

Codes of length 2^4 over the group algebra of non-abelian groups

Sudesh Sehwat *

Department of Mathematics

Govt. College Jatauli Haily Mandi

Gurugram

Haryana

India

Manju Pruthi [†]

Department of Mathematics

Indira Gandhi University

Meerpur

Rewari 123401

Haryana

India

Abstract

Let FG be a group algebra over the non-abelian group G of order 2^4 . We have studied the codes of length 2^4 using character tables and corresponding generating idempotents. Minimum distance and dimension of the codes are also obtained.

Subject Classification (2020): 20C15, 20E45.

Keywords: Semi simple artinian ring, Characters, Linear and non-linear idempotents.

1. Introduction

Group codes, are classical codes over finite fields, have recently attracted attention for their applications in cryptography, coding theory, and quantum computing. The group algebra FG is recognized as a semisimple algebra, which can be expressed as a direct sum of minimal ideals. Such a decomposition arises whenever $\text{char}(F) \nmid O(G)$. It is also well established that every ideal of FG is generated by an idempotent element.

If G is non abelian group, then a group code in FG is described as one-sided ideal. Many authors have obtained the non abelian codes of different

* E-mail: sudesh2421@yahoo.com (Corresponding Author)

[†] E-mail: manju.pruthi@yahoo.com

lengths. Wong and Ang [1] developed the group codes of order 6,8,10,12 in the Dihedral group algebra. In [3], Dutra, Ferraz and Polcino Milies constructed Dihedral and Quaternion codes and also determined specific conditions on the parameters q and n such that $F_q D_n$ and QD_n have an equal number of irreducible components. In [4], Guerreiro provided an overview on the group algebra and coding theory. In [2], Admasu and Sehgal derived explicit formulas to calculate the number of subgroups of a specified order in finite abelian p -groups of rank 3. In [13], Sivaranjani et al. determined the composition of the unit group of semisimple group algebra $K_q GL(2, \mathbb{Z}_5)$. In [6], Pruthi computed the idempotents in the group ring of quaternions over finite field $\mathbb{Z}_p$. Pruthi and Sudesh [7] obtained the idempotents in the Dihedral group algebra.

In this article, we constructed the group codes of length 16 generated by linear and non linear idempotents. It is well known that there are 14 non-isomorphic groups exist of order 16, comprising 5 abelian and 9 non-abelian. In this paper, our attention is restricted to the non-abelian cases. Section 2 is devoted to determining the generating idempotents in the corresponding group algebras, while Section 3 deals with computing the parameters of the associated group codes. Some non-abelian groups of order 16 have been investigated in our earlier studies: in [10], codes arising from the group algebra of the dihedral group D_{16} were studied; in [11], those over the dicyclic group T_{16} were examined; and in [9],[12], codes defined on $D_8 \times C_2$ and $Q_8 \times C_2$ were analyzed.

“[14] Let F be a field and $G = \{g_1, g_2, \dots, g_n\}$ be a finite group. A vector space over F with $g_1, g_2, \dots, g_n$ as a basis is the group algebra FG . The elements of FG are expressed as $\lambda_1 g_1 + \dots + \lambda_n g_n$ where $\lambda_i \in F$ and the operations addition and scalar multiplication are defined as:

$$u+v = \sum_{i=1}^n (\lambda_i + \mu_i) g_i \text{ and } \lambda u = \sum_{i=1}^n (\lambda \lambda_i) g_i$$

where $u = \sum_{i=1}^n \lambda_i g_i$ and $v = \sum_{i=1}^n \mu_i g_i$. So FG is a vector space over F with dimension n .

And the multiplication is defined as $uv = (\sum_{g \in G} \lambda_g g) (\sum_{h \in G} \mu_h h) = (\sum_{g, h \in G} \lambda_g \mu_h) (gh)$ then FG is group algebra of G over F .

The *weight* of any element $u = \sum_{g \in G} \alpha_g g$ is equal to $|\{\alpha_g : \alpha_g \neq 0\}|$ and is denoted by $wt(u)$.”

“Let $E = \{e_i\}_{i=1}^s$ be the collection of all idempotents in FG . If I is an ideal generated by $A = \{e_j\}_{j=1}^t \subseteq E$ and $\mu = E \setminus \{e_j\}_{j=1}^t$ then $I_A = \{u \in FG : ue = 0 \forall e \in \mu\}$. Minimum distance of the group code I_A is defined by $d(I_A) = \min\{wt(u) : 0 \neq u \in I_A\}$. The length n of a group code I_A is defined to be order of G . If I_A has dimension k and minimum distance d then I_A is called an (n, k, d) group code.”

Remark 1.1: We know $FG = (\oplus_{e_i \in E_L} FG_{e_i}) \oplus (\oplus_{e_j \in E_N} FG_{e_j})$ where E_L is the set consisting of all linear idempotents in FG and E_N is the set consisting of all nonlinear idempotents in FG and FG_{e_i} is minimal ideal generated by e_i . Thus $E =$

$E_L \cup E_N$. Note that if $e_i \in E_L$, then $\dim(FG_{e_i}) = 1$; and if $e_j \in E_N$, then $\dim(FG_{e_j}) = m^2$ where $m = \chi_j(1)$ where χ_j is the j th nonlinear character of G .

Proposition 1.2: If x and y are conjugate elements of the group G , then $\chi(x) = \chi(y)$ for all characters χ of G .

Proposition 1.3: Let χ be the character of the FG -module. Then the idempotent corresponding to the character χ is given by

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

Theorem 1.4: ([8] Maschke's Theorem): Let G be a finite group and F is a field. The group algebra FG is semisimple if and only if the characteristic of F does not divide the order of G .

2. Idempotents in the Group Algebra FG

There are exactly three non-abelian groups of order 2^4 for which $G/K \cong D_8$ where $K = G' \cap Z(G)$. Two of these groups namely, $G_1 = D_{16}$ and G_2 , Generalized quaternion group have been studied in [10],[11].

