Canad. Math. Bull. Vol. **54** (2), 2011 pp. 237–243
doi:10.4153/CMB-2010-098-5

The Structure of the Unit Group of the Group Algebra $\mathbb{F}_{2^k}D_8$

Leo Creedon and Joe Gildea

Abstract. Let RG denote the group ring of the group G over the ring R. Using an isomorphism between RG and a certain ring of $n \times n$ matrices in conjunction with other techniques, the structure of the unit group of the group algebra of the dihedral group of order 8 over any finite field of chracteristic 2 is determined in terms of split extensions of cyclic groups.

1 Introduction

Let RG denote the group ring of the group G over the ring R. When a ring S contains the identity 1_S, an element a of S is invertible if and only if there exists an element $s \in S$ such that $a \cdot s = s \cdot a = 1_S$. The set of all the invertible elements of S forms a group called the unit group of S, denoted by $\mathcal{U}(S)$. The homomorphism $\varepsilon\colon RG \to R$ given by

$$\varepsilon\Big(\sum_{g\in G} a_g g\Big) = \sum_{g\in G} a_g$$

is called the augmentation mapping of RG. The normalized unit group of RG denoted by $V(RG)$ consists of all the invertible elements of RG of augmentation 1. It is a well-known fact that $\mathcal{U}(RG) \cong \mathcal{U}(R) \times V(RG)$. For further details and background see Polcino Milies and Sehgal [10]. In [11], a basis for $V(\mathbb{F}_p G)$ is determined where $\mathbb{F}_p$ is the Galois field of p elements and G is an abelian p-group.

We are interested in the structure of $\mathcal{U}(FG)$ where F is a field of characteristic 2 and G is a finite 2-group. If G is a finite 2-group and F is a 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 $\mathbb{F}_2 D_8$ is established in [12], where D_8 is the dihedral group of order 8. In [7], the unit group of $\mathbb{F}_{p^m} G$ is described where $|\mathbb{F}_{p^m} G| < 2^{10}$.

The map $*\colon KG \longrightarrow KG$ defined by

$$\Big(\sum_{g\in G} a_g g\Big)^* = \sum_{g\in G} a_g g^{-1}$$

is an antiautomorphism 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. In [1], a basis for $V_*(FG)$ is established, where F is any finite field and G is an abelian p-group. In [3], V. Bovdi and A. L. Rosa determine the order

Received by the editors May 1, 2008; revised February 16, 2009.
Published electronically August 26, 2010.
AMS subject classification: **16U60**, 16S34, 20C05, 15A33.

of $V_*(\mathbb{F}_{2^k}D_8)$ where $D_8 = \langle x, y \mid x^4 = 1, y^2 = 1, yx = x^{-1}y\rangle$. Since D_8 is extra special, $V_*(\mathbb{F}_{2^k}D_8)$ is normal in $V(\mathbb{F}_{2^k}D_8)$ by Bovdi and Kovács [2].

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

The main result is that the unit group of $\mathbb{F}_{2^k}D_8$ is isomorphic to

$$\big[(((C_2{}^k \times C_4{}^k) \rtimes C_4{}^k) \times C_2{}^k) \rtimes C_{2^k})\big] \times C_{2^k-1}.$$

The techniques described in this paper can be easily implemented using the LAGUNA package [4] for the GAP system [13].

1.1 Background

Definition 1.1 A circulant matrix over a ring R is a square $n \times n$ matrix of the form

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

where $a_i \in R$.

For further details on circulant matrices, see Davis [6].

