unramified" means in this paper that every finite prime is unramified.

THEOREM 1. *Let k be an algebraic number field of finite degree. Let a and b be integers of k. K denotes the minimal splitting field of a polynomial*

$$f(X) = X^n - aX + b,$$

i.e., $K = k(\alpha_1, \cdots, \alpha_n)$ where $\alpha_1, \cdots, \alpha_n$ are the roots of $f(X) = 0$. Let $D = \prod_{i<j} (\alpha_i - \alpha_j)^2$ be the discriminant of $f(X)$. If $(n-1)a$ and nb are relatively prime, K is unramified over $k(\sqrt{D})$.

THEOREM 2. *Let $n \geqq 3$ be an integer, and A_n be an alternating group of degree n. Then there exist infinitely many quadratic number fields which have unramified Galois extensions with Galois groups A_n.*

1. Proof of Theorem 1. Let $\mathfrak{P}$ be any finite prime of K, and let $\mathfrak{p} = \mathfrak{P} \cap k$. Let G be the Galois group of K over k. Then G is a permutation group of $(\alpha_1, \cdots, \alpha_n)$. Let H be the subgroup of G consisting of the even permutations. H corresponds to $k(\sqrt{D})$. We shall prove Theorem 1 by showing that H meets with the inertia group of $\mathfrak{P}$ trivially. First we consider the factorization of $f(X)$ mod $\mathfrak{p}$. From $f(X) = X^n - aX + b$ and $f'(X) = nX^{n-1} - a$, it follows

$$Xf'(X) - nf(X) = (n-1)aX - nb.$$

1) After I prepared the manuscript of this paper, I knew that Y. Yamamoto had already obtained the same results which is to appear in Osaka Math. J. before long.

As $((n-1)a, nb)=1$, this does not vanish mod $\mathfrak{p}$. So $(n-1)aX-nb$ is the g. c. d. of $f(X)$ and $f'(X)$ mod $\mathfrak{p}$, if $f(X)$ and $f'(X)$ have common factors mod $\mathfrak{p}$. Therefore $f(X)$ is factorized as

$$f(X)\equiv\bar{f}_1(X)\cdots\bar{f}_r(X) \qquad (\mathrm{mod}\ \mathfrak{p})$$

or

$$f(X)\equiv((n-1)aX-nb)^2\bar{g}_2(X)\cdots\bar{g}_s(X) \qquad (\mathrm{mod}\ \mathfrak{p}),$$

according as $f(X)$ has only simple roots mod $\mathfrak{p}$ or not. In the above each $\bar{f}_i(X)$ is irreducible mod $\mathfrak{p}$ and $\bar{f}_i(X)\not\equiv\bar{f}_j(X)$ for $i\neq j$. Each $\bar{g}_i(X)$, $2\leqq i\leqq s$, is irreducible mod $\mathfrak{p}$ and $\bar{g}_i(X)\not\equiv\bar{g}_j(X)$ for $i\neq j$, and also $\bar{g}_i(X)\not\equiv(n-1)aX-nb$. By Hensel's lemma $f(X)$ is factorized in the local field $k_\mathfrak{p}$ in the form

$$(1) \qquad f(X)=f_1(X)\cdots f_r(X)$$

or

$$(2) \qquad f(X)=g_1(X)\cdots g_s(X),$$

where $f_i(X)\equiv\bar{f}_i(X)$ (mod $\mathfrak{p}$), $g_j(X)\equiv\bar{g}_j(X)$ (mod $\mathfrak{p}$), $j\geqq 2$ and $g_1(X)\equiv((n-1)aX-nb)^2$ (mod $\mathfrak{p}$). $K_\mathfrak{P}$ is obtained from $k_\mathfrak{p}$ by adjoining the roots of $f(X)=0$. The roots of $f_i(X)=0$ or $g_j(X)=0$, $j\geqq 2$, generate unramified extensions of $k_\mathfrak{p}$. So $K_\mathfrak{P}$ is unramified over $k_\mathfrak{p}$ in the case (1). If $K_\mathfrak{P}$ is ramified over $k_\mathfrak{p}$ in the case (2), $g_1(X)$ is irreducible of degree 2 and the inertia group is generated by the transposition of the roots of $g_1(X)=0$. So it meets with H trivially, and $\mathfrak{P}$ is unramified over $k(\sqrt{D})$. As we took $\mathfrak{P}$ arbitrarily, K is unramified over $k(\sqrt{D})$.

