International Electronic Journal of Algebra
Volume 9 (2011) 171-176

THE STRUCTURE OF THE UNITARY UNITS OF THE GROUP ALGEBRA $\mathbb{F}_{2^k}D_8$

Joe Gildea

Received: 23 July 2010; Revised: 13 September 2010
Communicated by A. Çiğdem Özcan

Abstract. The structure of the unitary unit group of the group algebra of the dihedral group of order 8 over any finite field of characteristic 2 is established.

Mathematics Subject Classification (2000): 16U60, 16S34, 20C05, 15A33
Keywords: group ring, group algebra, unitary unit group, dihedral group

1. Introduction

Let KG denote the group ring of the group G over the field K. The homomorphism $\varepsilon : KG \longrightarrow K$ given by $\varepsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g$ is called the augmentation mapping of KG. The normalized unit group of KG denoted by $V(KG)$ consists of all the invertible elements of RG of augmentation 1. For further details and background see Polcino Milies and Sehgal [10]. In [11], a basis for $V(\mathbb{F}_pG)$ is determined where $\mathbb{F}_p$ is the Galois field of p elements and G is an abelian p-group.

If G is a finite 2-group and F is a finite field of characteristic 2, then $V(FG)$ is a finite 2-group of order $|F|^{|G|-1}$. The structure of the unit group of the group algebra $\mathbb{F}_2D_8$ is established in [12] where D_8 is the dihedral group of order 8. In [5], the structure of $\mathcal{U}(\mathbb{F}_{2^k}D_8)$ is established.

The map $* : KG \longrightarrow KG$ defined by $\left(\sum_{g\in G} a_g g\right)^* = \sum_{g\in G} a_g g^{-1}$ is an antiautomorphism of of KG of order 2. An element v of $V(KG)$ satisfying $v^{-1} = v^*$ is called unitary. We denote by $V_*(KG)$ the subgroup of $V(KG)$ formed by the unitary elements of KG.

Let $char(K)$ be the characteristic of the field K. In [4], A.Bovdi and A. Szákacs construct a basis for $V_*(KG)$ where $char(K) > 2$. Also A. Bovdi and L. Erdei [1] determine the structure of $V_*(\mathbb{F}_2G)$ for all groups of order 8 and 16 where $\mathbb{F}_2$ is the Galois field of 2 elements. Additionally in [3], V. Bovdi and A.L. Rosa determine the order of $V_*(\mathbb{F}_{2^k}G)$ for special cases of G. Since D_8 is extraspecial, $V_*(\mathbb{F}_{2^k}D_8)$

is normal in $V(\mathbb{F}_{2^k}D_8)$ by Bovdi and Kovács [2]. In [6], the structure of $V_*(\mathbb{F}_{2^k}Q_8)$ is established where Q_8 ie the quaternion group of order 8.

Let $M_n(R)$ be the ring of $n \times n$ matrices over a ring R. Using an established isomorphism between RG and a subring of $M_n(R)$ and other techniques, we establish the structure of $V_*(\mathbb{F}_{2^k}D_8)$ to be ${C_2}^{5k} \rtimes {C_2}^k$.

2. Background

Definition 2.1. A *circulant matrix* over a ring R is a square $n \times n$ matrix, which takes the form

$$\mathrm{circ}(a_1, a_2, \ldots, a_n) = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_n \\ a_n & a_1 & a_2 & \ldots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \ldots & a_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & a_4 & \ldots & a_1 \end{pmatrix}$$

where $a_i \in R$.

Note that the $n \times n$ circulant matrices over a commutative ring R form a commutative ring and that inverses of circulant matrices are also circulant. For further details on circulant matrices see Davis [7].

If $G = \{g_1, \ldots, g_n\}$, then denote the matrix $M(G) = ({g_i}^{-1}g_j)$ where $i, j = 1, \ldots, n$. Similarly, if $w = \sum_{i=1}^{n} \alpha_{g_i} g_i \in RG$, then denote the matrix $M(RG, w) = (\alpha_{{g_i}^{-1}g_j})$, which is called the RG-matrix of w. The following theorem can be found in [9].