Fix a labeling of elements of G by indices $\{1, 2, \dots, n\}$, so $G = \{g_1, g_2, \dots, g_n\}$. Then the matrix

$$\begin{pmatrix} g_1{}^{-1}g_1 & g_1{}^{-1}g_2 & g_1{}^{-1}g_3 & \dots & g_1{}^{-1}g_n \\ g_2{}^{-1}g_1 & g_2{}^{-1}g_2 & g_2{}^{-1}g_3 & \dots & g_2{}^{-1}g_n \\ g_3{}^{-1}g_1 & g_3{}^{-1}g_2 & g_3{}^{-1}g_3 & \dots & g_3{}^{-1}g_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g_n{}^{-1}g_1 & g_n{}^{-1}g_2 & g_n{}^{-1}g_3 & \dots & g_n{}^{-1}g_n \end{pmatrix}$$

is called the matrix of G (with respect to this labeling) and is denoted by $M(G)$. Let $w = \sum_{i=1}^{n} \alpha_{g_i} g_i \in RG$ where R is a ring. Then the matrix

$$\begin{pmatrix} \alpha_{g_1{}^{-1}g_1} & \alpha_{g_1{}^{-1}g_2} & \alpha_{g_1{}^{-1}g_3} & \dots & \alpha_{g_1{}^{-1}g_n} \\ \alpha_{g_2{}^{-1}g_1} & \alpha_{g_2{}^{-1}g_2} & \alpha_{g_2{}^{-1}g_3} & \dots & \alpha_{g_2{}^{-1}g_n} \\ \alpha_{g_3{}^{-1}g_1} & \alpha_{g_3{}^{-1}g_2} & \alpha_{g_3{}^{-1}g_3} & \dots & \alpha_{g_3{}^{-1}g_n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{g_n{}^{-1}g_1} & \alpha_{g_n{}^{-1}g_2} & \alpha_{g_n{}^{-1}g_3} & \dots & \alpha_{g_n{}^{-1}g_n} \end{pmatrix}$$

is called the RG-matrix of w and is denoted by $M(RG, w)$. The following result can be found in [9].

Theorem 1.2 *Given a labeling of the elements of a group G of order n, there is a ring isomorphism between RG and the* $n \times n$ *G-matrices over R. This isomorphism is given by* $\sigma\colon w \mapsto M(RG, w)$.

Example 1.3 Let $D_{2n} = \langle x, y \mid x^n = 1, y^2 = 1, yx = x^{-1}y\rangle$ 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 $a_i, b_j \in \mathbb{F}_{p^k}$, p is a prime and $m \in \mathbb{N}_0$, then $\sigma(\kappa) = \left(\begin{smallmatrix} A & B \\ B^T & A^T \end{smallmatrix}\right)$, where $A = \operatorname{circ}(a_0, a_1, \ldots, a_{n-1})$ and $B = \operatorname{circ}(b_0, b_1, \ldots, b_{n-1})$.

The next result can be found in [5].

Theorem 1.4 *Let A, B, C, and D be* $n \times n$ *matrices. Then* $\det\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) = \det(AD - BC)$ *if C and D commute.*

The next two results can be found in [8].

Proposition 1.5 *Let* $A = \operatorname{circ}(a_0, a_2, \ldots, a_{p^m-1})$, *where* $a_i \in \mathbb{F}_{p^k}$, *p is a prime and* $m \in \mathbb{N}_0$. *Then*

$$\det(A) = \sum_{i=0}^{p^m-1} a_i{}^{p^m}.$$

Proposition 1.6 *Let* $A = \operatorname{circ}(a_1, a_2, \ldots, a_{p^m})$ *and* $B = \operatorname{circ}(b_1, b_2, \ldots, b_{p^m})$, *where* $a_i, b_j \in \mathbb{F}_{p^k}$, *p is a prime and* $m \in \mathbb{N}_0$. *Then*

$$\det(A \pm B) = \det(A) \pm \det(B).$$

Theorem 1.7 $\mathcal{U}(\mathbb{F}_{2^k}C_2) \cong C_2{}^k \times C_{2^k-1}$.

