Acta Math. Hungar.
70 (3) (1996), 185–192.

RELATIVE INTEGRAL BASES FOR QUARTIC FIELDS OVER QUADRATIC SUBFIELDS

B. K. SPEARMAN (Kelowna) and K. S. WILLIAMS* (Ottawa)

Let L be a quartic number field with quadratic subfield $K = Q\left(\sqrt{c}\right)$, where Q denotes the rational number field. Then $L = Q\left(\sqrt{c}, \sqrt{a+b\sqrt{c}}\right)$, 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. In [6] (see also [5]) the discriminant $d(L)$, as well as an integral basis for L were obtained explicitly in terms of a, b, c. Four cases naturally arose: (A) $c \equiv 2 \pmod 4$, (B) $c \equiv 3 \pmod 4$, (C) $c \equiv 5 \pmod 8$, and (D) $c \equiv 1 \pmod 8$. Each of these cases was subdivided into a number of subcases depending upon congruences involving a, b and c. We refer the reader to [6] (or [5]) for details.

In this paper we determine the relative discriminant $d(L/K)$ (Theorem 1), as well as a necessary and sufficient condition for L to have a relative integral basis (RIB) over K and an explicit relative integral basis when it exists (Theorem 2). Part of Theorem 2 is a special case of a result of Artin [1]. Theorem 2 extends the results of [2], [3], [4], [7], [8], [9], [10], [11], [12], [13] to an arbitrary quartic field possessing a quadratic subfield.

THEOREM 1. *Let $\mu = a + b\sqrt{c}$, where $a + b\sqrt{c}$ is not a square in $K = Q(\sqrt{c})$ and a, b, c are integers with (a, b) and c squarefree. Set $\mu O_K = RS^2$, where R and S are integral ideals of O_K with R squarefree. Then the relative discriminant $d(L/K)$ is given as follows:*

in cases A1, A5, B2, B5, C2, C7, D3, D16, D20

$$d(L/K) = R;$$

in cases A2, A6, B3, B6

$$d(L/K) = 2R;$$

in cases A3, A4, A7, A8, B1, B4, B7, B8, C1, C3, C4, C5, C6, C8, D4, D5, D6, D8, D10, D11, D12, D13, D19, D23, D26, D27

$$d(L/K) = 4R;$$

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

in cases D1, D9, D15, D17, D22, D24

$$d(L/K) = \left\langle 2, \frac{1}{2}\left(1+\sqrt{c}\right)\right\rangle^2 R;$$

in cases D2, D7, D14, D18, D21, D25

$$d(L/K) = \left\langle 2, \frac{1}{2}\left(1-\sqrt{c}\right)\right\rangle^2 R.$$

In each case $d(L/K) = T^2 R$ *for some integral ideal* T.

THEOREM 2. $L = K\left(\sqrt{a+b\sqrt{c}}\right)$ *has a relative integral basis over* $K = Q\left(\sqrt{c}\right)$ *if and only if*

$$S = T\langle\gamma\rangle$$

for some $\gamma(\neq 0) \in K$.

If $S = T\langle\gamma\rangle$, *where* $\gamma(\neq 0) \in K$, *then a relative integral basis for* L *over* K *is* $\{1, \kappa\}$, *where* κ *is given in the table below.*

κ	cases
$\dfrac{\sqrt{\mu}}{2\gamma}$	A3, A4, A7, A8, B1, B4, B7, B8, C1, C3, C4, C5, C6, C8, D4, D5, D6, D8, D10, D11, D12, D13, D19, D23, D26, D27
$\dfrac{\gamma+\sqrt{\mu}}{2\gamma}$	A1*, A5*, B2*, B5*, C2†, D3, D16, D20
$\dfrac{\gamma\sqrt{c}+\sqrt{\mu}}{2\gamma}$	A2, A6, B2**, B5**
$\dfrac{\gamma+\gamma\sqrt{c}+\sqrt{\mu}}{2\gamma}$	A1**, A5**, B3, B6
$\dfrac{\gamma+\gamma\sqrt{c}+2\sqrt{\mu}}{4\gamma}$	D1, D9, D15, D17, D22, D24
$\dfrac{-\gamma+\gamma\sqrt{c}+2\sqrt{\mu}}{4\gamma}$	D2, D7, D14, D18, D21, D25
$\dfrac{b'\gamma+\gamma\sqrt{c}+2\sqrt{\mu}}{4\gamma}$	C2‡, C7

