JOURNAL OF NUMBER THEORY 51, 87–102 (1995)

Integral Bases for Quartic Fields with Quadratic Subfields

JAMES G. HUARD

Department of Mathematics, Canisius College, Buffalo, New York 14208

BLAIR K. SPEARMAN

Department of Mathematics, Okanagan University College, Kelowna, British Columbia, Canada V1Y 4X8

AND

KENNETH S. WILLIAMS*

Department of Mathematics and Statistics, Carleton University, Ottawa, Ontario, Canada K1S 5B6

Communicated by Alan C. Woods

Received December 31, 1991; revised June 15, 1993

Let L be a quartic number field with quadratic subfield $Q(\sqrt{c})$. Then $L = Q(\sqrt{c}, \sqrt{a+b\sqrt{c}})$, where $a+b\sqrt{c}$ is not a square in $Q(\sqrt{c})$ and where a, b, and c may be taken to be integers with both c and (a, b) squarefree. The discriminant of L, as well as an integral basis for L, is determined explicitly in terms of congruences involving a, b, and c. These results unify the existing results in the literature for quartic fields which are pure, bicyclic, cyclic, or dihedral, and complete the incomplete results in the literature for dihedral quartic fields. It is also shown that for each squarefree integer c there are infinitely many non-pure, dihedral quartic fields L with a power basis. © 1995 Academic Press, Inc.

Let L be a quartic number field with quadratic subfield $Q(\sqrt{c})$, where Q denotes the rational number field. Then $L = Q(\sqrt{c}, \sqrt{a+b\sqrt{c}})$, where $a+b\sqrt{c}$ is not a square in $Q(\sqrt{c})$ and where a, b, and c may be taken to be integers with both c and the greatest common divisor (a, b) squarefree.

* Research supported by the Natural Sciences and Engineering Research Council of Canada under Grant A-7233.

0022-314X/95 $6.00

Let $\hat{L}$ denote the normal closure of L. The Galois group $\mathrm{Gal}(\hat{L}/Q)$ is the Klein 4-group, the cyclic group of order 4, or the dihedral group of order 8; L is called a bicyclic, cyclic, or dihedral extension of Q, respectively. It is known that

$$\begin{aligned} &L \text{ is bicyclic} \Leftrightarrow a^2-b^2c=k^2 \text{ for some integer } k,\\ &L \text{ is cyclic} \Leftrightarrow a^2-b^2c=ck^2 \text{ for some integer } k, \qquad (1)\\ &L \text{ is dihedral} \Leftrightarrow a^2-b^2c\neq k^2 \text{ or } ck^2 \text{ for any integer } k; \end{aligned}$$

see, for example, [7, Theorem 3]. When L is bicyclic $L=Q(\sqrt{c}, \sqrt{2(a-k)}, \sqrt{2(a+k)})$.

In this paper we give a simple, explicit determination of the discriminant $d(L)$ of L using Godwin's extension [2] of a theorem of Hilbert [4, Satz 4]. Hilbert's theorem gives a necessary and sufficient condition for a prime ideal P of the ring O_K of integers of an algebraic number field K to divide the relative discriminant $d(L/K)$ of a quadratic extension L/K in terms of the solvability in O_K of a certain congruence modulo a power of P. The relative discriminant $d(L/K)$ of the relative quadratic extension L/K is the ideal of O_K generated by the set of all elements of the form $(\theta-\theta')^2$, where $\theta\in O_L$ and θ' denotes the conjugate of θ in L with respect to K. The discriminant $d(L)$ is given by the formula

$$d(L)=d(K)^2\, N_{K/Q}(d(L/K)), \qquad (2)$$

where $N_{K/Q}$ denotes the norm from K to Q [10, Prop. 4.9, p. 159]. A slightly reformulated version of Godwin's extension of Hilbert's theorem is Proposition 1 below. For integers (or ideals) A and B, we write $A \mid B$ to mean A divides B, and $A^m \parallel B$ to mean $A^m \mid B$, $A^{m+1} \nmid B$ (m a positive integer).

PROPOSITION 1 (Hilbert and Godwin). *Let K be an algebraic number field. Let $\mu\in O_K-O_K^2$ and set $L=K(\sqrt{\mu})$ so that $[L:K]=2$. Let P be a prime ideal of O_K and define the nonnegative integers l_P, m_P, and w_P* by

$$P^{l_P}\parallel 2, \qquad P^{m_P}\parallel \mu, \qquad P^{w_P}\parallel d(L/K).$$

Then w_P is the least nonnegative integer h with $h\equiv m_P$ (mod 2) *for which the congruence*

$$\alpha^2\equiv\mu \qquad (\mathrm{mod}\ P^{2l_P+m_P\quad h})$$

is solvable with $\alpha\in O_K$.

For brevity we suppress the subscript P in l_P, m_P, w_P; that is, we write w for w_P, w_1 for w_{P_1}, w_2 for w_{P_2}, etc.