Proof Let $C_2 = \langle x \mid x^2 = 1\rangle$. Clearly $|V(\mathbb{F}_{2^k}C_2)| = 2^k$. Let $\alpha = a + bx \in V(\mathbb{F}_{2^k}C_2)$, where $a, b \in \mathbb{F}_{2^k}$. Then $\alpha^2 = a^2 + b^2 = (a + b)^2 = 1$, since $\alpha \in V(\mathbb{F}_{2^k}C_2)$. Therefore $V(\mathbb{F}_{2^k}C_2)$ has exponent 2. ■

2 The Structure of $\mathcal{U}(\mathbb{F}_{2^k}D_8)$

Define the group epimorphism $\theta\colon \mathcal{U}(\mathbb{F}_{2^k}D_8) \to \mathcal{U}(\mathbb{F}_{2^k}C_2)$ given by

$$\sum_{i=0}^{3} a_i x^i + \sum_{j=0}^{3} b_j x^j y \longmapsto \sum_{i=0}^{3} a_i + \sum_{j=0}^{3} b_j\, \overline{y},$$

where $a_i, b_j \in \mathbb{F}_{2^k}$, where $\overline{y}$ is the generator of the group C_2.

Define the group homomorphism $\psi\colon \mathcal{U}(\mathbb{F}_{2^k}C_2) \to \mathcal{U}(\mathbb{F}_{2^k}D_8)$ by $a + b\overline{y} \mapsto a + by$. Then $\theta \circ \psi(a + b\overline{y}) = \theta(a + by) = a + b\overline{y}$. Therefore, $\mathcal{U}(\mathbb{F}_{2^k}D_8)$ is a split extension of $\mathcal{U}(\mathbb{F}_{2^k}C_2)$ by $\ker(\theta)$.

https://doi.org/10.4153/CMB-2010-098-5 Published online by Cambridge University Press

Therefore,

$$\mathcal{U}(\mathbb{F}_{2^k}D_8) \cong H \rtimes \mathcal{U}(\mathbb{F}_{2^k}C_2) \cong H \rtimes (C_2{}^k \times C_{2^k-1}) \cong (H \rtimes C_2{}^k) \times C_{2^k-1},$$

where $H \cong ker(\theta)$. Note that

$$|H| = \frac{2^{7k}(2^k-1)}{2^k(2^k-1)} = 2^{6k}.$$

Proposition 2.1 *H has exponent* 4.

Proof Let

$$\alpha = \sum_{i=0}^{3} a_i x^i + \sum_{j=0}^{3} b_j x^j y \in \mathcal{U}(\mathbb{F}_{2^k}D_8),$$

where $a_i, b_j \in \mathbb{F}_{2^k}$. Then

$$\alpha \in H \Longleftrightarrow \sum_{i=0}^{3} a_i = 1 \text{ and } \sum_{j=0}^{3} b_j = 0,$$

$$\begin{aligned}\alpha^2 = (a_0+a_2)^2 + \Big(\sum_{j=0}^{3} b_j\Big)^2 &+ (b_0+b_2)(b_1+b_3)x + (a_1+a_3)^2x^2 \\ &+ (b_0+b_2)(b_1+b_3)x^3 + (a_1+a_3)(b_1+b_3)y + (a_1+a_3)(b_0+b_2)xy \\ &+ (a_1+a_3)(b_1+b_3)x^2y + (a_1+a_3)(b_0+b_2)x^3y.\end{aligned}$$

Therefore every element of order 2 has the form $1 + s + tx + sx^2 + tx^3 + uy + vxy + ux^2y + vx^3y$, where $s, t, u, v \in \mathbb{F}_{2^k}$.

Then

$$\alpha^4 = \sum_{i=0}^{3} a_i{}^4 + \sum_{j=0}^{3} b_j{}^4 = \Big(\sum_{i=0}^{3} a_i\Big)^4 + \Big(\sum_{j=0}^{3} b_j\Big)^4 = 1. \qquad \blacksquare$$

Proposition 2.2 *Let* $\alpha \in H$. *Then* $[\sigma(\alpha)]^{-1} = [\sigma(\alpha)]^*$, *where* $[\sigma(\alpha)]^*$ *is the adjoint matrix of* $\sigma(\alpha)$.

