International Journal of Pure and Applied Mathematics
Volume 46 No. 2 2008, 267-272

ON THE ORDER OF $\mathcal{U}(\mathbb{F}_{p^k} D_{2p^m})$

Joe Gildea
Department of Mathematics
National University of Ireland
University Road, Galway, IRELAND
e-mail: joseph.gildea@nuigalway.ie

Abstract: Let RG denote the group ring G of the group G over the ring R. Using an established isomorphism between RG and a certain ring of $n \times n$ matrices in conjunction with other techniques, we are able to establish the order of $\mathcal{U}(\mathbb{F}_{p^k} D_{2p^m})$, where p is an odd prime.

AMS Subject Classification: 20C05, 16S34, 15A15, 15A33
Key Words: group ring, group algebra, unit group, dihedral

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 form a group called the Unit Group of S, denoted by $\mathcal{U}(S)$. The homomorphism $\varepsilon : RG \longrightarrow R$ given by $\varepsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g$ 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 also a well known fact that $\mathcal{U}(RG) \cong \mathcal{U}(R) \times V(RG)$. For further details and background see Milies and Sehgal [4].

We are interested in the order of $\mathcal{U}(FG)$, where F is a field of characteristic p and G is a finite group. If G is a finite p-group and F is a field of characteristic p, then $V(FG)$ is a finite p-group of order $|F|^{|G|-1}$.

Let $M_n(R)$ be the ring of $n \times n$ matrices over R. Using an isomorphism

Received: December 18, 2007

between RG and a subring of $M_n(R)$ and other techniques, we establish the order of $\mathcal{U}(RG)$ when R is $\mathbb{F}_{p^k}$, the Galois field of p^k-elements, G is D_{2p^m}, the Dihedral Group of order $2p^m$, p is an odd prime and $m \in \mathbb{N}_0$. We establish the order of $\mathcal{U}(\mathbb{F}_{p^k}D_{2p^m})$ to be $p^{2k(p^m-1)}(p^k-1)^2$, where p is an odd prime and $m \in \mathbb{N}_0$. If $p = 2$, D_{2p^m} is a 2-group and the order of $\mathcal{U}(\mathbb{F}_{p^k}D_{2p^m})$ is known as already stated.

1.1. Background

Definition 1. A circulant matrix over a ring R is a square $n \times n$ matrix, which takes the form

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

where $a_i \in R$.

For further details on circulant matrices see Davis [2].

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 theorems can be found in [3].

Theorem 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 $\sigma : w \mapsto M(RG, w)$.*

Theorem 3. *Suppose R has an identity. Then $w \in RG$ is a unit if and only if $\sigma(w)$ is a unit in $M_n(R)$.*

Corollary 4. *When R is commutative, w is a unit in RG if and only if $\sigma(w)$ is a unit in $M_n(R)$ if and only if $\det(\sigma(w))$ is a unit in R.*

Example 5. *Let $C_n = \langle x \,|\, x^n = 1\rangle$ and $\alpha = \sum_{i=1}^{n} a_i x^{i-1} \in \mathbb{F}_{p^k}C_n$, where $a_i \in \mathbb{F}_{p^k}$ and p is a prime. Then $\sigma(\alpha) = \operatorname{circ}(a_1, a_2, \ldots, a_n)$.*

Example 6. *Let $D_{2n} = \langle x, y \,|\, x^n = 1, y^2 = 1, yx = x^{-1}y\rangle$ and $\kappa = \sum_{i=1}^{n} a_i x^{i-1} + \sum_{j=1}^{n} b_j x^{j-1} y \in \mathbb{F}_{p^k}D_{2n}$, 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 $A = \operatorname{circ}(a_1, a_2, \ldots, a_n)$ and $B = \operatorname{circ}(b_1, b_2, \ldots, b_n)$.

The following is known and can be found in [1].

