André Luís dos Santos Duarte da Silva

On Nilpotent and Constacyclic Codes

Santo André, 2021

Federal University of ABC

Center for Mathematics, Computing and Cognition

André Luís dos Santos Duarte da Silva

On Nilpotent and Constacyclic Codes

Advisor: Prof. Dr. Francisco César Polcino Milies

Co-advisor: Prof. Dr. Raul Antônio Ferraz

Thesis submitted to the Center for Mathematics, Computing and Cognition in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Mathematics.

Este exemplar corresponde à versão final da tese
defendida pelo aluno André Luís dos Santos Duarte da Silva,
e orientada pelo Prof. Dr. Francisco César Polcino Milies.

Santo André, 2021

Sistema de Bibliotecas da Universidade Federal do ABC
Elaborada pelo Sistema de Geração de Ficha Catalográfica da UFABC
com os dados fornecidos pelo(a) autor(a).

Duarte da Silva, André Luís dos Santos
On Nilpotent and Constacyclic Codes / André Luís dos Santos Duarte da Silva. — 2021.

94 fls.

Orientador: Francisco César Polcino Milies

Tese (Doutorado) — Universidade Federal do ABC, Programa de Pós-Graduação em Matemática, Santo André, 2021.

1. Álgebras de Grupo. 2. Álgebras de Grupo Twisted. 3. Códigos Corretores de Erros. I. Polcino Milies, Francisco César. II. Programa de Pós-Graduação em Matemática, 2021. III. Título.

Este exemplar foi revisado e alterado em relação à versão original, de acordo com as observações levantadas pela banca examinadora no dia da defesa, sob responsabilidade única do(a) autor(a) e com a anuência do(a) (co)orientador(a).

Santo André, **13 de Julho de 2021 .**

ANDRÉ LUÍS ~~DOS~~ SANTOS DUARTE DA SILVA

Nome completo e Assinatura do(a) autor(a)

Nome completo e Assinatura do(a) (co)orientador(a)

Francisco César Polcino Milies

MINISTÉRIO DA EDUCAÇÃO
Fundação Universidade Federal do ABC
Avenida dos Estados, 5001 – Bairro Santa Terezinha – Santo André – SP
CEP 09210-580 · Fone: (11) 4996-0017

FOLHA DE ASSINATURAS

Assinaturas dos membros da Banca Examinadora que avaliou e aprovou a Defesa de Tese de Doutorado do candidato, ANDRE LUIS DOS SANTOS DUARTE DA SILVA realizada em 05 de Julho de 2021:

Prof.(a) ANDRE LUIZ MARTINS PEREIRA
UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO

Prof.(a) EDSON RYOJI OKAMOTO IWAKI
UNIVERSIDADE FEDERAL DO ABC

Prof.(a) RAUL ANTONIO FERRAZ
UNIVERSIDADE DE SÃO PAULO

Prof.(a) ROBSON RICARDO DE ARAÚJO
INSTITUTO FEDERAL DE SÃO PAULO

Prof.(a) NAZAR ARAKELIAN
UNIVERSIDADE FEDERAL DO ABC

Prof.(a) FRANCISCO CESAR POLCINO MILIES
UNIVERSIDADE DE SÃO PAULO - Presidente

* Por ausência do membro titular, foi substituído pelo membro suplente descrito acima: nome completo, instituição e assinatura

This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001

To my family

ACKNOWLEDGEMENTS

This thesis would not have been possible without the help and support of all my colleagues and teachers. I want to thank the members of the examine board: Raul Ferraz, André Pereira, Samir Assuena, Robson Araújo, Edson Iwaki, Nazar Arakalian; and for the members of our seminar meetings: Vitor Garcia, César Batista, Rafael Budaibes, Edite Taufer and Gladys Chalom.

Thank you to my parents, Edson and Genilda, for their unwavering and unconditional support. To everyone at UFABC, I could not have wished for a better place to spend four years of my life. Special thanks to Prof. Maria L. M. Giuliani for her help with bureaucratic issues.

To all my teachers, mentors and co-authors, for their willingness to share their wisdom, and for inspiring me to pursue a career in mathematics. In particular to my supervisor, César Polcino, for his unfailing patience, and his generosity with his time and knowledge.

If error is corrected whenever it is recognised,
the path of error is the path of truth.

Hans Reichenbach

RESUMO

Nos últimos duzentos anos houve muitas inovações nas comunicações que ajudaram as pessoas no mundo todo a se conectar. Porém, ainda lidamos com o problema fundamental da comunicação, reproduzir num ponto exatamente ou aproximadamente a mensagem enviada desde outro ponto. Deste problema, novos ramos da matemática foram criados, tais como a Teoria de Códigos e a Teoria da Informação.

Na primeira parte desta tese estudamos "códigos nilpotentes" e tratamos do problema da equivalência entre códigos. Além disso, damos condições para a equivalência monomial entre códigos numa álgebra de grupo; em particular para códigos cíclicos. No caso dos códigos minimais nilpotentes é dada uma condição suficiente para serem equivalentes por permutação a códigos abelianos.

A segunda parte é dedicada a apresentar um método diferente para computar o número de componentes simples de uma álgebra de grupo "twisted". Além disso, calculamos os idempotentes centrais primitivos de uma álgebra de grupo "twisted" de um grupo cíclico e, na última parte, damos um exemplo de idempotentes de uma álgebra de grupo "twisted".

Palavras-chave: Teoria de Códigos, Álgebras de Grupo, Álgebras de Grupo Twisted, Códigos Constacíclicos.

ABSTRACT

In two hundred years many innovations in communication have helped people all over the globe to connect. However, we still deal with the fundamental problem of communication, reproducing at one point either exactly or approximately a message send from another point. From this problem, new branches of mathematics were created, such as Coding Theory and Information Theory.

In the first part of this thesis, we study "nilpotent codes" and approach the problem of permutation equivalence between codes. In addition, we give conditions for monomial equivalence between codes in a group algebra; in particular to cyclic codes. In the case of minimal nilpotent codes a sufficient codition is given for being permutation equivalent to abelian codes.

The second part is devoted to present a different method of computing the number of simple components of a twisted group algebra. In addition, we compute the centrally primitive idempotents of the twisted group algebras of a cyclic group and in the last part we provide an example of idempotents in twisted group algebras.

Keywords: Coding Theory, Group Algebras, Twisted Group Algebras, Constacyclic Codes.

CONTENTS

TABLE OF NOTATIONS

$\mathbb{N}$	Natural numbers
$\mathbb{Z}$	Integer numbers
$Im(f)$	Image of map f
$M_n(R)$	Full $n \times n$ matrix ring over the ring R
$dim_{\mathbb{F}}(V)$	Dimension of the $\mathbb{F}$-vector space V
$Span_{\mathbb{F}}(X)$	Linear subspace generated by X over $\mathbb{F}$
$\mathbb{F}_q$	Finite field with q elements
$char(\mathbb{F})$	Characteristic of $\mathbb{F}$
$\|G\|$	Order of the group G
$\mathcal{Z}(G)$	Center of the group G
$C_G(X)$	Centralizer of the $X \subset G$
C_n	Cyclic group of order n
D_n	Dihedral group of order $2n$
S_n	Symmetric group of degree n
Q_8	Quaternion group
$A \rtimes B$	Semidirect product of the groups A and B
$A \circ B$	Central product of the groups A and B
a^g	Action of $g \in G$ on $a \in A$
$Z^2(G, A)$	Group of 2-cocycles of G over A
$H^2(G, A)$	Second cohomology group of G over A
$\Delta(G)$	Augmentation ideal
$\Delta(G, H)$	Kernel of the canonical projection $RG \to R[G/H]$

INTRODUCTION

Communication is an essential part of life and along the centuries many inventions enabled people to get their messages through. Nowadays, we use inventions such as cell phones, internet, email, wearable technology, virtual reality and mobile network to connect with the world in the blink of an eye. However, we expect not just to send and receive messages instantaneously, but achieve a reliable data transmission. For this reason of "doing things right", R. W. Hamming in 1947 established the modern theory of error-correcting codes by giving a method of constructing efficient codes, even though the first mention of the modern approach to codes and the Hamming's method appears in the paper "A Mathematical Theory of Communication" [45] by C. E. Shannon in 1948, which is the genesis of Information theory.

In his article, Shannon proved that 'good' error correcting codes exist, but his proof gave no hints on how to construct them. In 1949, M. Golay generalize the $(7,4)$-code presented in Shannon's article to all other Hamming codes, prompting a dispute over the actual creator of this family of codes. Golay invented four additional codes, of which two are perfect codes. One of these, a tertiary $(23,12)$-code denoted G_{23} introduces a non-binary code in the literature and Cocke, a decade later, introduced codes in the case where the symbols are taken from an arbitrary finite field.

In 1950, due to patent delays, Hamming in [19] created codes that enabled computers to correct occurring error in transmissions and, as we said before, establish the modern theory of error correcting codes. In his paper, Hamming defines the concept of systematic codes, parity check, Hamming distance, equivalent codes and apply concepts of linear algebra and metric topology in the theory of error correcting codes. It is worth mentioning that the notion of equivalence of codes was explored by Fontaine and Prange in 1959 by considering codes as vector spaces and using the concept of "combinatorial equivalence" of matrices defined by Tucker [48].

In 1957, E. Prange was the first person to study an important class of codes, the cyclic codes [38] and in [34] W. W. Peterson and D. T. Brown introduced cyclic codes from a new viewpoint, the well-known algebraic description of cyclic codes as ideals in the algebra of polynomials modulo $X^n - 1$. In the same year, H. F. Mattson and

G. Solomon [27] obtain a new class of codes, the pseudo-cyclic codes, by associating every code word of odd length p with a certain polynomial. Later on, the pseudo-cyclic codes were defined as ideals in the algebra of polynomials modulo some monic polynomial $f(X) \in \mathbb{F}[X]$ (See [35]). Constacyclic codes were defined by Berlekamp [2] as a particular case of pseudo-cyclic codes, when $f(X)$ is a binomial. Constacyclic codes are an extension of cyclic and negacyclic codes, which were introduced by E. Berlekamp [3].

Blake started to study cyclic codes over $\mathbb{Z}_m$ in 1972 and presented generalized notions of Hamming codes, Reed-Solomon codes and BCH codes over arbitrary integer residue rings [6]. Spiegel in [47] continued this work, concentrating on BCH codes involving group algebras over rings of p-adic integers. Shankar [44] considered BCH codes over integer residue rings as well, but started with monic divisors of $X^n - 1$ in $R[X]$ used as generator polynomials for these codes.

Slepian [46] introduced the theory of group codes, considering sequences of binary digits as elements of a group. In 1967, generalizing the study of cyclic codes, the russian mathematician S. D. Berman [5] introduced the abelian codes, a more general class of codes using the concept of group algebra. In this paper, Berman proved that the well known Reed-Muller codes over $GF(2)$ are also a particular case of abelian codes and used the methods of the finite group representations theory to study of abelian codes. Afterwards, the Generalized Reed-Muller codes were described by Chapin [9] as ideals in abelian group algebras over $GF(p)$ and by Landrock and Manz [24] as abelian group algebras over $GF(q)$, where p is a rational prime integer and q is a power of a prime.

In 2009, Bernal, Del Río and Simón obtained a criterion to decide when a linear code is a group code and as an application they provided a family of groups for which every two-sided group code is an abelian group code. They also proved that Reed-Solomon codes are cyclic, the parity check extensions of Reed-Solomon codes are elementary abelian group codes and determine the Cauchy codes which are left group codes.

In the same paper [4], they introduced the concept of an abelian decomposition for an arbitrary group G, and showed that if G has an abelian decomposition then every G-code is an abelian code. So, some natural questions arise: under which conditions a G-code is an abelian code? A cyclic code? When all minimal G-codes are abelian? When G is nilpotent, do there exist G-codes which are not equivalent to an abelian code? Some counterexamples to the last question were provided by [30], [31] and [36].

In this thesis we shall approach the other questions and explore in more details the nilpotent case. In addition, we will study codes that are actually better than cyclic and abelian codes, the constacyclic codes.

In the first chapter we provide the definitions of nilpotent groups, permutation groups and cohomology of groups. In addition, we cover all the background on crossed product, group rings and codes that will be needed in the rest of this thesis.

The next two chapters contains the actual work of the author. In Chapter 2 we shall study essential idempotents which were introduced by G. Chalom, R. Ferraz and C. Polcino [8] in order to provide non repetition codes, since repetition codes have bad performance and low rate of transmission. Furthermore, we will present conditions for monomial equivalence between codes in a group algebra and cyclic codes. Finally, in the two last sections, we shall study permutation equivalence between minimal nilpotent codes and abelian codes and provide some computations considerations.

Chapter 3 contains results about constacyclic codes when these are considered as ideals in a twisted group algebra or ideals in the algebra of polynomials modulo $X^n - \lambda$. In the first section we present a different method of computing the number of simple components of a twisted group algebra. Then, we determine necessary and sufficient conditions for the set of minimal idempotents of the twisted group algebra $\mathbb{F}^\gamma G$ to coincide with the set of minimal idempotents of a subalgebra which is group algebra. Finally, in the last section, we show how to compute the minimal idempotents in twisted group algebras by providing an example.

1 PRELIMINARIES

PRELIMINARIES

In this chapter we gather the needed background. We introduce notation and conventions which will be used throughout this thesis. In most cases we do not provide a proof, but we give classical references where it can be found.

1.1 SOLVABLE AND NILPOTENT GROUPS

Let G be a group. A *normal series* for G is a chain of subgroups

$$G = G_1 \supset G_2 \supset \cdots \supset G_r = \{1\}$$

in which $G_{i+1} \lhd G_i$, $1 \leq i \leq r-1$. The *factors of the normal series* are the factor groups $G_1/G_2, \cdots, G_{r-1}/G_r$. We say that G is *solvable* if G has a normal series in which all of the factor groups are abelian.

Theorem 1.1.1. *[37, p.29]*

1. *Subgroups of solvable groups are solvable.*
2. *Homomorphic images of solvable groups are solvable.*
3. *If $H \lhd G$ is such that both H and G/H are solvable, then G is also solvable.*

We say that H is a *minimal normal subgroup* of G if $H \lhd G$ and between H and the identity subgroup there are no other normal subgroup of G.

The *(ascending) central series* of a finite group G is the sequence of subgroups

$$\{1\} = \mathcal{Z}_0 \subset \mathcal{Z}_1 \subset \mathcal{Z}_2 \subset \cdots$$

where $\mathcal{Z}_{i+1}$ is the uniquely determined normal subgroup of G such that $\mathcal{Z}_{i+1}/\mathcal{Z}_i$ is the center of $G/\mathcal{Z}_i$. We call G *nilpotent* if $G = \mathcal{Z}_n$ for some n.

Lemma 1.1.2. *[37, Lemma 1.5.12] Subgroups and factor groups of nilpotent groups are nilpotent.*

If x and y are elements of a group G, their commutator $[x, y]$ is defined by

$$[x, y] = x^{-1}y^{-1}xy.$$

The subgroup of G generated by all commutators $[x, y]$, $x, y \in G$, is called the *commutator subgroup* of G and is denoted by G'.

Proposition 1.1.3. *[37, p.33] The following statements are true for nilpotent groups:*

1. *A finite p-group is nilpotent.*
2. *Finite direct products of nilpotent groups are nilpotent.*
3. *If $\{1\} \neq H \lhd G$ then $H \cap \mathcal{Z}(G) \neq \{1\}$.*
4. *A minimal nontrivial normal subgroup of a nilpotent group is contained in its center.*

The following is a useful characterization of finite nilpotent groups.