* *indicates* $a' \equiv 1 \pmod 4$ *where* $\mu/\gamma^2 = a' + b'\sqrt{c}$
** *indicates* $a' \equiv 3 \pmod 4$ *where* $\mu/\gamma^2 = a' + b'\sqrt{c}$
† *indicates* $a' \equiv b' \equiv 0 \pmod 2$ *where* $\mu/\gamma^2 = \left(a' + b'\sqrt{c}\right)/2$
‡ *indicates* $a' \equiv b' \equiv 1 \pmod 2$ *where* $\mu/\gamma^2 = \left(a' + b'\sqrt{c}\right)/2$

PROOF OF THEOREM 1. Let P be a prime ideal of O_K. Define m_P by $P^{m_P} \| \mu O_K$ and w_P by $P^{w_P} \| d(L/K)$.

If $P \nmid 2O_K$, as $\mu O_K = RS^2$ with R squarefree, we have

$$\begin{aligned} P\|R &\Leftrightarrow m_P \text{ odd} \\ &\Leftrightarrow w_P = 1 \qquad \text{(by [5, Corollary 1 (iii)])} \\ &\Leftrightarrow P\|d(L/K). \end{aligned}$$

If $P|2O_K$ the value of w_P is given in [6 (or 5), Tables A, B, C, D].
Combining these results, we obtain the assertion of Theorem 1. □

PROOF OF THEOREM 2. Suppose L has a relative integral basis over K. This basis may be taken as $\{1, \theta\}$, where $\theta \in O_K$. We express θ in the form $\theta = \alpha + \beta\sqrt{\mu}$, where $\alpha, \beta \in K$. Then we have

$$\begin{vmatrix} 1 & \theta \\ 1 & \theta' \end{vmatrix}^2 O_K = d(L/K),$$

and so, by Theorem 1, $\langle 2\beta \rangle^2 \mu O_K = T^2 R$. As $\mu O_K = S^2 R$ we deduce $\langle 2\beta \rangle S = T$, so that $S = T\langle \gamma \rangle$, for some nonzero $\gamma \in K$.

Suppose now that $S = T\langle \gamma \rangle$ for some nonzero $\gamma \in K$. Then

$$d(L/K) = RT^2 = \frac{1}{\gamma^2} RS^2 = \frac{\mu}{\gamma^2} O_K.$$

Let $\alpha, \beta \in K$. Then

$$\begin{aligned} &\{1, \alpha + \beta\sqrt{\mu}\} \text{ is a RIB for } L/K \\ &\Leftrightarrow \alpha + \beta\sqrt{\mu} \in O_L \text{ and } \begin{vmatrix} 1 & \alpha + \beta\sqrt{\mu} \\ 1 & \alpha - \beta\sqrt{\mu} \end{vmatrix}^2 O_K = d(L/K) \\ &\Leftrightarrow \alpha + \beta\sqrt{\mu} \in O_L \text{ and } 4\beta^2 \mu O_K = \frac{\mu}{\gamma^2} O_K \\ &\Leftrightarrow \alpha + \beta\sqrt{\mu} \in O_L \text{ and } 4\beta^2\gamma^2 = \text{ unit of } O_K \\ &\Leftrightarrow \alpha + \beta\sqrt{\mu} \in O_L \text{ and } 2\beta\gamma = \text{ unit of } O_K \\ &\Leftrightarrow \alpha + \frac{\varepsilon}{2\gamma}\sqrt{\mu} \in O_L \text{ for some unit } \varepsilon \text{ of } O_K. \end{aligned}$$

We treat cases on μ. In each of the cases A1-D27 specified in [6] (or [5]) we give a value of $\alpha \in K$ for which $\alpha + \frac{1}{2\gamma}\sqrt{\mu} \in O_L$.

