Proc. Indian Acad. Sci. (Math. Sci.) Vol. 121, No. 4, November 2011, pp. 379–396.

Semisimple metacyclic group algebras

GURMEET K BAKSHI[1], SHALINI GUPTA[2]
and INDER BIR S PASSI[1,2]

[1]Centre for Advanced Study in Mathematics, Panjab University, Chandigarh 160 014, India
[2]Indian Institute of Science Education and Research, Mohali, MGSIPA Complex, Sector 26, Chandigarh 160 019, India
E-mail: gkbakshi@pu.ac.in, shalinigupta@iisermohali.ac.in; ibspassi@yahoo.co.in

MS received 20 October 2010; revised 20 January 2011

Abstract. Given a group G of order p_1p_2, where p_1, p_2 are primes, and $\mathbb{F}_q$, a finite field of order q coprime to p_1p_2, the object of this paper is to compute a complete set of primitive central idempotents of the semisimple group algebra $\mathbb{F}_q[G]$. As a consequence, we obtain the structure of $\mathbb{F}_q[G]$ and its group of automorphisms.

Keywords. Semisimple group algebra; primitive central idempotents; Wedderburn decomposition; automorphism group.

1. Introduction

Let $F[G]$ be the group algebra of a finite group G over a field F. The group algebra $F[G]$ is of interest in both pure and applied algebra. A good description of the Wedderburn decomposition of $F[G]$ is useful for describing the automorphism group of $F[G]$, for studying the unit group of $F[G]$ and has applications in coding theory. The problem of computing the Wedderburn decomposition of $F[G]$ naturally leads to the computation of the primitive central idempotents of $F[G]$. These problems have attracted the attention of several authors (see [1–8], [10], [11], [12], [14–21]).

In this paper, we restrict to the case, when $F = \mathbb{F}_q$ is a finite field with q elements and G is a group of order p_1p_2 coprime to q. In this case, we give explicit expressions for a complete set of primitive central idempotents (Theorem 1) and Wedderburn decomposition (Theorems 2 and 3) of $\mathbb{F}_q[G]$. Our result may be compared with the one provided in this case by Corollary 9 of [4]. As a consequence, we also derive the group of automorphisms of $\mathbb{F}_q[G]$ (Theorems 4 and 5). Finally, we give some illustrative examples.

2. Primitive central idempotents

Let $\mathbb{F}_q$ be a finite field with q elements and $\bar{\mathbb{F}}_q$ its algebraic closure. Let G be a finite group with $o(G)$, the order of G, coprime to q. We begin by recalling some standard facts about the irreducible characters of G over the algebraically closed field $\bar{\mathbb{F}}_q$. If $\chi \in \mathrm{Irr}(G)$, the set of irreducible characters of G over $\bar{\mathbb{F}}_q$, then

$$e(\chi) := \frac{\chi(1)}{o(G)} \sum_{g \in G} \chi(g) g^{-1}$$

is a primitive central idempotent of $\bar{\mathbb{F}}_q[G]$ and $\chi \mapsto e(\chi)$ is a 1-1 correspondence between $\mathrm{Irr}(G)$ and the set of all primitive central idempotents of $\bar{\mathbb{F}}_q[G]$. The Galois group $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ acts on $\mathrm{Irr}(G)$ by setting

$${}^{\sigma}\chi = \sigma \circ \chi, \quad \sigma \in \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q), \quad \chi \in \mathrm{Irr}(G).$$

Let $\mathrm{orb}(\chi)$ denote the orbit of $\chi \in \mathrm{Irr}(G)$ under this action. Observe that $\mathrm{orb}(\chi)$ is equal to $\{{}^{\sigma}\chi \mid \sigma \in \mathrm{Gal}(\mathbb{F}_q(\chi)/\mathbb{F}_q)\}$, where $\mathbb{F}_q(\chi)$ is the field obtained by adjoining to $\mathbb{F}_q$, all the character values $\chi(g)$, $g \in G$. It is known that for any $\chi \in \mathrm{Irr}(G)$,

$$e_{\mathbb{F}_q}(\chi) := \sum_{\psi \in \mathrm{orb}(\chi)} e(\psi) = \sum_{\sigma \in \mathrm{Gal}(\mathbb{F}_q(\chi)/\mathbb{F}_q)} e({}^{\sigma}\chi)$$

is a primitive central idempotent of $\mathbb{F}_q[G]$, and the map $\mathrm{orb}(\chi) \mapsto e_{\mathbb{F}_q}(\chi)$ is a 1-1 correspondence between the set $\{\mathrm{orb}(\chi) \mid \chi \in \mathrm{Irr}(G)\}$ of orbits and the primitive central idempotents of $\mathbb{F}_q[G]$ (see [22]; the treatment in [22] is when $\mathrm{char}\, F = 0$ but the arguments work in the present case).

Suppose G has order $p_1 p_2$, where $p_1,\ p_2$ are primes. If G is abelian, a description of the primitive central idempotents of $\mathbb{F}_q[G]$ can be read from the results in [2], [4], [18] and [19]. We thus assume throughout the rest of this section that G is a non-abelian group of order $p_1 p_2$ with $p_1 > p_2$ (say). In this case, we must have $p_1 \equiv 1 \mod p_2$. Let

$$G = \langle a, b \mid a^{p_1} = b^{p_2} = 1,\ b^{-1}ab = a^u \rangle, \tag{1}$$

where u is an element of order p_2 in $\mathbb{Z}_{p_1}^* = \mathbb{Z}_{p_1} \backslash \{0\}$, be a presentation of G. Let $f_1 := \mathrm{ord}_{p_1}(q)$, $f_2 := \mathrm{ord}_{p_2}(q)$ and $f_3 := \mathrm{ord}_{p_1 p_2}(q)$ be the multiplicative orders of q modulo p_1, p_2 and $p_1 p_2$ respectively. Let

$$e_1 := \frac{p_1 - 1}{f_1} \quad e_2 := \frac{p_2 - 1}{f_2} \quad e_3 := \frac{(p_1 - 1)(p_2 - 1)}{f_3}. \tag{2}$$

Let g_i be a primitive root modulo p_i and ζ_i a primitive p_i-th root of unity in $\bar{\mathbb{F}}_q$ ($i = 1$, 2). For $k \geq 0$, define

$$\eta_k^{(1)} := \sum_{j=0}^{f_1 - 1} \zeta_1^{g_1^k q^j}, \quad \eta_k^{(2)} := \sum_{j=0}^{f_2 - 1} \zeta_2^{g_2^k q^j}. \tag{3}$$

Set

$$K := \mathbb{F}_q \left(\sum_{r=0}^{p_2 - 1} \zeta_1^{iu^r} \mid i = 1, 2, \ldots, p_1 - 1 \right). \tag{4}$$

Our main result on primitive central idempotents of $\mathbb{F}_q[G]$ is the following:

Theorem 1.

(i) *If $p_2 \mid f_1$, then $\mathbb{F}_q[G]$ has exactly the following $e_1 + e_2 + 1$ distinct primitive central idempotents*:

$$\frac{1}{p_1 p_2} \sum_{g \in G} g,$$

$$\frac{1}{p_1 p_2} \left(f_2 \sum_{x=0}^{p_1-1} a^x + \sum_{j=0}^{p_2-2} \eta^{(2)}_{m+j} \left(\sum_{x=0}^{p_1-1} a^x b^{g_2^j} \right) \right), \quad 0 \le m \le e_2 - 1,$$

$$\frac{p_2}{p_1 \, [\mathbb{F}_q(\zeta_1) : K]} \left(f_1 + \sum_{k=0}^{p_1-2} \eta^{(1)}_{n+k} a^{g_1^k} \right), \quad 0 \le n \le e_1 - 1.$$

(ii) *If $p_2 \nmid f_1$, then $\mathbb{F}_q[G]$ has exactly the following $\frac{e_1}{p_2} + e_2 + 1$ distinct primitive central idempotents*:

$$\frac{1}{p_1 p_2} \sum_{g \in G} g,$$

$$\frac{1}{p_1 p_2} \left(f_2 \sum_{x=0}^{p_1-1} a^x + \sum_{j=0}^{p_2-2} \eta^{(2)}_{m+j} \left(\sum_{x=0}^{p_1-1} a^x b^{g_2^j} \right) \right), \quad 0 \le m \le e_2 - 1,$$

$$\frac{1}{p_1 \, [\mathbb{F}_q(\zeta_1) : K]} \left(f_1 p_2 + \sum_{i=0}^{p_1-2} \left(\sum_{j=0}^{p_2-1} \eta^{(1)}_{n+i+j.\frac{e_1}{p_2}} \right) a^{g_1^i} \right), \quad 0 \le n \le \frac{e_1}{p_2} - 1.$$

We will prove the theorem in a number of steps.

