DOI: 10.28919/ejma.2022.2.10

Eur. J. Math. Appl. (2022)2:10
URL: http://ejma.euap.org

CYCLIC CODES AND PRIMITIVE IDEMPOTENTS IN THE FINITE CYCLIC GROUP ALGEBRAS

AZHAR O. ALMALKI* AND AHMED A. KHAMMASH

Abstract. We parallelly discuss the construction of cyclic linear codes as ideals in the finite cyclic group ring as well as zero-divisors therein. We also determine a complete set of primitive idempotents in the finite cyclic group ring over a field of characteristic p.

Introduction

Cyclic codes are among the most important types of codes in algebraic coding theory. They provide a substantial link between coding theory and various algebraic structures, and they are important for both theoretical and practical reasons; in fact, most existing linear codes in use are cyclic codes. The first connection between codes and group rings of finite groups appeared in the work of F.G. MacWilliams 1969 [4] in which cyclic codes were identified with ideals in the group algebras of cyclic groups (see also [5]), consequently, two sided ideals in a group algebra are named codes. Since then the algebraic structure of the group ring has been deeply involved in the study and constructions of codes. In particular properties of (central) primitive idempotents in the group algebra of finite groups over finite fields are heavily used in codes construction [6], [7]. On the other hand it is shown in [3] that cyclic codes are exactly zero-divisor codes in group rings of cyclic groups. Also Reed-Muller codes are extended cyclic codes and have been shown to be associated with the group ring of the elementary abelian 2-group [5]. In this paper, the zero divisor construction of cyclic codes is investigated in parallel with the ideal construction in the cyclic group ring. The main aim is to determine a complete set of primitive orthogonal idempotents of the group algebra of a cyclic group over a field of characteristic p (Theorem 3.1.1) and investigate the structure of the ideal codes (projective indecomposable modules) generated by primitive idempotents (Theorem 3.1.5). We also investigate the cyclic codes generated by those primitive idempotents as zero divisor type codes in the group ring of the cyclic group (Theorem 3.2.1).

1. Preliminaries

Here we explain the concept of linear cyclic codes and how they are realized as ideals in the group rings of the cyclic groups as well as zero divisors therein.

Department of mathematical sciences, Umm Al-Qura University, Saudi Arabia
*Corresponding author
E-mail addresses: azharobaidm@gmail.com, prof.khammash@gmail.com.

Key words and phrases. cyclic codes; group rings; idempotents.
Received 25/01/2022.

1.1. **Linear Codes.** Let $\mathbb{F}$ be a finite field with q elements and $n \in \mathbb{N}$. A code of length n on $\mathbb{F}$ is subset C of $\mathbb{F}^n$ for $n \in \mathbb{N}$. A code C of $\mathbb{F}^n$ called a trivial code if $q = 1$, a binary code if $q = 2$, and if $q = 3$ is ternary code, etc. It is known that $\mathbb{F}^n = \{(a_1, \ldots, a_n) | a_i \in \mathbb{F}\}$ is a vector space over $\mathbb{F}$ such that

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$$

$$\lambda(a_1, \ldots, a_n) = (\lambda a_1, \ldots, \lambda a_n)$$

where $\lambda \in \mathbb{F}$. If the code C is subspace of $\mathbb{F}^n$, then it is called linear code (or $[n, k]$-code on $\mathbb{F}$ where $k = dim_{\mathbb{F}} C$). As such if C is subspace of $\mathbb{F}^n$ is an $[n, k]$-code then $|C| = |\mathbb{F}|^k$; that is, C consists of $|\mathbb{F}|^k = q^k$ vectors (codewords). In particular $[n, k]$-binary codes has 2^k codewords. The $(k \times n)$-matrix whose rows are the basis vectors of an $[n, k]$-code C of $\mathbb{F}^n$ is called a generator matrix $G(C)$ of C (since a subspace in priniciple has more than one basis, a code has more than one generator matrix). A parity check matrix $H(C)$ for a $[n, k]$-linear code C is $((n - k) \times n)$-matrix satisfying $G(C)H(C)^T = 0$ where 0 is $(k \times (n - k))$-zero matrix, and $H(C)^T$ is the transpose of $H(C)$. The distance between two code words in C of $\mathbb{F}^n$ is the number of positions in which they differ. The minimum distance d of $C \subseteq \mathbb{F}^n$ is the minimum number among all codword distances. An $[n, k]$-code with minimum distance d is referred to as $[n, k, d]$-code. The minimum distance of a code C controls the error detection and correction capability of C; an $[n, k, d]$-code $C \subseteq \mathbb{F}^n$ has detection capability $l = d - 1$, correction capability $t = \lfloor \frac{d-1}{2} \rfloor$, and (Singleton Bound) $d \leqslant n - k + 1$. A code achieving this bound is called maximum distance separable (MDS for short). A cyclic shift is a linear map

$$\pi : \mathbb{F}^n \to \mathbb{F}^n$$

$$\pi\left(a_1, \ldots, a_n\right) = (a_n, a_1, \ldots, a_{n-1})$$

for $(a_1, \ldots, a_n) \in \mathbb{F}^n$. A cyclic code C is an $[n, k]$-linear code over $\mathbb{F}^n$ which the cyclic shift of each codeword in C is also in C. Note that this implies that if $(a_1, \ldots, a_n) \in C$ then all its circular permutations are in C.

1.2. **Cyclic Codes as Ideals in the Group Ring $\mathbb{F}C_n$.** To explain the connection between cyclic codes and the cyclic group rings note first that we have a linear isomorphism

$$\varphi : \mathbb{F}^n \to \mathbb{F}[x] / < x^n - 1 >$$

$$\varphi\left((a_0, a_1, \ldots, a_{n-1})\right) = \left[a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}\right]$$

where $[g(x)] = g(x) + < x^n - 1 >$ for all $g(x) \in \mathbb{F}[x]$. On the other hand cyclic codes are ideals in $\mathbb{F}[x] / < x^n - 1 >$ according to the following

Lemma 1.2.1. A linear code C is cyclic if and only if $\varphi(C)$ is an ideal $\mathbb{F}[x] / < x^n - 1 >$.

Proof. If a linear code C is cyclic. then $(a_0, a_1, \ldots, a_{n-1}) \in C \Rightarrow (a_{n-1}, a_0, a_1, \ldots, a_{n-2}) \in C$, this implies $[a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}] \in \varphi(C) \Rightarrow [a_{n-1}, a_0 x + a_1 x^2 + \ldots + a_{n-2} x^{n-1}] \in \varphi(C)$ and so $\varphi(C)$ is closed under multiplication by $[x], [x^2], [x^3], \ldots$ which generate $\mathbb{F}[x] / < x^n - 1 >$, therefore $\varphi(C)$ ideal in $\mathbb{F}[x] / < x^n - 1 >$. Conversely, suppose $\varphi(C)$ is an ideal in $\mathbb{F}[x] / < x^n - 1 >$. This means that $\varphi(C)$ is closed under multiplication by $[x], [x^2], [x^3], \ldots$. But this is equivalent to the fact that C (the inverse image) is closed under taking shifts, hence C cyclic. □

Note that a commutative quotient ring $\mathbb{F}[x]/ < x^n - 1 >$ is principal ideal ring (PIR for short). We deduced that from the following Lemma

Lemma 1.2.2. (see [8]): The polynomial ring (algebra) $\mathbb{F}[x]$ is a principle ideal domain. □

That means if C be an ideal (cyclic code) in a quotient ring $\mathbb{F}[x]/ < x^n - 1 >$; that is, C of length n, then there is generator polynomial $f(x)$ because $\mathbb{F}[x]/ < x^n - 1 >$ is PIR, which is unique monic polynomial of minimum degree in C, and divide $x^n - 1$. If $\deg(f(x)) = r$, then dimension C is $k = n - r$; that is,

$$C =< f(x) >= \{q(x)f(x) \bmod (x^n - 1) \mid q(x) \in \mathbb{F}[x]\}.$$

A generator matrix of C when a generator polynomial $f(x) = c_0 + c_1 x + \ldots + c_r x^r$ where $c_0 \neq 0$ and $\left\{f(x), xf(x), \ldots, x^{k-1}f(x)\right\}$ is basis for C is

$$G(C) = \begin{pmatrix} c_0 & c_1 & c_2 & \ldots & c_r & 0 & 0 & \cdots & 0 \\ 0 & c_0 & c_1 & c_2 & \ldots & c_r & 0 & \cdots & 0 \\ 0 & 0 & c_0 & c_1 & c_2 & \ldots & c_r & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & 0 & \ldots & 0 & c_0 & c_1 & c_2 & \ldots & c_r \end{pmatrix}$$

Thus, a cyclic code can be generated from singular circulant matrix. If $f(x)r(x) \equiv 0 \bmod (x^n - 1)$ where $r(x)$ be the polynomial of minimal degree, then $r(x)$ is check polynomial gives a check matrix $H(C)$ of the code C.

