ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 20, Number 1, Winter 1990

THE INTEGERS OF A CYCLIC QUARTIC FIELD

R.H. HUDSON[(1)] AND K.S. WILLIAMS[(2)]

ABSTRACT. A simple explicit integral basis is given for a cyclic quartic extension of the rationals.

In [**3**] the authors show that a cyclic quartic extension K of the rational number field Q can be expressed uniquely in the form

$$K = Q\left(\sqrt{A(D+B\sqrt{D})}\right), \tag{1}$$

where A, B, C, D are integers such that

$$A \text{ is squarefree and odd,} \tag{2}$$

$$D = B^2 + C^2 \text{ is squarefree,} \qquad B > 0, C > 0, \tag{3}$$

$$GCD(A, D) = 1. \tag{4}$$

This representation of K is simpler than those given in [**2**] and [**4**]. The field K is totally real if $A > 0$ and totally imaginary if $A < 0$. It is also shown in [**3**] that the discriminant $d(K)$ of K is given by

$$d(K) = \begin{cases} 2^8A^2D^3, & \textit{if } D \equiv 0 \pmod 2, \\ 2^6A^2D^3, & \textit{if } D \equiv 1 \pmod 2,\ B \equiv 1 \pmod 2, \\ 2^4A^2D^3, & \textit{if } D \equiv 1 \pmod 2,\ B \equiv 0 \pmod 2, \\ & \quad A+B \equiv 3 \pmod 4, \\ A^2D^3, & \textit{if } D \equiv 1 \pmod 2,\ B \equiv 0 \pmod 2, \\ & \quad A+B \equiv 1 \pmod 4. \end{cases} \tag{5}$$

Key words and phrases: Cyclic quartic extension, integral 1 basis.
Subject Classification Numbers: 12A30, 12A50.
(1) Research supported in part by a research grant from the University of South Carolina.
(2) Research supported by Natural Sciences and Engineering Research Council of Canada grant A-7233.
Received by the editors on September 16, 1986 and in revised form on February 18, 1987.

These results enable us to give a simple explicit integral basis for K. We prove the following theorem.

THEOREM. *Let $K = Q(\sqrt{A(D+B\sqrt{D})})$ be a cyclic quartic extension of Q where A, B, C, D are integers satisfying* (2), (3) *and* (4). *Set*

$$\alpha = \sqrt{A(D+B\sqrt{D})}, \qquad \beta = \sqrt{A(D-B\sqrt{D})}. \tag{6}$$

Then an integral basis for K is given as follows:

(i) $\{1, \sqrt{D}, \alpha, \beta\}$, *if* $D \equiv 0 \pmod 2$;

(ii) $\{1, \frac{1}{2}(1+\sqrt{D}), \alpha, \beta\}$, *if* $D \equiv B \equiv 1 \pmod 2$;

(iii) $\{1, \frac{1}{2}(1+\sqrt{D}), \frac{1}{2}(\alpha+\beta), \frac{1}{2}(\alpha-\beta)\}$, *if* $D \equiv 1 \pmod 2, B \equiv 0 \pmod 2, A+B \equiv 3 \pmod 4$;

(iv) $\{1, \frac{1}{2}(1+\sqrt{D}), \frac{1}{4}(1+\sqrt{D}+\alpha+\beta), \frac{1}{4}(1-\sqrt{D}+\alpha-\beta)\}$, *if* $D \equiv 1 \pmod 2, B \equiv 0 \pmod 2, A+B \equiv 1 \pmod 4, A \equiv C \pmod 4$;

(v) $\{1, \frac{1}{2}(1+\sqrt{D}), \frac{1}{4}(1+\sqrt{D}+\alpha-\beta), \frac{1}{4}(1-\sqrt{D}+\alpha+\beta)\}$, *if* $D \equiv 1 \pmod 2, B \equiv 0 \pmod 2, A+B \equiv 1 \pmod 4, A \equiv -C \pmod 4$.

This theorem corrects and simplifies the integral basis for K given by Albert [**1**] in 1930. As observed by the authors and Xianke [**4**], independently, Albert's work contains a number of errors and so cannot be relied upon.