The primitive central idempotents of the group algebra $\mathbb{F}_q[\mathbb{Z}_{p^n}]$, where $\mathbb{Z}_{p^n}$ is the cyclic group of order p^n, p a prime, $n \ge 1$ and $p \nmid q$, have been computed in [18], [19]. We need the case $n = 1$, in which case, the description of primitive central idempotents is as follows:

Lemma 1. *Let $\langle a \rangle$ be a cyclic group of order p, where p is a prime coprime to q. Let $f = \mathrm{ord}_p(q)$, $e = (p-1)/f$ and g a primitive root modulo p. The group algebra $\mathbb{F}_q[\langle a \rangle]$ has exactly the following $e + 1$ distinct primitive* (*central*) *idempotents*:

$$\frac{1}{p}(1 + a + \cdots + a^{p-1}),$$

$$\frac{1}{p} \left(f + \sum_{j=0}^{p-2} \eta_{i+j} a^{g^j} \right), \quad 0 \le i \le e - 1$$

where $\eta_k = \sum_{j=0}^{f-1} \zeta^{g^k q^j}$, ζ a primitive p-th root of unity in $\bar{\mathbb{F}}_q$.

The complex irreducible characters of G have been computed in Theorem 25.10 of [9]; the same proof also works for the irreducible characters of G over the algebraically closed field $\bar{\mathbb{F}}_q$, thus yielding the following:

Lemma 2. *The group* $G = \langle a, b \mid a^{p_1} = b^{p_2} = 1,\ b^{-1}ab = a^u\rangle$, *has exactly* $p_2 + \frac{p_1-1}{p_2}$ *irreducible characters over* $\bar{\mathbb{F}}_q$, *of which* p_2 *characters are of degree* 1 *and* $\frac{p_1-1}{p_2}$ *are of degree* p_2. *The non-trivial irreducible characters*, ψ_m, $0 \le m \le p_2 - 2$, *of degree* 1 *are given by*

$$\psi_m(a^x b^y) = \zeta_2^{-g_2^m y}, \quad a^x b^y \in G, \quad 0 \le m \le p_2 - 2$$

and the irreducible characters ϕ_n, $0 \le n \le \frac{p_1-1}{p_2} - 1$, *of degree* p_2 *over* $\bar{\mathbb{F}}_q$ *are given by*

$$\phi_n(a^x b^y) = \begin{cases} 0, & y \neq 0, \\ \sum_{j=0}^{p_2-1} \zeta_1^{-x.g_1^{\frac{p_1-1}{p_2}.j+n}}, & y = 0. \end{cases}$$

We now describe the primitive central idempotents of $\mathbb{F}_q[G]$ associated with the irreducible characters of degree 1. Let $\iota : G \to \bar{\mathbb{F}}_q$ be the trivial character of G. Clearly

$$e_{\mathbb{F}_q}(\iota) = \frac{1}{p_1 p_2} \sum_{g \in G} g. \tag{5}$$

Lemma 3. *For* $0 \le m \le p_2 - 2$,

$$e_{\mathbb{F}_q}(\psi_m) = \frac{1}{p_1 p_2}\left(f_2 \sum_{x=0}^{p_1-1} a^x + \sum_{j=0}^{p_2-2} \eta_{m+j}^{(2)} \left(\sum_{x=0}^{p_1-1} a^x b^{g_2^j} \right)\right),$$

and $e_{\mathbb{F}_q}(\psi_m) = e_{\mathbb{F}_q}(\psi_{m'})$ *if, and only if,* $m \equiv m' \bmod e_2$.

Proof. Let $0 \le m \le p_2 - 2$.

$$\begin{aligned} e_{\mathbb{F}_q}(\psi_m) &= \sum_{\sigma \in \mathrm{Gal}(\mathbb{F}_q(\psi_m)/\mathbb{F}_q)} e({}^{\sigma}\psi_m) \\ &= \sum_{\sigma \in \mathrm{Gal}(\mathbb{F}_q(\zeta_2)/\mathbb{F}_q)} e({}^{\sigma}\psi_m), \quad \text{since } \mathbb{F}_q(\psi_m) = \mathbb{F}_q(\zeta_2) \\ &= \frac{1}{p_1 p_2}\left(\sum_{x=0}^{p_1-1} \sum_{y=0}^{p_2-1} \left(\sum_{\sigma \in \mathrm{Gal}(\mathbb{F}_q(\zeta_2)/\mathbb{F}_q)} \sigma(\zeta_2^{g_2^m y}) \right) a^x b^y \right) \\ &= \frac{1}{p_1 p_2}\left(f_2 \sum_{x=0}^{p_1-1} a^x + \sum_{y=1}^{p_2-1} \left(\sum_{i=0}^{f_2-1} (\zeta_2^{g_2^m y})^{q^i} \right) \left(\sum_{x=0}^{p_1-1} a^x b^y \right)\right) \end{aligned}$$

$$= \frac{1}{p_1 p_2}\left(f_2 \sum_{x=0}^{p_1-1} a^x + \sum_{j=0}^{p_2-2}\left(\sum_{i=0}^{f_2-1} (\zeta_2^{g_2^{m+j}})^{q^i}\right)\left(\sum_{x=0}^{p_1-1} a^x b^{g_2^j}\right)\right)$$

$$= \frac{1}{p_1 p_2}\left(f_2 \sum_{x=0}^{p_1-1} a^x + \sum_{j=0}^{p_2-2} \eta_{m+j}^{(2)}\left(\sum_{x=0}^{p_1-1} a^x b^{g_2^j}\right)\right).$$

As $\eta_i^{(2)} = \eta_{i+e_2}^{(2)}$ for all $i \geq 0$, it follows that $e_{\mathbb{F}_q}(\psi_m) = e_{\mathbb{F}_q}(\psi_{m+e_2})$. Furthermore, $e_{\mathbb{F}_q}(\psi_m)$, for $0 \leq m \leq e_2 - 1$, are distinct since, in view of Lemma 1, tuple $(\eta_m^{(2)}, \eta_{m+1}^{(2)}, \eta_{m+2}^{(2)}, \ldots)$ is not equal to the tuple $(\eta_{m'}^{(2)}, \eta_{m'+1}^{(2)}, \eta_{m'+2}^{(2)}, \ldots)$ for $0 \leq m,\ m' \leq e_2 - 1, m \neq m'$. □

In the next lemma, we describe the primitive central idempotents $e_{\mathbb{F}_q}(\phi_n)$, $0 \leq n \leq \frac{p_1-1}{p_2} - 1$, associated with non-linear irreducible characters.

Lemma 4.

(i) *If* $p_2 \mid f_1$, *then, for* $0 \leq n \leq \frac{p_1-1}{p_2} - 1$,

$$e_{\mathbb{F}_q}(\phi_n) = \frac{p_2}{p_1[\mathbb{F}_q(\zeta_1) : K]}\left(f_1 + \sum_{k=0}^{p_1-2} \eta_{n+k}^{(1)} a^{g_1^k}\right)$$

and $e_{\mathbb{F}_q}(\phi_n) = e_{\mathbb{F}_q}(\phi_{n'})$ *if and only if* $n \equiv n' \bmod e_1$.

(ii) *If* $p_2 \nmid f_1$, *then, for* $0 \leq n \leq \frac{p_1-1}{p_2} - 1$,

$$e_{\mathbb{F}_q}(\phi_n) = \frac{1}{[\mathbb{F}_q(\zeta_1) : K]\, p_1}\left(f_1 p_2 + \sum_{i=0}^{p_1-2}\left(\sum_{j=0}^{p_2-1} \eta^{(1)}_{n+i+j\cdot\frac{e_1}{p_2}}\right) a^{g_1^i}\right)$$

and $e_{\mathbb{F}_q}(\phi_n) = e_{\mathbb{F}_q}(\phi_{n'})$ *if and only if* $n \equiv n' \bmod \frac{e_1}{p_2}$.