The group algebra of a finite group G over a field $\mathbb{F}$ is $\mathbb{F}G = \left\{\sum_{g\in G} \alpha_g g \mid \alpha_g \in \mathbb{F}\right\}$ which consists of all formal $\mathbb{F}$-linear combinations of elements of G and satisfying the following (algebra) operations:

(1) $\left(\sum_{g\in \mathrm{G}} \alpha_g g\right) + \left(\sum_{g\in \mathrm{G}} \beta_g g\right) = \sum_{g\in \mathrm{G}} (\alpha_g + \beta_g)\, g.$

(2) $\left(\sum_{x\in \mathrm{G}} \alpha_x x\right) \left(\sum_{y\in \mathrm{G}} \beta_y y\right) = \sum_{x\in \mathrm{G}} \left(\sum_{y\in \mathrm{G}} \alpha_x \beta_y xy\right) = \sum_{x\in \mathrm{G}} \left(\sum_{g\in \mathrm{G}} \alpha_g \beta_{g^{-1}x}\right) x.$

(3) $\lambda \left(\sum_{g\in \mathrm{G}} \alpha_g g\right) = \sum_{g\in \mathrm{G}} \lambda \alpha_g g$, for $\lambda \in \mathbb{F}$.

where the elements of G form an $\mathbb{F}$-basis for $\mathbb{F}G$; that is, $\dim_{\mathbb{F}}(\mathbb{F}G) = |G|$. If G is abelian group, then $\mathbb{F}G$ is commutative $\mathbb{F}$-algebra. A group ring RG is generalization of a group algebra $\mathbb{F}G$ where R is a ring. The following demonstrates the connection between the commutative $\mathbb{F}$-algebras $\mathbb{F}[x]/ < x^n - 1 >$ and $\mathbb{F}C_n$ where $C_n =< g \mid g^n = 1 >$

Lemma 1.2.3. $\mathbb{F}[x]/ < x^n - 1 > \cong \mathbb{F}C_n$ (algebra isomorphism); the group ring of the cyclic group C_n over the field $\mathbb{F}$.

Proof. The map $\psi : \mathbb{F}[x] \to \mathbb{F}C_n$ given by $\psi(f(x)) = f(g)$; for all $f(x) \in \mathbb{F}[x]$ is clearly an algebra epimorphism with $\ker\psi =< x^n - 1 >$. □

Since the quotient ring $\mathbb{F}[x]/ < x^n - 1 >$ is principal ideal ring and as $\mathbb{F}[x]/ < x^n - 1 > \cong \mathbb{F}C_n$ (ring isomorphism), then we conclude the following

Proposition 1.2.4. The group algebra $\mathbb{F}C_n$ is a principal ideal ring. □

That means every ideal in $\mathbb{F}C_n$ is principal has the form $\mathbb{F}C_n a = \{ra \mid r \in \mathbb{F}C_n\}$ which generated by element a in $\mathbb{F}C_n$. Combining proposition 1.2.4, Lemma 1.2.3 and Lemma 1.2.1 we conclude the following theorem

Theorem 1.2.5. Every cyclic code of length n over a field $\mathbb{F}$ is an ideal in the group algebra $\mathbb{F}C_n$. □

Therefore, a cyclic code in $\mathbb{F}C_n$ has the form $\mathbb{F}C_n a$ where $a \in \mathbb{F}C_n$, which is denoted by $\mathcal{C}(a)$.

2. Codes From Group Rings

F. MacWilliams [4] was the first one to consider cyclic codes as ideals of the group ring $\mathbb{F}C_n$. In 2006, T. Hurley [2] proved a characterization of the group ring RG; where G is a finite group of order n and R is a ring, as a ring of $n \times n$ matrices over R. Then P. Hurley and T. Hurley in [3] used that characterization to study properties of group ring elements in terms of the properties of the corresponding matrices in order to construct and analyze systems of zero-divisors and unit-derived codes which are more general codes from ideals such as cyclic codes. In this section we describe the Hurley characterization of RG and his algorithm for constructing zero-divisor type code.

2.1. Hurely Characterization of Group Rings.

Suppose that $G = \{g_1 = i, g_2, g_3, \dots, g_n\}$ is a fixed listing for the elements of a group G. Consider the $n \times n$ (coding) matrix of G

$$\mathrm{M}(G) = \begin{pmatrix} g_1^{-1}g_1 & g_1^{-1}g_2 & \dots & g_1^{-1}g_n \\ g_2^{-1}g_1 & g_2^{-1}g_2 & \dots & g_2^{-1}g_n \\ \vdots & \vdots & \vdots & \vdots \\ g_n^{-1}g_1 & g_n^{-1}g_2 & \dots & g_n^{-1}g_n \end{pmatrix}_{n\times n}$$

Then for each $a = \sum_{i=1}^{n} \alpha_{g_i} g_i \in RG$, define the matrix $\mathrm{M}(RG, a) \in \mathrm{M}_n(R)$ as follows:

$$\mathrm{M}(RG, a) = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \dots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \dots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \dots & \alpha_{g_n^{-1}g_n} \end{pmatrix}_{n\times n}$$

In [2], T.Hurley proved that the correspondence $a \dashleftarrow\dashrightarrow \mathrm{M}(RG, a)$ defines a ring isomorphism.

2.2. Zero Divizors Type Codes.

Given a zero-divisor $u \in RG$ such that $uv = 0; v \in (RG)^*$, and let W be an R-submodule of RG with a basis of a group elements $S \subseteq G$. The zero-divisor code derived from $\boldsymbol{u}$ is either the left code $C = uW = \{ux \mid x \in W\}$ or the right code $C = Wu = \{xu \mid x \in W\}$. Thus a code is constructed from a zero divisor in RG, an R-submodule W and, when RG is non-commutative, a left or right encoding; so we use $\mathcal{C}[\boldsymbol{u}, \boldsymbol{S}]$ to denote the left code $C = uW$ and $\mathcal{C}[\boldsymbol{S}, \boldsymbol{u}]$ to denote the right code $C = Wu$. Clearly in both cases the code C is of length $n = |G|$ and $\dim C$ will depend on the choice of W. A code C may be derived from different zero divisors and different submodules. We shall use the right encoding $C = Wu$ as the left encoding is similar; u is called a generator element of the code C relative to the submodule W. In particular if we take $W = RG$, then $C = RGu$ is a left ideal in the group ring RG; this is the special case when $\operatorname{rank} U = \dim Wu$. Since u is a zero-divisor with $uv = 0; v \in (RG)^*$, it follows that $Cv = Wuv = 0$ and we may express

$C = \{y \in RG \mid yv = 0\}$; the (non-zero) element v is called the right check element of C. Since W is generated by the subset S of G, it follows that C is an $[n, k]$-code where $k = \operatorname{rank} Su$.