PROOF OF THE THEOREM. We begin by showing that all the elements of K listed in (i)–(v) are integers of K. This is clear except in the case of the following:

(a) $\frac{1}{2}(\alpha+\epsilon\beta)$, if $D \equiv 1 \pmod 2, B \equiv 0 \pmod 2, A+B \equiv 3 \pmod 4$;

(b) $\frac{1}{4}(1+\epsilon\sqrt{D}+\alpha+\epsilon\beta)$, if $D \equiv 1 \pmod 2, B \equiv 0 \pmod 2, A+B \equiv 1 \pmod 4, A \equiv C \pmod 4$;

(c) $\frac{1}{4}(1+\epsilon\sqrt{D}+\alpha-\epsilon\beta)$, if $D \equiv 1 \pmod 2, B \equiv 0 \pmod 2, A+B \equiv 1 \pmod 4, A \equiv -C \pmod 4$;

where $\epsilon = \pm 1$. Let tr (resp. N) denote the trace (resp. norm) from K to $Q(\sqrt{D})$. We shall show that $\mathrm{tr}(\gamma)$ and $N(\gamma)$ are integral in $Q(\sqrt{D})$ for each element $\gamma \in K$ listed in (a),(b) and (c), proving that each γ is an integer of K. Let $\tau \in \mathrm{Gal}(K/Q(\sqrt{D}))$ so that

$$(7) \qquad \mathrm{tr}(\gamma) = \gamma + \tau(\gamma), \qquad N(\gamma) = \gamma\tau(\gamma).$$

We note that

$$(8) \qquad \tau(\sqrt{D}) = \sqrt{D}, \qquad \tau(\alpha) = -\alpha, \qquad \tau(\beta) = -\beta,$$

and

$$(9) \qquad \alpha^2 + \beta^2 = 2AD, \qquad \alpha\beta = AC\sqrt{D}.$$

Case (a). In this case we have

$$\mathrm{tr}\Big(\frac{1}{2}(\alpha + \varepsilon\beta)\Big) = 0$$

and

$$N\Big(\frac{1}{2}(\alpha + \epsilon\beta)\Big) = -\frac{1}{4}(\alpha + \epsilon\beta)^2 = -\frac{AD}{2} - \frac{\epsilon}{2}AC\sqrt{D}.$$

The latter is clearly an integer of $Q(\sqrt{D})$ as A, C, D are all odd.

Case (b). In this case we have

$$\mathrm{tr}\Big(\frac{1}{4}(1 + \epsilon\sqrt{D} + \alpha + \epsilon\beta\Big) = \frac{1}{2} + \frac{\epsilon}{2}\sqrt{D},$$

which is clearly an integer of $Q(\sqrt{D})$, and

$$\begin{aligned} N\Big(\frac{1}{4}(1 + \epsilon\sqrt{D} + \alpha + \epsilon\beta)\Big) &= \frac{1}{16}\Big((1 + \epsilon\sqrt{D})^2 - (\alpha + \epsilon\beta)^2\Big) \\ &= \frac{1}{16}\Big((1 + D + 2\epsilon\sqrt{D}) \\ &\qquad - (2AD + 2\epsilon AC\sqrt{D})\Big) \\ &= \frac{1}{2}(X + Y\sqrt{D}), \end{aligned}$$

where

$$X = (1 + D - 2AD)/8, \qquad Y = \epsilon(1 - AC)/4.$$

As

$$A \equiv B + 1 \pmod 4, \qquad D \equiv 2B + 1 \pmod 8,$$

we have

$$1 + D - 2AD \equiv 1 + 2B + 1 - 2(B+1) \equiv 0 \pmod 8$$

so that X is a rational integer. Further, as $AC \equiv 1 \pmod 4), Y$ is a rational integer. Lastly X and Y are of the same parity as

$$\begin{aligned}
8(X + \epsilon Y) &= 3 + D - 2AC - 2AD \\
&= 3 + B^2 + C^2 - 2AC - 2A(B^2 + C^2) \\
&= 3 + B^2 + (C - A)^2 - A^2 - 2AB^2 - 2AC^2 \\
&\equiv 3 + B^2 - A^2 - 2B^2 - 2A \pmod{16} \\
&\equiv 4 - B^2 - (A+1)^2 \pmod{16} \\
&\equiv 4 - B^2 - (B+2)^2 \pmod{16} \\
&\equiv -4B - 2B^2 \pmod{16} \\
&\equiv 0 \pmod{16}.
\end{aligned}$$

This proves that $\frac{1}{2}(X + Y\sqrt{D})$ is an integer of $Q(\sqrt{D})$.

Case (c). This case can be treated similarly to case (b).