Proof. Observe that $\mathbb{F}_q(\phi_n) = K$ for all $n \geq 0$. Therefore,

$$\begin{aligned}
[\mathbb{F}_q(\zeta_1) : K] e_{\mathbb{F}_q}(\phi_n) &= [\mathbb{F}_q(\zeta_1) : K] \sum_{\sigma \in \mathrm{Gal}(\mathbb{F}_q(\phi_n)/\mathbb{F}_q)} e({}^{\sigma}\phi_n) \\
&= [\mathbb{F}_q(\zeta_1) : K] \sum_{\sigma \in \mathrm{Gal}(K/\mathbb{F}_q)} e({}^{\sigma}\phi_n) \\
&= \sum_{\sigma \in \mathrm{Gal}(\mathbb{F}_q(\zeta_1)/\mathbb{F}_q)} e({}^{\sigma}\phi_n) \\
&= \sum_{\sigma \in \mathrm{Gal}(\mathbb{F}_q(\zeta_1)/\mathbb{F}_q)} \left(\frac{p_2}{p_1 p_2} \sum_{x=0}^{p_1-1} \sigma(\phi_n(a^{-x})) a^x\right)
\end{aligned}$$

$$
\begin{aligned}
&= \frac{p_2}{p_1p_2}\sum_{x=0}^{p_1-1}\sum_{j=0}^{p_2-1}\sum_{\sigma\in \mathrm{Gal}(\mathbb{F}_q(\zeta_1)/\mathbb{F}_q)} \sigma\left(\zeta_1^{x\cdot g_1^{\frac{p_1-1}{p_2}\cdot j+n}}\right)a^x \\
&= \frac{1}{p_1}\sum_{x=0}^{p_1-1}\sum_{j=0}^{p_2-1}\sum_{l=0}^{f_1-1}\left(\zeta_1^{x\cdot g_1^{\frac{p_1-1}{p_2}\cdot j+n}}\right)^{q^l} a^x \\
&= \frac{1}{p_1}\left(f_1p_2+\sum_{i=0}^{p_1-2}\sum_{j=0}^{p_2-1}\sum_{l=0}^{f_1-1}\left(\zeta_1^{g_1^{\frac{p_1-1}{p_2}\cdot j+n+i}}\right)^{q^l} a^{g_1^i}\right).
\end{aligned} \tag{6}
$$

Case 1. $p_2 \mid f_1$. In this case, $g_1^{\frac{p_1-1}{p_2}\cdot j} \in \langle q\rangle \subseteq \mathbb{Z}_{p_1}^*$ for all j, $0\le j\le p_2-1$. Therefore,

$$
\sum_{l=0}^{f_1-1}\left(\zeta_1^{g_1^{\frac{p_1-1}{p_2}\cdot j+n+i}}\right)^{q^l} = \sum_{l=0}^{f_1-1}\left(\zeta_1^{g_1^{n+i}}\right)^{q^l} = \eta_{n+i}^{(1)}
$$

for $0\le j\le p_2-1$. Substituting in eq. (6), we get

$$
\begin{aligned}
[\mathbb{F}_q(\zeta_1):K]e_{\mathbb{F}_q}(\phi_n) &= \frac{1}{p_1}\left(f_1p_2+\sum_{i=0}^{p_1-2}\sum_{j=0}^{p_2-1}\eta_{n+i}^{(1)}a^{g_1^i}\right) \\
&= \frac{1}{p_1}\left(f_1p_2+p_2\sum_{i=0}^{p_1-2}\eta_{n+i}^{(1)}a^{g_1^i}\right) \\
&= \frac{p_2}{p_1}(f_1+\sum_{i=0}^{p_1-2}\eta_{n+i}^{(1)}a^{g_1^i}).
\end{aligned}
$$

Since the right-hand side of the above equation is non-zero, it follows that $[\mathbb{F}_q(\zeta_1):K]$ is invertible in $\mathbb{F}_q$ and, consequently,

$$
e_{\mathbb{F}_q}(\phi_n) = \frac{p_2}{[\mathbb{F}_q(\zeta_1):K]\,p_1}\left(f_1+\sum_{i=0}^{p_1-2}\eta_{n+i}^{(1)}a^{g_1^i}\right).
$$

Since $\eta_i^{(1)} = \eta_{i+e_1}^{(1)}$ for all $i\ge 0$, we have $e_{\mathbb{F}_q}(\phi_n) = e_{\mathbb{F}_q}(\phi_{n+e_1})$. Also $e_{\mathbb{F}_q}(\phi_n)$, $0\le n\le e_1-1$ are all distinct, since, in view of Lemma 1, the tuple $(\eta_n^{(1)}, \eta_{n+1}^{(1)}, \eta_{n+2}^{(1)}, \ldots)$ is not equal to the tuple $(\eta_{n'}^{(1)}, \eta_{n'+1}^{(1)}, \eta_{n'+2}^{(1)}, \ldots)$ for $0\le n,\ n'\le e_1-1$, $n\ne n'$.

Case 2. $p_2 \nmid f_1$. For $1\le j\le p_2-1$, let j' be the remainder obtained on dividing $f_1 j$ by p_2. We observe that $\left(g_1^{\frac{p_1-1}{p_2}\cdot j-\frac{e_1}{p_2}\cdot j'}\right)^{f_1} = g_1^{e_1f_1\frac{f_1j-j'}{p_2}} \equiv 1 \mod p_1$. This gives

$g_1^{\frac{p_1-1}{p_2}\cdot j - \frac{e_1}{p_2}\cdot j'} \in \langle q \rangle \subseteq \mathbb{Z}_{p_1}^*$. Hence,

$$\sum_{l=0}^{f_1-1}\left(\zeta_1^{g_1^{\frac{p_1-1}{p_2}\cdot j+n+i}}\right)^{q^l} = \sum_{l=0}^{f_1-1}\left(\zeta_1^{g_1^{\frac{e_1}{p_2}\cdot j'+n+i}}\right)^{q^l} = \eta^{(1)}_{n+i+\frac{e_1}{p_2}\cdot j'}.$$

Note that as j runs through 1 to $p_2 - 1$, so does j'. Therefore,

$$\sum_{j=1}^{p_2-1}\sum_{l=0}^{f_1-1}\left(\zeta_1^{g_1^{\frac{p_1-1}{p_2}\cdot j+n+i}}\right)^{q^l} = \sum_{j'=1}^{p_2-1}\eta^{(1)}_{n+i+\frac{e_1}{p_2}\cdot j'}. \tag{7}$$

From equations (6) and (7), we obtain

$$\begin{aligned}
&[\mathbb{F}_q(\zeta_1) : K]e_{\mathbb{F}_q}(\phi_n)\\
&= \frac{1}{p_1}\left(f_1 p_2 + \sum_{i=0}^{p_1-2}\sum_{j=0}^{p_2-1}\sum_{l=0}^{f_1-1}\left(\zeta_1^{g_1^{\frac{p_1-1}{p_2}\cdot j+n+i}}\right)^{q^l} a^{g_1^i}\right)\\
&= \frac{1}{p_1}\left(f_1 p_2 + \sum_{i=0}^{p_1-2}\left(\sum_{l=0}^{f_1-1}(\zeta_1^{g_1^{n+i}})^{q^l} + \sum_{j=1}^{p_2-1}\sum_{l=0}^{f_1-1}(\zeta_1^{g_1^{\frac{p_1-1}{p_2}\cdot j+n+i}})^{q^l}\right)a^{g_1^i}\right)\\
&= \frac{1}{p_1}\left(f_1 p_2 + \sum_{i=0}^{p_1-2}\left(\eta^{(1)}_{n+i} + \sum_{j=1}^{p_2-1}\eta^{(1)}_{n+i+\frac{e_1}{p_2}\cdot j}\right)a^{g_1^i}\right)\\
&= \frac{1}{p_1}\left(f_1 p_2 + \sum_{i=0}^{p_1-2}\left(\sum_{j=0}^{p_2-1}\eta^{(1)}_{n+i+j\frac{e_1}{p_2}}\right)a^{g_1^i}\right).
\end{aligned} \tag{8}$$

We next see that the right-hand side of eq. (8) is non-zero. Suppose not, then

$$\eta^{(1)}_{n+i} + \eta^{(1)}_{n+i+\frac{e_1}{p_2}} + \eta^{(1)}_{n+i+2\cdot\frac{e_1}{p_2}} + \cdots + \eta^{(1)}_{n+i+(p_2-1)\frac{e_1}{p_2}} = 0,$$

for $0 \le i \le p_1 - 2$. In particular,

$$\eta^{(1)}_0 + \eta^{(1)}_{\frac{e_1}{p_2}} + \eta^{(1)}_{2\cdot\frac{e_1}{p_2}} + \cdots + \eta^{(1)}_{(p_2-1)\frac{e_1}{p_2}} = 0$$

$$\eta^{(1)}_1 + \eta^{(1)}_{1+\frac{e_1}{p_2}} + \eta^{(1)}_{1+2\cdot\frac{e_1}{p_2}} + \cdots + \eta^{(1)}_{1+(p_2-1)\frac{e_1}{p_2}} = 0$$

$\cdots$

$$\eta^{(1)}_{\frac{e_1}{p_2}-1} + \eta^{(1)}_{\frac{e_1}{p_2}-1+\frac{e_1}{p_2}} + \eta^{(1)}_{\frac{e_1}{p_2}-1+2\cdot\frac{e_1}{p_2}} + \cdots + \eta^{(1)}_{\frac{e_1}{p_2}-1+(p_2-1)\frac{e_1}{p_2}} = 0.$$