2.3. **Cyclic Codes as Zero Divisor Type Codes In $\mathbb{F}C_n$.**

Here we shall take the ring R in section 2.2 to be a field $\mathbb{F}$ of characteristic $p > 0$ and $G = C_n$; the cyclic group of order n. The following theorem shows that all cyclic codes over $\mathbb{F}$ (or $\mathbb{F}$-codes) are zero divisor type codes

Theorem 2.3.1. Every cyclic code of length n over a field $\mathbb{F}$ is a zero-divisor type code in $\mathbb{F}C_n$.

Proof. According to Lemma 1.2.3 and Theorem 1.2.5. Let $f(x)$ be generator polynomial of a cyclic code C of length n in $\mathbb{F}[x]/ < x^n - 1 >$. Thus, $f(x)$ divides $x^n - 1$; that is, there is nonzero polynomial $r(x)$ in $\mathbb{F}[x]/ < x^n - 1 >$ such that $f(x)r(x) \equiv 0 \bmod(x^n - 1)$. This means that $f(x)$ is a zero divisor in $\mathbb{F}[x]/ < x^n - 1 > \cong \mathbb{F}C_n$ and C is a zero divisor type code. □

3. Idempotents In $\mathbb{F}C_n$

From now on we assume that $p \mid n$; hence the group algebra $\mathbb{F}C_n$ is not semisimple. We note that idempotents in $\mathbb{F}C_n$ are zero divisors and, as such, they generate ideal codes in the group algebra $\mathbb{F}C_n$ (Theorem 1.2.5) as well as zero-divisor type codes therein (see section 2.2). If $0 \neq e \in \mathbb{F}C_n$ is a primitive idempotent then $P = \mathbb{F}C_n e$ is a minimal ideal in $\mathbb{F}C_n$, hence defines a cyclic code $\mathcal{C}(e)$ in $\mathbb{F}C_n$. On the other hand e is a zero-divisor in $\mathbb{F}C_n$ (as $e \neq 0$ and $e(e-1) = 0; (1 - e) \neq 0$), hence generates a zero-divisor type code $\mathcal{C}[S, e] = \mathbb{F}Se$ with respect to a subset S of $G = C_n$. We shall compare the two constructions and determine for which subset $S \subseteq G$ the two codes $\mathcal{C}(e)$ and $\mathcal{C}[S, e]$ are identical. First, we shall describe a complete set of primitive idempotents in $\mathbb{F}C_n$.

3.1. **Primitive Idempotents in $\mathbb{F}C_n$.**

In this section we give a complete set of primitive idempotents in $\mathbb{F}C_n$. Suppose that $n = p^a r; p \nmid r$ for $a, r \in \mathbb{N}$ and the field $\mathbb{F}$ is taken to be a splitting field for all subgroups of C_n. It is known (see [1], p.34) that $\mathbb{F}C_n$ has r multiplicative characters $\Phi_j; j = 0, 1, 2, \ldots, r - 1$ defined in terms of a primitive r-th roots of unity $\lambda \in \mathbb{F}$ as follows: $\Phi_j(x) = \lambda^j$. Write $S_0, S_1, \ldots, S_{r-1}$ for the one dimensional $\mathbb{F}C_n$-modules which afford the characters $\Phi_j; j = 0, 1, 2, \ldots, r - 1$. Every idempotent e in $\mathbb{F}C_n$ is central because for all $a \in \mathbb{F}C_n$ we have $ea = ae$, since $\mathbb{F}C_n$ commutative algebra. An idempotent e in $\mathbb{F}C_n$ is primitive if $\mathbb{F}C_n e$ is indecomposable.

Theorem 3.1.1. If $\Lambda = \mathbb{F}G; G = C_n; n = p^a r; p \nmid r, \operatorname{char}\mathbb{F} = p$. If $\lambda \in \mathbb{F}$ is a primitive r-th root of unity and $H =< x^{p^a} > \leq G$, then the

$$e_j = \frac{1}{r}\sum_{t=0}^{r-1}(\lambda^t)^j x^{tp^a} = \frac{1}{r}\sum_{t=0}^{r-1}\lambda^{tj}x^{tp^a}; j = 0, 1, ..., r - 1$$

is a complete set of primitive r central orthogonal idempotents in $\mathbb{F}C_n$.

Note that

$$\begin{aligned}
e_0 &= \frac{1}{r}\left(i + x^{p^a} + x^{2p^a} + \ldots + x^{p^a(r-1)}\right)\\
e_1 &= \frac{1}{r}\left(i + \lambda x^{p^a} + \lambda^2 x^{2p^a} + \ldots + \lambda^{r-1} x^{p^a(r-1)}\right)\\
e_2 &= \frac{1}{r}\left(i + \lambda^2 x^{p^a} + \lambda^4 x^{2p^a} + \ldots + \lambda^{r-2} x^{p^a(r-1)}\right)\\
\vdots \quad & \quad \vdots\\
e_{r-1} &= \frac{1}{r}\left(i + \lambda^{r-1} x^{p^a} + \lambda^{r-2} x^{2p^a} + \ldots + \lambda x^{p^a(r-1)}\right)
\end{aligned}$$

are elements in the group algebra of $\mathbb{F}H = \mathbb{F} < x^{p^a} >$. Since $\text{char}\mathbb{F} = p \nmid r, \mathbb{F} < x^{p^a} >$ is semisimple and as such it has r simple (1-dimensional) characters $\psi_j; j = 0, \ldots, r-1$ where $\psi_j\left(x^{p^a}\right) = \lambda^{r-j}$, ($\psi_0$ is the trivial character). Moreover for all $j = 0, 1, 2, \ldots, r-1$, $x^{p^a} e_j = \lambda^{r-j} e_j$. This means that $\mathbb{F}e_j \cong_{\mathbb{F}<x^{p^a}>} \psi_{r-j}; j = 0, 1, 2, \ldots, r-1$. Let $L_j = \mathbb{F} < x^{p^a} > e_j$; $j = 0, 1, \ldots, r-1$ be the one dimensional $\mathbb{F} < x^{p^a} >$-module which affords ψ_{r-j}. Write $P_j = \mathbb{F}C_n e_j; 0 \leqslant j \leqslant r-1$; the ideal of $\mathbb{F}C_n$ generated by e_j. Clearly P_j is an $\mathbb{F}C_n$-submodule of the regular module ${}_{\mathbb{F}C_n}\mathbb{F}C_n$. We shall discuss the primitivity of e_j by studying the structure of P_j.

Proving the primitivity of the elements $e_j; j = 0, 1, \ldots, r-1$ in Theorem 3.1.1 usually amounts to proving that the (Hecke) algebra $e_j\mathbb{F}C_n e_j$ is local algebra (i.e. has no idempotents other than 0 and e_j). However, to reach that conclusion and to avoid long calculation, we shall use the technique of the induced module and apply the Green's indecomposability Theorem. The following lemma proves that P_j is an induced module from the subgroup H. Lemma 3.1.2 (3) follows directly by applying the Green's indecomposability Theorem (see [9], Theorem 11.10).

Lemma 3.1.2. (1) $x^{p^a} e_j = \lambda^{r-j} e_j; 0 \leq j \leq r-1$, hence $\mathbb{F}e_j \cong_{F<x^{p^a}>} \psi_{r-j}$.
(2) $P_j = \mathbb{F}C_n e_j \cong_{\mathbb{F}C_n} \text{Ind}_H^{C_n} L_j$; in particular $\dim_{\mathbb{F}} P_j = [C_n : H] = p^a$.
(3) P_j is indecomposable ; $\forall j = 0, 1, \ldots, r-1$. □

The following Lemma is essential in the proof of Theorem 3.1.1

Lemma 3.1.3. Fix $r \in \mathbb{N}$. For all $0 \leq \gamma \leq r-1; \mid \{(s,t); 0 \leq s,t \leq r-1 \mid s+t \equiv_r \gamma\} \mid= r$.

Example 3.1.4.

