International Electronic Journal of Algebra
Volume 18 (2015) 21-33

UNITS IN $\mathbb{F}_{q^k}(C_p \rtimes_r C_q)$

N. Makhijani, R. K. Sharma and J. B. Srivastava

Received: 5 February 2014
Communicated by A. Çiğdem Özcan

Abstract. Let q be a prime, $\mathbb{F}_{q^k}$ be a finite field having q^k elements and $C_n \rtimes_r C_q$ be a group with presentation $\langle\ a,\ b \mid a^n,\ b^q, b^{-1}ab = a^r\ \rangle$, where $(n, rq) = 1$ and q is the multiplicative order of r modulo n. In this paper, we address the problem of computing the Wedderburn decomposition of the group algebra $\mathbb{F}_{q^k}(C_n \rtimes_r C_q)$ modulo its Jacobson radical. As a consequence, the structure of the unit group of $\mathbb{F}_{q^k}(C_p \rtimes_r C_q)$ is obtained when p is a prime different from q.

Mathematics Subject Classification (2010): 16U60, 16S34, 20C05
Keywords: Unit group, group algebra, Wedderburn decomposition

1. Introduction

Let FG be the group algebra of a finite group G over a field F and $\mathcal{U}(FG)$ be its unit group. The study of the group of units is one of the classical topics in group ring theory and has applications in coding theory (cf. [17, 28]) and cryptography (cf. [18]). Results obtained in this direction are useful for the investigation of Lie properties of group rings, isomorphism problem and other open questions in this area [6]. In [3], Bovdi gave a comprehensive survey of results concerning the group of units of a modular group algebra of characteristic p. There is a long tradition on the study of the unit group of finite group algebras [4, 5, 12–16, 22, 25, 26]. In general, the structure of $\mathcal{U}(FG)$ is elusive if $|G| = 0$ in F.

Let $J(FG)$ be the Jacobson radical of FG. Then

$$1 \longrightarrow 1 + J(FG) \xrightarrow{inc} \mathcal{U}(FG) \xrightarrow{\psi} \mathcal{U}\left(\frac{FG}{J(FG)}\right) \longrightarrow 1$$

where $\psi(x) = x + J(FG),\ \forall x \in \mathcal{U}(FG)$, is a short exact sequence of groups and if F is a perfect field, then by *Wedderburn-Malcev* Theorem [9, Theorem 72.19], there exists a semisimple subalgebra B of FG such that $FG = B \oplus J(FG)$ showing that the above sequence is split and hence

$$\mathcal{U}(FG) \cong (1 + J(FG)) \rtimes \mathcal{U}\left(FG/J(FG)\right)$$

Thus a good description of the Wedderburn decomposition of $FG/J(FG)$ is useful for studying the unit group of FG.

The computation of the Wedderburn decomposition of finite semisimple group algebras and in particular, of the primitive central idempotents, has attracted the attention of several authors (cf. [1, 2, 7, 27]). This raises the following question: Is it possible to efficiently compute the decomposition of $FG/J(FG)$ when FG is a finite group algebra that is not semi-simple? An expression for the decomposition of $\mathbb{F}_2 D_{2p}/J(\mathbb{F}_2 D_{2p})$ was obtained by Kaur and Khan in [21], where D_{2p} is a dihedral group of order $2p$ and p is an odd prime. Recently, the authors generalized this expression and computed the decomposition of $\mathbb{F}_{2^k} D_{2n}/J(\mathbb{F}_{2^k} D_{2n})$ for an arbitrary odd number n in [24]. In this paper, we focus on the computation of the Wedderburn decomposition of the group algebra $\mathbb{F}_{q^k}(C_n \rtimes_r C_q)$ modulo its Jacobson radical when q is a prime and $C_n \rtimes_r C_q$ is the group with presentation $\langle\, a,\ b \mid a^n,\ b^q,\ b^{-1}ab = a^r \,\rangle$ such that $(n, rq) = 1$ and the multiplicative order of r modulo n is q.

It was proved by Kaur and Khan during the conference on Groups, Group Rings and Related Topics (cf. [20]) that if p and q are distinct primes and F is a finite field of characteristic q having a primitive p^{th} root of unity, then

$$\frac{\mathcal{U}(F(C_p \rtimes C_q))}{1 + J(F(C_p \rtimes C_q))} \cong F^* \times GL(q, F)^{\frac{p-1}{q}}$$

The structure of unit group is however open to be explored in the absence of a primitive p^{th} root of unity in F. We use the decomposition obtained in Section 4 to determine the structure of the unit group of $F(C_p \rtimes C_q)$ for any finite field F of characteristic q.

