STRUCTURE OF FINITE DIHEDRAL GROUP ALGEBRA

F. E. BROCHERO MARTÍNEZ

Abstract. In this article, we show the relation between the irreducible idempotents of the cyclic group algebra \( F_q C_n \) and the central irreducible idempotents of the group algebras \( F_q D_{2n} \), where \( F_q \) is a finite field with \( q \) elements and \( D_{2n} \) is the dihedral group of order \( 2n \), where \( \gcd(q, n) = 1 \).

In addition, if every divisor of \( n \) divides \( q - 1 \), we show explicitly all central irreducible idempotents of this group algebra and its Wedderburn decomposition.

1. Introduction

Let \( K \) be a field and \( G \) be a group with \( n \) elements. It is known that, if \( \text{char}(K) \nmid n \), then the group algebra \( KG \) is semisimple and as consequence of Wedderburn Theorem, we have that \( KG \) is isomorphic to a direct sum of matrix algebras over division rings, such that each division algebra is a finite algebra over the field \( K \), i.e, there exists an isomorphism

\[
\rho : KG \rightarrow M_{l_1}(D_1) \oplus M_{l_2}(D_2) \oplus \cdots \oplus M_{l_t}(D_t),
\]

where \( D_j \) are division rings such that \( |G| = \sum_{j=1}^{t} l_j^2[D_j : K] \). Observe that \( KG \) has \( t \) central irreducible idempotents, each one of the form

\[
e_i = \rho^{-1}(0 \oplus \cdots \oplus 0 \oplus I_i \oplus 0 \cdots \oplus 0),
\]

where \( I_i \) is the identity matrix of the component \( M_{l_i}(D_i) \). Then, the isomorphism \( \rho \) determines explicitly each central irreducible idempotent.

In the case \( K = \mathbb{Q} \), the calculus of central idempotents and Wedderburn decomposition is widely studied; the classical method to calculate the primitive central idempotents of group algebras depends on computing the character group table. Other method is shown in [8], where Jespers, Leal and Paques describe the central irreducible idempotents when \( G \) is a nilpotent group, using the structure of its subgroups, without employing the characters of the group. Generalizations and improvements of this method can be found in [11], where the authors provide information about the Wedderburn decomposition of \( \mathbb{Q}G \). This computational method is also used in [2] to compute the Wedderburn decomposition and the primitive central idempotents of a semisimple finite group algebra \( KG \), where \( G \) is an abelian-by-supersolvable group \( G \) and \( K \) is a finite field.

The structure of \( KG \) when \( G = D_{2n} \) is the dihedral group with \( 2n \) elements is well known for \( K = \mathbb{Q} \) (see [7]). In [5], Dutra, Ferraz and Polcino Milies impose conditions over \( q \) and \( n \) in order for \( \mathbb{F}_q D_{2n} \) to have the same number of irreducible components that \( \mathbb{Q} D_{2n} \). This result is generalized in [6], where Ferraz Goodaire...
and Polcino Milies find, for some families of groups, conditions under \( q \) and \( G \) in order for \( \mathbb{F}_qG \) to have the minimum number of simple components.

In this article, assuming that every prime factor of \( n \) divides \( q - 1 \), we show explicitly the central irreducible idempotents of \( \mathbb{F}_qD_{2n} \) and an isomorphism between the group algebra \( \mathbb{F}_qD_{2n} \) and its Wedderburn decomposition. Observe that this isomorphism also shows the structure of \( U(\mathbb{F}_qD_{2n}) \), the unit group of \( \mathbb{F}_qD_{2n} \).

2. Idempotents of Cyclic Group Algebra

Throughout this article, \( \mathbb{F}_q \) denotes a finite field of order \( q \), where \( q \) is a power of a prime and \( n \) is a positive integer such that \( \gcd(n, q) = 1 \). For every polynomial \( g(x) \) with \( g(0) \neq 0 \), \( g^* \) denotes the reciprocal polynomial of \( g \), i.e., \( g^*(x) = x^\deg(g/g(1/x)) \). The polynomial \( x^n - 1 \in \mathbb{F}_q[x] \) splits in monic irreducible factors as

\[
x^n - 1 = f_1 f_2 \cdots f_r f_{r+1} f_{r+1} f_{r+2} f_{r+2} f_{r+3} \cdots f_{r+s} f_{r+s},
\]

where \( f_1 = x - 1 \), \( f_2 = x + 1 \) if \( n \) is even, and \( f^*_j = f_j \) for \( 2 \leq j \leq r \), where \( r \) is the number of auto-reciprocal factors in the factorization and \( 2s \) the number of non-auto-reciprocal factors.