$r = 3:$

0	1	2
$(0,0)$	$(1,0)$	$(0,2)$
$(1,2)$	$(0,1)$	$(2,0)$
$(2,1)$	$(2,2)$	$(1,1)$

$r = 4:$

0	1	2	3
$(0,0)$	$(1,0)$	$(0,2)$	$(3,0)$
$(2,2)$	$(0,1)$	$(2,0)$	$(0,3)$
$(3,1)$	$(2,3)$	$(1,1)$	$(1,2)$
$(1,3)$	$(3,2)$	$(3,3)$	$(2,1)$

$r = 5:$

0	1	2	3	4
$(0,0)$	$(0,1)$	$(0,2)$	$(0,3)$	$(0,4)$
$(1,4)$	$(1,0)$	$(1,1)$	$(1,2)$	$(1,3)$
$(2,3)$	$(2,4)$	$(2,0)$	$(2,1)$	$(2,2)$
$(3,3)$	$(3,3)$	$(3,4)$	$(3,0)$	$(3,1)$
$(4,1)$	$(4,2)$	$(4,3)$	$(4,4)$	$(4,0)$

PROOF OF THEOREM 3.1.1: It is clear (since λ is a primitive r-th root of unity) that $\sum_{0\le j\le r-1} e_j = i$. It remains to show that $e_j; j = 0, 1, \dots, r-1$ are primitive orthogonal idempotents.

(1) We show that $e_j; 0 \le j \le r-1$ are orthogonal idempotents. Consider the product

$$\begin{aligned} e_j e_k &= \frac{1}{r^2}\left(\sum_{s=0}^{r-1} \lambda^{sj} x^{sp^a}\right)\left(\sum_{t=0}^{r-1} \lambda^{tk} x^{tp^a}\right) \\ &= \frac{1}{r^2}\sum_{s,t=0}^{r-1} \lambda^{sj}\lambda^{tk} x^{sp^a} x^{tp^a} \\ &= \frac{1}{r^2}\sum_{0\le\gamma\le r-1}\left[\sum_{0\le s,t\le r-1: s+t\equiv_r \gamma} \lambda^{sj+tk}\right] x^{\gamma p^a} \end{aligned}$$

Hence the coefficient of $x^{\gamma p^a}; 0 \le \gamma \le r-1$, in $e_j e_k$ is

$$c^{\gamma}_{j,k} = \frac{1}{r^2}\sum_{0\le s,t\le r-1: s+t\equiv_r \gamma} \lambda^{sj+tk}$$

(I) If $j = k$, then the coefficient of $x^{\gamma p^a}$ in ${e_j}^2$

$$\begin{aligned} \frac{1}{r^2}\left(\sum_{0\le s,t\le r-1: s+t\equiv_r \gamma} \lambda^{sj+tj}\right) &= \frac{1}{r^2}\left(\sum_{0\le s,t\le r-1: s+t=\equiv_r \gamma} \lambda^{(s+t)j}\right) \\ &= \frac{1}{r^2} \mid \{(s,t); 0 \le s,t \le r-1 : s+t \equiv_r \gamma\} \mid \lambda^{\gamma j} \\ &= \frac{1}{r^2} r \lambda^{\gamma j} \qquad \text{By Lemma 3.1.3} \\ &= \frac{1}{r}\lambda^{\gamma j} \\ &= \text{Cf. of } x^{\gamma p^a} \text{ in } e_j; \text{ for all } 0 \le \gamma \le r-1 \end{aligned}$$

Hence ${e_j}^2 = e_j$; for all $0 \le j \le r-1$ and so e_j is an idempotent.

(II) If $j \ne k$, then the coefficient of $x^{\gamma p^a}; 0 \le \gamma \le r-1$, in $e_j e_k$ is

$$c^{\gamma}_{j,k} = \frac{1}{r^2}\sum_{0\le s,t\le r-1: s+t\equiv_r \gamma} \lambda^{sj+tk}$$

The summation in $c^{\gamma}_{j,k}$ involves r terms (Lemma 3.1.3) consists of different r-th roots of unity in $\mathbb{F}$, hence this summation equals 0 . Therefore $c^{\gamma}_{j,k} = 0$; for all $0 \le j \ne k, \gamma \le r-1$ and so $e_j e_k = 0$; for all $0 \le j \ne k, \gamma \le r-1$ which means that the idempotents $e_j; j = 0, \dots, r-$ 1 are orthogonal.

(2) Finally, to show that e_j is primitive we consider the module $P_j = \mathbb{F}C_n e_j \cong_{\mathbb{F}C_n} \operatorname{Ind}_H^{C_n} L_j$. Since $[C_n : H] = p^a$, it follows from the Green indecomposability theorem (see [9], Theorem 11.10), that $P_j = \mathbb{F}C_n e_j$ is indecomposable, hence e_j is primitive. □

It follows that the module $P_j = \mathbb{F}C_n e_j$ is a direct summand of the regular $\mathbb{F}C_n$-module ${}_{\mathbb{F}C_n}\mathbb{F}C_n$. As such P_j is a projective indecomposable $\mathbb{F}C_n$-module and also an ideal in $\mathbb{F}C_n$. We shall discuss the structure of P_j in the next section. The following determines the structure of P_j as a cyclic code.

Theorem 3.1.5. If $\Lambda = \mathbb{F}C_n$ and e_j as in Theorem 3.1.1, then $\mathcal{C}(e_j) = P_j = \mathbb{F}C_n e_j = \sum_{0\leq u\leq p^a-1}^{\oplus} \mathbb{F}x^u e_j$ is an $[n, p^a, r]$-code.

Proof. Since $C_n = \dot{\bigcup}_{0\leq u\leq p^a-1} Hx^u$, we have $P_j = \mathbb{F}C_n e_j = \sum_{0\leq u\leq p^a-1}^{\oplus} \mathbb{F}x^u e_j$, and $\dim_{\mathbb{F}} \mathcal{C}(e_j) = \dim_{\mathbb{F}} \mathbb{F}C_n e_j = \dim_{\mathbb{F}} \operatorname{Ind}_H^{C_n} L_j = [C_n : H] = p^a$. Also the minimum weight of $\mathcal{C}(e_j)$ is r. □

3.2. **Which Subset $S \subseteq G$ Gives $\mathcal{C}[S, e] \approx \mathcal{C}(e)$?** Since the index $[C_n : H] = p^a$, then the cosets $iH, xH, \ldots, x^{p^a-1}H$ of H partition C_n into p^a disjoint sets of cardinality r, hence a transversal set for the $C_n\backslash H$ has p^a elements which contain only one element of each coset of H.

Theorem 3.2.1. Suppose $\Lambda = \mathbb{F}C_n, n = p^a r; p \nmid r, \text{char}\mathbb{F} = p$. If e_j is the primitive orthogonal idempotent in Theorem 3.1.1. Let $S \subseteq G = C_n$ be a transversal for the $C_n\backslash H; H = < x^{p^a} >$. Then the ideal code $\mathbb{F}C_n e_j$ is a zero-divisor type code and $\mathbb{F}C_n e_j = \mathcal{C}[S, e_j]$.

Proof. Clearly $\mathbb{F}C_n e_j = \sum_{0\leq u\leq p^a-1} \mathbb{F}x^u e_j = \sum_{s\in S} \mathbb{F}s e_j$ where $S = \{x^u\}_{0\leq u\leq p^a-1}$. □

4. The Structure of the Projective Indecomposables P_j

The group algebra $\Lambda = \mathbb{F}C_n, n = p^a r; p \nmid r$, $\text{char}\,\mathbb{F} = p$ is known to have r blocks each block contains one projective indecomposable $\mathbb{F}C_n$-module $P_j; 0 \leq j \leq r-1$ and hence contains one simple $\mathbb{F}C_n$-module. It follows that P_j is uniserial with a single composition factor. The following determines the structure of P_j.