Finally we show that the discriminant of each of the sets (i)–(v) is equal to the field discriminant $d(K)$ given in (5). We just give the proof in case (v), as the details are similar in the other cases. The Galois group of the extension K/Q is a cyclic group of order 4 generated by the automorphism θ defined by

$$\theta(\alpha) = \beta.$$

We have

$$\theta(\sqrt{D}) = -\sqrt{D}, \qquad \theta(\beta) = -\alpha.$$

The conjugates of $\gamma = \frac{1}{4}(1 + \sqrt{D} + \alpha - \beta)$ over Q are

$$\gamma, \quad \theta(\gamma) = \frac{1}{4}(1 - \sqrt{D} + \alpha + \beta),$$
$$\theta^2(\gamma) = \frac{1}{4}(1 + \sqrt{D} - \alpha + \beta), \quad \theta^3(\gamma) = \frac{1}{4}(1 - \sqrt{D} - \alpha - \beta),$$

and

$$\begin{aligned}
&\begin{vmatrix} 1 & \frac{1}{2}(1+\sqrt{D}) & \gamma & \theta(\gamma) \\ 1 & \frac{1}{2}(1-\sqrt{D}) & \theta(\gamma) & \theta^2(\gamma) \\ 1 & \frac{1}{2}(1+\sqrt{D}) & \theta^2(\gamma) & \theta^3(\gamma) \\ 1 & \frac{1}{2}(1-\sqrt{D}) & \theta^3(\gamma) & \gamma \end{vmatrix} \\
&\qquad = \frac{1}{2}\sqrt{D}\begin{vmatrix} 1 & 1 & \gamma & \theta(\gamma) \\ 1 & -1 & \theta(\gamma) & \theta^2(\gamma) \\ 1 & 1 & \theta^2(\gamma) & \theta^3(\gamma) \\ 1 & -1 & \theta^3(\gamma) & \gamma \end{vmatrix} \\
&\qquad = \frac{1}{2}\sqrt{D}\begin{vmatrix} 1 & 1 & \gamma & \theta(\gamma) \\ 0 & -2 & \theta(\gamma)-\gamma & \theta^2(\gamma)-\theta(\gamma) \\ 0 & 0 & \theta^2(\gamma)-\gamma & \theta^3(\gamma)-\theta(\gamma) \\ 0 & 0 & \theta^3(\gamma)-\theta\gamma & \gamma-\theta^2(\gamma) \end{vmatrix} \\
&\qquad = -\sqrt{D}\begin{vmatrix} \theta^2(\gamma)-\gamma & \theta^3(\gamma)-\theta(\gamma) \\ \theta^3(\gamma)-\theta(\gamma) & \gamma-\theta^2(\gamma) \end{vmatrix} \\
&\qquad = \sqrt{D}((\theta^2(\gamma)-\gamma)^2+(\theta^3(\gamma)-\theta(\gamma))^2) \\
&\qquad = \sqrt{D}\Big(\Big(\frac{\alpha-\beta}{2}\Big)^2+\Big(\frac{\alpha+\beta}{2}\Big)^2\Big) \\
&\qquad = \frac{\sqrt{D}}{2}(\alpha^2+\beta^2) \\
&\qquad = AD^{\frac{3}{2}},
\end{aligned}$$

so that, by (5),

$$\operatorname{discrim}\{1, \frac{1}{2}(1+\sqrt{D}), \gamma, \theta(\gamma)\} = (AD^{3/2})^2 = A^2D^3 = d(K).$$

Hence $\{1, \frac{1}{2}(1+\sqrt{D}), \gamma, \theta(\gamma)\}$ is an integral basis for K as asserted.

This completes the proof of the theorem. □

REFERENCES

1. A.A. Albert, *The Integers of Normal Quartic Fields*, Annals Math. **31** (1930), 381–418.

2. H. Edgar and B. Peterson, *Some Contributions to the Theory of Cyclic Quartic Extensions of the Rationals*, J. Number Theory **12** (1980), 77–83.

3. K. Hardy, R.H. Hudson, D. Richman, K.S. Williams and N.M. Holtz, *Calculation of Class Numbers of Imaginary Cyclic Quartic Fields*, Carleton-Ottawa Mathematical Lecture Note Series Number **7**, July 1986, 201 pp.

4. Z. Xianke, *Cyclic Quartic Fields and Genus Theory of their Subfields*, J. Number Theory **18** (1984), 350–355.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SOUTH CAROLINA, COLUMBIA, SOUTH CAROLINA, U.S.A. 29208

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