2. Notations

We introduce some basic notations where l and m are coprime integers, R is a ring, $g \in G$ and X is any subset of G.

$\mathbb{Z}_m$	ring of integers modulo m
$ord_m(l)$	multiplicative order of l modulo m
$irr_F(\alpha)$	minimal polynomial of α over F
$\varphi(n)$	Euler's totient function of n
F^*	$F \setminus \{0\}$
$\widehat{X}$	$\sum_{x \in X} x$
$\widehat{g}$	$\widehat{\langle\, g \,\rangle}$

$o(g)$	order of g
$[\ g\ ]$	conjugacy class of g
G^m	external direct product of m copies of G
R^m	external direct sum of m copies of R
$M(m, F)$	algebra of all $m \times m$ matrices over F
$GL(m, F)$	general linear group of all $m \times m$ invertible matrices over F

3. Preliminaries

The following results will be useful for our investigation.

Proposition 3.1. [19, Chapter 1, Proposition 6.16] *Let $f : R_1 \to R_2$ be a surjective homomorphism of rings. Then $f\,(J(R_1)) \subseteq J(R_2)$ with equality if $ker\ f \subseteq J(R_1)$.*

Remark 3.2. *Note that if we add the semi-simplicity of the ring R_2 in the above proposition, then $J(R_1) \subseteq ker\ f$.*

Theorem 3.3. *Let $E = F(\xi)/F$ be a finite separable extension, K be any field extension of F and $g(X) = irr_F(\xi)$. If*

$$g(X) = \prod_{i=1}^{r} g_i(X)$$

as a product of irreducible polynomials $g_i(X) \in K[X]$, then

$$K \otimes_F E \cong \mathop{\oplus}_{i=1}^{r} K(\xi_i)$$

as K-algebras, where ξ_i is a root of $g_i(X)$ in an algebraic closure L of K.

Proof. For each $i,\ 1 \leq i \leq r$, the map $\lambda_i : K \times E \to K(\xi_i)$ given by the assignment

$$(\alpha, f(\xi)) \mapsto \alpha f(\xi_i)\ \forall\ \alpha \in K,\ f(X) \in F[X]$$

is F-bilinear and hence induces a K-algebra homomorphism $\lambda_i^* : K \otimes_F E \to K(\xi_i)$ such that

$$\alpha \otimes f(\xi) \mapsto \alpha f(\xi_i)$$

Evidently λ_i^* is onto. Therefore $ker\ \lambda_i^*$ is a maximal ideal of $K \otimes_F E$ for all $i,\ 1 \leq i \leq r$ and $ker\ \lambda_i^*\ +\ ker\ \lambda_j^* = K \otimes_F E$ for any $i \neq j$ as $1 \otimes g_i(\xi) \in\ ker\ \lambda_i^* \setminus ker\ \lambda_j^*$. It follows from [8, Chapter 5, Theorem 2.2] that the K-algebra homomorphism $\lambda : K \otimes_F E \to \mathop{\oplus}_{i=1}^{r} K(\xi_i)$ defined by

$$\lambda(A) = (\lambda_1^*(A), \ldots, \lambda_r^*(A)) \qquad \forall\ A \in K \otimes_F E$$

is onto. Since $dim_K K \otimes_F E = dim_F E = deg\, g(X) = \sum_{i=1}^{r} deg\, g_i(X) = dim_K \bigoplus_{i=1}^{r} K(\xi_i)$, the proof follows. □

Theorem 3.4. [23, Theorem 2.21] *The distinct automorphisms of $\mathbb{F}_{u^k}$ over $\mathbb{F}_u$ are exactly the mappings $\sigma_0, \ldots, \sigma_{k-1}$, defined by $\sigma_j(\alpha) = \alpha^{u^j}$ for $\alpha \in \mathbb{F}_{u^k}$ and $0 \leq j \leq k-1$.*

Thus if $v = u^k$, then

$$\mathbb{F}_v \otimes_{\mathbb{F}_u} \mathbb{F}_{u^m} \cong \left(\mathbb{F}_{v^{o_m^k}} \right)^{(m,k)} \tag{3.1}$$

as $\mathbb{F}_v$-algebras where $o_m^k = ord_{u^m-1}(v) = m/(m,k)$.

Theorem 3.5. [10, Theorem 7.9] *Let A be an F-algebra, E be an extension field of F and suppose that for each simple A-module M, the $E \otimes_F A$ module $E \otimes_F M$ is semi-simple (This hypothesis certainly holds whenever E is a finite separable extension of F). Then*

(1) $J(E \otimes_F A) = E \otimes_F J(A)$

(2) $E \otimes_F \dfrac{A}{J(A)} \cong \dfrac{E \otimes_F A}{E \otimes_F J(A)}$

As a consequence, if A is a finite dimensional F-algebra, then $dim_E\, J(E \otimes_F A) = dim_F\, J(A)$.