Proof Let

$$\alpha = \sum_{i=0}^{3} a_i x^i + \sum_{j=0}^{3} b_j x^j y \in H$$

where $a_i, b_j \in \mathbb{F}_{2^k}$. Then $\sigma(\alpha) = \left(\begin{smallmatrix} A & B \\ B^T & A^T \end{smallmatrix}\right)$ where $A = \text{circ}(a_0, a_1, a_2, a_3)$, $B =$

https://doi.org/10.4153/CMB-2010-098-5 Published online by Cambridge University Press

$\operatorname{circ}(b_0, b_1, b_2, b_3)$. Using Theorem 1.4 and Propositions 1.5 and 1.6, it is clear that

$$\begin{aligned}\det(\sigma(\alpha)) &= \det(AA^T - BB^T)\\ &= \det(AA^T) + \det(BB^T)\\ &= \det(A^2) + \det(B^2)\\ &= (\det(A) + \det(B))^2\\ &= \Big(\sum_{i=0}^{3} {a_i}^4 + \sum_{j=0}^{3} {b_j}^4\Big)^2 \quad = \Big(\Big(\sum_{i=0}^{3} a_i\Big)^4 + \Big(\sum_{j=0}^{3} b_j\Big)^4\Big)^2 = 1,\end{aligned}$$

since $\alpha \in H$. ■

Proposition 2.3 *Let S be the subset of H consisting of elements of the form*

$$\Big(1 + \sum_{i=0}^{3} a_i\Big) + \sum_{i=0}^{3} a_i x^i + \sum_{i=0}^{3} a_i y + \sum_{i=0}^{3} a_i x^i y,$$

where $a_i \in \mathbb{F}_{2^k}$ and $\sum_{i=0}^{3} a_i = 1$. Then S is a group and $S \cong {C_2}^k \times {C_4}^k$.

Proof Let

$$x_1 = \Big(1 + \sum_{i=0}^{3} a_i\Big) + \sum_{i=0}^{3} a_i x^i + \sum_{i=0}^{3} a_i y + \sum_{i=0}^{3} a_i x^i y$$

and

$$x_2 = \Big(1 + \sum_{j=0}^{3} b_j\Big) + \sum_{j=0}^{3} b_j x^j + \sum_{j=0}^{3} b_j y + \sum_{j=0}^{3} b_j x^j y,$$

where $a_i, b_j \in \mathbb{F}_{2^k}$, $\sum_{i=0}^{3} a_i = 1$ and $\sum_{j=0}^{3} b_j = 1$. Then

$$x_1x_2 = \Big(1+\gamma+\sum_{i=0}^{3}(a_i+b_i)\Big) + \sum_{i=0}^{3}(a_i+b_i+\gamma)x^i + \sum_{i=0}^{3}(a_i+b_i+\gamma)y + \sum_{i=0}^{3}(a_i+b_i+\gamma)x^i y,$$

where $\gamma = (a_1+a_3)(b_1+b_3)$. Therefore S is closed under multiplication and $|S| = 2^{3k}$. It can easily be shown that S is abelian.

Therefore $S \cong {C_2}^l \times {C_4}^m$ for some l and m. Consider ${C_2}^l \times {C_4}^m$. The number of elements of order 2 or 1 is $2^l 2^m = 2^{l+m}$. Therefore the number of elements of order 4 is $2^l 4^m - 2^{l+m} = 2^{l+m}(2^m - 1)$. Then

$${x_1}^2 = 1 + \sum_{i=1}(a_1 + a_3)^2 x^i + \sum_{j=1}(a_1 + a_3)^2 x^j y \quad \text{and} \quad {x_1}^2 = 1 \Longleftrightarrow a_1 = a_3.$$

