ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 25, Number 2, Spring 1995

UNRAMIFIED QUADRATIC EXTENSIONS OF A QUADRATIC FIELD

BLAIR K. SPEARMAN AND KENNETH S. WILLIAMS

ABSTRACT. Given a quadratic field K, we determine the number of quadratic extensions of K, which are unramified at all finite primes.

Let Q denote the field of rational numbers. Let K be a quadratic extension of Q, and let L be a quadratic extension of K. We show (Theorem 1) that if L/K is unramified at all finite primes then L is a bicyclic extension of Q, that is, $\mathrm{Gal}(L/Q) \simeq Z_2 \times Z_2$. Then in Theorem 2 we give the precise form of those bicyclic extensions L such that L/K is unramified at all finite primes. Theorem 2 then enables us to determine for a given quadratic field K the number of unramified quadratic extensions of K (Theorem 3).

Theorem 1. *Let K be a quadratic extension of Q. Let L be a quadratic extension of K. If L/K is unramified at all finite primes, then L is a bicyclic extension of Q.*

Proof. As K is a quadratic extension of Q, we have $K = Q(\sqrt{c})$, where c is a square-free integer not equal to 1. As L is a quadratic extension of K, there exists a nonsquare integer μ of K such that $L = K(\sqrt{\mu})$. We set $\mu O_K = RS^2$, where R and S are integral ideals of the ring O_K of integers of K with R square-free. It was shown in [**5**, Theorem 1] that the relative discriminant of L over K is given by $d(L/K) = RT^2$, for some integral ideal T of O_K. As L/K is unramified at all finite primes, we have $R = T = O_K$, and thus $\mu O_K = S^2$.

Let $P_1, \ldots, P_t$ be the distinct prime ideals of O_K which divide $d(K) = c$ or $4c$. It is well known (see, for example, [**1**, p. 249]) that the class

Received by the editors on September 15, 1993.
Research of the second author was supported by Natural Sciences and Engineering Research Council of Canada grant A-7233.
1991 *Mathematics Subject Classification.* Primary 11S15, 11R16.
Key words and phrases. Unramified quadratic extensions, biquadratic fields.

of the ideal S contains the ideals $P_{i_1}\cdots P_{i_r}$ and $(P_1\cdots P_t)/(P_{i_1}\cdots P_{i_r})$ for some integers $i_1,\dots,i_r$ with $1\le i_1<\cdots<i_r\le t$ and $0\le r\le t$. At least one of $N_{K/Q}(P_{i_1}\cdots P_{i_r})$ and $N_{K/Q}((P_1\cdots P_t)/(P_{i_1}\cdots P_{i_r}))$ is odd and is a positive divisor d of c. Hence, $S\sim\langle d,\sqrt{c}\rangle$. Thus there exist $\alpha(\neq 0)\in O_K$ and $\beta(\neq 0)\in O_K$ with $\alpha S=\beta\langle d,\sqrt{c}\rangle$. Squaring we obtain (as $\mu O_K=S^2$) $\alpha^2\mu O_K=\beta^2 dO_K$. Hence there is a unit ε of O_K such that $\alpha^2\mu=\beta^2 d\varepsilon$. As μ is not a square in O_K, $d\varepsilon$ is not a square in O_K, and $L=K(\sqrt{\mu})=K(\sqrt{d\varepsilon})$.

If $\varepsilon=\pm 1$, then $L=Q(\sqrt{c},\sqrt{\pm d})$ is bicyclic. If $c=-1$ the only other units of O_K are $\varepsilon=\pm i$. As d is a positive divisor of c we have $d=1$. Hence,

$$L=Q(\sqrt{-1},\sqrt{\pm i})=Q(\sqrt{i})=Q\left(\frac{1+i}{\sqrt{2}}\right)=Q(\sqrt{-1},\sqrt{2})$$

is a bicyclic extension of Q. However, $L=Q(\sqrt{-1},\sqrt{2})$ is not an unramified extension of $Q(\sqrt{-1})$ since $\langle 1+i\rangle=\langle 1+(1+i)/\sqrt{2}\rangle^2$ in O_L, so this possibility in fact cannot occur.

