Far East J. Math. Sci. (FJMS) **21**(2) (2006), 235-240

CYCLIC QUARTIC FIELDS WITH A UNIQUE NORMAL INTEGRAL BASIS

BLAIR K. SPEARMAN and KENNETH S. WILLIAMS

(Received February 26, 2006)

Submitted by K. K. Azad

Abstract

Cyclic quartic fields possessing a unique normal integral basis are characterized and the normal integral basis is given explicitly.

1. Introduction

Let K be an abelian extension of finite degree over the rational field $\mathbb{Q}$. By the Kronecker-Weber theorem [8, Theorem 6.5, p. 289], K is contained in a cyclotomic field $\mathbb{Q}(\zeta_m)$ $(\zeta_m = e^{2\pi i/m})$ for some positive integer m. The least positive integer f with the property $K \subseteq \mathbb{Q}(\zeta_f)$ is called the *conductor* of K and is denoted by $f(K)$ [8, p. 421]. Moreover [8, Proposition 8.1, p. 421]

$$K \subseteq \mathbb{Q}(\zeta_m) \text{ if and only if } f(K) \mid m. \tag{1.1}$$

It is known [8, p. 175] that an abelian field K has a normal integral basis if and only if it is contained in a cyclotomic field $\mathbb{Q}(\zeta_m)$ with m

2000 Mathematics Subject Classification: 11R16, 11R29.

Keywords and phrases: cyclic quartic field, normal integral basis, conductor.

Research of both authors is supported by grants from the Natural Sciences and Engineering Research Council of Canada.

squarefree, that is, by (1.1) if and only if $f(K)$ is squarefree. If K is abelian with squarefree conductor $f(K)$, then the normal integral basis of K is unique (up to permutation and change of sign) precisely when either $\text{Gal}(K/\mathbb{Q})$ is the direct product of cyclic groups of order 4 and/or order 2, or $\text{Gal}(K/\mathbb{Q})$ is the direct product of cyclic groups of order 3 and/or order 2, see Thompson [10, Theorem 1, p. 1119] or Higman [4, Theorem 6].

In this note we determine explicitly a normal integral basis for K in radical form, when K is a cyclic quartic field with squarefree conductor. To do this we make use of the representation of K given by Hardy et al. [3, Theorem 1, p. 1], the formula for the conductor of K given in [3, Theorem 5, p. 34] or [9], and the integral basis for K given by Hudson and Williams [6, Theorem, p. 146]. From a theoretical point of view we can give the normal integral basis as the conjugates of $Tr_{\mathbb{Q}(\zeta_f)/K}(\zeta_{f(K)})$ [8, Proposition 4.15(i), p. 174]. However this is not a practical way of obtaining a normal integral basis as the degree of $\mathbb{Q}(\zeta_f)/\mathbb{Q}$ can be large. This was observed by Acciaro and Fieker [1] in the case of cyclic fields of prime degree.

It is shown in [3] that a cyclic quartic extension $K/\mathbb{Q}$ can be expressed uniquely in the form

$$K = \mathbb{Q}(\sqrt{A(D + B\sqrt{D})}), \tag{1.2}$$

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

$$A \text{ is squarefree and odd}, \tag{1.3}$$

$$D = B^2 + C^2 \text{ is squarefree}, \ B > 0, \ C > 0, \tag{1.4}$$

$$GCD(A, \ D) = 1. \tag{1.5}$$

An algorithm to express K in this form has been given by Huard et al. [5]. The conductor of $f(K)$ of K is given by

$$f(K) = 2^l |A| D, \tag{1.6}$$

where

$$l = \begin{cases} 3, & \text{if } D \equiv 2 \pmod 4 \text{ or } D \equiv 1 \pmod 4,\ B \equiv 1 \pmod 2, \\ 2, & \text{if } D \equiv 1 \pmod 4,\ B \equiv 0 \pmod 2,\ A + B \equiv 3 \pmod 4, \\ 0, & \text{if } D \equiv 1 \pmod 4,\ B \equiv 0 \pmod 2,\ A + B \equiv 1 \pmod 4, \end{cases} \tag{1.7}$$

see [3], [9]. Thus

$$\begin{aligned} &f(K) \text{ is squarefree} \Leftrightarrow l = 0 \\ &\Leftrightarrow D \equiv 1 \pmod 4,\ B \equiv 0 \pmod 2,\ A + B \equiv 1 \pmod 4. \end{aligned} \tag{1.8}$$