We denote by \( C_n \) the cyclic group of order \( n \). It is well known that \( \mathbb{F}_q C_n \cong \mathcal{R}_n = \frac{\mathbb{F}_q[x]}{(x^n - 1)} \), and by the Chinese Remainder Theorem

\[
\frac{\mathbb{F}_q[x]}{(x^n - 1)} \cong \bigoplus_{j=1}^{r+s} \frac{\mathbb{F}_q[x]}{(f_j)} \oplus \bigoplus_{j=r+1}^{r+s} \frac{\mathbb{F}_q[x]}{(f_j)}
\]

is exactly the Wedderburn decomposition of the group algebra \( \mathcal{R}_n \), so every primitive idempotent generates a maximal ideal of \( \mathcal{R}_n \) and also one component of this direct sum.

In addition, since \( \mathcal{R}_n \) is a principal ideal domain, every ideal of \( \mathcal{R}_n \) is generated by a polynomial \( g \) that is a divisor of \( x^n - 1 \). The relation between the generator of the ideal and its principal idempotent is shown in the following lemma.

Lemma 2.1. Let \( \mathcal{I} \subset \mathcal{R}_n \) be an ideal generated by the monic polynomial \( g \), that is divisor of \( x^n - 1 \), and define \( f = \frac{x^n - 1}{g} \). Then the principal idempotent of \( \mathcal{I} \) is

\[
e_f = -\left(\frac{(f^*)^*}{n}\right) \frac{x^n - 1}{f}.
\]

Proof: Let \( t \) be an integer such that \( n \) divides \( q^t - 1 \). By Theorem 2.1 in [1] (see also Theorem 3.4 in [3]), every primitive idempotent of \( \frac{\mathbb{F}_q[x]}{(x^n - 1)} \) is given by

\[
u_\lambda = \frac{\lambda}{n} \frac{x^n - 1}{x - \lambda} = \frac{1}{n} \sum_{i=0}^{n-1} \lambda^{-i} x^i
\]

where \( \lambda^n = 1 \).

Since \( f \) divides \( x^n - 1 \), then \( f \) splits in \( \mathbb{F}_q[x] \) as \( (x - \lambda_1) \cdots (x - \lambda_k) \) and

\[
(f^*)^t = \sum_{i=1}^{k} (-\lambda_i) \prod_{i \neq j}(1 - \lambda_j x) = f^* \sum_{i=1}^{k} -\lambda_i \frac{x^n - 1}{x - \lambda_j x},
\]

hence

\[
e_f = -\left(\frac{(f^*)^*}{n}\right) \frac{x^n - 1}{f} = \sum_{i=1}^{k} \frac{\lambda_i}{n} \frac{x^n - 1}{x - \lambda} = \sum_{i=1}^{k} \nu_{\lambda_i}.
\]
Therefore $e_f$ is an idempotent of $\mathbb{F}_q[x]$. In order to prove that $e_f$ is the principal idempotent of $I$, it is enough to show that $g \cdot e_f = g$. Observe that, using partial fraction decomposition we obtain

$$g = \frac{x^n - 1}{f} = \sum_{i=1}^{k} A_i u_{\lambda_i},$$

where $A_i = \frac{1}{\prod_{j \neq i} (\lambda_i - \lambda_j)}$ and then

$$g \cdot e_f = \sum_{i=1}^{k} A_i u_{\lambda_i} \cdot \sum_{j=1}^{k} u_{\lambda_j} = \sum_{1 \leq i, j \leq k} A_i u_{\lambda_i} u_{\lambda_j} = \sum_{i=1}^{k} A_i u_{\lambda_i} = g$$

as we wanted to prove. □

Remark 2.2. This lemma is also true for fields with characteristic zero, it suffices to change in the proof the field $\mathbb{F}_q[t]$ by the splitting field of the polynomial $f$.

