J. Algebra Comb. Discrete Appl.
3(1) • 1–6

Received: 5 August 2015
Accepted: 20 October 2015

Journal of Algebra Combinatorics Discrete Structures and Applications

The unit group of group algebra $\mathbb{F}_q SL(2, \mathbb{Z}_3)$

Research Article

Swati Maheshwari, R. K. Sharma

Abstract: Let $\mathbb{F}_q$ be a finite field of characteristic p having q elements, where $q = p^k$ and $p \geq 5$. Let $SL(2, \mathbb{Z}_3)$ be the special linear group of 2×2 matrices with determinant 1 over $\mathbb{Z}_3$. In this note we establish the structure of the unit group of $\mathbb{F}_q SL(2, \mathbb{Z}_3)$.

2010 MSC: 16U60, 20C05

Keywords: Group algebra, Unit group, Finite field

1. Introduction

Let FG be a group algebra of a finite group G over a field F and $\mathcal{U}(FG)$ be the group of units in FG. It is a classical problem to study units and their properties in group ring theory. The case, when G is a finite abelian group, the structure of FG is studied by Perlis and Walker in [14]. In 2006, T. Hurley introduced a correspondence between group ring and certain ring of matrices (see [6]). As an application of units of a group ring, T. Hurley gave a method to construct convolutional codes from units in group ring (see [7]).

A lot of work has been done for finding the algebraic structure of the unit group $\mathcal{U}(FG)$ of a group algebra FG, when G is a finite non-abelian group. Here we are providing some literature survey for the same. For dihedral groups, the structure of the unit group $\mathcal{U}(FG)$ over a finite field F is discussed in [1, 4, 10, 12]. J. Gildea et.al. (see [3]) and R. K. Sharma et.al. (see [15]) have given the structure of the unit group $\mathcal{U}(FG)$, where G is alternating group A_4. Unit group of algebra of circulant matrix has been discussed in [11, 17]. The unit group of group algebras of some non-abelian groups with small orders are established in [16, 18, 19]).

In this article, we are interested in studying the structure of the unit group of $\mathbb{F}_q SL(2, \mathbb{Z}_3)$ over a finite field of characteristic greater than 3.

This work was supported by IIT Delhi, India through GATE Senior Research Fellowship.
Swati Maheshwari (Corresponding Author), R. K. Sharma; Department of Mathematics, Indian Institute of Technology Delhi, India (email: swatimahesh88@gmail.com, rksharmaiitd@gmail.com).

http://dx.doi.org/10.13069/jacodesmath.83854 ISSN 2148-838X

2. Preliminaries

The following results provide useful information about the decomposition of $A/J(A)$, where $A = FG$, $J(A)$ be its Jacobson radical and F being a field of characteristic p. For basic definitions and results, we refer to [13]. We briefly introduce some definitions and notations those will be needed subsequently.

Definition 2.1. *An element $g \in G$ is said to be p-regular if $p \nmid o(g)$. Let s be the l.c.m. of the orders of the p-regular elements of G, ζ be a primitive s-th root of unity over F. Then $T_{G,F}$ be the multiplicative group consisting of those integers t, taken modulo s, for which $\zeta \mapsto \zeta^t$ defines an automorphism of $F(\zeta)$ over F. That is, $T_{G,F}$ is $Gal(F(\zeta)/F)$ seen as a subgroup of $\mathcal{U}(\mathbb{Z}_s)$.*

Note that if u is a power of a prime such that $(u, s) = 1$ and $c = ord_s\ (u)$ is the multiplicative order of u modulo s, then

$$T_{G,F_u} = \{1, u, \ldots, u^{c-1}\} \bmod s$$

and $F_u(\zeta) \cong F_{u^c}$ follow using [8, Theorem 2.21].