Now let K be a cyclic quartic extension of $\mathbb{Q}$ with a squarefree conductor $f(K)$ so that K has a unique normal integral basis. Then K can be expressed uniquely in the form (1.2), where A, B, C and D are integers satisfying (1.3)-(1.5) and

$$D \equiv 1 \pmod 4,\ B \equiv 0 \pmod 2,\ C \equiv 1 \pmod 2,\ A + B \equiv 1 \pmod 4. \tag{1.9}$$

We set

$$\alpha = \sqrt{A(D + B\sqrt{D})}, \quad \beta = \sqrt{A(D - B\sqrt{D})}, \tag{1.10}$$

and define $\varepsilon = \pm 1$ by

$$A \equiv \varepsilon C \pmod 4. \tag{1.11}$$

An integral basis for K is

$$\left\{1, \frac{1}{2}(1 + \sqrt{D}), \frac{1}{4}(1 + \sqrt{D} + \alpha + \varepsilon\beta), \frac{1}{4}(1 - \sqrt{D} + \alpha - \varepsilon\beta)\right\}, \tag{1.12}$$

see [6, Theorem, p. 146]. We prove

Theorem. *Let K be a cyclic quartic field with a squarefree conductor. Then its unique (up to permutation and change of sign) normal integral basis consists of the following four elements*

$$\frac{1}{4}(1 + \sqrt{D} + \alpha + \varepsilon\beta), \frac{1}{4}(1 - \sqrt{D} - \alpha + \varepsilon\beta), \frac{1}{4}(1 + \sqrt{D} - \alpha - \varepsilon\beta)$$

and

$$\frac{1}{4}(1 - \sqrt{D} + \alpha - \varepsilon\beta),$$

where α and β are defined in (1.10) *and ε in* (1.11).

2. Proof of Theorem

The first element specified in the theorem, namely $\frac{1}{4}(1+\sqrt{D}+\alpha+\varepsilon\beta)$, is the third element in the integral basis given in (1.12) and so is an integer of K. Using the automorphism of K given by

$$\alpha \to \beta, \quad \beta \to -\alpha, \quad \sqrt{D} \to -\sqrt{D},$$

we see that the other three elements given in the theorem are the conjugates of $\frac{1}{4}(1+\sqrt{D}+\alpha+\varepsilon\beta)$ and so are also integers of K. Since the first and fourth elements in the theorem are members of (1.12), the sum of all four elements is 1, and the sum of the first and third elements is $\frac{1}{2}(1+\sqrt{D})$, it is clear that the four elements of the theorem comprise a normal integral basis for K.

3. Example

Let $K = \mathbb{Q}(\sqrt{-(13+2\sqrt{13})})$. Here

$$A = -1, \quad B = 2, \quad C = 3, \quad D = 13, \quad \varepsilon = 1,$$

$$\alpha = \sqrt{-13-2\sqrt{13}}, \quad \beta = \sqrt{-13+2\sqrt{13}},$$

so by the theorem a normal integral basis for K consists of the four elements

$$\frac{1}{4}(1+\sqrt{13}+\sqrt{-13-2\sqrt{13}}+\sqrt{-13+2\sqrt{13}}),$$

$$\frac{1}{4}(1-\sqrt{13}-\sqrt{-13-2\sqrt{13}}+\sqrt{-13+2\sqrt{13}}),$$

$$\frac{1}{4}(1+\sqrt{13}-\sqrt{-13-2\sqrt{13}}-\sqrt{-13+2\sqrt{13}}),$$

$$\frac{1}{4}(1-\sqrt{13}+\sqrt{-13-2\sqrt{13}}-\sqrt{-13+2\sqrt{13}}).$$

We conclude by determining the unique normal integral basis of K by means of a trace calculation. By (1.6) and (1.7) the conductor of K is $f(K) = 13$. Let $\omega = \zeta_{13} = e^{2\pi i/13}$. We have $[\mathbb{Q}(\omega) : \mathbb{Q}] = \phi(13) = 12$. $[K : \mathbb{Q}] = 4$ and $[\mathbb{Q}(\omega) : K] = 3$. We determine