On adding the above system of equations, we get $\eta_0^{(1)} + \eta_1^{(1)} + \cdots + \eta_{e_1-1}^{(1)} = 0$, which is a contradiction, since $\sum_{i=0}^{e_1-1} \eta_i^{(1)} = -1$. Consequently, $[\mathbb{F}_q(\zeta_1) : K]$ is invertible in $\mathbb{F}_q$ and

$$e_{\mathbb{F}_q}(\phi_n) = \frac{1}{[\mathbb{F}_q(\zeta_1) : K]\, p_1} \left(f_1 p_2 + \sum_{i=0}^{p_1-2} \left(\sum_{j=0}^{p_2-1} \eta^{(1)}_{n+i+j\frac{e_1}{p_2}} \right) a^{g_1^i} \right).$$

It is clear from the above expression that $e_{\mathbb{F}_q}(\phi_n) = e_{\mathbb{F}_q}(\phi_{n+\frac{e_1}{p_2}})$. That the idempotents $e_{\mathbb{F}_q}(\phi_n)$, $0 \le n \le \frac{e_1}{p_2} - 1$ are all distinct is a consequence of the following:

Lemma 5. *For* $0 \le n,\ n' \le \frac{e_1}{p_2} - 1$, $n \ne n'$, *there exists* i, $0 \le i \le p_1 - 2$, *such that*

$$\sum_{j=0}^{p_2-1} \eta^{(1)}_{n+i+j\frac{e_1}{p_2}} \ne \sum_{j=0}^{p_2-1} \eta^{(1)}_{n'+i+j\frac{e_1}{p_2}}.$$

Proof. Let $\theta_i := \frac{1}{p_1}(f_1 + \sum_{j=0}^{p_1-2} \eta_{i+j}^{(1)} a^{g_1^j})$, $0 \le i \le e_1 - 1$ be the primitive central idempotents of $\mathbb{F}_q[\langle a \rangle]$ as given in Lemma 1. Suppose the lemma is not true, i.e., we have

$$\sum_{j=0}^{p_2-1} \eta^{(1)}_{n+i+j\frac{e_1}{p_2}} = \sum_{j=0}^{p_2-1} \eta^{(1)}_{n'+i+j\frac{e_1}{p_2}},$$

for $0 \le i \le p_1 - 2$. It then follows that

$$\sum_{j=0}^{p_2-1} \theta_{k+j\frac{e_1}{p_2}} = \sum_{j=0}^{p_2-1} \theta_{k+n'-n+j\frac{e_1}{p_2}},$$

for $0 \le k \le \frac{e_1}{p_2} - 1$. Therefore,

$$\begin{aligned}
\sum_{j=0}^{p_2-1} \theta_{k+j\frac{e_1}{p_2}} &= \left(\sum_{j=0}^{p_2-1} \theta_{k+j\frac{e_1}{p_2}} \right)^2 \\
&= \left(\sum_{i=0}^{p_2-1} \theta_{k+i\cdot\frac{e_1}{p_2}} \right) \left(\sum_{j=0}^{p_2-1} \theta_{k+n'-n+j\cdot\frac{e_1}{p_2}} \right) \\
&= \sum_{i=0}^{p_2-1} \sum_{j=0}^{p_2-1} \theta_{k+i\cdot\frac{e_1}{p_2}} \theta_{k+n'-n+j\cdot\frac{e_1}{p_2}}.
\end{aligned}$$

However, for $0 \le i,\ j \le p_2 - 1$, $n \ne n'$, the idempotent $\theta_{k+i\cdot\frac{e_1}{p_2}}$ is orthogonal to $\theta_{k+n'-n+j\cdot\frac{e_1}{p_2}}$. Thus we have

$$\sum_{j=0}^{p_2-1} \theta_{k+j\frac{e_1}{p_2}} = 0, \quad 0 \le k \le \frac{e_1}{p_2} - 1.$$

Adding these equations, we get

$$\sum_{k=0}^{\frac{e_1}{p_2}-1} \sum_{j=0}^{p_2-1} \theta_{k+j\frac{e_1}{p_2}} = 0.$$

Now the left-hand side of the above equation is equal to $\sum_{i=0}^{e_1-1} \theta_i$. We thus have a contradiction, since

$$\sum_{i=0}^{e_1-1} \theta_i = 1 - \frac{1}{p_1} \sum_{i=0}^{p_1-1} a^i \neq 0. \qquad \square$$

Remark 1. It turns out (see eq. (14)) that

$$[\mathbb{F}_q(\zeta_1) : K] = \begin{cases} p_2, & p_2 \mid f_1, \\ 1, & p_2 \nmid f_1. \end{cases}$$

Theorem 1 is now an immediate consequence of the foregoing lemmas.

3. Wedderburn decomposition of $\mathbb{F}_q[G]$

If G is an abelian group of order $p_1 p_2$, then $G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$ (in case $p_1 = p_2 = p$, say); otherwise $G \cong \mathbb{Z}_{p_1} \oplus \mathbb{Z}_{p_2}$. Let

$$f := \mathrm{ord}_p(q) \quad \text{and} \quad f' := \mathrm{ord}_{p^2}(q). \tag{9}$$

Set

$$e := \frac{p-1}{f} \quad \text{and} \quad e' := \frac{p(p-1)}{f'}. \tag{10}$$

The Wedderburn decomposition of $\mathbb{F}_q[G]$ in this case given in Proposition 2 of [4] can be seen to read as follows:

Theorem 2.

(i) *If* $G \cong \mathbb{Z}_{p^2}$, *then*

$$\mathbb{F}_q[G] \cong \mathbb{F}_q \oplus \underbrace{\mathbb{F}_{q^f} \oplus \cdots \oplus \mathbb{F}_{q^f}}_{e} \oplus \underbrace{\mathbb{F}_{q^{f'}} \oplus \cdots \oplus \mathbb{F}_{q^{f'}}}_{e'}.$$

(ii) *If* $G \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$, *then*

$$\mathbb{F}_q[G] \cong \mathbb{F}_q \oplus \underbrace{\mathbb{F}_{q^f} \oplus \cdots \oplus \mathbb{F}_{q^f}}_{e(p+1)}.$$

(iii) *If* $G \cong \mathbb{Z}_{p_1} \oplus \mathbb{Z}_{p_2}$, *then*

$$\mathbb{F}_q[G] \cong \mathbb{F}_q \oplus \underbrace{\mathbb{F}_{q^{f_1}} \oplus \cdots \oplus \mathbb{F}_{q^{f_1}}}_{e_1} \oplus \underbrace{\mathbb{F}_{q^{f_2}} \oplus \cdots \oplus \mathbb{F}_{q^{f_2}}}_{e_2} \oplus \underbrace{\mathbb{F}_{q^{f_3}} \oplus \cdots \oplus \mathbb{F}_{q^{f_3}}}_{e_3}.$$

For $\chi \in \mathrm{Irr}(G)$, let $A(\chi, \mathbb{F}_q) := \mathbb{F}_q[G]e_{\mathbb{F}_q}(\chi)$. The following theorem describes the Wedderburn decomposition of $\mathbb{F}_q[G]$, when G is a non-abelian group of order $p_1 p_2$.

Theorem 3. *Let* $G = \langle a, b \mid a^{p_1} = b^{p_2} = 1,\ b^{-1}ab = a^u \rangle$ *be a metacyclic group of order* $p_1 p_2$, *where* p_1 *and* p_2 *are primes*, $p_2 \mid p_1 - 1$ *and* u, *an element of order* p_2 *in* $\mathbb{Z}_{p_1}^*$.

(i) *If* $p_2 | f_1$ *and* $f_1 = p_2 r$ (*say*), *then*

$$\mathbb{F}_q[G] \cong \mathbb{F}_q \oplus \underbrace{\mathbb{F}_{q^{f_2}} \oplus \cdots \oplus \mathbb{F}_{q^{f_2}}}_{e_2} \oplus \underbrace{M_{p_2}(\mathbb{F}_{q^r}) \oplus \cdots \oplus M_{p_2}(\mathbb{F}_{q^r})}_{e_1}.$$

(ii) *If* $p_2 \nmid f_1$, *then*

$$\mathbb{F}_q[G] \cong \mathbb{F}_q \oplus \underbrace{\mathbb{F}_{q^{f_2}} \oplus \cdots \oplus \mathbb{F}_{q^{f_2}}}_{e_2} \oplus \underbrace{M_{p_2}(\mathbb{F}_{q^{f_1}}) \oplus \cdots \oplus M_{p_2}(\mathbb{F}_{q^{f_1}})}_{\frac{e_1}{p_2}}.$$

Proof. Let

$$\tilde{e} := \begin{cases} e_1, & p_2 \mid f_1, \\ \frac{e_1}{p_2}, & p_2 \nmid f_1. \end{cases} \tag{11}$$

By Theorem 1, $e_{\mathbb{F}_q}(\iota)$, $e_{\mathbb{F}_q}(\psi_m)$, $e_{\mathbb{F}_q}(\phi_n)$, $0 \le m \le e_2 - 1$, $0 \le n \le \tilde{e} - 1$ constitute a complete set of distinct primitive central idempotents of $\mathbb{F}_q[G]$. Therefore,

$$\begin{aligned} \mathbb{F}_q[G] \ \cong\ & A(\iota, \mathbb{F}_q) \oplus A(\psi_0, \mathbb{F}_q) \oplus \cdots \oplus A(\psi_{e_2-1}, \mathbb{F}_q) \\ & \oplus A(\phi_0, \mathbb{F}_q) \oplus \cdots \oplus A(\phi_{\tilde{e}-1}, \mathbb{F}_q). \end{aligned}$$

We have $e_{\mathbb{F}_q}(\iota) = \frac{1}{p_1 p_2} \sum_{g \in G} g$ and $A(\iota, \mathbb{F}_q) = \mathbb{F}_q[G]e_{\mathbb{F}_q}(\iota) \cong \mathbb{F}_q$.