Definition 2.2. *If $g \in G$ is a p-regular element, then the sum of all conjugates of $g \in G$ is denoted by γ_g and the cyclotomic F-class of g is defined to be the set*

$$SF(\gamma_g) = \{\gamma_{g^t} \ \mid t \in T_{G,F}\}.$$

Proposition 2.3. *[2, Theorem 1.2] The number of simple components of $FG/J(FG)$ is equal to the number of cyclotomic F-classes in G.*

Theorem 2.4. *[2, Theorem 1.3] Suppose that $Gal(F(\zeta)/F)$ is cyclic. Let w be the number of cyclotomic F-classes in G. If $K_1, K_2, \ldots, K_w$ are the simple components of $Z(FG/J(FG))$ and $S_1, S_2, \ldots, S_w$ are the cyclotomic F-classes of G, then with a suitable re-ordering of indices,*

$$\mid Si \mid = [K_i : F].$$

Lemma 2.5. *[9, Observation 2.2.1, p.22] Let $\mathfrak{B}_1$,$\mathfrak{B}_2$ be two finite dimensional F-algebras such that $\mathfrak{B}_2$ is semisimple. If $f : \mathfrak{B}_1 \to \mathfrak{B}_2$ is an onto homomorphism of F-algebras, then there exists a semisimple F-algebra ℓ such that*

$$\mathfrak{B}_1/J(\mathfrak{B}_1) \cong \ell \oplus \mathfrak{B}_2.$$

Throughout this article, $G = SL(2, \mathbb{Z}_3)$. $\mathbb{F}_q$ is a field of characteristic p, where $q = p^k$ and k is a positive integer. The conjugacy class of $g \in G$ is denoted by $[g]$.

3. Main result

We shall use the presentation of G given in [5],

$$\langle a, b \mid a^3, b^4, (ab)^3 = b^2, (a^2b)^6\rangle$$

where $a = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ and $b = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$.

We can see that G has 7 conjugacy classes as follows:

representative	elements in the class	order of element
$[a]$	$a, (ba)^4, (ab)^4, b^{-1}ab$	3
$[a^{-1}]$	$a^{-1}, (ba)^2, (ab)^2, aba$	3
$[b]$	$b, b^{-1}, a^2ba, aba^2, ab^{-1}a^2, a^2b^{-1}a$	4
$[b^2]$	b^2	2
$[ab]$	ab, ba, a^2ba^2, ab^2	6
$[(ab)^{-1}]$	$(ab)^{-1}, a^2b^{-1}, ab^{-1}a, a^2b^2$	6

We have $(p, |G|) = 1$ and so $J(\mathbb{F}_{p^k}G) = 0$. Further, we discuss the decomposition of $\mathbb{F}_{p^k}G$.

Theorem 3.1. *Let $\mathbb{F}_q$ be a finite field of characteristic p, where $p \geq 5$. Then the Wedderburn decomposition of $\mathbb{F}_qG$ is given by*

condition on k	$\mathbb{F}_qG$
k is even	$\mathbb{F}_q^3 \oplus M(2, \mathbb{F}_q)^3 \oplus M(3, \mathbb{F}_q)$
k is odd *$p \equiv 1$ mod 3 and $p \equiv \pm 1$mod 4*	$\mathbb{F}_q^3 \oplus M(2, \mathbb{F}_q)^3 \oplus M(3, \mathbb{F}_q)$
k is odd *$p \equiv -1$ mod 3 and $p \equiv \pm 1$mod 4*	$\mathbb{F}_q \oplus \mathbb{F}_{q^2} \oplus M(2, \mathbb{F}_q) \oplus M(2, \mathbb{F}_{q^2}) \oplus M(3, \mathbb{F}_q)$

Proof. Since $\mathbb{F}_qG$ is semisimple, so it has the Wedderburn decomposition which is given by

$$\mathbb{F}_qG \cong \oplus_{i=1}^{r} M(n_i, \mathbb{F}_i),$$

where for each $i, n_i \geq 1$and $\mathbb{F}_i$ is a finite extension of $\mathbb{F}_q$. By using Lemma 2.5, we have

$$\mathbb{F}_qG \cong \mathbb{F}_q \oplus_{i=1}^{r-1} M(n_i, \mathbb{F}_i). \tag{1}$$

Further, we find n_i's and $\mathbb{F}_i$'s. Since $| G |= 24$, hence any element $g \in G$ is a p- regular element. For finding cyclotomic $\mathbb{F}_q$ - classes of G, first we assume that k is even. We have

$$p^k \equiv 1 \text{ mod } 4 \text{ and } p^k \equiv 1 \text{ mod } 3.$$

Then by Chinese remainder theorem

$$p^k \equiv 1 \text{ mod } 12.$$

By using above observation, we have

$$S_{\mathbb{F}_q}(\gamma_g) = \{\gamma_g\} \text{ and } | S_{\mathbb{F}_q}(\gamma_g) |= 1.$$

