Mathematical Journal of Okayama University

Volume 47, *Issue* 1 2005 *Article* 6

JANUARY 2005

Dihedral Quintic Fields with a Power Basis

Melissa J. Lavallee[*] Blair K. Spearman[†]
Kenneth S. Williams[‡] Qiduan Yang[**]

[*]Okanagan University College
[†]Okanagan University College
[‡]Carleton University
[**]Okanagan University College

Dihedral Quintic Fields with a Power Basis

Melissa J. Lavallee, Blair K. Spearman, Kenneth S. Williams, and Qiduan Yang

Abstract

It is shown that there exist infinitely many dihedral quintic fields with a power basis.

KEYWORDS: Dihedral quintic field, power basis, monogenic

Math. J. Okayama Univ. **47** (2005), 75–79

DIHEDRAL QUINTIC FIELDS WITH A POWER BASIS

Melissa J. LAVALLEE, Blair K. SPEARMAN, Kenneth S. WILLIAMS and Qiduan YANG

Abstract. It is shown that there exist infinitely many dihedral quintic fields with a power basis.

1. Introduction

Let K be an algebraic number field of degree n. Let O_K denote the ring of integers of K. The field K is said to possess a power basis if there exists an element $\theta \in O_K$ such that $O_K = \mathbb{Z} + \mathbb{Z}\theta + \cdots + \mathbb{Z}\theta^{n-1}$. A field having a power basis is called monogenic. Every quadratic field is monogenic. Dedekind [3] gave an example of a cubic field which is not monogenic. If K is a cyclic cubic field Gras [7], [8] and Archinard [1] have given necessary and sufficient conditions for K to be monogenic. Dummit and Kisilevsky [4] have shown that there exist infinitely many cyclic cubic fields which are monogenic. The same has been shown for non-cyclic cubic fields, pure quartic fields, bicyclic quartic fields, dihedral quartic fields by Spearman and Williams [15], Funakura [6], Nakahara [14], Huard, Spearman and Williams [10] respectively. It is not known if there are infinitely many monogenic cyclic quartic fields. If K is a cyclic field of prime degree $p \geq 5$ then Gras [9] has proved that K is monogenic if and only if K is the maximal real subfield of a cyclotomic field. In particular there is only one monogenic cyclic quintic field.

In this paper we exhibit infinitely many monogenic dihedral quintic fields. After giving some preliminary results in Section 2, we prove the following theorem in Section 3.

Theorem. *There are infinitely many integers b such that the quintic fields*

$$\mathbb{Q}(\theta), \quad \theta^5 - 2\theta^4 + (b+2)\theta^3 - (2b+1)\theta^2 + b\theta + 1 = 0,$$

are distinct, dihedral and monogenic.

2. A parametric family of quintics

For an integer b we define

$$F_b(x) := x^5 - 2x^4 + (b+2)x^3 - (2b+1)x^2 + bx + 1, \quad b \in \mathbb{Z}.$$

Mathematics Subject Classification. 11R21.

Key words and phrases. Dihedral quintic field, power basis, monogenic.

The second, third and fourth authors were supported by research grants from the Natural Sciences and Engineering Research Council of Canada.

As x^5+x^2+1 and $x^5+x^3+x^2+x+1$ are irreducible (mod 2), we have

Lemma 2.1. *$F_b(x)$ is irreducible for all $b \in \mathbb{Z}$.*

Using MAPLE we find

Lemma 2.2. *disc($F_b(x)$)* $= (4b^3+28b^2+24b+47)^2$.

We note that the cubic polynomial $4b^3+28b^2+24b+47$ is irreducible. The polynomial $F_b(x)$ is a special case of the polynomial $R_{a,b}(x)$ $(a,\, b \in \mathbb{Z})$ given by

$$R_{a,b}(x) = x^5+(a-3)x^4+(b-a+3)x^3+(a^2-a-1-2b)x^2+bx+a,$$

which was studied by Brumer [2] and Kondo [12]. Our polynomial $F_b(x)$ is obtained by setting $a=1$. It is shown in [11, pp. 44-46] that the $R_{a,b}$ form a generic dihedral family and it is known when the Galois group of $R_{a,b}$ is cyclic of order 5. From this work we have the following two lemmas.

Lemma 2.3.

$$\begin{aligned} Gal(F_b(x)) &= \mathbb{Z}_5, \text{ if } -(4b^3+28b^2+24b+47) \text{ is a square in } \mathbb{Z}. \\ Gal(F_b(x)) &= D_5, \text{ if } -(4b^3+28b^2+24b+47) \text{ is not a square in } \mathbb{Z}. \end{aligned}$$

Lemma 2.4. *If $-(4b^3+28b^2+24b+47) \neq$ square in $\mathbb{Z}$ then the quadratic subfield of the splitting field of $F_b(x)$ is*

$$\mathbb{Q}\left(\sqrt{-4b^3-28b^2-24b-47}\right).$$

3. Proof of theorem

By a theorem of Erdös [5] there are infinitely many integers b such that $4b^3+28b^2+24b+47$ is squarefree. For each such b let θ_b be a root of $F_b(x)=0$ and set $K_b=\mathbb{Q}(\theta_b)$. By Lemma 2.3 each K_b is a dihedral quintic field. The discriminant $d(K_b)$ of K_b is given by

$$d(K_b) = d_b^2 f_b^4,$$

where

$$d_b = \text{discriminant of the quadratic subfield of the splitting field of } F_b(x)$$