For $0 \le m \le e_2 - 1$, ψ_m being a linear character, $A(\psi_m, \mathbb{F}_q)$ is commutative and so $A(\psi_m, \mathbb{F}_q)$ is equal to its centre. But, in view of Proposition 1.4 of [22], the centre of $A(\psi_m, \mathbb{F}_q)$ is isomorphic to $\mathbb{F}_q(\psi_m) = \mathbb{F}_q(\zeta_2)$. Hence $A(\psi_m, \mathbb{F}_q) \cong \mathbb{F}_q(\zeta_2)$ for $0 \le m \le e_2 - 1$.

For $0 \le i \le \tilde{e} - 1$, by Wedderburn structure theorem, $A(\phi_i, \mathbb{F}_q) = \mathbb{F}_q[G]e_{\mathbb{F}_q}(\phi_i) \cong M_{n_i}(D_i)$ for some finite dimensional division algebra D_i, say, over $\mathbb{F}_q$ and $n_i \ge 1$. Since $\mathbb{F}_q$ is a finite field, D_i is a finite division algebra and therefore D_i is a field and so the centre of $A(\phi_i, \mathbb{F}_q)$ is isomorphic to D_i. However, again in view of *loc. cit.* of [22], the centre of $A(\phi_i, \mathbb{F}_q)$ is isomorphic to $\mathbb{F}_q(\phi_i) = K$. Therefore, $D_i \cong K$. Observe that

$A(\phi_i, \mathbb{F}_q)$ $0 \le i \le \tilde{e}-1$ are all isomorphic as $\mathbb{F}_q$-vector spaces. Therefore, it follows that $n_0 = n_1 = \cdots = n_{\tilde{e}} = \tilde{n}$ (say). Consequently, $A(\phi_i, \mathbb{F}_q) \cong M_{\tilde{n}}(K)$ for $0 \le i \le \tilde{e}-1$ and

$$\mathbb{F}_q[G] \cong \mathbb{F}_q \oplus \underbrace{\mathbb{F}_q(\zeta_2) \oplus \cdots \oplus \mathbb{F}_q(\zeta_2)}_{e_2} \oplus \underbrace{M_{\tilde{n}}(K) \oplus \cdots \oplus M_{\tilde{n}}(K)}_{\tilde{e}} . \tag{12}$$

Furthermore,

$$Z(\mathbb{F}_q[G]) \cong \mathbb{F}_q \oplus \underbrace{\mathbb{F}_q(\zeta_2) \oplus \cdots \oplus \mathbb{F}_q(\zeta_2)}_{e_2} \oplus \underbrace{K \oplus \cdots \oplus K}_{\tilde{e}} , \tag{13}$$

where $Z(\mathbb{F}_q[G])$ is the centre of $\mathbb{F}_q[G]$. On comparing the dimension over $\mathbb{F}_q$ on both sides of eqs (12) and (13), we obtain that $\tilde{n} = p_2$ and

$$[K : \mathbb{F}_q] = \begin{cases} \dfrac{f_1}{p_2}, & p_2 \mid f_1, \\ \\ f_1, & p_2 \nmid f_1. \end{cases} \tag{14}$$

This completes the proof. $\square$

4. Automorphism group

Let $n \ge 1$. Let S_n denote the symmetric group on n symbols; $\mathbb{Z}_n$, the cyclic group of order n; and $\mathrm{SL}_n(F)$, the group of $n \times n$ invertible matrices over the field F of determinant 1. For any group H, $H^{(n)}$ denotes a direct sum of n copies of H. By $H_1 \rtimes H_2$, we mean the split extension of the group H_1 by the group H_2. For any $\mathbb{F}_q$-algebra $\mathbf{A}$, $\mathrm{Aut}(\mathbf{A})$ denotes the group of $\mathbb{F}_q$-automorphism of the algebra $\mathbf{A}$.

Theorem 4. *Let G be as in Theorem* 2.

(i) *If $G \cong \mathbb{Z}_{p^2}$, then*

$$\mathrm{Aut}(\mathbb{F}_q[G]) \cong \begin{cases} (\mathbb{Z}_f^{(e)} \rtimes S_e) \oplus (\mathbb{Z}_{f'}^{(e')} \rtimes S_{e'}), & f \ne f',\ f \ne 1, \\ S_{e+1} \oplus (\mathbb{Z}_{f'}^{(e')} \rtimes S_{e'}), & f \ne f',\ f = 1, \\ \mathbb{Z}_f^{(e+e')} \rtimes S_{e+e'}, & f = f',\ f \ne 1, \\ S_{e+e'+1}, & f = f' = 1. \end{cases}$$

(ii) *If $G \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$, then*

$$\mathrm{Aut}(\mathbb{F}_q[G]) \cong \begin{cases} \mathbb{Z}_f^{(e(p+1))} \rtimes S_{e(p+1)}, & f \ne 1, \\ S_{e(p+1)+1}, & f = 1. \end{cases}$$

(iii) *If* $G \cong \mathbb{Z}_{p_1} \oplus \mathbb{Z}_{p_2}$, *then*

$$\mathrm{Aut}(\mathbb{F}_q[G]) \cong \begin{cases} (\mathbb{Z}_{f_1}^{(e_1)} \rtimes S_{e_1}) \oplus (\mathbb{Z}_{f_2}^{(e_2)} \rtimes S_{e_2}) \oplus (\mathbb{Z}_{f_3}^{(e_3)} \rtimes S_{e_3}), & f_1 \neq f_2,\ f_1 \neq 1,\ f_2 \neq 1, \\ S_{e_1+1} \oplus (\mathbb{Z}_{f_2}^{(e_2+e_3)} \rtimes S_{e_2+e_3}), & f_1 \neq f_2,\ f_1 = 1, \\ S_{e_2+1} \oplus (\mathbb{Z}_{f_1}^{(e_1+e_3)} \rtimes S_{e_1+e_3}), & f_1 \neq f_2,\ f_2 = 1, \\ \mathbb{Z}_{f_1}^{(e_1+e_2+e_3)} \rtimes S_{e_1+e_2+e_3}, & f_1 = f_2,\ f_1 \neq 1, \\ S_{e_1+e_2+e_3+1}, & f_1 = f_2 = 1. \end{cases}$$

Proof.

(i) We have, by Theorem 2(i),

$$\mathbb{F}_q[G] \cong \mathbb{F}_q \oplus \mathcal{A} \oplus \mathcal{A}',$$

where $\mathcal{A} = \underbrace{\mathbb{F}_{q^f} \oplus \cdots \oplus \mathbb{F}_{q^f}}_{e}$ and $\mathcal{A}' = \underbrace{\mathbb{F}_{q^{f'}} \oplus \cdots \oplus \mathbb{F}_{q^{f'}}}_{e'}$.

We first consider the case when $f \neq f'$, $f \neq 1$. Since $f | f'$, we also have in this case that $f' \neq 1$. Observe, in view of Lemma 3.8 of [13], that any $\sigma \in \mathrm{Aut}(\mathbb{F}_q[G])$, is identity on $\mathbb{F}_q$ and keeps $\mathcal{A}$ and $\mathcal{A}'$ invariant, i.e $\sigma(\mathcal{A}) = \mathcal{A}$ and $\sigma(\mathcal{A}') = \mathcal{A}'$. This gives a map $\mathrm{Aut}(\mathbb{F}_q[G]) \to \mathrm{Aut}(\mathcal{A}) \oplus \mathrm{Aut}(\mathcal{A}')$ by setting $\sigma \mapsto (\sigma|_{\mathcal{A}}, \sigma|_{\mathcal{A}'})$, which is an isomorphism, where $\sigma|_{\mathcal{A}}$ (resp. $\sigma|_{\mathcal{A}'}$) is the restriction of σ to $\mathcal{A}$ (resp. $\mathcal{A}'$).

