THE ALGEBRAIC STRUCTURE OF FINITE METABELIAN GROUP ALGEBRAS

Gurmeet K. Bakshi, Shalini Gupta, and Inder Bir S. Passi

1Centre for Advanced Study in Mathematics, Panjab University, Chandigarh, India
2Department of Mathematics, Punjabi University, Patiala, India
3Indian Institute of Science Education and Research, Mohali, India

An algorithm for the explicit computation of a complete set of primitive central idempotents, Wedderburn decomposition, and the automorphism group of the semisimple group algebra of a finite metabelian group is developed. The algorithm is illustrated with its application to the semisimple group algebra of an arbitrary metacyclic group, and certain indecomposable groups whose central quotient is the Klein four-group.

Key Words: Automorphism group; Finite semisimple group algebra; Metabelian group; Primitive central idempotent; Wedderburn decomposition.

2010 Mathematics Subject Classification: 16S34; 20C05; 16K20.

1. INTRODUCTION

Let $\mathbb{F}_q[G]$ be the group algebra of a finite group $G$ over the finite field $\mathbb{F}_q$ with $q$ elements. In order to understand the algebraic structure of $\mathbb{F}_q[G]$, in the semisimple case, i.e., when $q$ is coprime to the order of $G$, an essential step is to compute a complete set of primitive central idempotents and the Wedderburn decomposition of $\mathbb{F}_q[G]$. These computations, in turn, help to investigate the automorphism group and the unit group of $\mathbb{F}_q[G]$.

Let $(H, K)$ be a strongly Shoda pair [3, Definition 5] of $G$, and let $C$ be a $q$-cyclotomic coset of $\text{Irr}(K/H)$, the set of irreducible characters of $K/H$ over the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$, corresponding to a generator of $\text{Irr}(K/H)$. Broche and Rio [3, Theorem 7] proved that the pair $((H, K), C)$ defines a primitive central idempotent, $e_C(G, K, H)$, of $\mathbb{F}_q[G]$. They further proved that, if $G$ is an abelian-by-supersolvable group, then every primitive central idempotent of the semisimple group algebra $\mathbb{F}_q[G]$ is defined by a pair of the type $((H, K), C)$. However, it is possible that two distinct such pairs may define the same primitive central idempotent. Thus, in order to determine the algebraic structure of $\mathbb{F}_q[G]$, $G$ abelian-by-supersolvable, the problem lies in finding a set $\Xi$ of pairs of type $((H, K), C)$.
so that \( \{ e_C(G, K, H) \mid ((H, K), C) \in \Xi \} \) is a complete irredundant set of primitive central idempotents of \( \mathbb{F}_q[G] \).

Following the method developed in [2] and [9], where this problem has been investigated for rational group algebras. In Section 2, we provide an efficient algorithm for computing the structure of \( \mathbb{F}_q[G] \), \( G \) metabelian (Theorem 2). Our analysis, in turn, leads to an explicit description of the Wedderburn decomposition and the automorphism group of \( \mathbb{F}_q[G] \) (Theorem 3).

In Section 3, we illustrate our algorithm with its application to an arbitrary finite metacyclic group \( G = \langle a, b \mid a^n = 1, b^r = a^k, b^{-1}ab = a' \rangle \), \( n, t, k, r \) natural numbers, \( r' \equiv 1 \pmod{n} \), \( k(r - 1) \equiv 0 \pmod{n} \), of order \( nt \) coprime to \( q \), and provide an alternative way of finding a complete set of the primitive central idempotents to those given in [1].

We next apply our result, in Section 4, to indecomposable groups \( G \) whose central quotient, \( G/Z(G) \), is the Klein four-group. It is known [7, Chapter 5], that such groups breakup into five different classes. Ferraz, Goodearl, and Polcino Milies [5] have given, in each case, a lower bound on the number of simple components of the semisimple finite group algebra \( \mathbb{F}_q[G] \). We provide the complete algebraic structure of the semisimple group algebra \( \mathbb{F}_q[G] \) for group \( G \) in two of the five classes, thus improving Theorems 3.1 and 3.2 of [5].

# 2. METABELIAN GROUPS

Let \( G \) be a finite group. We adopt the following notation:

\[
\begin{align*}
\varepsilon_{\mathfrak{F}_q}(\chi) & = \frac{1}{|G|} \sum_{g \in G} \sigma(\chi(g))g^{-1}, \\
\mathcal{C}(K/H) & = \{ \text{the set of pairs } (H, K), \text{where } H \leq K \leq G \text{ and } K/H \text{ is cyclic} \}, \\
R(K/H) & = \{ \text{the set of distinct orbits of } \mathcal{C}(K/H) \text{ under the action of } N_G(H) \cap N_G(K) \text{ on } \mathcal{C}(K/H) \text{ given by } g \cdot C = C^g(= g^{-1}Cg), g \in N_G(H) \cap N_G(K), C \in \mathcal{C}(K/H), \text{where } N_G(H) \text{ denotes the normalizer of } H \text{ in } G; \\
E_G(K/H) & = \{ \text{the stabilizer of any } C \in \mathcal{C}(K/H) \text{ under the above action of } N_G(H) \cap N_G(K) \text{ on } \mathcal{C}(K/H) \text{ (note that this stabilizer does not depend on } C); \\
e_C(K, H) & = \left| K \right|^{-1} \sum_{g \in K} \text{tr}_{\mathfrak{F}_q[G]}(\chi(\zeta))g^{-1}, \text{where } \chi \text{ is a representative of the } q\text{-cyclotomic coset } C, \text{ and } \zeta \text{ is a primitive } [K: H]\text{-th root of unity in } \mathbb{F}_q^\times \text{ (H, K) }\in \mathcal{C}(K/H), C \in \mathcal{C}(K/H); \\
e_C(G, K, H) & = \text{the sum of distinct } G\text{-conjugates of } e_C(K, H).
\end{align*}
\]

For the rest of this section, we assume \( G \) to be a finite metabelian group.

## 2.1. Primitive Central Idempotents

We follow the notation introduced in [2].

- \( \mathfrak{A} \) : a fixed maximal abelian subgroup of \( G \) containing its derived subgroup \( G' \).
- \( \mathcal{F} \) : the set of all subgroups \( D \) of \( G \) with \( D \leq \mathfrak{A} \) and \( \mathfrak{A}/D \) cyclic.
For $D_1, D_2 \in \mathcal{T}$, we say that $D_1$ is equivalent to $D_2$ if there exists $g \in G$ such that $D_2 = D_1^g$.

- $\mathcal{T}_G :=$ a set of representatives of the distinct equivalence classes of $\mathcal{T}$.

For $D \in \mathcal{T}$, let

- $K_D :=$ a fixed maximal element of $\{ K \mid \mathcal{A} \leq K \leq G, K' \leq D \}$;
- $\mathcal{R}(D) :=$ the set of those linear representations of $K_D$ over $\mathbb{F}_q$ whose restriction to $\mathcal{A}$ has kernel $D$;
- $\mathcal{R}_c(D) :=$ a complete set of those representations in $\mathcal{R}(D)$ which are not mutually $G$-conjugate.

The following result is proved in [2] for complex irreducible representations. However, the analogous proof works for the irreducible representations of $G$ over $\mathbb{F}_q$.

**Theorem 1** ([2]). Let $G$ be a finite metabelian group with $\mathcal{A}$ and $\mathcal{T}_G$ as defined above. Then

$$\Omega = \{ \rho^G \mid \rho \in \mathcal{R}_c(D), \ D \in \mathcal{T}_G \},$$

is a complete set of inequivalent irreducible representations of $G$ over $\mathbb{F}_q$, where $\rho^G$ denotes $\rho$ induced to $G$.

Furthermore, $\rho^G \in \Omega$ is faithful if, and only if, $D$ is core-free in $G$, i.e., $\bigcap_{x \in G} D^x = \{1\}$.