However, the number of elements in S of order 2 or 1 is 2^{2k}. Therefore the number of elements of S of order 4 is $2^{3k} - 2^{2k} = 2^{2k}(2^k - 1)$. Thus $l + m = 2k$, $m = k \Longrightarrow l = m = k$ and $S \cong {C_2}^k \times {C_4}^k$. ■

https://doi.org/10.4153/CMB-2010-098-5 Published online by Cambridge University Press

Proposition 2.4 *Let N be the subset of H consisting of elements of the form $1 + px + px^3 + qy + rxy + rx^2y + qx^3y$, where $p, q, r \in \mathbb{F}_{2^k}$. Then N is a group, $N \cong {C_2}^k \times {C_4}^k$ and $N \lhd H$.*

Proof Let

$$n_1 = 1 + p_1x + p_1x^3 + q_1y + r_1xy + r_1x^2y + q_1x^3y \in Y \text{ and}$$
$$n_2 = 1 + p_2x + p_2x^3 + q_2y + r_2xy + r_2x^2y + q_2x^3y \in Y,$$

where $p_i, q_r, r_l \in \mathbb{F}_{2^k}$. Then

$$n_1n_2 = 1 + (p_1 + p_2 + \gamma_1)x + (p_1 + p_2 + \gamma_1)x^3 + (q_1 + q_2 + \gamma_2)y + (r_1 + r_2 + \gamma_2)xy + (r_1 + r_2 + \gamma_2)x^2y + (q_1 + q_2 + \gamma_2)x^3,$$

where $\gamma_1 = q_1q_2 + r_1q_2 + q_1r_2 + r_1r_2$ and $\gamma_2 = p_1q_2 + p_1r_2 + r_1p_2 + q_1p_2$. Therefore N is closed under multiplication and $|N| = 2^{3k}$. It can easily be shown that N is abelian.

Let

$$\alpha = 1 + px + px^3 + qy + rxy + rx^2y + qx^3y \in N \text{ and}$$
$$h = \sum_{i=0}^{3} a_ix^i + \sum_{j=0}^{3} b_jx^jy \in H,$$

where $p, q, r, a_i, b_j \in \mathbb{F}_{2^k}$. Then

$$\sigma(h^{-1}\alpha h) = \begin{pmatrix} E & F \\ F^T & E^T \end{pmatrix}^* \begin{pmatrix} A & B \\ B^T & A \end{pmatrix} \begin{pmatrix} E & F \\ F^T & E^T \end{pmatrix} = \begin{pmatrix} A & G \\ G^T & A \end{pmatrix},$$

where

$$\begin{aligned} &A = \operatorname{circ}(1, p, 0, p), && B = \operatorname{circ}(q, r, r, q), \\ &E = \operatorname{circ}(a_0, a_1, a_2, a_3), && F = \operatorname{circ}(b_0, b_1, b_2, b_3), \\ &G = \operatorname{circ}(q + \lambda, r + \lambda, r + \lambda, q + \lambda), && \lambda = (r + q)(a_1 + a_3). \end{aligned}$$

Thus $N \lhd H$.

Also $\alpha^2 = 1 + (r + q)(x + x^3)$. Therefore $\alpha^2 = 1 \iff r = q$. Repeating the argument used in the previous lemma, $N \cong {C_2}^k \times {C_4}^k$. ■

Proposition 2.5 *$H = NS$.*

Proof By the second Isomorphism Theorem, $S/S\cap N \cong NS/N$. Thus $|NS/N| = 2^{3k}$ and $|NS| = 2^{6k}$. Therefore $H = NS$. ■

Theorem 2.6 *$\mathcal{U}(\mathbb{F}_{2^k}D_8) \cong [((({C_2}^k \times {C_4}^k) \rtimes {C_4}^k) \times {C_2}^k) \rtimes C_{2^k})] \times C_{2^k-1}$.*

https://doi.org/10.4153/CMB-2010-098-5 Published online by Cambridge University Press

Proof Clearly $N \cap S = 1$, therefore $H \cong N \rtimes S$ and $\mathcal{U}(\mathbb{F}_{2^k}D_8) \cong ((N \rtimes S) \rtimes C_2{}^k) \times C_{2^k-1}$.