Corollary 2.3. The cyclic group ring $R_n$ has $r + 2s$ irreducible idempotents of the form $e_f$ given by Lemma 2.1, where the polynomials $f$’s are the irreducible factors of $x^n - 1 \in \mathbb{F}_q[x]$.

3. Central idempotents of Dihedral Group Algebra

Throughout this section, $\alpha_j$ denotes a root of the polynomial $f_j$ and $D_{2n}$ denotes the dihedral group of order $2n$, i.e.

$$D_{2n} = \langle x, y | x^n = 1, y^2 = 1, xy = yx^{-1} \rangle.$$

We define integer numbers $\epsilon$ and $\delta$ as

$$\epsilon = \begin{cases} 0 & \text{if } \text{char}(q) = 2 \\ 1 & \text{if } \text{char}(q) \neq 2 \text{ and } n \text{ is odd} \\ 2 & \text{if } \text{char}(q) \neq 2 \text{ and } n \text{ is even} \end{cases}$$

and $\delta = \max\{\epsilon, 1\}$.

The following theorem shows explicitly the dependence of the Wedderburn decomposition of the Dihedral group algebra over a finite field $\mathbb{F}_q$ with the factorization of $x^n - 1 \in \mathbb{F}_q[x]$.

Theorem 3.1. The group algebra $\mathbb{F}_q D_{2n}$ has Wedderburn decomposition of the form

$$\mathbb{F}_q D_{2n} \cong \bigoplus_{j=1}^{r+s} A_j$$

where

$$A_j = \begin{cases} \mathbb{F}_q \oplus \mathbb{F}_q & \text{if } j \leq \delta, \\ M_2(\mathbb{F}_q[\alpha_j + \alpha_j^{-1}]) & \text{if } \delta + 1 \leq j \leq r, \\ M_2(\mathbb{F}_q[\alpha_j]) & \text{if } r + 1 \leq j \leq r + s, \end{cases}$$

Proof: For each $j \in \{1, \ldots, s + r\}$, let $\tau_j$ be the homomorphism of $\mathbb{F}_q$-algebras defined by the generators of the group $D_{2n}$ as

$$\tau_j : \mathbb{F}_q D_{2n} \rightarrow \mathbb{F}_q \oplus \mathbb{F}_q$$

$$x \mapsto (1, 1)$$

$$y \mapsto (1, -1),$$

and then $g \cdot e_f = g$.
in the case $\epsilon \geq 1$ and
\[
\tau_2 : \mathbb{F}_q D_{2n} \to \mathbb{F}_q \oplus \mathbb{F}_q \\
x \mapsto (-1, -1) \\
y \mapsto (1, -1),
\]
in the case $\epsilon = 2$, where the sum and product in $\mathbb{F}_q \oplus \mathbb{F}_q$ is defined by adding and multiplying the corresponding components of the same coordinates. Finally, for every $j \geq \epsilon + 1$
\[
\tau_j : \mathbb{F}_q D_{2n} \to M_2(\mathbb{F}_q[\alpha_j]) \\
x \mapsto \begin{pmatrix} \alpha_j & 0 \\ 0 & \alpha_j^{-1} \end{pmatrix} \\
y \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.
\]
It is easy to prove that $(\tau_j(x))^n = I$, $(\tau_j(y))^2 = I$ and $\tau_j(x)\tau_j(y) = \tau_j(y)\tau_j(x)^{-1}$.

Observe that in the case of characteristic 2, i.e. $\epsilon = 0$, we have that
\[
\text{dim}_{\mathbb{F}_q}(\text{img}(\tau_j)) = 2 \quad \text{in all cases.}
\]
In addition, if $n$ is even, then dim$_{\mathbb{F}_q}(\text{img}(\tau_2)) = 2$.

