www.theoryofgroups.ir

International Journal of Group Theory
ISSN (print): 2251-7650, ISSN (on-line): 2251-7669
Vol. 2 No. 4 (2013), pp. 1-6.
© 2013 University of Isfahan

www.ui.ac.ir

UNIT GROUP OF ALGEBRA OF CIRCULANT MATRICES

R. K. SHARMA* AND POOJA YADAV

Communicated by Victor Bovdi

ABSTRACT. Let $Cr_n(F_p)$ denote the algebra of $n \times n$ circulant matrices over F_p, the finite field of order p a prime. The order of the unit groups $\mathcal{U}(Cr_3(F_p))$, $\mathcal{U}(Cr_4(F_p))$ and $\mathcal{U}(Cr_5(F_p))$ of algebras of circulant matrices over F_p are computed.

1. Introduction

Throughout this paper, a ring R will denote a nontrivial associative ring with identity 1. The set of all invertible elements of a ring R form a group called the unit group of R denoted by $\mathcal{U}(R)$. Let C_n denote the cyclic group of order n and RC_n denote the group ring of group C_n over the ring R. If $R = K$ is a field then KG is the group algebra of G over the field K. V. Bovdi ([1],[3]) has done a lot of work on units in integral group ring and group algebras.

A circulant matrix or simply a circulant over a ring R is a square $n \times n$ matrix which takes the form:

$$circ(a_1, \ldots, a_n) = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_n \\ a_n & a_1 & a_2 & \ldots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \ldots & a_{n-2} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_2 & a_3 & a_4 & \ldots & a_1 \end{pmatrix} \qquad (a_i \in R).$$

The set of all $n \times n$ circulant matrices over a ring R will be denoted by $Cr_n(R)$.
Let R be a ring and C_n be the cyclic group of order n. Then

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

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

Keywords: Algebra, Unit group, Circulant matrices.

Received: 28 September 2012, Accepted: 22 February 2013.

*Corresponding author .

defined by $\sigma\left(\sum_{i=0}^{n-1} a_i g^i\right) = circ(a_0, a_1, ..., a_{n-1})$ is an isomorphism from RC_n to $Cr_n(R)$ i.e. the circulant matrices of order n over ring R; see [10] for details.

Gildea in [7] determines the order of $\mathcal{U}(F_{r^k}C_p)$ where r^k is of the form $p^k + 1$. The next result can be found in [7] and [6].

Theorem 1.1. *Let $\alpha_n = (1 + (n-1)a) + (1-a)(\sum_{i=1}^{n-1} x^i) \in F_{p^n}C_n$ where a generates $\mathcal{U}(F_{p^n})$, p is a prime and $C_n = \langle x | x^n = 1\rangle$. If $p \not| n$ then*

(i) $\langle \alpha_n \rangle \cong C_{p^n-1}$;
(ii) $\mathcal{U}(F_{p^n}C_2) = \langle \alpha_2, a\rangle$.

We shall use the following

Theorem 1.2. ***[Maschke]*** *Let G be a group and R a ring with identity. Then, the group ring RG is semisimple if and only if the following conditions hold:*

(i) *R is a semisimple ring.*
(ii) *G is finite.*
(iii) *$|G|$ is invertible in R.*

Theorem 1.3. *Let G be a finite group and K a field such that char $K \nmid |G|$. Then*

$$KG \cong \oplus_{i=1}^{s} M_{n_i}(D_i) \cong K \oplus \left(\oplus_{i=1}^{s-1} M_{n_i}(D_i)\right)$$

Theorem 1.4 (Higman's Theorem)**.** *Let G be an abelian group of order n and K a field such that char $K \nmid n$. If K contains a primitive root of unity of order n then*

$$KG \cong \underbrace{K \oplus ... \oplus K}.$$

2. Unit Group of $Cr_n(F_q)$

Theorem 2.1. $|\mathcal{U}(Cr_3(F_{p^k})| = \begin{cases} (p^k-1)^3 & \text{when } 3|(p^k-1) \\ (p^k-1)^2(p^k+1) & \text{when } 3 \nmid (p^k-1) \text{ and } p \neq 3. \end{cases}$