Therefore by using Equation (1), Proposition 2.3 and Theorem 2.4, we have

$$\mathbb{F}_qG \cong \mathbb{F}_q \oplus_{i=1}^{6} M(n_i, \mathbb{F}_q)$$

for some $n_i \geq 1$. As dimension of $\mathbb{F}_qG$ is 24, we get

$$\sum_{i=1}^{6} n_i^2 = 23.$$

Using above equality, $1 \leq n_i \leq 3$. Clearly any $n_i = n_j = 3$ for $1 \leq i \neq j \leq 3$ not possible. So the only possible choice for n_i's is

$$n_1 = n_2 = 1, n_3 = n_4 = n_5 = 2 \text{ and } n_6 = 3.$$

Therefore the decomposition $\mathbb{F}_qG$ is given by

$$\mathbb{F}_qG \cong \mathbb{F}_q^3 \oplus M(2, \mathbb{F}_q)^3 \oplus M(3, \mathbb{F}_q).$$

Now we consider the case when k is odd. We shall discuss this case into two parts

1. $p \equiv 1 \mod 3$ and $p \equiv \pm 1 \mod 4$
2. $p \equiv -1 \mod 3$ and $p \equiv \pm 1 \mod 4$

Case 1. Suppose k is odd with $p \equiv 1 \mod 3$ and $p \equiv \pm 1 \mod 4$.

Observe that

$$p^k \equiv p \bmod 4 \text{ and } p^k \equiv p \bmod 3.$$

Then by Chinese remainder theorem

$$p^k \equiv p \bmod 12.$$

Since $[b] = [b^{-1}]$. We have

$$S_{\mathbb{F}_q}(\gamma_g) = \{\gamma_g\}.$$

Hence n_i's and $\mathbb{F}_i$'s are same as above. So the decomposition of $\mathbb{F}_qG$ is given by

$$\mathbb{F}_qG \cong \mathbb{F}_q^3 \oplus M(2, \mathbb{F}_q)^3 \oplus M(3, \mathbb{F}_q).$$

Case 2. Suppose k is odd with $p \equiv -1 \mod 3$ and $p \equiv \pm 1 \mod 4$. Using the observation in case 1, we have

$$p^k \equiv p \bmod 12.$$

$$S\mathbb{F}_q(\gamma_b) = \{\gamma_b\}, S\mathbb{F}_q(\gamma_{b^2}) = \{\gamma_{b^2}\},$$

$$S\mathbb{F}_q(\gamma_a) = \{\gamma_a, \gamma_{a^{-1}}\} \text{ and } S\mathbb{F}_q(\gamma_{ab}) = \{\gamma_{ab}, \gamma_{(ab)^{-1}}\}.$$

Therefore by using Equation (1), Proposition 2.3 and Theorem 2.4, we have

$$\mathbb{F}_qG \cong \mathbb{F}_q \oplus M(n_1, \mathbb{F}_q) \oplus M(n_2, \mathbb{F}_q) \oplus M(n_3, \mathbb{F}_{q^2}) \oplus M(n_4, \mathbb{F}_{q^2})$$

for some $n_i \geq 1$.
As dimension of $\mathbb{F}_qG$ is 24, we get

$$n_1^2 + n_2^2 + 2n_3^2 + 2n_4^2 = 23$$

and hence, $1 \leq n_i \leq 3, \forall 1 \leq i \leq 4$. Clearly n_3 and n_4 can not be equal to 3. So the only possible choice for n_i's is $n_1 = 2, n_2 = 3, n_3 = 1, n_4 = 2$. Therefore the decomposition of $\mathbb{F}_qG$ is given by

$$\mathbb{F}_qG \cong \mathbb{F}_q \oplus \mathbb{F}_{q^2} \oplus M(2, \mathbb{F}_q) \oplus M(2, \mathbb{F}_{q^2}) \oplus M(3, \mathbb{F}_q).$$