The following results are due to Ferraz.

Let G be a finite group and char $F = p$. Also let s be the L.C.M. of the orders of the p-regular elements of G, ξ be a primitive s^{th} root of unity over F and $T_{G,F}$ be the multiplicative group consisting of those integers t, taken modulo s, for which $\xi \mapsto \xi^t$ defines an automorphism of $F(\xi)$ over F.

If $F = \mathbb{F}_u$, then by Theorem 3.4,

$$T_{G,F} = \{1, u, \cdots, u^{c-1}\} \bmod s$$

where $c = ord_s(u)$.

We denote the sum of all conjugates of $g \in G$ by γ_g.

Definition 3.6. If $g \in G$ is a p-regular element, then the cyclotomic F-class of γ_g is defined to be the set

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

Proposition 3.7. [11, Proposition 1.2] *The number of simple components of $FG/J(FG)$ is equal to the number of cyclotomic F-classes in G.*

Theorem 3.8. [11, Theorem 1.3] *Suppose that $Gal(F(\xi):F)$ is cyclic. Let w be the number of cyclotomic F-classes in G. If $K_1,\cdots,K_w$ are the simple components of $\mathcal{Z}(FG/J(FG))$ and $S_1,\cdots,S_w$ are the cyclotomic F-classes of G, then with a suitable re-ordering of indices, $\mid S_i \mid = [K_i : F]$.*

Note that the conjugacy class of a p-regular element of G is referred to as a p-regular conjugacy class.

4. Wedderburn decomposition

In this section, we compute a general expression for the Wedderburn decomposition of the group algebra $\mathbb{F}_{q^k}(C_n \rtimes_r C_q)$ modulo its Jacobson radical.

Lemma 4.1. *Let F be a finite field of characteristic q containing a primitive nth root of unity ζ and $G = C_n \rtimes_r C_q$. Then*

$$FG/J(FG) \;\cong\; F^{1+\sum_{d\in\mathcal{A}_n}\varphi(d)} \;\oplus\; M(q,F)^{\sum_{d\in\mathcal{B}_n}\frac{\varphi(d)}{q}}$$

where

$$\begin{aligned}\mathcal{A}_n &= \{\ d \ \mid d>1,\ d\mid n \quad and \quad ord_d(r)=1\ \},\\ \mathcal{B}_n &= \{\ d \ \mid d>1,\ d\mid n \quad and \quad ord_d(r)=q\ \}.\end{aligned}$$

Proof. A q-regular conjugacy class of G is either $\{1\}$ or of the form

$$[\ a^i\ ] = \begin{cases} \{\ a^i\ \} & \text{if } o(a^i)\in\mathcal{A}_n \\ \left\{\ a^i,\ a^{ri},\ \cdots, a^{r^{q-1}i}\ \right\} & \text{if } o(a^i)\in\mathcal{B}_n \end{cases}$$

showing that if $d \in \mathcal{B}_n$, then there are $s_d = \varphi(d)/q$ distinct conjugacy classes in G containing elements of order d, each of size q. Let $\left\{\ a^{I_d^m}\ \middle|\ 1\le m\le s_d\ \right\}$ be the representatives of these classes and $\mathcal{C}_n = \{\ (d,m) \mid d\in\mathcal{B}_n,\ 1\le m\le s_d\ \}$.

Define the following F-algebra homomorphisms:

(a) $\phi_1 : FG \to F$ by the assignment $a\mapsto 1,\ b\mapsto 1$.

(b) For each $(d,m)\in\mathcal{C}_n,\ \theta_d^m : FG\to M(q,F)$ by

$$a\mapsto \begin{bmatrix} \zeta^{I_d^m} & 0 & 0 & \cdots & 0 \\ 0 & \zeta^{I_d^m\, r} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & \cdots & \zeta^{I_d^m\, r^{q-1}} \end{bmatrix}_{q\times q},\quad b\mapsto \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}_{q\times q}$$

Firstly suppose that $\mathcal{A}_n \neq \emptyset$ and for each $d \in \mathcal{A}_n$, define the F-algebra homomorphism

$$\phi_d : FG \to F^{\varphi(d)}$$

by the assignment

$$a \mapsto \left(\zeta^{\frac{n}{d} i}\right)_{i \,\in\, \mathcal{U}(\mathbb{Z}_d)}, \; b \mapsto \underbrace{(\,1, \cdots, 1\,)}_{\varphi(d)}$$

We claim that if $\theta : FG \to F \oplus F^{\sum_{d \in \mathcal{A}_n} \varphi(d)} \;\oplus\; M(q,F)^{\sum_{d \in \mathcal{B}_n} s_d}$ is defined as

$$\theta = \phi_1 \oplus \left(\bigoplus_{d \in \mathcal{A}_n} \phi_d \right) \oplus \left(\bigoplus_{(d,m) \in \mathcal{C}_n} \theta_d^m \right),$$

then $dim_F \; ker \; \theta = (q-1) \left(1 + \sum_{d \in \mathcal{A}_n} \varphi(d) \right)$.