We now proceed to analyze the third group and the group $G_3 = \langle a, b : b^2 = a^8 = 1, b^{-1}ab = a^3 \rangle$. There are seven conjugacy classes in the group G_3 , which are listed as follows

$$\{1\}, \{a^4\}, \{a^2, a^6\}, \{a, a^3\}, \{a^5, a^7\}, \{a^i b : i \text{ is even}\}, \{a^i b : i \text{ is odd}\}.$$

2.1 The Explicit forms of seven irreducible idempotents in the group algebra FG_3 .

Group G_3 admits four linear characters, denoted by $\phi_1, \phi_2, \phi_3, \phi_4$ and three non linear characters ψ_1, ψ_2, ψ_3 , which are given in the following character table

[5] The character table of G_3

Table 1

"Class	1	a^4	a^2	a	a^5	$a^i b : i \text{ even}$	$a^i b : i \text{ odd}$
ϕ_1	1	1	1	1	1	1	1
ϕ_2	1	1	1	1	1	-1	-1
ϕ_3	1	1	1	-1	-1	1	-1
ϕ_4	1	1	1	-1	-1	-1	1
ψ_1	2	2	-2	0	0	0	0
ψ_2	2	-2	0	$\sqrt{2}i$	$-\sqrt{2}i$	0	0
ψ_3	2	-2	0	$-\sqrt{2}i$	$\sqrt{2}i$	0	0

Based on Table [1] and Proposition (1.3) the group algebra FG_3 has four linear irreducible idempotents $\{e_i\}_{i=1}^4$ and three non-linear irreducible idempotents $\{e_j\}_{j=5}^7$ which can be expressed explicitly as follows

$$\begin{aligned}
e_1 &= \frac{1}{16} S_+(a, b) \\
e_2 &= \frac{1}{16} S_-(a, b) \\
e_3 &= \frac{1}{16} S_+(-a, b) \\
e_4 &= \frac{1}{16} S_-(-a, b) \\
e_5 &= \frac{1}{8} (2 - 2a^2 + 2a^4 - 2a^6) = \frac{1}{4} (1 - a^2 + a^4 - a^6) \\
e_6 &= \frac{1}{8} (2 - \sqrt{2}i (a + a^3) - 2a^4 + \sqrt{2}i (a^5 + a^7)) \\
e_7 &= \frac{1}{8} (2 + \sqrt{2}i (a + a^3) - 2a^4 - \sqrt{2}i (a^5 + a^7))
\end{aligned}$$

Idempotents in $F_q G_3$

Now we examine the group algebra $F_q G_3$ where F_q is the finite field of order $q = p^s$, with p being an odd prime s.t. $\gcd(\text{char}(F_q), 16) = 1$.

The character table of G_3 considered over the field $F = F_5$. Since $\sqrt{2}i \notin F$, we extend the field to $F_{5^2} (= GF(5^2)) = \frac{F_5[x]}{\langle f(x) \rangle}$ where $f(x) = x^2 + 2$ is the minimal polynomial of $\sqrt{2}i$, irreducible over F_5 . Every element of F_{5^2} can be expressed as $ax + b + \langle x^2 + 2 \rangle$ with $a, b \in F_5$. Let $\alpha = x + \langle x^2 + 2 \rangle$. Defining $\beta = \alpha + 1$, we obtain a primitive element of F_{5^2} , satisfying $\beta^3 = \alpha$.

$$\begin{aligned}
e_1 &= S_+(a, b) \\
e_2 &= S_-(a, b) \\
e_3 &= S_+(-a, b) \\
e_4 &= S_-(-a, b) \\
e_5 &= 4(1 - a^2 + a^4 - a^6) \\
e_6 &= 2(2 - \beta^3 (a + a^3) - 2a^4 + \beta^3 (a^5 + a^7)) \\
e_7 &= 2(2 + \beta^3 (a + a^3) - 2a^4 - \beta^3 (a^5 + a^7))
\end{aligned}$$

where $S_+(a, b) = \sum_{i=0}^7 a^i (1 + b)$ and $S_-(a, b) = \sum_{i=0}^7 a^i (1 - b) \dots \square$

2.2 The Explicit forms of ten irreducible idempotents in FG_4, FG_5, FG_6 .

There exist exactly three non-abelian groups for which the quotient group $G/K \cong C_4 \times C_2$ where $K = G' \cap Z(G)$.

$$G_4 = \langle a, b, z : b^2 = z^2 = 1, a^4 = z, b^{-1}ab = az \rangle$$

$$G_5 = \langle a, b, z : z^2 = 1, a^4 = 1, b^2 = z, b^{-1}ab = az \rangle$$

$$G_6 = \langle a, b, z : a^4 = b^2 = z^2 = 1, b^{-1}ab = az, az = za, bz = zb \rangle$$

Each of the groups G_4, G_5, G_6 possesses 10 conjugacy classes, and hence admits 10 irreducible characters. Among these, eight are linear, denoted by $\{\chi_i\}_{i=1}^8$ and two are non linear $\{\psi_j\}_{j=1}^2$ characters.

The corresponding conjugacy classes of G_4, G_5, G_6 are as follows

$$\begin{aligned}
\mathcal{C}_1 &= \{1\}, \mathcal{C}_2 = \{z\}, \\
\mathcal{C}_3 &= \{a^2\}, \mathcal{C}_4 = \{a^2z\}, \\
\mathcal{C}_5 &= \{a, az\}, \mathcal{C}_6 = \{a^3z, a^3\}, \\
\mathcal{C}_7 &= \{b, bz\}, \mathcal{C}_8 = \{a^2b, a^2bz\}, \\
\mathcal{C}_9 &= \{ab, abz\}, \mathcal{C}_{10} = \{a^3b, a^3bz\}
\end{aligned}$$