Applying Proposition 1 with $K = Q(\sqrt{c})$, $\mu = a + b\sqrt{c}$, $L = Q(\sqrt{c}, \sqrt{a+b\sqrt{c}})$, we obtain the relative discriminant $d(L/K)$ and then, by (2), the discriminant $d(L)$ of L. We also give an integral basis for L. The details are given in [5].

Theorem 1. *Let L be a quartic field with quadratic subfield $K = Q(\sqrt{c})$. Write $L = Q(\sqrt{c}, \sqrt{a+b\sqrt{c}})$, where a, b, and c are integers with both c and (a, b) squarefree and $\mu = a + b\sqrt{c}$ is not a square in K. Let r denote the nonnegative integer such that $2^r \parallel a^2 - b^2c$, and let s denote the squarefree part of $a^2 - b^2c$. Set*

$$N = \frac{(a, b, cs)}{(a, b)} \sqrt{\frac{(a^2 - b^2c)}{s}},$$

so that N is an integer such that $N^2 \mid a^2 - b^2c$.

Then the discriminant of L is given by

$$d(L) = \frac{2^e(a^2 - b^2c)\,c^2}{N^2} = 2^e sc^2 \left(\frac{(a, b)}{(a, b, cs)}\right)^2, \tag{3}$$

TABLE A

$(c \equiv 2 \pmod 4)$

			$P = \langle 2, \sqrt{c} \rangle, \quad 2 = P^2$				
r	a	b	Congruence conditions	w	$d = w + 6$	e	Case
0	1(2)	0(2)	$a + b \equiv 1(4)$	0	6	4	A1
			$a + b \equiv 3(4)$	2	8	6	A2
		1(2)		4	10	8	A3
1	0(2)	1(2)		5	11	8	A4
2	2(4)	0(4)	$a + b \equiv c(8)$	0	6	4	A5
			$a + b \equiv -c(8)$	2	8	6	A6
		2(4)		4	10	8	A7
3	0(4)	2(4)		5	11	8	A8

TABLE B

$(c \equiv 3 \pmod{4})$

			$P = \langle 2, 1+\sqrt{c}\rangle, \quad 2 = P^2$				
r	a	b	Congruence conditions	w	$d = w+4$	e	Case
0	0(2)	1(2)		4	8	8	B1
	1(2)	0(4)		0	4	4	B2
		2(4)		2	6	6	B3
1	1(2)	1(2)		5	9	8	B4
2	0(4)	2(4)	$a \equiv c+1(8)$	0	4	2	B5
			$a \equiv c+5(8)$	2	6	4	B6
	2(4)	0(4)		4	8	6	B7
3	2(4)	2(4)		5	9	8	B8

where the values of the integer e are given in Tables A, B, C, D. Set

$$a_1 = \frac{a}{(a,b)}, \qquad b_1 = \frac{b}{(a,b)}, \qquad N_1 = (N, c),$$

$$N_2 = N/N_1, \qquad Y_1 = a_1^{\phi(4N_2^2)-1} b_1 c,$$

and let Y be such that $Y \equiv Y_1 \pmod{4N}$, $0 \leqslant Y < 4N$.

Then an integral basis for L is given in Tables A′, B′, C′, D′.

TABLE C

$(c \equiv 5 \pmod{8})$

			$P = \langle 2 \rangle$				
r	a	b	Congruence conditions	w	$d = 2w$	e	Case
0	0(2)	1(2)		2	4	4	C1
	1(2)	0(2)	$a+b \equiv 1(4)$	0	0	0	C2
			$a+b \equiv 3(4)$	2	4	4	C3
2	1(2)	1(2)		3	6	6	C4
	0(2)	0(2)	$a+b \equiv 2(4)$	3	6	4	C5
4	2(8)	2(4)		2	4	2	C6
	6(8)	2(4)	$a-b-c \equiv 3$ or $15(16)$	0	0	-2	C7
			$a-b-c \equiv 7$ or $11(16)$	2	4	2	C8

Tables A, B, C, D also give the values of d and w, where $2^d \parallel d(L)$ and $P^w \parallel d(L/K)$. Here P denotes a prime ideal factor of 2 in the ring O_K of integers of $K = Q(\sqrt{c})$. The cases in the tables arise naturally from studying the congruence of Proposition 1 for such P's.

Formula (3) unifies known results given here as corollaries.

COROLLARY 1. (Williams [13]). *Let a and c be distinct squarefree integers ($\neq 1$). Then*

$$d(Q(\sqrt{a}, \sqrt{c})) = 2^e \frac{a^2c^2}{(a, c)^2},$$

where the values of e are given in Table E.