Theorem 4.0.1. Let $\alpha_j = \sum_{0\leq u\leq p^a-1} \lambda^{c_u} x^u e_j \in P_j; c_u \in \{0, 1, \ldots, r-1\}$. Then

(1) $x\alpha_j = \lambda^\gamma \alpha_j; \gamma \in \{0, 1, \ldots, r-1\}$ if and only if $\gamma p^a \equiv_r (r-j)$; there is a unique value of such γ. In particular $S_\lambda =$ Socle of P_j and P_j is the projective cover of S_λ.

(2) For any $c \in \{0, 1, \ldots, r-1\}$, take the p^a-tuple $(c + u(r-j))_{0\leq u\leq p^a-1} = (\mu_u)_{0\leq u\leq p^a-1}$. Then $\alpha_j = \sum_{0\leq u\leq p^a-1} \lambda^{\mu_u} x^u e_j \in P_j$ satisfies $\mathbb{F}.\alpha_j \cong_{\mathbb{F}C_n} S_\lambda \leq_{\mathbb{F}C_n} P_j$.

Proof. (1) We have $x\alpha_j = \sum_{0\leq u\leq p^a-1} \lambda^{c_u} x^{u+1} e_j = \left[\sum_{0\leq u\leq p^a-2} \lambda^{c_u} x^{u+1} e_j\right] + \lambda^{c_{p^a-1}} x^{p^a} e_j$. Hence

$$x\alpha_j = \lambda^{c_{p^a-1}-j} e_j + \sum_{0\leq u\leq p^a-2} \lambda^{c_u} x^{u+1} e_j, \text{as} \quad x^{p^a} e_j = \lambda^{r-j} e_j$$

While $\lambda^\gamma \alpha_j = \sum_{0\leq u\leq p^a-1} \lambda^{c_u+\gamma} x^u e_j$. Therefore $x\alpha_j = \lambda^\gamma \alpha_j$ if and only if

$$\lambda^{c_{p^a-1}-j} e_j + \sum_{0\leq u\leq p^a-2} \lambda^{c_u} x^{u+1} e_j = \lambda^{c_0+\gamma} e_j + \sum_{1\leq u\leq p^a-1} \lambda^{c_u+\gamma} x^u e_j$$

which is equivalent to the equality

$$\lambda^{c_{p^a-1}-j}e_j + \sum_{1\le u\le p^a-1} \lambda^{c_{u-1}}x^u e_j = \lambda^{c_0+\gamma}e_j + \sum_{1\le u\le p^a-1} \lambda^{c_u+\gamma}x^u e_j$$

By comparing coefficients, we have $x\alpha_j = \lambda^\gamma \alpha_j \Leftrightarrow$

$$(1) \quad \lambda^{c_0+\gamma} = \lambda^{c_{p^a-1}-j}, \qquad (2) \quad \lambda^{c_u+\gamma} = \lambda^{c_{u-1}}; \forall 1 \le u \le p^a - 1$$

This is equivalent to the following system of congruent linear equations:

$$(1) \quad c_0 + \gamma \equiv_r c_{p^a-1} + (r-j), \qquad (2) \quad c_u + \gamma \equiv_r c_{u-1}; \forall 1 \le u \le p^a - 1 \qquad (*)$$

Solving this system $(*)$ for c_{p^a-1} by recursive substitution we get from equation (1)

$$c_{p^a-1} + p^a\gamma \equiv_r c_{p^a-1} + (r-j)$$

which is equivalent to the modular identity $p^a\gamma \equiv_r (r-j)$. Since r, γ are relatively prime, γ is uniquely determined for each $j \in \{0, 1, \ldots, r-1\}$.

(2) Fix the (unique) solution $\gamma \in \{0, 1, \ldots, r-1\}$ for the modular identity $p^a\gamma \equiv_r (r-j)$. The solution set for system $(*)$ of linear congruences consists of r of p^a-tuples

$$\{(c_0, c_0 + (r-j), c_0 + 2(r-j), \ldots, c_0 + (p^a-1)(r-j)\}; c_0 \in \{0, 1, 2, \ldots, r-1\}$$

(sum and product inside tuples are taken $\bmod r$). For any $c = c_0 \in \{0, 1, \ldots, r-1\}$, the solution
$(c, c+(r-j), c+2(r-j), \ldots, c+(p^a-1)(r-j)) = (c+u(r-j))_{0\le u\le p^a-1} = (\mu_u)_{0\le u\le p^a-1}$
gives rise to an element $\alpha_j = \sum_{0\le u\le p^a-1} \lambda^{\mu_u}x^u e_j \in \mathrm{P}_j$ which generates S_γ.

□

5. Examples

5.1. **Primitive Idempotents in the Group Algebra $\mathbb{F}C_6$.** We have $6 = 2\times 3$, so we consider the two (non-semisimple) cases when $\mathrm{char}\mathbb{F} = 2 \vee 3$.

5.1(1) $\mathrm{char}\mathbb{F} = 2$: Take the extention field $\mathbb{F} = \mathbb{Z}_2[x]/ < x^2 + x + 1 >= \{0, 1, \lambda, \lambda^2 = \lambda + 1\}$, since $x^2 + x + 1$ is irreducible over $\mathbb{Z}_2$. It is clear that $1, \lambda, \lambda^2$ are 3-th roots of unity in $\mathbb{F}$ satisfying $\lambda^2 + \lambda + 1 = 0$. $\mathbb{F}C_6$ has 3 simple (1-dimensional) representations S_0, S_1 and S_2. The three primitive idempotents are

$$e_0 = i + x^2 + x^4, \quad e_1 = i + \lambda x^2 + \lambda^2 x^4, \quad e_2 = i + \lambda^2 x^2 + \lambda x^4$$

Hence $\quad {}_{\mathbb{F}C_6}\mathbb{F}C_6 = P_0 \oplus P_1 \oplus P_2; P_j = \mathbb{F}C_6 e_j = \mathbb{F}e_j \oplus \mathbb{F}xe_j; j = 0, 1, 2, x^2 e_j = \lambda^{3-j}e_j; j = 0, 1, 2.$

$$\text{For } \gamma, j \in 0, 1, 2 : 2\gamma \equiv_3 (3-j) \Leftrightarrow \begin{cases} \gamma = 0 \wedge j = 0 & \quad S_0 \le P_0 \\ \gamma = 1 \wedge j = 1 & , \text{hence } S_1 \le P_1 \\ \gamma = 2 \wedge j = 2 & \quad S_2 \le P_2 \end{cases}$$

(1) In $P_0 = \mathbb{F}C_6 e_0 = \mathbb{F}e_0 \oplus \mathbb{F}xe_0, \alpha_0 = e_0 + xe_0 = \sum_{g\in C_6} g \in P_0$ generates S_0, hence $P_0 = \begin{matrix} S_0 \\ S_0 \end{matrix}$

(2) In $P_1 = \mathbb{F}C_6 e_1 = \mathbb{F}e_1 \oplus \mathbb{F}xe_1, \alpha_1 = e_1 + \lambda^2 xe_1 \in P_1$ generates S_1, hence $P_1 = \begin{matrix} S_1 \\ S_1 \end{matrix}$

[We get $\alpha_1 = e_1 + \lambda^2 xe_1 \in P_1$ by taking $c = 0$ in the proof of Theorem 4.0.1(2) to get the 2-tuple $(0, 0 +_3 (3-1)) = (0, 2)$. The other two 2-tuples $(1, 1 +_3 (3-1)) = (1, 0)$ and

$(2, 2 +_3 (3-1)) = (2,1)$ give two choices: $\alpha_1 = \lambda e_1 + xe_1$ or $\alpha_1 = \lambda^2 e_1 + \lambda xe_1$ in both cases $x\alpha_1 = \lambda\alpha_1$)

(3) In $P_2 = \mathbb{F}C_6e_2 = \mathbb{F}e_2 \oplus \mathbb{F}xe_2, \alpha_2 = e_2 + \lambda xe_2 \in P_2$ generates S_2, hence $P_2 = \begin{matrix} S_2 \\ S_2 \end{matrix}$

