www.theoryofgroups.ir

International Journal of Group Theory
ISSN (print): 2251-7650, ISSN (on-line): 2251-7669
Vol. 3 No. 4 (2014), pp. 13-16.

www.ui.ac.ir

THE UNIT GROUP OF ALGEBRA OF CIRCULANT MATRICES

N. MAKHIJANI*, R. K. SHARMA AND J. B. SRIVASTAVA

Communicated by Evgeny Vdovin

Abstract. Let $Cr_n(F)$ denote the algebra of $n \times n$ circulant matrices over the field F. In this paper, we study the unit group of $Cr_n(\mathbb{F}_{p^m})$, where $\mathbb{F}_{p^m}$ denotes the Galois field of order p^m, p prime.

1. Introduction

Throughout this paper, all the rings considered are associative with identity $1 \neq 0$. The set of all invertible elements of a ring R form a group $\mathcal{U}(R)$, called the unit group of R. Let RG be the group ring of the group G over the ring R. A lot is known about the unit group of group rings of finite groups [1, 2, 3, 4, 5, 6, 7, 8, 12, 13].

A circulant matrix over the ring R is an $n \times n$ matrix of the form

$$circ(\alpha_0, \dots, \alpha_{n-1}) = \begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \cdots & \alpha_{n-1} \\ \alpha_{n-1} & \alpha_0 & \alpha_1 & \cdots & \alpha_{n-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_0 \end{pmatrix}, \ \alpha_i \in R$$

Let $C_n = \langle\, a \mid a^n \,\rangle$. The idea that any element of the group ring RC_n can be written as a circulant matrix over R was introduced by Hurley in [7]. In fact, if $Cr_n(R)$ is the ring of $n \times n$ circulant matrices over R, then

$$\sigma : RC_n \to Cr_n(R)$$

MSC(2010): Primary: 16U60; Secondary: 20C05.

Keywords: Group Algebra, Unit Group, Circulant Matrices.

Received: 24 October 2013, Accepted: 7 March 2014.

*Corresponding author.

defined by $\sigma\left(\sum_{i=0}^{n-1}\alpha_i a^i\right) = circ\left(\alpha_0, \ldots, \alpha_{n-1}\right)$ is an isomorphism. Therefore the study of units in RC_n suffices to establish the structure of the unit group of $Cr_n(R)$.

Let p be any prime number. In [12], Sharma and Yadav computed the order of the unit groups of some semi-simple algebras of circulant matrices over Galois fields of prime order. In continuation to this investigation, we study the unit group of the $\mathbb{F}_{p^m}$-algebra $Cr_n\left(\mathbb{F}_{p^m}\right)$.

2. Units in $Cr_n\left(\mathbb{F}_{p^m}\right)$

If the $\mathbb{F}_{p^m}$-algebra $Cr_n\left(\mathbb{F}_{p^m}\right)$ is semi-simple, the structure of its unit group is given by the following result which is a consequence of the well known theorem by Perlis and Walker about the structure of semi-simple group algebras of abelain groups.

Theorem 2.1. *If $(n,p)=1$ and $q=p^m$, then*

$$\mathcal{U}\left(Cr_n\left(\mathbb{F}_q\right)\right) \cong C_{q-1} \times \left(\prod_{\substack{l|n \\ l>1}} C_{q^{d_l}-1}^{\ e_l}\right)$$

where d_l is the multiplicative order of q modulo l and $e_l = \dfrac{\varphi(l)}{d_l}$.

Proof. Using [10, Theorem 1] and [9, Theorem 2.21, pp. 53], it follows that

$$\mathbb{F}_q C_n \cong \mathbb{F}_q \ \oplus \ \bigoplus_{\substack{l|n \\ l>1}} \mathbb{F}_{q^{d_l}}^{\ e_l} \tag{2.1}$$

and hence the proof. □

Remark 2.2. The results in [12] can be obtained using Theorem 2.1.

Now consider the case when $p \mid n$.