□

Corollary 3.2. *Let $q = p^k$, where $p \geq 5$ is a prime. Then the structure of $\mathcal{U}(\mathbb{F}_qG)$ is given by*

condition on k	$\mathcal{U}(\mathbb{F}_qG)$
k is even	$\mathcal{C}_{q-1}^3 \oplus GL(2,\mathbb{F}_q)^3 \oplus GL(3,\mathbb{F}_q)$
k is odd $p \equiv 1 \ mod \ 3$ *and* $p \equiv \pm 1 mod \ 4$	$\mathcal{C}_{q-1}^3 \oplus GL(2,\mathbb{F}_q)^3 \oplus GL(3,\mathbb{F}_q)$
k is odd $p \equiv -1 \ mod \ 3, \pm 1 mod \ 4$	$\mathcal{C}_{q-1} \oplus \mathcal{C}_{q^2-1} \oplus GL(2,\mathbb{F}_q) \oplus GL(2,\mathbb{F}_{q^2}) \oplus GL(3,\mathbb{F}_q)$

Proof. It follows by the fact that, if R and S are two rings then

$$\mathcal{U}(R \oplus S) = \mathcal{U}(R) \oplus \mathcal{U}(S).$$

□

References

[1] L. Creedon, J. Gildea, The structure of the unit group of the group algebra $\mathbb{F}_{2^k}D_8$, Canad. Math. Bull. 54(2) (2011) 237–243.
[2] R. A. Ferraz, Simple components of the center of $\mathbb{F}G/J(\mathbb{F}G)$, Comm. Algebra 36(9) (2008) 3191–3199.
[3] J. Gildea, The structure of the unit group of the group algebra $\mathbb{F}_2^kA_4$, Czechoslovak Math. J. 61(2) (2011) 531–539.
[4] J. Gildea, F. Monaghan, Units of some group algebras of groups of order 12 over any finite field of characteristic 3, Algebra Discrete Math. 11(1) (2011) 46–58.
[5] P. R. Helm, A presentation for $SL(2,\mathbb{Z}_{p^r})$, Comm. Algebra 10(15) (1982) 1683–1688.
[6] T. Hurley, Group rings and ring of matrices, Int. J. Pure Appl. Math. 31(3) (2006) 319–335.
[7] T. Hurley, Convolutional codes from units in matrix and group rings, Int. J. Pure Appl. Math. 50(3) (2009) 431–463.
[8] R. Lidl, H. Niederreiter, Introduction to finite fields and their applications, Cambridge University Press, New York, 2000.
[9] N. Makhijani, Units in finite group algebras, IIT Delhi, 2014.
[10] N. Makhijani, R. K. Sharma, J. B. Srivastava, A note on units in $\mathbb{F}_{p^m}D_{2p^n}$, Acta Math. Acad. Paedagog. Nyházi. 30(1) (2014) 17–25.
[11] N. Makhijani, R. K. Sharma, J. B. Srivastava, The unit group of algebra of circulant matrices, Int. J. Group Theory. 3(4) (2014) 13–16.
[12] N. Makhijani, R. K. Sharma, J. B. Srivastava, The unit group of $\mathbb{F}_q[D_{30}]$, Serdica Math. J. 41(2-3) (2015) 185–198.
[13] C. P. Milies, S. K. Sehgal, An introduction to group rings, Kluwer Academic Publishers, 2002.
[14] S. Perlis, G. L. Walker, Abelian group algebras of finite order, Trans. Amer. Math. Soc. 68(3) (1950) 420–426.
[15] R. K. Sharma, J. B. Srivastava, M. Khan, The unit group of $\mathbb{F}A_4$, Publ. Math. Debrecen 71(1-2) (2007) 21–26.
[16] R. K. Sharma, J. B. Srivastava, M. Khan, The unit group of $\mathbb{F}S_3$, Acta Math. Acad. Paedagog. Nyházi. 23(2) (2007) 129–142.
[17] R. K. Sharma, P. Yadav, Unit group of algebra of circulant matrices, Int. J. Group Theory. 2(4) (2013) 1–6.

[18] R. K. Sharma, P. Yadav, The unit group of $\mathbb{Z}_p Q_8$, Algebras Groups Geom. 25(4) (2008) 425–429.
[19] G. Tang, Y. Wei, Nanning, Y. Li, Units group of group algebras of some small groups, Czechoslovak Math. J. 64(1) (2014) 149–157.