Theorem 2.2. *Given a listing of the elements of a group G of order n there is a bijective ring homomorphism between RG and the $n \times n$ G-matrices over R. This bijective ring homomorphism is given by $\sigma : w \mapsto M(RG, w)$.*

Example 2.3. *Let $D_{2n} = \langle x, y \,|\, x^n = 1, y^2 = 1, yx = x^{-1}y \rangle$ and $\kappa = \sum_{i=0}^{n-1} a_i x^i + \sum_{j=0}^{n-1} b_j x^j y \in \mathbb{F}_{p^k} D_{2n}$ where $a_i, b_j \in \mathbb{F}_{p^k}$ and p is a prime, then*

$$\sigma(\kappa) = \begin{pmatrix} A & B \\ B^T & A^T \end{pmatrix}$$

where $A = circ(a_0, a_1, \ldots, a_{n-1})$ and $B = circ(b_0, b_1, \ldots, b_{n-1})$.

It is important to note that if $\kappa = \sum_{i=0}^{3} a_i x^i + \sum_{j=0}^{3} b_j x^j y \in \mathbb{F}_{2^k} D_8$ where $a_i, b_j \in \mathbb{F}_{2^k}$, then $\sigma(\kappa^*) = (\sigma(\kappa))^T$.

The next result appears in [8].

Theorem 2.4. *Let $A = circ(a_1, a_2, \dots, a_{p^m})$, where $a_i \in \mathbb{F}_{p^k}$, p is a prime and $m \in \mathbb{N}_0$. Then*

$$A^{p^m} = \sum_{i=1}^{p^m} {a_i}^{p^m}.I_{p^m}.$$

The next result can be found in [3].

Theorem 2.5. *Let K be a finite field of characteristic 2. If $D_{2^{n+1}} = \langle a, b \,|\, a^{2^n} = 1,\, b^2 = 1,\, a^b = a^{-1}\rangle$ is the dihedral group of order 2^{n+1}, then*

$$|V_*(KD_{2^{n+1}})| = |K|^{3\cdot 2^{n-1}}.$$

3. The Structure of $V_*(\mathbb{F}_{2^k}D_8)$

Lemma 3.1. *Let N be the set of elements $V_*(\mathbb{F}_{2^k}D_8)$ of the form $1+a_2+a_3+a_5+a_1(x+x^3)+a_2x^2+a_3y+a_4(xy+x^3y)+a_5x^2y$ where $a_i \in \mathbb{F}_{2^k}$. Then $N \cong {C_2}^{5k}$.*

Proof. Let $n_1 = 1+a_2+a_3+a_5+a_1(x+x^3)+a_2x^2+a_3y+a_4(xy+x^3y)+a_5x^2y \in N$ and $n_2 = 1+b_2+b_3+b_5+b_1(x+x^3)+b_2x^2+b_3y+b_4(xy+x^3y)+b_5x^2y \in N$ where $a_i, b_j \in \mathbb{F}_{2^k}$. Then

$$\begin{aligned} n_1n_2 &= 1+a_2+a_3+a_5+b_2+b_3+b_5+\delta_1+(a_1+b_1+\delta_2)(x+x^3) \\ &\quad + (a_2+b_2+\delta_1)x^2+(a_3+b_3+\delta_1)y+(a_4+b_4+\delta_2)(xy+x^3y) \\ &\quad + (a_5+b_5+\delta_1)x^2y \end{aligned}$$

where

$$\begin{aligned} \delta_1 &= a_2(b_3+b_5)+a_3(b_2+b_5)+a_5(b_2+b_3) \\ \delta_2 &= (b_1+b_4)(a_3+a_5)+(a_1+a_4)(b_3+b_5). \end{aligned}$$

Therefore N is closed under multiplication. It can easily be shown that N is abelian.

Now $n \in V_*(\mathbb{F}_{2^k}D_8)$ if and only if $n^{-1} = n^*$ for all $n \in N$. Then

$$\begin{aligned} \sigma(n^{-1}) = \sigma(n^*) &\iff \sigma(n)^{-1} = \sigma(n^*) \\ &\iff \sigma(n)^{-1} = \sigma(n)^T \\ &\iff \sigma(n)\sigma(n)^T = I. \end{aligned}$$