COROLLARY 2. (Funakura [1]). *Let n be a fourth-power free integer such that the polynomial $X^4 - n$ is irreducible over Q. Let n^* denote the squarefree part of n. Then*

$$d(Q(\sqrt[4]{n})) = -2^e \frac{n(n^*)^3}{(n, (n^*)^3)},$$

where

$$e = \begin{cases} 2, & \text{if } n \equiv 1 \pmod 8 \text{ or } n \equiv 28 \pmod{32}, \\ 4, & \text{if } n \equiv 5 \pmod 8, n \equiv 4 \pmod{16}, \text{ or } n \equiv 12 \pmod{32}, \\ 8, & \text{if } n \equiv 2, 3 \pmod 4, \text{ or } n \equiv 8 \pmod{16}. \end{cases}$$

COROLLARY 3. (Hardy, Hudson, Richman, Williams and Holtz [3]). *Let L be a cyclic quartic field. It is known* [3] *that there exists a unique representation of L in the form*

$$L = Q(\sqrt{A(D + B\sqrt{D})}),$$

where A, B, C, D are integers such that A is squarefree and odd, $D = B^2 + C^2$ is squarefree, $B > 0$, $C > 0$, and $(A, D) = 1$. Then

$$d(Q(\sqrt{A(D + B\sqrt{D})})) = 2^e A^2 D^3,$$

where

$$e = \begin{cases} 8, & \text{if } D \equiv 2 \pmod 8, \\ 6, & \text{if } D \equiv 1 \pmod 4, B \equiv 1 \pmod 2, \\ 4, & \text{if } D \equiv 1 \pmod 4, B \equiv 0 \pmod 2, A + B \equiv 3 \pmod 4, \\ 0, & \text{if } D \equiv 1 \pmod 4, B \equiv 0 \pmod 2, A + B \equiv 1 \pmod 4. \end{cases}$$

TABLE D

($c \equiv 1 \pmod 8$)

$P_1 = \langle 2, \frac{1}{2}(1+\sqrt{c})\rangle$, $P_2 = \langle 2, \frac{1}{2}(1-\sqrt{c})\rangle$, $2 = P_1 P_2$

r	a	b	Congruence conditions	$\frac{a^2-b^2c}{2^r}$ (mod 4)	m_1	m_2	w_1	w_2	$d = w_1 + w_2$	e	Case
0	0(2)	1(2)	$a+b \equiv 1(4)$		0	0	2	0	2	2	D1
			$a+b \equiv 3(4)$		0	0	0	2	2	2	D2
	1(2)	0(2)	$a+b \equiv 1(4)$		0	0	0	0	0	0	D3
			$a+b \equiv 3(4)$		0	0	2	2	4	4	D4
2	0(2)	0(2)	$a+b \equiv 2(4)$		1	1	3	3	6	4	D5
Odd $\geqslant 3$	1(2)	1(2)	$a \equiv b(4)$	$-a+2^{r-2}$	$r-1$	1	2	3	5	4	D6
				$a+2^{r-2}$	$r-1$	1	0	3	3	2	D7
			$a \equiv -b(4)$	$-a+2^{r-2}$	1	$r-1$	3	2	5	4	D8
				$a+2^{r-2}$	1	$r-1$	3	0	3	2	D9
Even $\geqslant 4$	1(2)	1(2)	$a \equiv b(4)$		$r-1$	1	3	3	6	6	D10
			$a \equiv -b(4)$		1	$r-1$	3	3	6	6	D11

5	2(8)	2(8)		3	2	3	2	5	4	D12
	2(8)	6(8)		2	3	2	3	5	4	D13
	6(8)	2(8)		2	3	0	3	3	2	D14
	6(8)	6(8)		3	2	3	0	3	2	D15
Even $\geqslant 6$	2(8)	2(8)	1	$r-2$	2	0	0	0	-2	D16
			-1	$r-2$	2	2	0	2	0	D17
	6(8)	6(8)	-1	$r-2$	2	0	2	2	0	D18
			1	$r-2$	2	2	2	4	2	D19
	2(8)	6(8)	1	2	$r-2$	0	0	0	-2	D20
			-1	2	$r-2$	0	2	2	0	D21
	6(8)	2(8)	-1	2	$r-2$	2	0	2	0	D22
			1	2	$r-2$	2	2	4	2	D23
Odd $\geqslant 7$	2(8)	2(8)		$r-2$	2	3	0	3	2	D24
	2(8)	6(8)		2	$r-2$	0	3	3	2	D25
	6(8)	2(8)		2	$r-2$	2	3	5	4	D26
	6(8)	6(8)		$r-2$	2	3	2	5	4	D27

TABLE A′

($c \equiv 2 \pmod 4$)

A1	$1, \frac{1+\sqrt{\mu}}{2}, \sqrt{c}, \frac{(Y-\sqrt{c})(N+\sqrt{\mu})}{2N},$	if $a \equiv 1 \pmod 4, b \equiv 0 \pmod 4$
	$1, \sqrt{\mu}, \frac{1+\sqrt{\mu}+\sqrt{c}}{2}, \frac{(Y-\sqrt{c})(N+\sqrt{\mu})}{2N},$	if $a \equiv 3 \pmod 4, b \equiv 2 \pmod 4$
A2	$1, \sqrt{\mu}, \sqrt{c}, \frac{(Y-\sqrt{c})(N+\sqrt{\mu})}{2N},$	
A3, A4	$1, \sqrt{\mu}, \sqrt{c}, \frac{(Y-\sqrt{c})\sqrt{\mu}}{N}$	
A5	$1, \sqrt{\mu}, \frac{\sqrt{\mu}+\sqrt{c}}{2}, \frac{(Y-\sqrt{c})((b/2+\sqrt{c})N/2+\sqrt{\mu})}{2N}$	
A6	$1, \sqrt{\mu}, \frac{\sqrt{\mu}+\sqrt{c}}{2}, \frac{(Y-\sqrt{c})\sqrt{\mu}}{N}$	
A7, A8	$1, \sqrt{\mu}, \sqrt{c}, \frac{(Y-\sqrt{c})\sqrt{\mu}}{N}$	

