Yamamura, K.
Osaka J. Math.
23 (1986), 471–478

ON UNRAMIFIED GALOIS EXTENSIONS OF REAL QUADRATIC NUMBER FIELDS

KEN YAMAMURA

(Received February 26, 1985)

1. Introduction

The purpose of this note is to construct infinitely many real quadratic number fields each having an A_5-extension which is unramified at all primes including the infinite primes (abbrev. strictly unramified). Here, a G-extension means a Galois extension having G as its Galois group, and S_n (resp. A_n) denotes the symmetric group (resp. the alternating group) of degree n. In [12], Yamamoto constructed infinitely many real quadratic number fields each having an A_n-extension which is unramified at all finite primes (abbrev. weakly unramified) for each $n \geqq 4$, but they are always ramified at the two infinite primes. In this note, we shall prove the following

Theorem. *Let S_1 and S_2 be given finite sets of prime numbers satisfying $S_1 \cap S_2 = \emptyset$ and $2,5 \notin S_2$. Then there exist infinitely many real quadratic number fields F satisfying the following conditions:*
(a) *F has a strictly unramified A_5-extension.*
(b) *All primes in S_1 are unramified in F.*
(c) *All primes in S_2 are ramified in F.*

Composing such an A_5-extension with some real quadratic number field, we obtain infinitely many real quadratic number fields with a strictly unramified S_5-extension. Furthermore, we describe a method for constructing infinitely many real quadratic number fields having a strictly unramified A_n-extension for larger n, and give some examples of real quadratic number fields with class number one having a strictly or weakly unramified A_n-extension, for $n=5$, 6, and 7.

This note is based on a part of the author's Master's thesis [13].

2. Proof of the theorem

Take a polynomial of the form

$$f(x) = x^5 - 2m^2 x^3 + (6m^2 - 1)x - (m-4)\,.$$

(m: a positive integer)

Our proof consists in showing that under some assumptions on m $\boldsymbol{Q}(\sqrt{D})$ is a real quadratic number field and the splitting field K of $f(x)$ over $\boldsymbol{Q}$ is a strictly unramified A_5-extension of it, where D is the discriminant of $f(x)$. Imposing on m some congruence conditions, we prove them and the conditions (b) and (c). Our proof is based on the following two lemmas.

Lemma 1. *Let k be an algebraic number field of finite degree, and $f(x)$ be a monic irreducible polynomial over k with integral coefficients and discriminant D. Let K be the splitting field of $f(x)$ over k. If, for each prime ideal $\mathfrak{p}$ of k which is ramified in K, $f(x)$ mod $\mathfrak{p}$ has exactly one multiple root and its multiplicity is two, then $K/k(\sqrt{D})$ is weakly unramified.*

This can be proved easily as in Yamamoto's proof for the case $k=\boldsymbol{Q}$ ([12], pp. 69).

Lemma 2. *Suppose that a polynomial*

$$f(x) = x^5-2ax^3+bx+c, \qquad a, b, c\in\boldsymbol{Z}$$

satisfies the following conditions:
(i) *$f(x)$ is irreducible over $\boldsymbol{Q}$.*
(ii) $b\equiv c\equiv 1 \pmod 2$.
(iii) *$a>0$, $a^2>b>0$, and*

$$4(-2a+d)(3a+d)^{3/2}>25\sqrt{5}\,|c|\,,$$
$$4(2a+d)(3a-d)^{3/2}>25\sqrt{5}\,|c|\,,$$

where $d=\sqrt{9a^2-5b}$; This is a necessary and sufficient condition that all roots of $f(x)$ are real.
(iv) $(a,b,5)=(b(a^2-b),c,D)=1$.
(v) *Any prime factors of (A,B,D) are those of $2ac$, where D is the discriminant, of $f(x)$:*

$$D = 3125c^4-4000ab^2c^2+256b^5+7200a^3bc^2-512a^2b^4-3456a^5c^2+256a^4b^3\,,$$

and

$$A = 5ac^2(3a^2-5b)+8b^2(a^2-b)^2\,,$$
$$B = 125ac^2-16b(a^2-b)(6a^2-5b)\,.$$

Then $\boldsymbol{Q}(\sqrt{D})$ is a real quadratic number field and the splitting field K of $f(x)$ is a strictly unramified A_5-extension of it.