For each $\delta < j \leq r$, if we define $Z_j = \begin{pmatrix} 1 & -\alpha_j \\ 1 & -\alpha_j^{-1} \end{pmatrix}$, then
\[
\sigma_j : M_2(\mathbb{F}_q[\alpha_j]) \to M_2(\mathbb{F}_q[\alpha_j]) \\
X \mapsto Z_j^{-1}XZ_j
\]
is an automorphism such that
\[
\sigma_j \circ \tau_j(x) = \begin{pmatrix} 0 & 1 \\ -1 & \alpha_j + \alpha_j^{-1} \end{pmatrix} \quad \text{and} \quad \sigma_j \circ \tau_j(y) = \begin{pmatrix} 1 & -(\alpha_j + \alpha_j^{-1}) \\ 0 & -1 \end{pmatrix},
\]
so the images of the generators of $D_n$ are in $\mathbb{F}_q(\alpha_j + \alpha_j^{-1})$. It follows that for each $j$ such that $\delta < j \leq r$ we have
\[
\text{dim}_{\mathbb{F}_q}(\text{img}(\tau_j)) = \text{dim}_{\mathbb{F}_q}(\text{img}(\sigma_j \circ \tau_j)) \leq 4 \text{dim}_{\mathbb{F}_q}(\mathbb{F}_q(\alpha_j + \alpha_j^{-1})) = 2 \deg(f_j)
\]
and in the case $r + 1 \leq j \leq r + s$, we know that
\[
\text{dim}_{\mathbb{F}_q}(\text{img}(\tau_j)) \leq 4 \text{dim}_{\mathbb{F}_q}(\mathbb{F}_q(\alpha_j)) = 4 \deg(f_j).
\]

Now, let $\tau$ be the homomorphism of $\mathbb{F}_q$-algebras defined by $\bigoplus_{j=1}^{\epsilon+r} \tau_j$. Observe that this homomorphism is injective. In fact, let $u$ be an element of $\mathbb{F}_q D_n$ such that $\tau(u) = 0$. If we write $u = P_1(x) + P_2(x)y$, where $P_1$ and $P_2$ are polynomials of degree less than $n$, for each $j > \epsilon$, we have
\[
\tau_j(u) = \begin{pmatrix} P_1(\alpha_j) & P_2(\alpha_j) \\ P_2(\alpha_j^{-1}) & P_1(\alpha_j^{-1}) \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},
\]
so, $P_1(\alpha_j) = P_1(\alpha_j^{-1}) = 0$ and $P_2(\alpha_j) = P_2(\alpha_j^{-1}) = 0$. In addition, if $\epsilon \geq 1$, then
\[
\tau_1(u) = (P_1(1) + P_2(1), P_1(1) - P_2(1)) = 0,
\]
and if $\epsilon = 2$ we have
\[
\tau_2(u) = (P_1(-1) + P_2(-1), P_1(-1) - P_2(-1)) = 0.
\]
It follows that $P_1$ and $P_2$ are divisible by the polynomial $x^n - 1$ and since the degrees of these polynomials are less that $n$, we conclude that $P_1$ and $P_2$ are null polynomials and therefore $\tau$ is an injective homomorphism.

Finally, we observe that the homomorphism $\rho : \mathbb{F}_q D_{2n} \rightarrow \bigoplus_{j=1}^{r+s} A_j$ defined by $\rho = \bigoplus_{j=1}^{r+s} \rho_j$ where $\rho_j = \begin{cases} \sigma_j \circ \tau_j & \text{if } \epsilon < j \leq r \\ \tau_j & \text{otherwise} \end{cases}$ is injective. Furthermore, $\dim_{\mathbb{F}_q}(\mathbb{F}_q D_n) = 2n$ and

$$\dim_{\mathbb{F}_q} \left( \bigoplus_{j=1}^{r+s} A_j \right) = 2\epsilon + 4 \sum_{j=\epsilon+1}^r \dim_{\mathbb{F}_q}(\mathbb{F}_q[\alpha_j + \alpha_j^{-1}]) + 4 \sum_{j=r+1}^{r+s} \dim_{\mathbb{F}_q}(\mathbb{F}_q[\alpha_j])$$

$$= 2\epsilon + 2 \sum_{j=\epsilon+1}^r \deg(f_j) + 4 \sum_{j=r+1}^{r+s} \deg(f_j)$$

$$= 2 \deg(x^n - 1) = 2n.$$

Therefore $\rho$ is an isomorphism. \hfill \Box

**Remark 3.2.** In the proof of the theorem we use the following facts: if $\beta$ is a root of the polynomial $g \in \mathbb{F}_q[x]$, then $\beta^{-1}$ is root of the polynomial $g^*$. In addition, when $g$ is auto-reciprocal and $\pm 1$ are not roots of $g$, there exists a polynomial $h \in \mathbb{F}_q[x]$ of degree $\frac{\deg(g)}{2}$, such that $\beta$ is a root of $g$ if and only if $\beta + \beta^{-1}$ is a root of $h$. In fact, since $g$ is symmetrical, we can write $g$ as

$$g(x) = \sum_{j=0}^t a_j (x^{t+j} + x^{t-j}) = x^t \sum_{j=0}^t a_j (x^j + x^{-j}) = x^t \sum_{j=0}^t a_j D_j(z, 1) = x^t h(z)$$

where $D_j$ is the Dickson polynomial of degree $j$ and $z = x + x^{-1}$ (see [9] or [10]).