TABLE B′

($c \equiv 3 \pmod 4$)

B1	$1, \sqrt{\mu}, \sqrt{c}, \frac{(Y-\sqrt{c})\sqrt{\mu}}{N}$	
B2	$1, \frac{1+\sqrt{\mu}}{2}, \sqrt{c}, \frac{(Y+N-\sqrt{c})(N+\sqrt{\mu})}{2N},$	if $a \equiv 1 \pmod 4$
	$1, \sqrt{\mu}, \frac{\sqrt{\mu}+\sqrt{c}}{2}, \frac{(Y+N-\sqrt{c})(N+\sqrt{\mu})}{2N},$	if $a \equiv 3 \pmod 4$
B3	$1, \sqrt{\mu}, \sqrt{c}, \frac{(Y+N-\sqrt{c})(N+\sqrt{\mu})}{2N}$	
B4	$1, \sqrt{\mu}, \sqrt{c}, \frac{(Y-\sqrt{c})\sqrt{\mu}}{N}$	
B5	$1, \sqrt{\mu}, \frac{1+\sqrt{\mu}+\sqrt{c}}{2}, \frac{(Y+N-\sqrt{c})((b/2+\sqrt{c})N+\sqrt{\mu})}{4N}$	
B6	$1, \sqrt{\mu}, \frac{1+\sqrt{\mu}+\sqrt{c}}{2}, \frac{(Y+N-\sqrt{c})\sqrt{\mu}}{2N}$	
B7	$1, \sqrt{\mu}, \sqrt{c}, \frac{(Y+N-\sqrt{c})\sqrt{\mu}}{2N}$	
B8	$1, \sqrt{\mu}, \sqrt{c}, \frac{(Y-\sqrt{c})\sqrt{\mu}}{N}$	

TABLE C'

$(c \equiv 5 \pmod 8)$

C1	$1, \sqrt{\mu}, \frac{1+\sqrt{c}}{2}, \frac{(Y+N-\sqrt{c})\sqrt{\mu}}{2N}$
C2	$1, \frac{1+\sqrt{\mu}}{2}, \frac{1+\sqrt{c}}{2}, \frac{(Y+N-\sqrt{c})(N+\sqrt{\mu})}{4N}$
C3	$1, \sqrt{\mu}, \frac{1+\sqrt{c}}{2}, \frac{(Y+N-\sqrt{c})\sqrt{\mu}}{2N}$
C4	$1, \sqrt{\mu}, \frac{1+\sqrt{c}}{2}, \frac{(Y-\sqrt{c})\sqrt{\mu}}{N}$
C5	$1, \sqrt{\mu}, \frac{1+\sqrt{c}}{2}, \frac{(Y+N-\sqrt{c})\sqrt{\mu}}{2N}$
C6	$1, \frac{\sqrt{\mu}}{2}, \frac{1+\sqrt{c}}{2}, \frac{(Y-\sqrt{c})\sqrt{\mu}}{2N}$
C7	$1, \frac{\sqrt{\mu}}{2}, \frac{b/2+\sqrt{\mu}+\sqrt{c}}{4}, \frac{(Y-\sqrt{c})((b/2+\sqrt{c})N/2+\sqrt{\mu})}{4N}$
C8	$1, \frac{\sqrt{\mu}}{2}, \frac{1+\sqrt{c}}{2}, \frac{(Y-\sqrt{c})\sqrt{\mu}}{2N}$

TABLE D'

$(c \equiv 1 \pmod 8)$

D1	$1, \sqrt{\mu}, \frac{1+\sqrt{c}}{2}, \frac{((Y+N+1)(N+1)-1-\sqrt{c})(N+\sqrt{\mu})}{4N}$
D2	$1, \sqrt{\mu}, \frac{1+\sqrt{c}}{2}, \frac{((Y+N-1)(N+1)+1-\sqrt{c})(N+\sqrt{\mu})}{4N}$
D3	$1, \frac{1+\sqrt{\mu}}{2}, \frac{1+\sqrt{c}}{2}, \frac{(Y+N-\sqrt{c})(N+\sqrt{\mu})}{4N}$
D4, D5	$1, \sqrt{\mu}, \frac{1+\sqrt{c}}{2}, \frac{(Y+N-\sqrt{c})\sqrt{\mu}}{2N}$
D6	$1, \sqrt{\mu}, \frac{1+\sqrt{c}}{2}, \frac{(Y-\sqrt{c})\sqrt{\mu}}{2N}$
D7	$1, \sqrt{\mu}, \frac{1+\sqrt{c}}{2}, \frac{(N^2+Y-\sqrt{c})(N+\sqrt{\mu})}{4N}$
D8	$1, \sqrt{\mu}, \frac{1+\sqrt{c}}{2}, \frac{(Y-\sqrt{c})\sqrt{\mu}}{2N}$
D9	$1, \sqrt{\mu}, \frac{1+\sqrt{c}}{2}, \frac{(N^2+Y-\sqrt{c})(N+\sqrt{\mu})}{4N}$
D10, D11	$1, \sqrt{\mu}, \frac{1+\sqrt{c}}{2}, \frac{(Y-\sqrt{c})\sqrt{\mu}}{N}$
D12, D13	$1, \frac{\sqrt{\mu}}{2}, \frac{1+\sqrt{c}}{2}, \frac{(Y-\sqrt{c})\sqrt{\mu}}{N}$