Proof. First we show that K is an S_5-extension of $\boldsymbol{Q}$, which implies that D is not a square and K is an A_5-extension of quadratic number field $\boldsymbol{Q}(\sqrt{D})$. Let G be the Galois group of $K/\boldsymbol{Q}$. Since $f(x)$ is an irreducible polynomial of

degree five, G is a transitive subgroup of S_5. By (ii), the irreducible decomposition of $f(x)$ mod 2 is

$$f(x)\equiv x^5+x+1\equiv(x^2+x+1)(x^3+x^2+1) \pmod 2. \tag{1}$$

Hence G contains a permutation τ of type $(i,j)(k,l,m)$, so $\tau^3=(i,j)\in G$, i.e., G contains a transposition. Therefore $G=S_5$.

Next we prove the unramifiedness of $K/\boldsymbol{Q}(\sqrt{D})$. By easy computations, we can verify that (iii) is a necessary and sufficient condition that all roots of $f(x)$ are real. Therefore, K is totally real; so all infinite primes are unramified in $K/\boldsymbol{Q}(\sqrt{D})$. To show the unramifiedness of finite primes, we verify that $f(x)$ satisfies the condition of Lemma 1. By (1), 2 is unramified in K. Hence each prime divisor of 2 in $\boldsymbol{Q}(\sqrt{D})$ is unramified in K. Since the primes which are ramified in K are prime factors of D, it is sufficient to show (*) below for each odd prime $p\,|\,D$.

(*) $f(x)\equiv 0 \pmod p$ has at most one multiple root, and if it has, then its multiplicity is two.

By (iv), $\bar{x}=0$ is not a multiple root of $\bar{f}(x)=0$, where $\bar{}$ denotes the reduction modulo p. Therefore, if $\bar{f}(x)=0$ has a multiple root, then it is a non-zero root of $\bar{f}'(x)=0$, so it is a non-zero root of $\bar{g}(x)=0$;

$$g(x) = 5f(x)-xf'(x) = -4ax^3+4bx+5c\,.$$

We have three cases; i.e., $p\,|\,a$, $p\,|\,c$ and $p\nmid ac$. In the case $p\,|\,a$: By (iv), $\bar{g}(x)$ has degree at most one and is not zero. Hence in this case, (*) holds.

In the following, let $p\nmid a$. If $\bar{f}(x)=0$ and $\bar{g}(x)=0$ have a common root, then it is a root of $\bar{h}(x)$;

$$h(x) = 4a^2f(x)+(ax^2-2a^2+b)\,g(x) = 5acx^2-4b(a^2-b)\,x-c(6a^2-5b)\,.$$

In the case $p\,|\,c$: By (iv)

$$\bar{h}(x) = -4\bar{b}(\bar{a}^2-\bar{b})\,\bar{x}\neq 0\,.$$

Therefore, $\bar{f}(x)=0$ and $\bar{g}(x)=0$ do not have any common root other than zero.

In the case $p\nmid ac$: If $\bar{g}(x)=0$ and $\bar{h}(x)=0$ have a common root, then it is a root of

$$25ac^2\,g(x)+\{20acx+16b(a^2-b)\}\,h(x) = -8Ax+Bc\equiv 0 \pmod p.$$

Hence by (v), (*) holds.

REMARK. The conditions of Lemma 2 are too complicated for us to use in this form. So we slightly simplify them. Take a triple (a,b,c) satisfying (ii), (iv), and $a>0$, $a^2>b>0$. For such (a,b,c), if $f(x)$ is reducible, then $2\,|\,a\,|\leqq |c|^2+3\,|c|$ and $|b|\leqq 3\,|c|^2$ follow from (1) and easy computations. Therefore,

(i)′ If $2|a|>|c|^2+3|c|$, or $|b|>3|c|^2$, then $f(x)$ is irreducible.

When $5\nmid D$, (v) is equivalent to

(v)′ Any prime factors of (B, d^2d', D) are those of $2ac$, where $d'=4a^2-5b$, because

$$2(6a^2-5b)A+b(a^2-b)B = 5ac^2d^2d' .$$

Let $B_1=5^5c^2-2^6\cdot 3^3a^5$ and $B_2=5^5c^2-2^7a^5$. Then

$$5^2B\equiv aB_1 \pmod{d^2},\ 5^2B\equiv aB_2 \pmod{d'} ,$$

and

$$5^5D\equiv 0 \pmod{(B_1, d^2)},\ 5^5D\equiv 0 \pmod{(B_2, d')} .$$

Therefore, when $5\nmid D$, (v) is equivalent to

(vi) Any prime factors of (B_1, d^2) and (B_2, d') are those of $10ac$.