Theorem 1.1.4. *[37, Theorem 1.5.21] Let G be a finite group. Then, the following conditions are equivalent:*

1. *G is nilpotent.*
2. *Every Sylow subgroup of G is normal in G.*
3. *G is the direct product of its Sylow subgroups.*

1.2 PERMUTATION GROUPS

If X is a nonempty set, a subgroup G of the symmetric group $SymX$ is called a *permutation group* on X.

Definition 1.2.1. The permutation group G is called *transitive* if, given any pair of elements x, y of X, there exists a permutation π in G such that $\pi(x) = y$. The *stabilizer* of x in G is

$$St_G(x) = \{\sigma \in G | \sigma(x) = x\}.$$

The permutation group G is said to be *semiregular* if $St_G(x) = \{1\}$ for all $x \in X$. A *regular* group is one that is both transitive and semiregular.

Theorem 1.2.2. *[42, Theorem 1.6.1] Let G be a permutation group on a set X.*

1. *Let $x \in X$. Then the mapping $St_G(x) \mapsto \pi(x)$ is a bijection between the set of right cosets of $St_G(x)$ and the orbit of x. Hence the latter has cardinality $[G : St_G(x)]$.*
2. *If G is transitive, then $|G| = |X||St_G(x)|$ for all $x \in X$.*
3. *If G is regular, then $|G| = |X|$.*

Let X be the set $\{1, \cdots, n\}$. Then by the Theorem 1.2.2, the subgroup G of S_n is regular if and only if it is transitive and of order n (equivalently, $|G| = n$ and $\sigma(x) \neq x$ for every $1 \neq \sigma \in G$ and $x \in X$).

For a positive integer n denote $\mathbb{N}_n = \{1, 2, \cdots, n\}$. The next result is an important technical tool.

Lemma 1.2.3. *[4, Lemma 1.1] Let H be a regular subgroup of S_n and fix an element $i_0 \in \mathbb{N}_n$. Let $\psi : H \to \mathbb{N}_n$ be the bijection given by $\psi(h) = h(i_0)$. Then there is an anti-isomorphism $\sigma : H \to C_{S_n}(H)$, mapping $h \in H$ to σ_h, where*

$$\sigma_h(i) = \psi^{-1}(i)(h(i_0)) \quad (i \in \mathbb{N}_n).$$

Moreover $\sigma_h = h$ for every $h \in \mathcal{Z}(H)$ and so $\mathcal{Z}(H) = \mathcal{Z}(C_{S_n}(H))$.

1.3 COHOMOLOGY OF GROUPS

Assume that G acts on an abelian group A. A map

$$\gamma : G \times G \to A$$

is called a *2-cocycle* if for all $g, h, k \in G$

$$\gamma(g, h)\gamma(gh, k) = \gamma(h, k)^g \gamma(g, hk)$$

Let $Z^2(G, A)$ denote the set of all 2-cocycles of G with coefficients in the G-module A. If γ_1 and γ_2 are 2-cocycles, then their product $\gamma_1\gamma_2$ defined by

$$(\gamma_1\gamma_2)(g, h) := \gamma_1(g, h)\gamma_2(g, h), \quad g, h \in G$$

is again a 2-cocycle. It follows that $Z^2(G,A)$ constitutes an abelian group. The identity element of $Z^2(G,A)$ is the 1-valued 2-cocycle and the inverse γ^{-1} of γ is given by

$$\gamma^{-1}(g,h) := \gamma(g,h)^{-1} \quad \text{for all } x,y \in G.$$

Let $t : G \to A$ be any map such that $t(1) = 1$. Then the map

$$\delta t : G \times G \to A$$

defined by

$$\delta t(g,h) = t(h)^g t(g) t(gh)^{-1} \quad g,h \in G$$

is a 2-cocycle. We shall refer to δt as a *coboundary* and denote by $B^2(G,A)$ the set of all coboundaries. In addition, we say that the 2-cocycles γ and $\widetilde{\gamma}$ are *cohomologous* if there exist a coboundary δt such that $\gamma(g,h) = \delta t(g,h)\widetilde{\gamma}(g,h)$ for all $g,h \in G$.

It is straightfoward to verify that $B^2(G,A)$ is in fact a subgroup of $Z^2(G,A)$. The corresponding factor group

$$H^2(G,A) = \frac{Z^2(G,A)}{B^2(G,A)}$$

is called the *second cohomology group* of G over A. The elements of $H^2(G,A)$ are called *cohomology classes*. For any $f \in Z^2(G,A)$, we usually write $[f]$ for the cohomology class of f.

Definition 1.3.1. Let G and H be two groups and $\alpha \in Z^2(G,\mathbb{F}^*)$, $\beta \in Z^2(H,\mathbb{F}^*)$. Define $\gamma = \alpha \times \beta \in Z^2(G \times H, \mathbb{F}^*)$ by

$$\gamma((g,h),(g',h')) = \alpha(g,g').\beta(h,h'),$$

for all $(g,h),(g',h') \in G \times H$.

1.4 CROSSED PRODUCTS AND GROUP RINGS

From now on, let R be a ring with unity and let G be a group. Then the *crossed product* $R * G$ of G over R is an associative ring which contains R and has as an R-basis the set $\overline{G}$, a copy of G. Thus each element of $R * G$ is uniquely a finite sum $\sum_{g \in G} a_g \overline{g}$ with

$a_g \in R$. Addition is as expected and multiplication is determined by the two rules below. Specifically for $g, h \in G$ we have

$$\overline{g}\overline{h} = \gamma(g,h)\overline{gh} \quad \text{(twisting)}$$

where $\gamma \in Z^2(G, R^*)$. Furthermore for $g, h \in G$ and $r \in R$ we have

$$\overline{g}r = r^{\eta(g)}\overline{g} \quad \text{(action)}$$

where $\eta : G \to Aut(R)$ is a homomorphism. We sometimes also denote the crossed product by $R *_\eta^\gamma G$.

Certain special cases of crossed products have their own names. If there is no action or twisting, that is if $\eta(g) = 1$ and $\gamma(g,h) = 1$ for all $g, h \in G$, then $R *_\eta^\gamma G = RG$ is an ordinary *group ring*. In case where R is commutative, RG is also called the *group algebra* of G over R. If the action is trivial, then $R *_\eta^\gamma G = R^\gamma G$ is a *twisted group ring*. Finally if the twisting is trivial, then $R *_\eta^\gamma G$ is a *skew group ring*.

In the case of twisted group algebras of cyclic groups, we will need the following result.

Proposition 1.4.1. *[22, Proposition 2.2.1] Let $\mathbb{F}$ be an arbitrary field and G a cyclic group of order n generated by g, let $\gamma \in Z^2(G, \mathbb{F}^*)$ and let $\lambda = \prod_{i=1}^{n} \gamma(g, g^i)$. Then*

$$\mathbb{F}^\gamma G \cong \frac{\mathbb{F}[X]}{\langle x^n - \lambda \rangle} \quad \textit{as } \mathbb{F}\textit{-algebras.}$$

Lemma 1.4.2. *[22, Lemma 3.6.1] Let G and H be groups, let $\mathbb{F}$ be an arbitrary field, and let $\alpha \in Z^2(G, \mathbb{F}^*)$, $\beta \in Z^2(H, \mathbb{F}^*)$. Then*

$$\mathbb{F}^\alpha G \otimes_{\mathbb{F}} \mathbb{F}^\beta H \cong \mathbb{F}^{\alpha\times\beta}(G \times H) \quad \textit{as } \mathbb{F}\textit{-algebras.}$$

Given an element $\alpha = \sum_{g\in G} a_g \overline{g} \in R *_\eta^\gamma G$ we define the *support* of α to be the subset of elements in G that appear effectively in the expression of α, that is:

$$supp(\alpha) = \{g \in G : a_g \neq 0\}.$$

We shall now consider the case when $R *_\eta^\gamma G = RG$ is a group ring. Let H be a subgroup of G. We shall denote $\Delta_R(G, H)$ (or simply $\Delta(G, H)$) the left ideal of RG generated by the set $\{h - 1 : h \in H\}$, that is,

$$\Delta(G, H) = \left\{ \sum_{h\in H} a_h(h-1) : a_h \in RG \right\}.$$

If $H \lhd G$, then the canonical homomorphism $\omega : G \to G/H$ can be extended to an epimorphism $\omega^* : RG \to R(G/H)$ such that

$$\omega^* \left(\sum_{g \in G} a_g g \right) = \sum_{g \in G} a_g \omega(g).$$

Since $Ker(\omega^*) = \Delta(G, H)$, we have that $\Delta(G, H)$ is a two-sided ideal of RG and

$$\frac{RG}{\Delta(G, H)} \cong R(G/H).$$

If $H \neq \{1\}$ is a normal subgroup of G such that $|H|$ is invertible in R, we define

$$\widehat{H} = \frac{1}{|H|} \sum_{h \in H} h \in RG.$$

Proposition 1.4.3. *[37, Proposition 3.6.7] Let R be a ring and let H be a normal subgroup of a group G. If $|H|$ is invertible in R then*

$$RG = RG\widehat{H} \oplus RG(1 - \widehat{H})$$

where

$$RG\widehat{H} \cong R(G/H) \quad \textit{and} \quad RG(1 - \widehat{H}) = \Delta(G, H).$$

1.5 SEMISIMPLE RINGS

An R-module M is called *semisimple* if every submodule of M is a direct summand. A ring R is called *semisimple* if the module ${}_RR$ is semisimple. A left ideal I of R is *minimal* if every non-zero left ideal J of R included in I coincides with I; similarly for right and two-sided ideals.

Theorem 1.5.1. *[37, Theorem 2.6.4] Let R be a semisimple ring and A_i, $1 \leq i \leq s$, all minimal two-sided ideals of R. Then:*

1. *$A_i A_j = (0)$ if $i \neq j$.*
2. *$R = \oplus_{i=1}^{s} A_i$ as rings, where s is the number of isomorphic classes of minimal left ideals of R.*

Proposition 1.5.2. *[37, Theorem 2.6.7] Let $R = \oplus_{i=1}^{s} A_i$ be the decomposition of a semisimple ring R as a direct sum of minimal ideals two-sided. Then*

1. *Every two-sided ideal I of R can be written in the form $I = A_{i_1} \oplus \cdots \oplus A_{i_t}$, where $1 \leq i_1 < \cdots < i_t \leq s$.*

2. *If $R = \oplus_{i=1}^{s} B_i$ is another decomposition of R into a direct sum of minimal two-sided ideals, then $s = r$ and, after a possible renumbering of the indices, $A_i = B_i$, for all i.*

Definition 1.5.3. The unique minimal two-sided ideals of a semisimple ring R are called the *simple components* of R.

Theorem 1.5.4. *[37, Theorem 2.6.9] Let $R = \oplus_{i=1}^{s} A_i$ be a decomposition of a semisimple ring as a direct sum of minimal two-sided ideals. Then, there exists a family $\{e_i, \cdots, e_s\}$ of elements of R such that:*

1. *$e_i \neq 0$ is a central idempotent, $1 \leq i \leq s$.*

2. *If $i \neq j$ then $e_i e_j = 0$.*

3. *$1 = e_1 + \cdots + e_s$.*

4. *e_i cannot be written as $e_i = e_i^* + e_i^{**}$ where e_i^*, e_i^{**} are central idempotents such that $e_i^*, e_i^{**} \neq 0$ and $e_i^* e_i^{**} = 0$, $1 \leq i \leq s$.*

Definition 1.5.5. The elements of $\{e_i, \cdots, e_s\}$ in the theorem above are called the *centrally primitive idempotents* of R.

Theorem 1.5.6 (Wedderburn-Artin)**.** *[37, Theorem 2.6.18] A ring R is semisimple if and only if is isomorphic to a direct sum of matrix algebras over division rings:*

$$R \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_s}(D_s).$$

Now, we shall concentrate on semisimple group rings and semisimple twisted group algebras.

Theorem 1.5.7 (Maschke)**.** *[37, Theorem 3.4.7] Let G be group. Then, the group ring RG is semisimple if and only if the following conditions hold:*

1. *R is a semisimple ring.*

2. *G is finite.*

3. *$|G|$ is invertible in R.*

Theorem 1.5.8. *[22, Theorem 3.3.6] Let $\mathbb{F}$ be an arbitrary field of characteristic $p \geq 0$, let G be a finite group and let $\gamma \in Z^2(G, \mathbb{F}^*)$. Then the following conditions are equivalent:*

1. *$R = \mathbb{F}^\gamma G$ is a semisimple ring.*
2. *$p = 0$ or $p > 0$ and there exists an abelian Sylow p-subgroup P of G, say of order p^n, $n \geq 0$, such that the elements $\overline{g}^{p^n}$ with $g \in P$ are $\mathbb{F}^{p^n}$-linearly independent.*

1.6 CODES

Let $\mathbb{F}$ be a finite field with q elements. Let $\mathbb{F}^n$ denote the vector space of all n-tuples over $\mathbb{F}$. An (n, k) linear code $\mathcal{C}$ over $\mathbb{F}$ is a subspace of $\mathbb{F}^n$ of dimension k. The *Hamming distance* $d(x, y)$ between two vectors $x, y \in \mathbb{F}^n$ is defined to be the number of coordinates in which x and y differ. The *minimum distance* of a code C is the smallest distance between distinct codewords. The *Hamming weight* $wt(x)$ of a vector $x \in \mathbb{F}^n$ is the number of nonzero coordinates in x. The *minimum weight* of a code C is the weight of the lowest-weight non-zero codeword. Since we only work with the Hamming distance and Hamming weight in this thesis, we shall ommit the use of the word "Hamming".

Theorem 1.6.1. *[26, Theorem 1.1] If $x, y \in \mathbb{F}^n$, then $d(x, y) = wt(x - y)$. If $\mathcal{C}$ is a linear code, the minimum distance d is the same as the minimum weight of the nonzero codewords of C.*

By the last Theorem, the minimum distance of a linear code C is equal to the minimum weight of C.

Let us consider the action of the symmetric group S_n on the n-dimensional space $\mathbb{F}^n$ defined by:

$$\sigma(a_1, \cdots, a_n) := (a_{\sigma(1)}, \cdots, a_{\sigma(n)}) \quad \text{for all } (a_1, \cdots, a_n) \in \mathbb{F}^n. \tag{1}$$

The codes $\mathcal{C}_1, \mathcal{C}_2 \subset \mathbb{F}^n$ are *permutation equivalent* if there exists a permutation $\sigma \in S_n$ such that $C_2 = \sigma(C_1)$. For a given code $\mathcal{C} \subset \mathbb{F}^n$, the group of all permutations $\sigma \in S_n$ such that $\sigma(\mathcal{C}) = \mathcal{C}$ is denoted by $PAut(\mathcal{C})$. In addition, given $\sigma \in S_n$ and $\lambda_1, \cdots, \lambda_n \in \mathbb{F}^*$, the map $T : \mathbb{F}^n \to \mathbb{F}^n$ defined by

$$T(a_1, \cdots, a_n) = (\lambda_1 a_{\sigma(1)}, \cdots, \lambda_n a_{\sigma(n)}) \tag{2}$$

is called a *monomial transformation* of degree n. Note that, we may identify T with $Diag(\lambda_1, \cdots, \lambda_n).\sigma \in (\mathbb{F}^*)^n \rtimes S_n$. Then, by Equation 2 we have an action of the group

$M(\mathbb{F}^n) := (\mathbb{F}^*)^n \rtimes S_n$ on the set $\mathbb{F}^n$. The codes $\mathcal{C}_1, \mathcal{C}_2 \subset \mathbb{F}^n$ are *monomially equivalent* if there is a permutation $\sigma \in S_n$ and a matrix $M = Diag(\lambda_1, \cdots, \lambda_n)$ for which $C_2 = M.\sigma(C_1)$. Let C be a linear code in $\mathbb{F}^n$. The group of all monomial transformations T of degree n in $M(\mathbb{F}^n)$ for which $T(C) = C$ is denoted by $MAut(C)$.