For $N \trianglelefteq G$ with

$\mathcal{A}_N/N :=$ a maximal abelian subgroup of $G/N$ containing $(G/N)'$,

define

$$\mathcal{T}_{G/N} := \{ (D/N, \mathcal{A}_N/N) \mid D/N \in \mathcal{T}_{G/N}, D/N \text{ core-free in } G/N \}.$$ Let

$$\mathcal{S} := \{ (N, D/N, \mathcal{A}_N/N) \mid N \trianglelefteq G, \mathcal{T}_{G/N} \neq \emptyset, (D/N, \mathcal{A}_N/N) \in \mathcal{T}_{G/N} \}.$$ By [2, Lemma 6], each element $(N, D/N, \mathcal{A}_N/N) \in \mathcal{S}$ defines a strongly Shoda pair $(D, \mathcal{A}_N)$ in $G$ and the mapping $((N, D/N, \mathcal{A}_N/N) \mapsto (D, \mathcal{A}_N))$ from $\mathcal{S}$ to the set of strongly Shoda pairs of $G$ is one-one. Thus $\mathcal{S}$ may be regarded as a subset of strongly Shoda pairs of $G$.

Let ord$_n(q)$ denote the order of $q$ modulo $n, n \geq 1$. We prove the following theorem.

**Theorem 2.** Let $\mathbb{F}_q$ be a finite field with $q$ elements and $G$ a finite metabelian group. Suppose that $\gcd(q, |G|) = 1$. Theorem 2.
(i) \( \{ e_c(G, \mathcal{A}_N, D) \mid (N, D/N, \mathcal{A}_N/N) \in \mathcal{P}, C \in R(\mathcal{A}_N/D) \} \) is a complete set of primitive central idempotents of \( \mathbb{F}_q[G] \).

(ii) For \( (N, D/N, \mathcal{A}_N/N) \in \mathcal{P} \) and \( C \in R(\mathcal{A}_N/D) \), the simple component \( \mathbb{F}_q[G] e_c(G, \mathcal{A}_N, D) \) is isomorphic to \( M_{[G:G]}(\mathbb{F}_q^{|G|/|\mathcal{A}_N|}) \), the algebra of \( [G : \mathcal{A}_N] \times [G : \mathcal{A}_N] \) matrices over the field \( \mathbb{F}_q^{|G|/|\mathcal{A}_N|} \), where \( o(\mathcal{A}_N, D) = \text{ord}_{[G:G]}(q) \).

**Proof.** (i) Let

\[
\Xi := \{((N, D/N, \mathcal{A}_N/N), C) \mid (N, D/N, \mathcal{A}_N/N) \in \mathcal{P}, C \in R(\mathcal{A}_N/D) \}.
\]

If \( ((N, D/N, \mathcal{A}_N/N), C) \in \Xi \), then, by [2, Lemma 6], \( (D, \mathcal{A}_N) \) is a strongly Shoda pair in \( G \), and therefore, by [3, Theorem 7], \( e_c(G, \mathcal{A}_N, D) \) is a primitive central idempotent of \( \mathbb{F}_q[G] \). Thus we have a map

\[
\pi: ((N, D/N, \mathcal{A}_N/N), C) \mapsto e_c(G, \mathcal{A}_N, D)
\]

from \( \Xi \) to a complete set of primitive central idempotents of \( \mathbb{F}_q[G] \). In order to prove the theorem, we need to prove that \( \pi \) is 1-1 and onto.

To show that \( \pi \) is onto, let \( e \) be a primitive central idempotent of \( \mathbb{F}_q[G] \). We have \( e = e_x(\chi) \), for some \( \chi \in \text{Irr}(G) \). Let \( \tau \) be a representation affording \( \chi \) and \( N = \text{kerr} \tau \), the kernel of the character \( \tau \). Let \( \psi \) be the corresponding faithful representation of \( G/N \). By Theorem 1, it follows that there exists a unique pair \( (D/N, \mathcal{A}_N/N) \in \mathcal{P}_{G/N} \) and a representation \( \overline{\psi} \) of \( \mathcal{A}_N/N \) with kernel \( D/N \) such that \( \overline{\psi} = \overline{\rho}(\mathcal{A}_N/N) \). This yields \( \chi = \psi^G \), where \( \psi^G \) is the character afforded by \( \rho: \mathcal{A}_N \to \mathbb{F}_q \) given by \( \rho(x) = \overline{\rho}(xN) \). Since \( \text{kerr} \psi = D \), by [1, Lemma 1], we have

\[
e_{\mathbb{F}_q}(\chi) = e_c(G, \mathcal{A}_N, D),
\]

where \( C \in \mathcal{R}(\mathcal{A}_N/D) \) is the \( q \)-cyclotomic coset of \( \overline{\psi} \) and consequently \( \pi \) is onto.

To show that \( \pi \) is 1-1, let \( ((N, D/N, \mathcal{A}_N/N), C) \) and \( ((\tilde{N}, \tilde{D}/\tilde{N}, \tilde{\mathcal{A}}_N/\tilde{N}), \tilde{C}) \in \Xi \) be such that

\[
e_c(G, \mathcal{A}_N, D) = e_{\mathbb{F}_q}(\chi) = e_{\mathbb{F}_q}(\tilde{\chi}),
\]

where \( \chi \) and \( \tilde{\chi} \) be the characters afforded by \( \rho^G_0 \) and \( \tilde{\rho}^G \), respectively. By [1, Lemma 1], \( e_{\mathbb{F}_q}(\chi) = e_c(G, \mathcal{A}_N, D) \) and \( e_{\mathbb{F}_q}(\tilde{\chi}) = e_{\mathbb{F}_q}(G, \mathcal{A}_N, D) \). Therefore, Eq. (3) implies that \( e_{\mathbb{F}_q}(\chi) = e_{\mathbb{F}_q}(\tilde{\chi}) \), which, in turn, implies that

\[
\tilde{\chi} = \sigma \circ \chi, \quad \sigma \in \text{Gal}(\mathbb{F}_q(\chi)/\mathbb{F}_q).
\]

Consequently, \( \tilde{N} = \text{kerr}(\tilde{\chi}) = \text{kerr}(\chi) = N \). Also, by going modulo \( N \), it follows from Eq. (4) and Theorem 1 that \( D/N \) and \( \tilde{D}/N \) are conjugate in \( G/N \). This gives \( D/N = \tilde{D}/N \), i.e., \( D = \tilde{D} \). Next, if \( \{ z_1, z_2, \ldots, z_k \} \) is a transversal of \( E_G(\mathcal{A}_N/D) \) in \( G \), then, by [3, Lemma 4] and Eq. (3), we have

\[
\sum_{j=1}^k e_{c}(\mathcal{A}_N, D^{z_j}) = \sum_{j=1}^k e_{\mathbb{F}_q}(\mathcal{A}_N, D^{z_j}).
\]
Since both the sides of the above equation are primitive central idempotents in $\mathbb{F}_q[\mathbb{A}_N]$, it follows that, for some $j$, $1 \leq j \leq k$,

$$e_C(\mathbb{A}_N, D) = e_{\tilde{C}^j}(\mathbb{A}_N, D^j).$$  (6)

However, by [3, Proposition 2], $e_C(\mathbb{A}_N, D) = e_{\mathbb{F}_q}(\rho)$, and $e_{\tilde{C}^j}(\mathbb{A}_N, D^j) = e_{\mathbb{F}_q}(\tilde{\rho}^j)$. Therefore, we have by Eq. (6), $e_{\mathbb{F}_q}(\rho) = e_{\mathbb{F}_q}(\tilde{\rho}^j)$, which, as before, gives $D = \ker\rho = \ker\tilde{\rho}^j = D^j$, i.e., $z_j \in N_\alpha(D)$. Consequently, $C$ and $C'$ have the same orbits. This proves that $\pi$ is 1-1.

(ii) follows from [3, Corollary 9].

\[ \square \]

2.2. Wedderburn Decomposition and Automorphism Group

We continue with the notation introduced in Subsection 2.1. Let $\text{Aut}(\mathbb{F}_q[G])$ be the group of $\mathbb{F}_q$-automorphisms of $\mathbb{F}_q[G]$. For $n \geq 1$, let $\mathbb{Z}_n$ be the additive group of integers modulo $n$, $S_n$ the symmetric group of degree $n$, $SL_n(K)$ the group of invertible $n \times n$ matrices over the field $K$ of determinant 1, and for any algebra $K$, let $K^{(n)}$ denote the direct sum of $n$ copies of $K$. Let $\xi$ be a primitive $|G|$-th root of unity in $\mathbb{F}_q$. Let $(N, D/N, \mathbb{A}_N/N) \in \mathcal{F}$. Then $\mathbb{A}_N/D$ is a cyclic group generated by $aD$, say. Let $x_1, x_2, \ldots, x_i$ be a transversal of $\mathbb{A}_N$ in $G$, and $r_i$, $1 \leq i \leq t$, be integers such that $x_i^{-1}ax_iD = a^rD$. Let $\xi = \xi^{(G)/|D'|}$, and $\mathcal{R}(N, D/N, \mathbb{A}_N/N)$ be the subfield of $\mathbb{F}_q$ obtained by adjoining the $t$ elements $\sum_{i=1}^{t} \xi^{r_i}$, $1 \leq j \leq t - 1$ to $\mathbb{F}_q$. It is easily seen that the field $\mathcal{R}(N, D/N, \mathbb{A}_N/N)$ is independent of the choice of transversal of $\mathbb{A}_N$ in $G$.