Let $X = \sum_{j=0}^{q-1} \sum_{i=0}^{n-1} \alpha_i^j \; b^j a^i \in ker \; \theta$ and $F_j(X) = \sum_{i=0}^{n-1} \alpha_i^j \; X^i \in F[X]$ for all j, $0 \leq j \leq q-1$.

Then

(a) $\sum_{j=0}^{q-1} \sum_{i=0}^{n-1} \alpha_i^j = 0$

(b) $\sum_{j=0}^{q-1} \theta_d^m(b)^j \; F_j\left(\theta_d^m(a)\right) = O \qquad \forall \; (d,m) \in \mathcal{C}_n$

$\Rightarrow F_j(\zeta^{I_d^m r^i}) = 0 \qquad \forall \; (d,m) \in \mathcal{C}_n, \; 0 \leq i, \; j \leq q-1$

Since $\Phi_d(X) = \prod_{m=1}^{s_d} \prod_{i=0}^{q-1} (X - \zeta^{I_d^m r^i}) \; \forall \; d \in \mathcal{B}_n$, therefore

$$F_j(X) = G_j(X) \left(\prod_{d \in \mathcal{B}_n} \Phi_d(X) \right)$$

for some $G_j(X) = \sum_{i=0}^{m'} \beta_i^j X^i \in F[X]$, where $m' = n-1-\sum_{d \in \mathcal{B}_n} \varphi(d) = \sum_{d \in \mathcal{A}_n} \varphi(d)$.

(c) $\sum_{j=0}^{q-1} F_j\left(\zeta^{\frac{n}{d} i}\right) = 0 \qquad \forall \; i \in \mathcal{U}(\mathbb{Z}_d), d \in \mathcal{A}_n$.

$\Rightarrow \sum_{j=0}^{q-1} F_j(X) = \left(\prod_{d \in \mathcal{A}_n} \Phi_d(X) \right) g(X)$, for some $g(X) \in F[X]$.

$$\Rightarrow \left(\sum_{j=0}^{q-1} G_j(X)\right)\left(\prod_{d\in\mathcal{B}_n} \Phi_d(X)\right) = \left(\prod_{d\in\mathcal{A}_n} \Phi_d(X)\right) g(X)$$

Due to degree constraints, we have
$g(X) = \alpha \left(\prod_{d\in\mathcal{B}_n} \Phi_d(X)\right)$ for some $\alpha \in F$.

Using (a), $g(1) = 0$ and hence

$$\begin{aligned}
&\Rightarrow \ g(X) = 0 \\
&\Rightarrow \ \sum_{j=0}^{q-1} G_j(X) = 0 \\
&\Rightarrow \ \sum_{j=0}^{q-1} \beta_i^j = 0 \ \forall \ 0 \le i \le m' \\
&\Rightarrow \ dim_{\ F} \ ker \ \theta = (q-1)(1+m') = (q-1)\left(1 + \sum_{d\in\mathcal{A}_n} \varphi(d)\right)
\end{aligned}$$

Hence the claim follows.

Evidently if $\mathcal{A}_n = \emptyset$ and $\theta : FG \to F \ \oplus \ M(q,F)^{\sum_{d\in\mathcal{B}_n} \frac{\varphi(d)}{q}}$ is defined as

$$\theta = \phi_1 \ \oplus \ \left(\underset{(d,m)\in\mathcal{C}_n}{\oplus} \ \theta_d^m \right)$$

then $dim_{\ F} \ ker \ \theta = q - 1$.

Thus in either case, θ is onto and hence $J(FG) \subseteq ker \ \theta$ showing that $\theta^* : FG/J(FG) \to \theta(FG)$ defined by

$$\theta^*\left(X + J(FG)\right) = \theta(X) \qquad \forall \ X \in FG$$

is a well-defined surjective F-algebra homomorphism.

As $FG/J(FG)$ is semi-simple, it follows that

$$FG/J(FG) \cong C \oplus \theta(FG)$$

for the semi-simple F-algebra $C = ker \ \theta^*$.