Proof. For $p \neq 3$, p does not divide 3 and hence from Mashke's theorem $F_{p^k}C_3$ is semisimple. Thus from Theorem 1.4, $F_{p^k}C_3 \cong F_{p^k} \oplus A$. Now either $F_{p^k}C_3 \cong F_{p^k} \oplus F_{p^k} \oplus F_{p^k}$ or $F_{p^k}C_3 \cong F_{p^k} \oplus F_{(p^k)^2}$ by counting dimensions. By Theorem 1.4, $F_{p^k}C_3 \cong F_{p^k} \oplus F_{p^k} \oplus F_{p^k}$ when $3|(p^k-1)$ and thus $|\mathcal{U}(Cr_3(F_{p^k})| = (p^k-1)^3$. Otherwise when $3 \nmid (p^k-1)$, $F_{p^k}C_3 \cong F_{p^k} \oplus F_{(p^k)^2}$ and $|\mathcal{U}(Cr_3(F_{p^k})| = (p^k-1)^2(p^k+1)$ □

Theorem 2.2. *$\mathcal{U}(Cr_3(F_p)) = \langle A, \alpha_3$, where $A = \alpha x$, α is a primitive $(p-1)^{th}$ root of unity in F_p and $\alpha_3 = circ(1+2\alpha, 1-\alpha, 1-\alpha)$, $p \neq 3$ and p is of the form $(3k-1)$ for some integer k.*

Proof. Let $A = \alpha x = circ(0, \alpha, 0)$, α is a primitive root mod p. As $A^p = (\alpha x)^p = \alpha x^p$ and thus $A^{p^2} = \alpha x = A$ so we have $A^{p^2-1} = 1$. Now suppose if $A^n = 1$ for $n < p^2 - 1$, then $\alpha^n x^n = 1$ that gives $\alpha^n = 1$ which implies n is a multiple of $p-1$ and also $x^n = 1$ gives $n \geq p^2 - 1$. Thus the order of A

is p^2-1. Any arbitrary power of A is either of the form $circ(\alpha^i,0,0)$ or $circ(0,\alpha^i,0)$ or $circ(0,0,\alpha^i)$. The order of α_3 is $p-1$ as given in [2]. Also from [2], ${\alpha_3}^n = 3^{n-2}circ(1+2\alpha^n, 1-\alpha^n, 1-\alpha^n)$. Clearly, no power of α_3 is in $\{A^i | 0 \leq i \leq p^2-2\}$. Hence the result. □

Theorem 2.3. $|\mathcal{U}(Cr_4(F_p^k))| = \begin{cases} (p^k-1)^4 & \text{when } 4|(p^k-1) \\ (p^k+1)(p^k-1)^3 & \text{when } 4 \nmid (p^k-1) \text{ and } p \neq 2. \end{cases}$

Proof. When $p \neq 2$, from Mashke's theorem $F_{p^k}C_4$ is semisimple and $F_{p^k}C_4 \cong F_{p^k} \oplus A$ by Theorem 1.4. Now $F_{p^k}C_4 \cong F_{p^k} \oplus F_{p^k} \oplus F_{p^k} \oplus F_{p^k}$ or $F_{p^k}C_4 \cong F_{p^k} \oplus F_{p^k} \oplus F_{(p^k)^2}$ or $F_{p^k}C_4 \cong F_{p^k} \oplus F_{(p^k)^3}$. When $4|(p^k-1)$, $F_{p^k}C_4 \cong F_{p^k} \oplus F_{p^k} \oplus F_{p^k} \oplus F_{p^k}$ from Theorem 1.4 and thus $|\mathcal{U}(Cr_4(F_p^k))| = (p^k-1)^4$.