For $d \mid [G : G']$ and $l \mid [\mathbb{F}_q(\xi) : \mathbb{F}_q]$, let $\mathcal{S}_{d,l}$ be the set of those $(N, D/N, \mathbb{A}_N/N) \in \mathcal{F}$ such that the following equations hold:

(i) $[G : \mathbb{A}_N] = d$;
(ii) $[\mathcal{R}(N, D/N, \mathbb{A}_N/N) : \mathbb{F}_q] = l$.

Clearly, $\mathcal{S}_{d,l} \cap [G : G'], l \mid [\mathbb{F}_q(\xi) : \mathbb{F}_q]$, are disjoint and \(\mathcal{F} = \bigcup_{d \mid [G : G']} \mathcal{S}_{d,l} \cap [G : G'], l \mid [\mathbb{F}_q(\xi) : \mathbb{F}_q]\).

Theorem 3. With the above notation, we have as follows:

(i) $\mathbb{F}_q[G] \cong \bigoplus_{d \mid [G : G']} \bigoplus_{l \mid [\mathbb{F}_q(\xi) : \mathbb{F}_q]} \mathbb{M}_d(\mathbb{F}_q)^{(x_d)}$;

(ii) $\text{Aut}(\mathbb{F}_q[G]) \cong \bigoplus_{d \mid [G : G']} \bigoplus_{l \mid [\mathbb{F}_q(\xi) : \mathbb{F}_q]} K_{d,l}^{(x_d)} \rtimes S_{x_d,l}$.

Here $K_{d,l} = SL_n(\mathbb{F}_q) \rtimes \mathbb{Z}_l$, a semidirect product of $SL_n(\mathbb{F}_q)$ by $\mathbb{Z}_l$, and $x_{d,l} = \sum_{(N, D/N, \mathbb{A}_N/N) \in \mathcal{S}_{d,l}} [R(\mathbb{A}_N/D)]$.

Proof. (i) It follows from Theorem 2 that for $(N, D/N, \mathbb{A}_N/N) \in \Xi$, where $\Xi$ is as defined in Eq. (1),

$$\mathbb{F}_q[G] \cong M_{[G : \mathbb{A}_N]}(\mathbb{F}_q^{a_{d,l}}).$$
Thus we have
\[ \mathbb{F}_q[G] \cong \bigoplus_{(N,D)/N, \mathbb{A}_N} \mathbb{F}_q[G] e_{C}(G, \mathbb{A}_N, D) \]
\[ \cong \bigoplus_{(N,D)/N, \mathbb{A}_N} \mathbb{F}_q[G] e_{C}(G, \mathbb{A}_N, D) \]
\[ \cong \bigoplus_{(N,D)/N, \mathbb{A}_N} M_{G: \mathbb{A}_N}(\mathbb{F}_{q^d \mathbb{A}_N}) \]
\[ \cong \bigoplus_{d \mid [G:G'], l \mid [\mathbb{F}_q(\xi) : \mathbb{F}_q], (N,D)/N, \mathbb{A}_N} M_{G: \mathbb{A}_N}(\mathbb{F}_{q^{d^2 \mathbb{A}_N}}) \left( \mathbb{R}_{q^{d^2 / \mathbb{A}_N}} \right) . \]

For \( d \mid |G : G'| \), \( l \mid |\mathbb{F}_q(\xi) : \mathbb{F}_q| \), and \((N,D)/N, \mathbb{A}_N) \in \mathcal{F}_{d,l} \), we show that
\[ o(\mathbb{A}_N, D) = [\mathbb{R}(N, D/N, \mathbb{A}_N / N) : \mathbb{F}_q] = l. \tag{7} \]

If \( \rho \in \mathbb{R}_C(D) \) and \( \chi \) is the character afforded by \( \rho^G \), then, by [1, Lemma 1],
\[ [E_G(\mathbb{A}_N / D) : \mathbb{A}_N] = [\mathbb{F}_q(\xi) : \mathbb{F}_q(\chi)]. \]

However, note that
\[ \mathbb{F}_q(\chi) = \mathbb{R}(N, D/N, \mathbb{A}_N / N). \]

Therefore, we have,
\[ [\mathbb{R}(N, D/N, \mathbb{A}_N / N) : \mathbb{F}_q] = [\mathbb{F}_q(\xi) : \mathbb{F}_q][E_G(\mathbb{A}_N / D) : \mathbb{A}_N] = o(\mathbb{A}_N, D). \]

This proves (7), and we thus have
\[ \mathbb{F}_q[G] \cong \bigoplus_{d \mid [G:G'], l \mid [\mathbb{F}_q(\xi) : \mathbb{F}_q]} M_d(\mathbb{F}_q^{(\mathbb{R}(\mathbb{A}_N / D))}) \]
\[ \cong \bigoplus_{d \mid [G:G'], l \mid [\mathbb{F}_q(\xi) : \mathbb{F}_q]} M_d(\mathbb{F}_q^{(\mathbb{A}_N)}), \]
where \( \mathbb{A}_N = \sum_{(N,D)/N, \mathbb{A}_N} [\mathbb{R}(\mathbb{A}_N / D)]. \) This proves (i).

(ii) It follows from (i) and the standard results on automorphisms of finite dimensional algebras. \( \square \)
3. METACYCLIC GROUPS

We now illustrate Theorem 2 with its application to metacyclic groups; thus obtaining an alternative way of finding a complete set of primitive central idempotents of $\mathbb{F}_q[G]$ with $G$ given by presentation

$$G = \langle a, b \mid a^n = 1, b^k = a^t, b^{-1}ab = a^r \rangle,$$

where $n, t, k, r$ are natural numbers with $r' \equiv 1 \pmod{n}$, $k(r-1) \equiv 0 \pmod{n}$.

For a divisor $v$ of $n$, let the following equations hold:

- $o_v = \text{ord}_v(r)$;
- $G_{o_v} = \langle a, b^{o_v} \rangle$;
- $\mathcal{B}_{o_v} = \{(w, i, c) \in \mathbb{Z}^3 \mid w > 0, w \mid n, w \mid r^v - 1, o_v c > 0, o_v t | t, w | k + i \frac{c}{o_v} \}$.

Let

$$\mathcal{Y} = \left\{(v, i, c) \in \mathbb{Z}^3 \mid v > 0, v \mid n, c > 0, c \mid t, 0 \leq i \leq v - 1, v | k + i \frac{c}{o_v}, o_v | c \text{ and } v | i(r - 1) \right\}.$$

For $(v, i, c) \in \mathcal{Y}$, define as follows:

- $H_{v,i,c} = \langle a^v, a^{t c} \rangle$;
- $X_{v,i,c} = \{(v, z, \beta) \mid z \beta_{o_v} | c, z \equiv i \pmod{v}, \beta = \frac{c \text{gcd}(v(r-1), c)}{v_{o_v}}, \text{gcd}(v, z, \beta) = 1, \text{ and } (v, z, \beta) \in \mathcal{B}_{o_v} \}$.

Define a relation, denoted $\sim$, on $X_{v,i,c}$ as follows. For $(v, x_1, \beta_1), (v, x_2, \beta_2) \in X_{v,i,c}$, we say that $(v, x_1, \beta_1) \sim (v, x_2, \beta_2) \iff \beta_1 = \beta_2$ and $x_1 \equiv x_2 r^{v} \pmod{v}$ for some $j$. It is easy to see that $\sim$ is an equivalence relation on $X_{v,i,c}$. Let $\mathcal{X}_{v,i,c}$ denote the set of distinct equivalence classes of $X_{v,i,c}$ under the equivalence relation $\sim$.