Let $n = 1+a_2+a_3+a_5+a_1(x+x^3)+a_2x^2+a_3y+a_4(xy+x^3y)+a_5x^2y \in N$, then

$$\begin{aligned}\sigma(n)\sigma(n)^T = (\sigma(n))^2 &= \begin{pmatrix} A & B \\ B & A \end{pmatrix}^2 \\ &= \begin{pmatrix} A^2+B^2 & 2AB \\ 2AB & A^2+B^2 \end{pmatrix} \\ &= \begin{pmatrix} A^2+B^2 & 0 \\ 0 & A^2+B^2 \end{pmatrix}\end{aligned}$$

since $\sigma(n)^T = \sigma(n)$, where $A = \mathrm{circ}(1 + a_2 + a_3 + a_5, a_1, a_2, a_1)$, $B = \mathrm{circ}(a_3, a_4, a_5, a_4)$. Now, using Theorem 2.4

$$\begin{aligned}A^2 + B^2 &= [(1 + a_2 + a_3 + a_5)^2 + {a_1}^2 + {a_2}^2 + {a_1}^2 + {a_3}^2 + {a_4}^2 + {a_5}^2 + {a_4}^2]I_4 \\ &= [1 + {a_2}^2 + {a_2}^2 + {a_5}^2 + {a_2}^2 + {a_3}^2 + {a_5}^2]I_4 \\ &= I_4.\end{aligned}$$

Therefore $N \cong {C_2}^{5k} < V_*(\mathbb{F}_{2^k} D_8)$. □

Lemma 3.2. *Let H be the set of elements $V_*(\mathbb{F}_{2^k} D_8)$ of the form $1 + \alpha \sum_{i=1}^{3} x^i + \alpha \sum_{j=0}^{2} x^j y$ where $\alpha \in \mathbb{F}_{2^k}$. Then $H \cong {C_2}^k$.*

Proof. Let $h_1 = 1 + \alpha \sum_{i=1}^{3} x^i + \alpha \sum_{j=0}^{2} x^j y \in H$ and $h_2 = 1 + \beta \sum_{i=1}^{3} x^i + \beta \sum_{j=0}^{2} x^j y \in H$ where $\alpha, \beta \in \mathbb{F}_{2^k}$. Then

$$h_1 h_2 = 1 + (\alpha + \beta) \sum_{i=1}^{3} x^i + (\alpha + \beta) \sum_{j=0}^{2} x^j y \in H.$$

Therefore H is closed under multiplication. It can easily be shown that H is abelian. Let $h = 1 + \alpha \sum_{i=1}^{3} x^i + \alpha \sum_{j=0}^{2} x^j y \in H$ where $\alpha \in \mathbb{F}_{2^k}$, then

$$\begin{aligned}(\sigma(h))^2 &= \begin{pmatrix} A & B \\ B & A \end{pmatrix}^2 \\ &= \begin{pmatrix} A^2+B^2 & 0 \\ 0 & A^2+B^2 \end{pmatrix}\end{aligned}$$

where $A = \mathrm{circ}(1, \alpha, \alpha, \alpha)$, $B = \mathrm{circ}(\alpha, \alpha, \alpha, 0)$. Now $A^2+B^2 = (1+3\alpha^2)I_4+3\alpha^2 I_4 = (1 + 6\alpha^2)I_4 = I_4$ by Theorem 2.4. Thus $\sigma(h)^{-1} = \sigma(h)$.

Let Consider $\sigma(h^*)$. $\sigma(h^*) = (\sigma(h))^T = \sigma(h) = \sigma(h)^{-1}$. Therefore $H \cong {C_2}^k < V_*(\mathbb{F}_{2^k} D_8)$. □

Theorem 3.3. $V_*(\mathbb{F}_{2^k}D_8) \cong {C_2}^{5k} \rtimes {C_2}^{k}$.

Proof. $N = \{1+a_2+a_3+a_5+a_1(x+x^3)+a_2x^2+a_3y+a_4(xy+x^3y)+a_5x^2y \mid a_i \in \mathbb{F}_{2^k}\}$ and $H = \{1+\alpha\sum_{i=1}^{3} x^i + \alpha\sum_{j=0}^{2} x^jy \mid \alpha \in \mathbb{F}_{2^k}\}$. Clearly $N \cap H = 1$. We will show that $NH = \{nh \mid n \in N,\ h \in h\}$ is a group.
Let $n = 1+a_2+a_3+a_5+a_1(x+x^3)+a_2x^2+a_3y+a_4(xy+x^3y)+a_5x^2y \in N$ and $h = 1+\alpha\sum_{i=1}^{3} x^i + \alpha\sum_{j=0}^{2} x^jy \in H$ where $a_i, \alpha \in \mathbb{F}_{2^k}$. Therefore

