International Journal of Pure and Applied Mathematics

Volume 49 No. 4 2008, 525-530

ON THE ORDER OF $\mathcal{U}(\mathbb{F}_{2^k}D_{10})$ WHEN $5 \mid (2^k - 1)$

Joe Gildea

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

Abstract: Let $\mathcal{U}(RG)$ denote the unit group of the group ring 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 $\mathcal{U}(\mathbb{F}_{2^k}D_{10})$ when $5 \mid (2^k - 1)$.

AMS Subject Classification: 05C25
Key Words: unit group of the group ring, *LAGUNA* package,

1. Introduction

Let RG denote the group ring of the group G over the ring R. The set of all the invertible elements of a ring S form a group called the unit group of S, denoted by $\mathcal{U}(S)$. For further details and background see Polcino Milies and Sehgal [5].

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 order of $\mathcal{U}(RG)$ when R is $\mathbb{F}_{2^k}$, the Galois field of 2^k-elements, G is D_{10}, the Dihedral Group of order 10 and $5 \mid (2^k - 1)$. We establish the order of $\mathcal{U}(\mathbb{F}_{2^k}D_{10})$ to be $2^{3k}(2^k - 1)^5(2^k + 1)^2$ when $5 \mid (2^k - 1)$. In [4], the structure of $\mathcal{U}(\mathbb{F}_{2^k}D_6)$ is established.

Using the *LAGUNA* package, see [1], the order and structure of $\mathcal{U}(\mathbb{F}_{2^k}D_{10})$ can be determined for small cases.

Received: August 14, 2008

1.1. Background

Definition 1.1. 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 $a_i \in R$.

Definition 1.2. Let K be a field that contains a primitive root of unity ω of order n. The $n \times n$ Fourier matrix over K is defined to be:

$$\mathcal{F}_n = \frac{1}{\sqrt{n}} \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \omega & \omega^2 & \ldots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \ldots & \omega^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \omega^{n-2} & \ldots & \omega \end{pmatrix},$$

where $\sqrt{n}$ denotes an element of K (or an extension of K whose square is n).

Note that ${\mathcal{F}_n}^{-1}$ is obtained by replacing ω with ω^{-1} in $\mathcal{F}_n$.

Theorem 1.3. *Let C be a $n \times n$ circulant matrix over a field F. Then there exists a diagonal matrix D such that:*

$$C = \mathcal{F}_n D {\mathcal{F}_n}^{-1}.$$

Definition 1.4. Let A be a $m \times n$ matrix and B be a $p \times q$ matrix. Then the *tensor product* of A and B is that $mp \times nq$ matrix defined by

$$A \otimes B = \begin{pmatrix} a_{1,1}B & a_{1,2}B & \cdots & a_{1,n}B \\ a_{1,1}B & a_{1,2}B & \cdots & a_{1,n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1}B & a_{m,2}B & \cdots & a_{m,n}B \end{pmatrix}.$$

Definition 1.5. Let $CB_{m,n}$ be a $mn \times mn$ matrix:

$$CB_{m,n} = \begin{pmatrix} A_{1,1} & A_{1,2} & \dots & A_{1,m} \\ A_{2,1} & A_{2,2} & \dots & A_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ A_{m,1} & A_{m,2} & \dots & A_{m,m} \end{pmatrix}$$

where each $A_{i,j}$ block is an $n \times n$ circulant matrix.

We cannot diagonalise any $A \in CB_{m,n}$; however we can form a matrix with diagonal blocks (called DB) as follows :

$$DB = (I_m \otimes \mathcal{F}_n{}^{-1})A(I_m \otimes \mathcal{F}_n)\,.$$

See [2] for further details on circulant matrices.

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

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

is called the matrix of G (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:

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

is called the RG-matrix of w and is denoted by $M(RG, w)$. The following can be found in [3].

Theorem 1.6. *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 1.7. *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 1.8. *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 1.9. 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 $A = \mathrm{circ}(a_0, a_1, \ldots, a_{n-1})$ and $B = \mathrm{circ}(b_1, b_2, \ldots, b_{n-1})$.

2. The Order of $\mathcal{U}(\mathbb{F}_{2^k} D_{10})$ when $5 \,|\, (2^k - 1)$

Lemma 2.1. *$|\mathcal{U}(\mathbb{F}_{2^k} D_{10})| = 2^{3k}(2^k - 1)^5(2^k + 1)^2$ when $5 \,|\, (2^k - 1)$.*

Proof. Let $\alpha = \sum_{i=0}^{4} a_i x^i + \sum_{j=0}^{4} b_j\, x^j y \in \mathbb{F}_{2^k} D_{10}$, where $a_i \in \mathbb{F}_{2^k}$. By [3], $\sigma(\alpha) = \begin{pmatrix} A & B \\ B^T & A^T \end{pmatrix}$ where $A = \mathrm{circ}(a_0, a_1, a_2, a_3, a_4)$ and $B = \mathrm{circ}(b_0, b_1, b_2, b_3, b_4)$. Now $\alpha \in \mathcal{U}(\mathbb{F}_{2^k} D_{10}) \iff det(\sigma(\alpha)) \neq 0 \iff \begin{vmatrix} A & B \\ B^T & A^T \end{vmatrix} \neq 0$.