**Theorem 3.3.** The dihedral group algebra $\mathbb{F}_q D_{2n}$ has $\epsilon + r + s$ central irreducible idempotents:

1. $2\epsilon$ idempotents of the form $\frac{1+\alpha}{2} e_{f_j}$ and $\frac{1-\alpha}{2} e_{f_j}$, where $j \leq \epsilon$.
2. $r-\epsilon$ idempotents $e_{f_j}$, where $j = \epsilon+1, \ldots, r$, generated by the auto-reciprocals factor of $x^n - 1$.
3. $s$ idempotents $e_{f_j} + e_{f_j^*}$, where $j = r+1, \ldots, r+s$.

**Proof:** Since the homomorphism $\tau$ in the proof of Theorem 3.1 is injective, then the image of a central primitive idempotent $u$ by the homomorphism has to be zero in every component, except for one component where the image is the identity, i.e., for some $i$ fixed, $\tau_j(u) = \delta_{i,j} I_j$, where $I_j$ is the identity over the component $A_j$. Let $u = P(x) + Q(x)y$ be a representation of $u$, where $P$ and $Q$ are polynomials in $\mathbb{F}_q[x]$ of degree less than or equal to $n-1$. Observe that $Q$ is zero when calculated at each root of the polynomial $x^n - 1 = 0$, so $Q$ is the null polynomial. In addition, $P$ is one when we calculate it at the roots of the polynomials $f_j$ and $f_j^*$ and zero when we calculate it at the other roots of the polynomial $x^n - 1$. The unique polynomial of degree less or equal to $n-1$ that satisfies that proprieties is $e_{f_j}$, when $f_j = f_j^*$ and $e_{f_j} + e_{f_j^*}$ when $f_j \neq f_j^*$. Finally, if $j \leq \epsilon$ the image $\tau_j(e_{f_j}) = (1, 1)$ is not a primitive idempotent, and we can decompose this idempotent in two central primitive idempotents, $(\frac{1+\alpha}{2}) e_{f_j}$ and $(\frac{1-\alpha}{2}) e_{f_j}$, such that $\tau_j((\frac{1+\alpha}{2}) e_{f_j}) = (1, 0)$ and $\tau_j((\frac{1-\alpha}{2}) e_{f_j}) = (0, 1)$. \hfill \Box
4. Explicit form of the idempotents when \( \text{rad}(n)|(q-1) \)

Throughout this section, we assume that every prime factor of \( n \) divides \( q-1 \), \( \kappa \) and \( \nu \) denote the numbers \( \gcd(n, q-1) \) and \( \min\{\nu_2(\frac{n}{2}), \nu_2(q+1)\} \) respectively, \( \theta \) and \( \alpha \) are generators of \( F_q^* \) and \( F_{q^2}^* \) such that \( \alpha^{q+1} = \theta \). In the following results, we show the explicit form of the idempotents of the cyclic group algebra \( F_q C_n \) and the Wedderburn decomposition of the Dihedral group algebra \( F_q D_{2n} \). In other to show that representation, we need the following lemma

**Lemma 4.1.** [Corollary 3.3 and Corollary 3.6] The factorization of \( x^n - 1 \) in irreducible factors of \( F_q[x] \) depends on \( n \) and \( q \) in the following form:

(i) If \( 8 \nmid n \) or \( q \neq 3 \) \( (\text{mod } 4) \), then
\[
x^n - 1 = \prod_{t \in \mathcal{S}_t} \prod_{1 \leq u \leq \gcd(u, t) = 1} (x^t - \theta^{ul}),
\]
where \( m = \frac{n}{2\kappa} \) and \( l = \frac{q-1}{2} \). In addition, for each \( t \) such that \( t|m \), the number of irreducible factors of degree \( t \) is \( \frac{\varphi(t)}{t} \cdot \kappa \), where \( \varphi \) denotes the Euler Totient function.