But $T_{G,F} = \{1\}$ mod n. Thus the cyclotomic F-classes in G are precisely the q-regular conjugacy classes in G and by Proposition 3.7, the number of simple components in the decomposition of $FG/J(FG)$ is

$$1 + \sum_{d\in\mathcal{A}_n} \varphi(d) + \sum_{d\in\mathcal{B}_n} \frac{\varphi(d)}{q}$$

which is same as the number of simple components in $\theta\,(FG)$. Hence

$$FG/J(FG) \cong \theta(FG)$$

and the proof follows. $\square$

The decomposition may vary if F does not contain a primitive nth root of unity.

Theorem 4.2. *If $u = q^k$, then*

$$\mathbb{F}_u G/J(\mathbb{F}_u G) \;\cong\; \mathbb{F}_u \;\oplus\; \left(\bigoplus_{d \in \mathcal{A}_n} (\,\mathbb{F}_{u^{o_d}})^{\,x_d} \right) \;\oplus\; \left(\bigoplus_{d \in \mathcal{B}_n} M\,(q, \mathbb{F}_{u^{i_d}})^{y_d} \right) \qquad (4.1)$$

where

(a) $o_d = ord_d(u)\ \forall\ d \mid n,\ d > 1$.

(b) $x_d = \frac{\varphi(d)}{o_d}\ \forall\ d \in \mathcal{A}_n$ (if $\mathcal{A}_n \neq \emptyset$).

(c) for each $d \in \mathcal{B}_n$, i_d is the least positive integer such that

$$u^{i_d} \equiv r^j \ mod\ d$$

for some $0 \leq j \leq q-1$ and $y_d = \frac{\varphi(d)}{q\ i_d}$.

Proof. Let $g \in G \setminus \{1\}$ be a q-regular element and $d = o(g)$. The following hold:

(1) If $\mathcal{A}_n \neq \emptyset$ and $d \in \mathcal{A}_n$, then

$$S_{\mathbb{F}_u}\,(\gamma_g) = \dot{\bigcup_{0\ \leq\ j\ \leq\ o_d - 1}} \left\{\ \gamma_{g^{u^j}} \right\}$$

(2) However if $d \in \mathcal{B}_n$, then

$$[\ g\ ] = [\ a^{I_d^m}\ ] \text{ for some } m,\ 1 \leq m \leq s_d$$

For any $l,\ l' \in \mathbb{N}$,

$$\begin{aligned} & \gamma_{g^{u^l}} = \gamma_{g^{u^{l'}}} \\ \Leftrightarrow\quad & [\ a^{u^l I_d^m}\ ] = [\ a^{u^{l'} I_d^m}\ ] \\ \Leftrightarrow\quad & u^{|l-l'|} \equiv r^j \bmod d \ \text{ for some } j,\ 0 \leq j \leq q-1 \end{aligned}$$

Therefore

$$S_{\mathbb{F}_u}\,(\gamma_g) = \dot{\bigcup_{0\ \leq\ j\ \leq\ i_d - 1}} \left\{\ \gamma_{g^{u^j}} \right\}$$

Thus there are

(a) x_d distinct cyclotomic $\mathbb{F}_u$-classes in G, each of order o_d, for all $d \in \mathcal{A}_n$ (if $\mathcal{A}_n \neq \emptyset$).

(b) y_d cyclotomic $\mathbb{F}_u$-classes, each of order i_d, for all $d \in \mathcal{B}_n$.

In view of the Wedderburn structure theorem and Theorem 3.8,

$$\begin{aligned}&\mathbb{F}_uG/J(\mathbb{F}_uG) \\ &\cong \mathbb{F}_u \oplus \left(\underset{d\in\mathcal{A}_n}{\oplus} \overset{x_d}{\underset{l=1}{\oplus}} M\left(n_l, \mathbb{F}_{u^{o_d}}\right)\right) \oplus \left(\underset{d\in\mathcal{B}_n}{\oplus} \overset{y_d}{\underset{j=1}{\oplus}} M\left(m_j, \mathbb{F}_{u^{i_d}}\right)\right)\end{aligned} \tag{4.2}$$

for some $n_l,\ m_j \geq 1$.