[We may also take $\alpha_2 = \lambda e_2 + \lambda^2 xe_2$ or $\alpha_2 = \lambda^2 e_2 + xe_2$ in both cases $x\alpha_2 = \lambda^2\alpha_2$ as above]
For clarity, we explain the product coefficients $c^{\gamma}_{j,k}$ discussed in Theorem 3.1.1 through this example

$$c^{\gamma}_{j,k} = \begin{cases} \frac{1}{3^2} \mid \{(s,t); 0 \le s,t \le 2 : s+t \equiv_r \gamma\} \mid \lambda^{\gamma j} & \text{if } j = k \\ \frac{1}{3^2} \sum_{0 \le s,t \le 2 : s+t \equiv_r \gamma} \lambda^{sj+tk} & \text{if } j \ne k \end{cases}$$

For example we determine $c^1_{1,2}$ (coef. of $x^{1.2}$ in e_1e_2) , $c^1_{2,2}$ (coef. of $x^{1.2}$ in ${e_2}^2$).

$$(*) \qquad c^1_{1,2} = \frac{1}{3^2} \sum_{0 \le s,t \le 2 : s+t \equiv_3 1} \lambda^{sj+tk} = \sum_{0 \le s,t \le 2 : s+t \equiv_3 1} \lambda^{sj+tk}; \quad as \quad \frac{1}{3^2} \equiv 1 \quad in \quad \mathbb{F}$$

The pairs $(s,t); 0 \le s,t \le 2 : s+t \equiv_3 1 : (0,1), (1,0), (2,2)$. Substituting in $(*)$, we have

$$c^1_{1,2} = \lambda^{01+12} + \lambda^{11+02} + \lambda^{21+22} = \lambda^2 + \lambda^1 + \lambda^6 = \lambda^2 + \lambda^1 + 1 = 0$$

$$(**) \qquad c^1_{2,2} = \frac{1}{3^2} \mid \{(s,t); 0 \le s,t \le 2 : s+t \equiv_3 1\} \mid \lambda^{1.2}$$

$(s,t); 0 \le s,t \le 2 : s+t \equiv_3 1 : (0,1), (1,0), (2,2)$. Substituting in $(**)$, we have
$c^1_{2,2} = \lambda^2 =$ the coefficient of $x^{1.2} = x^2$ in ${e_2}^2$, $c^0_{2,2} = 1 =$ the coefficient of i in ${e_2}^2$, $c^2_{2,2} = \lambda =$ the coefficient of $x^{2.2} = x^4$ in ${e_2}^2$. Therefore ${e_2}^2 = i + \lambda^2 x^2 + \lambda x^4 = e_2, \ldots$ etc.

5.1(2) char$\mathbb{F} = 3$: Take $\mathbb{F} = \mathbb{Z}_3$. It is clear that $-1 = 2$ is 2-th root of unity in $\mathbb{F}$. $\mathbb{F}C_6$ has 2 simple (1-dimensional) representations S_0 and S_1. The two primitive idempotents are:
$e_0 = \frac{1}{2}(i + x^3)\,[= 2(i + 1x^3)]$, $\quad e_1 = \frac{1}{2}(i - x^3)\,[= 2(i + 2x^3)]$ (Note $\frac{1}{2} = 2^{-1} = 2 = -1$ in $\mathbb{Z}_3$).

(1) In $P_0 = \mathbb{Z}_3C_6e_0 = \mathbb{Z}_3e_0 \oplus \mathbb{Z}_3xe_0 \oplus \mathbb{Z}_3x^2e_0$. For $\gamma \in 0, 1$, $x\alpha_0 = \lambda^{\gamma}\alpha_0 \Leftrightarrow 3\gamma \equiv_2 (2-0) \Leftrightarrow \gamma = 0$. Hence P_0 is the projective cover of S_0; in fact $\alpha_0 = e_0 + xe_0 + x^2e_0 \in P_0$ generates S_0, hence

$$P_0 = \begin{matrix} S_0 \\ S_0 \\ S_0 \end{matrix}$$

(2) In $P_1 = \mathbb{Z}_3C_6e_1 = \mathbb{Z}_3e_1 \oplus \mathbb{Z}_3xe_1 \oplus \mathbb{Z}_3x^2e_1$. For $\gamma \in 0, 1$, $x\alpha_1 = \lambda^{\gamma}\alpha_1 \Leftrightarrow 3\gamma \equiv_2 (2-1) \Leftrightarrow \gamma = 1$. Hence P_1 is the projective cover of S_1; in fact $\alpha_1 = e_1 - xe_1 + x^2e_1 \in P_1$ generates S_1, hence

$$P_1 = \begin{matrix} S_1 \\ S_1 \\ S_1 \end{matrix}$$

Note that $\alpha_1 = e_1 + \lambda xe_1 + \lambda^2x^2e_1 \in P_1$ corresponds to the 3-tuple $(0, 0+1(2-1), 0+2(2-1))$ $= (0,1,2)$.
[We mayalso take $\alpha_1 = -e_1 + xe_1 - x^2e_1 \in P_1$, this also gives $x\alpha_1 = -\alpha_1 = \lambda\alpha_1$ hence generates S_1]

5.2. **Primitive idempotents in the group algebra $\mathbb{F}C_{10}$.** We have $10 = 2 \times 5$, so we consider the two (non-semisimple) cases when $\text{char}\mathbb{F} = 2 \vee 5$.

5.2(1) $\text{char}\mathbb{F} = 2$: Take the extention field $\mathbb{F} = \mathbb{Z}_2[x]/ < x^4 + x^3 + x^2 + x + 1 >$ of order 16 (note that $x^4 + x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$ is irreducible polynomial). It is clear that λ is 5-th root of unity in $\mathbb{F}$ satisfying $\lambda^4+\lambda^3+\lambda^2+\lambda+1 = 0$. $\mathbb{F}C_{10}$ has 5 simple (1-dimensional) representations S_0, S_1, S_2, S_3 and S_4. The primitive idempotents are:

$$\begin{aligned}
e_0 &= i + x^2 + x^4 + x^6 + x^8 & & \\
e_1 &= i + \lambda x^2 + \lambda^2 x^4 + \lambda^3 x^6 + \lambda^4 x^8 &, \quad & x^2 e_1 = \lambda^4 e_1 \\
e_2 &= i + \lambda^2 x^2 + \lambda^4 x^4 + \lambda x^6 + \lambda^3 x^8 &, \quad & x^2 e_2 = \lambda^3 e_2 \\
e_3 &= i + \lambda^3 x^2 + \lambda x^4 + \lambda^4 x^6 + \lambda^2 x^8 &, \quad & x^2 e_3 = \lambda^2 e_3 \\
e_4 &= i + \lambda^4 x^2 + \lambda^3 x^4 + \lambda^2 x^6 + \lambda x^8 &, \quad & x^2 e_4 = \lambda e_4
\end{aligned}$$

Such that $\sum_{0\le j\le 4} e_j = i$. Hence we have the following decomposition:

$$\mathbb{F}C_{10} = \sum_{0\le j\le 4}^{\oplus} \mathbb{F}C_{10}e_j = \sum_{0\le j\le 4}^{\oplus} P_j; P_j = \mathbb{F}C_{10}e_j = \sum_{0\le u\le 1} \mathbb{F}x^u e_j = \mathbb{F}e_j \oplus \mathbb{F}xe_j, \quad x^2 e_j = \lambda^{5-j} e_j$$

For $\gamma, j \in \{0, 1, 2, 3, 4\} : 2\gamma \equiv_5 (5 - j) \Leftrightarrow \begin{cases} j = 0 \wedge \gamma = 0 \\ j = 1 \wedge \gamma = 2 \\ j = 2 \wedge \gamma = 4 \\ j = 3 \wedge \gamma = 1 \\ j = 4 \wedge \gamma = 3 \end{cases}$, hence $\begin{matrix} S_0 \le P_0 \\ S_2 \le P_1 \\ S_4 \le P_2 \\ S_1 \le P_3 \\ S_3 \le P_4 \end{matrix}$

