B. K. SPEARMAN AND K. S. WILLIAMS
KODAI MATH. J.
19 (1996), 293-307

NORMAL RELATIVE INTEGRAL BASES FOR QUARTIC FIELDS OVER QUADRATIC SUBFIELDS

BLAIR K. SPEARMAN AND KENNETH S. WILLIAMS*

Abstract

Let L be a quartic number field with a quadratic subfield K. In 1986 Kawamoto gave a necessary and sufficient condition for L to have a normal relative integral basis (NRIB) over K. In this paper the authors explicitly construct a NRIB for L/K when such exists using their previous work on relative integral bases. The special cases when L is bicyclic, cyclic and pure are examined in detail.

1. Introduction

Let L be a quartic number field with quadratic subfield $K=Q(\sqrt{c})$, 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. Let O_L (resp. O_K) denote the ring of integers of L (resp. K). In this paper we assume that L has a relative integral basis (RIB) over K, and determine when L has a normal relative integral basis (NRIB) over K. Those L which have a relative integral basis (RIB) over K have been characterized in [9]. It is shown in [9, Theorem 2] that such L have a RIB over K of the form $\{1, \kappa\}$, where

(1.1) $$\kappa=\frac{\theta}{2}+\frac{\sqrt{\mu}}{2\gamma}\in O_L,$$

(1.2) $$\theta=0,\ 1,\ \sqrt{c},\ 1+\sqrt{c},\ \frac{1+\sqrt{c}}{2} \text{ or } \frac{-1+\sqrt{c}}{2}$$

depending on congruence conditions involving a, b, c,

(1.3) $$\mu=a+b\sqrt{c},$$

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

1991 Mathematics Subject Classification: 11R16, 11R04.

Key words and phrases. quartic fields with quadratic subfields, normal relative integral basis.

Received August 3, 1994; revised March 22, 1996.

(1.4) $\mu O_K = RS^2$, where R and S are integral ideals of O_K with R squarefree,

(1.5) $d(L/K)=RT^2$, where $T^2=O_K$, $2O_K$, $4O_K$, $\left\langle 2, \frac{1}{2}(1+\sqrt{c})\right\rangle^2$ or $\left\langle 2, \frac{1}{2}(1-\sqrt{c})\right\rangle^2$ depending on congruence conditions involving a, b, c,

(1.6) $S=T\langle\gamma\rangle$, where $\gamma\in K\setminus\{0\}$.

It is convenient to define the nonnegative integer r by

$$2^r \| a^2-b^2c, \tag{1.7}$$

and the integers a' and b' by

$$\mu/\gamma^2=\begin{cases} (a'+b'\sqrt{c})/2, & \text{if } c\equiv 1 \pmod 4, \\ a'+b'\sqrt{c}, & \text{if } c\equiv 2,\ 3 \pmod 4. \end{cases} \tag{1.8}$$

When $c\equiv 1 \pmod 4$, as $\mu/\gamma^2 \in O_K$, a', b' are integers with $a'\equiv b' \pmod 2$.

If $c>0$, we let ε_c denote the fundamental unit (>1) of $K=Q(\sqrt{c})$, and set

$$N(c)=\text{norm of } \varepsilon_c = \pm 1 \tag{1.9}$$

and

$$F(c)=\begin{cases} +1, & \text{if } \varepsilon_c=(t+u\sqrt{c})/2 \text{ for odd integers } t \text{ and } u, \\ -1, & \text{if } \varepsilon_c=t+u\sqrt{c} \quad \text{for integers } t \text{ and } u. \end{cases} \tag{1.10}$$

In Section 2 we prove the following theorem, which extends a theorem of Kawamoto [5, Theorem 7].

THEOREM 1. *Let a, b, c be integers with (a, b) squarefree, c squarefree, and $a+b\sqrt{c}$ not a square in $Q(\sqrt{c})$. Set $L=Q(\sqrt{c}, \sqrt{a+b\sqrt{c}})$ and $K=Q(\sqrt{c})$. Suppose L has a relative integral basis over K. Define μ, γ, r, a', b', $N(c)$, $F(c)$, t and u as in (1.3)-(1.10). Then L possesses a NRIB over K only in the cases listed below. In each case an integer ω of K is given so that $\{\omega, \omega'\}$ is a NRIB. [For compactness we write $x\equiv y(m)$ for $x\equiv y \pmod m$.]*

$c\equiv 2(4)$

(i) $a\equiv 1(2)$, $b\equiv 0(2)$, $a+b\equiv 1(4)$, $a'\equiv 1(4)$,
(ii) $a\equiv 1(2)$, $b\equiv 0(2)$, $a+b\equiv 1(4)$, $a'\equiv 3(4)$, $c>0$, $N(c)=-1$,
(iii) $a\equiv 2(4)$, $b\equiv 0(4)$, $a+b\equiv c(8)$, $a'\equiv 1(4)$,
(iv) $a\equiv 2(4)$, $b\equiv 0(4)$, $a+b\equiv c(8)$, $a'\equiv 3(4)$, $c>0$, $N(c)=-1$.

$$\omega=\frac{1}{2}+\frac{\sqrt{\mu}}{2\gamma} \text{ (i) (iii)} \qquad \omega=\frac{t+u\sqrt{c}}{2}+\frac{\sqrt{\mu}}{2\gamma} \text{ (ii) (iv)}$$

$c\equiv 3(4)$

(i) $a\equiv 1(2)$, $b\equiv 0(4)$, $a'\equiv 1(4)$,
(ii) $a\equiv 1(2)$, $b\equiv 0(4)$, $a'\equiv 3(4)$, $c=-1$,
(iii) $a\equiv 1(2)$, $b\equiv 0(4)$, $a'\equiv 3(4)$, $c>0$, $t\equiv 0(2)$, $u\equiv 1(2)$,
(iv) $a\equiv 0(4)$, $b\equiv 2(4)$, $a\equiv c+1(8)$, $a'\equiv 1(4)$,
(v) $a\equiv 0(4)$, $b\equiv 2(4)$, $a\equiv c+1(8)$, $a'\equiv 3(4)$, $c=-1$,
(vi) $a\equiv 0(4)$, $b\equiv 2(4)$, $a\equiv c+1(8)$, $a'\equiv 3(4)$, $c>0$, $t\equiv 0(2)$, $u\equiv 1(2)$.