2. Proof of Theorem 2. In this section the ground field is taken as the field Q of the rational numbers. We find pairs of rational integers (a, b) such that $((n-1)a, nb)=1$ and the equations $f(X)=X^n-aX+b=0$ which have symmetric groups S_n as Galois groups. If we have infinitely many different $Q(\sqrt{D})$, Theorem 2 follows from Theorem 1. If a polynomial $f(X)$ is irreducible over Q, the Galois group of K over Q is a transitive permutation group. To find the Galois group, we apply the following

LEMMA [4, Theorem 13.3]. *If a primitive permutation group contains a transposition, it is a symmetric group.*

As we have seen in the proof of Theorem 1, the inertia group of a prime $\mathfrak{P}$ contains a transposition if $\mathfrak{P}$ is ramified. As the field Q has no unramified extension, there exist primes of K ramified over Q. Therefore the Galois group of K over Q contains a transposition. If we show it is primitive, it is a symmetric group by the above lemma. As any transitive group of a prime degree is primitive [4, Theorem 8.3], we have

PROPOSITION. *If $n=l$ is a prime and if $f(X)$ is irreducible over Q, the Galois group of K over Q is a symmetric group S_l. Therefore K is an unramified extension of $Q(\sqrt{D})$ with Galois group A_l.*

Now we show that there exist pairs of integers (a, b) satisfying the conditions in the first paragraph of this section. Let l be a prime number such that

$$l \equiv 1 \pmod{n-1}.$$

If b is divisible by l, then

$$X^n - aX + b \equiv X(X^{n-1} - a) \pmod{l} \tag{3}$$

holds. As Z/lZ contains all the $(n-1)$-st roots of unity, $X^{n-1} - a$ is irreducible mod l if a is a primitive root mod l. Then $X^n - aX + b$ has irreducible factors of degree 1 and degree $n-1$, if it is reducible over Q. But it has no factor of degree 1 if a is sufficiently large. Then $X^n - aX + b$ is irreducible over Q, and its Galois group is primitive by the factorization (3). We can choose a and b as $((n-1)a, nb) = 1$. Then all the conditions are satisfied.

Now let p be any prime number such that $(p, ln(n-1)) = 1$, where l is fixed as above. We show that there exists a pair (a, b) such that $D = D(a, b) = p \cdot D_0$, $(p, D_0) = 1$ and that satisfies the above conditions. Then we have infinitely many different $Q(\sqrt{D})$. D is calculated as

$$D = (-1)^{\frac{n(n-1)}{2}} \prod_i f'(\alpha_i) = (-1)^{\frac{n(n-1)}{2}} \prod_i (n\alpha_i^{n-1} - a)$$

$$= (-1)^{\frac{n(n-1)}{2}} \{n^n b^{n-1} - (n-1)^{n-1} a^n\}.$$

Let b be a multiple of l such that $b \equiv n-1 \pmod{p}$ and $(b, n-1) = 1$. As $(p, n) = 1$, we have a sufficiently large integer a_1 such that $a_1 \equiv n \pmod{p}$, $(a_1, nb) = 1$ and a_1 is a primitive root mod l. Then $D_1 = D(a_1, b)$ is divisible by p. If D_1 is divisible by p^2, we replace a_1 by

$$a = a_1 + nblp.$$

Then $D=D(a,b)$ is divisible by p, bue not divisible by p^2. This completes the proof.