[5] The character table of G_4, G_5 and G_6

Table 2

“Class	$\mathcal{C}_1$	$\mathcal{C}_2$	$\mathcal{C}_3$	$\mathcal{C}_4$	$\mathcal{C}_5$	$\mathcal{C}_6$	$\mathcal{C}_7$	$\mathcal{C}_8$	$\mathcal{C}_9$	$\mathcal{C}_{10}$
χ_1	1	1	1	1	1	1	1	1	1	1
χ_2	1	1	-1	-1	i	-i	1	-1	i	-i
χ_3	1	1	1	1	-1	-1	1	1	-1	-1
χ_4	1	1	-1	-1	-i	i	1	-1	-i	i
χ_5	1	1	1	1	1	1	-1	-1	-1	-1
χ_6	1	1	-1	-1	i	-i	-1	1	-i	i
χ_7	1	1	1	1	-1	-1	-1	-1	1	1
χ_8	1	1	-1	-1	-i	i	-1	1	i	-i
ψ_1	2	-2	α	β	0	0	0	0	0	0
ψ_2	2	-2	β	α	0	0	0	0	0	0

For G_4 , $\alpha = 2i = -\beta$

And for G_5, G_6 , $\alpha = 2 = -\beta$

Using the character table [2] and pro. (1.3), idempotents of FG_4 are expressed as follows

$$e_1 = \rho \sum_{\tau \in \mathcal{C}_\eta} \tau \text{ for } \eta = 1 \text{ to } 10$$

$$\begin{aligned}
e_2 = \rho [& \sum_{\eta=1}^2 \sum_{\tau \in \mathcal{C}_\eta} \tau - \sum_{\eta=3}^4 \sum_{\tau \in \mathcal{C}_\eta} \tau - i \sum_{\tau \in \mathcal{C}_5} \tau + i \sum_{\tau \in \mathcal{C}_6} \tau + \sum_{\tau \in \mathcal{C}_7} \tau - \sum_{\tau \in \mathcal{C}_8} \tau - \\
& i \sum_{\tau \in \mathcal{C}_9} \tau + i \sum_{\tau \in \mathcal{C}_{10}} \tau]
\end{aligned}$$

$$e_3 = \rho [\sum_{\eta=1}^4 \sum_{\tau \in \mathcal{C}_\eta} \tau - \sum_{\eta=5}^6 \sum_{\tau \in \mathcal{C}_\eta} \tau + \sum_{\eta=7}^8 \sum_{\tau \in \mathcal{C}_\eta} \tau - \sum_{\eta=9}^{10} \sum_{\tau \in \mathcal{C}_\eta} \tau]$$

$$\begin{aligned}
e_4 = \rho [& \sum_{\eta=1}^2 \sum_{\tau \in \mathcal{C}_\eta} \tau - \sum_{\eta=3}^4 \sum_{\tau \in \mathcal{C}_\eta} \tau + i \sum_{\tau \in \mathcal{C}_5} \tau - i \sum_{\tau \in \mathcal{C}_6} \tau + \sum_{\tau \in \mathcal{C}_7} \tau - \sum_{\tau \in \mathcal{C}_8} \tau + \\
& i \sum_{\tau \in \mathcal{C}_9} \tau - i \sum_{\tau \in \mathcal{C}_{10}} \tau]
\end{aligned}$$

$$e_5 = \rho [\sum_{\eta=1}^6 \sum_{\tau \in \mathcal{C}_\eta} \tau - \sum_{\eta=7}^{10} \sum_{\tau \in \mathcal{C}_\eta} \tau]$$

$$\begin{aligned}
e_6 = \rho [& \sum_{\eta=1}^2 \sum_{\tau \in \mathcal{C}_\eta} \tau - \sum_{\eta=3}^4 \sum_{\tau \in \mathcal{C}_\eta} \tau - i \sum_{\tau \in \mathcal{C}_5} \tau + i \sum_{\tau \in \mathcal{C}_6} \tau - \sum_{\tau \in \mathcal{C}_7} \tau + \sum_{\tau \in \mathcal{C}_8} \tau + \\
& i \sum_{\tau \in \mathcal{C}_9} \tau - i \sum_{\tau \in \mathcal{C}_{10}} \tau]
\end{aligned}$$

$$e_7 = \rho [\sum_{\eta=1}^4 \sum_{\tau \in \mathcal{C}_\eta} \tau - \sum_{\eta=5}^8 \sum_{\tau \in \mathcal{C}_\eta} \tau + \sum_{\eta=9}^{10} \sum_{\tau \in \mathcal{C}_\eta} \tau]$$

$$\begin{aligned}
e_8 &= \rho \left[\sum_{\eta=1}^2 \sum_{\tau \in \mathcal{C}_\eta} \tau - \sum_{\eta=3}^4 \sum_{\tau \in \mathcal{C}_\eta} \tau + i \sum_{\tau \in \mathcal{C}_5} \tau - i \sum_{\tau \in \mathcal{C}_6} \tau - \sum_{\tau \in \mathcal{C}_7} \tau + \sum_{\tau \in \mathcal{C}_8} \tau - \right. \\
&\quad \left. i \sum_{\tau \in \mathcal{C}_9} \tau + i \sum_{\tau \in \mathcal{C}_{10}} \tau \right] \\
e_9 &= \frac{1}{4} \left[\sum_{\tau \in \mathcal{C}_1} \tau - \sum_{\tau \in \mathcal{C}_2} \tau - i \sum_{\tau \in \mathcal{C}_3} \tau + i \sum_{\tau \in \mathcal{C}_4} \tau \right] \\
e_{10} &= \frac{1}{4} \left[\sum_{\tau \in \mathcal{C}_1} \tau - \sum_{\tau \in \mathcal{C}_2} \tau + i \sum_{\tau \in \mathcal{C}_3} \tau - i \sum_{\tau \in \mathcal{C}_4} \tau \right] \text{ where } \rho = \frac{1}{16}.
\end{aligned}$$