$$Tr_{\mathbb{Q}(\omega)/K}(\omega) = \omega + \omega^3 + \omega^9$$

and its conjugates. From the evaluation of the quartic Gauss sum given by Matthews [7], see [2, Theorem 4.2.4, p. 163] (with $p = 13$, $a = 3$, $|b| = 2$, $C = 1$), we have

$$1 + 4(\omega + \omega^3 + \omega^9) = \sum_{n=0}^{12} \omega^{n^4} = \sqrt{13} + i\sqrt{26 - 6\sqrt{13}}.$$

Hence

$$\begin{aligned}\omega + \omega^3 + \omega^9 &= \frac{1}{4}(-1 + \sqrt{13} + \sqrt{-26 + 6\sqrt{13}}) \\ &= \frac{1}{4}(-1 + \sqrt{13} + \sqrt{-13 - 2\sqrt{13}} - \sqrt{-13 + 2\sqrt{13}}).\end{aligned}$$

Similarly we have

$$\begin{aligned}\omega^2 + \omega^5 + \omega^6 &= \frac{1}{4}(-1 - \sqrt{13} + \sqrt{-26 - 6\sqrt{13}}) \\ &= \frac{1}{4}(-1 - \sqrt{13} + \sqrt{-13 - 2\sqrt{13}} + \sqrt{-13 + 2\sqrt{13}}),\end{aligned}$$

$$\begin{aligned}\omega^4 + \omega^{10} + \omega^{12} &= \frac{1}{4}(-1 + \sqrt{13} - \sqrt{-26 + 6\sqrt{13}}) \\ &= \frac{1}{4}(-1 + \sqrt{13} - \sqrt{-13 - 2\sqrt{13}} + \sqrt{-13 + 2\sqrt{13}}),\end{aligned}$$

$$\begin{aligned}\omega^7 + \omega^8 + \omega^{11} &= \frac{1}{4}(-1 - \sqrt{13} - \sqrt{-26 - 6\sqrt{13}}) \\ &= \frac{1}{4}(-1 - \sqrt{13} - \sqrt{-13 - 2\sqrt{13}} - \sqrt{-13 + 2\sqrt{13}}).\end{aligned}$$

Thus the normal integral basis obtained from $Tr_{\mathbb{Q}(\omega)/K}(\omega)$ and its conjugates is (as it should be!) the same as the one determined above.

References

[1] V. Acciaro and C. Fieker, Finding normal integral bases of cyclic number fields of prime degree, J. Symbolic Comput. 30 (2000), 239-252.

[2] B. C. Berndt, R. J. Evans and K. S. Williams, Gauss and Jacobic Sums, Wiley-Interscience Publication, 1998.

[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, Vol. 7, July 1986, pp. 201.

[4] G. Higman, The units of group rings, Proc. London Math. Soc. (2) 46 (1940), 231-238.

[5] J. G. Huard, B. K. Spearman and K. S. Williams, Integral bases for quartic fields with quadratic subfields, Carleton University-University of Ottawa Centre for Research in Algebra and Number Theory Mathematical Research Series, Vol. 4, June 1991, pp. 44.

[6] R. H. Hudson and K. S. Williams, The integers of a cyclic quartic field, Rocky Mountain J. Math. 20 (1990), 145-150.

[7] C. R. Matthews, Gauss sums and elliptic functions. II, The quartic sum, Invent. Math. 54 (1979), 23-52.

[8] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, 2nd ed., Springer-Verlag, Berlin, Heidelberg, New York, 1990.

[9] B. K. Spearman and K. S. Williams, The conductor of a cyclic quartic field using Gauss sums, Czechoslovak Math. J. 47 (1997), 453-462.

[10] R. C. Thompson, Normal matrices and the normal basis in abelian number fields, Pacific J. Math. 12 (1962), 1115-1124.

Department of Mathematics and Statistics
University of British Columbia Okanagan
Kelowna, B. C. Canada V1V 1V7
e-mail: blair.spearman@ubc.bc.ca

School of Mathematics and Statistics
Carleton University
Ottawa, Ontario, Canada K1S 5B6
e-mail: williams@math.carleton.ca