Table continued

TABLE D′—*Continued*

$(c \equiv 1 \pmod 8)$

D14, D15	$1, \frac{\sqrt{\mu}}{2}, \frac{1+\sqrt{c}}{2}, \frac{(N/2+Y-\sqrt{c})(N/2+\sqrt{\mu})}{2N}$
D16	$1, \frac{\sqrt{\mu}}{2}, \frac{1+\sqrt{\mu}+\sqrt{c}}{4}, \frac{(N^2/2+Y-\sqrt{c})(N+\sqrt{\mu})}{4N}$
D17	$1, \frac{\sqrt{\mu}}{2}, \frac{1+\sqrt{\mu}+\sqrt{c}}{4}, \frac{(Y-\sqrt{c})\sqrt{\mu}}{2N}$
D18	$1, \frac{\sqrt{\mu}}{2}, \frac{1+\sqrt{c}}{2}, \frac{(N^2/2+Y-\sqrt{c})(N+\sqrt{\mu})}{4N}$
D19	$1, \frac{\sqrt{\mu}}{2}, \frac{1+\sqrt{c}}{2}, \frac{(Y-\sqrt{c})\sqrt{\mu}}{2N}$
D20	$1, \frac{\sqrt{\mu}}{2}, \frac{-1+\sqrt{\mu}+\sqrt{c}}{4}, \frac{(N^2/2+Y-\sqrt{c})(N+\sqrt{\mu})}{4N}$
D21	$1, \frac{\sqrt{\mu}}{2}, \frac{-1+\sqrt{\mu}+\sqrt{c}}{4}, \frac{(Y-\sqrt{c})\sqrt{\mu}}{2N}$
D22	$1, \frac{\sqrt{\mu}}{2}, \frac{1+\sqrt{c}}{2}, \frac{(N^2/2+Y-\sqrt{c})(N+\sqrt{\mu})}{4N}$
D23	$1, \frac{\sqrt{\mu}}{2}, \frac{1+\sqrt{c}}{2}, \frac{(Y-\sqrt{c})\sqrt{\mu}}{2N}$
D24	$1, \frac{\sqrt{\mu}}{2}, \frac{1+\sqrt{\mu}+\sqrt{c}}{4}, \frac{(Y-\sqrt{c})\sqrt{\mu}}{N}$
D25	$1, \frac{\sqrt{\mu}}{2}, \frac{-1+\sqrt{\mu}+\sqrt{c}}{4}, \frac{(Y-\sqrt{c})\sqrt{\mu}}{N}$
D26, D27	$1, \frac{\sqrt{\mu}}{2}, \frac{1+\sqrt{c}}{2}, \frac{(Y-\sqrt{c})\sqrt{\mu}}{N}$

TABLE E

e	a	c
0	1 (mod 4)	1 (mod 4)
4	1 (mod 4)	2, 3 (mod 4)
	2, 3 (mod 4)	1 (mod 4)
	3 (mod 4)	3 (mod 4)
	2 (mod 8)	2 (mod 8)
	6 (mod 8)	6 (mod 8)
6	2 (mod 4)	3 (mod 4)
	3 (mod 4)	2 (mod 4)
	2 (mod 8)	6 (mod 8)
	6 (mod 8)	2 (mod 8)

TABLE F

e	a	b	c
-2	$2 \pmod 8$	$2 \pmod 4$	$1 \pmod 8$
	$6 \pmod 8$	$2 \pmod 4$	$5 \pmod 8$
0	$1 \pmod 4$	$0 \pmod 4$	$1 \pmod 8$
	$3 \pmod 4$	$2 \pmod 4$	$5 \pmod 8$
2	$6 \pmod 8$	$2 \pmod 4$	$1 \pmod 8$
	$2 \pmod 8$	$2 \pmod 4$	$5 \pmod 8$
4	$2 \pmod 4$	$0 \pmod 4$	$1 \pmod 4$
	$3 \pmod 4$	$0 \pmod 4$	$1 \pmod 8$
	$1 \pmod 4$	$2 \pmod 4$	$5 \pmod 8$
6	$1 \pmod 2$	$1 \pmod 2$	$1 \pmod 4$
8	$4 \pmod 8$	$2 \pmod 4$	$2 \pmod 8$
	$2 \pmod 4$	$1 \pmod 2$	$2 \pmod 8$

The next result does not depend on the special representation used in Corollary 3.