Let $G = \{g_0 = 1, g_1, ..., g_{n-1}\}$ be a finite group. Any (left) ideal I of the group algebra $\mathbb{F}G$ defines a (left) group code $\mathcal{K}(I)$ of length n over $\mathbb{F}$ by the rule

$$(a_0, \cdots, a_{n-1}) \in \mathcal{K}(I) \Leftrightarrow a_0 g_0 + a_1 g_1 + \cdots + a_{n-1} g_{n-1} \in I.$$

Any code that is permutation (monomially) equivalent to $\mathcal{K}(I)$ for some (left) ideal I of the algebra $\mathbb{F}G$ is called a (left) *G-code* (*G-mcode*).

Theorem 1.6.2. *[4, Lemma 1.2] Let C be a linear code of length n over a finite field $\mathbb{F}$ and G a finite group of order n.*

1. *C is a left G-code if and only if G is isomorphic to a transitive subgroup H of S_n contained in $PAut(C)$.*
2. *C is a G-code if and only if G is isomorphic to a transitive subgroup H of S_n such that $H \cup C_{S_n}(H) \subset PAut(C)$.*

By the action of $M(\mathbb{F}^n) := (\mathbb{F}^*)^n \rtimes S_n$ on $\mathbb{F}^n$, we obtain a homomorphism

$$\phi : M(\mathbb{F}^n) \to S_n, \quad \phi(M.\sigma) = \sigma \tag{3}$$

Theorem 1.6.3. *[30, Theorem 1] Let C be a linear code of length n over a finite field $\mathbb{F}$ and let G be a finite group of order n. Moreover, let ϕ be the homomorphism given in Equation 3. Then, it holds:*

1. *C is a left G-mcode if and only if G is isomorphic to a subgroup of $H \leq MAut(C)$ such that $\phi(H)$ is a regular subgroup of S_n.*
2. *C is a G-mcode if and only if G is isomorphic to a subgroup $H \leq MAut(C)$ such that $H \cup C_{M(\mathbb{F}^n)}(H) \subset MAut(C)$ and $\phi(H)$ is a regular subgroup of S_n.*

Let $\mathcal{B} = \{v_0, \cdots, v_{n-1}\}$ be an ordered basis of an algebra $\mathcal{A}$ over $\mathbb{F}_q$. We shall think codes as ideals of $\mathcal{A}$. For an element a in the algebra $\mathcal{A}$, the *Hamming weight* of a is the number of elements in its support; i.e., if $a = \sum_{i=0}^{n-1} a_i v_i$, then

$$w(a) = \mid \{i \mid a_i \neq 0\} \mid .$$

The *Hamming distance* d on $\mathcal{A}$ is defined as

$$d(\alpha, \alpha') = w(\alpha' - \alpha).$$

for $\alpha, \alpha' \in \mathcal{A}$.

The *weight* or the *minimum distance* of an ideal I in $\mathcal{A}$ is

$$w(I) = min\{w(\alpha) \mid \alpha \neq 0,\ \alpha \in I\}.$$

A code $\mathcal{C}$ is *cyclic* of length n if it is linear and whenever $(a_0, \cdots, a_{n-1})$ is in $\mathcal{C}$ then so is $(a_{n-1}, a_0 \cdots, a_{n-2})$. Note that the cyclic codes of length n are C_n-codes. However, not every C_n-code is a cyclic code.

2 | NILPOTENT CODES

NILPOTENT CODES

In this chapter we shall begin by studying essential idempotents, which will be our main tool in the study of permutation equivalence between codes. In addition, we will give conditions for monomial equivalence between codes in a group algebra and cyclic codes. Finally, for minimal nilpotent codes, a sufficient condition for permutation equivalence to abelian codes will be presented.

2.1 ESSENTIAL IDEMPOTENTS

Let G be a finite group and R a commutative finite ring with unity. If $H \neq \{1\}$ is a normal subgroup of G such that $|H|$ is invertible in R, then

$$\widehat{H} = \frac{1}{|H|} \sum_{h \in H} h,$$

is a central idempotent of RG and

$$RG = RG.\widehat{H} \oplus RG.(1 - \widehat{H}).$$

where $RG.(1 - \widehat{H}) = \Delta(G, H)$ and $RG.\widehat{H} \cong R(G/H)$. Notice that, if $H \subset K$ are subgroups of G, then $\widehat{H}\widehat{K} = \widehat{K}$.

Example 2.1.1. Let $C_6 = \langle g \rangle$. The normal subgroups of C_6 are:

$$H_1 = \{1\}, \quad H_2 = \{1, g^2, g^4\}, \quad H_3 = \{1, g^3\}, \quad H_4 = C_6.$$

Then

$$\begin{aligned}
\widehat{H_1} &= 1 \\
\widehat{H_2} &= 2 + 2g^2 + 2g^4 \\
\widehat{H_3} &= 3 + 3g^3 \\
\widehat{H_4} &= 1 + g + g^2 + g^3 + g^4 + g^5.
\end{aligned}$$

are central idempotents of $\mathbb{F}_5C_6$. So we consider the ideal generated by $\widehat{H_2}$

$$\mathbb{F}_5C_6\widehat{H_2} \cong \mathbb{F}_5C_2 \tag{4}$$

with $\{\widehat{H_2}, g^3\widehat{H_2}\}$ a basis over $\mathbb{F}_5$. The complement of $\mathbb{F}_5C_6\widehat{H_2}$ is

$$\mathbb{F}_5C_6(1-\widehat{H_2}) = \Delta(C_6, H_2) \tag{5}$$

which has a basis $\{1-g^2, 1-g^4, g^3-g^5, g^3-g\}$ over $\mathbb{F}_5$.

Example 2.1.2. Let D_4 be the dihedral group of order 8 and presentation

$$\langle a, b | a^4 = b^2 = 1, bab = a^{-1} \rangle.$$

The normal subgroups of D_4 are:

$$\begin{aligned} &K_1 = \{1\}, && K_2 = \{1, a^2\}, && K_3 = \{1, a, a^2, a^3\} \\ &K_4 = \{1, a^2, b, a^2b\}, && K_5 = \{1, a^2, ab, a^3b\}, && K_6 = D_4. \end{aligned}$$

Then, we have the following central idempotents of $\mathbb{F}_3D_4$:

$$\begin{aligned} \widehat{K_1} &= 1 \\ \widehat{K_2} &= 2 + 2a^2 \\ \widehat{K_3} &= 1 + a + a^2 + a^3 \\ \widehat{K_4} &= 1 + a^2 + b + a^2b \\ \widehat{K_5} &= 1 + a^2 + ab + a^3b \\ \widehat{K_6} &= 2(1 + a + a^2 + a^3 + b + ab + a^2b + a^3b). \end{aligned}$$

The ideals which are generated by these idempotents and their respective complements are

$$\mathbb{F}_3D_4\widehat{K_1} = \mathbb{F}_3D_4 \quad \text{and} \quad \mathbb{F}_3D_4(1-\widehat{K_1}) = (0); \tag{6}$$

$$\mathbb{F}_3D_4\widehat{K_2} \cong \mathbb{F}_3(C_2 \times C_2) \quad \text{and} \quad \mathbb{F}_3D_4(1-\widehat{K_2}) = \Delta(D_4, K_2); \tag{7}$$

with basis $\{\widehat{K_2}, b\widehat{K_2}, a\widehat{K_2}, ab\widehat{K_2}\}$ and $\{1-a^2, b-a^2b, a-a^3, ab-a^3b\}$, respectively;

$$\mathbb{F}_3D_4\widehat{K_3} \cong \mathbb{F}_3C_2 \quad \text{and} \quad \mathbb{F}_3D_4(1-\widehat{K_3}) = \Delta(D_4, K_3); \tag{8}$$

with basis $\{\widehat{K_3}, b\widehat{K_3}\}$ and $\{1-a, 1-a^2, 1-a^3, b-a^3b, b-a^2b, b-ab\}$, respectively;

$$\mathbb{F}_3D_4\widehat{K_4} \cong \mathbb{F}_3C_2 \quad \text{and} \quad \mathbb{F}_3D_4(1-\widehat{K_4}) = \Delta(D_4, K_4); \tag{9}$$

with basis $\{\widehat{K_4}, a\widehat{K_4}\}$ and $\{1-a^2, 1-b, 1-a^2b, a-a^3, a-ab, a-a^3b\}$, respectively.

Example 2.1.3. Let S_4 with presentation

$$< a, b, c, d | a^2 = b^2 = c^3 = d^2 = 1, cac^{-1} = dad = ab = ba, cbc^{-1} = a, bd = db, dcd = c^{-1} > .$$

For future use, we shall use the notations $a := (1,2)(3,4)$, $b := (1,3)(2,4)$, $c := (1,2,3)$ and $d := (1,2)$.

The normal subgroups of S_4 are:

$$L_1 = \{1\}, \qquad L_2 =< a, b, c > \cong A_4,$$
$$L_3 =< a, b > \cong K_4, \qquad L_4 = S_4.$$

Then we have the following central idempotents:

$$\widehat{L_1} = 1$$
$$\widehat{L_2} = 3(1 + a + b + c + c^2 + ab + ac + ac^2 + bc + bc^2 + abc + abc^2)$$
$$\widehat{L_3} = 4(1 + a + b + ab)$$
$$\widehat{L_4} = \widehat{S_4}.$$

The ideals which are generated by $\widehat{L_2}$ and its complement are

$$\mathbb{F}_5 S_4 \widehat{L_2} \cong \mathbb{F}_5 C_2 \quad \text{and} \quad \mathbb{F}_5 S_4 (1 - \widehat{L_2}) = \Delta(S_4, L_2);$$

with basis $\{\widehat{L_2}, d\widehat{L_2}\}$ and $\{t(1-h) | t \in \{1, d\},\ h \in L_2 \setminus \{1\}\}$, respectively.

Now, if $\alpha = \sum_{g \in G} a_g g \in RG\widehat{H}$, taking a transversal τ of H in G we can rewrite α as

$$\alpha = \sum_{t \in \tau} \alpha_t t \widehat{H}. \tag{10}$$

Since $\widehat{H}$ is central, it is a sum of centrally primitive idempotents called its *constituents*. Suppose that e is a constituent of $\widehat{H}$. Since $RGe \subset RG\widehat{H}$, we have that $\alpha \in RGe$ implies that α is of the form Equation (10). In terms of coding theory, this means that the code given by the minimal ideal RGe is a repetition code. Note that, if $e \in RG$ is a centrally primitive idempotent then, for all $H \lhd G$, we have $e\widehat{H} = e$ or $e\widehat{H} = 0$. We shall concentrate on the case that $e\widehat{H} = 0$, for all $\{1\} \neq H \lhd G$.

Definition 2.1.1. Let G be a finite group and R a finite commutative ring for which RG is semisimple ring. A centrally primitive idempotent $e \in RG$ for which $e.\widehat{H} = 0$, for all $\{1\} \neq H \lhd G$, is an *essential idempotent*. A minimal ideal of RG is called an *essential ideal* if it is generated by an essential idempotent and *non essential* otherwise.

Example 2.1.4. The centrally primitive idempotents of $\mathbb{F}_5C_6$ are:

$$\begin{aligned} e_0 &= \widehat{C_6} \\ e_1 &= 1 + 4g + g^2 + 4g^3 + g^4 + 4g^5 \\ e_2 &= 2 + 4g + 4g^2 + 2g^3 + 4g^4 + 4g^5 \\ e_3 &= 2 + g + 4g^2 + 3g^3 + 4g^4 + g^5. \end{aligned}$$

Since

$$\begin{aligned} \widehat{H_1} &= e_0 + e_1 + e_2 + e_3 \\ \widehat{H_2} &= e_0 + e_1 \\ \widehat{H_3} &= e_0 + e_2 \end{aligned}$$

by Example 2.1.1, we get the constituents of $\widehat{H_1}$, $\widehat{H_2}$ and $\widehat{H_3}$. Notice that $e_0\widehat{H_2} = e_0$, $e_1\widehat{H_2} = e_1$, $e_2\widehat{H_3} = e_2$ and $e_3\widehat{H_2} = e_3\widehat{H_3} = 0$, so the primitive idempotent e_3 is the unique essential idempotent of $\mathbb{F}_5C_6$. In addition, we get that

$$\begin{aligned} 1 - \widehat{H_1} &= 0 \\ 1 - \widehat{H_2} &= e_2 + e_3 \\ 1 - \widehat{H_3} &= e_1 + e_3. \end{aligned}$$

Example 2.1.5. The centrally primitive idempotents of $\mathbb{F}_3D_4$ are:

$$\begin{aligned} e'_0 &= \widehat{D_4} \\ e'_1 &= 2 + a + 2a^2 + a^3 + 2b + ab + 2a^2b + a^3b \\ e'_2 &= 2 + a + 2a^2 + a^3 + b + 2ab + a^2b + 2a^3b \\ e'_3 &= 2 + 2a + 2a^2 + 2a^3 + b + ab + a^2b + a^3b \\ e'_4 &= 2 + a^2. \end{aligned}$$

With the notation of Example 2.1.2, we express $\widehat{K_i}$ $(0 \leq i \leq 6)$ as

$$\begin{aligned} \widehat{K_1} &= e'_0 + e'_1 + e'_2 + e'_3 + e'_4 \\ \widehat{K_2} &= e'_0 + e'_1 + e'_2 + e'_3 \\ \widehat{K_3} &= e'_0 + e'_3 \\ \widehat{K_4} &= e'_0 + e'_1 \\ \widehat{K_5} &= e'_0 + e'_2 \\ \widehat{K_6} &= e'_0. \end{aligned}$$

In addition, we have

$$\begin{aligned}
1-\widehat{K_1} &= 0\\
1-\widehat{K_2} &= e_4'\\
1-\widehat{K_3} &= e_1'+e_2'+e_4'\\
1-\widehat{K_4} &= e_2'+e_3'+e_4'\\
1-\widehat{K_5} &= e_1'+e_3'+e_4'\\
1-\widehat{K_6} &= e_1'+e_2'+e_3'+e_4'.
\end{aligned}$$

Since e_0', e_1', e_2', e_3' are constituents of $\widehat{K_2}$, we have $e_i'\widehat{K_2} = e_i'$, $0 \leq i \leq 3$. In addition, $e_4'\widehat{K}_j = 0$, for $2 \leq j \leq 6$, which implies that e_4' is the unique essential idempotent of $\mathbb{F}_3D_4$.