By [10, Theorem 7.9], it follows that

$$\begin{aligned}\mathbb{F}_{u^{o_n}}G/J(\mathbb{F}_{u^{o_n}}G) &\cong \mathbb{F}_{u^{o_n}} \otimes_{\mathbb{F}_u} \mathbb{F}_uG/J(\mathbb{F}_uG) \\ &\cong \mathbb{F}_{u^{o_n}} \oplus \left(\underset{d\in\mathcal{A}_n}{\oplus} \overset{x_d}{\underset{l=1}{\oplus}} M\left(n_l, \mathbb{F}_{u^{o_n}} \otimes_{\mathbb{F}_u} \mathbb{F}_{u^{o_d}}\right)\right) \\ &\quad \oplus \left(\underset{d\in\mathcal{B}_n}{\oplus} \overset{y_d}{\underset{j=1}{\oplus}} M\left(m_j, \mathbb{F}_{u^{o_n}} \otimes_{\mathbb{F}_u} \mathbb{F}_{u^{i_d}}\right)\right)\end{aligned}$$

Since $\mathbb{F}_{u^{o_n}}$ contains a primitive nth root of unity, therefore the decomposition of $\mathbb{F}_{u^{o_n}}G/J(\mathbb{F}_{u^{o_n}}G)$ can be obtained using the previous lemma. As a consequence of equation (3.1) and the uniqueness of Wedderburn decomposition, we have $n_l,\ m_j = 1$ or q.

Let $\kappa : \mathbb{F}_uG \to \mathbb{F}_u$ be the $\mathbb{F}_u$-algebra homomorphism, coming from the trivial representation of G and $K = ker\ \kappa$.

If $\mathcal{A}_n \neq \emptyset$ and $d \in \mathcal{A}_n$, then

$$\Phi_d(X) = \prod_{i=1}^{x_d} f_d^i(X)$$

where $f_d^i(X) \in \mathbb{F}_u[X]$ is an irreducible polynomial of degree o_d for each $1 \leq i \leq x_d$.

Now for each $(d,i) \in \mathcal{G}_n = \{\ (d,i) \mid d \in \mathcal{A}_n,\ 1 \leq i \leq x_d\ \}$, let $\xi_d^i \in \mathbb{F}_{u^{o_d}}$ be a root of $f_d^i(X)$ and $\kappa_d^i : \mathbb{F}_uG \to \mathbb{F}_{u^{o_d}}$ be an $\mathbb{F}_u$-algebra homomorphism obtained from the assignment

$$a \mapsto \xi_d^i,\ b \mapsto 1$$

Observe that for all $(d,i) \in \mathcal{G}_n$, κ_d^i is onto and hence $K_d^i = ker\ \kappa_d^i$ is a maximal ideal of $\mathbb{F}_uG$. Since

$$f_d^i(a) \in K_d^i \setminus K_{d'}^{i'}\ \forall\ (d,i),\ (d',i') \in \mathcal{G}_n \text{ and } (d,i) \neq (d',i'),$$

it follows that

$$\left\{\ K,\ K_d{}^i\ \Big|\ (d,i) \in \mathcal{G}_n\ \right\}$$

is a collection of pairwise co-maximal ideals of $\mathbb{F}_uG$. Therefore by Chinese remainder theorem [8, Chapter 5, Theorem 2.2], it follows that

$$\frac{\mathbb{F}_uG}{K \bigcap \left(\bigcap\limits_{(d,i)\in\mathcal{G}_n} K_d^i \right)} \cong \mathbb{F}_u \oplus \left(\underset{d\in\mathcal{A}_n}{\oplus} (\ \mathbb{F}_{u^{o_d}}\ )^{x_d} \right)$$

Using this with Remark 3.2, there exists a surjective $\mathbb{F}_u$-algebra homomorphism

$$\lambda : \frac{\mathbb{F}_u G}{J(\mathbb{F}_u G)} \twoheadrightarrow \mathcal{M} = \mathbb{F}_u \ \oplus \ \left(\bigoplus_{d \in \mathcal{A}_n} (\ \mathbb{F}_{u^{o_d}}\ )^{x_d} \right)$$

showing that $\mathcal{M}$ occurs in the decomposition of $\mathbb{F}_u G/J(\mathbb{F}_u G)$ given in equation (4.2).

Recall that $n_l,\ m_j = 1$ or q and

$$\begin{aligned} & 1 \ + \sum_{d \in \mathcal{A}_n} o_d \times x_d \ + \ q^2 \left(\sum_{d \in \mathcal{B}_n} i_d \times y_d \right) \\ = \ & 1 \ + \sum_{d \in \mathcal{A}_n} \varphi(d) + \ q \left(\sum_{d \in \mathcal{B}_n} \varphi(d) \right) \\ = \ & n + (q-1) \left(\sum_{d \in \mathcal{B}_n} \varphi(d) \right) \\ = \ & nq - (q-1) \left(n - \sum_{d \in \mathcal{B}_n} \varphi(d) \right) \\ = \ & |G| - dim_{\ \mathbb{F}_{u^{o_n}}} \ J(\mathbb{F}_{u^{o_n}} G) \\ = \ & |G| - dim_{\ \mathbb{F}_u} \ J(\mathbb{F}_u G) \text{ using [10, Theorem 7.9]} \end{aligned}$$

Therefore

$$\mathbb{F}_u G/J(\mathbb{F}_u G) \ \cong \ \mathbb{F}_u \ \oplus \ \left(\bigoplus_{d \in \mathcal{A}_n} (\ \mathbb{F}_{u^{o_d}}\ )^{\ x_d} \right) \ \oplus \ \left(\bigoplus_{d \in \mathcal{B}_n} M\left(q, \mathbb{F}_{u^{i_d}}\right)^{y_d} \right)$$

Via similar arguments the theorem holds true even when $\mathcal{A}_n = \emptyset$. □

5. Main result

The main result of the paper is as follows.