$$\omega=\frac{1}{2}+\frac{\sqrt{\mu}}{2\gamma}\ \text{(i) (iv)}\quad \omega=\frac{\sqrt{c}}{2}+\frac{\sqrt{\mu}}{2\gamma}\ \text{(ii) (v)}$$

$$\omega=\frac{t+u\sqrt{c}}{2}+\frac{\sqrt{\mu}}{2\gamma}\ \text{(iii) (vi)}$$

$c\equiv 5(8)$

(i) $a\equiv 1(2)$, $b\equiv 0(2)$, $a+b\equiv 1(4)$, $a'\equiv b'\equiv 0(2)$,
(ii) $a\equiv 1(2)$, $b\equiv 0(2)$, $a+b\equiv 1(4)$, $a'\equiv b'\equiv 1(2)$, $c=-3$,
(iii) $a\equiv 1(2)$, $b\equiv 0(2)$, $a+b\equiv 1(4)$, $a'\equiv b'\equiv 1(2)$, $c>0$, $F(c)=1$,
(iv) $a\equiv 6(8)$, $b\equiv 2(4)$, $a-b-c\equiv 3$ *or* $15(16)$, $c=-3$,
(v) $a\equiv 6(8)$, $b\equiv 2(4)$, $a-b-c\equiv 3$ *or* $15(16)$, $c>0$, $F(c)=1$.

$$\omega=\frac{1}{2}+\frac{\sqrt{\mu}}{2\gamma}\ \text{(i)}\quad \omega=\frac{1+(-1)^{(1-b')/2}\sqrt{c}}{4}+\frac{\sqrt{\mu}}{2\gamma}\ \text{(ii) (iv)}$$

$$\omega=\frac{t+(-1)^{(t-b'u)/2}u\sqrt{c}}{4}+\frac{\sqrt{\mu}}{2\gamma}\ \text{(iii) (v)}$$

$c\equiv 1(8)$

(i) $a\equiv 1(2)$, $b\equiv 0(2)$, $a+b\equiv 1(4)$,
(ii) $a\equiv 2(8)$, $b\equiv 2(4)$, r *(even)* $\geqq 6$, $(a^2-b^2c)/2^r\equiv 1(4)$.

$$\omega=\frac{1}{2}+\frac{\sqrt{\mu}}{2\gamma}\ \text{(i) (ii)}$$

In Sections 3, 4 and 5 we investigate the special cases when L is cyclic, bicyclic, and pure respectively. We determine when the existence of a RIB and a squarefree relative discriminant are both necessary and sufficient for the existence of a NRIB.

THEOREM 2. *If L is a cyclic quartic field with quadratic subfield K, then L/K has a NRIB if and only if L/K has a RIB and $d(L/K)$ is squarefree.*

THEOREM 3. *Let c be a squarefree integer, and set $K=Q(\sqrt{c})$. Let L be a bicyclic quartic field containing K. Then $L=Q(\sqrt{c},\sqrt{a})$ for some squarefree integer a with $a\neq c$. As $L=Q(\sqrt{c},\sqrt{ac/(a,c)^2})$, we can choose between a and $ac/(a,c)^2$ when $c\neq -1$ so that $c\nmid a$.*

If $c=-3$, -1, *or* $c>0$, $N(c)=-1$, *then*

$$L/K \text{ has a } NRIB \Longleftrightarrow L/K \text{ has a } RIB \text{ and } d(L/K) \text{ is squarefree.}$$

If $c<-3$ *then*

$$L/K \text{ has a } NRIB \Longleftrightarrow L/K \text{ has a } RIB,\ d(L/K) \text{ is squarefree,} \quad \text{and } a\equiv 1 \pmod 4.$$

If $c>0$ *and* $N(c)=1$ *then*

$$L/K \text{ has a } NRIB \Longleftrightarrow L/K \text{ has a } RIB,\ d(L/K) \text{ is squarefree,}$$

and

$$\begin{cases} (a,c)=1,\ a\equiv 1 \pmod 4 \\ \qquad or \\ (a,c)=1,\ c\equiv 3 \pmod 4,\ a\equiv 3 \pmod 4,\ t\equiv 0 \pmod 2,\ u\equiv 1 \pmod 2 \\ \qquad or \\ (a,c)\neq 1,\ c\equiv 1 \pmod 4 \\ \qquad or \\ (a,c)\neq 1,\ c\not\equiv 1 \pmod 4,\ \dfrac{at}{(a,c)}\equiv 1 \pmod 4. \end{cases}$$

THEOREM 4. *If L is a pure quartic field then $L=Q(\sqrt{b\sqrt{c}})$, where b and c are squarefree integers with $(b, c)\neq(\pm 2, -1)$ and $c\nmid b$ if $c\neq -1$. Set $K=Q(\sqrt{c})$. Then*

$$L/K \text{ has a } NRIB \Longleftrightarrow L/K \text{ has a } RIB \text{ and } d(L/K) \text{ is squarefree.}$$

Kawamoto [5, Propositions 10 and 11] has different formulations of Theorems 2 and 3. Massy [6], [7] has given a necessary and sufficient condition for a quadratic field K to be a subfield of a cyclic quartic field L possessing a NRIB over K.

2. Proof of Theorem 1

Let $L=Q(\sqrt{c}, \sqrt{a+b\sqrt{c}})$ and $K=Q(\sqrt{c})$, where a, b, c are integers such that (a, b) and c are squarefree, and $a+b\sqrt{c}\notin K^2$. We suppose that L possesses a RIB over K, and take the RIB in the form $\{1, \kappa\}$, where κ is given by (1.1).