(ii) If \( 8 \mid n \) and \( q \equiv 3 \) \( (\text{mod } 4) \), then
\[
x^n - 1 = \prod_{t \text{ odd}} \prod_{1 \leq u \leq \kappa} (x^t - \theta^{ul}) \cdot \prod_{t \mid m'} \prod_{u \in \mathcal{S}_t} (x^{2t} - (\alpha^{ul'} + \alpha^{qul'})x^t + \theta^{ul'}),
\]
where \( m' = \frac{n}{2\kappa}, l' = \frac{q^2-1}{2\kappa} \), and \( \mathcal{S}_t \) is the set
\[
\left\{ u \in \mathbb{N} \mid 1 \leq u \leq 2^\nu \kappa, \gcd(u, t) = 1 \right\},
\]
where \( \{a\}_b \) denotes the remainder of the division of \( a \) by \( b \), i.e. the number \( 0 \leq c < b \) such that \( a \equiv c \) \( (\text{mod } b) \). In addition, for each \( t \) odd such that \( t|m' \), the number of irreducible binomials of degree \( t \) and \( 2t \) is \( \frac{\kappa \cdot \varphi(t)}{t} \) and \( \frac{\kappa \cdot \varphi(t)}{2t} \) respectively, and the number of irreducible trinomials of degree \( 2t \) is
\[
\begin{cases} 
\frac{\varphi(t)}{t} \cdot 2^{\nu-1} \kappa, & \text{if } t \text{ is even} \\
\frac{\varphi(t)}{t} \cdot (2^{\nu-1} - 1) \kappa, & \text{if } t \text{ is odd}.
\end{cases}
\]

The following corollary, direct from Lemmas 2.1 and 2.2, shows the explicit form of each idempotent of the cyclic group algebra \( F_q C_n \) when \( \text{rad}(n)|(q-1) \).

**Corollary 4.2.** Let \( m \), \( m' \), \( l \) and \( l' \) be as in Lemma 4.1

(1) If \( 8 \nmid n \) or \( n \neq 3 \) \( (\text{mod } 4) \), then every irreducible idempotent of the ring \( \mathcal{R}_n \) is of the form
\[
e_{t, ul} = \frac{\theta^{ul}}{n} \cdot \frac{x^n - 1}{x^t - \theta^{ul}},
\]
where \( t \) and \( u \) satisfy the condition of Lemma 4.1 item (i).

(2) If \( 8 \mid n \) or \( n \equiv 3 \) \( (\text{mod } 4) \), then every irreducible idempotent of the ring \( \mathcal{R}_n \) is of the form shown in (1) and of the form
\[
e_{t, ul'} = \frac{t}{n} \left( (\alpha^{ul'} + \alpha^{qul'})x^t - 2\theta^{ul'} \right) \frac{x^n - 1}{(x^{2t} - (\alpha^{ul'} + \alpha^{qul'})x^t + \theta^{ul'})},
\]
where \( t \) and \( u \) satisfy the condition of Lemma 4.1 item (ii).
Remark 4.3. By Theorem 3.3 If

- \( \text{char}(F_q) = 2 \), or
- \( n \) is odd and \( \theta^{ul} \neq 1 \), or
- \( n \) is even and \( \theta^{ul} \neq \pm 1 \),

then every idempotent found in Corollary 4.2 item (1) is a central irreducible idempotent of \( F_qD_{2n} \). Otherwise, the idempotent can be reduced to two central primitive idempotents \( \frac{1+e_{t,ul}}{2} \) and \( \frac{1-e_{t,ul}}{2} \).

In addition, \( e_{t,ul'} \) of item (2) is also a central irreducible idempotent of \( F_qD_{2n} \) if \( \theta^{ul'} = 1 \), otherwise, the central irreducible idempotent is \( e_{t,ul'} + e_{t,-ul'} \).

