International Journal of Pure and Applied Mathematics

Volume 45 No. 2 2008, 315-320

THE STRUCTURE OF THE UNIT GROUP OF THE GROUP ALGEBRA $\mathbb{F}_{3^k}D_6$

Leo Creedon[1 §], Joe Gildea[2]

[1,2]School of Engineering
Institute of Technology
Sligo, IRELAND

[1]e-mail: creedon.leo@itsligo.ie

[2]e-mail: gildeajoe@gmail.com

Abstract: The structure of the unit group of the group algebra of the dihedral group of order 6 over any finite field of chracteristic 3 is determined in terms of split extensions of cyclic groups.

AMS Subject Classification: 20C05, 16S84, 20H30, 15A33

Key Words: group ring, group algebra, unit group, dihedral

1. Introduction

The set of all the invertible elements of a ring S form a group called the unit group of S, denoted by $\mathcal{U}(S)$. Let $\mathbb{F}_{p^k}D_{2p^m}$ be the group algebra of D_{2p^m} over $\mathbb{F}_{p^k}$, where $\mathbb{F}_{p^k}$ is the Galois field of p^k-elements, D_{2p^m} is the dihedral group of order $2p^m$ and p is a prime. For further details on group algebras see [5]. In [2], the order of $\mathcal{U}(\mathbb{F}_{p^k}D_{2p^m})$ is established to be $p^{2k(p^m-1)}(p^k-1)^2$, where p is an odd prime and $m \in \mathbb{N}_0$.

Let C_n be the cyclic group of order n. 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 $\mathcal{U}(\mathbb{F}_{3^k}D_6)$ to be $(({C_3}^{3k} \rtimes {C_3}^k) \rtimes C_{3^k-1}) \times C_{3^k-1}$.

Received: April 17, 2008

§Correspondence author

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 $a_i \in R$.

For further details on circulant matrices see Davis [1].

Let $\{g_1, g_2, \ldots, g_n\}$ be a fixed listing of the elements of a group G. Then the following matrix:

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

is called the matrix of G (relative to this listing) 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 following matrix:

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

is called the RG-matrix of w and is denoted by $M(RG, w)$.

The following Theorem can be found in [3].

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 $D_{2n} = \langle x, y \mid x^n = 1, y^2 = 1, yx = x^{-1}y \rangle$ 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 $a_i, b_j \in \mathbb{F}_{p^k}$ and p is a prime, then

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

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

The next result can be found in [5].

Lemma 2.4. *Let G be an Abelian group of order n and K a field such that the characteristic of K does not divide n. If K contains a primitive root of unity of order n then $KG \cong \underbrace{K \oplus \cdots \oplus K}_{n}$.*

Example 2.5. $\mathcal{U}(\mathbb{F}_{p^k} C_2) \cong C_{p^k-1} \times C_{p^k-1}$ when $p \neq 2$.

Proof. Since $p \neq 2$, $\mathbb{F}_{p^k}$ contains primitive roots of unity of order 2. Therefore $\mathbb{F}_{p^k} C_2 \cong \mathbb{F}_{p^k} \oplus \mathbb{F}_{p^k}$ and $\mathcal{U}(\mathbb{F}_{p^k} C_2) \cong C_{p^k-1} \times C_{p^k-1}$. □

The next two results appear in [2]

Proposition 2.6. *Let $A = \text{circ}(a_1, a_2, \ldots, a_{p^m})$, where $a_i \in \mathbb{F}_{p^k}$, p is a prime and $m \in \mathbb{N}_0$. Then*

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

Theorem 2.7. *$|\mathcal{U}(\mathbb{F}_{p^k} D_{2p^m})| = p^{2k(p^m-1)}(p^k-1)^2$, where p is an odd prime and $m \in \mathbb{N}_0$.*

3. The Structure of $\mathcal{U}(\mathbb{F}_{3^k} D_6)$

Define the ring homomorphism $\theta : \mathbb{F}_{3^k} D_6 \longrightarrow \mathbb{F}_{3^k} C_2$ by

$$\sum_{i=0}^{2} a_i x^i + \sum_{j=0}^{2} b_j x^j y \longmapsto \sum_{i=0}^{2} a_i + \sum_{j=0}^{2} b_j \,.\overline{y}.$$

Now define the group epimorphism $\theta' : \mathcal{U}(\mathbb{F}_{3^k} D_6) \longrightarrow \mathcal{U}(\mathbb{F}_{3^k} C_2)$, where θ' is θ restricted to $\mathcal{U}(\mathbb{F}_{3^k} D_6)$. Let $\psi : \mathcal{U}(\mathbb{F}_{3^k} C_2) \longrightarrow \mathcal{U}(\mathbb{F}_{3^k} D_6)$ be the group homomorphism defined by $a + b.\overline{y} \mapsto a + b.Y$. Then $\theta' \circ \psi(a + b.\overline{y}) = \theta(a + b.Y) = a + b.\overline{y}$. Therefore $\mathcal{U}(\mathbb{F}_{3^k} D_6)$ is a split extension of $\mathcal{U}(\mathbb{F}_{3^k} C_2)$ by $\ker(\theta')$. Thus $\mathcal{U}(\mathbb{F}_{3^k} D_6) \cong H \rtimes \mathcal{U}(\mathbb{F}_{3^k} C_2)$, where $H = \ker(\theta')$.