Now when $4 \nmid (p^k-1)$, then $4 \nmid (p^k-1)(p^{2k}+p^k+1)$ since $p^{2k}+p^k+1$ is odd. Thus $F_{p^k} \oplus F_{(p^k)^3}$does not contain a unit of order 4, so $F_{p^k}C_4 \ncong F_{p^k} \oplus F_{(p^k)^3}$. Therefore, $F_{p^k}C_4 \cong F_{p^k} \oplus F_{p^k} \oplus F_{(p^k)^2}$ and hence $|\mathcal{U}(Cr_4(F_p^k))| = (p^k+1)(p^k-1)^3$ when $4 \nmid (p^k-1)$.

□

Theorem 2.4. *Order of an element in $\mathcal{U}(Cr_4(F_p))$ is at most $(p-1)$ when $p = 4k+1$ and is at most (p^2-1) when $p = 4k-1$ for some integer k.*

Theorem 2.5. *The order of the unit group $\mathcal{U}(Cr_5(F_p))$ of algebra $Cr_5(F_p)$ of circulant matrices of order 5×5 over F_p, where F_p is a finite field having p, p-odd, elements, is $(p-1)(p^4-1)$ when 5 is a quadratic non-residue mod p.*

Proof. Let $A = circ(a,b,c,d,e) = \begin{pmatrix} a & b & c & d & e \\ e & a & b & c & d \\ d & e & a & b & c \\ c & d & e & a & b \\ b & c & d & e & a \end{pmatrix}$. Order of the unit group $\mathcal{U}(Cr_5(F_p))$ is the number of matrices of non-zero determinant. It is known [3] that circulant matrix is diagonalized by a Fourier matrix F.

In particular,

$$circ(c_1, c_2, ..., c_n) = F^{-1}\Lambda F = diag(p_\gamma(1), p_\gamma(\omega), ..., p_\gamma(\omega^{n-1})),$$

where $p_\gamma(\omega^i) = \sum_{j=0}^{n-1} c_{j+1}(\omega^i)^j$ and ω is primitive $n-$th root of unity.

Thus $\det(A) = A_1A_2A_3A_4A_5$, where $A_i = \sum_{j=0}^{4} c_{j+1}(\omega^i)^j$ and $\{\omega = e^{\frac{2n\Pi\iota}{5}} | 0 \leq n \leq 4\}$. Thus, $A_1 = a+b+c+d+e$,

$$\begin{aligned} A_2 &= a + b(\cos 72 + \iota \sin 72) + c(\cos 144 + \iota sin 144) \\ &\quad + d((\cos 144 - \iota \sin 144)) + e(\cos 72 - \iota \sin 72) \\ &= a + (b+e)\frac{(\sqrt{5}-1)}{4} + (c+d)\frac{(-\sqrt{5}-1)}{4} + \iota\big((b-e)\frac{\sqrt{10+2\sqrt{5}}}{4} \\ &\quad + (c-d)\frac{\sqrt{10-2\sqrt{5}}}{4}\big) \end{aligned}$$

Similarly,

$$\begin{aligned}A_3 =&a+(c+d)\frac{(\sqrt{5}-1)}{4}+(b+e)\frac{(-\sqrt{5}-1)}{4}+\iota\big((c-d)\frac{\sqrt{10+2\sqrt{5}}}{4}\\&+(b-e)\frac{\sqrt{10-2\sqrt{5}}}{4}\big);\\A_4 =&a+(c+d)\frac{(\sqrt{5}-1)}{4}+(b+e)\frac{(-\sqrt{5}-1)}{4}+\iota\big((d-c)\frac{\sqrt{10+2\sqrt{5}}}{4}\\&+(e-b)\frac{\sqrt{10-2\sqrt{5}}}{4}\big);\\A_5 =&a+(b+e)\frac{(\sqrt{5}-1)}{4}+(c+d)\frac{(-\sqrt{5}-1)}{4}+\iota\big((e-b)\frac{\sqrt{10+2\sqrt{5}}}{4}\\&+(d-c)\frac{\sqrt{10-2\sqrt{5}}}{4}\big).\end{aligned}$$