Before proving Theorem 1, we prove four lemmas. We denote the group of units of O_K by U_K.

LEMMA 1. *Let the fields L and K be as specified above. If the relative discriminant $d(L/K)$ is not squarefree, then L/K does not possess a NRIB.*

Proof. Let $\{1, \kappa\}$ be the RIB for L/K specified above, and suppose that L/K possesses a NRIB, say, $\{\alpha+\beta\kappa, \alpha+\beta\kappa'\}$, where α, $\beta\in O_K$ and κ' denotes the conjugate of κ over K. As $\{\alpha+\beta\kappa, \alpha+\beta\kappa'\}$ is a RIB for L/K, there exist λ, $\phi\in O_K$ with

$$1=\lambda(\alpha+\beta\kappa)+\phi(\alpha+\beta\kappa'). \tag{2.1}$$

Taking the conjugates of (2.1) over K, we obtain

$$1=\lambda(\alpha+\beta\kappa')+\phi(\alpha+\beta\kappa). \tag{2.2}$$

From (2.1) and (2.2), we see that $\lambda=\phi$. Then (2.1) gives $1=\lambda(2\alpha+\beta(\kappa+\kappa'))$, so that $2\alpha+\beta(\kappa+\kappa')\in U_K$. Next, we have

$$\begin{aligned} d(L/K)&=\begin{vmatrix}\alpha+\beta\kappa & \alpha+\beta\kappa' \\ \alpha+\beta\kappa' & \alpha+\beta\kappa\end{vmatrix}^2 O_K \\ &=((\alpha+\beta\kappa)^2-(\alpha+\beta\kappa')^2)^2 O_K \\ &=\beta^2(\kappa-\kappa')^2(2\alpha+\beta(\kappa+\kappa'))^2 O_K \\ &=\beta^2(\kappa-\kappa')^2 O_K . \end{aligned}$$

Now suppose that $d(L/K)$ is not squarefree. Thus there exists a prime ideal P of O_K with $P^2 | d(L/K)$, so that

$$P^2 | \beta^2(\kappa-\kappa')^2 O_K . \tag{2.3}$$

Let $\mathcal{P}$ be a prime ideal in O_L lying above P. Then, from (2.3), we see that

$$\mathcal{P} | \beta(\kappa-\kappa') O_L .$$

From (1.4) and (1.5), we deduce that $P|2O_K$, so that $\mathcal{P}|2O_L$. Hence we have

$$\mathcal{P} | (\beta(\kappa-\kappa')+2(\alpha+\beta\kappa'))O_L ,$$

contradicting that $2\alpha+\beta(\kappa+\kappa')\in U_K$. □

LEMMA 2. *Let the fields L and K be as specified above with relative integral basis* $\{1, \kappa\}$, *where* κ *is defined in* (1.1). *Then* L/K *has a NRIB if and only if there exists* $\lambda\in U_K$ *such that*

$$2 | \lambda-\theta , \tag{2.4}$$

where θ *is given by* (1.2). *When* (2.4) *holds, a NRIB for* L/K *is*

$$\left\{\frac{\lambda}{2}+\frac{\sqrt{\mu}}{2\gamma}, \frac{\lambda}{2}-\frac{\sqrt{\mu}}{2\gamma}\right\}.$$

Proof. Suppose L/K has a NRIB, say, $\{\alpha+\beta\kappa, \alpha+\beta\kappa'\}$. Then, exactly as in the proof of Lemma 1, we deduce that $\varepsilon=2\alpha+\beta(\kappa+\kappa')=2\alpha+\beta\theta\in U_K$. As $\{\alpha\varepsilon^{-1}+\beta\varepsilon^{-1}\kappa, \alpha\varepsilon^{-1}+\beta\varepsilon^{-1}\kappa'\}$ is also a NRIB for L/K, we may take $\varepsilon=1$ without loss of generality, so that

$$2\alpha+\beta\theta=1. \tag{2.5}$$

As $\{\alpha+\beta\kappa, \alpha+\beta\kappa'\}$ is a RIB for L/K, there exist $\rho, \tau\in O_K$ such that

$$\kappa=\rho(\alpha+\beta\kappa)+\tau(\alpha+\beta\kappa'),$$

and so, by (1.1), we have

$$\frac{\theta}{2}+\frac{\sqrt{\mu}}{2\gamma}=\rho\left(\alpha+\beta\frac{\theta}{2}+\beta\frac{\sqrt{\mu}}{2\gamma}\right)+\tau\left(\alpha+\beta\frac{\theta}{2}-\beta\frac{\sqrt{\mu}}{2\gamma}\right). \tag{2.6}$$

Equating coefficients of $\sqrt{\mu}/2\gamma$ in (2.6), we obtain $1=(\rho-\tau)\beta$, showing that $\beta\in U_K$. We define $\lambda\in U_K$ by $\lambda=1/\beta$, and, from (2.5), we deduce that $2\mid\lambda-\theta$, and a NRIB for L/K is

$$\begin{aligned}\{\lambda(\alpha+\beta\kappa), \lambda(\alpha+\beta\kappa')\} &= \{\lambda\alpha+\kappa, \lambda\alpha+\kappa'\}\\ &=\left\{\frac{\lambda-\theta}{2}+\frac{\theta}{2}+\frac{\sqrt{\mu}}{2\gamma}, \frac{\lambda-\theta}{2}+\frac{\theta}{2}-\frac{\sqrt{\mu}}{2\gamma}\right\}\\ &=\left\{\frac{\lambda}{2}+\frac{\sqrt{\mu}}{2\gamma}, \frac{\lambda}{2}-\frac{\sqrt{\mu}}{2\gamma}\right\}.\end{aligned}$$

Conversely suppose that $\lambda\in U_K$ with $2\mid\lambda-\theta$. Then we have $\alpha=(\lambda-\theta)/2\in O_K$. We claim that $\{\lambda/2+\sqrt{\mu}/2\gamma, \lambda/2-\sqrt{\mu}/2\gamma\}=\{\alpha+\kappa, \alpha+\kappa'\}$ is a NRIB. This is clear as

$$1=\frac{1}{\lambda}(\alpha+\kappa)+\frac{1}{\lambda}(\alpha+\kappa')$$

and

$$\kappa=\left(\frac{\lambda+\theta}{2\lambda}\right)(\alpha+\kappa)-\left(\frac{\lambda-\theta}{2\lambda}\right)(\alpha+\kappa'). \qquad \square$$

The next lemma summarizes some elementary properties of the form of the units of O_K when $c>0$. The proof of the lemma is an easy exercise in elementary number theory.