Lemma 3.1. *H has exponent 3.*

Proof. Let $\alpha = \sum_{i=0}^{2} a_i x^i + \sum_{j=0}^{2} b_j x^j y \in H$, where $a_i, b_j \in \mathbb{F}_{3^k}$. Note that $\sum_{i=0}^{2} a_i = 1$ and $\sum_{j=0}^{2} b_j = 0$ since $\alpha \in H$. Then

$$(\sigma(\alpha))^3 = \begin{pmatrix} A & B \\ B^T & A^T \end{pmatrix}^3 =$$

$$\begin{pmatrix} A^3 + 2ABB^T + A^T BB^T & A^2B + AA^TB + B^2B^T + (A^T)^2B \\ A^2B^T + B(B^T)^2 + AA^TB^T + (A^T)^2B^T & ABB^T + 2A^TBB^T + (A^T)^3 \end{pmatrix},$$

where $A = \mathrm{circ}(a_0, a_1, a_2)$ and $B = \mathrm{circ}(b_0, b_1, b_2)$. Note that A, B, A^T and B^T commute, since they are circulant matrices.

Define $E = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$. Now $BB^T = \gamma_1 E$, where $\gamma_1 = 2b_1^2 + 2b_1b_2 + 2b_2^2$. Thus $ABB^T = A\gamma_1 E = \gamma_1 \sum_{i=0}^{2} a_i E = \gamma_1 E$. Similarly $A^T BB^T = \gamma_1 E$. Also $B^2B^T = B\gamma_1 E = \gamma_1 \sum_{j=0}^{2} b_j E = 0$. Similarly $A^2B + AA^TB + (A^T)^2B = B(A^2 + AA^T + (A^T)^2) = \mathrm{circ}(b_0, b_1, b_2)\gamma_2 E = \gamma_2 \sum_{j=0}^{2} b_j E = 0$, where $\gamma_2 = {a_0}^2 + a_0a_2 + {a_2}^2$. Finally $A^3 = (A^T)^3 = \sum_{i=0}^{2} {a_i}^3 I_3 = I_3$ by Proposition 2.6. Thus $(\sigma(\alpha))^3 = I_6$. □

Lemma 3.2. $C_H(x) = \left\{ \sum_{i=0}^{2} a_i x^i + b \sum_{j=0}^{2} x^j y \mid \sum_{i=0}^{2} a_i = 1,\ a_i, b \in \mathbb{F}_{3^k} \right\} \cong {C_3}^{3k}$ *and* $C_H(x) \lhd H$.

Proof. $C_H(x) = \{h \in H \mid hx = xh\}$. Let $h = \sum_{i=0}^{2} a_i x^i + \sum_{j=0}^{2} b_j x^j y \in H$ where

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

$$hx - xh = \left(\sum_{i=0}^{2} a_i x^i + \sum_{j=0}^{2} b_j x^j y\right) x - x\left(\sum_{i=0}^{2} a_i x^i + \sum_{j=0}^{2} b_j x^j y\right)$$

$$= \sum_{i=0}^{2} a_i x^{i+1} + \sum_{j=0}^{2} b_j x^{j-1} y - \sum_{i=0}^{2} a_i x^{i+1} - \sum_{j=0}^{2} b_j x^{j+1} y = \sum_{j=0}^{2} b_j x^{j-1} y - \sum_{j=0}^{2} b_j x^{j+1} y$$

$$= (b_1 - b_2)y + (b_2 - b_0)xy + (b_0 - b_1)x^2 y = 0 \Longleftrightarrow b_0 = b_1 = b_2.$$