Example 2.1.6. With the notations of the example 2.1.3, we can use GAP to compute the centrally primitive idempotents of $\mathbb{F}_5S_4$

$$\begin{aligned}
f_0 &= \widehat{S_4};\\
f_1 &= -1+d+cd+abc^2d+c^2d+bcd+ad-a-b-ab-c+c^2\\
&\quad -bc^2-abc-abc^2-bc+abcd+ac^2d+abd+bc^2d-bd+acd;\\
f_2 &= 1+a+b+ab-3c-3c^2+3bc^2+3abc-3abc^2-3bc;\\
f_3 &= 2(3-d-cd-abc^2d-c^2d-bcd-ad-a-b-ab+abcd+ac^2d+abd+bc^2d+bd+acd);\\
f_4 &= 2(3+d+cd+abc^2d+c^2d+bcd+ad-a-b-ab-abcd-ac^2d-abd-bc^2d-bd-acd)
\end{aligned}$$

so, we can write $\widehat{L_1}$, $\widehat{L_2}$ and $\widehat{L_3}$ as:

$$\begin{aligned}
\widehat{L_1} &= f_0+f_1+f_2+f_3+f_4;\\
\widehat{L_2} &= f_0+f_1;\\
\widehat{L_3} &= f_0+f_1+f_2.
\end{aligned}$$

Furthermore, we can compute the idempotents

$$\begin{aligned}
1-\widehat{L_1} &= 0;\\
1-\widehat{L_2} &= f_2+f_3+f_4;\\
1-\widehat{L_3} &= f_3+f_4.
\end{aligned}$$

As f_0, f_1 and f_2 are constituients of $\widehat{L_3}$, we have $f_i\widehat{L_3} = f_i$ for $0 \leq i \leq 2$. Since $f_3\widehat{L_j} = 0 = f_4\widehat{L_j}$ for $j = 2, 3$, we have that f_3 and f_4 are essential idempotents of $\mathbb{F}_5S_4$.

We shall now highlight some results about essential idempotents in the case when $R = \mathbb{F}$ is a finite field.

Proposition 2.1.2. *[8, Proposition 2.3] Let $e \in \mathbb{F}G$ be a centrally primitive idempotent. Then e is essential if and only if the map $\pi : G \to Ge$, $g \mapsto ge$, is an isomorphism of groups.*

Theorem 2.1.3. *[8, Corollary 2.4] If A is abelian and $\mathbb{F}A$ contains an essential idempotent, then A is cyclic.*

Corollary 2.1.4. *[8, Corollary 2.5] Let A be an abelian group non-cyclic. Then, for every finite field $\mathbb{F}$, every minimal code of $\mathbb{F}A$ is a repetition code.*

On the other hand, we also know that if G is a cyclic group, then $\mathbb{F}G$ always contains an essential idempotent.

We shall show that similar results hold when G is a finite nilpotent group and $\mathbb{F}$ a finite field for which $\mathbb{F}G$ is a semisimple. We begin with the p-group case.

Lemma 2.1.5. *Let G be a p-group. Then G contains only one minimal normal subgroup if and only if $\mathcal{Z}(G)$ is cyclic.*

Proof. Let us first prove that every minimal normal subgroup is a central subgroup. Let $\{1\} \neq H$ be a normal minimal subgroup of G. Since G is nilpotent, $G = \mathcal{Z}_n(G)$ for some index n, there exists an index i which is the least positive integer such that $H \cap \mathcal{Z}_i(G) \neq \{1\}$. Then $[H \cap \mathcal{Z}_i(G), G] \subset H \cap \mathcal{Z}_{i-1}(G) = \{1\}$ and thus $H \cap \mathcal{Z}_i(G) \subset H \cap \mathcal{Z}(G)$. Since H is a minimal normal subgroup and $\{1\} \neq H \cap \mathcal{Z}(G) \subset H$ is normal, it follows that $H = H \cap \mathcal{Z}(G)$, i.e. $H \subset \mathcal{Z}(G)$.

Assume, by way of contradiction, that $\mathcal{Z}(G)$ is not cyclic. Then, there are H and K two different minimal subgroups of $\mathcal{Z}(G)$. However, H and K are minimal normal subgroups of G, a contradiction. Conversely, since every minimal normal subgroup of G is a minimal subgroup of $\mathcal{Z}(G)$, if $\mathcal{Z}(G)$ is cyclic, then G contains only one minimal normal subgroup. □

The results in [8] can be extended as follows.

Proposition 2.1.6. *If G is a p-group whose center is cyclic then $\mathbb{F}G$ contains at least one essential idempotent.*

Proof. Let G be a p-group whose center is cyclic. Then, G has a unique minimal normal subgroup H of order p. In this case, take $e_0 = 1 - \widehat{H} \neq 0$. Since H is normal in G it

follows that e_0 is a central idempotent of $\mathbb{F}G$, thus $e_0 = \sum_i e_i$, where e_i are centrally primitive idempotents of $\mathbb{F}G$. Let $\{1\} \neq K$ be a normal subgroup of G. Since H is the unique minimal normal subgroup of G, we have $H \subset K$ which implies that $e_0\widehat{K} = 0$. Then $e_i\widehat{K} = e_ie_0\widehat{K} = 0$, for all e_i. Since $e_0 \neq 0$ we have that G has at least one essential idempotent. □

Let G be a nilpotent group and let $\mathcal{F}$ be the family of all minimal normal subgroups of G. For a field $\mathbb{F}$ such that $char(\mathbb{F}) \nmid |G|$, we define

$$e(G) = \prod_{K \in \mathcal{F}} (1 - \widehat{K}) \in \mathbb{F}G.$$

Lemma 2.1.7. *With the notation above, $e(G)$ is the sum of all the essential idempotents of $\mathbb{F}G$.*

Proof. Let e be a minimal central idempotent of $\mathbb{F}G$. If e is essential, we have:

$$e.e(G) = \prod_{K \in \mathcal{F}} e(1 - \widehat{K}) = \prod_{K \in \mathcal{F}} e = e.$$

On the other hand, if e is not essential, there exists a normal subgroup H in G such that $e\widehat{H} = e$. If K is a minimal normal subgroup of G contained in H we have

$$e(1 - \widehat{K}) = e\widehat{H}(1 - \widehat{K}) = e\widehat{H} - e\widehat{H}\widehat{K} = e\widehat{H} - e\widehat{H} = 0.$$

Consequently, $e.e(G) = 0$.

Since a minimal central idempotent e is a constituent of a central idempotent f if and only if $ef = e$, the result follows.

□

We are now ready to extend Theorem 2.1.3 to the case when G is nilpotent.

Theorem 2.1.8. *Let $G = P_1 \cdots P_r$ be a nilpotent group with cyclic center in which P_i is the Sylow p_i-subgroup of G, $1 \leq i \leq r$. Suppose that e is a centrally primitive idempotent of $\mathbb{F}G$. Then, $e \in \mathbb{F}G$ is an essential idempotent if and only if $e.e(G) = e$.*

Proof. Let $e \in \mathbb{F}G$ be an essential idempotent. Then, by the Lemma above, it follows that $e.e(G) = e$.

Conversely, assume, by way of contradiction, that we have $e.e(G) = e$ but e is non essential. Then, there exists a normal subgroup H of G such that $e\widehat{H} = e$. Moreover, for any minimal normal subgroup $K_i \subset H$ we have $\widehat{H}(1 - \widehat{K_i}) = 0$. Consequently, $e(G)\widehat{H} = 0$ and

$$e.e(G) = (e.\widehat{H}).e(G) = e.(\widehat{H}.e(G)) = 0$$

a contradiction. □

Example 2.1.7. Using the notation of examples 2.1.4, 2.1.5 and 2.1.6, we have that H_2, H_3 are the minimal normal subgroups of C_6; K_2 is the unique minimal normal subgroup of D_4; L_3 is the unique minimal normal subgroup of S_4. Taking into account the previous examples, we get

$$\begin{aligned} e(C_6) &= (1-\widehat{H_2})(1-\widehat{H_3}) = e_3; \\ e(D_4) &= 1-\widehat{K_2} = e_4'; \\ e(S_4) &= 1-\widehat{L_3} = f_3+f_4. \end{aligned}$$

$$\begin{aligned} e_3.e(C_6) &= e_3; \\ e_4'.e(D_4) &= e_4'; \\ f_3.e(S_4) &= f_3; \\ f_4.e(S_4) &= f_4. \end{aligned}$$

Theorem 2.1.9. *Let G be a finite nilpotent group and $\mathbb{F}$ a field with characteristic relatively prime with the order of G. Then $\mathbb{F}G$ contains at least one essential idempotent if and only if the center of G is cyclic.*

Proof. Let G be a nilpotent group with cyclic center and order $m = \prod_{i=1}^{r} p_i^{\alpha_i}$, where p_i are prime rational integers, $1 \leq i \leq r$. Then, G is the product of their Sylow subgroups P_i, where $1 \leq i \leq r$. For each i there exists a unique minimal normal subgroup K_i of P_i. In this case

$$e(G) = (1-\widehat{K_1}) \cdots (1-\widehat{K_r}).$$

Since K_i is a minimal normal subgroup of G, we have $K_i \subset \mathcal{Z}(G)$. Therefore, K_i is also a cyclic group. Without loss of generality we can assume $K_i =< a_i >$ of order p_i. As $\mathbb{F}G$ is semisimple, the order of G is invertible in $\mathbb{F}$, hence $p_1, \cdots, p_r$ are invertible too. Thus

$$e(G) = \left(1 - \frac{1 + a_1 + \cdots a_1^{p_1-1}}{p_1}\right) \cdots \left(1 - \frac{1 + a_r + \cdots a_r^{p_r-1}}{p_r}\right).$$

Notice that the coefficient of $a_1 \cdots a_r$ is $(-1)^r(1/p_1)\cdots(1/p_r) \neq 0$. We conclude that $e(G) \neq 0$. Consequently, its constituents are essential idempotents in $\mathbb{F}G$.

Conversely, when G is a finite nilpotent group with non-cyclic center, we have, by [21, Lemma 2.2], that $e(G) = 0$. Consequently, $\mathbb{F}G$ contains no essential idempotents.

□

2.2 GROUP CODES EQUIVALENCE

Let G_1 and G_2 be two groups of the same order. Let R be a ring with unity and $\gamma : G_1 \to G_2$ a bijection. Denote by $\overline{\gamma} : RG_1 \to RG_2$ the linear extension of γ. Clearly, $\overline{\gamma}$ is a Hamming isometry, i.e., elements corresponding under this map have the same Hamming weight. Two codes $I_1 \subset RG_1$ and $I_2 \subset RG_2$ such that $\overline{\gamma}(I_1) = I_2$ are said to be *permutation equivalent*.

Remark. *Note that, the last definition given above is essentially the same as in Section 1.6 in case of group algebras.*

Example 2.2.1. As a consequence of example 2.1.5 we get that 1 - $\widehat{K_2} = e_4' = 2 + a^2$ is an essential idempotent. Now, consider $I_1 = (\mathbb{F}_3 D_4)e_4' = \Delta(D_4, K_2)$ with basis

$$\mathcal{B}_1 = \{1 - a^2, b - a^2 b, a - a^3, ab - a^3 b\}$$

over $\mathbb{F}_3$ and $I_2 = \mathbb{F}_3 C_8(1 - \widehat{H}) = \Delta(C_8, H)$, where $H =< g^4 > \subset C_8$, with basis

$$\mathcal{B}_2 = \{1 - g^4, g - g^5, g^2 - g^6, g^3 - g^7\}$$

over $\mathbb{F}_3$. Let us define $\gamma : D_4 \to C_8$ by

$$\begin{aligned} \gamma(1) &= 1 & \gamma(b) &= g \\ \gamma(a) &= g^2 & \gamma(ab) &= g^3 \\ \gamma(a^2) &= g^4 & \gamma(a^2 b) &= g^5 \\ \gamma(a^3) &= g^6 & \gamma(a^3 b) &= g^7. \end{aligned}$$

Because $\gamma(\mathcal{B}_1) = \mathcal{B}_2$, we have $\gamma(I_1) = I_2$. So, we conclude that the essential code I_1 is permutation equivalent to the cyclic code I_2.

More generally, the codes C_1 and C_2 are said to be *monomially equivalent* if there exists a monomial transformation T (See chapter 1) such that $T(C_1) = C_2$. It is straightforward to verify that if two codes are permutation equivalent then these codes are monomially equivalent. By [30], there exists a nilpotent code which is not monomially equivalent to an abelian code. Hence, by the remark above, there exists a nilpotent code which is not permutation equivalent to an abelian code.

Given an arbitrary finite semisimple group algebra $\mathbb{F}G$, we are now ready to determine sufficient conditions for ideals in $\mathbb{F}G$ and abelian codes to be permutation equivalent.

It is well know that all ideals in a group algebra $\mathbb{F}G$ are to be permutation equivalent to abelian codes whenever G has an abelian decomposition, i.e., $G = AB$, where A and B are abelian subgroups of G. We shall determine another sufficient condition for permutation equivalence between ideals and abelian codes.

Theorem 2.2.1. *Let G be a finite group of order n and $\mathbb{F}$ a finite field. If $e \in \mathbb{F}G$ is an idempotent such that $e\widehat{H} = e$ for some non-trivial subgroup H of G, then $\mathbb{F}Ge$ is permutation equivalent to an abelian code.*

Proof. Let $I = \mathbb{F}Ge$. Since $e\widehat{H} = e$, it follows that $I \subseteq \mathbb{F}G\widehat{H}$. Let $\{v_1, \cdots, v_t\}$ be a basis of I over $\mathbb{F}$, $\{x_i\}_{i=1}^{r}$ a transversal of H in G and $m = |H|$. Since $\{x_1\widehat{H}, x_2\widehat{H}, \cdots x_r\widehat{H}\}$ is a basis of $\mathbb{F}G\widehat{H}$, we have

$$v_i = \sum_j a_{ij} x_j \widehat{H}, \quad a_{ij} \in \mathbb{F},$$

for all $1 \leq i \leq t$.

Suppose that $G = \{g_1, g_2, \cdots, g_n\}$ with $n = mr$ and

$$x_i H = \{g_{(i-1)m+1}, g_{(i-1)m+2}, \cdots, g_{im}\}.$$

So, if we fix the m-cycle $\sigma_i = ((i-1)m+1, (i-1)m+2, \cdots, im) \in S_n$, $1 \leq i \leq r$, we have $\sigma_i(v_j) = v_j$ for all $1 \leq j \leq t$. This implies that $\sigma_i \in PAut(I)$ and consequently $A = \langle \sigma_1, \sigma_2, \cdots, \sigma_r \rangle \subseteq PAut(I)$. Since the m-cycles σ_i, $1 \leq i \leq r$, are disjoint, we have that A is an abelian group. In addition, as

$$A \cong \underbrace{C_m \times \cdots \times C_m}_{\text{r times}}$$

we have $|A| = n = |G|$.

We shall show now that A is a regular subgroup of S_n. Let $\sigma \in A$. Then

$$\sigma(i) = \begin{cases} i+1, & \text{if } m \text{ does not divide } i \\ i-m+1, & \text{if } m \text{ divides } i. \end{cases}$$

Thus, $\sigma(i) \neq i$ for all $i \in \{1, 2, \cdots, n\}$; so we conclude that A is a regular subgroup of S_n. It follows by Theorem 1.6.2 that $\mathbb{F}Ge$ is permutation equivalent to a left A-code. Since $\mathbb{F}A$ is commutative, we have that $\mathbb{F}Ge$ is actually equivalent to an abelian code.

□

Remark. *In the proof of the last theorem, we could have used the second part of Theorem 1.6.2; we only need to compute $C_{S_n}(A)$. Notice that*

$$\begin{aligned}\sigma^{-1}\sigma_i\sigma = \sigma_i &\Leftrightarrow (\sigma((i-1)m+1),\cdots,\sigma(im)) = ((i-1)m+1,\cdots,im)\\ &\Leftrightarrow \sigma\big|_{\{(i-1)m+1,\cdots,im\}} = \sigma_i^{\ell_i}\\ &\Leftrightarrow \sigma = \sigma_1^{\ell_1}\cdots\sigma_r^{\ell_r}\end{aligned}$$

for all $\sigma \in C_{S_n}(A)$. Then $A = C_{S_n}(A)$.

In [8], it was shown that every minimal abelian code is permutation equivalent to a minimal cyclic code. In what follows, we wish to find sufficient conditions on ideals of an arbitrary finite semisimple group algebra which guarantee that they are monomially equivalent to cyclic codes.