Case 2: For the group algebra FG_5 , the idempotents $(e_i : 1 \leq i \leq 8)$ are coincide with those in FG_4 . The remaining two idempotents are given by the following expressions

$$\begin{aligned}
e_9 &= \frac{1}{4} \left[\sum_{\tau \in \mathcal{C}_1} \tau - \sum_{\tau \in \mathcal{C}_2} \tau + \sum_{\tau \in \mathcal{C}_3} \tau - \sum_{\tau \in \mathcal{C}_4} \tau \right] \\
e_{10} &= \frac{1}{4} \left[\sum_{\tau \in \mathcal{C}_1} \tau - \sum_{\tau \in \mathcal{C}_2} \tau - \sum_{\tau \in \mathcal{C}_3} \tau + \sum_{\tau \in \mathcal{C}_4} \tau \right]
\end{aligned}$$

Case 3: The idempotents of FG_6 are coincide with those obtained for FG_5 . $\square$

2.3 The Explicit forms of ten irreducible idempotents in FG_9 .

There exist exactly three non-abelian groups for which the quotient group $G/K \cong C_2 \times C_2 \times C_2$ where $K = G' \cap Z(G)$.

$$G_7 = \langle a, b, z : a^4 = b^2 = z^2 = 1, b^{-1}ab = a^{-1}, az = za, bz = zb \rangle \cong D_8 \times C_2$$

$$G_8 = \langle a, b, z : a^4 = z^2 = 1, a^2 = b^2, b^{-1}ab = a^{-1}, az = za, bz = zb \rangle \cong Q_8 \times C_2$$

$$G_9 = \langle a, b, z : a^2 = b^2 = z^4 = 1, b^{-1}ab = az^2, az = za, bz = zb \rangle$$

The group G_7 , G_8 have already been examined in [9], [12]. We now proceed with the group G_9 , which contains 10 conjugacy classes, described as follows

$$\mathcal{C}_1 = \{1\}, \mathcal{C}_2 = \{z^2\},$$

$$\mathcal{C}_3 = \{z\}, \mathcal{C}_4 = \{z^3\},$$

$$\mathcal{C}_5 = \{a, az^2\}, \mathcal{C}_6 = \{az, az^3\},$$

$$\mathcal{C}_7 = \{b, bz^2\}, \mathcal{C}_8 = \{bz, bz^3\},$$

$$\mathcal{C}_9 = \{ab, abz^2\}, \mathcal{C}_{10} = \{abz, abz^3\}$$

From the character table of G_9 given in [5] and Pro.(1.3), the group algebra FG_9 admits eight linear $\{e_i\}_{i=1}^8$ and two non linear $\{e_j\}_{j=9}^{10}$ irreducible idempotents which are expressed as follows

$$e_1 = \rho \sum_{\tau \in \mathcal{C}_\eta} \tau \text{ for } \eta = 1 \text{ to } 10$$

$$e_2 = \rho \left[\sum_{\eta=1}^6 \sum_{\tau \in \mathcal{C}_\eta} \tau - \sum_{\eta=7}^{10} \sum_{\tau \in \mathcal{C}_\eta} \tau \right]$$

$$e_3 = \rho \left[\sum_{\eta=1}^4 \sum_{\tau \in \mathcal{C}_\eta} \tau - \sum_{\eta=5}^6 \sum_{\tau \in \mathcal{C}_\eta} \tau + \sum_{\eta=7}^8 \sum_{\tau \in \mathcal{C}_\eta} \tau - \sum_{\eta=9}^{10} \sum_{\tau \in \mathcal{C}_\eta} \tau \right]$$

$$\begin{aligned}
e_4 &= \rho \left[\sum_{\eta=1}^2 \sum_{\tau \in \mathcal{C}_\eta} \tau - \sum_{\eta=3}^4 \sum_{\tau \in \mathcal{C}_\eta} \tau + \sum_{\eta=5}^{10} \sum_{\tau \in \mathcal{C}_\eta} \tau (-1)^{\eta+1} \right] \\
e_5 &= \rho \left[\sum_{\eta=1}^4 \sum_{\tau \in \mathcal{C}_\eta} \tau - \sum_{\eta=5}^{10} \sum_{\tau \in \mathcal{C}_\eta} \tau \right] \\
e_6 &= \rho \left[\sum_{\text{for } \eta=1,2,5,8,10} \sum_{\tau \in \mathcal{C}_\eta} \tau - \sum_{\text{for } \eta=3,4,6,7,9} \sum_{\tau \in \mathcal{C}_\eta} \tau \right] \\
e_7 &= \rho \left[\sum_{\text{for } \eta=1,2,6,7,10} \sum_{\tau \in \mathcal{C}_\eta} \tau - \sum_{\text{for } \eta=3,4,5,8,9} \sum_{\tau \in \mathcal{C}_\eta} \tau \right] \\
e_8 &= \rho \left[\sum_{\text{for } \eta=1,2,6,8,9} \sum_{\tau \in \mathcal{C}_\eta} \tau - \sum_{\text{for } \eta=3,4,5,7,10} \sum_{\tau \in \mathcal{C}_\eta} \tau \right] \\
e_9 &= \frac{1}{4} \left[\sum_{\tau \in \mathcal{C}_1} \tau - \sum_{\tau \in \mathcal{C}_2} \tau - i \sum_{\tau \in \mathcal{C}_3} \tau + i \sum_{\tau \in \mathcal{C}_4} \tau \right] \\
e_{10} &= \frac{1}{4} \left[\sum_{\tau \in \mathcal{C}_1} \tau - \sum_{\tau \in \mathcal{C}_2} \tau + i \sum_{\tau \in \mathcal{C}_3} \tau - i \sum_{\tau \in \mathcal{C}_4} \tau \right] \text{ where } \rho = \frac{1}{16} \square
\end{aligned}$$

3. Codes over Group Algebra FG

Remark 3.1: The group algebra FG_3 decomposes as

$FG_3 \cong_{i=1}^7 \oplus FG_{e_i}$ where $FG_{e_i} \cong M_1(F)$ for $1 \leq i \leq 4$ and $FG_{e_j} \cong M_2(F)$ for $5 \leq j \leq 7$. Consequently, $\dim(FG_{e_i}) = 1$ and $\dim(FG_{e_j}) = 2^2 = 4$.

