Tôhoku Math. Journ.
22(1970), 138-141.

UNRAMIFIED EXTENSIONS OF QUADRATIC NUMBER FIELDS, I

KÔJI UCHIDA

(Received November 20, 1969)

In this paper we study equations of type $X^n - aX + b = 0$, and give examples of (non-solvable) unramified extensions of quadratic number fields. "Unramified" means that any finite prime is unramified.

1. Proof of Theorem 1.

THEOREM 1. *Let k be an algebraic number field of finite degree. Let a and b be integers of k. K denotes the 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 $f(X) = 0$. If $(n-1)a$ and nb are relatively prime, any prime ideal of K has the ramification index 1 or 2 over k.

PROOF. Let $\mathfrak{p}$ be a prime of k and let $\mathfrak{P}$ be a prime of K over $\mathfrak{p}$. We consider splitting of the polynomial $f(X)$ over a local field $k_\mathfrak{p}$. If the congruence equation $f(X) \equiv 0 \pmod{\mathfrak{p}}$ has no multiple roots, $f(X)$ splits as

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

over $k_\mathfrak{p}$, where $f_i(X)$ are irreducible over $k_\mathfrak{p}$ and also mod $\mathfrak{p}$. Then $K_\mathfrak{P}$ is unramified over $k_\mathfrak{p}$. Now we assume $f(X) \equiv 0 \pmod{\mathfrak{p}}$ has multiple roots. As

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

and $((n-1)a, nb) = 1$, $\mathfrak{p} \nmid (n-1)a$ holds. Then the $(n-1)aX - nb$ is the g.c.d. of $f(X)$ and $f'(X)$ mod $\mathfrak{p}$. So

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

holds, where each $\bar{g}_i(X)$ is irreducible and relatively prime to $\bar{g}_j(X)$, $j \neq i$, and to $(n-1)aX-nb$. By Hensel's lemma $f(X)$ splits over $k_{\mathfrak{p}}$ in the form

$$f(X) = g_1(X)g_2(X)\cdots g_s(X),$$

where $g_i(X)\equiv\bar{f}_i(X) \pmod{\mathfrak{p}}$, $i\geqq 2$. The roots of $g_i(X)=0$, $i\geqq 2$, generate unramified extensions of $k_{\mathfrak{p}}$. As $g_1(X)$ is of degree 2, the ramification index of $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ is at most 2.

COROLLARY. *Let $k=Q$ be the field of the rational numbers. Let*

$$D=\prod_{i<j}(\alpha_i-\alpha_j)^2$$

be the discriminant of $f(X)=0$. Assume that any prime number which appears in D appears odd times. Then $K=Q(\alpha_1,\cdots,\alpha_n)$ is unramified over $Q(\sqrt{D})$.

PROOF. Every prime number which is ramified in K/Q appears in D. By assumption it is ramified in $Q(\sqrt{D})/Q$. As the ramification index is 2, it is unramified in $K/Q(\sqrt{D})$.

2. As applications of Theorem 1, we obtain some examples of unramified extensions of quadratic fields.

THEOREM 2. *$f(X)=X^n-X+1$ $(n=5,6,7)$ satisfy the condition of Corollary of Theorem 1. Galois groups of $f(X)=0$ are symmetric groups. Therefore there exist unramified extensions of quadratic fields with alternating groups A_5, A_6, A_7 or symmetric groups S_5, S_6, S_7 as Galois groups.*

PROOF. 1) We first show that the condition of Corollary is satisfied. In the general case,

$$D=\prod_{i<j}(\alpha_i-\alpha_j)^2=(-1)^{n(n-1)/2}\prod_i f'(\alpha_i),$$

and

$$\begin{aligned}\prod_i f'(\alpha_i) &= \prod_i (n\alpha_i^{n-1}-a)\\ &= \prod_i ((n-1)a\alpha_i-nb)/\prod_i \alpha_i\end{aligned}$$

$$= n^n b^{n-1} - (n-1)^{n-1} a^n$$

hold. Let D_5, D_6 and D_7 be discriminants D corresponding to $n=5, 6$ and 7 respectively. Then

$$D_5 = 5^5 - 4^4 = 3125 - 256 = 2869 = 19 \times 151$$

$$D_6 = 5^5 - 6^6 = 3125 - 46656 = -43531 = -101 \times 431$$

and

$$D_7 = 6^6 - 7^7 = 46656 - 823543 = -776887 \text{ (prime)}$$

hold.

