THE UNIT GROUP OF ALGEBRA OF CIRCULANT MATRICES

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

Communicated by Evgeny Vdovin

Abstract. Let $C_{r_n}(F)$ denote the algebra of $n \times n$ circulant matrices over the field $F$. In this paper, we study the unit group of $C_{r_n}(F_{p^m})$, where $F_{p^m}$ 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 $U(R)$, 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

$$
circ(a_0, \ldots, a_{n-1}) = \begin{pmatrix}
\alpha_0 & \alpha_1 & \alpha_2 & \cdots & \alpha_{n-1} \\
\alpha_{n-1} & \alpha_0 & \alpha_1 & \cdots & \alpha_{n-2} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_0 
\end{pmatrix}, \quad \alpha_i \in R
$$

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 $C_{r_n}(R)$ is the ring of $n \times n$ circulant matrices over $R$, then

$$
\sigma : RC_n \to C_{r_n}(R)
$$

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 \( \sigma \left( \sum_{i=0}^{n-1} \alpha_i a^i \right) = \text{circ} (\alpha_0, \ldots, \alpha_{n-1}) \) is an isomorphism. Therefore the study of units in \( R C_n \) 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 \( Cr_n(\mathbb{F}_{p^m}) \).

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

If the \( \mathbb{F}_{p^m} \)-algebra \( Cr_n(\mathbb{F}_{p^m}) \) 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 abelian groups.

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

\[
\mathcal{U}(Cr_n(\mathbb{F}_q)) \cong C_{q-1} \times \left( \prod_{l | n, l > 1} C^{e_l}_{q^{d_l-1}} \right)
\]

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

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

\[
\mathbb{F}_q C_n \cong \mathbb{F}_q \oplus \bigoplus_{l | n, l > 1} \mathbb{F}_{q^{d_l}}^{e_l}
\]

and hence the proof. \( \square \)

**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

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

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

**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 \( \mathcal{U}(\mathbb{F}_{p^m} C_{p}) \cong C_p^{m(p-1)} \times C_{p^m-1} \). Now suppose that \( k \geq 2 \).
If \( C_{p^k} = \langle a \mid a^{p^k} \rangle \), then every element \( X \in \Delta(C_{p^k}) \) is expressible as

\[
X = \sum_{i=1}^{p-1} \sum_{j=0}^{k-1} \sum_{l=0}^{p^{k-j-1} - 1} \beta_{i,j,l} (a^{p^j(lp^i)} - 1)
\]

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

For any \( t, \ 1 \leq t \leq k-1 \),

\[
(1 + X)^{p^t} = 1
\]

\[\Leftrightarrow \quad X^{p^t} = 0 \]

\[\Leftrightarrow \quad \sum_{i=1}^{p-1} \sum_{j=0}^{k-1} \sum_{l=0}^{p^{k-j-1} - 1} \beta_{i,j,l} (a^{p^{j+t}(lp^i)} - 1) = 0 \]

\[\Leftrightarrow \quad \sum_{i=1}^{p-1} \sum_{j=0}^{k-1} \sum_{l=0}^{p^{k-j-1} - 1} \beta_{i,j,l} (a^{p^{j+t}(lp^i)} - 1) = 0 \]

\[\Leftrightarrow \quad \sum_{i=1}^{p-1} \sum_{j=0}^{k-1} \sum_{l=0}^{p^{k-j-1} - 1} \left( \sum_{s=0}^{p^{j+t} - 1} \beta_{i,j,l+sp^k+j-t-1} \right) (a^{p^{j+t}(lp^i)} - 1) = 0 \]

\[\Leftrightarrow \quad \sum_{s=0}^{p^{j+t} - 1} \beta_{i,j,l+sp^k+j-t-1} = 0 \ \forall \ 1 \leq i \leq p-1, \ 0 \leq j \leq k-t-1, \ 0 \leq l \leq p^{k-j-t-1} - 1 \]

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

\[
N_t = (p^t - 1) (p - 1) \sum_{j=0}^{k-t-1} p^{k-j-t-1} + (p - 1) \sum_{j=k-t}^{k-1} p^{k-j-1}
\]

\[
= (p^t - 1) (p^{k-t} - 1) + (p^t - 1)
\]

\[
= (p^t - 1) p^{k-t}
\]

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

\[
\sum_{i=1}^{t} in_i + t \sum_{i=1}^{k} n_i = mN_t \ \forall \ t, \ 1 \leq t \leq k-1
\]

and

\[
\sum_{i=1}^{k} in_i = m(p^k - 1) = mN_k \ (\text{say})
\]

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 \( 1 < t < k \). □
Theorem 2.4. Let \( n = p^k n_1 \), where \((n_1, p) = 1\) and \( k \geq 1 \). Then

\[
\mathcal{U}(Cr_n(F_{p^m})) \cong \mathcal{U}(\mathbb{F}_{p^m} C_{p^k}) \times \left( \prod_{l | n_1, l > 1} \mathcal{U}(\mathbb{F}_{p^{md_l}} C_{p^k})^{e_l} \right)
\]

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

Proof. Observe that

\[
Cr_n(F_{p^m}) \cong \mathbb{F}_{p^m}(C_{n_1} \times C_{p^k})
\]

\[
\cong (\mathbb{F}_{p^m} C_{n_1}) C_{p^k}
\]

\[
\cong \mathbb{F}_{p^m} C_{p^k} \oplus \bigoplus_{l | n_1, l > 1} \left( \mathbb{F}_{p^{md_l}} C_{p^k} \right)^{e_l} \text{ by equation (2.1)}
\]

Using this and Lemma 2.3, the structure of the unit group of \( Cr_n(F_{p^m}) \) can be obtained. \( \square \)

References


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