If $c=-3$ the only other units of O_K are $\varepsilon=\pm(1/2)(-1\pm\sqrt{-3})$. As d is a positive odd divisor of c, we have $d=1$ or 3. Thus, as $[L:Q]=4$, we have $L=Q\left(\sqrt{-3},\sqrt{-(1/2)(-1\pm\sqrt{-3})}\right)=Q(\sqrt[12]{1})=Q(\sqrt{-3},\sqrt{-1})$ is a bicyclic extension of Q. However, $Q(\sqrt{-3},\sqrt{-1})$ is not an unramified extension of $Q(\sqrt{-3})$ as $\langle 2\rangle=\langle 1+i\rangle^2$ in O_L, so this possibility in fact cannot occur. Any further units must come from real quadratic fields K. Thus, it remains to consider $c>0$ and $\varepsilon\neq\pm 1$.

Let ε_0 be the fundamental unit (>1) of O_K. Let $\eta=x+y\sqrt{c}$ be the least unit of O_K with x and y positive integers. Then $\eta=\varepsilon_0^k$, where $k=1$ or 3, and $\varepsilon=\pm\varepsilon_0^g$ for some integer $g\neq 0$. Hence

$$L=K(\sqrt{d\varepsilon})=K\left(\sqrt{\pm d\varepsilon_0^g}\right)=K\left(\sqrt{\pm d\varepsilon_0^{kg}}\right)=K\left(\sqrt{\pm d\eta^g}\right)$$
$$=\begin{cases}K(\sqrt{\pm d}), & \text{if } g\equiv 0 \pmod 2,\\ K(\sqrt{\pm d\eta}), & \text{if } g\equiv 1 \pmod 2.\end{cases}$$

When g is even, $L=Q(\sqrt{c},\sqrt{\pm d})$ is a bicyclic extension of Q. When g is odd and $x^2-cy^2=1$,

$$L=Q\left(\sqrt{c},\sqrt{\pm d(x+y\sqrt{c})}\right)=Q(\sqrt{c},\sqrt{2d(\pm x-1)})$$

is bicyclic (see, for example, [3, Section 1]). Finally, when g is odd and $x^2 - cy^2 = -1$, we have the following table of congruences, where the corresponding values of the ideal T have been determined from [5, Theorem 1].

c	$\pm dx$	$\pm dy$	T
$c \equiv 2 \pmod 4$	$1 \pmod 2$	$1 \pmod 2$	$2O_K$
$c \equiv 3 \pmod 4$	cannot occur	cannot occur	
$c \equiv 5 \pmod 8$	$2 \pmod 4$	$1 \pmod 2$	$2O_K$
$c \equiv 1 \pmod 8$	$0 \pmod 4$	$1 \pmod 2$	$\langle 2, (1/2)(1 - \sqrt{c})\rangle$ or $\langle 2, (1/2)(1 + \sqrt{c})\rangle$

This table shows that some prime ideal of O_K lying above 2 ramifies in O_L, contradicting that L/K is unramified at all finite primes. □

Theorem 2. *Let K be a quadratic extension of Q so that $K = Q(\sqrt{c})$ where c is a square-free integer not equal to 1. Let L be a quadratic extension of K which is unramified at all finite primes. Then $L = K(\sqrt{m})$, where m is a divisor $(\neq 1, c)$ of c with $m \equiv 1 \pmod 4$). Conversely, any such field is unramified at all finite primes of O_K.*

Proof. As L is a quadratic extension of K which is unramified at all finite primes, by Theorem 1, L is a bicyclic extension of Q, say $L = Q(\sqrt{c}, \sqrt{m})$, where $m \neq 1, c$.