Lemma 2.2.2. *Let I be an ideal of the group algebra $\mathbb{F}G$ of dimension t. If I contains a basis $\{u_i\}_{i=1}^t$ whose elements have disjoint support, then there exists $g_1,\cdots,g_t \in G$ such that the elements $g_1u_1,\cdots,g_tu_1$ have disjoint support and form a basis of I.*

Proof. We may assume, without loss of generality, that $|Supp(u_1)| = \min\{|Supp(u_i)| : 1 \leq i \leq t\}$. Since $\{gu_1,\cdots,gu_t\}$ is basis of I with $Supp(gu_i) \cap Supp(gu_j) = \emptyset$, whenever $i \neq j$, we assume that $1 \in Supp(u_1)$. Set $g_1 = 1$, $g_i \in Supp(u_i)$, $2 \leq i \leq t$. For $1 \leq i \leq t$, we have

$$g_iu_1 = \sum_{j=1}^{t} a_ju_j.$$

As $g_i \in Supp(g_iu_1) \cap Supp(u_i)$, we have $a_i \neq 0$. From the minimality of $|Supp(g_iu_1)| = |Supp(u_1)|$ and from the fact that u_i, $1 \leq i \leq t$, have disjoint support, it follows that $g_iu_1 = a_iu_i$.

□

For $\sigma \in S_n$ we consider the permutation matrix $[\sigma] \in M_n(\mathbb{F})$ defined by

$$[\sigma]_{ij} = \begin{cases} 1, & \text{if } j = \sigma(i)\\ 0, & \text{otherwise.}\end{cases}$$

Lemma 2.2.3. *Let $\lambda_1,\cdots,\lambda_n \in \mathbb{F}$ and $\pi \in S_n$. Then*

$$[\pi].Diag(\lambda_1,\cdots,\lambda_n) = Diag(\lambda_{\pi(1)},\cdots,\lambda_{\pi(n)}).[\pi].$$

Proof. Assume that $A = [\pi].Diag(\lambda_1, \cdots, \lambda_n)$ and $B = Diag(\lambda_{\pi(1)}, \cdots, \lambda_{\pi(n)})[\pi]$. Since the entries of A and B are

$$[A]_{ij} = \begin{cases} \lambda_j, & j = \pi(i) \\ 0, & \text{otherwise} \end{cases}$$

and

$$[B]_{ij} = \begin{cases} \lambda_{\pi(i)}, & j = \pi(i) \\ 0, & \text{otherwise} \end{cases}$$

respectively, we conclude that $A = B$. □

Theorem 2.2.4. *Let G be a finite group of order n and let $\mathbb{F}$ be a finite field. Suppose that $I \neq (0)$ is a code in $\mathbb{F}G$ with dimension t and basis whose elements have disjoint support. Then, I is monomially equivalent to a cyclic code.*

Proof. Let $\{u_i\}_{i=1}^t$ be a basis of I whose elements have disjoint support. By Lemma 2.2.2, the code I contains a basis of the form $v_1 = g_{i_1}u_1, ..., v_t = g_{i_t}u_1$ for some $g_{i_j} \in G$, $1 \leq j \leq t$. Since $I \neq (0)$ there exists $0 \neq \alpha \in I$. Then, for $g \in supp(\alpha)$ we have that $h \in supp(hg^{-1}\alpha)$, for all $h \in G$. Since $hg^{-1}\alpha \in I$, it follows that $G = \cup_{i=1}^t supp(v_i)$. So, the subsets $supp(v_j)$ form a partition of G, because are disjoint sets. As $v_j = g_{i_j}u_1$, we have, for $1 \leq j \leq t$, that $supp(v_j)$ are sets of equal cardinality $m = n/t$. Then we enumerate the elements of G so that we can write

$$\begin{array}{rcl} supp(v_1) & = & \{g_1, \ g_{t+1}, \ g_{2t+1}, \ \cdots, \ g_{(m-1)t+1} \ \} \\ supp(v_2) & = & \{g_2, \ g_{t+2}, \ g_{2t+2}, \ \cdots, \ g_{(m-1)t+2} \ \} \\ supp(v_3) & = & \{g_3, \ g_{t+3}, \ g_{2t+3}, \ \cdots, \ g_{(m-1)t+3} \ \} \\ & \vdots & \\ supp(v_t) & = & \{g_t, \ g_{2t}, \ g_{3t}, \ \cdots, \ g_{mt} \ \} \end{array}$$

and thus $v_i = \sum_{j=0}^{m-1} a_{j+1} g_{jt+i}$, with $a_i \in \mathbb{F}$.

We can define an action of S_n on G by $\tau.g_i = g_{\tau(i)}$, for all $\tau \in S_n$, and extend linearly to $\mathbb{F}G$. Take the n-cycle $\sigma = (1, 2, \cdots, n) \in S_n$. Set

$$\mathrm{M} = \left(\begin{array}{ccccc|ccccc|c|ccccc} a_m^{-1}a_1 & 0 & 0 & \cdots & 0 & & & & & & & & & & \\ 0 & 1 & 0 & \cdots & 0 & & & & & & & & & & \\ \vdots & \vdots & \vdots & \vdots & \vdots & & & & & & & & & & \\ 0 & 0 & 0 & \cdots & 1 & & & & & & & & & & \\ \hline & & & & & a_2^{-1}a_3 & 0 & 0 & \cdots & 0 & & & & & \\ & & & & & 0 & 1 & 0 & \cdots & 0 & & & & & \\ & & & & & \vdots & \vdots & \vdots & \vdots & \vdots & & & & & \\ & & & & & 0 & 0 & 0 & \cdots & 1 & & & & & \\ \hline & & & & & & & & & & \ddots & & & & \\ \hline & & & & & & & & & & & a_{m-1}^{-1}a_m & 0 & 0 & \cdots & 0 \\ & & & & & & & & & & & 0 & 1 & 0 & \cdots & 0 \\ & & & & & & & & & & & \vdots & \vdots & \vdots & \vdots & \vdots \\ & & & & & & & & & & & 0 & 0 & 0 & \cdots & 1 \end{array}\right).$$

As M is a diagonal matrix, we can identify $M.\sigma = M.[\sigma] \in GL_n(\mathbb{F})$ with the element $(\lambda_1, \cdots, \lambda_m).\sigma$ in the group $(\mathbb{F}^*)^n \rtimes S_n$, where $(\lambda_1, \cdots, \lambda_m)$ is the diagonal of M.

Since $(M.[\sigma]^{-1})v_i = v_{i+1}$ for $1 \leq i \leq t-1$ and $(M.[\sigma]^{-1})v_t = v_1$, we have $M.[\sigma]^{-1}(I) = I$ which implies that $M.[\sigma]^{-1} \in MAut(I)$. We claim that $M.[\sigma]^{-1}$ has order n. Notice that if $M = Diag(\lambda_1, \cdots, \lambda_n)$, then by Lemma 2.2.3, we have

$$[\sigma]^{-1}.M = Diag(\lambda_{\sigma^{-1}(1)}, \cdots, \lambda_{\sigma^{-1}(n)}).[\sigma]^{-1}.$$

Now, $(M[\sigma]^{-1})^n = \prod_{k=0}^{n-1} Diag(\lambda_{\sigma^{-k}(1)}, \cdots, \lambda_{\sigma^{-k}(n)})[\sigma]^{-n}$ and the entry ij is

$$\begin{cases} \prod_{k=0}^{n-1} \lambda_{\sigma^{-k}(i)}, & \text{if } i = j \\ 0, & \text{otherwise.} \end{cases}$$

Since $\prod_{k=0}^{n-1} \lambda_{\sigma^{-k}(i)} = (a_m^{-1}a_1)(a_1^{-1}a_2)\cdots(a_{m-1}^{-1}a_m) = 1$ for any $1 \leq i \leq n$, we have that $(M[\sigma]^{-1})^n$ is the identity matrix. As n is the order of $[\sigma]$, we conclude that $M[\sigma]^{-1}$ has order n.

Let $H = \langle M.\sigma \rangle \subseteq MAut(C)$ and $\phi : (\mathbb{F}^*)^n \rtimes S_n \to S_n$, $\phi(A.\pi) = \pi$ as defined in Equation (3). Since every n-cycle generates a transitive group, we have that $\phi(H) = \langle \sigma \rangle$

is a regular subgroup of S_n. By Theorem 1.6.3 (1), we conclude that I is monomially equivalent to a cyclic code. □

Now, assume that R is a commutative ring. Let K_1 and K_2 be normal subgroups of G_1 and G_2, respectively, where G_1 and G_2 are of the same order such that $G_1/K_1 \cong G_2/K_2$. Then

$$R[G_1/K_1] \cong R[G_2/K_2]$$

and

$$RG_1.\widehat{K_1} \cong R[G_1/K_1] \cong R[G_2/K_2] \cong RG_2\widehat{K_2}.$$

Denote by $\mu : R[G_1/K_1] \to R[G_2/K_2]$ the linear extension of the isomorphism $G_1/K_1 \cong G_2/K_2$ and denote by $\theta : RG_1.\widehat{K_1} \to RG_2\widehat{K_2}$ the corresponding isomorphism.

Let $\mathcal{T}_1 = \{g_1, \cdots, g_t\}$ be a transversal of K_1 in G_1. Choose any $\eta_i \in G_2$ such that $\eta_i K_2 = \mu(g_i K_1)$. Then $\mathcal{T}_2 = \{\eta_1, \cdots, \eta_t\}$ is a transversal of K_2 in G_2. Suppose that $f : K_1 \to K_2$ is a bijection. We can define a map $\eta : G_1 \to G_2$ by $\eta(g_i k) = \eta_i f(k)$, for all $g_i \in \mathcal{T}_1$ and $k \in K_1$.

If $\alpha \in RG_1.\widehat{K_1}$, then it follows from Equation (10) that

$$\alpha = \sum_{i=0}^{t-1} \alpha_i g_i \widehat{K_1}.$$

Then

$$\theta(\alpha) = \sum_{i=1}^{t} \alpha_i \eta_i \widehat{K_2} = \sum_{i=1}^{t} \alpha_i \eta_i \Big(\frac{1}{|K_2|} \sum_{k' \in K_2} k' \Big) = \frac{1}{|K_1|} \sum_{i=1}^{t} \alpha_i \eta_i \Big(\sum_{k \in K_1} f(k) \Big).$$

By comparing the expressions for α and $\theta(\alpha)$, we see that the linear extension $\overline{\eta} : RG_1 \to RG_2$ of η coincides with θ in $RG_1.\widehat{K_1}$.

Proposition 2.2.5. *Let K_1 and K_2 be normal subgroups of G_1 and G_2, respectively, where G_1 and G_2 have the same order and $G_1/K_1 \cong G_2/K_2$. If e_1 is an idempotent of RG_1 where $e_1 \in RG_1\widehat{K_1}$, then $RG_1.e_1$ is permutation equivalent to $RG_2.e_2$, with $e_2 = \theta(e_1)$.*

Proof. Since $RG_1.e_1 \subset RG_1\widehat{K_1}$, we have

$$\theta(RG_1.e_1) = \theta(RG_1\widehat{K_1})\theta(e_1) = RG_2\widehat{K_2}.e_2 = RG_2.e_2.$$

As η coincides with θ in $RG_1.e_1$, we conclude that $RG_1.e_1$ is permutation equivalent to $RG_2.e_2$, with $e_2 = \theta(e_1)$. □

Example 2.2.2. Let $G_1 = S_4$ and $K_1 = L_2$, where L_2 is the same as in example 2.1.3. Let $G_2 = C_{24} =< g >$ and $K_2 =< g^2 >$. Since $S_4/L_2 \cong C_{24}/K_2$, it follows that $(\mathbb{F}_5 S_4)\widehat{L_2} \cong (\mathbb{F}_5 C_{24})\widehat{K_2}$. Set $\tau_1 = \{1, d\}$ a transversal of L_2 in S_4 and $\tau_2 = \{1, g\}$ a transversal of K_2 in C_{24}. Consider $f : L_2 \to K_2$ a bijection between L_2 and K_2; define $\eta : S_4 \to C_{24}$ by $\eta(dh) = g.f(h)$ for all $h \in L_2$; take $\overline{\eta} : (\mathbb{F}_5 S_4)\widehat{L_2} \to (\mathbb{F}_5 C_{24})\widehat{K_2}$ the linear extension of η. By example 2.1.3, the set $\{\widehat{L_2}, d\widehat{L_2}\}$ is a basis of $(\mathbb{F}_5 S_4)\widehat{L_2}$ over $\mathbb{F}_5$. Then

$$\overline{\eta}(\alpha_1\widehat{L_2} + \alpha_2 d\widehat{L_2}) = \alpha_1\widehat{K_2} + \alpha_2 g\widehat{K_2}$$

for every $\alpha_1, \alpha_2 \in \mathbb{F}_5$. As $\{\widehat{K_2}, g\widehat{K_2}\}$ is a basis of $(\mathbb{F}_5 C_{24})\widehat{K_2}$, we conclude that $\overline{\eta} : (\mathbb{F}_5 S_4)\widehat{L_2} \to (\mathbb{F}_5 C_{24})\widehat{K_2}$ is bijective. In addition,

$$\begin{aligned}\overline{\eta}\left((\alpha_1\widehat{L_2} + \alpha_2 d\widehat{L_2})(\beta_1\widehat{L_2} + \beta_2 d\widehat{L_2})\right) &= \overline{\eta}\left((\alpha_1\beta_1 + \alpha_2\beta_2)\widehat{L_2} + (\alpha_1\beta_2 + \alpha_2\beta_1)d\widehat{L_2})\right) \\ &= (\alpha_1\beta_1 + \alpha_2\beta_2)\widehat{K_2} + (\alpha_1\beta_2 + \alpha_2\beta_1)g\widehat{K_2}) \\ &= (\alpha_1\widehat{K_2} + \alpha_2 d\widehat{K_2})(\beta_1\widehat{K_2} + \beta_2 g\widehat{K_2})\end{aligned}$$

which implies that $\theta = \overline{\eta} : (\mathbb{F}_5 S_4)\widehat{L_2} \to (\mathbb{F}_5 C_{24})\widehat{K_2}$ is an isomorphism of algebras over $\mathbb{F}_5$. Again, by the example 2.1.3, we have $\widehat{L_2} = e_0 + e_1$, where e_0, e_1 are centrally primitive idempotents. Since $e_1 \in (\mathbb{F}_5 S_4)\widehat{L_2}$ and can be expressed as

$$\begin{aligned}e_1 = &-1 + d + cd + abc^2d + c^2d + bcd + ad - a - b - ab - c + c^2 \\ &- bc^2 - abc - abc^2 - bc + abcd + ac^2d + abd + bc^2d - bd + acd,\end{aligned}$$

we obtain

$$\theta(e_1) = \overline{\eta}(e_1) = -\sum_{i=0}^{23}(-1)^i g^i = e_2,$$

where e_2 is an idempotent of $(\mathbb{F}_5 C_{24})\widehat{K_2}$. We conclude that $(\mathbb{F}_5 S_4)e_1$ is permutation equivalent to $(\mathbb{F}_5 C_{24})e_2$.

2.3 MINIMAL NILPOTENT CODES

In this section, we shall prove that every non essential centrally primitive idempotent generates a code which is permutation equivalent to an abelian code. In addition, we shall determine a condition on the given group so that every minimal nilpotent code is permutation equivalent to an abelian code.

Let G be a finite group and R a finite semisimple ring such that $|G|$ is invertible in R. Let $e \in RG$ be a centrally primitive idempotent. We define

$$K_e = \{g \in G : ge = e\}. \tag{11}$$

Notice that K_e is the kernel of the homomorphism of groups $\pi : G \to Ge$, $g \mapsto ge$. Thus

$$\frac{G}{K_e} \cong Ge.$$

The following Lemma will be a useful result.