Also, by Lemma 3.8 of [13], any $\sigma \in \mathrm{Aut}(\mathcal{A})$ defines a permutation $\tilde{\sigma}$, say, in S_e. Therefore, we have a map $\sigma \mapsto \tilde{\sigma}$ from $\mathrm{Aut}(\mathcal{A})$ to S_e, which can be seen to be an epimorphism with kernel $(\mathrm{Gal}(\mathbb{F}_{q^f}/\mathbb{F}_q))^{(e)} \cong \mathbb{Z}_f^{(e)}$. Thus $\mathrm{Aut}(\mathcal{A})$ is an extension of $\mathbb{Z}_f^{(e)}$ by S_e. One can check that this extension splits. Hence $\mathrm{Aut}(\mathcal{A}) \cong \mathbb{Z}_f^{(e)} \rtimes S_e$. Similarly $\mathrm{Aut}(\mathcal{A}') \cong \mathbb{Z}_{f'}^{(e')} \rtimes S_{e'}$, which proves the first case of (i). Similarly the other cases of (i) follow.

(ii) and (iii) can be proved similarly. □

Theorem 5. *Let G be as in Theorem* 3.

(i) *If* $p_2 \mid f_1$, *then*

$$\mathrm{Aut}(\mathbb{F}_q[G]) \cong \begin{cases} (\mathbb{Z}_{f_2}^{(e_2)} \rtimes S_{e_2}) \oplus (H_1^{(e_1)} \rtimes S_{e_1}), & f_2 \neq 1, \\ S_{e_2+1} \oplus (H_1^{(e_1)} \rtimes S_{e_1}), & f_2 = 1, \end{cases}$$

where $H_1 = \mathrm{SL}_{p_2}(\mathbb{F}_{q^r}) \rtimes \mathbb{Z}_r$.

(ii) *If* $p_2 \nmid f_1$, *then*

$$\mathrm{Aut}(\mathbb{F}_q[G]) \cong \begin{cases} (\mathbb{Z}_{f_2}^{(e_2)} \rtimes S_{e_2}) \oplus (H_2^{(e_1/p_2)} \rtimes S_{e_1/p_2}), & f_2 \neq 1, \\ S_{e_2+1} \oplus (H_2^{(e_1/p_2)} \rtimes S_{e_1/p_2}), & f_2 = 1, \end{cases}$$

where $H_2 = \mathrm{SL}_{p_2}(\mathbb{F}_{q^{f_1}}) \rtimes \mathbb{Z}_{f_1}$.

Proof.

(i) We have, by Theorem 3(i),

$$\mathbb{F}_q[G] \cong \mathbb{F}_q \oplus \mathcal{B} \oplus \mathbb{C},$$

where $\mathcal{B} = \underbrace{\mathbb{F}_{q^{f_2}} \oplus \cdots \oplus \mathbb{F}_{q^{f_2}}}_{e_2}$ and $\mathcal{C} = \underbrace{M_{p_2}(\mathbb{F}_{q^r}) \oplus \cdots \oplus M_{p_2}(\mathbb{F}_{q^r})}_{e_1}$.

Suppose that $f_2 \neq 1$. As before, we have

$$\mathrm{Aut}(\mathbb{F}_q[G]) \cong \mathrm{Aut}(\mathcal{B}) \oplus \mathrm{Aut}(\mathcal{C})$$

and

$$\mathrm{Aut}(\mathcal{B}) \cong \mathbb{Z}_{f_2}^{(e_2)} \rtimes S_{e_2}, \quad \mathrm{Aut}(\mathcal{C}) \cong (\mathrm{Aut}(M_{p_2}(\mathbb{F}_{q^r}))^{(e_1)} \rtimes S_{e_1}.$$

We now show that $\mathrm{Aut}(M_{p_2}(\mathbb{F}_{q^r})) \cong \mathrm{SL}_{p_2}(\mathbb{F}_{q^r}) \rtimes \mathbb{Z}_r$. Observe that any $\sigma \in \mathrm{Aut}(M_{p_2}(\mathbb{F}_{q^r}))$ restricted to its centre, $\mathrm{Z}(M_{p_2}(\mathbb{F}_{q^r})) \cong \mathbb{F}_{q^r}$, defines an element in $\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$. This gives a map $\sigma \mapsto \sigma|_{\mathrm{Z}(M_{p_2}(\mathbb{F}_{q^r}))}$ from $\mathrm{Aut}(M_{p_2}(\mathbb{F}_{q^r}))$ to $\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$, which is an epimorphism with the kernel, the group of $\mathbb{F}_{q^r}$-automorphisms of $M_{p_2}(\mathbb{F}_{q^r})$. However, by Skolem–Noether theorem, the group of $\mathbb{F}_{q^r}$-automorphisms of $M_{p_2}(\mathbb{F}_{q^r})$ is isomorphic to $\mathrm{SL}_{p_2}(\mathbb{F}_{q^r})$. Therefore, $\mathrm{Aut}(M_{p_2}(\mathbb{F}_{q^r}))$ is an extension of $\mathrm{SL}_{p_2}(\mathbb{F}_{q^r})$ by $\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q) \cong \mathbb{Z}_r$. Furthermore, we see that this extension splits because for each $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$, there is an automorphism of $M_{p_2}(\mathbb{F}_{q^r})$ given by letting σ act on each entry of its matrices. This proves the first case of (i).

It can be similarly be proved that if $f_2 = 1$, then

$$\mathrm{Aut}(\mathbb{F}_q[G]) \cong S_{e_2+1} \oplus (H_1^{(e_1)} \rtimes S_{e_1}).$$

(ii) This can be proved similarly. □

5. Examples

In this section, we give some examples to illustrate the computation of primitive central idempotents, Wedderburn decomposition and automorphism group as obtained from Theorems 1–5.

5.1 *The group algebra* $\mathbb{F}_q[S_3]$

As the first example, let us consider $S_3 = \langle a, b \mid a^3 = b^2 = 1,\ b^{-1}ab = a^2 \rangle$, the symmetric group of degree 3. In this case $p_1 = 3$ and $p_2 = 2$ and $\gcd(q, 6) = 1$. The following two cases arise:

5.1.1 $q \equiv 1 \bmod 6$. In this case, we have $f_1 = 1$, $e_1 = 2$, $f_2 = 1$, $e_2 = 1$. We fix $g_1 = 2$. If ζ is a primitive 3rd root of unity in $\mathbb{F}_q$, then $\eta_0^{(1)} = \zeta$, $\eta_1^{(1)} = \zeta^2$ and $\eta_i^{(1)} = \eta_{i+2}^{(1)}$ for all $i \geq 0$. Also $\eta_i^{(2)} = \eta_0^{(2)} = -1$ for all i.

5.1.2 $q \equiv 5 \bmod 6$. In this case, we have $f_1 = 2$, $e_1 = 1$, $f_2 = 1$, $e_2 = 1$. Further, $\eta_i^{(1)} = \eta_0^{(1)} = -1$ and $\eta_i^{(2)} = \eta_0^{(2)} = -1$ for all $i \geq 0$.

In both the above cases, by Theorem 1, $\mathbb{F}_q[S_3]$ has the following three distinct primitive central idempotents:

$$\frac{1}{6}\sum_{g\in S_3} g,$$
$$\frac{1}{6}\left(\sum_{i=0}^{2} a^i - \sum_{i=0}^{2} a^i b\right),$$
$$\frac{1}{3}\left(2 - \sum_{i=1}^{2} a^i\right).$$

Furthermore, by Theorem 3,

$$\mathbb{F}_q[S_3] = \mathbb{F}_q \oplus \mathbb{F}_q \oplus M_2(\mathbb{F}_q)$$

is the Wedderburn decomposition of $\mathbb{F}_q[S_3]$, which is proved in [21].

Also, by Theorem 5, $\mathrm{Aut}(\mathbb{F}_q[S_3]) \cong S_2 \oplus SL_2(\mathbb{F}_q)$.

5.2 *The group algebra* $\mathbb{F}_q[D_{10}]$

We next consider the group $D_{10} = \langle a, b \mid a^5 = 1,\ b^2 = 1,\ b^{-1}ab = a^{-1}\rangle$, the dihedral group of order 10. In this case $p_1 = 5$, $p_2 = 2$ and $\gcd(q, 10) = 1$. Fix $g_1 = 2$ and ζ is a primitive 5th root of unity in $\bar{\mathbb{F}}_q$. The following cases arise:

5.2.1 $q \equiv 1 \bmod 10$. $f_1 = 1, e_1 = 4, f_2 = 1, e_2 = 1$. $\eta_0^{(1)} = \zeta$, $\eta_1^{(1)} = \zeta^2$, $\eta_2^{(1)} = \zeta^4$, $\eta_3^{(1)} = \zeta^3$ and $\eta_i^{(1)} = \eta_{i+4}^{(1)}$ for all $i \geq 0$. Also $\eta_i^{(2)} = \eta_0^{(2)} = -1$ for all i.

5.2.2 $q \equiv 3$ or $7 \bmod 10$. $f_1 = 4, e_1 = 1, f_2 = 1, e_2 = 1$. $\eta_i^{(1)} = \eta_0^{(1)} = -1$, $\eta_i^{(2)} = \eta_0^{(2)} = -1$ for all i.