Let p be a rational prime which ramifies in $Q(\sqrt{m})$. Then p ramifies in L. But L/K is unramified at all finite primes so p must ramify in $K = Q(\sqrt{c})$. Hence, recalling that

$$d(Q(\sqrt{m})) = \begin{cases} m, & \text{if } m \equiv 1 \pmod 4 \\ 4m, & \text{if } m \equiv 2, 3 \pmod 4, \end{cases}$$

(and similarly for $Q(\sqrt{c})$) we see that

$$\begin{cases} m | 2c, & \text{if } c \equiv 3 \pmod 4,\ m \equiv 2 \pmod 4, \\ m | c, & \text{otherwise.} \end{cases}$$

If $c \equiv 2 \pmod 4$, then $m|c$, and as $L = Q(\sqrt{c}, \sqrt{m}) = Q(\sqrt{c}, \sqrt{c/m})$, we may assume that m is odd. As L/K is unramified at $\langle 2, \sqrt{c}\rangle$ we see from [**3** or **4**, Table A] that L falls under case A1 so that $m \equiv 1 \pmod 4$.

If $c \equiv 3 \pmod 4$ and $m \not\equiv 2 \pmod 4$, then $m|c$ and as $L = Q(\sqrt{c}, \sqrt{m}) = Q(\sqrt{c}, \sqrt{c/m})$, we may assume that $m \equiv 1 \pmod 4$.

If $c \equiv 3 \pmod 4$ and $m \equiv 2 \pmod 4$, then from case B7 of [**3** or **4**, Table B] we see that $\langle 2, 1 + \sqrt{c}\rangle$ ramifies in $L = Q(\sqrt{c}, \sqrt{m})$, contradicting that L/K is unramified at all finite primes.

If $c \equiv 5 \pmod 8$, then $m|c$ and, as L/K is unramified at $2O_K$ we see from [**3** or **4**, Table C] that L falls under case C2 so that $m \equiv 1 \pmod 4$.

If $c \equiv 1 \pmod 8$, then $m|c$ and, as L/K is unramified at both $\langle 2, (1/2)(1+\sqrt{c})\rangle$ and $\langle 2, (1/2)(1-\sqrt{c})\rangle$, we see from [**3** or **4**, Table D] that L falls under case D3 so that $m \equiv 1 \pmod 4$.

Conversely, suppose that $L = K(\sqrt{m})$, where m is a divisor of c with $m \equiv 1 \pmod 4$). We recall from the proof of Theorem 1 that $d(L/K) = RT^2$. As $m \equiv 1 \pmod 4$, we see from cases A1, B2, C2 and D3 of Tables A, B, C and D of [**3** or **4**] that $T = O_K$. Finally, as $mO_K = \langle m, \sqrt{c}\rangle^2$, it follows that $R = O_K$, so $d(L/K) = O_K$. □

The case $c < 0$ of Theorem 2 is given in [**2**, Lemma 6.8].

Theorem 3. *Let K be a quadratic extension of Q so that $K = Q(\sqrt{c})$ for some square-free integer $c \neq 1$. Let n denote the number of distinct primes dividing $d(K)$. Then the number N of quadratic extensions L of K such that L/K is unramified at all finite primes is given by*

$$N = 2^{n-1} - 1.$$

The number N' of quadratic extensions L of K such that L/K is unramified (that is, unramified at all primes both finite and infinite) is given by

$$N' = \begin{cases} 2^{n-2} - 1, & \text{if } c > 0 \text{ and there exists at least one prime} \\ & q \equiv 3 \pmod 4 \text{ which divides } c, \\ 2^{n-1} - 1, & \text{otherwise.} \end{cases}$$

Proof. By Theorem 2, remembering that $Q(\sqrt{c}, \sqrt{m}) = Q(\sqrt{c}, \sqrt{c}/m)$, we see that

$$N = \theta \sum_{\substack{m|c \\ m \neq 1,c \\ m \equiv 1 \pmod 4}} 1,$$

where m runs through positive and negative divisors of c, and

$$\theta = \begin{cases} 1, & \text{if } c \equiv 2,3 \pmod 4, \\ 1/2, & \text{if } c \equiv 1 \pmod 4. \end{cases}$$