Cases A3, A4, A7, A8, B1, B4, B7, B8, C1, C3, C4, C5, C6, C8, D4, D5, D6, D8, D10, D11, D12, D13, D19, D23, D26, D27. In these cases $T^2 = 4O_K$, by Theorem 1, so $\frac{\mu}{4\gamma^2}O_K = R$, and thus $\frac{\mu}{4\gamma^2} \in O_K$. Hence $\frac{\sqrt{\mu}}{2\gamma}$ is an algebraic integer in L. Thus we can choose $\alpha = 0$.

Cases D1, D9, D15, D17, D22, D24. In these cases $T = P_1$. From Table D of [6] (or [5]) we see that P_2 divides μ to an even exponent so that $P_2 \nmid R$. Further

$$\frac{\mu}{\gamma^2}O_K = \frac{1}{\gamma^2}RS^2 = RP_1^2,$$

so that $\mu/\gamma^2 \in O_K$. If $\mu/\gamma^2 = x + y\sqrt{c}$, where x and y are integers, then x and y are of opposite parity as $2 \nmid \mu/\gamma^2$. Thus $N(\mu/\gamma^2) = x^2 - cy^2$ is odd, contradicting $N(\mu/\gamma^2)O_K = 4RR'$. Hence $\mu/\gamma^2 = \frac{1}{2}(x + y\sqrt{c})$, where x and y are odd integers. We set $\mu' = 4\mu/\gamma^2 = 2x + 2y\sqrt{c}$. Clearly $P_2^2 \| \mu'$. From the values of m_1 in Table D of [6] (or [5]), we deduce that

$$P_1^4 \| \mu', \quad \text{in cases D1, D17, D22,}$$

$$P_1^5 \| \mu', \quad \text{in cases D9, D15, D24.}$$

Hence, for μ in cases D1, D9, D15, D17, D22, D24, the corresponding cases for μ' are D17, D24, D24, D17, D17, D24, and, from Table D′ of [6] (or Table (viii) of [5]), we may choose $\alpha = \frac{1+\sqrt{c}}{4}$ as

$$\frac{1+\sqrt{c}}{4} + \frac{1}{2\gamma}\sqrt{\mu} = \frac{1}{4}\left(1 + \sqrt{c} + \sqrt{\mu'}\right) \in O_L$$

by cases D17 and D24 of Table D′ of [6] (or Table (viii) of [5]).

Cases D2, D7, D14, D18, D21, D25. These cases can be treated in exactly the same way as the preceding cases with the roles of P_1 and P_2 interchanged.

Cases A1, A5, B2, B5, C2†, D3, D16, D20. In these cases $T = O_K$. From Tables A-D of [6] (or [5]) we see that R and $2O_K$ are relatively prime.

Further

$$\frac{\mu}{\gamma^2}O_K = \frac{1}{\gamma^2}RS^2 = R,$$

so that $\mu/\gamma^2 \in O_K$. We claim that $\mu/\gamma^2 = x + y\sqrt{c}$, where x and y are integers. This is automatically true for the cases A1, A5, B2, B5 and C2†. For

D3, D16, D20 assume that $\mu/\gamma^2 = \frac{1}{2}(x + y\sqrt{c})$, where x and y are odd integers. Set $a' + b'\sqrt{c} = 4\mu/\gamma^2$, so that a', b' must fall into one of the cases in Table D of [6] (or [5]). However this is not the case as the corresponding values of r, m_1, m_2, w_1, w_2 are 4, 2, 2, 0, 0 respectively. Set $\mu' = \mu/\gamma^2 = x + y\sqrt{c}$, where x and y are integers. As $\mu' O_K = R$ the corresponding value of r for μ' is 0, and, as $d(L/K) = R$, we see that for μ in cases A1, A5, B2, B5, C2†, D3, D16, D20 the corresponding cases for μ' are cases A1, A1, B2, B2, C2, D3, D3, D4. Thus, by Tables A$'$-D$'$ of [6] (or Table (viii) of [5]), we may choose $\alpha = \frac{1}{2}$ as

$$\frac{1}{2} + \frac{1}{2\gamma}\sqrt{\mu} = \frac{1}{2}\left(1 + \sqrt{\mu'}\right) \in O_L$$

except in the cases A1**, A5** when we must choose $\alpha = \frac{1+\sqrt{c}}{2}$ and in cases B2**, B5** when we choose $\alpha = \frac{1}{2}\sqrt{c}$.