COROLLARY 4. *If $Q(\sqrt{a+b\sqrt{c}})$ is a cyclic quartic field then*

$$d(Q(\sqrt{a+b\sqrt{c}})) = 2^e \frac{(a,b)^2 c^3}{(a,b,c)^2},$$

where the values of e are given in Table F.

We remark that Sommer [12, pp. 298–299] gives an integral basis for L which is less explicit than that of Theorem 1.

The integral bases given by Williams [13] for bicyclic quartic fields (with $\sqrt{m_1 n_1}$ replaced by $\sqrt{m_1}\sqrt{n_1}$ throughout [13]), by Funakura [1] for pure quartic fields, and by Hudson and Williams [6] for cyclic quartic fields are consistent with our Theorem 1.

We now turn to dihedral quartic extensions L. In [8] Lederman and van der Ploeg determine integral bases for a dihedral extension $L = Q(\sqrt{a+b\sqrt{c}})$ for $c \equiv 2, 3 \pmod 4$ and $c \equiv 5 \pmod 8$ but not for $c \equiv 1 \pmod 8$. In [8, Theorem 1] they express their integral bases in terms of an integer r, where r, s, u, v is the solution of a certain nonlinear system of three equations, but do not give r explicitly. Their equations

TABLE G

A	B	d	Integral basis
$3 \pmod 4$	$2 \pmod 4$	$2 \pmod 4$	$\left\{1, \sqrt{\alpha}, \frac{1+\sqrt{d}+\sqrt{\alpha}}{2}, \frac{\sqrt{d}+\eta}{2}\right\}$
$3 \pmod 4$	$0 \pmod 4$	$3 \pmod 4$	$\left\{1, \sqrt{\alpha}, \frac{\sqrt{d}+\sqrt{\alpha}}{2}, \frac{1+\sqrt{d}+\eta}{2}\right\}$
$0 \pmod 8$ $4 \pmod 8$	$6 \pmod 8$ $6 \pmod 8$	$7 \pmod 8$ $3 \pmod 8$	$\left\{1, \sqrt{\alpha}, \frac{1+\sqrt{d}+\sqrt{\alpha}}{2}, \frac{2+\eta}{4}\right\}$

define r uniquely modulo C, where their C can be shown to be the odd part of our N, and their r satisfies $r \equiv r_0 \pmod C$, where

$$r_0 = \begin{cases} -Y_1, & \text{if } c \equiv 2, 3 \pmod 4, \\ (1-Y_1)(C+1)/2, & \text{if } c \equiv 1 \pmod 4). \end{cases}$$

In Table 1 on page 370 of [8] the corrections shown in Table G should be made, and Table 2 on page 371 should be replaced by Table H.

In [11] Schmal determines $d(L)$ and an integral basis for $L = K(\sqrt{\omega})$, $K = Q(\sqrt{c})$, $\omega \in O_K$, $N_{K/Q}(\omega)$ squarefree. These are our cases A1–A4, B1–B4, C1–C3, D1–D4 with $N = 1$, and cases C6–C8 and D12–D15 with $N = 4$.

Next we determine when $L = Q(\sqrt{c}, \sqrt{a+b\sqrt{c}})$ is a pure quartic extension of Q, that is, when there exists an integer n such that $L = Q(\sqrt[4]{n})$. Analogous to (1), we prove

TABLE H

$A \pmod 4$	$B \pmod 4$	$d \pmod{16}$	Integral basis
1	0	5, 13	$\left\{1, \frac{1+\sqrt{\alpha}}{2}, \frac{1+\sqrt{d}}{2}, \frac{(1+\sqrt{d})/2+\eta}{2}\right\}$
1 3	1 1	5 13	$\left\{1, \sqrt{\alpha}, \frac{(1+\sqrt{d})/2+\sqrt{\alpha}}{2}, \frac{1+\eta}{2}\right\}$
2 0	3 3	5 13	$\left\{1, \sqrt{\alpha}, \frac{1+(1+\sqrt{d})/2+\sqrt{\alpha}}{2}, \frac{1+\eta}{2}\right\}$
	Otherwise		$\left\{1, \sqrt{\alpha}, \frac{1+\sqrt{d}}{2}, \eta\right\}$

PROPOSITION. 2. *Let a, b, c be integers such that (a, b) is squarefree, c is squarefree ($\neq 1$), and $a+b\sqrt{c}$ is not a square in $Q(\sqrt{c})$. Then the quartic field $L=Q(\sqrt{c}, \sqrt{a+b\sqrt{c}})$ is a pure field if and only if there exists an integer k such that*

$$a^2-b^2c=-ck^2, \tag{4}$$

in which case $L=Q(\sqrt[4]{4c(b-k)^2})$.