and

$$f_b = \text{conductor of } K_b \in \mathbb{N},$$

see [13, p. 836]. By Lemma 2.4 we have

$$d_b = -4b^3-28b^2-24b-47$$

so that

$$d(K_b) = (4b^3+28b^2+24b+47)^2 f_b^4.$$

By Lemma 2.2 we have

$$\mathrm{disc}(F_b(x)) = (4b^3 + 28b^2 + 24b + 47)^2.$$

As $d(K_b)$ divides $\mathrm{disc}(F_b(x))$, we deduce that $f_b = 1$ so that

$$d(K_b) = \mathrm{disc}(F_b(x)) = \pm(4b^3 + 28b^2 + 24b + 47)^2.$$

Hence K_b has a power basis (namely $\{1, \theta_b, \theta_b^2, \theta_b^3, \theta_b^4\}$) and so is monogenic. As

$$4k^3 + 28k^2 + 24k + 47 = \pm(4b^3 + 28b^2 + 24b + 47)$$

has at most six solutions for a given integer b, we can pick an infinite subsequence of the original sequence of b's for which $4b^3 + 28b^2 + 24b + 47$ is squarefree in such a way that all the fields K_b are distinct. □

If $4b^3 + 28b^2 + 24b + 47$ is squarefree the dihedral quintic field K_b has the power basis $\{1, \theta, \theta^2, \theta^3, \theta^4\}$, where we have written θ for θ_b. In addition K_b also has the power bases $\{1, \phi, \phi^2, \phi^3, \phi^4\}$ with

$$\phi_1 = b\theta - (b+1)\theta^2 + \theta^3 - \theta^4$$

and

$$\phi_2 = (2b+1)\theta - (b+2)\theta^2 + 2\theta^3 - \theta^4.$$

This follows as the minimal polynomials of ϕ_1 and ϕ_2 are by MAPLE

$$x^5 + x^4 + (b+3)x^3 + (b+4)x^2 + 3x + 1$$

and

$$\begin{gathered} x^5 - 4bx^4 + (6b^2 - 2b - 1)x^3 + (-4b^3 + 6b^2 + 4b + 2)x^2 \\ + (b^4 - 6b^3 - 5b^2 - 4b - 2)x + (2b^4 + 2b^3 + 2b^2 + 2b + 1) \end{gathered}$$

respectively, each of discriminant $(4b^3 + 28b^2 + 24b + 47)^2$.

When $b = 0$, we have the additional eight power bases $\{1, \phi, \phi^2, \phi^3, \phi^4\}$ given by

$$\begin{aligned} \phi_1 &= \theta^3 - \theta^4, \\ \phi_2 &= 2\theta - 2\theta^2 + 2\theta^3 - \theta^4, \\ \phi_3 &= \theta + \theta^3, \\ \phi_4 &= \theta - 2\theta^2 + \theta^3, \\ \phi_5 &= 6\theta - 7\theta^2 + 5\theta^3 - 2\theta^4, \\ \phi_6 &= \theta^2 - \theta^3, \\ \phi_7 &= \theta - \theta^2 + \theta^3, \\ \phi_8 &= \theta - \theta^2. \end{aligned}$$

We do not know if there are any more power bases when $b = 0$.

References

[1] G. Archinard, *Extensions cubiques cycliques de $\mathbb{Q}$ dont l'anneau des entiers est monogéne,* Enseignement Math. **20** (1974), 179-203.

[2] A. Brumer, preprint.

[3] R. Dedekind, *Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen,* Abh. Kgl. Ges. Wiss. Göttingen **23 (**1878), 1-23.

[4] D. S. Dummit and H. Kisilevsky, *Indices in cyclic cubic fields,* in "Number Theory and Algebra", Academic Press, 1977, 29-42.

[5] P. Erdös, *Arithmetic properties of polynomials,* J. London Math. Soc. **28** (1953), 416-425.

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

[7] M.-N. Gras, *Sur les corps cubiques cycliques dont l'anneau des entiers monogène,* Ann. Sci. Univ. Besançon **3,** No. 6, 26 pp, 1973.

[8] M.-N. Gras, *Lien entre le groupe des unités et la monogéneite des corps cubiques cycliques,* Ann. Sci. Univ. Besançon No. 1, 19 pp, 1975-76.

[9] M.-N. Gras, *Non monogénéité de l'anneau des entiers des extensions cycliques de $\mathbb{Q}$ de degré premier $l \geq 5$*, J. Number Theory **23** (1986), 347-353.

[10] 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.

[11] C. U. Jensen, A. Ledet and N. Yui, *Generic Polynomials, Constructive Aspects of the Inverse Galois Problem,* Mathematical Sciences Research Institute Publications, Cambridge University Press, 2002.

[12] T. Kondo, *Some examples of unramified extensions over quadratic fields*, Sci. Rep. Tokyo Woman's Christian Univ., No. 120-121 (1977), 1399-1410.

[13] D. C. Meyer, *Multiplicities of dihedral discriminants*, Math. Comp. **58** (1992), 831-847.

[14] T. Nakahara, *On the indices and integral bases of non-cyclic but abelian biquadratic fields,* Arch. Math. **41** (1983), 504-508.

[15] B. K. Spearman and K. S. Williams, *Cubic fields with a power basis,* Rocky Mountain J. Math. **31** (2001), 1103-1109.

Melissa J. Lavallee
Department of Mathematics and Statistics,
Okanagan University College,
Kelowna, B.C. Canada V1V 1V7

Blair K. Spearman
Department of Mathematics and Statistics,
Okanagan University College,
Kelowna, B.C. Canada V1V 1V7

e-mail address: BSpearman@ouc.bc.ca

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

Qiduan Yang
Department of Mathematics and Statistics,
Okanagan University College,
Kelowna, B.C. Canada V1V 1V7

(*Received September 24, 2004*)
(*Revised January 12, 2005*)