LEMMA 3. *Let c be a positive squarefree integer.*

If $c\equiv 2 \pmod 4$ then $F(c)=-1$, $N(c)=\pm 1$, and every unit of O_K is of the form $x+y\sqrt{c}$, where the integers x and y satisfy

$$x\equiv 1 \pmod 2,\quad y\equiv 0 \pmod 2,\quad \textit{if } x^2-cy^2=1,$$

$$x\equiv 1 \pmod 2,\quad y\equiv 1 \pmod 2,\quad \textit{if } x^2-cy^2=-1.$$

If $c\equiv 3 \pmod 4$ then $F(c)=-1$, $N(c)=1$, and every unit of O_K is of the form $x+y\sqrt{c}$, where the integers x and y satisfy

$$x \equiv 0 \pmod 2), \quad y \equiv 1 \pmod 2)$$

or

$$x \equiv 1 \pmod 2), \quad y \equiv 0 \pmod 2).$$

If $c \equiv 5 \pmod 8$ *and* $F(c)=1$, *then* $N(c)=\pm 1$ *and every unit of* O_K *is of the form* $(x+y\sqrt{c})/2$, *where the integers* x *and* y *satisfy*

$$x \equiv y \equiv 1 \pmod 2)$$

or

$$x \equiv 0 \pmod 4), \quad y \equiv 2 \pmod 4), \quad x^2-cy^2=-4,$$

or

$$x \equiv 2 \pmod 4), \quad y \equiv 0 \pmod 4), \quad x^2-cy^2=4.$$

If $c \equiv 5 \pmod 8$ *and* $F(c)=-1$, *then* $N(c)=\pm 1$ *and every unit of* O_K *is of the form* $x+y\sqrt{c}$, *where the integers* x *and* y *satisfy*

$$x \equiv 0 \pmod 2), \quad y \equiv 1 \pmod 2), \quad \textit{if } x^2-cy^2=-1,$$

or

$$x \equiv 1 \pmod 2), \quad y \equiv 0 \pmod 2), \quad \textit{if } x^2-cy^2=1.$$

If $c \equiv 1 \pmod 8$ *then* $F(c)=-1$, $N(c)=\pm 1$, *and every unit of* O_K *is of the form* $x+y\sqrt{c}$, *where the integers* x *and* y *satisfy*

$$x \equiv 1 \pmod 2), \quad y \equiv 0 \pmod 4), \quad \textit{if } x^2-cy^2=1,$$

$$x \equiv 0 \pmod 4), \quad y \equiv 1 \pmod 2), \quad \textit{if } x^2-cy^2=-1.$$

In Lemma 4 we make use of Lemma 3 to determine $\lambda \in U_K$ satisfying (2.4) when such λ exists.

LEMMA 4. *Let* c *be a squarefree integer.*

If $c \equiv 2 \pmod 4$ *then* $\theta=0, 1, \sqrt{c}$ *or* $1+\sqrt{c}$, *and there exists* $\lambda \in U_K$ *with* $2 \mid \lambda-\theta$ *if and only if*

$$\theta=1 \quad (\lambda=1)$$

or

$$\theta=1+\sqrt{c}, \quad c>0, \quad N(c)=-1 \quad (\lambda=\varepsilon_c).$$

If $c \equiv 3 \pmod 4$ *then* $\theta=0, 1, \sqrt{c}$ *or* $1+\sqrt{c}$, *and there exists* $\lambda \in U_K$ *with* $2 \mid \lambda-\theta$ *if and only if*

$$\theta=1 \quad (\lambda=1)$$

or

$$\theta=\sqrt{c}, \quad c>0, \quad t \equiv 0 \pmod 2), \quad u \equiv 1 \pmod 2) \quad (\lambda=\varepsilon_c)$$

or

$$\theta=\sqrt{c}, \quad c=-1 \quad (\lambda=\sqrt{-1}).$$

If $c\equiv 5 \pmod 8$ *then* $\theta=0, 1$, *or* $(b'+\sqrt{c})/2$, *and there exists* $\lambda\in U_K$ *with* $2|\lambda-\theta$ *if and only if*

$$\theta=1 \quad (\lambda=1)$$

or

$$\theta=\frac{b'+\sqrt{c}}{2}, \quad c=-3 \quad \left(\lambda=\frac{1+(-1)^{(1-b')/2}\sqrt{-3}}{2}\right)$$

or

$$\theta=\frac{b'+\sqrt{c}}{2}, \quad c>0, \quad \textit{and} \quad F(c)=1 \quad \left(\lambda=\frac{t+(-1)^{(t-b'u)/2}u\sqrt{c}}{2}\right).$$

If $c\equiv 1 \pmod 8$ *then* $\theta=0, 1, (1+\sqrt{c})/2$, *or* $(-1+\sqrt{c})/2$, *and there exists* $\lambda\in U_K$ *with* $2|\lambda-\theta$ *if and only if*

$$\theta=1 \quad (\lambda=1).$$

Proof. The values of θ corresponding to the residue class of c modulo 4 or 8 follow from [9, Theorem 2]. The remaining assertions of the lemma follow easily from Lemma 3. □

We are now ready to prove Theorem 1.