Lemma 2.3.1. *Let $e \in RG$ be a centrally primitive idempotent and let K be a normal subgroup in G. Then $e.\widehat{K} = e$ if and only if $K \subset K_e$. Furthermore, if $K \not\subset K_e$ then $e.\widehat{K} = 0$.*

Proof. Assume that $e.\widehat{K} = e$. For any $k \in K$, we have $ek = e.\widehat{K}k = e.\widehat{K} = e$. Then $K \subset K_e$. Conversely, if $K \subset K_e$ then, for any $k \in K$, we have $ek = e$, which implies that $e.\widehat{K} = e$. Finally, if $K \not\subset K_e$ then $e.\widehat{K} \neq e$. As e is a centrally primitive idempotent, we conclude that $e.\widehat{K} = 0$. □

The following is Theorem 3.1 of [8] slightly generalized.

Theorem 2.3.2. *Let $e \neq \widehat{G}$ be a centrally primitive idempotent of RG and ψ the natural projection $\psi : RG\widehat{K_e} \to R[G/K_e]$, $g\widehat{K_e} \mapsto gK_e \in G/K_e$ for each $g \in G$. Then, the element $\psi(e)$ is an essential idempotent of $R[G/K_e]$.*

Proof. Since ψ is an isomorphism of rings, it follows that

$$\psi(e)^2 = \psi(e)\psi(e) = \psi(e^2) = \psi(e),$$

i.e., $\psi(e)$ is an idempotent of $R[G/K_e]$. If $\beta \in R[G/K_e]$ then $\beta = \psi(\alpha)$, for some $\alpha \in RG\widehat{K_e}$. It follows that $\beta.\psi(e) = \psi(\alpha.e) = \psi(e.\alpha) = \psi(e).\beta$ which implies that $\psi(e)$ is central. Suppose that $\psi(e) = f_1 + f_2$ expresses $\psi(e)$ as a sum of two orthogonal central idempotents of $R[G/K_e]$. Then $f_i = \psi(e_i)$, where e_i is an idempotent for $i = 1, 2$. Since e_1, e_2 are orthogonal idempotents, we have that $e_1 = 0$ or $e_2 = 0$, hence, $f_1 = 0$ or $f_2 = 0$. Now, we want to prove that $\psi(e)$ is essential. Assume that $\mathcal{K} = K/K_e$ is a non-trivial normal subgroup of G/K_e. Let T be a transversal of K_e in K. Then

$$\widehat{K} = \frac{1}{|K|}\sum_{k\in K} k = \frac{|K_e|}{|K|}\sum_{t\in T} t\widehat{K_e} = \frac{1}{|\mathcal{K}|}\sum_{t\in T} t\widehat{K_e}.$$

Thus, we have

$$\psi(\widehat{K}) = \frac{1}{|\mathcal{K}|}\sum_{t\in T}\psi(t\widehat{K_e}) = \frac{1}{|\mathcal{K}|}\sum_{t\in T} tK_e = \widehat{\mathcal{K}}.$$

Since $K \not\subset K_e$, by Lemma 2.3.1 we conclude

$$\psi(e).\widehat{\mathcal{K}} = \psi(e)\psi(\widehat{K}) = \psi(e\widehat{K}) = 0.$$

□

Example 2.3.1. Let Q_8 be the quaternion group with presentation

$$< a, b | a^4 = 1. b^2 = a^2, bab^{-1} = a^{-1} > .$$

Consider $G = C_2 \times Q_8$ with $C_2 = \{1, g\}$. The centrally primitive idempotents of $\mathbb{F}_3 G$ not associated to linear characters are

$$e_1 = (1+g) - (1+g)a^2$$
$$e_2 = (1-g) - (1-g)a^2.$$

Note that $K_{e_1} = \{x \in G : xe_1 = e_1\} = \{1, g\}$ and $K_{e_2} = \{x \in G : xe_2 = e_2\} = \{1, ga^2\}$. If we consider $\psi_i : \mathbb{F}_3 G\widehat{K_{e_i}} \to \mathbb{F}_3[G/K_{e_i}]$ with $i = 1, 2$, then $\psi_1(e_1) = 2(1-a^2)K_{e_1}$ and, since $ga^2K_{e_2} = K_{e_2}$ and $gK_{e_2} = a^2K_{e_2}$, we have $\psi_2(e_2) = 2(1-a^2)K_{e_2}$. In both cases, we have that $G/K_{e_i} \cong Q_8$, with $i = 1, 2$. As $2(1-a^2) \in \mathbb{F}_3 Q_8$ is an essential idempotent (unique in this case) we have that $\psi_1(e_1)$ and $\psi_2(e_2)$ are essential idempotents.

Now, let us take $R = \mathbb{F}_3 C_2$ instead of $\mathbb{F}_3$. As $RQ_8 \cong \mathbb{F}_3 G$, we have the same centrally primitive idempotents. In addition, since

$$\tilde{K}_{e_1} = \{x \in Q_8 : xe_1 = e_1\} = \{1\} = \{x \in Q_8 : xe_2 = e_2\} = \tilde{K}_{e_2}$$

we conclude that e_1 and e_2 are essential idempotents of RQ_8.

Corollary 2.3.3. *Let $e \neq \widehat{G}$ be a centrally primitive idempotent of RG. Then, the group G/K_e has cyclic center.*

Proof. By the last theorem, we have that $R[G/K_e]$ contains an essential idempotent. It follows from Theorem 2.1.9 that G/K_e is cyclic. □

It was proved in [8] that every minimal abelian code is permutation equivalent to a cyclic code. The main idea of the proof is, for every minimal idempotent e of the abelian group algebra $\mathbb{F}A$, to consider a cyclic group C which has the same order as A and a

subgroup H of C such that $A/K_e \cong C/H$. Now, if we want to use the same argument for a nilpotent group G, we shall need that, for any centrally primitive idempotent $e \in \mathbb{F}G$, there exists a nilpotent group N with cyclic center and a subgroup H of N for which $G/K_e \cong N/H$. However, as the next example shows, the same does not happen necessarily with the nilpotent groups.

Example 2.3.2. Consider the group $G = C_4 \rtimes C_4$ with presentation

$$G =< a, b | a^4 = b^4 = 1, bab^{-1} = a^{-1} >$$

and center $\mathcal{Z}(G) = \{1, a^2, b^2, a^2b^2\}$. The element $e = 2 + 5b^2 + 5a^2 + 2a^2b^2 \in \mathbb{F}_7G$ is a central idempotent. Notice that

$$a^ib^je = \begin{cases} a^{i \bmod 2}b^{j \bmod 2}e, & \text{if } i,j = 0,1 \\ 6a^{i \bmod 2}b^{j \bmod 2}e, & \text{if } i = 0,1 \text{ and } j = 2,3 \\ 6a^{i \bmod 2}b^{j \bmod 2}e, & \text{if } i = 2,3 \text{ and } j = 0,1 \\ a^{i \bmod 2}b^{j \bmod 2}e, & \text{if } i,j = 2,3. \end{cases}$$

Then, $\mathbb{F}_7Ge$ is generated by the set $\mathcal{B} = \{e, ae, be, abe\}$ as a $\mathbb{F}$-vector space. Since e, ae, be, abe have disjoint support we have that $\mathcal{B}$ is a basis of $\mathbb{F}_7Ge$. It follows from

$$(ae)(be) = 2ab + 5a^3b + 5ab^3 + 2a^3b^3 \neq 2 + 5a^2 + 5b^2 + 2a^3b = (be)(ae)$$

that $\mathbb{F}_7Ge \cong M_2(\mathbb{F}_7)$ implying that e is a centrally primitive idempotent. Note that $K_e = \{g \in G | ge = e\} = \{1, a^2b^2\}$ and $G/K_e \cong Q_8$ the quaternion group of order 8. By [13] there exists six groups of order 16 with cyclic center:

$$\begin{aligned} &C_{16} = \langle g \rangle; \\ &D_8 = \langle a, b | a^8 = b^2 = 1, bab = a^{-1} \rangle; \\ &Q_{16} = \langle a, b | a^8 = 1, b^2 = a^4, bab^{-1} = a^{-1} \rangle; \\ &SD_{16} = \langle a, b | a^8 = b^2 = 1, bab = a^3 \rangle; \\ &M_4(2) = \langle a, b | a^8 = b^2 = 1, bab = a^5 \rangle; \\ &C_4 \circ D_4 = \langle a, b, c | a^4 = c^2 = 1, b^2 = a^2, ab = ba, ac = ca, cbc = a^2b \rangle. \end{aligned}$$

It follows from Lemma 2.1.5 that there exist a unique minimal normal subgroup in each of these subgroups. The correspondent factor group are isomorphic to

$$C_8,\ D_4,\ D_4,\ D_4,\ C_2 \times C_4,\ C_2^3,$$

respectively. Then, it is not possible to find a group N of order 16 with cyclic center and a subgroup H for which $G/K_e \cong N/H$. However, since the elements of $\mathcal{B}$ have disjoint supports of the same cardinality, by the Theorem 2.2.4, we conclude that $\mathbb{F}Ge$ is monomially equivalent to a cyclic code.

As the previous example suggests, it will be of interest to determine when minimal nilpotent codes are equivalent to abelian codes. The following theorem is an answer to this question.

Theorem 2.3.4. *Let $e \in \mathbb{F}G$ be a non essential centrally primitive idempotent. Then $\mathbb{F}Ge$ is permutation equivalent to an abelian code.*

Proof. Since e is non essential idempotent, it follows that $K_e \neq \{1\}$. By Lemma 2.3.1, we have that $e\widehat{K_e} = e$ and by Theorem 2.2.1 we conclude that $\mathbb{F}Ge$ is permutation equivalent to an abelian code. □

Corollary 2.3.5. *If G is a finite nilpotent group which has a non-cyclic center, then every minimal code in $\mathbb{F}G$ is permutation equivalent to an abelian code.*

Proof. Let e be a centrally primitive idempotent of $\mathbb{F}G$. Since the center of G is non-cyclic, we have that e is a non essential idempotent. Then the result follows from Theorem 2.3.4. □

In Theorem 2.2.4, we determined a sufficient condition for a code to be monomially equivalent to a cyclic code. Now, we shall present a sufficient condition for a code to be permutation equivalent to a cyclic code depending on the group structure. For every element g in a group G, denote by C_g^+ the sum of the elements of the G-conjugacy class of g, i.e.,

$$C_g^+ = \sum_{h \in C_g} h.$$

We begin with the following result of [21].

Lemma 2.3.6. *[21, Lemma 2.3] Let G be a finite group and $g \in G$. If $g^{-1}C_g \cap \mathcal{Z}(G) \neq \{1\}$, then G contains a central element z of prime order so that $C_g^+ = C_g^+\widehat{z}$.*

Let G be a finite nilpotent group and let $e \in \mathbb{F}G$ be a centrally primitive idempotent. Let $\tilde{G}$ be the subgroup of G such that $\tilde{G}/K_e = \mathcal{Z}(G/K_e)$. We already know that $\tilde{G}/K_e$ is cyclic.

Lemma 2.3.7. *If G/K_e is nilpotent of class $c \leq 2$, then $Supp(e) \subset \tilde{G}$.*

Proof. If $c = 1$ then G/K_e is cyclic and we are done. Now, assume that $c = 2$. Let $\mathcal{C}$ be the full set of representatives of the conjugacy classes of G/K_e. Let $\bar{e}$ be the image of e by $\psi : \mathbb{F}G \to \mathbb{F}(G/K_e)$, ψ the linear extension of the projection $G \to G/K_e$. From Theorem 2.3.2, it follows that $\bar{e}$ is an essential idempotent, in particular, a centrally primitive idempotent. Since $\tilde{G}/K_e = \mathcal{Z}(G/K_e)$, we can write

$$\bar{e} = \sum_{\bar{g} \in \tilde{G}/K_e} \beta_g \bar{g} + \sum_{\bar{g} \in \mathcal{C} \setminus (\tilde{G}/K_e)} \beta_g C_{\bar{g}}^+$$

where $C_{\bar{g}}$ denote the conjugacy class of $\bar{g} \in G/K_e$ and $\beta_g \in \mathbb{F}$ for $\bar{g} \in \mathcal{C}$.

Again, as $\tilde{G}/K_e = \mathcal{Z}(G/K_e) \neq G/K_e$, we have that, for any $\bar{g} \in \mathcal{C} \setminus (\tilde{G}/K_e)$, there exists an $\bar{x} \in G/K_e$ such that $\bar{1} \neq [\bar{g}, \bar{x}] \in \bar{g}^{-1} C_{\bar{g}} \cap \mathcal{Z}(G/K_e)$. So, by the previous Lemma, there exists $\omega_g \in \mathcal{Z}(G/K_e)$ of prime order such that $C_{\bar{g}}^+ = C_{\bar{g}}^+ . \widehat{\omega_g}$. Then, we can rewrite $\bar{e}$ as

$$\bar{e} = \sum_{\bar{g} \in \tilde{G}/K_e} \beta_g \bar{g} + \sum_{\bar{g} \in \mathcal{C} \setminus (\tilde{G}/K_e)} \beta_g C_{\bar{g}}^+ . \widehat{\omega_g}.$$

Since $\bar{e} \in \mathbb{F}(G/K_e)$ is an essential idempotent, it follows from Theorem 2.1.8 that $\bar{e}.e(G/K_e) = \bar{e}$. As every minimal normal subgroup of G/K_e is central, we have that $e(G/K_e) \in \mathbb{F}(\tilde{G}/K_e)$. Then

$$\begin{aligned} \bar{e} = \bar{e}.e(G/K_e) &= \sum_{\bar{g} \in \tilde{G}/K_e} \beta_g \bar{g}.e(G/K_e) + \sum_{\bar{g} \in \mathcal{C} \setminus (\tilde{G}/K_e)} \beta_g C_{\bar{g}}^+ . \widehat{\omega_g}.e(G/K_e) \\ &= \sum_{\bar{g} \in \tilde{G}/K_e} \beta_g \bar{g}.e(G/K_e) \end{aligned}$$

because $\widehat{\omega_g}.e(G/K_e) = 0$, for all $\bar{g} \in \mathcal{C} \setminus (\tilde{G}/K_e)$. By the last formula we conclude that $\bar{e} \in \mathbb{F}(\tilde{G}/K_e)$. We can express $e = \alpha + \beta$, where $Supp(\alpha) \subset \tilde{G}$ and $Supp(\beta) \subset G \setminus \tilde{G}$. Then, $\bar{e} = \overline{\alpha} + \overline{\beta}$, which implies, by comparing the support, that $\overline{\beta} = \overline{0}$. As the kernel of $\psi : \mathbb{F}G \to \mathbb{F}(G/K_e)$ is $\mathbb{F}G(1 - \widehat{K_e})$, we have that $\beta \in \mathbb{F}G(1 - \widehat{K_e})$ and so, $\beta \widehat{K_e} = 0$. Since $e\widehat{K_e} = e$, it follows that $\alpha + \beta = \alpha \widehat{K_e} \in \mathbb{F}\tilde{G}$. Then $\beta = 0$.

□

Now we are ready to prove the following result.