**Theorem 4.** Let $\mathbb{F}_q$ be a finite field with $q$ elements and $G$ the group given by the presentation (8). If $\text{gcd}(q, nt) = 1$, then

$$\bigcup_{(v, i, c) \in \mathcal{Y}} \left\{ e_c(G, G_{o_v}, H_{v,i,c}) \mid (v, z, \beta) \in \mathcal{X}_{v,i,c}, C \in R(G_{o_v}/H_{v,i,c}) \right\}$$

is a complete set of primitive central idempotents of the group algebra $\mathbb{F}_q[G]$.

We prove the above result in a number of steps.

**Lemma 1.** $H_{v,i,c}, (v, i, c) \in \mathcal{Y}$, are all the distinct normal subgroups of $G$.

**Proof.** Let $N \triangleleft G$. Suppose $N \cap \langle a \rangle = \langle a^v \rangle$, $v \mid n, v > 0$. Now, if $N/N \cap \langle a \rangle$, as a subgroup of $G/\langle a \rangle$, is generated by $\langle b^c \langle a \rangle \rangle$, $c > 0$, $c \mid t$, then clearly,

$$N = \langle a^v, a^t b^c \rangle \text{ for some } i, 0 \leq i \leq v - 1.$$
Now $N$ being a normal subgroup of $G$, we must have $b^{-1}a'brb$, $a^{-1}a'b' a$ and $(a'b')^{t/c}$ all belong to $N$. This gives

$$v \mid i(r - 1), \quad o_v \mid c, \quad v \mid k + i t/c.$$  \hfill (10)

Consequently, Eqs. (9) and (10) yield that $(v, i, c) \in \mathfrak{R}$ and $N = H_{v, i, c}$.

Conversely, it is easy to see that for any $(v, i, c) \in \mathfrak{R}$, $H_{v, i, c}$ is normal subgroup of $G$. Furthermore,

$$|H_{v, i, c}| = \frac{nt}{vc}. \quad (11)$$

In order to complete the proof of the lemma, we need to show that $H_{v', i', c'}$, $(v, i, c) \in \mathfrak{R}$, are distinct. Let $(v_1, i_1, c_1)$, $(v_2, i_2, c_2) \in \mathfrak{R}$ be such that $H_{v_1, i_1, c_1} = H_{v_2, i_2, c_2}$. Then $\langle a^{v_1} \rangle = H_{v_1, i_1, c_1} \cap \langle a \rangle = H_{v_2, i_2, c_2} \cap \langle a \rangle = \langle a^{v_2} \rangle$ implies that $v_1 = v_2 = v$, say. Also, in view of Eq. (11), $|H_{v_1, i_1, c_1}/\langle a^{v_1} \rangle| = |H_{v_2, i_2, c_2}/\langle a^{v_2} \rangle|$ implies that $c_1 = c_2 = c$, say. Further, $a^v b^r \in H_{v_1, i_1, c_1}$, $a^v b^r \in H_{v_2, i_2, c_2}$, and $H_{v_1, i_1, c_1} = H_{v_2, i_2, c_2}$ gives that $a^{i_1 - i_2} \in H_{v, i, c} \cap \langle a \rangle = \langle a^v \rangle$. Hence $i_1 \equiv i_2 \mod v_1$, i.e., $i_1 = i_2$. This proves the lemma. \hfill \Box

**Lemma 2.** Let $(v, i, c) \in \mathfrak{R}$ and $N = H_{v, i, c}$. Then

(i) $G_v/N$ is a maximal abelian subgroup of $G/N$ containing $(G/N)^c$;

(ii) $H/N$ is a subgroup of $G_v/N$ with cyclic quotient and $H/N$ core-free in $G/N$ if, and only if, $H = H_{u, x, \beta_0}$, $(v, x, \beta) \in X_{u, x, \beta}$.

**Proof.** (i) By [4, p. 336], $G_v/N = \langle a^{v-1} \rangle$. Since $v \mid r^n - 1$, we have $G_v/N \leq \langle a^{v} \rangle \leq N$, and therefore, $G_v/N$ is abelian. Furthermore, $G_v/N$ contains $(G/N)^c$ as $G = \langle a^{v-1} \rangle \leq \langle a, b^v \rangle = G_v$. Thus $G_v/N$ is an abelian subgroup of $G/N$ containing $(G/N)^c$.

If $o_v = 1$, then clearly, $G_v/N = G/N$ is a maximal abelian subgroup of $G/N$ containing $(G/N)^c$. Let $o_v > 1$. Suppose that $K/N$ is an abelian subgroup of $G/N$ with $G_v/N \leq K/N \leq G/N$. Since $o_v > 1$, $G/N$ is not abelian. Thus $K/N \leq G/N$. Now $K \cap \langle a \rangle = \langle a \rangle$ implies that $K = \langle a, b^r \rangle$ for some $j \mid o_v$. However, $K' \leq N$ implies that $\langle a^{r-1} \rangle \leq N$, which gives that $v \mid r - 1$, i.e., $o_v \mid j$. Thus $j = o_v$ and $K/N = G_v/N$. This proves (i).

(ii) Let $H/N$ be a subgroup of $G_v/N$ with cyclic quotient. By [8, Lemma 2.2], we have

$$H = H_{u, x, \beta_0}, \quad (u, x, \beta) \in \mathfrak{B}_v \quad \text{and} \quad \text{gcd}(u, x, \beta) = 1.$$ 

Since $N \leq H$, we must have $a^v \in H$ and $a'b^r \in H$, which holds, if, and only if,

$$u \mid v, \quad \beta_0 \mid c \quad \text{and} \quad x \equiv i (\mod u). \quad (12)$$
We claim that \( \text{core}(H) \), the largest normal subgroup of \( G \) contained in \( H \), is given by

\[
\text{core}(H) = \langle a^\alpha, a^{\frac{\beta_u \alpha_v}{\gcd(\alpha(r-1),u)}} b^\delta \rangle,
\]

\[
\delta = \frac{\beta_u \alpha_v}{\gcd(\alpha(r-1),u)}.
\]

Let \( K = \langle a^\alpha, a^{\frac{\beta_u \alpha_v}{\gcd(\alpha(r-1),u)}} b^\delta \rangle \) with \( \delta \) as above. Since \((u, \frac{\beta_u \alpha_v}{\gcd(\alpha(r-1),u)}, \delta) \in \mathbb{N} \), by Lemma 1, it follows that \( K \) is a normal subgroup of \( G \). Since \( ab^\alpha a^{-1} b^{-\alpha} \in \langle a^\alpha \rangle \), we have

\[
a^\frac{\beta_u \alpha_v}{\gcd(\alpha(r-1),u)} \in \langle a^\alpha \rangle.
\]

Thus \( K \) is a subgroup of \( H_{u,z_1,b_1 \alpha_v} = H \).

In order to show that \( \text{core}(H) = K \), we need to show that \( K \) is the largest normal subgroup of \( G \) contained in \( H = H_{u,z_1,b_1 \alpha_v} \). Let \( L \) be a normal subgroup of \( G \) contained in \( H_{u,z_1,b_1 \alpha_v} \). By Lemma 1, \( L = H_{u,v;f;f} \) for some \((w, \gamma, f) \in \mathbb{N} \). Since \( \langle a^\alpha \rangle = L \cap \langle a^\alpha \rangle \subseteq H_{u,z_1,b_1 \alpha_v} \cap \langle a^\alpha \rangle = \langle a^\alpha \rangle \), it follows that \( u \mid w \). Next observe that an arbitrary element of \( H_{u,z_1,b_1 \alpha_v} \) is of the type \( a^j b^k \) with \( \beta_{a^\alpha} \mid s \) and \( j \equiv s \mod{u} \). Therefore, \( L = H_{u,v;f} \) is a subgroup of \( H_{u,z_1,b_1 \alpha_v} \), if, and only if, \( \beta_{a^\alpha} \mid f \) and \( \gamma \equiv \frac{\alpha}{\beta_{a^\alpha}} \mod{u} \). Since \( \gamma(r-1) \equiv 0 \mod{u} \), we have \( \alpha(r-1) \equiv 0 \mod{u} \). This gives that \( \delta \mid f \) and consequently \( L = H_{u,v;f} \) is contained in \( K = \langle a^\alpha, a^{\frac{\beta_u \alpha_v}{\gcd(\alpha(r-1),u)}} b^\delta \rangle \). This proves that \( K \) is the largest normal subgroup of \( G \) contained in \( H_{u,z_1,b_1 \alpha_v} \), which proves the claim.