Proof of Theorem 1. Recall that we are assuming that L/K has the RIB $\{1, \kappa\}$. Suppose further that L/K has a NRIB. By Lemma 1 $d(L/K)$ is squarefree. Appealing to [9, Theorem 1] a, b, c must fall into one of the following cases:

Case 1: $a\equiv 1 \pmod 2$, $b\equiv 0 \pmod 2$, $c\equiv 2 \pmod 4$, $a+b\equiv 1 \pmod 4$,
Case 2: $a\equiv 2 \pmod 4$, $b\equiv 0 \pmod 4$, $c\equiv 2 \pmod 4$, $a+b\equiv c \pmod 8$,
Case 3: $a\equiv 1 \pmod 2$, $b\equiv 0 \pmod 4$, $c\equiv 3 \pmod 4$,
Case 4: $a\equiv 0 \pmod 4$, $b\equiv 2 \pmod 4$, $c\equiv 3 \pmod 4$, $a\equiv c+1 \pmod 8$,
Case 5: $a\equiv 1 \pmod 2$, $b\equiv 0 \pmod 2$, $c\equiv 5 \pmod 8$, $a+b\equiv 1 \pmod 4$,
Case 6: $a\equiv 6 \pmod 8$, $b\equiv 2 \pmod 4$, $c\equiv 5 \pmod 8$, $a-b-c\equiv 3$ or $15 \pmod{16}$,
Case 7: $a\equiv 1 \pmod 2$, $b\equiv 0 \pmod 2$, $c\equiv 1 \pmod 8$, $a+b\equiv 1 \pmod 4$,
Case 8: $a\equiv 2 \pmod 8$, $b\equiv 2 \pmod 8$, $c\equiv 1 \pmod 8$, r (even)$\geqq 6$, $(a^2-b^2c)/2^r\equiv 1 \pmod 4$,
Case 9: $a\equiv 2 \pmod 8$, $b\equiv 6 \pmod 8$, $c\equiv 1 \pmod 8$, r (even)$\geqq 6$, $(a^2-b^2c)/2^r\equiv 1 \pmod 4$.

We emphasize that if a, b, c do not satisfy one of Cases 1 to 9 then $d(L/K)$ is not squarefree and L/K does not possess a NRIB. We now examine each of the above cases making use of Lemma 4 to determine the additional constraints on a, b, c in order for L/K to have a NRIB.

Cases 1 and 2. By [9, Theorem 2] we have

$$\theta=\begin{cases} 1, & \text{if } a'\equiv 1 \pmod 4, \\ 1+\sqrt{c}, & \text{if } a'\equiv 3 \pmod 4). \end{cases}$$

Thus, by Lemmas 2 and 4, L/K has NRIB in this case if and only if

$$a'\equiv 1 \pmod 4$$

or

$$a'\equiv 3 \pmod 4, \quad c>0, \quad N(c)=-1.$$

The NRIB's are respectively

$$\left\{\frac{1}{2}+\frac{\sqrt{\mu}}{2\gamma}, \frac{1}{2}-\frac{\sqrt{\mu}}{2\gamma}\right\}$$

and

$$\left\{\frac{t+u\sqrt{c}}{2}+\frac{\sqrt{\mu}}{2\gamma}, \frac{t+u\sqrt{c}}{2}-\frac{\sqrt{\mu}}{2\gamma}\right\}.$$

Cases 3 and 4. By [9, Theorem 2] we have

$$\theta=\begin{cases} 1, & \text{if } a'\equiv 1 \pmod 4, \\ \sqrt{c}, & \text{if } a'\equiv 3 \pmod 4). \end{cases}$$

Then, by Lemmas 2 and 4, L/K has a NRIB in this case if and only if

$$a'\equiv 1 \pmod 4$$

or

$$a'\equiv 3 \pmod 4, \quad c=-1,$$

or

$$a'\equiv 3 \pmod 4, \quad c>0, \quad t\equiv 0 \pmod 2, \quad u\equiv 1 \pmod 2.$$

The NRIB's are respectively

$$\left\{\frac{1}{2}+\frac{\sqrt{\mu}}{2\gamma}, \frac{1}{2}-\frac{\sqrt{\mu}}{2\gamma}\right\},$$

$$\left\{\frac{\sqrt{c}}{2}+\frac{\sqrt{\mu}}{2\gamma}, \frac{\sqrt{c}}{2}-\frac{\sqrt{\mu}}{2\gamma}\right\},$$

and

$$\left\{\frac{t+u\sqrt{c}}{2}+\frac{\sqrt{\mu}}{2\gamma}, \frac{t+u\sqrt{c}}{2}-\frac{\sqrt{\mu}}{2\gamma}\right\}.$$

Case 5. By [9, Theorem 2] we have

$$\theta=\begin{cases} 1, & \text{if } a'\equiv b'\equiv 0 \pmod 2, \\ \dfrac{b'+\sqrt{c}}{2}, & \text{if } a'\equiv b'\equiv 1 \pmod 2). \end{cases}$$

Then, by Lemmas 2 and 4, L/K has a NRIB in this case if and only if

$$a'\equiv b'\equiv 0 \pmod 2$$

or

$$a'\equiv b'\equiv 1 \pmod 2, \quad c=-3$$

or

$$a'\equiv b'\equiv 1 \pmod 2, \quad c>0, \quad F(c)=1.$$

The NRIB's are respectively

$$\left\{\frac{1}{2}+\frac{\sqrt{\mu}}{2\gamma}, \frac{1}{2}-\frac{\sqrt{\mu}}{2\gamma}\right\},$$

$$\left\{\frac{1+(-1)^{(1-b')/2}\sqrt{c}}{4}+\frac{\sqrt{\mu}}{2\gamma}, \frac{1+(-1)^{(1-b')/2}\sqrt{c}}{4}-\frac{\sqrt{\mu}}{2\gamma}\right\},$$

$$\left\{\frac{t+(-1)^{(t-b'u)/2}u\sqrt{c}}{4}+\frac{\sqrt{\mu}}{2\gamma}, \frac{t+(-1)^{(t-b'u)/2}u\sqrt{c}}{4}-\frac{\sqrt{\mu}}{2\gamma}\right\}.$$