Thus, in this case when 5 is a quadratic non-residue mod p, clearly $10\pm 2\sqrt{5}$ will also be quadratic non-residue mod p, and hence A_2, A_3, A_4 and A_5 exist only when $b = e$ and $c = d$. Thus $A_1 = a + b + c + d + e$ and $A_2 = a - b$ with $b = e = c = d$, and A_3, A_4 and A_5 will be same as A_2. When $A_1 \equiv 0 \pmod p$, the total number of matrices with this condition is p^4 and the the total number of matrices, when $A_2 \equiv 0 \pmod p$ is p. Further, A_1 and A_2 are simultaneously zero modulo p only when $a = b = c = d = e = 0$, i.e., only one matrix of this type. Hence, the total number of matrices with zero determinant is $p^4 + p - 1$ and therefore the order of the unit group $\mathcal{U}(Cr_5(F_p))$ is $p^5 - p^4 - p + 1 = (p - 1)(p^4 - 1)$. Hence the result is proved.

□

Theorem 2.6. *The order of unit group $\mathcal{U}(Cr_5(F_p))$ is*

(i) $(p-1)(p^2-1)^2$ *when* 5 *and* $10\pm 2\sqrt{5}$ *are quadratic residues mod* p *and* -1 *is a quadratic non-residue mod* p.

(ii) $(p-1)^2(p^3+p^2+p-1)$ *when* 5 *is a quadratic residue mod* p *and* -1, *and any of* $10\pm 2\sqrt{5}$ *or both are quadratic non-residues mod* p.

Proof. Let $A = circ(a, b, c, d, e)$ and $\det(A) = A_1A_2A_3A_4A_5$ as defined in the previous theorem. All the matrices having determinant non zero will give the whole unit group. If we compute the number of matrices of determinant zero modulo p, we get the order of $\mathcal{U}(Cr_5(F_p))$. Observe that order of $Cr_5(F_p)$ is p^5.

Thus when 5 is a quadratic residue and -1 is a quadratic non-residue mod p then the order of the unit group depends on two cases as follows:

Case 1: When $10\pm 2\sqrt{5}$ are quadratic residues mod p.

In this case we get, $A_1 = a+b+c+d+e$, $A_2 = a+(b+e)\frac{(\sqrt{5}-1)}{4}+(c+d)\frac{(-\sqrt{5}-1)}{4}$, where $(b-e)k_1 + (c-d)k_2 = 0$ for $k_1 = 10+2\sqrt{5}$ and $k_2 = 10-2\sqrt{5}$ and $A_3 = a+(c+d)\frac{(\sqrt{5}-1)}{4}+(b+e)\frac{(-\sqrt{5}-1)}{4}$, where $(b-e)k_2+(c-d)k_1 = 0$ for $k_1 = 10+2\sqrt{5}$ and $k_2 = 10-2\sqrt{5}$. A_4 and A_5 are same as A_2 and A_3, respectively.

Clearly, the number of matrices when $A_1 \equiv 0 \pmod{p}$ is p^4. When $A_2 \equiv 0 \pmod{p}$, we get the number of independent variables to be 3, and thus the number of such type of matrices is p^3. Similarly, the number of matrices when $A_3 \equiv 0 \pmod{p}$ is also p^3. When A_1 and A_2 both are zero modulo p, then we get $(b+e)\frac{(\sqrt{5}-5)}{4} - (c-d)\frac{(\sqrt{5}-3)}{4}$ and $b = e + (d-c)k$, where $k = k_2k_1^{-1}$. Thus the number of such matrices is p^2. Similarly, the number of matrices when both A_1 and A_3 are zero modulo p is p^2. Further, A_2 and A_3 both zero modulo p gives $a = b = c = d = e$, and hence number of matrices of such type is p. A_1, A_2 and A_3 all are simultaneously zero modulo p only when $a = b = c = d = e = 0$, so there is only one matrix for which A_1, A_2 and A_3 all are zero modulo p.