Theorem 3.2: The following table no. 3 describes the group codes with generating idempotents over the group ring FG_3

Table 3

Sr.	Group codes	Distance	Dimension
(i)	$I_{\mathcal{A}}, \mathcal{A} = \{e_1, e_2, e_3, e_4\}$	4	4
(ii)	$I_{\mathcal{B}}, \mathcal{B} = \{e_1, e_2, e_3\}$	8	3
(iii)	$I_{\{e_1, e_2\}}$	8	2
(iv)	$I_{\mathcal{T}}, \mathcal{T} = \{e_5, e_6, e_7\}$	2	12
(v)	$I_{\mathcal{S}}, \mathcal{S} = \{e_6, e_7\}$	2	8
(vi)	$I_{\vartheta}, \vartheta = \{e_i, 1 \leq i \leq 5\}$	2	8
(vii)	$I_{\Lambda}, \Lambda = \{e_i, 2 \leq i \leq 7\}$	2	15

Proof: Let $u = \sum_{t=1}^8 \lambda_t a^{t-1} + \sum_{t=1}^8 \lambda_{t+8} a^{t-1} b \in FG_3$ then

$$ue_1 = (\sum_{i=1}^{16} \lambda_i) e_1 \quad (3.1)$$

$$ue_2 = (\sum_{i=1}^8 \lambda_i - \sum_{i=9}^{16} \lambda_i) e_2 \quad (3.2)$$

$$ue_3 = (\sum_{i=1}^{16} (-1)^{i+1} \lambda_i) e_3 \quad (3.3)$$

$$ue_4 = (\sum_{i=1}^8 (-1)^{i+1} \lambda_i - \sum_{i=9}^{16} (-1)^{i+1} \lambda_i) e_4 \quad (3.4)$$

$$ue_5 = \frac{1}{4} [(\lambda_1 - \lambda_3 + \lambda_5 - \lambda_7) (1 - a^2 + a^4 - a^6) +$$

$$(\lambda_2 - \lambda_4 + \lambda_6 - \lambda_8) (a - a^3 + a^5 - a^7) +$$

$$(\lambda_9 - \lambda_{11} + \lambda_{13} - \lambda_{15}) (b - a^2 b + a^4 b - a^6 b) +$$

$$(\lambda_{10} - \lambda_{12} + \lambda_{14} - \lambda_{16}) (ab - a^3b + a^5b - a^7b)] \quad (3.5)$$

$$\begin{aligned} ue_6 = & \frac{1}{8} [\{2(\lambda_1 - \lambda_5) + \sqrt{2}i(\lambda_2 + \lambda_4 - \lambda_6 - \lambda_8)(1 - a^4) + \\ & \{2(\lambda_2 - \lambda_6) + \sqrt{2}i(-\lambda_1 + \lambda_3 + \lambda_5 - \lambda_7)\}(a - a^5) + \\ & \{2(\lambda_3 - \lambda_7) + \sqrt{2}i(-\lambda_2 + \lambda_4 + \lambda_6 - \lambda_8)\}(a^2 - a^6) + \\ & \{2(\lambda_4 - \lambda_8) + \sqrt{2}i(-\lambda_3 + \lambda_5 - \lambda_1 + \lambda_7)\}(a^3 - a^7) + \\ & \{2(\lambda_9 - \lambda_{13}) + \sqrt{2}i(\lambda_{10} + \lambda_{12} - \lambda_{14} - \lambda_{16})\}(b - a^4b) + \\ & \{2(\lambda_{10} - \lambda_{14}) + \sqrt{2}i(-\lambda_9 + \lambda_{11} + \lambda_{13} - \lambda_{15})\}(ab - a^5b) + \\ & \{2(\lambda_{11} - \lambda_{15}) + \sqrt{2}i(-\lambda_{10} + \lambda_{12} + \lambda_{14} - \lambda_{16})\}(a^2b - a^6b) + \\ & \{2(\lambda_{12} - \lambda_{16}) + \sqrt{2}i(-\lambda_9 - \lambda_{11} + \lambda_{13} + \lambda_{15})\}(a^3b - a^7b)] \quad (3.6) \end{aligned}$$

$$\begin{aligned} ue_7 = & \frac{1}{8} [\{2(\lambda_1 - \lambda_5) - \sqrt{2}i(\lambda_2 + \lambda_4 - \lambda_6 - \lambda_8)(1 - a^4) + \\ & \{2(\lambda_2 - \lambda_6) - \sqrt{2}i(-\lambda_1 + \lambda_3 + \lambda_5 - \lambda_7)\}(a - a^5) + \\ & \{2(\lambda_3 - \lambda_7) - \sqrt{2}i(-\lambda_2 + \lambda_4 + \lambda_6 - \lambda_8)\}(a^2 - a^6) + \\ & \{2(\lambda_4 - \lambda_8) - \sqrt{2}i(-\lambda_3 + \lambda_5 - \lambda_1 + \lambda_7)\}(a^3 - a^7) + \\ & \{2(\lambda_9 - \lambda_{13}) - \sqrt{2}i(\lambda_{10} + \lambda_{12} - \lambda_{14} - \lambda_{16})\}(b - a^4b) + \\ & \{2(\lambda_{10} - \lambda_{14}) - \sqrt{2}i(-\lambda_9 + \lambda_{11} + \lambda_{13} - \lambda_{15})\}(ab - a^5b) + \\ & \{2(\lambda_{11} - \lambda_{15}) - \sqrt{2}i(-\lambda_{10} + \lambda_{12} + \lambda_{14} - \lambda_{16})\}(a^2b - a^6b) + \\ & \{2(\lambda_{12} - \lambda_{16}) - \sqrt{2}i(-\lambda_9 - \lambda_{11} + \lambda_{13} + \lambda_{15})\}(a^3b - a^7b)] \quad (3.7) \end{aligned}$$