Lemma 2.3. *Let $k \in \mathbb{N}$. Then*

$$\mathcal{U}\left(\mathbb{F}_{p^m}C_{p^k}\right) \cong \begin{cases} C_p^{m(p-1)} \times C_{p^m-1} & \text{if } k=1 \\ \prod_{t=1}^{k} C_{p^t}^{n_t} \ \times \ C_{p^m-1} & \text{otherwise} \end{cases}$$

where $n_k = m(p-1)$ and $n_t = mp^{k-t-1}(p-1)^2 \ \forall\ t,\ 1 \le t < k$.

Proof. As a direct consequence of Wedderburn Malcev theorem, it follows that

$$\mathcal{U}(\mathbb{F}_{p^m}C_{p^k}) \cong (1+\Delta(C_{p^k})) \times \mathbb{F}_{p^m}^*$$

where $\Delta(C_{p^k})$ is the augmentation ideal of $\mathbb{F}_{p^m}C_{p^k}$.

It is obvious that $\mathcal{U}\left(\mathbb{F}_{p^m}C_p\right) \cong C_p^{m(p-1)} \times C_{p^m-1}$. Now suppose that $k \ge 2$.

If $C_{p^k} = \langle\ a \mid a^{p^k}\ \rangle$, then every element $X \in \Delta(C_{p^k})$ is expressible as

$$X = \sum_{i=1}^{p-1} \sum_{j=0}^{k-1} \sum_{l=0}^{p^{k-j-1}-1} \beta_{i,j,l} \left(a^{p^j(lp+i)} - 1\right)$$

for some $\beta_{i,j,l} \in \mathbb{F}_{p^m}$.

For any $t,\ 1 \leq t \leq k-1$,

$$\begin{aligned}
& (1+X)^{p^t} = 1 \\
\Leftrightarrow\ & X^{p^t} = 0 \\
\Leftrightarrow\ & \sum_{i=1}^{p-1} \sum_{j=0}^{k-1} \sum_{l=0}^{p^{k-j-1}-1} \beta_{i,j,l}^{p^t} \left(a^{p^{j+t}(lp+i)} - 1\right) = 0 \\
\Leftrightarrow\ & \sum_{i=1}^{p-1} \sum_{j=0}^{k-t-1} \sum_{l=0}^{p^{k-j-1}-1} \beta_{i,j,l}^{p^t} \left(a^{p^{j+t}(lp+i)} - 1\right) = 0 \\
\Leftrightarrow\ & \sum_{i=1}^{p-1} \sum_{j=0}^{k-t-1} \sum_{l=0}^{p^{k-j-t-1}-1} \left(\sum_{s=0}^{p^t-1} \beta_{i,j,l+sp^{k-j-t-1}}\right)^{p^t} \left(a^{p^{j+t}(lp+i)} - 1\right) = 0 \\
\Leftrightarrow\ & \sum_{s=0}^{p^t-1} \beta_{i,j,l+sp^{k-j-t-1}} = 0\ \forall\ 1 \leq i \leq p-1,\ 0 \leq j \leq k-t-1,\ 0 \leq l \leq p^{k-j-t-1}-1
\end{aligned}$$

Thus from above, we conclude that for any $t,\ 1 \leq t \leq k-1$, the number of elements of order $\leq p^t$ in $1 + \Delta(C_{p^k})$ is p^{mN_t}, where

$$\begin{aligned}
N_t &= \left(p^t - 1\right)(p-1) \sum_{j=0}^{k-t-1} p^{k-j-t-1} + (p-1) \sum_{j=k-t}^{k-1} p^{k-j-1} \\
&= \left(p^t - 1\right)\left(p^{k-t} - 1\right) + \left(p^t - 1\right) \\
&= \left(p^t - 1\right) p^{k-t}
\end{aligned}$$

If $1 + \Delta(C_{p^k}) = \prod_{i=1}^{k} C_{p^i}^{n_i}$, then

$$\begin{aligned}
& \sum_{i=1}^{t} i n_i + t \sum_{t+1}^{k} n_i = mN_t\ \forall\ t,\ 1 \leq t \leq k-1 \\
\text{and}\quad & \sum_{i=1}^{k} i n_i = m(p^k - 1) = mN_k\ (\text{say})
\end{aligned}$$