Theorem 2.3.8. *Let G be a finite nilpotent group of order n and $e \in \mathbb{F}G$ be a centrally primitive idempotent such that G/K_e of class $c \leq 2$. Then every code $C \subset \mathbb{F}G$ is permutation equivalent to a cyclic code C' in $\mathbb{F}C_n$.*

Proof. By last Lemma, we have $Supp(e) \subset \tilde{G}$. Then $e \in \mathbb{F}\tilde{G}$ and $\tilde{G}/K_e$ is cyclic. By Theorem 2.2.5 we have that $\mathbb{F}\tilde{G}e$ is permutation equivalent to a code in $\mathbb{F}C_m e'$, where $m = |\tilde{G}|$ and e' is an idempotent. Let $\psi : \mathbb{F}\tilde{G}e \to \mathbb{F}C_m e'$ be an isometry and $\tau_1 = \{g_1, \cdots, g_t\}$ a transversal of $\tilde{G}$ in G. Let C_n be a cyclic group of order $n = |G|$ and let C_m be its unique subgroup of order m. Let $\tau_2 = \{h_1, \cdots, h_t\}$ be a transversal of C_m in C_n. We can define an isometry of $\tilde{\psi} : \mathbb{F}Ge \to \mathbb{F}C_n e'$ by

$$\tilde{\psi}(g\alpha) = h_i \psi(\tilde{g}\alpha),$$

for all $g = g_i\tilde{g}$, $\tilde{g} \in \tilde{G}$, $\alpha \in \mathbb{F}\tilde{G}e$.

□

2.4 COMPUTATION CONSIDERATIONS

In Theorem 2.2.4, we saw that every code in a group algebra which has a basis whose elements have disjoint supports is monomially equivalent to a cyclic code. Now, we shall use the following algorithms (in GAP) to see how often this condition holds.

Given a finite group G, the GAP do an enumeration of G as set. Every element $x \in \mathbb{F}G$ associates to a sequence of coefficients of x.

```
ElementsAsRows:=function(G,q,x)
local SetG, S, L, i, g;
SetG:=AsList(G);
S:=CoefficientsAndMagmaElements(x);
L:=[];
for i in [1..Size(G)] do
Add(L, 0*Z(q));
od;
for g in SetG do
if g in S then L[Position(SetG,g)]:=S[Position(S,g)+1];
else L[Position( SetG , g) ] := 0*Z(q); fi;
od;
return L;
end;
```

Given the group algebra $\mathbb{F}G$, the next function gives a list of all the generator matrices of minimal central codes in $\mathbb{F}G$.

```
MatricesOfMinimalCodes:=function(FG)
local F, G, M, n, q, D, d, m, B, i;
D:=DirectSumDecomposition(FG);
G:=UnderlyingGroup(FG);
F:=UnderlyingField(FG);
q:=Size(F);
M:=[ ];
for d in D do
m:=[ ];
B:=Basis(d);
for i in [1..Length(B)] do
Add(m, ElementsAsRows(G,q,B[i]));
od;
Add(M,m);
od;
return M;
end;
```

The last function has a true value if all minimal codes in $\mathbb{F}G$ have bases whose elements have disjoint support.

```
HasDisjointBasis:=function(M,q)
local n, MT, m, i, j, L, HDB;
MT:=[ ];
HDB:=true;
for m in M do
Add(MT,TransposedMat(m));
od;
n:=DimensionsMat(MT[1])[1];
for i in [1..Length(MT)] do
for j in [1..n] do
L:=Set(MT[i][j]);
RemoveSet(L,0*Z(q));
```

```
if Size(L)>1 then HDB:=false;
elif Size(L)>1 then break; fi;
od;
od;
return HDB;
end;
```

Now, we shall use all these functions in the following algorithm. For each prime power q, we can use the same algorithm. Let us write the algorithm for $q = 3$ and compute the list of all non-abelian groups of order ≤ 100 such that all minimal codes in $\mathbb{F}_q G$ have bases whose elements have disjoint support and order relatively prime to 3.

```
L:=[ ];
for n in [1..100] do
for G in AllSmallGroups(Size, n, IsAbelian, false) do
FG:=GroupRing(GF(3),G);
if GcdInt(Size(G),3)=1 then M:=MatricesOfMinimalCodes(FG);
else break; fi;
if HasDisjointBasis(M,3) then Add(L,G); fi;
od;
od;
```

By using the above algorithms, we can produce a table. We say that a *group has disjunction* over a field $\mathbb{F}$ if all minimum codes have disjoint bases. In the table 1 all groups considered are non-abelian of order ≤ 100 and order relatively prime to q.

Table 1: Groups with order relatively prime to q

	Size of field $\mathbb{F}_q$					
	3	4	5	7	8	9
Total of groups	440	20	759	823	20	440
Nilpotent groups	326	12	388	397	12	326
Groups with disjunction	203	15	288	240	11	190
Nilpotent groups with disjunction	203	11	288	240	5	190

Note that there are many nilpotent groups with disjunction. When we consider the two bottom lines in the table above, we note that, for some fields, all groups with disjoint basis are nilpotent. Let us consider all minimum codes of non-abelian nilpotent group of order ≤ 100 with disjunction. In the table 2, all codes are in $\mathbb{F}G$, where G is nilpotent and $|G| \leq 100$. We shall use the abbreviation BDS for basis with disjoint supports.

Table 2: Number of minimum nilpotent codes over $\mathbb{F}_q$

	Size of field $\mathbb{F}_q$					
	3	4	5	7	8	9
Number of minimum codes with BDS	5248	226	7231	7368	108	6466
Number of minimum codes	5849	232	8312	8291	150	7370

Now, taking into account the Corollary 2.3.5, we can construct a table with the number of nilpotent groups which has non-cyclic center. Remember from 2.3.5, that the group algebras over these groups have minimal codes permutation equivalent to abelian codes. All the groups considered in the table 3 are nilpotents which have disjoint bases and with order relatively prime to q.

Table 3: Number of nilpotent groups with disjoint basis over $\mathbb{F}_q$

	Size of field $\mathbb{F}_q$					
	3	4	5	7	8	9
Cyclic center	43	7	55	56	3	29
Non cyclic center	160	8	233	184	2	161

3 CONSTACYCLIC CODES AND CONSTABELIAN CODES

CONSTACYCLIC CODES

The first part of this chapter is devoted to present a different method of computing the number of simple components of a twisted group algebra $\mathbb{F}^{\gamma}G$. In the second part we compute the centrally primitive idempotents of the twisted group algebras of a cyclic group and in the last part we shall provide an example of idempotents in twisted group algebras.

Let R be a finite commutative ring, $\mathcal{C}$ a linear code in R^n, that is, $\mathcal{C}$ is a R-submodule of R^n and let λ be a unit in R. Recall that $\mathcal{C}$ is a *λ-constacyclic code* if

$$(c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C} \Longrightarrow (\lambda c_{n-1}, c_0, \cdots, c_{n-2}) \in \mathcal{C}$$

for all $(c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C}$.

When $\lambda = 1$, the code is *cyclic* and, when $\lambda = -1$, the code is called *negacyclic*. Thus, constacyclic codes generalize cyclic and negacyclic codes and they have been studied for many authors ([39], [1], [11], [12]). Also, constacyclic codes can be realized as ideals in polynomial factor ring $R[x]/\langle x^n - \lambda \rangle$. We will intensively use this fact in the last two sections and to construct some examples.

3.1 THE NUMBER OF SIMPLE COMPONENTS

Let G be a finite group of exponent e and $\mathbb{F}$ a field of characteristic $p \geq 0$ such that p does not divide the order of G. We say that a 2-cocycle $\gamma \in Z^2(G, \mathbb{F}^*)$ is *normalized* if

$$\gamma(g, 1) = 1 = \gamma(1, g)$$

for all $g \in G$. Given a normalized 2-cocycle γ, an element $g \in G$ is said to be *γ-regular* if

$$\gamma(g, x) = \gamma(x, g)$$

for all $x \in C_G(g)$. Let C_g be the conjugacy class of $g \in G$ and let $\gamma \in Z^2(G, \mathbb{F}^*)$. We say that C_g is *γ-regular* if g is γ-regular.

Before exploring the theory any further, we compute some explicit examples. We shall need one result. The following is well-known but we include its proof for sake of completeness.

Lemma 3.1.1. *Let $C_n = \langle g \rangle$ be a cyclic group of order n and A be a finite C_n-module, i.e., A is a finite abelian group with an action of C_n in A. Let $A^{C_n} = \{a \in A : a^{g^i} = a \text{ for all } g^i \in C_n\}$. Also, define the norm map $N : A \to A^{C_n}$ by $N(a) = \prod_{i=0}^{n-1} a^{g^i}$.*

Then, for every $\lambda \in A^{C_n}$, we have that $\gamma_\lambda : C_n \times C_n \to A$ defined by

$$\gamma_\lambda(g^i, g^j) = \begin{cases} 1, & i+j < n \\ \lambda, & i+j \geq n \end{cases}$$

is a 2-cocycle and $H^2(C_n, A) = \{[\gamma_\lambda] : \lambda \in A\} \cong A^{C_n}/Im(N)$.

Proof. Let r_1 and r_2 be the residues of the division of $i+j$ and $j+k$ by n, respectively. Then

$$\gamma_\lambda(g^i, g^j).\gamma_\lambda(g^i g^j, g^k) = \begin{cases} 1, & \text{if } i+j < n \text{ and } r_1 + k < n \\ \lambda, & (\text{if } i+j < n \text{ and } r_1 + k \geq n) \text{ or } (i+j \geq n \text{ and } r_1 + k < n) \\ \lambda^2, & \text{if } i+j \geq n \text{ and } r_1 + k \geq n. \end{cases}$$

Since $\lambda^{g^i} = \lambda$ for all i, with $0 \leq i \leq n-1$, we have

$$\gamma_\lambda(g^j, g^k)^{g^i}.\gamma_\lambda(g^i, g^j g^k) = \begin{cases} 1, & \text{if } j+k < n \text{ and } i + r_2 < n \\ \lambda, & \text{if } (j+k < n \text{ and } i + r_2 \geq n) \text{ or } (j+k \geq n \text{ and } i + r_2 < n) \\ \lambda^2, & \text{if } j+k \geq n \text{ and } i + r_2 \geq n. \end{cases}$$

We wish to show that $\gamma_\lambda(g^i, g^j).\gamma_\lambda(g^i g^j, g^k) = \gamma_\lambda(g^j, g^k)^{g^i}.\gamma_\lambda(g^i, g^j g^k)$ for every $0 \leq i, j, k \leq n-1$. First we observe that

$$r_1 = \begin{cases} i+j, & \text{if } i+j < n \\ i+j-n, & \text{if } i+j \geq n \end{cases}$$

and

$$r_2 = \begin{cases} j+k, & \text{if } j+k < n \\ j+k-n, & \text{if } j+k \geq n. \end{cases}$$

Let us consider four cases:

1. Assume that $i+j<n$ and $r_1+k<n$. Then $i+j+k<n$ implying that $j+k<n$ and $i+r_2<n$.

2. Assume that $j+k<n$ and $i+r_2\geq n$. If $j+k<n$ then $i+r_2=i+j+k=r_1+k\geq n$. If $j+k\geq n$ then $i+r_2=i+j+k-n<k<n$.

3. Assume that $i+j\geq n$ and $r_1+k<n$. If $j+k<n$ then $i+r_2=i+j+k\geq n$. If $j+k\geq n$ then $i+r_2=i+j+k-n=r_1+k<n$.

4. Assume that $i+j\geq n$ and $r_1+k\geq n$. Then $j+k=(n-i)+r_1+k\geq n$ and $i+r_2=i+j+k-n=r_1+k\geq n$.

It follows from these four cases that γ_λ is a 2-cocycle.

Suppose that γ_λ and γ_μ are cohomologous. Then, there exists a coboundary $\delta: C_n\to A$ such that $\gamma_\lambda(g^i,g^j)=\gamma_\mu(g^i,g^j)\delta_i\delta_j^{g^i}\delta_{i+j}^{-1}$, where $\delta_k=\delta(g^k)$ for any $0\leq k\leq n-1$. Then

$$\lambda=\prod_{i=0}^{n-1}\gamma_\lambda(g^i,g)=\prod_{i=0}^{n-1}\gamma_\mu(g^i,g)\delta_i\delta_1^{g^i}\delta_{i+1}^{-1}=\mu\prod_{i=0}^{n-1}\delta_1^{g^i}=\mu N(\delta_1).$$

Let $\gamma\in Z^2(C_n,A)$. For any i, $0\leq i\leq n-1$, define $\delta: C_n\to A$ by

$$\delta_i=\delta(g^i)=\prod_{k=0}^{i-1}\gamma(g^k,g)^{-1}.$$

By the definition of 2-cocycle, we have

$$\gamma(g^i,g^j)\gamma(g^{i+j},g)=(\gamma(g^j,g))^{g^i}\gamma(g^i,g^{j+1}) \tag{12}$$

for all $0\leq i,j\leq n-1$. We can use the last formula again for i, $j+1$ to get $\gamma(g^i,g^{j+1})$ and substituting in 12 obtaining

$$\gamma(g^i,g^j)=(\gamma(g^j,g))^{g^i}(\gamma(g^{j+1},g))^{g^i}\gamma(g^{i+j},g)^{-1}\gamma(g^{i+j+1},g)^{-1}\gamma(g^i,g^{j+1})$$

Notice that, for a fixed i and j, we get that

$$\gamma(g^i,g^{j+\ell})\gamma(g^{i+j+\ell},g)=(\gamma(g^{j+\ell},g))^{g^i}\gamma(g^i,g^{j+\ell+1})$$

for all $0 \leq \ell \leq n-1$. Let r be the remainder when $i+j$ are divided by n. By induction, we can write $\gamma(g^i, g^j)$ as

$$\begin{aligned}\gamma(g^i, g^j) &= \prod_{\ell=0}^{n-k-1} \gamma(g^{j+\ell}, g)^{g^i} \gamma(g^{i+j+\ell}, g)^{-1} \\ &= \prod_{\ell=0}^{i-1} \gamma(g^\ell, g)^{-1} \prod_{\ell=0}^{j-1} \left(\gamma(g^\ell, g)^{g^i}\right)^{-1} \prod_{\ell=0}^{r-1} \gamma(g^\ell, g) \\ &= \gamma_\lambda(g^i, g^j)\delta_i(\delta_j^{g_i})(\delta_{i+j}^{-1}).\end{aligned}$$

Define the map $A^G \to H^2(G, A)$ by $\lambda \mapsto [\gamma_\lambda]$. Since

$$\prod_{\ell=0}^{n-1} \gamma_\lambda(g^\ell, g)\gamma_\mu(g^\ell, g) = \lambda\mu = \prod_{\ell=0}^{n-1} \gamma_{\lambda\mu}(g^\ell, g),$$

we have that $[\gamma_\lambda\gamma_\mu] = [\gamma_{\lambda\mu}]$, so the map is a homomorphism of groups. Since every 2-cocycle is cohomologous to a 2-cocycle of the form γ_λ, we have an epimorphism. Finally, γ_λ is cohomologous to γ_1 if and only if $\lambda = N(\delta_1)$ for some $\delta_1 \in A$. Then, the kernel is $im(N)$.

□

With this result in mind, we can produce our first example.

Example 3.1.1. Let $\mathbb{F}_7$ be a field with 7 elements and let $G = C_4 = \langle g \rangle$ be a cyclic group with 4 elements. Fix $\gamma = \gamma_6 : C_4 \times C_4 \to \mathbb{F}_7$ defined by

$$\gamma(g^i, g^j) = \begin{cases} 1, & i+j < 4 \\ 6, & i+j \geq 4. \end{cases}$$

It follows easily that γ is normalized and every element in G is γ-regular. In addition, notice that the γ-regular conjugacy classes are $C_{\bar{x}} = \{\bar{x}\}$ for $x \in G$.