Proof of the theorem. First, for each pair (S_1, S_2), we show the existence of such an F. We take

$$f(x) = x^5-2m^2x^3+(6m^2-5)x-(m-4) ,$$

where m is a positive integer satisfying the following conditions:

(1) For each $q_0\in S_0 = \{3, 29, 31\}-S_2$,
$m\equiv -1 \pmod{q_0}$.

(2) For each $q_1\in S_0' = S_1\cup\{2, 5, 7, 11, 13, 79, 271, 1481\}-S_0\cup S_2$,
$m\equiv 1 \pmod{q_1}$.

(3) For each $q_2\in S_2$,
$q_2\| m$.

Now we verify the conditions (i)–(v) of Lemma 2. In this case,

$$a = m^2,\ b = 6m^2-5,\ c=-(m-4),\ d = 3m^2-5,\ d' = 4m^4-30m^2+25 .$$

Since $b>3m^2>3|c|^2$, by (i)′ $f(x)$ is irreducible. By (2), (ii) holds. By the conditions (1) and (2), m is large enough that one can easily verify that (iii) is satisfied. Since $a\equiv b\equiv m^2\equiv 1 \pmod 5$, $(a, b, 5)=1$. Since

$$b+(6m+24)c = 91 = 7\cdot 13,\ a^2-b+(m^3+4m^2+10m+40)c = 165 = 3\cdot 5\cdot 11 ,$$

we have $(b(a^2-b), c)\,|\,3\cdot 5\cdot 7\cdot 11\cdot 13$, but from the conditions for m, c is prime to $3\cdot 5\cdot 7\cdot 11\cdot 13$. Therefore $(b(a^2-b), c)=1$. Hence (iv) is satisfied. Since $D\equiv 1 \pmod 5$, we show (vi) instead of (v). Now as greatest common divisors in $\boldsymbol{Z}[m]$, we have

$$(B_1, d) = 5^6\cdot 7\cdot 11 ,$$

and

$$(B_2, d') = 3^3 \cdot 5^7 \cdot 29^3 \cdot 79 \cdot 271 \cdot 1481 ,$$

but from the conditions for m, we have $d \not\equiv 0$ $(5 \cdot 7 \cdot 11)$, and $d' \not\equiv 0 \pmod{3 \cdot 5 \cdot 29 \cdot 79 \cdot 271 \cdot 1481}$. Therefore $(B_2, d')=1$. Hence (vi) is satisfied. By Lemma 2, it follows that (a) is satisfied. Now we verify (b) and (c). For any $q_0 \in S_0$, $a \equiv b \equiv 1$, $c \equiv 5 \pmod{q_0}$. Therefore,

$$D \equiv 5^2 \cdot 11 \cdot 7079 \not\equiv 0 \pmod{q_0} .$$

For any $q_1 \in S_0'$, $a \equiv b \equiv 1$, $c \equiv 3 \pmod{q_1}$. Therefore,

$$D \equiv 3^2 \cdot 29 \cdot 31^2 \not\equiv 0 \pmod{q_1} .$$

Hence for each $q \in S_0 \cup S_0'$, we have $q \nmid D$. Therefore, q is unramified in F. Since $S_1 \subseteq S_0 \cup S_0'$, (b) is satisfied. For each $q_2 \in S_2$,

$$a \equiv 0, \ b \equiv -5, \ c \equiv -m+4 \pmod{q_2^2} .$$

Since $D \equiv 5^5 c^4 + 4^4 b^5 \pmod{a}$, we obtain

$$D \equiv -4^4 5^5 m \pmod{q_2^2} .$$

Hence $q_2 \| D$, because $q_2 \neq 2, 5$. Therefore (c) is satisfied. Thus F satisfies the conditions (a)–(c).

It remains to be shown that the set $F(S_1, S_2)$ of such fields F satisfying the conditions (a)–(c) is infinite. Suppose $F(S_1, S_2)$ is finite:

$$F(S_1, S_2) = \{F_1, \cdots, F_s\} .$$

Then the set S_3 of all prime numbers which are ramified in at least one $F_i (1 \leqq i \leqq s)$ is finite. We take a prime number p such that $p \notin S_1 \cup \{2, 5\} \cup S_3$, and put $S_2' = S_2 \cup \{p\}$. Then $S_1 \cap S_2' = \phi$, and $2, 5 \in S_2$. Therefore, we have $F(S_1, S_2') \neq \phi$. Since by definition $F(S_1, S_2')$ is a subset of $F(S_1, S_2)$, $F' \in F(S_1, S_2)$ coincides with some F_i. Therefore p is ramified in F_i, which contradicts the choice of p. Hence $F(S_1, S_2)$ is infinite.