Theorem 7. *Let A, B, C and D be $n \times n$ matrices. Then* $\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det(AD - BC)$ *if C and D commute.*

2. The Determinant of Circulant and Block Matrices with Circulant Blocks

Proposition 8. *Let $A = \operatorname{circ}(a_1, a_2, \ldots, a_{p^m})$, where $a_i \in \mathbb{F}_{p^k}$, p is a prime and $m \in \mathbb{N}_0$. Then*

$$\text{(i) } A^{p^m} = \sum_{i=1}^{p^m} {a_i}^{p^m} . I_{p^m}. \qquad \text{(ii) } \det(A) = \sum_{i=1}^{p^m} {a_i}^{p^m}.$$

Proof. (i) Let $\alpha = \sum_{i=1}^{p^m} a_i x^{i-1} \in \mathbb{F}_{p^k}C_{p^m}$, where p is a prime and $m \in \mathbb{N}_0$.

Now $\alpha^{p^m} = \left(\sum_{i=1}^{p^m} a_i x^{i-1}\right)^{p^m} = \sum_{i=1}^{p^m} {a_i}^{p^m} (x^{i-1})^{p^m} = \sum_{i=1}^{p^m} {a_i}^{p^m} (x^{p^m})^{i-1} = \sum_{i=1}^{p^m} {a_i}^{p^m}$.
Let $A = \operatorname{circ}(a_1, a_2, \ldots, a_{p^m}) = \sigma(\alpha)$, where σ is the isomorphism described in [3]. $\sigma(\alpha^{p^m}) = [\sigma(\alpha)]^{p^m}$, therefore $A^{p^m} = \operatorname{diag}_{p^m}\left(\sum_{i=1}^{p^m} {a_i}^{p^m}\right) = \sum_{i=1}^{p^m} {a_i}^{p^m} . I_{p^m}$.

(ii) $\det(A^{p^m}) = \det(A)^{p^m} = \left(\sum_{i=1}^{p^m} {a_i}^{p^m}\right)^{p^m}$, therefore $\det(A) = \sum_{i=1}^{p^m} {a_i}^{p^m}$. □

Proposition 9. *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*

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

Proof. 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 $A \pm B = \operatorname{circ}(a_1 \pm b_1, a_2 \pm b_2, \ldots, a_{p^m} \pm b_{p^m})$ and $\det(A \pm B) = \sum_{i=1}^{p^m} (a_i \pm b_i)^{p^m} = \sum_{i=1}^{p^m} ({a_i}^{p^m} \pm {b_i}^{p^m}) = \sum_{i=1}^{p^m} {a_i}^{p^m} \pm \sum_{i=1}^{p^m} {b_i}^{p^m} = \det(A) \pm \det(B)$. □

Proposition 10. *Let $M = \begin{pmatrix} A & B \\ B^T & A^T \end{pmatrix}$, where $A = \operatorname{circ}(a_1, a_2, \ldots, a_{p^m})$ and $B = \operatorname{circ}(b_1, b_2, \ldots, b_{p^m})$, where $a_i, b_j \in \mathbb{F}_{p^k}$ and p is an odd prime and $m \in \mathbb{N}_0$. Then*

$$\det(M) = (\det(A) + \det(B))(\det(A) - \det(B))$$

Proof. Let $M = \begin{pmatrix} A & B \\ B^T & A^T \end{pmatrix}$, where $A = \operatorname{circ}(a_1, a_2, \ldots, a_{p^m})$ and $B = \operatorname{circ}(b_1, b_2, \ldots, b_{p^m})$, where $a_i, b_j \in \mathbb{F}_{p^k}$, p is an odd prime and $m \in \mathbb{N}_0$.

$$\begin{aligned} \det(M) &= \det(AA^T - BB^T) \quad \text{by Theorem 7} \\ &= \det(AA^T) - \det(BB^T) \quad \text{by Proposition 9} \\ &= \det(A)^2 - \det(B)^2 = (\det(A) + \det(B))(\det(A) - \det(B)). \end{aligned}$$

□

3. The Order of $\mathcal{U}(\mathbb{F}_{p^k}D_{2p^m})$

Theorem 11. *$|\mathcal{U}(\mathbb{F}_{p^k}D_{2p^m})| = p^{2k(p^m-1)}(p^k-1)^2$ where p is an odd prime and $m \in \mathbb{N}_0$.*