Proof. Suppose first that $L=Q(\sqrt{c}, \sqrt{a+b\sqrt{c}})$ is a pure quartic extension of Q, where a, b, c are integers satisfying the conditions stated in the proposition. Then there exists an integer n such that X^4-n is irreducible over Z and $L=Q(\sqrt[4]{n})$. Since $\sqrt{c}\in L$ there exist $\alpha, \beta\in Q(\sqrt{n})$ such that $\sqrt{c}=\alpha+\beta\sqrt[4]{n}$. Squaring, we obtain $c=(\alpha^2+\beta^2\sqrt{n})+2\alpha\beta\sqrt[4]{n}$. As c, $\alpha^2+\beta^2\sqrt{n}$, $2\alpha\beta$ all belong to the field $Q(\sqrt{n})$, we must have $\alpha\beta=0$. If $\alpha=0$ then $\sqrt{c}=\beta\sqrt[4]{n}$, which is impossible since

$$\begin{aligned}[Q(\beta\sqrt[4]{n}):Q]&=[Q(\beta\sqrt[4]{n}):Q(\sqrt{n})][Q(\sqrt{n}):Q]\\&=[Q(\sqrt[4]{n}):Q(\sqrt{n})][Q(\sqrt{n}):Q]\\&=[Q(\sqrt[4]{n}):Q]=4.\end{aligned}$$

Hence $\alpha\neq 0$ and we must have $\beta=0$. Thus $\sqrt{c}=\alpha\in Q(\sqrt{n})$ and so, as c is squarefree, we have $n=ct^2$, for some positive integer t: thus $Q(\sqrt{n})=Q(\sqrt{c})$ and $L=Q(\sqrt[4]{ct^2})$. As $\sqrt{a+b\sqrt{c}}\in L$, there exist $\gamma, \delta\in Q(\sqrt{c})$ such that $\sqrt{a+b\sqrt{c}}=\gamma+\delta\sqrt[4]{ct^2}$. Squaring, we obtain

$$a+b\sqrt{c}=(\gamma^2+\delta^2t\sqrt{c})+2\gamma\delta\sqrt[4]{ct^2}.$$

As $a+b\sqrt{c}$, $\gamma^2+\delta^2t\sqrt{c}$, and $2\gamma\delta$ all belong to $Q(\sqrt{c})$, we must have $\gamma\delta=0$. If $\delta=0$ then $a+b\sqrt{c}=\gamma^2$ is a square in $Q(\sqrt{c})$, which is impossible. Thus $\delta\neq 0$, $\gamma=0$, and so $\sqrt{a+b\sqrt{c}}=\delta\sqrt[4]{ct^2}$. Squaring, and taking norms, we obtain $a^2-b^2c=-(N_{Q(\sqrt{c})/Q}(\delta))^2t^2c=-ck^2$, where $k\in Q$. As c is squarefree, k must be an integer.

Conversely suppose that (4) holds. As c is squarefree there is an integer u such that

$$a=cu, \qquad b^2-k^2=cu^2.$$

We can express c in the form $c=c_1c_2$, where c_1 divides $b-k$ and c_2 divides $b+k$. Set

$$d=\left(\frac{b-k}{c_1}, \frac{b+k}{c_2}\right)$$

so that

$$\left(\frac{b-k}{c_1 d}\right)\left(\frac{b+k}{c_2 d}\right)=\left(\frac{u}{d}\right)^2.$$

The integers $(b-k)/c_1 d$ and $(b+k)/c_2 d$ are coprime so there exist integers ε $(=\pm 1)$, λ $(=\pm 1)$, g, and h such that

$$\frac{b-k}{c_1 d}=\varepsilon g^2, \qquad \frac{b+k}{c_2 d}=\varepsilon h^2, \qquad \frac{u}{d}=\lambda gh.$$

Then we have

$$a=\lambda c d g h, \qquad b=\tfrac{1}{2}\varepsilon d(c_1 g^2+c_2 h^2).$$

We define rationals X, Y and an integer R by

$$X=\frac{\varepsilon\lambda g}{2}, \qquad Y=\frac{h}{2c_1}, \qquad R=2\varepsilon c_1 d.$$

Then we have

$$2cXYR=a, \qquad (X^2+cY^2)\,R=b,$$

so that

$$(X+Y\sqrt{c})^2\,R\sqrt{c}=((X^2+cY^2)+2XY\sqrt{c})\,R\sqrt{c}=a+b\sqrt{c}.$$

Hence $L=Q(\sqrt{c},(X+Y\sqrt{c})\sqrt[4]{cR^2})=Q(\sqrt[4]{cR^2})=Q(\sqrt[4]{4cc_1^2d^2})=Q(\sqrt[4]{4c(b-k)^2})$ is a pure field of the specified form. ∎

Funakura [1] has shown that there are infinitely many pure quartic fields with a power basis. Using Theorem 1 and Proposition 2 we prove

THEOREM 2. *For each squarefree integer* c $(\neq 1)$ *there exist infinitely many non-pure, dihedral quartic fields* $Q(\sqrt{c},\sqrt{a+b\sqrt{c}})$ *with a power basis.*

Proof. Let c be a fixed squarefree integer $(\neq 1)$. We define the quadratic polynomial $f_c(k)$ for $k\in Z$ by

$$f_c(k)=\begin{cases}16k^2+24k+(9-4c), & \text{if } c\equiv 1 \pmod 4,\\ 4k^2+4(c+1)\,k+(c^2+c+1), & \text{if } c\equiv 2,3 \pmod 4.\end{cases}$$