5.2.3 $q \equiv 9 \bmod 10$. $f_1 = 2, e_1 = 2, f_2 = 1, e_2 = 1$. $\eta_0^{(1)} = \zeta + \zeta^4$, $\eta_1^{(1)} = \zeta^2 + \zeta^3$ and $\eta_i^{(1)} = \eta_{i+2}^{(1)}$ for all $i \geq 0$. Also $\eta_i^{(2)} = \eta_0^{(2)} = -1$ for all i.

Primitive central idempotents

5.2.4 $q \equiv 1, 9 \bmod 10$. In this case $\mathbb{F}_q[D_{10}]$ has the following four primitive central idempotents:

$$\frac{1}{10}\textstyle\sum_{g \in D_{10}} g,$$
$$\frac{1}{10}\left(\sum_{i=0}^{4} a^i - \sum_{i=0}^{4} a^i b\right),$$
$$\frac{1}{5}(2 + (\zeta + \zeta^4)(a + a^4) + (\zeta^2 + \zeta^3)(a^2 + a^3)),$$
$$\frac{1}{5}(2 + (\zeta^2 + \zeta^3)(a + a^4) + (\zeta + \zeta^4)(a^2 + a^3)).$$

5.2.5 $q \equiv 3, 7 \bmod 10$. In this case $\mathbb{F}_q[D_{10}]$ has the following three primitive central idempotents:

$$\frac{1}{10}\sum_{g \in D_{10}} g,$$
$$\frac{1}{10}\left(\sum_{i=0}^{4} a^i - \sum_{i=0}^{4} a^i b\right),$$
$$\frac{1}{5}\left(4 - \sum_{i=1}^{4} a^i\right).$$

Wedderburn decomposition:

$$\mathbb{F}_q[D_{10}] \cong \begin{cases} \mathbb{F}_q \oplus \mathbb{F}_q \oplus M_2(\mathbb{F}_q) \oplus M_2(\mathbb{F}_q), & q \equiv 1, 9 \bmod 10, \\ \mathbb{F}_q \oplus \mathbb{F}_q \oplus M_2(\mathbb{F}_{q^2}), & q \equiv 3, 7 \bmod 10. \end{cases}$$

Automorphism group:

$$\mathrm{Aut}(\mathbb{F}_q[D_{10}]) \cong \begin{cases} S_2 \oplus (SL_2(\mathbb{F}_q) \rtimes S_2), & q \equiv 1, 9 \bmod 10, \\ S_2 \oplus (SL_2(\mathbb{F}_{q^2}) \rtimes \mathbb{Z}_2), & q \equiv 3, 7 \bmod 10. \end{cases}$$

The Wedderburn decomposition of $\mathbb{F}_q[D_{10}]$ is obtained in [12].

5.3 *The group algebra* $\mathbb{F}_q[\mathbb{Z}_7 \rtimes \mathbb{Z}_3]$

Consider the presentation $\langle a, b \mid a^7 = 1,\ b^3 = 1,\ b^{-1}ab = a^2\rangle$ of $G := \mathbb{Z}_7 \rtimes \mathbb{Z}_3$. In this case, we have $p_1 = 7$, $p_2 = 3$ and $\gcd(q, 21) = 1$. Fix $g_1 = 3$ and $g_2 = 2$. Let ζ_1 be a primitive 7th root of unity and ζ_2, a primitive 3rd root of unity in $\bar{\mathbb{F}}_q$. The following cases arise:

5.3.1 $q \equiv 1 \bmod 21$. In this case, we have $f_1 = 1$, $e_1 = 6$, $f_2 = 1$, $e_2 = 2$, $\eta_0^{(1)} = \zeta_1$, $\eta_1^{(1)} = \zeta_1^3$, $\eta_2^{(1)} = \zeta_1^2$, $\eta_3^{(1)} = \zeta_1^6$, $\eta_4^{(1)} = \zeta_1^4$, $\eta_5^{(1)} = \zeta_1^5$ and $\eta_i^{(1)} = \eta_{i+6}^{(1)}\ \forall\, i \geq 0$. Also $\eta_0^{(2)} = \zeta_2$, $\eta_1^{(2)} = \zeta_2^2$ and $\eta_i^{(2)} = \eta_{i+2}^{(2)}\ \forall\, i \geq 0$.

5.3.2 $q \equiv 2, 11 \bmod 21$. $f_1 = 3,\ e_1 = 2,\ f_2 = 2,\ e_2 = 1$, $\eta_0^{(1)} = \zeta_1 + \zeta_1^2 + \zeta_1^4$, $\eta_1^{(1)} = \zeta_1^3 + \zeta_1^5 + \zeta_1^6$, and $\eta_i^{(1)} = \eta_{i+2}^{(1)}\ \forall\, i \geq 0$. Also $\eta_0^{(2)} = -1$, and $\eta_i^{(2)} = \eta_{i+1}^{(2)}\ \forall\, i \geq 0$.

5.3.3 $q \equiv 4, 16 \bmod 21$. $f_1 = 3,\ e_1 = 2,\ f_2 = 1,\ e_2 = 2$, $\eta_0^{(1)} = \zeta_1 + \zeta_1^2 + \zeta_1^4$, $\eta_1^{(1)} = \zeta_1^3 + \zeta_1^5 + \zeta_1^6$ and $\eta_i^{(1)} = \eta_{i+2}^{(1)}\ \forall\, i \geq 0$. $\eta_0^{(2)} = \zeta_2$, $\eta_1^{(2)} = \zeta_2^2$ and $\eta_i^{(2)} = \eta_{i+2}^{(2)}\ \forall\, i \geq 0$.

5.3.4 $q \equiv 5, 17 \bmod 21$. $f_1 = 6,\ e_1 = 1,\ f_2 = 2,\ e_2 = 1$, $\eta_0^{(1)} = -1$, and $\eta_i^{(1)} = \eta_{i+1}^{(1)}\ \forall\, i \geq 0$. $\eta_0^{(2)} = -1$, $\eta_i^{(2)} = \eta_{i+1}^{(2)}\ \forall\, i \geq 0$.

5.3.5 $q \equiv 8 \bmod 21$. $f_1 = 1,\ e_1 = 6,\ f_2 = 2,\ e_2 = 1$, $\eta_0^{(1)} = \zeta_1$, $\eta_1^{(1)} = \zeta_1^3$, $\eta_2^{(1)} = \zeta_1^2$, $\eta_3^{(1)} = \zeta_1^6$, $\eta_4^{(1)} = \zeta_1^4$, $\eta_5^{(1)} = \zeta_1^5$ and $\eta_i^{(1)} = \eta_{i+6}^{(1)}\ \forall\, i \geq 0$. $\eta_0^{(2)} = -1$ and $\eta_i^{(2)} = \eta_{i+1}^{(2)}\ \forall\, i \geq 0$.

5.3.6 $q \equiv 10, 19 \bmod 21$. $f_1 = 6,\ e_1 = 1,\ f_2 = 1,\ e_2 = 2$, $\eta_0^{(1)} = -1$ and $\eta_i^{(1)} = \eta_{i+1}^{(1)}\ \forall\, i \geq 0$. $\eta_0^{(2)} = \zeta_2$, $\eta_1^{(2)} = \zeta_2^2$ and $\eta_i^{(2)} = \eta_{i+2}^{(2)}\ \forall\, i \geq 0$.

5.3.7 $q \equiv 13 \bmod 21$. $f_1 = 2,\ e_1 = 3,\ f_2 = 1,\ e_2 = 2,\ \eta_0^{(1)} = \zeta_1 + \zeta_1^6,\ \eta_1^{(1)} = \zeta_1^3 + \zeta_1^4,\ \eta_2^{(1)} = \zeta_1^2 + \zeta_1^5$ and $\eta_i^{(1)} = \eta_{i+3}^{(1)}\ \forall\, i \geq 0$. Also $\eta_0^{(2)} = \zeta_2,\ \eta_1^{(2)} = \zeta_2^2$ and $\eta_i^{(2)} = \eta_{i+2}^{(2)}\ \forall i \geq 0$.

5.3.8 $q \equiv 20 \bmod 21$. $f_1 = 2,\ e_1 = 3,\ f_2 = 2,\ e_2 = 1,\ \eta_0^{(1)} = \zeta_1 + \zeta_1^6,\ \eta_1^{(1)} = \zeta_1^3 + \zeta_1^4,\ \eta_2^{(1)} = \zeta_1^2 + \zeta_1^5$ and $\eta_i^{(1)} = \eta_{i+3}^{(1)}\ \forall\, i \geq 0$. $\eta_0^{(2)} = -1$ and $\eta_i^{(2)} = \eta_{i+1}^{(2)}\ \forall\, i \geq 0$.