If $5 \,|\, (2^k - 1)$, then $\mathbb{F}_{2^k}$ contains a primitive root of unity of order 5 and let us call it ω. Thus we can block diagonalize $\sigma(\alpha)$ as follows:

$$(I_2 \otimes {\mathcal{F}_5}^{-1})\sigma(\alpha)(I_2 \otimes \mathcal{F}_5) = \begin{pmatrix} {\mathcal{F}_5}^{-1} A \mathcal{F}_5 & {\mathcal{F}_5}^{-1} B \mathcal{F}_5 \\ {\mathcal{F}_5}^{-1} B^T \mathcal{F}_5 & {\mathcal{F}_5}^{-1} A^T \mathcal{F}_5 \end{pmatrix} = \begin{pmatrix} D_1 & D_2 \\ D_3 & D_4 \end{pmatrix},$$

where

$$\begin{aligned} D_1 &= \mathrm{diag}(\rho_1(1), \rho_1(\omega), \rho_1(\omega^2), \rho_1(\omega^3), \rho_1(\omega^4)), \\ D_2 &= \mathrm{diag}(\rho_2(1), \rho_2(\omega), \rho_2(\omega^2), \rho_2(\omega^3), \rho_2(\omega^4)), \\ D_3 &= \mathrm{diag}(\rho_2(1), \rho_2(\omega^4), \rho_2(\omega^3), \rho_2(\omega^2), \rho_2(\omega)), \\ D_4 &= \mathrm{diag}(\rho_1(1), \rho_1(\omega^4), \rho_1(\omega^3), \rho_1(\omega^2), \rho_1(\omega)), \end{aligned}$$

$\rho_1(\omega) = \sum_{i=0}^{4} a_i \omega^i$ and $\rho_2(\omega) = \sum_{j=0}^{4} b_j\, \omega^j$. Therefore

$$\begin{aligned} det(\sigma(\alpha)) &= (\rho_1(1)^2 - \rho_2(1)^2)(\rho_1(\omega)\rho_1(\omega^4) \\ &\quad - \rho_2(\omega)\rho_2(\omega^4))^2(\rho_1(\omega^2)\rho_1(\omega^3) - \rho_2(\omega^2)\rho_2(\omega^3))^2 \\ &= (\rho_1(1)+\rho_2(1))^2(\rho_1(\omega)\rho_1(\omega^4)+\rho_2(\omega)\rho_2(\omega^4))^2(\rho_1(\omega^2)\rho_1(\omega^3)+\rho_2(\omega^2)\rho_2(\omega^3))^2. \end{aligned}$$

Let

$$A_1=\left\{\sum_{i=0}^{4}a_ix^i+\sum_{j=0}^{4}b_j\,x^jy\in\mathbb{F}_{2^k}D_{10}\,|\,(\rho_1(1)+\rho_2(1))^2=0\right\},$$

$$A_2=\left\{\sum_{i=0}^{4}a_ix^i+\sum_{j=0}^{4}b_j\,x^jy\in\mathbb{F}_{2^k}D_{10}\,|\,(\rho_1(\omega)\rho_1(\omega^4)-\rho_2(\omega)\rho_2(\omega^4))^2=0\right\},$$

$$A_3=\left\{\sum_{i=0}^{4}a_ix^i+\sum_{j=0}^{4}b_j\,x^jy\in\mathbb{F}_{2^k}D_{10}\,|\,(\rho_1(\omega^2)\rho_1(\omega^3)-\rho_2(\omega^2)\rho_2(\omega^3))^2=0\right\}.$$

First let us calculate the number of elements of $\mathbb{F}_{2^k}D_{10}$ that satisfy $det(\sigma(\alpha))=0$. We do this by the principle of Inclusion-Exclusion, i.e.

$$|A_1\cup A_2\cup A_3|=\sum_{i=1}^{3}|A_i|-\sum_{i\neq j}|A_i\cap A_j|+|A_1\cap A_2\cap A_3|.$$

$\underline{|\boldsymbol{A_1}|}$ $(\rho_1(1)+\rho_2(1))^2=0\Longleftrightarrow\sum_{i=0}^{4}(a_i+b_i)=0$. Thus $|A_1|=(2^k)^9=2^{9k}$.

$\underline{|\boldsymbol{A_2}|}$

$$\begin{aligned}(\rho_1(\omega)\rho_1(\omega^4)+\rho_2(\omega)\rho_2(\omega^4))^2=0&\\ \Longleftrightarrow\ \rho_1(\omega)\rho_1(\omega^4)=\rho_2(\omega)\rho_2(\omega^4)&\\ \Longleftrightarrow\ \rho_1(\omega)\rho_1(\omega^4)=0\wedge\rho_2(\omega)\rho_2(\omega^4)=0&\\ \text{or}\quad\rho_1(\omega)\rho_1(\omega^4)=1\wedge\rho_2(\omega)\rho_2(\omega^4)=1&\\ \text{or}\quad\rho_1(\omega)\rho_1(\omega^4)=a\ \wedge\rho_2(\omega)\rho_2(\omega^4)=a&\\ \vdots&\\ \text{or}\quad\rho_1(\omega)\rho_1(\omega^4)=a^{2^k-2}\wedge\rho_2(\omega)\rho_2(\omega^4)=a^{2^k-2},&\end{aligned}$$

where a generates $\mathcal{U}(\mathbb{F}_{2^k})$.