Clearly $f_c(k)$ is primitive and has nonzero discriminant and no fixed divisors >1. Hence, by a theorem of Nagel [9]

$$S_c=\{k\in Z \mid k>|c|, f_c(k)\text{ squarefree}\}$$

is an infinite set. For each $k \in S_c$ we note that $f_c(k) > |c|$ and set

$$\begin{aligned} a_k &= 4k+3, b_k = 2, && \text{if } c \equiv 1 \pmod 4, \\ a_k &= 2k+c+1, b_k = 1, && \text{if } c \equiv 2, 3 \pmod 4, \end{aligned}$$

so that $a_k \in Z^+$ and $a_k^2 - b_k^2 c = f_c(k)$. Thus $a_k^2 - b_k^2 c$ is squarefree and greater than $|c|$ for all $k \in S_c$. Hence for each $k \in S_c$ the field $L_k = Q(\sqrt{a_k + b_k \sqrt{c}})$ is a quartic extension of Q which, by (1) and Proposition 2, must be a non-pure dihedral field. Moreover L_k is of type A3, B1, C2, or D3 so by Theorem 1

$$d(L_k) = \begin{cases} (a_k^2 - 4c)\, c^2, & \text{if } c \equiv 1 \pmod 4, \\ 2^8(a_k^2 - c)\, c^2, & \text{if } c \equiv 2, 3 \pmod 4, \end{cases}$$

showing that for each fixed c the L_k $(k \in S_c)$ are distinct. Finally, set

$$\theta_k = \begin{cases} \frac{1}{2}(1 + \sqrt{a_k + 2\sqrt{c}}), & \text{if } c \equiv 1 \pmod 4, \\ \sqrt{a_k + \sqrt{c}}, & \text{if } c \equiv 2, 3 \pmod 4). \end{cases}$$

θ_k is an integer of L_k with

$$d(1, \theta_k, \theta_k^2, \theta_k^3) = \begin{cases} (a_k^2 - 4c)\, c^2, & \text{if } c \equiv 1 \pmod 4, \\ 2^8(a_k^2 - c)\, c^2, & \text{if } c \equiv 2, 3 \pmod 4). \end{cases}$$

Hence each of the infinitely many non-pure, dihedral, quartic fields L_k $(k \in S_c)$ possesses a power basis, namely $\{1, \theta_k, \theta_k^2, \theta_k^3\}$. ∎

ACKNOWLEDGMENT

The first two authors acknowledge the hospitality of the Centre for Research in Algebra and Number Theory at Carleton University, where they spent the academic year 1990–1991 on sabbatical leave.

REFERENCES

1. T. FUNAKURA, On integral bases of pure quartic fields, *Math. J. Okayama Univ.* **26** (1984), 27–41.
2. H. J. GODWIN, On relations between cubic and quartic fields, *Quart. J. Math. Oxford. Ser.* (2) **13** (1962), 206–212.
3. K. HARDY, R. H. HUDSON, D. RICHMAN, K. S. WILLIAMS, AND N. M. HOLTZ, "Calculation of the Class Numbers of Imaginary Cyclic Quartic Fields," Carleton Ottawa Mathematical Lecture Note Series No. 7, July 1986.
4. D. HILBERT, Über die Theorie des relativquadratischen Zahlkörpers, *Math. Ann.* **51** (1899), 1–127.

5. J. G. HUARD, B. K. SPEARMAN, AND K. S. WILLIAMS, "Integral Bases for Quartic Fields with Quadratic Subfields," Carleton University Centre for Research in Algebra and Number Theory Mathematical Research Series No. 4, June 1991.
6. R. H. HUDSON AND K. S. WILLIAMS, The integers of a cyclic quartic field, *Rocky Mountain J. Math.* **20** (1990), 145–150.
7. L.-C. KAPPE AND B. WARREN, An elementary test for the galois group of a quartic polynomial, *Amer. Math. Monthly* **96** (1989), 133–137.
8. W. LEDERMAN AND C. VAN DER PLOEG, Integral bases of dihedral number fields. I, *J. Austral. Math. Soc. Ser. A* **38** (1985), 351–371.
9. T. NAGEL, Zur Arithmetik der Polynome, *Abh. Math. Sem. Univ. Hamburg* **1** (1922), 179–194.
10. W. NARKIEWICZ, "Elementary and Analytic Theory of Algebraic Numbers," 2nd ed., Springer-Verlag, New York, 1990.
11. B. SCHMAL, "Existenz von relativen Ganzheitsbasen bei quartischen, insbesondere biquadratischen Erweiterungskörpern über quadratischen Grundkörpern," Diplomarbeit, Universität des Saarlandes, 1984.
12. J. SOMMER, Vorlesungen über Zahlentheorie, Teubner Verlag, Leipzig/Berlin, 1907.
13. K. S. WILLIAMS, Integers of biquadratic fields, *Canad. Math. Bull.* **13** (1970), 519–526.