Proof. $D_{2p^m} =< x, y \mid x^{p^m} = y^2 = 1,\ yx = x^{-1}y >$. Let $\kappa = \sum_{i=1}^{p^m} a_i x^{i-1} + \sum_{j=1}^{p^m} b_j x^{j-1}y \in \mathbb{F}_{p^k}D_{2p^m}$, where $a_i, b_j \in \mathbb{F}_{p^k}$, p is an odd prime and $m \in \mathbb{N}_0$. By [3], $\sigma(\kappa) = \begin{pmatrix} A & B \\ B^T & A^T \end{pmatrix}$, where $A = \mathrm{circ}(a_1, a_2, \ldots, a_{p^m})$ and $B = \mathrm{circ}(b_1, b_2, \ldots, b_{p^m})$. Now

$$\kappa \in \mathcal{U}(\mathbb{F}_{p^k}D_{2p^m}) \iff \det(\sigma(\kappa)) \neq 0 \iff \det\begin{pmatrix} A & B \\ B^T & A^T \end{pmatrix} \neq 0.$$

$\det\begin{pmatrix} A & B \\ B^T & A^T \end{pmatrix} = (\det(A) + \det(B))(\det(A) - \det(B))$. By Proposition 8, $\det(A) = \sum_{i=1}^{p^m} {a_i}^{p^m}$ and $\det(B) = \sum_{j=1}^{p^m} {b_j}^{p^m}$.

Let $A_1 = \left\{ \sum_{i=1}^{p^m} a_i x^{i-1} + \sum_{j=1}^{p^m} a_j x^{j-1}y \in \mathbb{F}_{p^k}D_{2p^m} \,\middle|\, \det(A) + \det(B) = 0 \right\}$ and $B_1 = \left\{ \sum_{i=1}^{p^m} a_i x^{i-1} + \sum_{j=1}^{p^m} a_j x^{j-1}y \in \mathbb{F}_{p^k}D_{2p^m} \,\middle|\, \det(A) - \det(B) = 0 \right\}$. First let's calculate the number of elements of $\mathbb{F}_{p^k}D_{2p^m}$ that satisfy $\det\begin{pmatrix} A & B \\ B^T & A^T \end{pmatrix} = 0$.

Clearly $|A_1| = (p^k)^{p^m}.(p^k)^{(p^m-1)} = p^{k(2p^m-1)}$ and similarly

$$|B_1| = (p^k)^{p^m}.(p^k)^{(p^m-1)} = p^{k(2p^m-1)}.$$

Every element of $A_1 \cap B_1$ satisfies $\sum_{i=1}^{p^m} {a_i}^{p^m} = 0$ and $\sum_{i=1}^{p^m} {b_i}^{p^m} = 0$. Thus there are $((p^k)^{(p^m-1)})((p^k)^{(p^m-1)}) = p^{2k(p^m-1)}$ elements that satisfy this condition.

Thus the number of elements that satisfy

$$\det\begin{pmatrix} A & B \\ B^T & A^T \end{pmatrix} = 0$$

is $\left(p^{k(2p^m-1)}+p^{k(2p^m-1)}\right)-p^{2k(p^m-1)} = 2p^{k(2p^m-1)}-p^{2k(p^m-1)}$. Now $\kappa \in \mathcal{U}(\mathbb{F}_{p^k}D_{2p^m}) \iff \det\begin{pmatrix} A & B \\ B^T & A^T \end{pmatrix} \neq 0$, thus the order of $\mathcal{U}(\mathbb{F}_{p^k}D_{2p^m})$ is equal the number of elements of $\mathbb{F}_{p^k}D_{2p^m}$ that satisfy $\det\begin{pmatrix} A & B \\ B^T & A^T \end{pmatrix} = 0$ subtracted from the size of $\mathbb{F}_{p^k}D_{2p^m}$. Therefore

$$\begin{aligned}|\mathcal{U}(\mathbb{F}_{p^k}D_{2p^m})| &= p^{2kp^m} - (2p^{k(2p^m-1)} - p^{2k(p^m-1)}) \\ &= p^{2k(p^m-1)}(p^{2k}-2p^k+1) = p^{2k(p^m-1)}(p^k-1)^2\,. \quad \square\end{aligned}$$

References

[1] M. Brookes, *The Matrix Reference Manual*, http://www.ee.is.ac.uk/hp/staff/dmb/matrix/intro.html (2005).

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

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

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