(1) $\alpha_0 = e_0 + xe_0 \in P_0$ generates S_0 and $P_0 \approx \begin{matrix} S_0 \\ S_0 \end{matrix}$

(2) $\alpha_1 = e_1 + \lambda^3 xe_1 \in P_1$ generates S_2 and $P_1 \approx \begin{matrix} S_2 \\ S_2 \end{matrix}$

(3) $\alpha_2 = e_2 + \lambda xe_2 \in P_2$ generates S_4 and $P_2 \approx \begin{matrix} S_4 \\ S_4 \end{matrix}$

(4) $\alpha_3 = e_3 + \lambda^4 xe_3 \in P_3$ generates S_1 and $P_3 \approx \begin{matrix} S_1 \\ S_1 \end{matrix}$

(5) $\alpha_4 = e_4 + \lambda^2 xe_4 \in P_4$ generates S_3 and $P_4 \approx \begin{matrix} S_3 \\ S_3 \end{matrix}$

Therefore the projective indecomposable $\mathbb{F}C_{10}$-module $P_j = \mathbb{F}C_{10}e_j; 0 \le j \le 4$ (of dimension 2) has the following composition series $P_j \approx \begin{matrix} S_{2j} \\ S_{2j} \end{matrix}$;($2j$ is taken mod 5).

The coefficient $c^{\gamma}_{2,4}$ of $x^m; m = 0, 2, 4, 6, 8$ in e_2e_4 is $1 + \lambda + \lambda^2 + \lambda^3 + \lambda^4 = 0$; i.e. $e_2e_4 = 0$. We use the formulae in Theorem 3.1.1 to determine the coefficients $c^2_{1,3}$ (coef. of $x^{2.2}$ in e_1e_3), $c^2_{3,3}$ (coef. of $x^{2.2}$ in $e_3{}^2$)

$$(*) \qquad c^2_{1,3} = \frac{1}{5^2} \sum_{0\le s,t\le 4: s+t\equiv_5 2} \lambda^{s.1+t.3} = \sum_{0\le s,t\le 4: s+t\equiv_5 2} \lambda^{s.1+t.3}$$

$0 \leq s,t \leq 4 : s+t \equiv_5 2 : (0,2),(2,0),(1,1),(3,4),(4,3)$; substituting in $(*)$, we get

$$c_{1,3}^2 = \sum_{0 \leq s,t \leq 4 : s+t \equiv_5 2} \lambda^{s.1+t.3} = \lambda^6 + \lambda^2 + \lambda^4 + \lambda^{15} + \lambda^{13} = \lambda + \lambda^2 + \lambda^4 + 1 + \lambda^3 = 0$$

$$(**) \qquad c_{3,3}^2 = \frac{1}{5^2} \mid \{(s,t); 0 \leq s,t \leq 4 : s+t \equiv_5 2\} \mid \lambda^{2.3}$$

$\mid (s,t); 0 \leq s,t \leq 4 : s+t \equiv_5 2 \mid = 5; (0,2),(2,0),(1,1),(3,4),(4,3)$
Substituting in $(**)$, we get $c_{3,3}^2$ (coef. of $x^{2.2} = x^4$ in $e_3{}^2) = \frac{1}{5}\lambda^{2.3} = \frac{1}{5}\lambda = \lambda =$ coef. of x^4 in e_3. Similarly we determine $c_{3,3}^0, c_{3,3}^1, c_{3,3}^3, c_{3,3}^4$ to see that $e_3{}^2 = e_3$.

5.2(2) char$\mathbb{F} = 5$: Take $\mathbb{F} = \mathbb{Z}_5$. A cyclic group $C_{10} =< x | x^{10} = i >$ has two simple (1-dimensional) modules $S_0 : x \mapsto 1$, and $S_1 : x \mapsto 4 \equiv -1$ defined in terms of the 2-th roots of unity $4(\equiv -1), 1 = 4^2 \in \mathbb{Z}_5$. Take the subgroup $H =< x^5 >= \{i, x^5\}$ of order 2. $\mathbb{F}C_{10}$ has two primitive orthogonal idempotents

$$e_0 = \frac{1}{2}\left(i + x^5\right) = 3(i + x^5), \quad e_1 = \frac{1}{2}\left(i - x^5\right) = 3(i - x^5)$$

Hence, ${}_{\mathbb{F}C_{10}}\mathbb{F}C_{10} = P_1 \oplus P_2$; $P_j = \mathbb{F}C_{10}e_j = \mathbb{F}e_j \oplus \mathbb{F}xe_j \oplus \mathbb{F}x^2e_j \oplus \mathbb{F}x^3e_j \oplus \mathbb{F}x^4e_j; j = 0,1, x^5e_j = \lambda^{2-j}e_j$.

For $\gamma, j \in \{0,1\} : 5\gamma \equiv_2 (2-j) \Leftrightarrow \begin{cases} \gamma = 0 \wedge j = 0 \\ \gamma = 1 \wedge j = 1 \end{cases}$, hence $\begin{array}{l} S_0 \leq P_0 \\ S_1 \leq P_1 \end{array}$

(1) $\alpha_0 = \sum_{0 \leq u \leq 4} x^u e_0 = e_0 + xe_0 + x^2e_0 + x^3e_0 + x^4e_0$ generates S_0
(2) $\alpha_1 = -e_1 + xe_1 - x^2e_1 + x^3e_1 - x^4e_1 \in P_1 = \mathbb{F}C_{10}e_1$ generates S_1

In both cases, $P_j = \begin{array}{c} S_j \\ S_j \\ S_j \\ S_j \\ S_j \end{array} ; j = 0,1$

5.3. **Primitive idempotents in the group algebra $\mathbb{F}C_{12}$.** We have $12 = 2^2 \times 3$, so we consider the two (non-semisimple) cases when char$\mathbb{F} = 2 \vee 3$.

5.3(1) char$\mathbb{F} = 3$: Take the extention field $\mathbb{F} = \mathbb{Z}_3[x]/ < x^2 + 1 >= \{0, 1, 2, \lambda, 2\lambda, \lambda + 1, \lambda + 2, 2\lambda + 1, 2\lambda + 2\}$, since $x^2 + 1$ is irreducible over $\mathbb{Z}_3$. It is clear that λ is 4-th root of unity in $\mathbb{F}$ satisfying $\lambda^2 + 1 = 0$, hence $\lambda^2 = -1 = 2$. $\mathbb{F}C_{12}$ has 4 simple (1-dimensional) representations S_0, S_1, S_2 and S_3. Take $H =< x^3 >= \{i, x^3, x^6, x^9\}$ subgroup of C_{12}. We have the following four primitive orthogonal idempotents in $\mathbb{F}C_{12}$

$$e_0 = i + x^3 + x^6 + x^9, \quad e_1 = i + \lambda x^3 + \lambda^2 x^6 + \lambda^3 x^9, \quad e_2 = i + \lambda^2 x^3 + x^6 + \lambda^2 x^9$$

$$e_3 = i + \lambda^3 x^3 + \lambda^2 x^6 + \lambda x^9$$

Hence ${}_{\mathbb{F}C_{12}}\mathbb{F}C_{12} = \sum_{0 \leq j \leq 3}^{\oplus} P_j; P_j = \mathbb{F}C_{12}e_j = \mathbb{F}e_j \oplus \mathbb{F}xe_j \oplus \mathbb{F}x^2e_j, x^3e_j = \lambda^{4-j}e_j$

For $\gamma, j \in \{0,1,2,3\} : 3\gamma \equiv_4 (4-j) \Leftrightarrow \begin{cases} \gamma = 0 \wedge j = 0 \\ \gamma = 1 \wedge j = 1 \\ \gamma = 2 \wedge j = 2 \\ \gamma = 3 \wedge j = 3 \end{cases}$, hence $\begin{array}{l} S_0 \leq P_0 \\ S_1 \leq P_1 \\ S_2 \leq P_2 \\ S_3 \leq P_3 \end{array}$

(1) $\alpha_0 = e_0 + xe_0 + x^2e_0 \in P_0$ generates S_0 and $P_0 \approx \begin{array}{c} S_0 \\ S_0 \\ S_0 \end{array}$.