- (i) Group code $I_{\mathcal{A}} = \{u \in FG_3 : ue_i = 0 \text{ for } i = 5, 6, 7\}$

From equations (3.5)-(3.7), it follows that no nonzero codeword u with $wt(u) < 4$ satisfies these conditions. Considering $u = \sum_{t=0}^3 \lambda_{2t+1} a^{2t}$ with $wt(u) = 4$, we observe that $ue_6 = ue_7 = 0$ holds precisely when $\lambda_1 = \lambda_5$, $\lambda_3 = \lambda_7$ while $ue_5 = 0$ occurs only under the condition $\lambda_1 = \lambda_5 = \lambda_3 = \lambda_7$. Hence $d(I_{\mathcal{A}}) = 4$. And $I_{\mathcal{A}} \cong FG_{e_1} \oplus FG_{e_2} \oplus FG_{e_3} \oplus FG_{e_4}$ so $\dim(I_{\mathcal{A}}) = 4$.

- (ii) Clearly, group code $I_{\mathcal{B}} = \{u \in FG_3 : ue_i = 0 \text{ for } i = 4, 5, 6, 7\}$

No non zero code word u with $wt(u) < 8$ satisfies these conditions. Considering $u = \sum_{t=1}^8 \lambda_t a^{t-1}$ with $wt(u) = 8$ then the relation $ue_i = 0$ for $4 \leq i \leq 7$ holds precisely when all λ_i are identical.

The remaining parts can be proved in a similar manner. $\square$

Theorem 3.3: *The following table no. 4 describes the group codes with generating idempotents over the group ring FG_4*

Table 4

Sr.	Group codes	Distance	Dimension
(i)	$I_A, A = \{e_i, 1 \leq i \leq 8\}$	2	8
(ii)	$I_B, B = \{e_i, 1 \leq i \leq 7\}$	4	7
(iii)	$I_{\{e_1, e_2\}}$	16	2
(iv)	$I_{\{e_1, e_2, e_3\}}$	16	3
(v)	$I_{\{e_1, e_2, e_3, e_4\}}$	16	4
(vi)	$I_\vartheta, \vartheta = \{e_i, 1 \leq i \leq 6\}$	8	6
(vii)	$I_{\{e_9, e_{10}\}}$	8	8
(viii)	$I_{\{e_8, e_9, e_{10}\}}$	8	9
(ix)	$I_\Lambda, \Lambda = \{e_i, 7 \leq i \leq 10\}$	8	10
(x)	$I_\Omega, \Omega = \{e_i, 6 \leq i \leq 10\}$	4	11
(xi)	$I_{\mathcal{F}}, \mathcal{F} = \{e_i, 5 \leq i \leq 10\}$	2	12

Proof: Let $u = \sum_{t=1}^4 \lambda_t a^{t-1} + \sum_{t=1}^4 \lambda_{t+4} a^{t-1} b + \sum_{t=1}^4 \lambda_{t+8} a^{t-1} z + \sum_{t=1}^4 \lambda_{t+12} a^{t-1} bz \in \text{FG}_4$ then

$$ue_1 = (\sum_{k=1}^{16} \lambda_k) e_1 \quad (3.8)$$

$$ue_2 = (\sum_{\text{for } k=1,5,9,13} \lambda_k - \sum_{\text{for } k=3,7,11,15} \lambda_k + \sum_{\text{for } k=2,6,10,14} i\lambda_k - \sum_{\text{for } k=4,8,12,16} i\lambda_k) e_2 \quad (3.9)$$

$$ue_3 = (\sum_{j=1}^{16} (-1)^{j+1} \lambda_j) e_3 \quad (3.10)$$

$$ue_4 = (\sum_{\text{for } j=1,5,9,13} \lambda_j - \sum_{\text{for } j=3,7,11,15} \lambda_j - \sum_{\text{for } j=2,6,10,14} i\lambda_j + \sum_{\text{for } j=4,8,12,16} i\lambda_j) e_4 \quad (3.11)$$

$$ue_5 = (\sum_{j=1}^4 \lambda_j - \sum_{j=5}^8 \lambda_j + \sum_{j=9}^{12} \lambda_j - \sum_{j=13}^{16} \lambda_j) e_5 \quad (3.12)$$

$$ue_6 = (\sum_{\text{for } j=1,7,9,15} \lambda_j - \sum_{\text{for } j=3,5,11,13} \lambda_j + \sum_{\text{for } j=2,8,10,16} i\lambda_j - \sum_{\text{for } j=4,6,12,14} i\lambda_j) e_6 \quad (3.13)$$

$$ue_7 = (\sum_{j=1}^4 (-1)^{j+1} \lambda_j + \sum_{j=5}^8 (-1)^j \lambda_j + \sum_{j=9}^{12} (-1)^{j+1} \lambda_j + \sum_{j=13}^{16} (-1)^j \lambda_j) e_7 \quad (3.14)$$

$$ue_8 = (\sum_{\text{for } j=1,7,9,15} \lambda_j - \sum_{\text{for } j=3,5,11,13} \lambda_j - \sum_{\text{for } j=2,8,10,16} i\lambda_j + \sum_{\text{for } j=4,6,12,14} i\lambda_j) e_8 \quad (3.15)$$

$$ue_9 = \frac{1}{4} [(\lambda_1 + i\lambda_3 - \lambda_9 - i\lambda_{11})(1 - z - ia^2 + ia^2 z) + (\lambda_2 + i\lambda_4 - \lambda_{10} - i\lambda_{12})(a - az - ia^3 + ia^3 z) + (\lambda_5 + i\lambda_7 - \lambda_{13} - i\lambda_{15})(b - bz - ia^2 b + ia^2 bz) + (\lambda_6 + i\lambda_8 - \lambda_{14} - i\lambda_{16})(ab - abz - ia^3 b + ia^3 bz)] \quad (3.16)$$

$$ue_{10} = \frac{1}{4} [(\lambda_1 - i\lambda_3 - \lambda_9 + i\lambda_{11})(1 - z + ia^2 - ia^2 z) + (\lambda_2 - i\lambda_4 - \lambda_{10} + i\lambda_{12})(a - az + ia^3 - ia^3 z) + (\lambda_5 - i\lambda_7 - \lambda_{13} + i\lambda_{15})(b - bz + ia^2 b - ia^2 bz) + (\lambda_6 - i\lambda_8 - \lambda_{14} + i\lambda_{16})(ab - abz + ia^3 b - ia^3 bz)] \quad (3.17)$$