It is now immediate from the claim that \( H/N \) is core-free in \( G/N \) if, and only if, \( u = v \) and \( \delta = c \). This proves \((ii)\). \( \square \)

**Lemma 3.** Let \((v, i, c) \in \mathbb{N} \) and \((v, \alpha_1, \beta_i) \in X_{v, i, c} \). Then \( H_{v,z_1,b_{j1} \alpha_v} \) and \( H_{v,z_2,b_{j2} \alpha_v} \) are conjugate in \( G \) if, and only if, \( \beta_1 = \beta_2 \) and \( \alpha_1 \equiv \alpha_2 r^j \mod{v} \), for some \( j \).

**Proof.** Suppose

\[
H_{v,z_1,b_{j1} \alpha_v} = g^{-1} H_{v,z_2,b_{j2} \alpha_v} g, \quad g = a^j b^r \in G.
\]

(13)

Then, in particular, in view of Eq. (11), we have

\[
|H_{v,z_1,b_{j1} \alpha_v}| = \frac{n t}{v \beta_i \alpha_v} = \frac{n t}{v \beta_2 \alpha_v} = |H_{v,z_2,b_{j2} \alpha_v}|,
\]

i.e.,

\[
\beta_1 = \beta_2.
\]

Further, Eq. (13) holds if, and only if,

\[
(a^j b^r)^{-1} a^{z_2 \beta_i \alpha_v} a^j b^r \in H_{v,z_1,b_{j1} \alpha_v}.
\]

Since \( ab^\alpha a^{-1} b^{-\alpha} \in \langle a^\alpha \rangle \), we have \((a^j b^r)^{-1} a^{z_2 \beta_i \alpha_v} a^j b^r (a^{z_2 \beta_i \alpha_v})^{-1} \in \langle a^\alpha \rangle \subseteq H_{v,z_1,b_{j1} \alpha_v} \),

which yields that

\[
\alpha_1 \equiv \alpha_2 r^j \mod{v}
\]

and proves the lemma. \( \square \)
Proof of Theorem 4. By Lemma 1, $H_{v,i,c}(v, i, c) \in \mathcal{Y}$, are all the distinct normal subgroups of $G$. For $(v, i, c) \in \mathcal{Y}$, and $N = H_{v,i,c}$, Lemma 2 implies that

$$\mathcal{F}_{G/N} = \{(H_{v,x,\beta}/, G_{\alpha}/N) | (v, x, \beta) \in \mathcal{X}_{v,i,c}\}.$$ 

Therefore, we have

$$\mathcal{F} = \bigcup_{(v, i, c) \in \mathcal{Y}} \{(H_{v,x,\beta}/, H_{v,x,\beta}/N, G_{\alpha}/N) | (v, x, \beta) \in \mathcal{X}_{v,i,c}\},$$

and consequently, Theorem 2 yields the required result. \qed

4. GROUPS WITH CENTRAL QUOTIENT KLEIN FOUR-GROUP

The groups $G$ of the type $G/Z(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, where $Z(G)$ denotes the centre of the group $G$, arose in the work of Goodaire [6] while studying Moufang loops. It is known [7, Chapter 5] that any group with $G/Z(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ is the direct product of an indecomposable group (with this property) and an abelian group; Moreover, the finite indecomposable groups with $G/Z(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ break into five classes as follows:

| Group | Generators | Relations |
|-------|------------|-----------|
| $D_1$ | $x, y, t$  | $x^2, y^2, r^p, y^{-1}x^{-1}yxt^{2m-1}, t$ central, $m \geq 1$ |
| $D_2$ | $x, y, t$  | $x^2r^{-1}, y^2r^{-1}, r^p, y^{-1}x^{-1}yxt^{2m-1}, t$ central, $m \geq 1$ |
| $D_3$ | $x, y, t_1, t_2$ | $x^2, y^2t_1^{-1}, t_1^{-m_1}, t_2^{-m_2}, y^{-1}x^{-1}yxt_1^{2m_1-1}, t_1, t_2$ central, $m_1, m_2 \geq 1$ |
| $D_4$ | $x, y, t_1, t_2$ | $x^2, y^2t_1^{-1}, y^2t_2^{-1}, t_1^{-m_1}, t_2^{-m_2}, t_1^{-1}x^{-1}yxt_1^{2m_1-1}, t_1, t_2$ central, $m_1, m_2 \geq 1$ |
| $D_5$ | $x, y, t_1, t_2, t_3$ | $x^2, y^2t_1^{-1}, y^2t_2^{-1}, t_1^{-m_1}, t_2^{-m_2}, t_3^{-m_3}, t_1^{-1}x^{-1}yxt_1^{2m_1-1}, t_1, t_2, t_3$ central, $m_1, m_2, m_3 \geq 1$ |

It thus becomes important to investigate the group algebra $\mathbb{F}_q[G]$, $G$ of type $D_i$, $1 \leq i \leq 5$. Recently, Ferraz, Goodaire, and Polcino Milies [5] have given a lower bound on the number of simple components of these semisimple finite group algebras. We improve Theorems 3.1 and 3.2 of [5] by providing the complete algebraic structure of $\mathbb{F}_q[G]$, $G$ of type $D_i$, $i = 1, 2$.

4.1. Groups of Type $D_i$

Observe that for $m = 1$, the group $G$ of type $D_1$ is isomorphic to $D_8$, the dihedral group of order 8, and the structure of group algebra $\mathbb{F}_q[D_8]$ can be read from Example 4.3 of [1].

Let $m \geq 2$. Define

$$N_0 := \langle 1 \rangle, \quad N_1 := \langle t, x \rangle, \quad N_2 := \langle t, y \rangle, \quad N_3 := \langle t, xy \rangle, \quad N_4(\alpha) := \langle t^2, x, y \rangle, \quad N_5(\beta) := \langle t^{2m}, x, yt^\beta \rangle, \quad N_6(\beta) := \langle t^{2m}, xt^\beta, y \rangle, \quad N_7(\beta) := \langle t^\beta, x, t^{2\beta} \rangle, \quad 0 \leq x \leq m - 1, \quad 0 \leq \beta \leq m - 2.$$
Let $\lambda$ be the highest power of 2 dividing $q - 1$ (resp. $q + 1$) according as $q \equiv 1$ (mod 4) (resp. $q \equiv -1$ (mod 4)).

Ferraz, Goodaire, and Polcino Milies [5, Theorem 3.1] proved that the Wedderburn decomposition of $F_q[G]$, $G$ of type $D_t$, contains at least $8m - 10$ simple components. If $q \equiv 3$ (mod 8), then this number is achieved with $8m - 12$ fields and 2 quaternion algebras, each necessarily a ring of $2 \times 2$ matrices. The following result improves the result of Ferraz et al. by providing a concrete description of $F_q[G]$, $G$ of type $D_t$.

**Theorem 5.** A complete set of primitive central idempotents, Wedderburn decomposition, and the automorphism group of $F_q[G]$, $G$ of type $D_t$, $m \geq 2$, are given by what follows:

**Primitive central idempotents**

- $e_C(G, N_1, \langle x \rangle)$, $C \in R(N_1/\langle x \rangle)$;
- $e_C(G, G, N_i)$, $C \in R(G/N_i)$, $1 \leq i \leq 3$;
- $e_C[G, G, N_4^{(x)}]$, $C \in R(G/N_4^{(x)})$, $0 \leq x \leq m - 1$;
- $e_C(G, G, N_j^{(y)})$, $C \in R(G/N_j^{(y)})$, $0 \leq y \leq m - 2$, $5 \leq j \leq 7$.