Solving the above system of equations over $\mathbb{F}_{p^m}$, we get $n_1 = m(2N_1 - N_2) = mp^{k-2}(p-1)^2,\ n_k = m(N_k - N_{k-1}) = m(p-1)$ and $n_t = m(2N_t - N_{t-1} - N_{t+1}) = mp^{k-t-1}(p-1)^2$ for all $1 < t < k$. $\square$

Theorem 2.4. *Let $n = p^k n_1$, where $(n_1, p) = 1$ and $k \geq 1$. Then*

$$\mathcal{U}\left(Cr_n(\mathbb{F}_{p^m})\right) \cong \mathcal{U}\left(\mathbb{F}_{p^m} C_{p^k}\right) \times \left(\prod_{\substack{l \mid n_1 \\ l > 1}} \mathcal{U}\left(\mathbb{F}_{p^{md_l}} C_{p^k}\right)^{e_l} \right)$$

where d_l is the multiplicative order of p^m modulo l and $e_l = \dfrac{\varphi(l)}{d_l}$.

Proof. Observe that

$$\begin{aligned} Cr_n(\mathbb{F}_{p^m}) &\cong \mathbb{F}_{p^m}(C_{n_1} \times C_{p^k}) \\ &\cong (\mathbb{F}_{p^m} C_{n_1})\, C_{p^k} \\ &\cong \mathbb{F}_{p^m} C_{p^k} \oplus \bigoplus_{\substack{l \mid n_1 \\ l > 1}} \left(\mathbb{F}_{p^{md_l}} C_{p^k}\right)^{e_l} \text{ by equation (2.1)} \end{aligned}$$

Using this and Lemma 2.3, the structure of the unit group of $Cr_n(\mathbb{F}_{p^m})$ can be obtained. □

References

[1] V. Bovdi, On symmetric units in group algebras, *Comm. Algebra*, **29** no. 12 (2001) 5411–5422.

[2] V. Bovdi, Group rings in which the group of units is hyperbolic, *J. Group Theory*, **15** no. 2 (2012) 227–235.

[3] L. Creedon and J. Gildea, The Structure of the Unit Group of the Group Algebra $\mathbb{F}_{2^k} D_8$, *Canad. Math. Bull.*, **54** no. 2 (2011) 237-243.

[4] J. Gildea, The special circulant matrix and units in group rings, *Acta Math. Acad. Paedagog. Nyhazi.*, **24** no. 2 (2008) 221–225.

[5] J. Gildea, The structure of the unit group of the group algebra $\mathbb{F}_{3^k}(C_3 \times D_6)$, *Comm. Algebra*, **38** no. 9 (2010) 3311–3317.

[6] J. Gildea, Units of the group algebra $\mathbb{F}_{2^k}(C_2 \times D_8)$, *J. Algebra Appl.*, **10** no. 4 (2011) 643–647.

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

[8] K. Kaur and M. Khan, Units in $F_2 D_{2p}$, *J. Algebra Appl.*, **13** no. 2 (2014) DOI: 10.1142/S0219498813500904.

[9] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, 2000.

[10] S. Perlis and G. L. Walker, Abelian group algebras of finite order, *Trans. Amer. Math. Soc.*, **68** no. 3 (1950) 420-426

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

[12] R. K. Sharma and P. Yadav, Unit group of algebra of circulant matrices, *Int. J. Group Theory*, **2** no. 4 (2013) 1–6.

[13] R. K. Sharma, P. Yadav and K. Joshi, Units in $\mathbb{Z}_2(C_2 \times D_\infty)$, *Int. J. Group Theory*, **1** no. 4 (2012) 33–41.

Neha Makhijani
Department of Mathematics, Indian Institute of Technology Delhi, New Delhi, India
Email: `nehamakhijani@gmail.com`

R. K. Sharma
Department of Mathematics, Indian Institute of Technology Delhi, New Delhi, India
Email: `rksharmaiitd@gmail.com`

J. B. Srivastava
Department of Mathematics, Indian Institute of Technology Delhi, New Delhi, India
Email: `jbsrivas@gmail.com`