- (i) Clearly, $I_A = \{u \in FG_4 : ue_i = 0 \text{ for } i = 9, 10\}$. Let $u = \lambda g \in FG_4$ with $wt(u) = 1$. In this case $ue_i \neq 0$ for $i = 9, 10$. Now consider, $u = \lambda_1 + \lambda_9 z$ with $wt(u) = 2$. Then $ue_9 = 0$ & $ue_{10} = 0$ hold if and only if $\lambda_1 = \lambda_9$. So $u \in I_A$. Therefore, I_A represents a $(16, 8, 2)$ group code.
- (ii) Clearly, $I_B = \{u \in FG_4 : ue_i = 0 \text{ for } i = 8, 9, 10\}$. From (3.15) to (3.17), no non zero code word u with $wt(u) < 4$ satisfies $ue_i = 0$ for $i = 8, 9, 10$. If we consider $u = \lambda_1 + \lambda_3 a^2 + \lambda_9 z + \lambda_{11} a^2 z$ then $ue_8 = ue_9 = ue_{10} = 0$ yield the following set of independent equations

$$\begin{aligned}\lambda_1 - \lambda_3 + \lambda_9 - \lambda_{11} &= 0 \\ \lambda_1 + i\lambda_3 - \lambda_9 - i\lambda_{11} &= 0 \\ \lambda_1 - i\lambda_3 - \lambda_9 + i\lambda_{11} &= 0\end{aligned}$$

On solving these, we obtain $\lambda_1 = \lambda_3 = \lambda_9 = \lambda_{11}$. Consequently $d(I_B) = 4$, and since $I_B \cong_{r=1}^7 \oplus FG_{e_r}$ it follows that $\dim(I_B) = 7$. Therefore, I_B represents a $(16, 7, 4)$ group code.

The proof of the remaining parts proceeds in the same manner. $\square$

Theorem 3.4: *The following table no. 5 describes the group codes with generating idempotents over the group ring FG_9*

Table 5

Sr.	Group codes	Distance	Dimension
(i)	$I_{\{e_1, e_2, e_3, e_4\}}$	8	4
(ii)	$I_{\{e_1, e_2, e_3, e_4, e_5\}}$	4	5
(iii)	$I_A, A = \{e_i, 1 \leq i \leq 8\}$	2	8
(iv)	$I_{\{e_1, e_2\}}$	8	2
(v)	$I_{\{e_9, e_{10}\}}$	2	8
(vi)	$I_{\{e_1, e_2, e_9, e_{10}\}}$	2	10
(vii)	$I_{\{e_1, e_9, e_{10}\}}$	2	9
(viii)	$I_{\{e_1, e_9\}}$	16	5
(ix)	$I_{\{e_i\}}, i=1, 2$	16	1

Proof: Let $u = \sum_{j=1}^2 (\lambda_j + \lambda_{2+j} b) a^{j-1} + \sum_{j=1}^3 (\lambda_{4+j} + \lambda_{7+j} a + \lambda_{10+j} b + \lambda_{13+j} ab) z^j \in FG_9$ then

$$ue_1 = (\sum_{j=1}^{16} \lambda_j) e_1 \quad (3.18)$$

$$ue_2 = (\sum_{j=1}^2 \lambda_j - \sum_{j=3}^4 \lambda_j + \sum_{j=5}^{10} \lambda_j - \sum_{j=11}^{16} \lambda_j) e_2 \quad (3.19)$$

$$ue_3 = (\sum_{j=1}^4 (-1)^{j+1} \lambda_j + \sum_{j=5}^7 \lambda_j - \sum_{p=8}^{10} \lambda_p + \sum_{k=11}^{13} \lambda_k - \sum_{l=14}^{16} \lambda_l) e_3 \quad (3.20)$$

$$ue_4 = (\sum_{j=1}^4 \lambda_j - \lambda_5 + \sum_{j=6}^7 (-1)^j \lambda_j + \sum_{j=8}^{10} (-1)^{j+1} \lambda_j + \sum_{j=11}^{13} (-1)^j \lambda_j + \sum_{j=14}^{16} (-1)^{j+1} \lambda_j) e_4 \quad (3.21)$$

$$ue_5 = (\lambda_1 - \sum_{j=2}^3 \lambda_j + \sum_{j=4}^7 \lambda_j - \sum_{t=8}^{13} \lambda_t + \sum_{p=14}^{16} \lambda_p) e_5 \quad (3.22)$$

$$ue_6 = (\sum_{j=1}^2 \lambda_j - \sum_{j=3}^5 \lambda_j + \sum_{j=6}^7 (-1)^j \lambda_j + \sum_{j=8}^{10} (-1)^{j+1} \lambda_j + \sum_{j=11}^{13} (-1)^{j+1} \lambda_j + \sum_{j=14}^{16} (-1)^j \lambda_j) e_6 \quad (3.23)$$

$$ue_7 = (\sum_{j=1}^4 (-1)^{j+1} \lambda_j + \sum_{j=5}^{16} (-1)^j \lambda_j) e_7 \quad (3.24)$$

$$ue_8 = (\sum_{j=1}^2 (-1)^{j+1} \lambda_j + \sum_{j=3}^{10} (-1)^j \lambda_j + \sum_{j=11}^{16} (-1)^{j+1} \lambda_j) e_8 \quad (3.25)$$