The asserted result now follows as

$$\sum_{\substack{m|c \\ m \neq 1,c \\ m \equiv 1 \pmod 4}} 1 = \begin{cases} 2^{n-1} - 1, & \text{if } c \equiv 2,3 \pmod 4, \\ 2^n - 2, & \text{if } c \equiv 1 \pmod 4. \end{cases}$$

To prove the assertion regarding N' we recall that $Q(\sqrt{c}, \sqrt{m})/Q(\sqrt{c})$ is ramified at infinity if and only if $c > 0$ and $m < 0$. Hence $N' = N$ if $c < 0$. If $c > 0$ we have by Theorem 2,

$$N' = \theta \sum_{\substack{d|c \\ d \equiv 1 \pmod 4 \\ d \neq 1,c}} 1$$

$$= \begin{cases} \frac{1}{2}\left(\sum\limits_{\substack{d|c \\ d \equiv 1 \pmod 4}} 1 \right) - 1, & \text{if } c \equiv 1 \pmod 4, \\ \left(\sum\limits_{\substack{d|c \\ d \equiv 1 \pmod 4}} 1 \right) - 1, & \text{if } c \equiv 2,3 \pmod 4, \end{cases}$$

where d runs through the positive divisors of c. The result now follows as

$$\sum_{\substack{d|c \\ d \equiv 1 \pmod 4}} 1 = \begin{cases} 2^l, & \text{if there does not exist a prime} \\ & q \equiv 3 \pmod 4 \text{ dividing } c, \\ 2^{l-1}, & \text{if there exists a prime} \\ & q \equiv 3 \pmod 4 \text{ dividing } c, \end{cases}$$

where l is the number of distinct odd prime divisors of c, that is,

$$l = \begin{cases} n, & \text{if } c \equiv 1 \pmod 4, \\ n-1, & \text{if } c \equiv 2,3 \pmod 4. \end{cases} \qquad \square$$

Example. The quadratic field $Q(\sqrt{30})$ has $2^{3-1} - 1 = 3$ quadratic extensions which are unramified at all finite primes (Theorem 3). These three fields are $Q(\sqrt{30}, \sqrt{-3})$, $Q(\sqrt{30}, \sqrt{5})$ and $Q(\sqrt{30}, \sqrt{-15})$ (Theorem 2). However, only $2^{3-2} - 1 = 1$ of these is an unramified extension of $Q(\sqrt{30})$, namely, $Q(\sqrt{30}, \sqrt{5})$.

REFERENCES

1. Z.I. Borevich and I.R. Shafarevich, *Number theory*, Academic Press, New York and London, 1966.

2. David A. Cox, *Primes of the form $x^2 + ny^2$*, in *Fermat, class field theory and complex multiplication*, John Wiley and Sons, New York, 1989.

3. James G. Huard, Blair K. Spearman and Kenneth S. Williams, *Integral bases for quartic fields with quadratic subfields*, Centre for Research in Algebra and Number Theory (Carleton University, Ottawa), Mathmeatical Research Series No. 4, June 1991.

4. ———, *Integral bases for quartic fields with quadratic subfields*, J. Number Theory, to appear.

5. Blair K. Spearman and Kenneth S. Williams, *Relative integral bases for quartic fields over quadratic subfields*, Acta Math. Hungar., to appear.

DEPARTMENT OF MATHEMATICS AND STATISTICS, OKANAGAN UNIVERSITY COLLEGE, KELOWNA, BC V1V 1V7, CANADA

DEPARTMENT OF MATHEMATICS AND STATISTICS, CARLETON UNIVERSITY, OTTAWA, ONTARIO K1S 5B6, CANADA