COROLLARY 1. *Let G be a finite group. Then there exists an algebraic number field k which has an unramified extension with Galois group G. If G is of order n, k is taken as* $[k:Q]\leqq 2\cdot(n-1)!$

PROOF. Let K be a Galois extension of Q with Galois group S_n, which is unramified over $Q(\sqrt{D})$. Let q be a prime number such that $(q,D)=1$. Then $K(\sqrt{q})$ is unramified over $Q(\sqrt{qD})$ and its Galois group is a symmetric group S_n. G can be considered as a subgroup of S_n. If k denotes the subfield of $K(\sqrt{q})$ corresponding to G, k satisfies the conditions of Corollary.

REMARK. This corollary was proved by Fröhlich [1], though $[k:Q]\leqq(n-1)!\times(n!)!$ in his case.

COROLLARY 2. *Let F be any field of characteristic zero. Let a and b be indeterminates. Then the equation*

$$X^n - aX + b = 0 \tag{4}$$

has the Galois group S_n *over* $F(a,b)$.

PROOF. First we show this in the case F is an algebraic number field of finite degree. We may assume that F is normal over Q. Let (a_0, b_0) be a pair of rational integers such that the Galois group of

$$X^n - a_0X + b_0 = 0 \tag{5}$$

is a symmetric group S_n. Let $D_0=D(a_0,b_0)$ be its discriminant. By the proof of Theorem 2, (a_0,b_0) can be taken as $Q(\sqrt{D_0})$ is not included in F. Then the Galois group of (5) over F is also S_n. So the Galois group of (4) over $F(a,b)$ is also S_n. Now let $\alpha_1,\cdots,\alpha_n$ be the roots of the equation (4). We put $K=Q(a,b,\alpha_1,\cdots,\alpha_n)$. Above argument shows that an algebraic closure of Q and K are linearly disjoint over Q. Hence K is a regular extension of Q. Let F be arbitrary. F and K are free over Q. As K is regular over Q, they are linearly disjont over Q [2. Chap. III. Theorem 3]. Therefore the Galois group of (4) over $F(a,b)$ is isomorphic to one over $Q(a,b)$, and the proof is completed.

REMARK. If F is not of characteristic zero this corollary does not hold in general. In fact, if F is of characteristic p, the Galois group of the equation

$$X^{p^m} - aX + b = 0$$

is solvable. It is easily shown from the fact that $(\alpha - \beta)^{p^m - 1} = a$, where α and β are two roots of above equation.

EXAMPLES. We give examples for small a, b and n. In all examples $f(X)$ are irreducible over Q and the Galois groups over $Q(\sqrt{D})$ are alternating groups.

n	a	b	D
5	1	1	$2869 = 19 \times 151$
5	-2	1	11317 (prime)
6	1	1	$-43531 = -101 \times 431$
6	1	-1	$49781 = 67 \times 743$
7	1	1	-776887 (prime)
7	-1	1	$-870199 = -11 \times 239 \times 331$
8	1	-1	$-17600759 = -11 \times 1600069$
9	1	1	$370643273 = 7 \times 11 \times 13 \times 43 \times 79 \times 109$
9	-1	1	$404197705 = 5 \times 197 \times 410353$
10	1	1	$-9612579511 = -29 \times 4127 \times 80317$
10	1	-1	$10387420489 = 173 \times 60042893$

REFERENCES

[1] A. Fröhlich, On non-ramified extensions with prescribed Galois group, Mathematika, 9(1962).
[2] S. Lang, Introduction to algebraic geometry, Interscience Publishers, 1958.
[3] K. Uchida, Unramified extensions of quadratic number fields, I, Tôhoku Math. J., 22(1970).
[4] H. Wielandt, Finite permutation groups, Academic Press, 1964.

MATHEMATICAL INSTITUTE,
TÔHOKU UNIVERSITY
SENDAI, JAPAN