Corollary to the theorem. *Let S_1, S_2 be given finite sets of prime numbers satisfying $S_1 \cap S_2 = \phi$, and $2, 5 \notin S_2$. Then there exist infinitely many real quadratic number fields L satisfying the following conditions:*

(a)′ *L has a strictly unramified S_5-exptension.*

(b)′ *All primes in S_1 are unramified in L.*

(c)′ *All primes in S_2 are ramified in L.*

Proof. For S_1 and S_2, we take $F = \boldsymbol{Q}(\sqrt{D})$ and K in the theorem. Take a prime number $p \equiv 1 \pmod 4$ not contained in $S_1 \cup \{5\}$ which is unramified in

F. Then $L=\boldsymbol{Q}(\sqrt{pD})$ satisfies the conditions above, and a composite field $K\cdot\boldsymbol{Q}(\sqrt{p})$ is a strictly unramified S_5-extension of L. These statements easily follow from the genus theory and Galois theory. The infiniteness follows from that of such prime numbers p.

3. Notes and examples

It is natural to expect that there exist infinitely many real quadratic number fields each having a strictly unramified A_n-extension for larger n. However, it seems difficult to construct such fields in the same way as above, because the number of terms of the polynomial whose roots are all real increases with its degree. Instead, we shall look at the discriminant, as follows:

Proposition. *Let $f(x)$ be a monic irreducible polynomial over $\boldsymbol{Q}$ of degree n with integral coefficients and square-free discriminant D. Let K be the splitting field of $f(x)$ over $\boldsymbol{Q}$. Then $K/\boldsymbol{Q}(\sqrt{D})$ is a weakly unramified A_n-extension.*

This follows from the following three lemmas; the unramifiedness follows from Lemma 3, and it follows from Lemma 4 and 5 that the Galois group of $K/\boldsymbol{Q}$ is S_n.

Lemma 3. *Let k be an algebraic number field of finite degree, and $f(x)$ be a monic irreducible polynomial over k with integral coefficients and discriminant D. Let K be the splitting field of $f(x)$ over k, and E be the field obtained by adjoining one root of $f(x)$ to k. If, for each prmie ideal $\mathfrak{p}$ of k which is ramified in K, $\mathfrak{p}\|D_{E/k}$ ($D_{E/k}$: the relative discriminant of E/k), then $K/k(\sqrt{D})$ is weakly unramified.*

Lemma 3 is easily deduced from Lemma 1. We note that the unramifiedness is based on the following fact: for each ramified prime of K, its inertia group with respect to K/k is a cyclic group generated by a transposition.

Lemma 4. *Let K be a Galois extension over $\boldsymbol{Q}$ with its Galois group G. For each finite prime $\mathfrak{P}$ of K, let $T_{\mathfrak{P}}$ denote the inertia group with respect to $\boldsymbol{Q}$. Let H be the group generated by all $T_{\mathfrak{P}}$, where $\mathfrak{P}$ runs over all finite primes of K. Then $H=G$.*

Proof. Let F be the fixed field of H. Then $F/\boldsymbol{Q}$ is unramified, whence $F=\boldsymbol{Q}$ by Minkowski's theorem.

Lemma 5. *Let H be a subgroup of S_n generated by transpositions. If H is transitive, then $H=S_n$.*

Proof. We call T a chain if T is a subset of S_n consisting of transpositions $(i_1\,i_2)$, $(i_2\,i_3)$, $\cdots$, $(i_{m-1}\,i_m)$ such that all i_j $(1\leqq j\leqq m)$ are mutually different, and we put $1(T)=m$. Let $M=\max\{1(T)\,|\,H\supset T\text{: chain}\}$. We claim that $M=n$. Suppose $M<n$. Take a chain $T_0\subset H$ such that $1(T_0)=M$. By the transitivity of

H, H contains a transposition $(i\,j)$ such that $i=i_s$ for some $s(1\leqq s\leqq M)$ and $j\neq i_t$ for any $t(1\leqq t\leqq M)$. Since T_0 generates S_M, we can replace T_0 and renumber such that $i=i_M$. Hence $1(T_0\cup\{(i\,j)\})>M$. It is a contradiction. Therefore, $M=n$. Hence $H=S_n$.

The author was taught Lemma 4 and 5 by Osada [5].

From this point of view, for our purpose it is sufficient to find polynomials over $\boldsymbol{Q}$ with integral coefficients and square-free discriminants. This enables us to give examples easily.