(2) $\alpha_1 = e_1 + \lambda^3 xe_1 + \lambda^2 x^2 e_1 \in P_1$ generates S_1 and $P_1 \approx \begin{array}{c} S_1 \\ S_1 \\ S_1 \end{array}$.

(3) $\alpha_2 = e_2 + \lambda^2 xe_2 + x^2 e_2 \in P_2$ generates S_2 and $P_2 \approx \begin{array}{c} S_2 \\ S_2 \\ S_2 \end{array}$.

(4) $\alpha_3 = e_3 + \lambda xe_3 + \lambda^2 x^2 e_3 \in P_3$ generates S_3 and $P_3 \approx \begin{array}{c} S_3 \\ S_3 \\ S_3 \end{array}$.

Hence P_j is the projective cover of S_j and has the following structure: $P_j : \begin{array}{c} S_j \\ S_j \\ S_j \end{array}$.

5.3(2) char$\mathbb{F} = 2$: Take the extention field $\mathbb{F} = \mathbb{Z}_2[x]/ < x^2 + x + 1 >= 0, 1, \lambda, \lambda + 1$. $\mathbb{F}C_{12}$ has 3 simple (1-dimensional) representations S_0, S_1 and S_2. The three primitive idempotents are:

$e_0 = i + x^4 + x^8, \quad e_1 = i + \lambda x^4 + \lambda^2 x^8, \quad e_2 = i + \lambda^2 x^4 + \lambda x^8$ (Note: $\frac{1}{3} \equiv 1$ in $\mathbb{F}$).

Hence ${}_{\mathbb{F}C_{12}}\mathbb{F}C_{12} = \sum^{\oplus}_{0 \le j \le 2} P_j; P_j = \mathbb{F}C_{12}e_j = \mathbb{F}e_j \oplus \mathbb{F}xe_j \oplus \mathbb{F}x^2e_j \oplus \mathbb{F}x^3e_j, x^4e_j = \lambda^{3-j}e_j$.

For $\gamma, j \in \{0, 1, 2\} : 4\gamma \equiv_3 (3 - j) \Leftrightarrow \begin{cases} \gamma = 0 \wedge j = 0 \\ \gamma = 2 \wedge j = 1 \\ \gamma = 1 \wedge j = 2 \end{cases}$, hence $\begin{array}{c} S_0 \le P_0 \\ S_2 \le P_1 \\ S_1 \le P_2 \end{array}$

(1) $\alpha_0 = e_0 + xe_0 + x^2e_0 + x^3e_0 \in P_0$ generates S_0 and $P_0 \approx \begin{array}{c} S_0 \\ S_0 \\ S_0 \\ S_0 \end{array}$

(2) $\alpha_1 = e_1 + \lambda xe_1 + \lambda^2x^2e_1 + x^3e_1 \in P_1$ generates S_2 and $P_1 \approx \begin{array}{c} S_2 \\ S_2 \\ S_2 \\ S_2 \end{array}$

(3) $\alpha_2 = e_2 + \lambda^2xe_2 + \lambda x^2e_2 + x^3e_2 \in P_2$ generates S_1 and $P_2 \approx \begin{array}{c} S_1 \\ S_1 \\ S_1 \\ S_1 \end{array}$

Consider the coefficient

$$c^{\gamma}_{j,k} = \begin{cases} \frac{1}{3^2} \mid \{(s,t); 0 \le s, t \le 2 : s + t \equiv_3 \gamma\} \mid \lambda^{\gamma j} & \text{if } j = k \\ \frac{1}{3^2} \sum_{0 \le s,t \le 2 : s+t \equiv_3 \gamma} \lambda^{sj+tk} & \text{if } j \ne k \end{cases}$$

- $c_{1,2}^{0} = \sum_{0\leq s,t\leq 2: s+t\equiv_3 0} \lambda^{s.1+t2} = \frac{1}{3^2}\sum_{0\leq s,t\leq 2: s+t\equiv_3 0} \lambda^{sj+tk} = \lambda^{0.1+0.2} + \lambda^{2.1+1.2} + \lambda^{1.1+2.2} = 1+\lambda+\lambda^2 = 0$
- $c_{1,2}^{1} = \sum_{0\leq s,t\leq 2: s+t\equiv_3 1} \lambda^{s.1+t2} = \lambda^{0.1+1.2} + \lambda^{1.1+0.2} + \lambda^{2.1+2.2} = \lambda^2+\lambda+1 = 0$
- $c_{1,2}^{2} = \sum_{0\leq s,t\leq 2: s+t\equiv_3 2} \lambda^{s.1+t2} = \lambda^{1.1+1.2} + \lambda^{2.1+0.2} + \lambda^{0.1+2.2} = 1+\lambda^2+\lambda = 0$

It follows that $e_1e_2 = 0$. On the other hand
- $c_{2,2}^{1} = \frac{1}{3^2} \mid \{(s,t); 0\leq s,t\leq 2 : s+t\equiv_3 1\} \mid \lambda^2 = 3.\lambda^2 = \lambda^2$
- $c_{2,2}^{0} = \frac{1}{3^2} \mid \{(s,t); 0\leq s,t\leq 2 : s+t\equiv_3 0\} \mid \lambda^0 = 3 = 1$
- $c_{2,2}^{2} = \frac{1}{3^2} \mid \{(s,t); 0\leq s,t\leq 2 : s+t\equiv_3 2\} \mid \lambda^1 = 3\cdot\lambda = \lambda$

Hence ${e_2}^2 = e_2$.

Conclusion

We have described a formula for a complete set of primitive central orthogonal idempotents of the cyclic group algebra $\mathbb{F}C_n$ where char$\mathbb{F} = p$ and $n = p^a r$; $p \nmid r$, as well as the structure of the projective indecomposable $\mathbb{F}C_n$-modules corresponding to those primitive idempotents. We also determine the parameters of the cyclic code generated by each primitive idempotent and a subset of C_n related to its zero-divisor type structure.

Acknowledgement

This work is a part of a dissertation written by the first author and submitted to Umm Al-Qura University as a partial fulfillment for the master degree in mathematics. The first author would like to thank her academic advisor Prof. Ahmed Khammash for his cooperation, support and encouragement.

References

[1] J. Alperin, Local representation theory, Cambridge University Press, Cambridge, 2010.

[2] T. Hurley, Group rings and rings of matrices, Int. J. Pure Appl. Math. 31 (2006) 319-335.

[3] P. Hurley, T. Hurley, Codes from zero-divisors and units in group rings, ArXiv:0710.5893 [Cs, Math]. (2007).

[4] F.G. MacWilliams, Codes and ideals in group algebra, Combinatorial mathematics and its applications, University of North Carolina Press, Chapel Hill, 1969.

[5] V. Pless, W. Huffman, Hand book of coding theory, Elsevier, New York, 1998.

[6] G. Chalom, R.A. Ferraz, M. Guerreiro, C.P. Milies, Minimal Binary Abelian Codes of length $p^m q^n$, ArXiv:1205.5699 [Cs, Math]. (2012).

[7] R.A. Ferraz, M. Guerreiro, C.P. Milies, G-equivalence in group algebras and minimal abelian codes, ArXiv:1203.5742 [Cs, Math]. (2012).

[8] T. Hungerford, Algebra, Springer, 8th edition, New York, 1980.

[9] P. Landrock, Finite group algebras and their modules, Cambridge University Press, Cambridge, 1983.