Primitive central idempotents:

The primitive central idempotents arising in the various cases are as follows:

5.3.9 $q \equiv 1, 4, 16 \bmod 21$.

$$\frac{1}{21}\textstyle\sum_{g\in G} g,$$
$$\frac{1}{21}\left(\sum_{i=0}^{6} a^i + \zeta_2 \sum_{i=0}^{6} a^i b + \zeta_2^2 \sum_{i=0}^{6} a^i b^2\right),$$
$$\frac{1}{21}\left(\sum_{i=0}^{6} a^i + \zeta_2^2 \sum_{i=0}^{6} a^i b + \zeta_2 \sum_{i=0}^{6} a^i b^2\right),$$
$$\frac{1}{7}(3 + (\zeta_1 + \zeta_1^2 + \zeta_1^4)(a + a^2 + a^4) + (\zeta_1^3 + \zeta_1^5 + \zeta_1^6)(a^3 + a^5 + a^6)),$$
$$\frac{1}{7}(3 + (\zeta_1^3 + \zeta_1^5 + \zeta_1^6)(a + a^2 + a^4) + (\zeta_1 + \zeta_1^2 + \zeta_1^4)(a^3 + a^5 + a^6)).$$

5.3.10 $q \equiv 2, 8, 11 \bmod 21$.

$$\frac{1}{21}\textstyle\sum_{g\in G} g,$$
$$\frac{1}{21}\left(2\sum_{i=0}^{6} a^i - \sum_{i=0}^{6} a^i b - \sum_{i=0}^{6} a^i b^2\right),$$
$$\frac{1}{7}(3 + (\zeta_1 + \zeta_1^2 + \zeta_1^4)(a + a^2 + a^4) + (\zeta_1^3 + \zeta_1^5 + \zeta_1^6)(a^3 + a^5 + a^6)),$$
$$\frac{1}{7}(3 + (\zeta_1^3 + \zeta_1^5 + \zeta_1^6)(a + a^2 + a^4) + (\zeta_1 + \zeta_1^2 + \zeta_1^4)(a^3 + a^5 + a^6)).$$

5.3.11 $q \equiv 5, 17, 20 \bmod 21$.

$$\sum_{g\in G} g,$$
$$\frac{1}{21}\left(2\sum_{i=0}^{6} a^i - \sum_{i=0}^{6} a^i b - \sum_{i=0}^{6} a^i b^2\right),$$
$$\frac{1}{7}\left(6 - \sum_{i=1}^{6} a^i\right).$$

5.3.12 $q \equiv 10, 13, 19 \bmod 21$.

$$\frac{1}{21}\sum_{g\in G} g,$$
$$\frac{1}{21}\left(\sum_{i=0}^{6} a^i + \zeta_2\left(\sum_{i=0}^{6} a^i b\right) + \zeta_2^2\left(\sum_{i=0}^{6} a^i b^2\right)\right),$$
$$\frac{1}{21}\left(\sum_{i=0}^{6} a^i + \zeta_2^2\left(\sum_{i=0}^{6} a^i b\right) + \zeta_2\left(\sum_{i=0}^{6} a^i b^2\right)\right),$$
$$\frac{1}{7}\left(6 - \sum_{i=1}^{6} a^i\right).$$

Wedderburn decomposition:

$$\mathbb{F}_q[\mathbb{Z}_7 \rtimes \mathbb{Z}_3] \cong \begin{cases} \mathbb{F}_q \oplus \mathbb{F}_q \oplus \mathbb{F}_q \oplus M_3(\mathbb{F}_q) \oplus M_3(\mathbb{F}_q), & q \equiv 1, 4, 16 \bmod 21,\\ \mathbb{F}_q \oplus \mathbb{F}_{q^2} \oplus M_3(\mathbb{F}_q) \oplus M_3(\mathbb{F}_q), & q \equiv 2, 8, 11 \bmod 21,\\ \mathbb{F}_q \oplus \mathbb{F}_{q^2} \oplus M_3(\mathbb{F}_{q^2}), & q \equiv 5, 17, 20 \bmod 21,\\ \mathbb{F}_q \oplus \mathbb{F}_q \oplus \mathbb{F}_q \oplus M_3(\mathbb{F}_{q^2}), & q \equiv 10, 13, 19 \bmod 21. \end{cases}$$

Automorphism group:

$$\mathrm{Aut}(\mathbb{F}_q[\mathbb{Z}_7 \rtimes \mathbb{Z}_3]) \cong \begin{cases} S_3 \oplus (\mathrm{SL}_3(\mathbb{F}_q) \rtimes S_2), & q \equiv 1, 4, 16 \bmod 21,\\ \mathbb{Z}_2 \oplus (\mathrm{SL}_3(\mathbb{F}_q) \rtimes S_2), & q \equiv 2, 8, 11 \bmod 21,\\ \mathbb{Z}_2 \oplus (\mathrm{SL}_3(\mathbb{F}_{q^2}) \rtimes \mathbb{Z}_2), & q \equiv 5, 17, 20 \bmod 21,\\ S_3 \oplus (\mathrm{SL}_3(\mathbb{F}_{q^2}) \rtimes \mathbb{Z}_2), & q \equiv 10, 13, 19 \bmod 21. \end{cases}$$

References

[1] Bakshi Gurmeet K and Raka Madhu, Minimal cyclic codes of length $p^n q$, *Finite Fields Appl.* **9(4)** (2003) 432–448

[2] Bakshi Gurmeet K, Raka Madhu and Sharma Anuradha, Idempotent generators of irreducible cyclic codes, Number theory and discrete geometry, 13–18, Ramanujan Math. Soc. Lect. Notes Ser. 6 (Mysore: Ramanujan Math. Soc.) (2008)

[3] Berman S D, On the theory of group codes, Kibernetika (Kiev) (1967) no. 1, pp. 31–39 (Russian); translated as *Cybernetics* **3(1)** (1969) 25–31

[4] Broche Osnel and del Rio Angel, Wedderburn decomposition of finite group algebras, *Finite Fields Appl.* **13(1)** (2007) 71–79

[5] Broche Cristo O and Polcino Milies C, Central idempotents in group algebras, Groups, rings and algebras, 75–87, Contemp. Math. 420 (Providence, RI: Amer. Math. Soc.) (2006)

[6] Coelho Sonia P, Jespers Eric and Polcino Milies C, Automorphisms of group algebras of some metacyclic groups, *Comm. Algebra* **24(13)** (1996) 4135–4145

[7] Ferraz Raul Antonio and Polcino Milies C, Idempotents in group algebras and minimal abelian codes, *Finite Fields Appl.* **13(2)** (2007) 382–393

[8] Herman Allen, On the automorphism groups of rational group algebras of metacyclic groups, *Comm. Algebra* **25(7)** (1997) 2085–2097

[9] James Gordon and Liebeck Martin, Representations and characters of groups, Second edition (New York: Cambridge University Press) (2001)

[10] Jespers Eric, Leal Guilherme and Paques Antonio, Central idempotents in the rational group algebra of a finite nilpotent group, *J. Algebra Appl.* **2(1)** (2003) 57–62

[11] Khan Manju, Structure of the unit group of FD_{10}, *Serdica Math. J.* **35(1)** (2009) 15–24

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

[13] Lam T Y, A first course in noncommutative rings, Second edition, Graduate Texts in Mathematics 131 (New York: Springer-Verlag) (2001)

[14] Olivieri Aurora, del Rio Angel and Simon Juan Jacobo, On monomial characters and central idempotents of rational group algebras, *Comm. Algebra* **32(4)** (2004) 1531–1550

[15] Olivieri Aurora, del Rio A and Simon Juan Jacobo, The group of automorphisms of the rational group algebra of a finite metacyclic group, *Comm. Algebra* **34(10)** (2006) 3543–3567

[16] Perlis Sam and Walker Gordon L, Abelian group algebras of finite order, *Trans. Am. Math. Soc.* **68** (1950) 420–426

[17] Pruthi Manju and Arora S K, Minimal codes of prime-power length, *Finite Fields Appl.* **3(2)** (1997) 99–113

[18] Sharma Anuradha, Bakshi Gurmeet K, Dumir V C and Raka Madhu, Cyclotomic numbers and primitive idempotents in the ring $\mathrm{GF}(q)[x]/(x^{p^n}-1)$, *Finite Fields Appl.* **10(4)** (2004) 653–673

[19] Sharma Anuradha, Bakshi Gurmeet K, Dumir V C and Raka Madhu, Irreducible cyclic codes of length 2^n, *Ars Combin.* **86** (2008) 133–146

[20] Sharma R K, Srivastava J B and Khan Manju, The unit group of FS_3, *Acta Math. Acad. Paedagog. Nyhzi. (N.S.)* **23(2)** (2007) 129–142

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

[22] Yamada Toshihiko, The Schur subgroup of the Brauer group, Lecture Notes in Mathematics, vol. 397 (Berlin-New York: Springer-Verlag) (1974)