Theorem 4.4. The Wedderburn decomposition of the group algebra \( F_qD_{2n} \) depends on \( n \) and \( q \) in the following form:

1. When \( n \) is odd, the decomposition is

\[
2F_q \oplus \frac{k-1}{2} M_2(F_q) \oplus \bigoplus_{t|m \atop t \neq 1} \frac{k \cdot \varphi(t)}{2t} M_2(F_{q^t}).
\]

2. When \( n \) is even,
   - (2.1) if \( q \equiv 1 \pmod{4} \) or \( 8 \nmid n \), the decomposition is
     \[
     4F_q \oplus \left( \frac{k}{2} - 1 \right) M_2(F_q) \oplus \bigoplus_{t|m \atop t \neq 1} \frac{k \cdot \varphi(t)}{2t} M_2(F_{q^t}),
     \]
   - (2.2) if \( q \equiv 3 \pmod{4} \) and \( 8 \mid n \), the decomposition is
     \[
     4F_q \oplus (k + 2^{\nu - 1}) M_2(F_q) \oplus (2^{\nu - 2} - k/4 + 1) M_2(F_{q^t}) \oplus \bigoplus_{t|m \atop t \mid 2i \atop t \neq 1} \frac{k \cdot \varphi(t)}{2t} M_2(F_{q^{2i}}) \oplus \bigoplus_{t|m' \atop t \equiv 0 \atop t \neq 1} \frac{2^{\nu - 1} - 1}{t} \frac{k \cdot \varphi(t)}{2t} M_2(F_{q^{2i}}).
     \]

where \( i = \begin{cases} 
0 & \text{if } \nu_2(q+1) > \nu_2(\frac{q}{2}) \\
1 & \text{if } \nu_2(q+1) \leq \nu_2(\frac{q}{2}).
\end{cases} \)

Proof: First, we consider the case \( n \neq 3 \pmod{4} \) or \( 8 \nmid n \), so every irreducible factor of \( x^n - 1 \) is a binomial, and except for the factors \( x-1 \) and \( x+1 \), we have that any irreducible factor of the form \( x^t - a \) is not auto-reciprocal. Thus, we have two cases to analyse:

i) If \( n \) is odd, we have that \( \epsilon = 0 \) or \( 1 \) and \( r = 1 \). By Lemma 3.3 there exist \( \frac{k \varphi(t)}{t} \) irreducible factors of degree \( t \) and by Theorem 3.3 there exist two components isomorphic to \( F_q \), \( \frac{k \varphi(t)}{2t} \) components of the form \( M_2(F_{q^t}) \) if \( t > 1 \) and \( \frac{k-1}{2} \) components of the form \( M_2(F_q) \) if \( t = 1 \), where \( t \) is a divisor of \( m \). So we obtain item (1).

ii) If \( n \) is even, we have that \( \epsilon = 2 \) and there exist four components isomorphic to \( F_q \). In addition, every factor of \( x^n - 1 \) different that \( x \pm 1 \) is a non-auto-reciprocal binomial, then \( r = 2 \), and by the same argument of the previous case there exist \( \frac{k \varphi(t)}{2t} \) components of the form \( M_2(F_{q^t}) \) if \( t > 1 \) and \( \frac{k-2}{2} \) components of the form \( M_2(F_q) \) if \( t = 1 \), where \( t \) is a divisor of \( m \). So, we obtain item (2.1).
Finally, in the case which $q \equiv 3 \pmod{4}$ and $8|n$, every factor of $x^n - 1$ is a binomial or a trinomial. The unique auto-reciprocal factor of the form $x^t - a$ with $t$ odd is $f_1 = x - 1$. Now, suppose that $x^{2t} - (\alpha u^t + \alpha q u^t) x^t + \theta u^t$ is an irreducible factor of $x^n - 1$ as in Lemma 4.1 item (b), such that it is an auto-reciprocal polynomial. It follows that $\theta u^t = 1$ and therefore $(q - 1)|u t'$. Since

$$l' = \frac{q - 1}{\gcd(n, q - 1)} \cdot \frac{q + 1}{2^\nu}.$$  

the polynomial is auto-reciprocal when $\gcd(n, q - 1)|u t' \cdot \frac{q + 1}{2^\nu}$ and we have two cases to consider:

i) If $\nu_2(q + 1) \leq \nu_2(\frac{u t'}{2^\nu})$ then $\frac{u t'}{2^\nu}$ is odd and $\gcd(\gcd(n, q - 1), \frac{u t}{2^\nu}) = 1$, therefore $\gcd(n, q - 1)|u$. But $t|m|n$ and $\gcd(t, u) = 1$, then these conditions imply that $t = 1$ and $u$ is a multiple of $\gcd(n, q - 1)$ not divisible by $2^\nu$ and less than $2^\nu \gcd(n, q - 1)$. So there exist $2^\nu - 2$ values of $u$ that generate $2^\nu - 1$ auto-reciprocal factors, all of them of degree 2, each one generating a component of the form $M_2(F_q)$. In addition, we have $\kappa - 2$ irreducible factors of degree 1, each one generating a component of the same type.