Case 6. By [9, Theorem 2] we have

$$\theta=\frac{b'+\sqrt{c}}{2}.$$

Thus, by Lemmas 2 and 4, L/K has a NRIB in this case if and only if

$$a'\equiv b'\equiv 1 \pmod 2, \quad c=-3$$

or

$$a'\equiv b'\equiv 1 \pmod 2, \quad c>0, \quad F(c)=1.$$

The NRIB's are respectively

$$\left\{\frac{1+(-1)^{(1-b')/2}\sqrt{c}}{4}+\frac{\sqrt{\mu}}{2\gamma}, \frac{1+(-1)^{(1-b')/2}\sqrt{c}}{4}-\frac{\sqrt{\mu}}{2\gamma}\right\},$$

$$\left\{\frac{t+(-1)^{(t-b'u)/2}u\sqrt{c}}{4}+\frac{\sqrt{\mu}}{2\gamma}, \frac{t+(-1)^{(t-b'u)/2}u\sqrt{c}}{4}-\frac{\sqrt{\mu}}{2\gamma}\right\}.$$

Cases 7, 8, 9. By [9, Theorem 2] we have $\theta=1$. Thus, by Lemmas 2 and 4, L/K has a NRIB namely,

$$\left\{\frac{1}{2}+\frac{\sqrt{\mu}}{2\gamma}, \frac{1}{2}-\frac{\sqrt{\mu}}{2\gamma}\right\}. \qquad \square$$

3. L cyclic: Proof of Theorem 2

Let L be a cyclic quartic field with unique quadratic subfield K, and assume that L/K has a RIB. By Lemma 1 we know that if $d(L/K)$ is not squarefree then L/K does not possess a NRIB. Thus to complete the proof it suffices to prove that if $d(L/K)$ is squarefree then L/K has a NRIB. It is known (see

[8]) that L may be taken in the form $L=Q(\sqrt{A(D+B\sqrt{D})})$, where A is squarefree and odd, $D=B^2+C^2$ is squarefree ($B>0$, $C>0$), and $(A, D)=1$. Then, appealing to [8, Lemma 2], we see that $d(L/K)$ squarefree implies

$$D\equiv 1 \pmod 4, \quad B\equiv 0 \pmod 2, \quad A+B\equiv 1 \pmod 4.$$

Further, by [8, Theorem 3], as L/K has a RIB, we can take the RIB as

$$\left\{1, \frac{1}{2}\left(1+\sqrt{A(D+B\sqrt{D})}\right)\right\}.$$

Thus L possesses a NRIB over K, namely,

$$\left\{\frac{1}{2}\left(1-\sqrt{A(D+B\sqrt{D})}\right), \frac{1}{2}\left(1+\sqrt{A(D+B\sqrt{D})}\right)\right\}. \qquad \square$$

4. L bicyclic: Proof of Theorem 3

If L/K has a NRIB then clearly L/K has a RIB and, by Lemma 1, $d(L/K)$ is squarefree.

Now suppose that L/K has a RIB and $d(L/K)$ is squarefree. There are nine possibilities for the pair $(c, a) \pmod 4$. The second assumption by [9, Theorem 1] eliminates four of these and leaves only the five possibilities

(4.1) $\quad (c, a)\equiv(1, 1), (2, 1), (2, 2)$ (with $a\equiv c \pmod 8$), $(3, 1), (3, 3) \pmod 4$.

Further, the first assumption by [9, Theorem 2] guarantees the existence of an element γ in O_K with $S=\gamma O_K$. Recalling that the only primes which ramify in K are the odd prime divisors of c and the prime 2 if $c\not\equiv 1 \pmod 4$, we see from (1.4) that $S^2=(a, c)O_K$. Thus

(4.2) $$\gamma^2=(a, c)\theta, \quad \text{for some unit } \theta \text{ of } O_K.$$

It is now convenient to treat cases.

$c=-3$. From (4.1) we have $a\equiv 1 \pmod 4$, and by Theorem 1 ($c\equiv 5 \pmod 8$, (i), (ii)) L/K has a NRIB.

$c=-1$. Here $\theta=\pm 1$ or $\pm i$. From (4.1) we have $a\equiv 1 \pmod 2$. Further $(a, c)=1$ as $\gamma^2=(a, c)\theta$ cannot hold with $\theta=\pm i$. Thus $\theta=\pm 1$, $\gamma^2=\pm 1$, $a'+b'i=a/\gamma^2=\pm a$, so $a'\equiv 1 \pmod 2$. Hence by Theorem 1 ($c\equiv 3 \pmod 4$, (i), (ii)) L/K has a NRIB.

$c>0$, $N(c)=-1$. As $N(c)=-1$, we have $c\not\equiv 3 \pmod 4$. Thus, by (4.1), we have $(c, a)\equiv(1, 1)$, $(2, 1)$ or $(2.2) \pmod 4$. Clearly, from (4.2), we see that we may assume without loss of generality that $\theta=\pm 1$ or $\theta=\pm\varepsilon_c$.

When $c\equiv 2 \pmod 4$, θ is of the form $x+y\sqrt{c}$ with x odd, so from $a'+b'\sqrt{c}=a/((a, c)\theta)$, we see that a' is odd. Hence, by Theorem 1 ($c\equiv 2 \pmod 4$, (i)-(iv)), L/K has a NRIB.

When $c\equiv 1 \pmod 8$, we have $a\equiv 1 \pmod 4$, and by Theorem 1 ($c\equiv 1 \pmod 8$, (i)) L/K has a NRIB.