Now we give examples of real quadratic number fields with class number one having a strictly or weakly unramified A_n-extension which is an S_n-extension of $\boldsymbol{Q}$ for $n=5$, 6, and 7. We have many examples, so we give a few examples in each case. In most cases, the first example is a field whose discriminant seems to be minimum among such fields. For example, it is true for $\boldsymbol{Q}(\sqrt{1609})$. (See 2(a) below.) We can prove it, using the following fact due to Hunter [3]:

"The minimum discriminant of quintic fields with one real and four imaginary conjugate fields is 1609."

In the following, h^+ denotes the class number in the narrow sense.

1. Strictly unramified cases.

(a) $n=5$.

$h^+=1$. $\boldsymbol{Q}(\sqrt{p})$: $p=36497, 81509, \cdots, 255877, \cdots, 422069, \cdots$.

$h^+=2$. $\boldsymbol{Q}(\sqrt{m})$: $m=81589, \cdots, 119649, \cdots, 274129, \cdots$.

(b) $n=6$.

$h^+=1$. $\boldsymbol{Q}(\sqrt{p})$: $p=592661, 1134389, \cdots$.

$h^+=2$. $\boldsymbol{Q}(\sqrt{m})$: $m=1202933, \cdots$.

(c) $n=7$.

$h^+=1$. The author does not know any examples.

$h^+=2$. $\boldsymbol{Q}(\sqrt{m})$: $m=20134393, \cdots$.

2. Weakly unramified cases.

(a) $n=5$.

$h^+=1$. $\boldsymbol{Q}(\sqrt{p})$: $p=1609, 1777, 2297, 3089, \cdots, 11317^*, \cdots$.

$h^+=2$. $\boldsymbol{Q}(\sqrt{m})$: $m=2869^{**}, 3017, 3233, \cdots, 4897, \cdots, 11469, \cdots$.

(b) $n=6$.

$h^+=1$. $\boldsymbol{Q}(\sqrt{p})$: $p=29077, 40277, \cdots, 104173, \cdots$.

$h^+=2$. $\boldsymbol{Q}(\sqrt{m})$: $m=31133, 39269, \cdots, 107417, \cdots, 192649, \cdots$.

(c) $n=7$.

$h^+=1$. $\boldsymbol{Q}(\sqrt{p})$: $p=1180241, \cdots, 1946657, \cdots, 2532637, \cdots$.

$h^+=2$. $\boldsymbol{Q}(\sqrt{m})$: $m=1264157, \cdots, 5543633, \cdots, 8058989, \cdots$.

(*, **: Given in [12] and [2] respectively.)

From the same point of view, it seems that we can obtain many such ex-

amples for larger n. Therefore, though we are lacking in examples, we may expect the following conjecturally statement:

"For each natural number $n \geqq 5$, there exist infinitely many real quadratic number fields with class number one each having an unramified A_n-extension for both strictly and weakly unramified cases."

References

[1] H. Cohn: *A numerical study of quintics of small discriminant,* Comm. Pure. Appl. Math. **8** (1955), 377–386.

[2] G. Fujisaki: *On an example of an unramified extension* (in Japanese), Sugaku **9** (1957), 97–99.

[3] J. Hunter: *The minimum discriminant of quintic fields,* Proc. Glasgow Math. Assoc. **3**, Part 2 (1957), 57–67.

[4] S. Lang: Algebraic number theory, Addison-Wesley, 1970.

[5] H. Osada: Private communication.

[6] M. Pohst: *The minimum discriminant of seventh degree totally real algebraic number fields,* Number theory and algebra, 235–240, Academic Press, New York, 1977.

[7] M. Pohst, P. Weiler and H. Zassenhaus: *On effective computation of fundamental units.* II, Math. Comp. **38** (1982), 293–329.

[8] T. Sasaki, Y. Kanada, and S. Watanabe: *Calculation of discriminant of high degree equation,* Tokyo J. Math. **4** (1981), 493–499.

[9] K. Uchida: *Unramified extensions of quadratic number fields* I, II, Tohoku Math. J. **23** (1970), 138–141, 220–224.

[10] H. Wada: Applications of computers to number theory (in Japanese), Lecture Note in Math. No. 7 (1980), Sophia Univ.

[11] ————: A table of ideal class numbers of real quadratic fields, Lecture Note in Math. No. 10 (1981), Sophia Univ.

[12] Y. Yamamoto: *On unramified Galois extensions of quadratic number fields,* Osaka J. Math. **7** (1970), 57–76.

[13] K. Yamamura: *On unramified extensions of algebraic number fields* (in Japanese), Master's thesis, 1984, Tokyo Univ.

Department of Mathematics
Faculty of Science,
University of Tokyo
Hongo, Tokyo 113, Japan