**Wedderburn decomposition**

$q \equiv 1$ (mod 4)

$$\begin{align*}
F_q[G] \cong \begin{cases}
F_q^{(2m+1)} \bigoplus M_2(F_q)^{(2m-1)}, & m \leq \lambda, \\
F_q^{(2m+1)} \bigoplus M_2(F_q)^{(2m-3)}, & m = \lambda + 1, \\
F_q^{(2m+2)} \bigoplus F_{q^{2m-1}}^{(2m+1)} \bigoplus M_2(F_{q^{2m-1}})^{(2m-1)}, & m \geq \lambda + 2.
\end{cases}
\end{align*}$$

$q \equiv -1$ (mod 4)

$$\begin{align*}
F_q[G] \cong \begin{cases}
F_q^{(8)} \bigoplus F_{q^{2m-4}}^{(2m-4)} \bigoplus M_2(F_{q^{2m-4}})^{(2m-2)}, & 2 \leq m \leq \lambda + 1, \\
F_q^{(8)} \bigoplus F_{q^{2m-4}}^{(2m-4)} \bigoplus M_2(F_{q^{2m-4}})^{(2m-2)}, & m = \lambda + 2, \\
F_q^{(8)} \bigoplus F_{q^{2m-4}}^{(2m-4)} \bigoplus F_{q^{2m-4}}^{(2m-2)} \bigoplus M_2(F_{q^{2m-4}})^{(2m-1)}, & m \geq \lambda + 3.
\end{cases}
\end{align*}$$

$q \equiv 1$ (mod 4)

$$\begin{align*}
\text{Aut}(F_q[G]) & \cong \begin{cases}
S_{2m+1} \bigoplus (\text{SL}_2(F_q)^{(2m-1)} \rtimes S_{2m-1}), & m \leq \lambda, \\
S_{2m+1} \bigoplus (\text{SL}_2(F_q^{2m-2}) \rtimes S_{2m-2}) & m = \lambda + 1, \\
S_{2m+2} \bigoplus (Z_{2m-3}^{(2m-1)} \rtimes S_{2m+1}) \bigoplus \mathcal{H} & m \geq \lambda + 2.
\end{cases}
\end{align*}$$
\[ q \equiv -1 \pmod{4} \]

\[
\text{Aut}(\mathbb{F}_q[G]) \cong \begin{cases} 
S_8 \bigoplus (\mathbb{Z}_2^{(2^{m-4})} \rtimes S_{2^{m-4}}) \bigoplus ((\text{SL}_2(\mathbb{F}_q) \rtimes \mathbb{Z}_2^{(2^{m-2})}) \rtimes S_{2^{m-1}}), & m \leq \lambda + 1, \\
S_8 \bigoplus (\mathbb{Z}_2^{(2^{m-4})} \rtimes S_{2^{m-4}}) \bigoplus ((\text{SL}_2(\mathbb{F}_q) \rtimes \mathbb{Z}_2^{(2^{m-3})} \rtimes S_{2^{m-1}}), & m = \lambda + 2, \\
S_8 \bigoplus (\mathbb{Z}_2^{(2^{m+2-4})} \rtimes S_{2^{m+2-4}}) \bigoplus (\mathbb{Z}_2^{(2^{m+2})} \rtimes S_{2^{m+1}}) \bigoplus \mathcal{H}, & m \geq \lambda + 3,
\end{cases}
\]

where \( \mathcal{H} = (\text{SL}_2(\mathbb{F}_{q^{2^{-m}}}) \rtimes \mathbb{Z}_{2^{m-j}}(2^{-1}) \rtimes S_{2}^{2^{-1}}. \)

In order to prove the above theorem, we first need to compute all the normal subgroups of \( G \), \( G \) of type \( D_1 \).

**Lemma 4.** All the distinct non-identity normal subgroups of \( G \) are given by what follows:

\( (i) \) \( \langle t^v x \rangle, \langle t^v y \rangle, \langle t^v x, x, y \rangle; \)

\( (ii) \) \( \langle t^v x \rangle, \langle t^\beta y \rangle, \langle t^v x, t^\beta y, t^{v-1}, x, t^\beta y \rangle; \)

\( (iii) \) \( \langle t^v \rangle. \)

Here \( 0 \leq \alpha \leq m - 1, 0 \leq \beta \leq m - 2 \) and \( 0 \leq \gamma \leq m - 1. \)

**Proof.** Observe that all the subgroups listed in the statement are distinct and normal in \( G \).

Let \( N \) be a normal subgroup of \( G \) not contained in \( \langle t \rangle \). If \( N \neq \langle 1 \rangle \), then it is easy to see that \( \langle t^{m-1} \rangle \leq N \). Therefore, \( N \cap \langle t \rangle = \langle t^v \rangle, 0 \leq v \leq m - 1. \)

Since \( N/N \cap \langle t \rangle \) is isomorphic to a subgroup of \( G/\langle t \rangle \), which is generated by \( x(t), y(t), \) it follows that \( N/N \cap \langle t \rangle \) is isomorphic to one of the following subgroups: \( \langle x(t) \rangle, \langle y(t) \rangle, \langle xy(t) \rangle, \) or \( \langle x(t), y(t) \rangle. \)

**Case I:** \( N/\langle t^2 \rangle \cong \langle x(t) \rangle. \)

In this case, \( N = \langle t^v, t^i x \rangle \), for some \( i, 0 \leq i \leq v \leq m - 1. \)

If \( i = v \), then \( N = \langle t^v, x \rangle. \) Since \( N \leq G, xt^{m-1} = y^{-1}xy \in N \), implies that \( t^{m-1} \in N \cap \langle t \rangle = \langle t^v \rangle \), which is possible only if \( v \leq m - 1. \)

If \( i < v \), then \( N = \langle t^v, t^i x \rangle = \langle t^i x \rangle \) as \( t^i \in \langle t^v \rangle \). Further, \( xt^{2v+2m-1} = y^{-1}t^2xy \in N \) implies that \( t^{m-1} \in \langle t^v \rangle \). Hence \( v \leq m - 1 \) and \( i \leq m - 2. \)

Thus, in this case, either

\[ N = \langle t^v, x \rangle, \quad 0 \leq i \leq m - 1, \quad (14) \]

or

\[ N = \langle t^i x \rangle, \quad 0 \leq i \leq m - 2. \quad (15) \]

**Case II:** \( N/\langle t^2 \rangle \cong \langle y(t) \rangle. \)

Computation analogous to those in Case I yield that

\[ N = \langle t^i y \rangle, \quad 0 \leq i \leq m - 2. \quad (16) \]
or

\[ N = \langle t^v, y \rangle, \quad 0 \leq i \leq m - 1. \]  \hspace{1cm} (17)

**Case III:** \( N/\langle t^v \rangle \cong \langle xy(t) \rangle \).

In this case, \( N = \langle t^v, t^2 xy \rangle \) for \( 0 \leq i \leq m - 1 \).

If \( i = v \), then \( N = \langle t^v, xy \rangle \). Since \( N \) is a normal subgroup of \( G \), \( xyt^{m-1} = y^{-1}xyy \in N \), implies that \( t^{2m-1} \in N \cap \langle t \rangle = \langle t^v \rangle \), which is possible only if \( v \leq m - 1 \).

If \( i < v \), then \( N = \langle t^v, t^i xy \rangle \), \( 0 \leq i \leq m - 2 \). Since \( \langle t^{2m-1}, t^2 xy \rangle \leq \langle t^v, t^i xy \rangle \) and

\[
 t^v = \begin{cases} 
 (t^v xy)^{2v-i} t^{2m-1}, & \text{if } v - i = 1, \\
 (t^v xy)^{2v-i}, & \text{if } v - i \geq 2,
\end{cases}
\]

it follows that \( \langle t^v, t^i xy \rangle = \langle t^{2m-1}, t^2 xy \rangle \).

Thus, in this case, either

\[ N = \langle t^v, xy \rangle, \quad 0 \leq i \leq m - 1 \]  \hspace{1cm} (18)

or

\[ N = \langle t^{2m-1}, t^i xy \rangle, \quad 0 \leq i \leq m - 2. \]  \hspace{1cm} (19)

**Case IV:** \( N/\langle t^v \rangle \cong \langle x(t), (y(t)) \rangle \).

In this case, \( N \) is one of the following forms:

(a) \( \langle t^{2v}, x, y \rangle \);

(b) \( \langle t^{2v}, t^v x, y \rangle \) for some \( i, 0 \leq i \leq v - 1 \);

(c) \( \langle t^{2v}, x, t^v y \rangle \) for some \( i, 0 \leq i \leq v - 1 \);

(d) \( \langle t^{2v}, t^v x, t^v y \rangle \) for some \( i, 0 \leq i \leq v - 1 \);

(e) \( \langle t^{2v}, t^v x, t^j y \rangle \) for some \( 1 \leq i, j \leq v - 1, i \neq j \).