Let

$$s = \left(1 + \sum_{i=0}^{3} a_i\right) + \sum_{i=0}^{3} a_i x^i + \sum_{i=0}^{3} a_i y + \sum_{i=0}^{3} a_i x^i y \in S \text{ and}$$

$$n = 1 + px + px^3 + qy + rxy + rx^2y + qx^3y \in N.$$

Then

$$n^s = 1 + px + px^3 + \big(q + (r+q)(a_1 + a_3)\big)\,y + \big(r + (r+q)(a_1 + a_3)\big)\,xy + \big(r + (r+q)(a_1 + a_3)\big)\,x^2y + \big(q + (r+q)(a_1 + a_3)\big)\,x^3y.$$

Therefore $n^s = n$ if and only if $a_1 = a_3$. If $a_1 = a_3$, then $s^2 = 1$. Therefore the elements of order 2 in S act trivially on N and

$$N \rtimes S \cong (C_2{}^k \times C_4{}^k) \rtimes (C_2{}^k \times C_4{}^k) \cong ((C_2{}^k \times C_4{}^k) \rtimes C_4{}^k) \times C_2{}^k.$$

Thus

$$\mathcal{U}(\mathbb{F}_{2^k}D_8) \cong \big[(((C_2{}^k \times C_4{}^k) \rtimes C_4{}^k) \times C_2{}^k) \rtimes C_2{}^k)\big] \times C_{2^k-1}. \qquad \blacksquare$$

References

[1] A. A. Bovdi and A. Szakács, *A basis for the unitary subgroup of the group algebra of units in a finite commutative group algebra.* Publ. Math. Debrecen **46**(1995), no. 1–2, 97–120.

[2] V. Bovdi and L. G. Kovács, *Unitary units in modular group algebras.* Manuscr. Math. **84**(1994), no. 1, 57–72. doi:10.1007/BF02567443

[3] V. Bovdi and A. L. Rosa, *On the order of the unitary subgroup of a modular group algebra.* Comm. Algebra **28**(2000), no. 4, 1897–1905. doi:10.1080/00927870008826934

[4] V. Bovdi, A. Konovalov, R. Rossmanith, and C. Schneider. LAGUNA — Lie AlGebras and UNits of group Algebras. http://www.gap-system.org/Packages/laguna.html

[5] M. Brooks, The Matrix reference Manual (online), 2005. http://www.ee.ic.ac.uk/hp/staff/dmb/matrix/intro.html

[6] P. J. Davis, *Circulant matrices.* John Wiley & Sons, New York-Chichester-Brisbane, 1979.

[7] L. Creedon, *The unit group of small group algebras and the minimum counterexample to the isomorphism problem.* Int. J. Pure Appl. Math. **49**(2008), no. 4, 531–537.

[8] J. Gildea, *On the order of* $\mathcal{U}(\mathbb{F}_{p^k}D_{2p^m})$. Int. J. Pure Appl. Math. **46**(2008), no. 2, 267–272.

[9] T. Hurley, *Group rings and rings of matrices.* Int. J. Pure Appl. Math. **31**(2006), no. 3, 319–335.

[10] C. Polcino Milies and S. K. Sehgal, *An introduction to group rings.* Algebras and Applications, 1, 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), no. 3, 337–346. doi:10.1016/0022-4049(84)90066-5

[12] ———, *Presentations for units groups of modular group algebras of groups of order* 16. Math. Comp. **59**(1992), no. 200, 689–701.

[13] The GAP Group, *GAP—groups, algorithms, programming.* Version 4.4.10, 2007. http://www.gap-system.org

School of Engineering, Institute of Technology, Sligo, Ireland
e-mail: creedon.leo@itsligo.ie
gildea.joe@itsligo.ie

https://doi.org/10.4153/CMB-2010-098-5 Published online by Cambridge University Press