Cases A2, A6. In these cases $T = P$. From Table A of [6] (or [5]) we see that P divides μ to an even power so that $P \nmid R$. Further

$$\frac{\mu}{\gamma^2} O_K = \frac{1}{\gamma^2} R S^2 = R P^2,$$

so that $\mu/\gamma^2 \in O_K$. Set $\mu' = \mu/\gamma^2$. Then μ' satisfies the conditions of case A6. Thus we may choose $\alpha = \frac{1}{2}\sqrt{c}$ as

$$\frac{1}{2}\sqrt{c} + \frac{1}{2\gamma}\sqrt{\mu} = \frac{\sqrt{c} + \sqrt{\mu'}}{2} \in O_L$$

in case A6.

Cases B3, B6. In these cases $T = P$. From Table B of [6] (or [5]) we see that P divides μ to an even exponent so that $P \nmid R$. Further

$$\frac{\mu}{\gamma^2} O_K = \frac{1}{\gamma^2} R S^2 = R P^2,$$

so that $\mu/\gamma^2 \in O_K$. Set $\mu' = \mu/\gamma^2$. Then μ' satisfies the conditions of case B6. Thus we may choose $\alpha = \frac{1+\sqrt{c}}{2}$ as

$$\frac{1 + \sqrt{c}}{2} + \frac{1}{2\gamma}\sqrt{\mu} = \frac{1 + \sqrt{c} + \sqrt{\mu'}}{2} \in O_L$$

in case B6.

Cases C2‡, C7. In these cases $T = O_K$. From Table C of [6] (or [5]) we see that P divides μ to an even exponent so that $P \nmid R$. Further

$$\frac{\mu}{\gamma^2} O_K = \frac{1}{\gamma^2} RS^2 = R,$$

so that $\mu/\gamma^2 \in O_K$. We now show that in case C7 we have $\mu/\gamma^2 = \frac{1}{2}(x + y\sqrt{c})$, where x and y are odd integers. From [6 (or 5), Table C] we see that $2^2 \| \mu$ so that $2 \| S = \langle \gamma \rangle$. Set $\gamma = 2\beta$, where $\beta \in O_K$. Then, as $\mu/\gamma^2 \in O_K$ and $\mu/\beta^2 = 4\mu/\gamma^2$, we have $\mu/\beta^2 = x' + y'\sqrt{c}$, where x' and y' are integers. The values of r and w are still 4 and 0 respectively for μ/β^2 in place of μ. Thus μ/β^2 falls under case C7 and so $x' \equiv y' \equiv 2 \pmod 4$. Hence $\mu/\gamma^2 = \mu/4\beta^2 = \frac{x'+y'\sqrt{c}}{4}$ is of the asserted form. In both cases C2‡ and C7 we have $\mu' = 4\mu/\gamma^2 = 2a' + 2b'\sqrt{c}$, where $a' \equiv b' \equiv 1 \pmod 2$, and μ' falls into case C7. Thus we may choose $\alpha = \frac{b'+\sqrt{c}}{4}$ as

$$\frac{b' + \sqrt{c}}{4} + \frac{1}{2\gamma}\sqrt{\mu} = \frac{b' + \sqrt{c} + \sqrt{\mu'}}{4} \in O_L$$

in case C7. □

REMARK. We remark that in case C2 both the possibilities $a' \equiv b' \equiv 0 \pmod 2$ and $a' \equiv b' \equiv 1 \pmod 2$ occur, where $\mu/\gamma^2 = (a' + b'\sqrt{c})/2$.

If we choose $a = -17$, $b = 18$, $c = 5$ then we can take $\gamma = \frac{1}{2}(-1 + 3\sqrt{5})$ (see Example 2 below) and $\mu/\gamma^2 = \frac{-17+18\sqrt{5}}{\left(\frac{1}{2}\left(-1+3\sqrt{5}\right)\right)^2} = \frac{-1+3\sqrt{5}}{2}$ so $a' = -1$, $b' = 3$.