Theorem 5.1. *Let* $u = q^k$ *and* $G = C_n \rtimes_r C_q$ *where* $(n, q) = 1$. *If* $ord_d(r) = q$ *for every divisor* $d(> 1)$ *of* n, *then*

$$\mathcal{U}\left(\mathbb{F}_u G\right) \cong C_q^{k(q-1)} \times \left(C_{u-1} \times \prod_{\substack{d\ > 1 \\ d\ |\ n}} GL(q, \mathbb{F}_{u^{i_d}})^{y_d} \right)$$

where i_d *is the least positive integer such that*

$$u^{i_d} \equiv r^j \ mod\ d$$

for some $0 \le j \le q-1$ *and* $y_d = \frac{\varphi(d)}{q\ i_d}$. *In particular,*

$$\mathcal{U}\left(\mathbb{F}_u (C_p \rtimes C_q)\right) \cong C_q^{k(q-1)} \rtimes (\ C_{u-1} \times GL\left(q, \mathbb{F}_{u^{i_p}}\right)^{y_p}\ )$$

where p is a prime different from q.

Proof. Since $b^i\widehat{a} \in \mathcal{Z}(\mathbb{F}_uG)\ \forall\ 0 \le i \le q-1$, therefore if $\sum_{i=0}^{q-1} \alpha_i = 0$, then for any $X \in \mathbb{F}_uG$,

$$\left(1 + X\sum_{i=0}^{q-1} \alpha_i\ b^i\widehat{a}\right)^q = 1$$

showing that

$$\left\{ \sum_{i=0}^{q-1} \alpha_i\ b^i\widehat{a}\ \middle|\ \alpha_i \in \mathbb{F}_u \text{ such that } \sum_{i=0}^{q-1} \alpha_i = 0 \right\} \subseteq J(\mathbb{F}_uG).$$

But from the proof of Theorem 4.2, it follows that $dim_{\ \mathbb{F}_u}\ J(\mathbb{F}_uG) = q-1$ and hence equality.

Thus $1 + J(\mathbb{F}_uG) \cong C_q^{k(q-1)}$. Since $J(\mathbb{F}_uG) \subseteq \mathcal{Z}(\mathbb{F}_uG)$ and

$$\mathcal{U}(\mathbb{F}_uG) \cong (1 + J(\mathbb{F}_uG)) \rtimes \mathcal{U}\left(\mathbb{F}_uG/J(\mathbb{F}_uG)\right)$$

therefore the proof follows by using Theorem 4.2. □

Corollary 5.2. *Let D_{2n} be the dihedral group of order $2n$, n odd and $u = 2^k$. Then*

$$\mathcal{U}\left(\mathbb{F}_uD_{2n}\right) \cong C_2^k \times \left(C_{u-1} \times \prod_{\substack{d\ >1 \\ d\ |\ n}} GL(2, \mathbb{F}_{u^{i_d}})^{y_d} \right)$$

where $o_d = ord_d(u)$,

$$i_d = \begin{cases} \dfrac{o_d}{2} & \text{if } o_d \text{ is even and } u^{o_d/2} \equiv -1 \bmod d \\ o_d & \text{otherwise} \end{cases}$$

and $y_d = \frac{\varphi(d)}{2i_d}$.

Remark 5.3. *This is in accordance with the structure of the unit group of $\mathbb{F}_{2^k}D_{2n}$ determined by the authors in [24] for odd n.*

References

[1] G. K. Bakshi, S. Gupta and I. B. S. Passi, *Semisimple metacyclic group algebras*, Proc. Indian Acad. Sci. Math. Sci., 121(4) (2011), 379–396.

[2] G. K. Bakshi, S. Gupta and I. B. S. Passi, *The structure of finite semisimple metacyclic group algebras*, J. Ramanujan Math. Soc., 28(2) (2013), 141–158.

[3] A. Bovdi, *The group of units of a group algebra of characteristic p*, Publ. Math. Debrecen, 52(1-2) (1998), 193–244.

[4] V. Bovdi, *Group algebras whose group of units is powerful*, J. Aust. Math. Soc., 87(3) (2009), 325–328.