When $c\equiv 5 \pmod 8$ we must examine θ more closely. Clearly $\theta=\gamma^2/(a, c)>0$ so that $\theta=1$ or ε_c. Further

$$N(\theta)=N(\gamma)^2/(a, c)^2>0$$

so that $\theta\neq\varepsilon_c$ as $N(\varepsilon_c)=-1$. Hence $\theta=1$, and $\gamma^2=(a, c)$. As $\gamma\in O_K$ we have $\gamma=(r+s\sqrt{c})/2$, where r, s are integers with $r\equiv s \pmod 2$. Thus

$$r^2+s^2c=4(a, c), \quad 2rs=0.$$

If $r=0$ then $s^2c=4(a, c)$ so $c\mid a$, a contradiction. If $s=0$ then $r^2=4(a, c)$ so $(r/2)^2=(a, c)$. But (a, c) is squarefree, so $r/2=\pm 1$, $(a, c)=1$, and $\gamma^2=1$. Thus $(a'+b'\sqrt{c})/2=a$, so $a'\equiv b'\equiv 0 \pmod 2$, and by Theorem 1 ($c\equiv 5 \pmod 8$, (i)) L/K has a NRIB.

$c<-3$. Here $\theta=\pm 1$. From (4.2) we have $\gamma^2=\pm(a, c)$. We show that the plus sign must hold and $(a, c)=1$, for otherwise (remembering that c and (a, c) are squarefree) we have $[Q(\sqrt{\pm(a, c)}): Q]=2$ and $\sqrt{\pm(a, c)}=\gamma\in Q(\sqrt{c})$, so $c=-(a, c)$ and thus $c\mid a$, a contradiction. Hence $\gamma^2=(a, c)=1$. Note that this rules out the case $c\equiv a\equiv 2 \pmod 4$. (There is no RIB in this case.) Now by (1.8) we have

$$a'+b'\sqrt{c}=\begin{cases} a, & \text{if } c\not\equiv 1 \pmod 4, \\ 2a, & \text{if } c\equiv 1 \pmod 4. \end{cases}$$

From Theorem 1 (examining cases), we see that L/K possesses a NRIB only when $a\equiv 1 \pmod 4$.

$c>0$, $N(c)=1$. From (4.2) we see without loss of generality that $\theta=\pm 1$ or $\theta=\pm\varepsilon_c$. As $\theta=\gamma^2/(a, c)>0$, we have $\theta=1$ or $\theta=\varepsilon_c$. If $(a, c)\neq 1$ we show that $\theta=\varepsilon_c$ Otherwise $\theta=1$, $[Q(\sqrt{(a, c)}): Q]=2$ and $\sqrt{(a, c)}=\gamma\in Q(\sqrt{c})$, so $(a, c)=c$ contradicting $c\nmid a$. If $(a, c)=1$ we show that $\theta=1$. Otherwise $\theta=\varepsilon_c=\gamma^2$, contradicting that ε_c is a fundamental unit.

If $(a, c)=1$ then $\theta=1$ and $\gamma^2=1$. Hence, by (1.8), we have

$$a'+b'\sqrt{c}=\begin{cases} a, & \text{if } c\not\equiv 1 \pmod 4, \\ 2a, & \text{if } c\equiv 1 \pmod 4. \end{cases}$$

From Theorem 1 (examining cases) we see that L/K possesses a NRIB only when

$$a\equiv 1 \pmod 4$$

or

$$c\equiv 3 \pmod 4, \quad a\equiv 3 \pmod 4, \quad t\equiv 0 \pmod 2, \quad u\equiv 1 \pmod 2.$$

If $(a, c)\neq 1$ then $\theta=\varepsilon_c$ and $\gamma^2=(a, c)\varepsilon_c$. Hence, by (1.8), (1.10) and Lemma 3, we have

$$a'+b'\sqrt{c}=\begin{cases}\dfrac{a}{(a,\ c)}(t-u\sqrt{c}), & \text{if } c\not\equiv 1 \pmod 4, \\ & \text{or} \\ & c\equiv 5 \pmod 8,\ F(c)=1, \\ \dfrac{2a}{(a,\ c)}(t-u\sqrt{c}), & \text{if } c\equiv 5 \pmod 8,\ F(c)=-1 \text{ or } c\equiv 1 \pmod 8.\end{cases}$$

Again by Theorem 1, after an examination of cases, we see that L/K possesses a NRIB only when

$$c\equiv 1 \pmod 4 \text{ or } c\not\equiv 1 \pmod 4,\ \frac{at}{(a,\ c)}\equiv 1 \pmod 4. \qquad \square$$

We note that Theorem 3 extends work of Brinkhuis [1] and Gras [2].

5. L pure: Proof of Theorem 4

Let L be a pure quartic field so that $L=Q(\sqrt{b\sqrt{c}})$, where b and c are squarefree integers with $(b,\ c)\neq(\pm 2,\ -1)$ and $c\nmid b$ if $c\neq -1$. Set $K=Q(\sqrt{c})$. Suppose L/K has a RIB and that $d(L/K)$ is squarefree. By Theorem 1 of [9] and the tables in [3] or [4] the latter assumption implies that

$$c\equiv 7 \pmod 8, \quad b\equiv 2 \pmod 4.$$

The first assumption guarantees the existence of $\gamma\in O_K$ and $\theta\in U_K$ such that

$$2(b,\ c)=\gamma^2\theta .$$

We show that $\theta=\pm 1$ is impossible. Suppose $\theta=\pm 1$ then $a'+b'\sqrt{c}=b\sqrt{c}/\pm 2(b,\ c)$ so $a'=0$. As L/K possesses a RIB, by Theorem 2 of [9], we see that a' is odd, a contradiction.