$$\begin{aligned}\sigma^{-1}(h)\sigma(n)\sigma(h) &= \sigma(h)\sigma(n)\sigma(h)\\ &= \begin{pmatrix} A & B \\ B & A\end{pmatrix}\begin{pmatrix} C & D \\ D^T & C^T\end{pmatrix}\begin{pmatrix} A & B \\ B & A\end{pmatrix}\\ &= \begin{pmatrix} E & F \\ F^T & D^T\end{pmatrix}\end{aligned}$$

where $A = \mathrm{circ}(1,\alpha,\alpha,\alpha)$, $B = \mathrm{circ}(\alpha,\alpha,\alpha,0)$, $C = \mathrm{circ}(1+a_2+a_3+a_5, a_1, a_2, a_1)$, $D = \mathrm{circ}(a_3, a_4, a_5, a_4)$ $E = \mathrm{circ}(1+a_2+a_3+a_5, a_1+\delta_1, a_2, a_1+\delta_1)$ $F = \mathrm{circ}(a_3+\delta_2, a_4, a_5+\delta_2, a_4)$, $\delta_1 = \alpha(\alpha+1)(a_3+a_5)$ and $\delta_2 = \alpha^2(a_3+a_5)$.

Clearly $h^{-1}nh \in N$. Thus $H^{-1}NH = N$, so S and N permute, so $\langle N, H\rangle = NH$. Now $|NH| = 2^{6k}$ and $|V_*(\mathbb{F}_{2^k}D_8)| = 2^{6k}$ by Theorem 2.5, therefore $NH = V_*(\mathbb{F}_{2^k}D_8)$ and $N \lhd NH = V_*(\mathbb{F}_{2^k}D_8)$. Therefore $V_*(\mathbb{F}_{2^k}D_8) \cong N \rtimes H \cong {C_2}^{5k} \rtimes {C_2}^{k}$. $\square$

Acknowledgment. The author would like to thank the referee for the valuable suggestions and comments.

References

[1] A.A. Bovdi and L. Erdei, *Unitary units in the modular group algebra of groups of order 16*, Technical Reports Debrecen, 94/4 (1996), 57–72.

[2] V.A. Bovdi and L.G. Kovács, *Unitary units in modular group algebras*, Manuscr. Math., 84(1) (1994), 57–72.

[3] V. Bovdi and A.L. Rosa, *On the order of the unitary subgroup of a modular group algebra*, Comm. Algebra, 28(4) (2000), 1897–1905.

[4] A.A. Bovdi and A. Szakács, *Unitary subgroup of the group of units of a modular group algebra of a finite abelian p-group*, Math. Zametki, 45(6) (1989), 23–29.

[5] L.Creedon and J. Gildea, *The Structure of the unit group of the group algebra $\mathbb{F}_{2^k}D_8$*, Canad. Math. Bull., Published electronically on August 26, 2010. doi:10.4153/CMB-2010-098-5.

[6] L.Creedon and J. Gildea, *Unitary units of the group algebra* $\mathbb{F}_{2^k}Q_8$, Internat. J. Algebra Comp., 19(2) (2009), 283–286.

[7] P.J. Davis, Circulant Matrices, Chelsea Publishing, New York, 1979.

[8] J. Gildea, *On the order of* $\mathcal{U}(\mathbf{F}_{p^k}D_{2p^m})$, Int. J. Pure Appl. Math., 46(2) (2008), 267–272.

[9] T. Hurley, *Group rings and rings of matrices*, Int. J. Pure Appl. Math., 31 (2006), 319–335.

[10] C. Polcino Milies and S.K. Sehgal, An Introduction to Group Rings (Algebras and Applications), Kluwer Academic Publishers, Dordrecht, 2002.

[11] R. Sandling, *Units in the modular group algebra of a finite abelian p-group*, J. Pure Appl. Algebra, 33 (1984), 337–346.

[12] R. Sandling, *Presentations for units groups of modular group algebras of groups of order 16*, Math. Comp., 59 (1992), 689–701.

Joe Gildea
Department of Mechanical and Electronic Engineering
School of Engineering
Institute of Technology Sligo
Ireland
e-mail: gildea.joe@itsligo.ie