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

Copyright ©2005 by the authors. Mathematical Journal of Okayama University is produced by The Berkeley Electronic Press (bepress). http://escholarship.lib.okayama-u.ac.jp/mjou
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
DIHEDRAL QUINTIC FIELDS WITH A POWER BASIS

MELISSA J. LAVALLEE, BLAIR K. SPEARMAN, KENNETH S. WILLIAMS
AND QI DUAN 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

$$F_b(x) := x^5 - 2x^4 + (b + 2)x^3 - (2b + 1)x^2 + bx + 1, \quad b \in \mathbb{Z}.$$
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.** \(\text{disc}(F_b(x)) = (4b^3 + 28b^2 + 24b + 47)^2\).

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.**

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

**Lemma 2.4.** If \(- (4b^3 + 28b^2 + 24b + 47) \neq \text{square in } \mathbb{Z}\) 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 Erdős [5] there are infinitely many integers \(b\) such that \(4b^3 + 28b^2 + 24b + 47\) is squarefree. For each such \(b\) let \(\theta_b\) 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
\[ \text{disc}(F_b(x)) = (4b^3 + 28b^2 + 24b + 47)^2. \]
As \( d(K_b) \) divides \( \text{disc}(F_b(x)) \), we deduce that \( f_b = 1 \) so that
\[ d(K_b) = \text{disc}(F_b(x)) = \pm(4b^3 + 28b^2 + 24b + 47)^2. \]
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. \( \square \)

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 \( \theta \) for \( \theta_b \). 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 \( \phi_1 \) and \( \phi_2 \) are by MAPLE
\[ x^5 + x^4 + (b + 3)x^3 + (b + 4)x^2 + 3x + 1 \]
and
\[ x^5 - 4bx^4 + (6b^2 - 2b - 1)x^3 + (-4b^3 + 6b^2 + 4b + 2)x^2 \\
+ (b^4 - 6b^3 - 5b^2 - 4b - 2)x + (2b^4 + 2b^3 + 2b^2 + 2b + 1) \]
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
\[
\begin{align*}
\phi_1 &= \theta^3 - \theta^4, \\
\phi_2 &= 2\theta - 2\theta^2 + 2\theta^3 - \theta^4, \\
\phi_3 &= \theta + \theta^3, \\
\phi_4 &= \theta - 2\theta^2 + \theta^3, \\
\phi_5 &= 6\theta - 7\theta^2 + 5\theta^3 - 2\theta^4, \\
\phi_6 &= \theta^2 - \theta^3, \\
\phi_7 &= \theta - \theta^2 + \theta^3, \\
\phi_8 &= \theta - \theta^2.
\end{align*}
\]
We do not know if there are any more power bases when \( b = 0 \).

References

DIHEDRAL QUINTIC FIELDS

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)