Observe that, for \( 0 \leq i \leq v - 1 \),

\[
 \langle t^{2v}, t^v x, y \rangle = \langle t^{2m-1}, t^v x, y \rangle,
\]

\[
 \langle t^{2v}, x, t^v y \rangle = \langle t^{2m-1}, x, t^v y \rangle,
\]

and

\[
 \langle t^{2v}, t^v x, t^v y \rangle = \langle t^{2m-1}, t^v x, t^v y \rangle.
\]

Also, for \( 1 \leq i, j \leq v - 1, i \neq j \),

\[
 \langle t^{2v}, t^v x, t^j y \rangle = \begin{cases} 
 \langle t^v x, y \rangle, & \text{if } i < j, \\
 \langle x, t^j y \rangle, & \text{if } j < i.
\end{cases}
\]
Proof of Theorem 5. In order to apply Theorem 2 to a group $G$ of type $D_4$, we need to compute $\mathcal{F}_{G/N}$ for all normal subgroups $N$ of $G$ given by Lemma 4.

Clearly, if $N = \langle 1 \rangle$, $\mathcal{F}_{G/N} = \{ \langle x \rangle, \langle t, x \rangle \}$.

Suppose $N$ is a non-identity normal subgroup of $G$. Then $N$ is one of the subgroups listed in Lemma 4. Since $G' = \langle t^{2m-1} \rangle \leq N$, we have $\mathfrak{A}_N / N = G / N$ and

$$S_{G/N} = \begin{cases} \{ \langle 1 \rangle, G/N \}, & \text{if } G/N \text{ is cyclic,} \\ \emptyset, & \text{otherwise.} \end{cases}$$

Next we see that among all the normal subgroups $N$ of $G$ stated in Lemma 4, only the following subgroups $N$ satisfy the condition that $G/N$ is cyclic:

$$N_i, \ N_i^{(\alpha)}, \ N_j^{(\beta)}, \ 1 \leq i \leq 3, \ 0 \leq \alpha \leq m - 1, \ 5 \leq j \leq 7, \ 0 \leq \beta \leq m - 2.$$ 

Therefore, $\mathcal{F} = \{ (N_0, \langle x \rangle, N_i) \} \cup \{ (N_i, \langle 1 \rangle, G/N) | 1 \leq i \leq 3 \} \cup \{ (N_i^{(\alpha)}, \langle 1 \rangle, G/N_i^{(\alpha)} | 0 \leq \alpha \leq m - 1 \} \cup \{ (N_j^{(\beta)}, \langle 1 \rangle, G/N_j^{(\beta)}) | 0 \leq \beta \leq m - 2 \}$, and thus (i) follows.

In order to prove (ii) and (iii), we first note that for any integer $\gamma \geq 2$,

$$\text{ord}_2(q) = \begin{cases} 2^{-i}, & \gamma \geq \lambda + 1, \ q \equiv 1 \text{ or } -1 \text{ (mod 4)}, \\ 1, & \gamma \leq \lambda, \ q \equiv 1 \text{ (mod 4)}, \\ 2, & \gamma \leq \lambda, \ q \equiv -1 \text{ (mod 4)}. \end{cases}$$

Direct calculations yield that for each $(N, D/N, A_N/N) \in \mathcal{F}$, the corresponding $o(\mathfrak{A}_N, D)$ and $|R(\mathfrak{A}_N/D)|$ are as given by the following tables:

**Case I:** $q \equiv 1 \text{ (mod 4)}$.
Case II: \( q \equiv -1 \pmod{4} \).

\[
\begin{array}{ccc}
(N, D/N, \mathbb{A}_N/N) & o(\mathbb{A}_N, D) & |R(\mathbb{A}_N/D)| \\
(N_i, (1), G/N), & 1 & 1 \\
1 \leq i \leq 3 & & \\
(N_i^{(a)}, (1), G/N_i^{(a)}), & 1 & 1 \\
0 \leq x \leq 1 & & \\
(N_i^{(a)}, (1), G/N_i^{(a)}), & 2^{x-j}, \quad x \geq \lambda + 2, & 2^{x-1}, \quad x \gtrless \lambda + 2, \\
2 \leq x \leq m-1 & 2, \quad x \leq \lambda + 1 & 2^{x-2}, \quad x \leq \lambda + 1 \\
(N_i^{(b)}, (1), G/N_i^{(b)}), & 1 & 1 \\
5 \leq j \leq 7, & & \\
(N_0, (x), N_1) & 2^{\beta+1-j}, \quad \beta \geq \lambda + 1, & 2^{x-1}, \quad \beta \geq \lambda + 1, \\
5 \leq j \leq 7, 1 \leq \beta \leq m-2 & 2, \quad \beta \leq \lambda & 2^{\beta-1}, \quad \beta \leq \lambda \\
2^{\lambda-1}, \quad m \geq \lambda + 2, & 2^{\lambda-2}, \quad m \geq \lambda + 2, \\
2, \quad m \leq \lambda & 2^{\lambda-2}, \quad m \leq \lambda + 1 &
\end{array}
\]

Thus, Theorem 3 together with the above two tables yields (ii) and (iii).

4.2. Groups of Type \( D_2 \)

Observe that for \( m = 1 \), the group \( G \) of type \( D_2 \) is isomorphic to \( Q_8 \), the quaternion group of order 8 and the structure of group algebra \( \mathbb{F}_q[G] \) can be read from Example 4.4 of [1].

Let \( m \geq 2 \). Define

\[
K_0 := (1), \quad K_1 := \langle x \rangle; \quad K_2^{(a)} := \langle x^\alpha, x^{2\alpha-1} \rangle, \quad K_3^{(a)} := \langle y^\beta, x^{2\beta-1} \rangle, \quad 0 \leq x \leq m, \quad 1 \leq \beta \leq m.
\]

Let \( \lambda \) be the highest power of 2 dividing \( q-1 \) (resp. \( q+1 \)) according as \( q \equiv 1 \) (mod 4) (resp. \( q \equiv -1 \) (mod 4)).

Ferraz, Goodeaire, and Polcino Milies proved [5, Theorem 3.2] that the Wedderburn decomposition of \( \mathbb{F}_q[G] \), \( G \) of type \( D_2 \), contains at least \( 4m \) simple components. If \( q \equiv 3 \) (mod 8), then this number is achieved with \( 4m-2 \) fields and 2 quaternion algebras, each necessarily a ring of \( 2 \times 2 \) matrices. The following theorem improves this result of Ferraz et al.

**Theorem 6.** A complete set of primitive central idempotents, Wedderburn decomposition and the automorphism group of \( \mathbb{F}_q[G] \), \( G \) of type \( D_2 \), \( m \geq 2 \), are given by what follows:
Primitive central idempotents

\[ e_c(G, K_1, K_0), \quad e_c(G, G, K_1), \quad e_c(G, G, K_2^{(2)}), \quad e_c(G, G, K_3^{(1)}), \quad e_c(G, G, K_3^{(β)}), \]

where

\[ q \equiv 1 \pmod{4} \]

\[ \mathbb{F}_q[G] \cong \begin{cases} \mathbb{F}_q^{(2^{n+1})} \bigoplus m M_2(\mathbb{F}_q)^{(2^{n-1})}, & m \leq \hat{\lambda}, \\ \mathbb{F}_q^{(2^{i+1})} \bigoplus \mathbb{F}_{q^{2i-2}}^{2(\hat{\lambda}+1)} \bigoplus M_2(\mathbb{F}_{q^{2i-2}})^{(2^{i-1})}, & m \geq \hat{\lambda} + 1. \end{cases} \]

\[ q \equiv -1 \pmod{4} \]

\[ \mathbb{F}_q[G] \cong \begin{cases} \mathbb{F}_q^{(4)} \bigoplus \mathbb{F}_{q^2}^{(2^{n-2})} \bigoplus M_2(\mathbb{F}_{q^2})^{(2^{n-1})}, & 2 \leq m \leq \hat{\lambda} + 1, \\ \mathbb{F}_q^{(4)} \bigoplus \mathbb{F}_{q^2}^{(2^{i+1}-2)} \bigoplus \mathbb{F}_{q^{2i-2}}^{2(\hat{\lambda}+1)} \bigoplus M_2(\mathbb{F}_{q^{2i-2}})^{(2^{i-1})}, & m \geq \hat{\lambda} + 2. \end{cases} \]