On the other hand if we choose $a = -1$, $b = 2$, $c = 5$ then

$$\langle \mu \rangle = \left\langle -1 + 2\sqrt{5} \right\rangle = RS^2$$

gives

$$R = \left\langle -1 + 2\sqrt{5} \right\rangle, \quad S = \langle 1 \rangle.$$

By Theorem 1 $T = \langle 1 \rangle$ so we can take $\gamma = 1$. Thus

$$\mu/\gamma^2 = -1 + 2\sqrt{5} \quad \text{so} \quad a' = -2, b' = 4.$$

We conclude with two examples.

EXAMPLE 1. We consider $L = Q\left(\sqrt{10+\sqrt{10}}\right)$. This is Example 2 of [12]. The quadratic subfield of L is $K = Q\left(\sqrt{10}\right)$. Here $a = 10, b = 1, c = 10$ so we are in case A4. Moreover $\langle \mu \rangle = \left\langle 10+\sqrt{10}\right\rangle = RS^2$, where $R = \left\langle \sqrt{10}\right\rangle$ and $S = \left\langle 3, 1+\sqrt{10}\right\rangle$. By Theorem 1 we have $d(L/K) = 4R$ so $T = \langle 2 \rangle$. As $\left\langle 3, 1+\sqrt{10}\right\rangle$ is not a principal ideal, $S \neq T\langle \gamma \rangle$ for any $\gamma(\neq 0) \in K$. Hence, by Theorem 2, L does not have a RIB over K.

EXAMPLE 2. We consider $L = Q\left(\sqrt{-17+18\sqrt{5}}\right)$. The quadratic subfield of L is $K = Q(\sqrt{5})$. Here $a = -17$, $b = 18$, $c = 5$ so we are in case C2. O_K is a PID so, by Theorem 2, L has a RIB over K. As $\mu = -17 + 18\sqrt{5} = \left(\frac{-1+3\sqrt{5}}{2}\right)^3$ we can take $R = S = \left\langle \frac{-1+3\sqrt{5}}{2} \right\rangle$. By Theorem 1 we have $d(L/K) = R$ so $T = \langle 1 \rangle$. Hence we can take $\gamma = \frac{1}{2}\left(-1+3\sqrt{5}\right)$ and a RIB for L over K is $\{1, \kappa\}$, where

$$\kappa = \frac{3\gamma + \gamma\sqrt{5} + 2\sqrt{\mu}}{4\gamma} = \frac{3+\sqrt{5}}{4} + \frac{1}{2}\sqrt{\frac{-1+3\sqrt{5}}{2}}.$$

References

[1] E. Artin, Questions de base minimale dans la théorie des nombres algébriques, *Alg. Th. des Nombres, Coll. Internat. CNRS,* **24** (1950), 19–20.

[2] R. H. Bird and C. J. Parry, Integral bases for bicyclic biquadratic fields over quadratic subfields, *Pacific J. Math.,* **66** (1976), 29–36.

[3] H. M. Edgar, A number field without any integral basis, *Math. Mag.,* **52** (1979), 248–251.

[4] T. Funakura, On integral bases of pure quartic fields, *Math. J. Okayama Univ.,* **26** (1984), 27–41.

[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, 44 pp.

[6] 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.

[7] J. A. Hymo and C. J. Parry, On relative integral bases for cyclic quartic fields, *J. Number Theory,* **34** (1990), 189–197.

[8] J. A. Hymo and C. J. Parry, On relative integral bases for pure quartic fields, *Indian J. Pure Appl. Math.,* **23** (1992), 359–376.

[9] R. MacKenzie and J. Scheuneman, A number field without a relative integral basis, *Amer. Math. Monthly,* **78** (1971), 882–883.

[10] M. Pohst, Berechnung unabhängiger Einheiten und Klassenzahlen in total reellen biquadratischen Zahlkörpern, *Computing,* **14** (1975), 67–78.

[11] B. Schmal, *Existenz von relativen ganzheitsbasen bei quartischen, insbesondere biquadratischen Erweiterungskörpern über quadratischen Grundkörpern* (Diplomarbeit), Universität des Saarlandes (1984).

[12] 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.
[13] Zhang Xianke, Cyclic quartic fields and genus theory of their subfields, *J. Number Theory*, **18** (1984), 350–355.

(Received May 24, 1994; revised September 7, 1994)

DEPARTMENT OF MATHEMATICS
OKANAGAN UNIVERSITY COLLEGE
KELOWNA, B.C. V1V 1V7
CANADA

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