Therefore there exist $(\kappa - 2) + (2^{\nu - 1} - 1) = \kappa + 2^{\nu - 1} - 3$ components $M_2(F_q)$ and

$$\frac{k}{4}(2^\nu - 1) - (2^{\nu - 1} - 1) = 2^{\nu - 2}\kappa - 2^{\nu - 1} - \frac{k}{4} + 1$$

components $M_2(F_q^2)$.

ii) If $\nu_2(q + 1) > \nu_2(\frac{u t}{2^\nu})$ then $\frac{u t}{2^\nu}$ is even and $\gcd(\gcd(n, q - 1), \frac{u t}{2^\nu}) = 2$, therefore $\frac{1}{2} \gcd(n, q - 1)|u$. Similarly, we obtain $t = 1$ and $u$ is a multiple of $\frac{1}{2} \gcd(n, q - 1)$ non divisible by $2^\nu$ and less than $2^\nu \gcd(n, q - 1)$. So there exist $2^{\nu + 1} - 2$ values of $u$ and then $2^\nu - 1$ auto-reciprocal factors, all of them of degree 2.

Then there exist $\kappa + 2^\nu - 3$ components $M_2(F_q)$ and $2^{\nu - 2}\kappa - 2^{\nu - 1} - \frac{k}{4} + 1$ components $M_2(F_q^2)$.

\[\square\]

**References**

[1] Arora, S. K., Pruthi M. *Minimal Codes of Prime-Power Length*. Finite Fields Appl. 3 (1997) 99-113

[2] Broche, O., del Río, À., *Wedderburn decomposition of finite group algebras*, Finite Fields Appl. 13 (2007) 71-79.

[3] Brochero Martínez, F.E., Giraldo Vergara, C.R., *Explicit Idempotents of Finite Group Algebras* Finite Fields Appl. 28 (2014) 123-131

[4] Brochero Martínez, F.E., Giraldo Vergara, C.R., Batista de Oliveira, L., *Explicit Factorization of $x^n - 1 \in F_q[x]$, submitted for publication in Designs, Codes and Cryptography. Preprint available on \[http://arxiv.org/abs/1404.6281\]

[5] Dutra,F., Ferraz, R., Polcino Milies, C., *Semisimple group codes and dihedral codes*, Algebra Discrete Math. 3 (2009), 28-48.

[6] Ferraz, R., Goodeire, E., Polcino Milies, C., *Some classes of semisimple group (and loop) algebras over finite fields*, J. of Algebra 324 (2010) 3457-3469

[7] Giraldo Vergara, C.R., Brochero Martínez, F. E. *Wedderburn decomposition of some special rational group algebras*. Lect. Mat. 23 , no. 2, (2002) 99-106.

[8] Jespers, E., Leal, G., Paques, A., *Central idempotents in rational group algebras of finite nilpotent groups*, J. Algebra Appl. 2 (1) (2003) 57-62.

[9] Lidl, R. Mullen, G. L., Turnwald, G., *Dickson polynomials*, Pitman Monographs and Surveys in Pure and Applied Math., Longman, London-Harlow-Essex, 1993.

[10] Meyn H. *Factorization of the cyclotomic polynomials $x^n + 1$ over finite fields*. Finite Fields Appl. 2, (1996) 439-442
[11] Olivieri, A., del Río, Á, Simón, J.J., *On monomial characters and central idempotents of rational group algebras*, Comm. Algebra 32 (4) (2004) 1531-1550.

Departamento de Matemática, Universidade Federal de Minas Gerais, UFMG, Belo Horizonte, MG, 30123-970, Brazil,

E-mail address: fbrocher@mat.ufmg.br