$\underline{\rho_1(\omega)\rho_1(\omega^4)=0\wedge\rho_2(\omega)\rho_2(\omega^4)=0}$.

The number of elements of $\mathbb{F}_{2^k}D_{10}$ that satisfies $\rho_1(\omega)\rho_1(\omega^4)=0$ is $2^{4k}+2^{4k}-2^{3k}=2^{4k+1}-2^{3k}$. Thus the number of elements that satisfy $\rho_1(\omega)\rho_1(\omega^4)=0\wedge\rho_2(\omega)\rho_2(\omega^4)=0$ is $(2^{4k+1}-2^{3k})^2$.

$\underline{\rho_1(\omega)\rho_1(\omega^4)=1\wedge\rho_2(\omega)\rho_2(\omega^4)=1}$,

$$\begin{aligned}\rho_1(\omega)\rho_1(\omega^4)=1\Longleftrightarrow\rho_1(\omega)=1\wedge\rho_1(\omega^4)=1&\\ \text{or}\quad\rho_1(\omega)=a\wedge\rho_1(\omega^4)=a^{-1}&\end{aligned}$$

$$\vdots$$

$$\text{or} \quad \rho_1(\omega) = a^{2^k-2} \wedge \rho_1(\omega^4) = (a^{2^k-2})^{-1}$$

The number of elements of $\mathbb{F}_{2^k}D_{10}$ that satisfies $\rho_1(\omega)\rho_1(\omega^4) = 1$ is $(2^k - 1)(2^{3k}) = 2^{4k} - 2^{3k}$. Thus the number of elements that satisfy $\rho_1(\omega)\rho_1(\omega^4) = 1 \wedge \rho_2(\omega)\rho_2(\omega^4) = 1$ is $(2^{4k} - 2^{3k})^2$.

$\underline{\rho_1(\omega)\rho_1(\omega^4) = a^t \wedge \rho_2(\omega)\rho_2(\omega^4) = a^t \text{ where } 1 \leq t \leq 2^k - 2.}$

Similarly the number of elements of $\mathbb{F}_{2^k}D_{10}$ that satisfies $\rho_1(\omega)\rho_1(\omega^4) = a^t \wedge \rho_2(\omega)\rho_2(\omega^4) = a^t$ where $1 \leq t \leq 2^k - 2$ is $(2^{4k} - 2^{3k})^2$.

Therefore $|A_2| = (2^{4k+1} - 2^{3k})^2 + (2^k - 1)(2^{4k} - 2^{3k})^2 = 2^{9k} + 2^{8k} - 2^{7k}$.

Using similar counting arguments, it can be shown that $|A_3| = |A_2|$, $|A_1 \cap A_2| = |A_1 \cap A_3| = 2^{8k} + 2^{7k} - 2^{6k}$, $|A_2 \cap A_3| = 2^{8k} + 2^{7k+1} - 2^{6k} - 2^{5k+1} + 2^{4k}$ and $|A_1 \cap A_2 \cap A_3| = 2^{7k} + 2^{6k+1} - 2^{5k} - 2^{4k+1} + 2^{3k}$.

Therefore the number of element of $\mathbb{F}_{2^k}D_{10}$ that satisfy $det(\sigma(\alpha)) = 0$ is $3.2^{9k} - 2^{8k} - 5.2^{7k} + 5.2^{6k} + 2^{5k} - 3.2^{4k} + 2^{3k}$. Thus the order of $\mathcal{U}(\mathbb{F}_{2^k}D_{10})$ when $5 \,|\, (2^k - 1)$ is equal to the number of elements of $\mathbb{F}_{2^k}D_{10}$ that satisfy $det(\sigma(\alpha)) = 0$ subtracted from the order of $\mathbb{F}_{2^k}D_{10}$.

Therefore

$$\begin{aligned} |\mathcal{U}(\mathbb{F}_{2^k}D_{10})| &= 2^{10k} - (3.2^{9k} - 2^{8k} - 5.2^{7k} + 5.2^{6k} + 2^{5k} - 3.2^{4k} + 2^{3k}) \\ &= 2^{3k}(2^k - 1)^5(2^k + 1)^2 \quad \text{when } 5 \,|\, (2^k - 1). \end{aligned}$$

References

[1] V. Bovdi, A. Konovalov, R. Rossmanith, C. Schneider, *LAGUNA – Lie Algebras and UNits of group Algebras*, Version 3.4 (2007), http://www.cs.st-andrews.ac.uk/ alexk/laguna.htm.

[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] 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).