Thus every element of $C_H(x)$ is of the form $\sum_{i=0}^{2} a_i x^i + b\sum_{j=0}^{2} x^j y$, where $\sum_{i=0}^{2} a_i = 1$ and $b \in \mathbb{F}_{3^k}$. Let $\alpha = \sum_{l=0}^{2} c_l x^l + d\sum_{m=0}^{2} x^m y \in C_H(x)$, where $c_l, d \in \mathbb{F}_{3^k}$. Then $\sigma(\alpha^h) = \sigma(h^{-1})\sigma(\alpha)\sigma(h) = \begin{pmatrix} A & B \\ B^T & A^T \end{pmatrix}^2 \begin{pmatrix} C & D \\ D & C^T \end{pmatrix} \begin{pmatrix} A & B \\ B^T & A^T \end{pmatrix} = \begin{pmatrix} C & F \\ F & C^T \end{pmatrix}$, where $A = \mathrm{circ}(a_0, a_1, a_2)$, $B = \mathrm{circ}(b_0, b_1, b_2)$, $C = \mathrm{circ}(c_0, c_1, c_2)$, $D = \mathrm{circ}(d, d, d)$, $F = \mathrm{circ}(\gamma_3, \gamma_3, \gamma_3)$ and $\gamma_3 = d + 2b_1c_1 + b_1c_2 + 2b_2c_2 + b_2c_1$. Therefore $C_H(x) \lhd H$. It can easily be shown that $C_H(x)$ is Abelian. □

Lemma 3.3. *Let T be the set of elements of H of the form $1 + r\sum_{i=1}^{2} ix^i + r\sum_{j=1}^{2} jx^{j-1}y$, where $r \in \mathbb{F}_{3^k}$. Then T is a group and is isomorphic to ${C_3}^k$.*

Proof. Let $\alpha = 1 + r\sum_{i=1}^{2} ix^i + r\sum_{j=1}^{2} jx^{j-1}y \in T$ and $\beta = 1 + s\sum_{i=1}^{2} ix^i + s\sum_{j=1}^{2} jx^{j-1}y \in T$, where $r, s \in \mathbb{F}_{3^k}$. Then $\alpha\beta = 1 + (r+s)\sum_{i=1}^{2} ix^i + (r+s)\sum_{j=1}^{2} jx^{j-1}y$. Thus T is closed under multiplication. It can easily be shown that T is Abelian. □

Lemma 3.4. *$H = C_H(x)T$.*

Proof. Clearly $C_H(x) \cap T = \{1_H\}$. By the Second Isomorphism Theorem $T/T \cap C_H(x) \cong T.C_H(x)/C_H(x)$. Thus $|T.C_H(x)/C_H(x)| = 3^k$ and $|C_H(x).T| = 3^{4k}$. Note that $|H| = \frac{3^{4k}(3^k-1)^2}{(3^k-1)^2} = 3^{4k}$ by Theorem 2.7 and Example 2.5. Therefore $H = C_H(x).T$. □

Theorem 3.5. $\mathcal{U}(\mathbb{F}_{3^k}D_6) \cong ((C_3{}^{3k} \rtimes C_3{}^k) \rtimes C_{3^k-1}) \times C_{3^k-1}$.

Proof. Recall that $\mathcal{U}(\mathbb{F}_{3^k}D_6) \cong H \rtimes \mathcal{U}(\mathbb{F}_{3^k}C_2)$. Note that $|H| = 3^{4k}$. Therefore $H \cong C_H(x) \rtimes T \cong C_3{}^{3k} \rtimes C_3{}^k$. Thus by Example 2.5. we have that $\mathcal{U}(\mathbb{F}_{3^k}D_6) \cong H \rtimes \mathcal{U}(\mathbb{F}_{3^k}C_2) \cong (C_3{}^{3k} \rtimes C_3{}^k) \rtimes (C_{3^k-1} \times C_{3^k-1}) \cong ((C_3{}^{3k} \rtimes C_3{}^k) \rtimes C_{3^k-1}) \times C_{3^k-1}$. □

After submission of this paper, the authors became aware of [4]. In [4] the subgroup V_1 of $\mathcal{U}(\mathbb{F}_{3^k}D_6)$ is studied, where $V_1 = 1 + J(\mathbb{F}_{3^k}D_6)$ and $J(\mathbb{F}_{3^k}D_6)$ is the Jacobson radical of $\mathbb{F}_{3^k}D_6$. They show that V_1 and $V_1/Z(V_1)$ are both elementary Abelian 3-groups, where $Z(V_1)$ is the center of V_1.

References

[1] P.J. Davis, *Circulant Matrices*, Chelsea Publishing, New York (1979).

[2] J. Gildea, On the order of $\mathcal{U}(\mathbb{F}_{p^k}D_{2p^m})$, *Int. J. Pure Appl. Math.*, To Appear.

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

[4] M. Khan, R.K. Sharma, J.B. Srivastava, The unit group of FS_3, *Acta. Math. Acad. Paedagog. Nyházi.*, **23**, No. 2 (2007), 129-142.

[5] C. Polcino Milies, S.K. Sehgal, *An Introduction to Group Rings*, Kluwer Academic Publishers (2002).