[5] V. Bovdi, L. G. Kovács and S. K. Sehgal, *Symmetric units in modular group algebras*, Comm. Algebra, 24(3) (1996), 803–808.

[6] A. A. Bovdi and J. Kurdics, *Lie properties of the group algebra and the nilpotency class of the group of units*, J. Algebra, 212(1) (1999), 28–64.

[7] O. Broche and Á. del Río, *Wedderburn decomposition of finite group algebras*, Finite Fields Appl., 13(1) (2007), 71–79.

[8] P. M. Cohn, Algebra, Vol. 2, Second edition, John Wiley & Sons, Ltd., Chichester, 1989.

[9] C. W. Curtis and I. Reiner, Representation Theory of Finite Groups and Associative Algebras, Pure and Applied Mathematics, Vol. XI, Interscience Publishers, a division of John Wiley & Sons, New York-London, 1962.

[10] C. W. Curtis and I. Reiner, Methods of Representation Theory, Vol. I, with applications to finite groups and orders, Pure and Applied Mathematics, a Wiley-Interscience Publication, John Wiley & Sons, Inc., New York, 1981.

[11] R. A. Ferraz, *Simple components of the center of $FG/J(FG)$*, Comm. Algebra, 36(9) (2008), 3191-3199.

[12] J. Gildea, *The structure of the unit group of the group algebra* $\mathbb{F}_{3^k}(C_3 \times D_6)$, Comm. Algebra, 38(9) (2010), 3311–3317.

[13] J. Gildea, *Units of the group algebra* $\mathbb{F}_{2^k}(C_2 \times D_8)$, J. Algebra Appl., 10(4) (2011), 643–647.

[14] J. Gildea, *The structure of the unitary units of the group algebra* $\mathbb{F}_{2^k}D_8$, Int. Electron. J. Algebra, 9 (2011), 171–176.

[15] J. Gildea, *Units of the group algebra* $\mathbb{F}_{5^k}(C_5 \rtimes C_4)$, Int. Electron. J. Algebra, 9 (2011), 220–227.

[16] J. Gildea, *The structure of the unit group of the group algebra* $\mathbb{F}_{2^k}A_4$, Czechoslovak Math. J., 61(136)(2) (2011), 531–539.

[17] P. Hurley and T. Hurley, *Codes from zero-divisors and units in group rings*, Int. J. Inf. Coding Theory, 1(1) (2009), 57–87.

[18] B. Hurley and T. Hurley, *Group ring cryptography*, Int. J. Pure Appl. Math., 69(1) (2011), 67–86.

[19] G. Karpilovsky, The Jacobson Radical of Group Algebras, North-Holland Mathematics Studies, 135, Notas de Matemtica [Mathematical Notes], 115, North-Holland Publishing Co., Amsterdam, 1987.

[20] K. Kaur and M. Khan, Structure of the Unit Group of $F(C_p \rtimes C_q)$, Conference on Groups, Group Rings and Related Topics, 2013.

[21] K. Kaur and M. Khan, *Units in* $\mathbb{F}_2 D_{2p}$, J. Algebra Appl., 13(2) (2014), 9 pp., DOI: 10.1142/S0219498813500904.

[22] M. Khan, R. K. Sharma and J. B. Srivastava, *The unit group of* FS_4, Acta Math. Hungar., 118(1-2), (2008), 105–113.

[23] R. Lidl and H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and its Applications, 20, Cambridge University Press, Cambridge, 1997.

[24] N. Makhijani, R. K. Sharma and J. B. Srivastava, *Units in* $\mathbb{F}_{2^k} D_{2n}$, Int. J. Group Theory, 3(3) (2014), 25–34.

[25] R. Sandling, *Units in the modular group algebra of a finite abelian p-group*, J. Pure Appl. Algebra, 33(3) (1984), 337–346.

[26] R. K. Sharma, J. B. Srivastava and M. Khan, *The unit group of* FA_4, Publ. Math. Debrecen, 71(1-2) (2007), 21–26.

[27] I. Van Gelder and G. Olteanu, *Finite group algebras of nilpotent groups: a complete set of orthogonal primitive idempotents*, Finite Fields Appl., 17(2) (2011), 157–165.

[28] I. Woungang, S. Misra and S. C. Misra, Selected Topics in Information and Coding Theory, Series on Coding Theory and Cryptology, 7, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2010.

N. Makhijani, R. K. Sharma and **J. B. Srivastava**
Department of Mathematics
Indian Institute of Technology
New Delhi, India
e-mails: nehamakhijani@gmail.com (N. Makhijani)
rksharmaiitd@gmail.com (R. K. Sharma)
jbsrivas@gmail.com (J. B. Srivastava)