Automorphism group

\[ \text{Aut}(\mathbb{F}_q[G]) \cong \begin{cases} S_{2^{n+1}} \bigoplus (\text{SL}_2(\mathbb{F}_q)^{(2^{n-1})} \rtimes S_{2^{n-1}}), & m \leq \hat{\lambda}, \\ S_{2^{i+1}} \bigoplus \bigoplus_{z=\hat{\lambda}+1} (\mathbb{Z}_{2^{2z-2}} \rtimes S_{2^{z-1}}) \bigoplus \mathcal{H}_z, & m \geq \hat{\lambda} + 1, \end{cases} \]

\[ q \equiv 1 \pmod{4} \]

\[ \text{Aut}(\mathbb{F}_q[G]) \cong \begin{cases} S_{4} \bigoplus (\mathbb{Z}_2^{(2^{n+1})} \rtimes S_{2^{n+1}}) \bigoplus ((\text{SL}_2(\mathbb{F}_q) \rtimes \mathbb{Z}_2)^{(2^{n-1})} \rtimes S_{2^{n-1}}), & m \leq \hat{\lambda} + 1, \\ S_{4} \bigoplus (\mathbb{Z}_2^{(2^{i+1}-2)} \rtimes S_{2^{i+1-2}}) \bigoplus \bigoplus_{z=\hat{\lambda}+2} (\mathbb{Z}_{2^{2z-2}} \rtimes S_{2}) \bigoplus \mathcal{H}_z, & m \geq \hat{\lambda} + 2, \end{cases} \]

where \( \mathcal{H}_z = (\text{SL}_2(\mathbb{F}_{q^{2z-2}}) \rtimes \mathbb{Z}_{2^{2z-2}})^{(2^{i-1})} \rtimes S_{2^{i-1}}. \)

Proof. We have

\[ G = \langle x, y \mid x^{2^{n+1}} = 1, y^2 = x^2, y^{-1}xy = x^{2^a+1} \rangle. \]

By Lemma 1, the non-identity normal subgroups of \( G \) are given as follows:

(i) \( \langle x^a \rangle, \langle x^a, x^{2^a-1}y \rangle, 0 \leq a \leq m; \)

(ii) \( \langle x^\beta \rangle, \langle x^\beta, x^{2^\beta-1}y \rangle, 1 \leq \beta \leq m. \)
Also, Lemmas 2 and 3 yield that \( \mathcal{S} = \{(K_0, \langle 1 \rangle, K_1) \cup \{(K_1, \langle 1 \rangle, G/K_1) \cup \{(K_1^{(i)}, \langle 1 \rangle, G/K_1^{(i)}) | 0 \leq \alpha \leq m \} \cup \{(K_3^{(i)}, \langle 1 \rangle, G/K_3^{(i)}) | 1 \leq \beta \leq m \} \}. Therefore, (i) follows from Theorem 4.

For each \( (N, D/N, A_N/N) \in \mathcal{S} \), the corresponding \( o(\partial_N, D) \) and \( |R(\partial_N/D)| \) in the cases \( q \equiv 1 \) (mod 4) or \( q \equiv -1 \) (mod 4) are as follows.

**Case I:** \( q \equiv 1 \) (mod 4).

| \((N, D/N, A_N/N)\) | \(o(\partial_N, D)\) | \(|R(\partial_N/D)|\) |
|----------------|-----------------|-----------------|
| \((K_1, \langle 1 \rangle, G/K_1)\) | 1 | 1 |
| \((K_1^{(i)}, \langle 1 \rangle, G/K_1^{(i)})\) | 1 | 1 |
| \((K_2^{(i)}, \langle 1 \rangle, G/K_2^{(i)})\) | \(2^{x-1}, x \geq \lambda + 1, \) | \(2^{x-1}, x \geq \lambda + 1, \) |
| \(1 \leq x \leq m\) | \(1, x \leq \lambda\) | \(2^{x-1}, x \leq \lambda\) |
| \((K_3^{(i)}, \langle 1 \rangle, G/K_3^{(i)})\) | \(2^{\beta-1}, \beta \geq \lambda + 1, \) | \(2^{\beta-1}, \beta \geq \lambda + 1, \) |
| \(1 \leq \beta \leq m\) | \(1, \beta \leq \lambda\) | \(2^{\beta-1}, \beta \leq \lambda\) |
| \((K_0, \langle 1 \rangle, K_1)\) | \(2^{m-1}, m \geq \lambda + 1, \) | \(2^{m-1}, m \geq \lambda + 1, \) |
| \(1, m \leq \lambda\) | \(2^{m-1}, m \leq \lambda\) |

**Case II:** \( q \equiv -1 \) (mod 4).

| \((N, D/N, A_N/N)\) | \(o(\partial_N, D)\) | \(|R(\partial_N/D)|\) |
|----------------|-----------------|-----------------|
| \((K_1, \langle 1 \rangle, G/K_1)\) | 1 | 1 |
| \((K_1^{(i)}, \langle 1 \rangle, G/K_1^{(i)})\) | 1 | 1 |
| \((K_2^{(i)}, \langle 1 \rangle, G/K_2^{(i)})\) | \(2^{x-1}, x \geq \lambda + 2, \) | \(2^{x-1}, x \geq \lambda + 2, \) |
| \(0 \leq x \leq 1\) | \(2, x \leq \lambda + 1\) | \(2^{x-1}, x \leq \lambda + 1\) |
| \((K_3^{(i)}, \langle 1 \rangle, G/K_3^{(i)})\) | 1 | 1 |
| \((K_3^{(j)}, \langle 1 \rangle, G/K_3^{(j)})\) | \(2^{\beta-1}, \beta \geq \lambda + 2, \) | \(2^{\beta-1}, \beta \geq \lambda + 2, \) |
| \(2 \leq \beta \leq m\) | \(2, \beta \leq \lambda + 1\) | \(2^{\beta-1}, \beta \leq \lambda + 1\) |
| \((K_0, \langle 1 \rangle, K_1)\) | \(2^{m-1}, m \geq \lambda + 2, \) | \(2^{m-1}, m \geq \lambda + 2, \) |
| \(2, m \leq \lambda + 1\) | \(2^{m-2}, m \leq \lambda + 1\) |

Thus Theorem 3, together with the above two tables yields (iii) and (iii).

**Remark.** The above analysis of the structure of \( \mathbb{F}_q[G] \), \( G \) of type \( D_1, D_2 \), provides a method for computing the algebraic structure of \( \mathbb{F}_q[G] \), for finite group \( G \) whose central quotient is Klein four-group. It will thus naturally be of interest to compute the algebraic structure of \( \mathbb{F}_q[G] \), \( G \) of type \( D_i, i = 3, 4, 5 \).
REFERENCES

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

[2] Bakshi, G. K., Kulkarni, R. S., Passi, I. B. S. (2013). The rational group algebra of a finite group. *J. Algebra Appl.* 12(3):1250168.

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

[4] Curtis, C. W., Reiner, I. (2006). *Representation Theory of Finite Groups and Associative Algebras*. Providence, RI: AMS Chelsea Publishing.

[5] Ferraz, R. A., Goodaire, E. G., Milies, C. P. (2010). Some classes of semisimple group (and loop) algebras over finite fields. *J. Algebra* 324(12):3457–3469.

[6] Goodaire, E. G. (1983). Alternative loop rings. *Publ. Math. Debrecen* 30(1–2):31–38.

[7] Goodaire, E. G., Jespers, E., Milies, C. P. (1996). *Alternative Loop Rings*. North-Holland Mathematics Studies, Vol. 184. Amsterdam: North-Holland Publishing Co.

[8] Olivieri, A., del Río, Á., Simón, J. J. (2006). The group of automorphisms of the rational group algebra of a finite metacyclic group. *Comm. Algebra* 34(10):3543–3567.

[9] Olivieri, A., del Río, Á., Simón, J. J. (2004). On monomial characters and central idempotents of rational group algebras. *Comm. Algebra* 32(4):1531–1550.