We now treat two cases according as $c<0$ or $c>0$. If $c<0$ we must have $c=-1$, $\theta=\pm i$. Thus $a'=\mp b/2\equiv 1 \pmod 2$ and L/K has a NRIB by Theorem 1. If $c>0$ we have without loss of generality $\theta=\pm\varepsilon_c$. Further $\theta=2(b,\ c)/\gamma^2>0$ so $\theta=\varepsilon_c$. Also $N(\varepsilon_c)=N(\theta)=4(b,\ c)^2/N(\gamma)^2>0$ so $N(\varepsilon_c)=1$. Hence $a'=bcu/2(b,\ c)$. As L/K possesses a RIB, by Theorem 2 of [9], a' is odd, so that $u\equiv 1 \pmod 2$, and thus $t\equiv 0 \pmod 2$. By Theorem 1 ($c\equiv 3 \pmod 4$, (iv), (vi)) L/K has a NRIB. $\square$

6. Examples

We conclude this paper with some examples.

Example 1. We consider $L=Q(\sqrt{-17+18\sqrt{5}})$. The quadratic subfield of L is $K=Q(\sqrt{5})$. It was shown in [9, Example 2] that L/K possesses a RIB. Here $a=-17$, $b=18$, $c=5$, $\mu=-17+18\sqrt{5}=((-1+3\sqrt{5})/2)^3$, $R=S=((-1+3\sqrt{5})$

/2), $T=(1)$, $\gamma=(-1+3\sqrt{5})/2$, $\varepsilon_5=(1+\sqrt{5})/2$, $t=u=1$, $F(5)=1$, $(a'+b'\sqrt{c})/2=\mu/\gamma^2=(-1+3\sqrt{5})/2$, $a'=-1$, $b'=3$. Thus by Theorem 1 ($c\equiv 5 \pmod 8$), (iii)) L/K has a NRIB, which can be taken as

$$\left\{\frac{1-\sqrt{5}}{4}+\frac{1}{2}\sqrt{\frac{-1+3\sqrt{5}}{2}},\ \frac{1-\sqrt{5}}{4}-\frac{1}{2}\sqrt{\frac{-1+3\sqrt{5}}{2}}\right\}.$$

Example 2. We take $L=Q(\sqrt{-5}, \sqrt{-1})$ and $K=Q(\sqrt{-5})$. Here $a=-1$, $b=0$, $c=-5$, $\mu=-1$, $R=S=T=O_K$, $\gamma=1$, L/K has a RIB by [9, Theorem 2], and $d(L/K)$ is squarefree. However, $a\not\equiv 1 \pmod 4$ so, by Theorem 3, L/K does not possess a NRIB.

Example 3. Let a and b be integers with (a, b) squarefree and $a+bi$ not a square in $K=Q(i)$. Then $L=Q(\sqrt{a+bi})$ possesses a NRIB over K if and only if

$$a\equiv 1 \pmod 2, \quad b\equiv 0 \pmod 4)$$

or

$$a\equiv 0 \pmod 8, \quad b\equiv 2 \pmod 4.$$

Example 4. Let a and b be integers with (a, b) squarefree and $a+b\sqrt{-3}$ not a square in $K=Q(\sqrt{-3})$. Then $L=Q(\sqrt{a+b\sqrt{-3}})$ possesses a NRIB over K if and only if

$$a\equiv 1 \pmod 2, \quad b\equiv 0 \pmod 2, \quad a+b\equiv 1 \pmod 4$$

or

$$a\equiv 6 \pmod 8, \quad b\equiv 2 \pmod 4, \quad a-b\equiv 0,\ 12 \pmod{16}.$$

Example 5. $L=Q(\sqrt{-7}, \sqrt{5})$ has a NRIB over $K=Q(\sqrt{-7})$, namely,

$$\left\{\frac{1+\sqrt{5}}{2},\ \frac{1-\sqrt{5}}{2}\right\}.$$

Example 6. This example was considered by Kawamoto [5, Remark 12]. $L=Q(\sqrt{3+2\sqrt{6}})$ has a RIB over $K=Q(\sqrt{6})$, namely

$$\left\{1,\ \frac{1}{2}\left(1+\sqrt{6}+\sqrt{3+2\sqrt{6}}\right)\right\},$$

but, by Theorem 1, L does not have a NRIB over K. Compare Sze [10, Theorem 1].

REFERENCES

[1] J. BRINKHUIS, Embedding problems and Galois modules, Doctoral Thesis, University of Leiden (1981).

[2] M.-N. GRAS, Bases d'entiers dans les extensions cycliques de degré 4 de $\boldsymbol{Q}$, Seminar on Number Theory, 1982-1983, Exp. No. 11, 11 pp.

[3] 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, 1991, 44 pp.

[4] J. G. HUARD, B. K. SPEARMAN AND K. S. WILLIAMS, Integral bases for quartic fields with quadratic subfields, J. Number Theory, **51** (1995), 87-102.

[5] F. KAWAMOTO, Normal integral bases and divisor polynomials, Ph. D. Thesis, Gakushuin University (1986).

[6] R. MASSY, Formules de construction de bases normales d'entiers relatives, C. R. Acad. Sci. Paris Sér. I Math., **313** (1991), 477-482.

[7] R. MASSY, Bases normales d'entiers relatives quadratiques, J. Number Theory, **38** (1991), 216-239.

[8] B. K. SPEARMAN AND K. S. WILLIAMS, Cyclic quartic fields with relative integral bases over their quadratic subfields, Proc. Amer. Math. Soc., **103** (1988), 687-694.

[9] B. K. SPEARMAN AND K. S. WILLIAMS, Relative integral bases for quartic fields over quadratic subfields, Acta Math. Hungar., **70** (1996), 185-192.

[10] A. SZE, A normal integral basis theorem, J. Algebra, **66** (1980), 544-549.

DEPARTMENT OF MATHEMATICS AND STATISTICS
OKANAGAN UNIVERSITY COLLEGE
KELOWNA, BRITISH COLUMBIA, CANADA
V1V 1V7
e-mail: bkspearm@okanagan. bc. ca

DEPARTMENT OF MATHEMATICS AND STATISTICS
CARLETON UNIVERSITY
OTTAWA, ONTARIO, CANADA
K1S 5B6
e-mail: williams@math. carleton. ca