$$\begin{aligned} ue_9 = & \frac{1}{4} [(\lambda_1 + i\lambda_5 - \lambda_6 - i\lambda_7)(1 - iz - z^2 + iz^3) \\ & + (\lambda_2 + i\lambda_8 - \lambda_9 - i\lambda_{10})(a - iaz - az^2 + iaz^3) \\ & + (\lambda_3 + i\lambda_{11} - \lambda_{12} - i\lambda_{13})(b - ibz - bz^2 + ibz^3) \\ & + (\lambda_4 + i\lambda_{14} - \lambda_{15} - i\lambda_{16})(ab - iabz - abz^2 + iabz^3)] \end{aligned} \quad (3.26)$$

$$\begin{aligned} ue_{10} = & \frac{1}{4} [(\lambda_1 - i\lambda_5 - \lambda_6 + i\lambda_7)(1 + iz - z^2 - iz^3) \\ & + (\lambda_2 - i\lambda_8 - \lambda_9 + i\lambda_{10})(a + iaz - az^2 - iaz^3) \\ & + (\lambda_3 - i\lambda_{11} - \lambda_{12} + i\lambda_{13})(b + ibz - bz^2 - ibz^3) \\ & + (\lambda_4 - i\lambda_{14} - \lambda_{15} + i\lambda_{16})(ab + iabz - abz^2 - iabz^3)] \end{aligned} \quad (3.27)$$

- (i) It is clear that the group code $I_{\{e_1, e_2, e_3, e_4\}} = \{u \in FG_9 : ue_i = 0 \text{ for } i = 5 \text{ to } 10\}$. No non zero code word with weight less than 8 in $I_{\{e_1, e_2, e_3, e_4\}}$.

Consider an arbitrary element of FG_9 of weight 8, given by $u = \lambda_1 + \lambda_2 a + \lambda_5 z + \lambda_6 z^2 + \lambda_7 z^3 + \lambda_8 az + \lambda_9 az^2 + \lambda_{10} az^3$. Thus, $ue_i = 0$ if and only if all λ_i 's are equal. Consequently, $d(I_{\{e_1, e_2, e_3, e_4\}}) = 8$.

Hence $I_{\{e_1, e_2, e_3, e_4\}}$ represents a (16,4,8) group code.

- (ii) It can be verified that no code word in $I_{\{e_1, e_2, e_3, e_4, e_5\}}$ has weight less than 4. Consider an element of FG_9 of the form $u = \lambda_1 + \lambda_5 z + \lambda_6 z^2 + \lambda_7 z^3$ with $wt(u) = 4$. Then $u \in I_{\{e_1, e_2, e_3, e_4, e_5\}}$ iff $\lambda_1 = \lambda_6 = \lambda_5 = \lambda_7$. Therefore, $d = 4$ and $dimension = 5$.
- (iii) From equations (3.26)&(3.27), I_A contains no code word of weight 1. Moreover, $u = \lambda_1 + \lambda_6 z^2 \in I_A$ exactly when $\lambda_1 = \lambda_6$. Hence, it follows that $d(I_A) = 2$. Furthermore, $dim(I_A) = 8$.
- (iv) Using the equations (3.20) to (3.27) it can be verified that the group code $I_{\{e_1, e_2\}}$ contains no code word of weight < 8. Furthermore, the element $1 + a + z + z^2 + z^3 + az + az^2 + az^3$ in $I_{\{e_1, e_2\}}$ has the minimum weight of 8. It is thereby concluded that $d(I_{\{e_1, e_2\}}) = 8$.

The proof of the remaining parts proceeds in the same manner. $\square$

References

- [1] D.C.K. Wong and M.H. Ang "Group codes define over dihedral groups of small order", *Malays. J. of Math. Sci.* Vol. 7(s), pp. 101-116 (2013).

- [2] F. S. Admasu, and A. Sehgal, "Counting subgroups of fixed order in finite abelian groups", *J. Discrete Math. Sci. Cryptogr*, Vol.24, no. 1, pp. 263–276 (2021).
- [3] F. Dutra, R. Ferraz, and C. P. Milies "Semisimple Group Codes and Dihedral Codes", *Algebra Discrete Math*, no. 3, pp. 28-48 (2009).
- [4] Marines Guerreiro, "Group Algebras and Coding theory", Instituto de Matematica e Estatistica da Uni. de Sao Paulo (2016).
- [5] G.D. James and M.W. Liebeck "Representations and Characters of Groups", Cambridge Uni. Press (1993).
- [6] M. Pruthi "Idempotents in the Group ring of Quaternions", *J. Inf. Optim. Sci.*, vol. 37, no.2, pp. 271-278 (2016).
- [7] M. Pruthi and Sudesh "Idempotents in the group algebra of dihedral groups", *J. Inf. Optim. Sci.*, vol. 39, no.2, pp. 461-465 (2018).
- [8] R. S. Pierce, "Associative Algebras", New York:Springer-Verlag (1982).
- [9] S. Sehrawat and M. Pruthi "Codes over $D_n \times C_t$ and $D_n \times D_n$ ", *Glob. J. Pure Appl. Math*, vol. 14, no.5, pp. 677-688 (2018).
- [10] S. Sehrawat and M. Pruthi "Codes Over Dihedral Groups", *J. Inf. Optim. Sci*, vol. 39, no.4, pp. 889-901 (2018).
- [11] S. Sehrawat and M. Pruthi "Codes over non-abelian groups", *J. Inf. Optim. Sci*, vol. 40, no.3, pp. 789-804 (2019).
- [12] S. Sehrawat and M. Pruthi, "Codes Over Group $Q_{4n} \times C_t$ ", *Int. J. Mech. Eng.*, vol. 7, no.6, pp. 189-197 (2022).
- [13] N. U. Sivaranjani, E. Nandakumar, G. Mittal, and R. K. Sharma, "On the unit group of the semisimple group algebra $K_q GL(2, Z_5)$ ", *J. Interdiscip. Math.*, vol 27, no.1, pp. 121–134 (2024).
- [14] L.R. Vermani "Elements of Algebraic Coding Theory", Chapman and Hall (1996).

Received December, 2024