2) Now we find the Galois groups of these equations. If $n=5$(resp. $n=7$), $f(X)$ is irreducible mod 5 (resp. mod 7). If $n=6$, it is irreducible mod 2. So $f(X)$ is irreducible in each case. When n is a prime number, a transitive permutation group of n letters is a symmetric group if it contains a transposition.

$$X^5 - X + 1 \equiv (X^2 - X + 1)(X^3 + X^2 + 1) \pmod 2$$

and

$$X^7 - X + 1 \equiv (X^2 - X - 1)(X^5 + X^4 - X^3 - X - 1) \pmod 3$$

are factorizations into prime factors mod 2 and mod 3 respectively. So in these cases Galois groups contain transpositions, and they are symmetric groups. When $n=6$,

$$X^6 - X + 1 \equiv (X+1)(X^2 + X - 1)(X^3 + X^2 + X - 1) \pmod 3$$

and

$$X^6 - X + 1 \equiv (X-2)(X^5 + 2X^4 - 3X^3 + X^2 + 2X + 3) \pmod 7$$

hold. The last factor of degree 5 is irreducible, because $X^6 - X + 1$ and $X^{49} - X$ have no common factors except $X-2$. So the Galois group is a symmetric group by [3. §61].

3) In every case $K/Q(\sqrt{D})$ is an unramified extension with an alternating group as the Galois group. Let p be a prime number which does not appear in D. Then each $K(\sqrt{p})/Q(\sqrt{pD})$ is unramified and its Galois group is a symmetric group.

REMARK. The case $n=5$ has been proved by Fujisaki [2]. Fröhlich [1] proves that every finite group appears as a Galois group of some unramified extension. Our theorem suggests that many non-solvable groups can be Galois groups of unramified extensions of quadratic fields. More numerical examples will be given in the forthcoming paper.

THEOREM 3. *There exist infinitely many real quadratic field with class numbers divisible by* 3.

PROOF. If a cubic irreducible equation $X^3-aX+b=0$ $(a, b \in Z)$ satisfies the condition of Theorem 1, the Galois group of K/Q is a symmetric group of three letters. Then $K/Q(\sqrt{D})$ is an unramified abelian extensions, and so the class number of $Q(\sqrt{D})$ is divisible by 3, where $D=4a^3-27b^2$ is the discriminant of a given equation. Therefore it is enough to prove there exist infinitely many different $Q(\sqrt{D})$ with positive D.

If we assume $a \geqq 2$, $a \equiv 1 \pmod 3$ and $b=1$, X^3-aX+1 is irreducible and satisfies the condition of Theorem 1 and $D>0$. Then if $p \neq 2$, 3 is a prime number, the necessary and sufficient condition for $p|D$ for some a is that 4 is a cubic residue mod p. If $p \equiv 2 \pmod 3$, any number is a cubic residue. So there exists $a_1>2$ such that

$$p|4a_1^3-27\,.$$

As the equation

$$a_1+rp \equiv 1 \pmod 3$$

has an integral solution r, we may assume that $a_1 \equiv 1 \pmod 3$. If $4a_1^3-27$ is divisible by p^2, we replace a_1 by $a=a_1+3p$. Then $4a^3-27$ is divisible by p but not by p^2. So p is ramified in $Q(\sqrt{D})/Q$. As there exist infinitely many p satisfying the above condition, there exist infinitely many different $Q(\sqrt{D})$.

REFERENCES

[1] A. FRÖHLICH, On non-ramified extensions with prescribed Galois group, Mathematika, 9(1962).

[2] G. FUJISAKI, On an example of an unramified Galois extension (in Japanese), Sûgaku, 9(1957). See MR 21(1960), n° 1968.

[3] B. L. VAN DER WAERDEN, Moderne Algebra, Bd. 1, Springer.

MATHEMATICAL INSTITUTE
TÔHOKU UNIVERSITY
SENDAI, JAPAN