Thus the total number of matrices with determinant zero modulo p is $p^4+2p^3-2p^2-p+1$. Therefore, order of the unit group in this case is $p^5 - p^4 - 2p^3 + 2p^2 + p - 1 = (p-1)(p^2-1)^2$.

Case 2: When either any one of $10 \pm 2\sqrt{5}$ is a quadratic non-residue or both are non-quadratic residue mod p.

In this case we get, $A_1 = a+b+c+d+e$, $A_2 = a + (b+e)\frac{(\sqrt{5}-1)}{4} + (c+d)\frac{(-\sqrt{5}-1)}{4}$, where $b = e, c = d$ and $A_3 = a + (c+d)\frac{(\sqrt{5}-1)}{4} + (b+e)\frac{(-\sqrt{5}-1)}{4}$, where $b = e, c = d$. A_4 and A_5 are same as A_2 and A_3 respectively.

Clearly, the number of matrices when $A_1 \equiv 0 \pmod{p}$ is p^4, when $A_2 \equiv 0 \pmod{p}$ is p^2, and when $A_3 \equiv 0 \pmod{p}$ is also p^2. When A_1 and A_2 both are zero modulo p, we get $b\frac{(\sqrt{5}-5)}{2} - c\frac{(\sqrt{5}-3)}{2} \equiv 0 \pmod{p}$. Thus the number of matrices in this case when A_1 and A_2 both are zero modulo p is p. Similarly, the number of matrices when both A_1 and A_3 are zero modulo p is p^2. Further, A_2 and A_3 both zero modulo p give $a = b = c = d = e$, and hence the number of matrices of such type is p. A_1, A_2 and A_3 all are simultaneously zero modulo p only when $a = b = c = d = e = 0$. Hence there is only one matrix for which A_1, A_2 and A_3 all are zero modulo p.

Thus the total number of matrices with determinant zero modulo p is $p^4 + 2p^2 - 3p + 1$. Therefore, order of the unit group in this case is $p^5 - p^4 - 2p^2 + 3p - 1 = (p-1)^2(p^3+p^2+p-1)^2$. □

Remark. The case when 5, $10 \pm 2\sqrt{5}$ and -1 are quadratic residues mod p, $(p-1)th$ root of unity,i.e., ω exists in F_p. In this case the order of the unit group of $Cr_5(F_p)$ is given by Gildea in [7].

References

[1] V. Bovdi, On symmetric units in group algebras, *Comm. Algebra*, **29** (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] V. Bovdi and M. M. Parmenter, Symmetric units in integral group rings, *Publ. Math. Debrecen*, **50** (1997) 369-372.

[4] L. Creedon, J. Gildea, The structure of the unit group of the group algebra $\mathbb{F}_{2^k}D_8$, *Canad. Math. Bull.*, **54** (2011) 237-243.

[5] P. J. Davis, *Circulant Matrices*, Chelsea Publication, New York, 1979.

[6] J. Gildea, *Units of Group Algebras*, PhD Thesis, National University of Ireland, Galway, October 2007.

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

[8] J. Gildea, The order of $\mathcal{U}(F_{2^k}D_{10})$ when $5|(2k-1)$, *Int. J. Pure Appl. Math.*, **49** no. 4 (2008) 525-530.

[9] G. Higman, The units of group rings, *Proc. London Math. Soc.*, **46** no. 2 (1940) 231-248.

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

R. K. Sharma
Department of Mathematics, Indian Institute of Technology, Delhi, India
Email: rksharma@maths.iitd.ernet.in

Pooja Yadav
Department of Mathematics, Indian Institute of Technology, Delhi, India
Email: iitd.pooja@gmail.com