Example 3.1.2. Let $G = C_4 \times C_{12} = \langle g_1 \rangle \times \langle g_2 \rangle$. Consider the following maps $\gamma_6^{(1)} : C_4 \times C_4 \to \mathbb{F}_7$ and $\gamma_3^{(2)} : C_{12} \times C_{12} \to \mathbb{F}_7$ given by

$$\gamma_6^{(1)}(g_1^i, g_1^j) = \begin{cases} 1, & i+j < 4 \\ 6, & i+j \geq 4. \end{cases}$$

and

$$\gamma_3^{(2)}(g_2^i, g_2^j) = \begin{cases} 1, & i+j < 12 \\ 3, & i+j \geq 12. \end{cases}$$

Let us define $\gamma : G \times G \to \mathbb{F}_7$ by

$$\gamma(g_1^{i_1}g_2^{i_2}, g_1^{j_1}g_2^{j_2}) = \gamma_6^{(1)}(g_1^{i_1}, g_1^{j_1})\,\gamma_3^{(2)}(g_2^{i_2}, g_2^{j_2}).$$

It is easy to verify that γ is normalized and every element in G is γ-regular.

Example 3.1.3. Let $G = C_2 \times C_6 = \langle g_1 \rangle \times \langle g_2 \rangle$ and let $\mathbb{F}_5$ be a field with 5 elements. Let us consider $\gamma : G \times G \to \mathbb{F}_5$ defined by

$$\gamma(g_1^{i_1}g_2^{i_2}, g_1^{j_1}g_2^{j_2}) = 4^{i_2 j_1}.$$

Then γ is normalized and $\{1, g_2^2, g_2^4\}$ is the set of γ-regular elements of G.

A 2-cocycle $\gamma \in Z^2(G, \mathbb{F}^*)$ is called a *normal cocycle* if

$$\gamma(x, g) = \gamma(xgx^{-1}, x)$$

for all $x \in G$ and all γ-regular $g \in G$. Notice that a 2-cocycle γ is normal if and only if $\bar{x}\bar{g}\bar{x}^{-1} = \overline{xgx^{-1}}$ for all $x \in G$ and all γ-regular $g \in G$. The following result shows that any 2-cocycle is cohomologous to a normal 2-cocycle.

Lemma 3.1.2. *[22, Lemma 2.6.2] Any 2-cocycle $\gamma \in Z^2(G, \mathbb{F}^*)$ is cohomologous to a normal cocycle.*

We shall use this lemma to work with twisted group algebras in which the 2-cocycle is normal. For these twisted group algebras we will extend the results about the number of components in [14]. Let us begin with the following definition.

Definition 3.1.3. Let A be a $\mathbb{F}$-algebra and let M be a simple left A-module with $dim_{\mathbb{F}} M < \infty$.

1. We say that M is an *absolutely simple* A-module if for any field extension $\mathbb{E} \supseteq \mathbb{F}$, $\mathbb{E} \otimes_{\mathbb{F}} M$ is a simple $\mathbb{E} \otimes A$-module.

2. We say that a field $\mathbb{E} \supseteq \mathbb{F}$ is a *splitting field* for A if every left simple $\mathbb{E} \otimes A$-module is absolutely simple.

Let n be a positive integer and let p be either a prime rational integer or zero. Then $n_{p'}$ denotes the p'-part of n if $p \neq 0$ and $n_{p'} = n$ if $p = 0$. We also write $exp(G)$ for the exponent of G.

The following result is an extension of a classic theorem of Brauer to twisted group algebras.

Theorem 3.1.4. *[23, Theorem 6.2.2] Let $\mathbb{E}$ be an algebraically closed field of characteristic $p \geq 0$ and let $\gamma \in Z^2(G, \mathbb{E}^*)$ be of finite order n. Assume that $\mathbb{F}$ is a subfield of $\mathbb{E}$ which contains a root of unity of order $m = n.exp(G)_{p'}$. Then, for any subgroup H of G , $\mathbb{F}$ is a splitting field for $\mathbb{F}^\gamma H$.*

Let $\gamma \in Z^2(G, \mathbb{F}^*)$ be a normal 2-cocycle and ℓ the minimal positive integer k such that $(\gamma(x,y))^k = 1$ for all $x, y \in G$.

Lemma 3.1.5. *Considering above notations, if $p > 0$ then the integers p and ℓ are relatively prime.*

Proof. Assume, by way of contradiction, that p divides ℓ. Since $\gamma(x,y)^\ell = 1$ for all $x, y \in G$, we have that $\gamma(x,y)$ are roots of the polynomial $X^\ell - 1 \in \mathbb{F}[X]$ for all $x, y \in G$. As p is the characteristic of $\mathbb{F}$, we get that $\gamma(x,y)$, $x, y \in G$, are roots of $X^{\ell/p} - 1$, with $\ell/p < \ell$. □

It follows from this lemma that we may take $n = \ell.e$, where $e = exp(G)$, and a primitive root of unity θ of order n. By Theorem 1.5.8 we have that $\mathbb{F}(\theta)^\gamma G$ is a semisimple algebra and by Theorem 3.1.4 we have that $\mathbb{F}(\theta)$ is a splitting field for $\mathbb{F}(\theta)^\gamma G$. Then, there exist an isomorphism

$$\psi : \mathbb{F}(\theta)^\gamma G \to \oplus_{i=1}^r M_{n_i}(\mathbb{F}(\theta)) \tag{13}$$

of $\mathbb{F}(\theta)$-algebras.

Example 3.1.4. As in example 3.1.1, let $G = C_4 = \langle g \rangle$ and $\gamma = \gamma_6 : C_4 \times C_4 \to \mathbb{F}_7$. Let $\ell = 2$, $e = exp(G) = 4$ and $n = \ell e = 8$. Suppose θ a primitive n^{th} root of unity. Since $x^8 - 1 = (x+1)(x+6)(x^2+1)(x^2+3x+1)(x^2+4x+1)$, we have $\mathbb{F}_7(\theta) \cong \mathbb{F}_{7^2}$. As $x^4 - 6 = (x^2+3x+1)(x^2+4x+1)$, by Proposition 1.4.1, we have

$$\mathbb{F}_7^\gamma G \cong \frac{\mathbb{F}_7[x]}{\langle x^4 - 6 \rangle} \cong \frac{\mathbb{F}_7[x]}{\langle x^2+3x+1 \rangle} \oplus \frac{\mathbb{F}_7[x]}{\langle x^2+4x+1 \rangle} \cong \mathbb{F}_{7^2} \oplus \mathbb{F}_{7^2}$$

and so, we conclude that

$$\mathbb{F}_{7^2}^\gamma G \cong \mathbb{F}_{7^2} \otimes_{\mathbb{F}_7} (\mathbb{F}_7^\gamma G) \cong \mathbb{F}_{7^2} \oplus \mathbb{F}_{7^2} \oplus \mathbb{F}_{7^2} \oplus \mathbb{F}_{7^2}.$$

Example 3.1.5. Let $G = C_4 \times C_{12}$. With the notations of the Example 3.1.2, assume $\ell = 6$, $e = 12$ and $n = \ell e = 72$. Using SAGE we can decompose in $\mathbb{F}_7[x]$

$$x^{72} - 1 = p(x)(x^6+2)(x^6+4)(x^6+x^3+4)(x^6+2x^3+3)(x^6+5x^3+2)(x^6+6x^3+4)$$

where the irreducible factors of $p(x)$ have degree less than 6. Since the roots of x^6+2 and x^6+4 are of order 36 in $\mathbb{F}_7^*$ and $\Phi(72)=24$, we conclude that all primitive roots of unity of order 72 are the roots of x^6+x^3+4, x^6+2x^3+3, x^6+5x^3+2, x^6+6x^3+4. Then, the root θ of x^6+x^3+4 is of order 72 in $\mathbb{F}_7^*$ and so $\mathbb{F}_7(\theta)\cong\mathbb{F}_{7^6}$. By Lemma 1.4.2, we get

$$\mathbb{F}_7^\gamma G \cong (\mathbb{F}_7^{\gamma_6^{(1)}} C_4)\otimes_{\mathbb{F}_7}(\mathbb{F}_7^{\gamma_3^{(2)}} C_{12}).$$

By the previous example $\mathbb{F}_7^{\gamma_6^{(1)}} C_4 \cong \mathbb{F}_{7^2}\oplus\mathbb{F}_{7^2}$ and since

$$\mathbb{F}_7^{\gamma_3^{(2)}} C_{12} \cong \frac{\mathbb{F}_7[x]}{\langle x^{12}-3\rangle} \cong \frac{\mathbb{F}_7[x]}{\langle x^6+2x^3+2\rangle}\oplus\frac{\mathbb{F}_7[x]}{\langle x^6+5x^3+2\rangle}\cong \mathbb{F}_{7^6}\oplus\mathbb{F}_{7^6}$$

we conclude that

$$\mathbb{F}_7^\gamma G \cong (\mathbb{F}_{7^2}\oplus\mathbb{F}_{7^2})\otimes_{\mathbb{F}_7}(\mathbb{F}_{7^6}\oplus\mathbb{F}_{7^6})\cong 8\mathbb{F}_{7^6}$$

and so $\mathbb{F}_{7^6}^\gamma G \cong 72\mathbb{F}_{7^6}$.

Example 3.1.6. Let $G=C_2\times C_6$. With the notations as in the example 3.1.3, we can also write $G=H\times\langle g_2^2\rangle$, where $H=\langle g_1,g_2^3\rangle=\langle g_1\rangle\times\langle g_2^3\rangle\cong C_2\times C_2$. Since $4^2\equiv 1(mod\,5)$, we have

$$\gamma((g^{i_1}g_2^{3i_2})g_2^{2i_3},(g^{j_1}g_2^{3j_2})g_2^{2j_3}) = 4^{(3i_2)j_1} = \gamma(g^{i_1}g_2^{3i_2},g^{j_1}g_2^{3j_2})$$

which implies that $\gamma=\tilde{\gamma}\times\alpha$, where $\tilde{\gamma}=\gamma|_{H\times H}$, $\alpha\in Z^2(\langle g_2^2\rangle,\mathbb{F}_5^*)$ and $\alpha=1$. Again, by Lemma 1.4.2, we get

$$\mathbb{F}_5^\gamma G\cong \mathbb{F}_5^{\tilde{\gamma}} H\otimes_{\mathbb{F}_5}\mathbb{F}_5\langle g_2^2\rangle.$$

If $h=g^{i_1}g_2^{3i_2}\in H$ is $\tilde{\gamma}$-regular, then $\gamma(h,g^{j_1}g_2^{3j_2})=\gamma(g^{j_1}g_2^{3j_2},h)$ for all $j_1,j_2=0,1$. Then, $4^{i_2j_1}=4^{i_1j_2}$ for all $j_1,j_2=0,1$, which implies that $i_2j_1\equiv i_1j_2(mod\,2)$ for all $j_1,j_2=0,1$. As the unique possibility is $i_1=i_2=0$, we conclude that $1\in H$ is the only $\tilde{\gamma}$-regular element of H. By [23, Theorem 8.2.8] we have

$$\mathbb{F}_5^{\tilde{\gamma}} H\cong M_2(\mathbb{F}_5).$$

Putting these two last formulas together, we get

$$\mathbb{F}_5^\gamma G\cong M_2(\mathbb{F}_5)\otimes_{\mathbb{F}_5}(\mathbb{F}_5\oplus\mathbb{F}_{5^2})\cong M_2(\mathbb{F}_5)\oplus M_2(\mathbb{F}_{5^2}).$$

Let $\ell=2$, $e=6$, $n=\ell e=12$ and θ a primitive n^{th} root of unity. Using SAGE we can decompose

$$x^{12}-1=\left(\prod_{a=1}^{4}(x+a)\right)(x^2+x+1)(x^2+2x+4)(x^2+3x+4)(x^2+4x+1)$$

into irreducible factors in $\mathbb{F}_5[x]$. Since $\mathbb{F}_5(\theta) \cong \mathbb{F}_{5^2}$ we conclude that

$$\mathbb{F}_{5^2}^{\gamma}G \cong M_2(\mathbb{F}_{5^2}) \oplus M_2(\mathbb{F}_{5^2}) \oplus M_2(\mathbb{F}_{5^2}).$$

Theorem 3.1.6 ([22], Theorem 6.3, p. 96). *Let $\mathbb{F}$ be an arbitrary field, let $\gamma \in Z^2(G, \mathbb{F}^*)$ and let T_γ be a full set of representatives for the γ-regular conjugacy classes of G. For each $g \in T_\gamma$ denote by τ_g a left transversal for $C_G(g)$ in G and by C_g the γ-regular conjugacy class of G containing g. Then the elements*

$$C_{\bar{g}}^{+} = \sum_{x \in \tau_g} \bar{x}^{-1}\bar{g}\bar{x}$$

constitute a $\mathbb{F}$-basis of $\mathcal{Z}(\mathbb{F}^{\gamma}G)$. In particular, if γ is a normal cocycle, then the elements

$$C_{\bar{g}}^{+} = \sum_{x \in C_g} \bar{g}$$

constitute a $\mathbb{F}$-basis of $\mathcal{Z}(\mathbb{F}^{\gamma}G)$.

Example 3.1.7. Let $G = C_2 \times C_6$. With notations of examples 3.1.3 and 3.1.6, suppose that $g = g^{i_1}g_2^{i_2} \in G$ is γ-regular. Then $\gamma(g, g^{j_1}g_2^{j_2}) = 4^{i_2 j_1} = 4^{i_1 j_2} = \gamma(g^{j_1}g_2^{j_2}, g)$ for all $0 \leq j_1 \leq 1$, $0 \leq j_2 \leq 5$. This implies that $i_2 j_1 \equiv i_1 j_2 (mod\ 2)$ for all $0 \leq j_1 \leq 1, 0 \leq j_2 \leq 5$. Since the possibilities are $i_1 = 0$ and $i_2 = 0, 2, 4$ we conclude that $\{1, g_2^2, g_2^4\}$ is the set of γ-regular elements. It follows from the last theorem that

$$C_1^{+} = \bar{1}, \quad C_2^{+} = \bar{g}_2^2, \quad C_3^{+} = \bar{g}_2^4$$

constitute a basis of $\mathcal{Z}(\mathbb{F}_5^{\gamma}G)$. Notice that example 3.1.6 tell us that

$$\mathcal{Z}(\mathbb{F}_5^{\gamma}G) \cong \mathcal{Z}\left(M_2(\mathbb{F}_5)\right) \oplus \mathcal{Z}\left(M_2(\mathbb{F}_{5^2})\right) \cong \mathbb{F}_5 \oplus \mathbb{F}_{5^2}$$

and 3 is, in fact, the dimension of $\mathcal{Z}(\mathbb{F}_5^{\gamma}G)$ over $\mathbb{F}_5$.

Example 3.1.8. Let D_8 be the *dihedral group* with 16 elements given by the presentation

$$\langle a, b | a^8 = b^2 = 1, bab = a^{-1} \rangle.$$

We define $\alpha : D_8 \times D_8 \to \mathbb{F}_3^*$ by

$$\alpha(a^i b^j, a^k b^\ell) = 2^{jk}.$$

We claim that $\alpha \in Z^2(D_8, \mathbb{F}_3^*)$. In fact, given $x = a^i b^j, y = a^k b^\ell, z = a^m b^n \in D_8$ we have

$$\alpha(x, y)\alpha(xy, z) = 2^{jk}2^{(j+\ell)m} \quad \text{and} \quad \alpha(y, z)\alpha(x, yz) = 2^{\ell m}2^{j(k-m)}$$

Since $jk + (j+\ell)m \equiv \ell m + j(k-m)(mod\ 2)$ and the order of $2 \in \mathbb{F}_3$ is equal to 2, we obtain the equality of both equations above and the claim follows.

The centralizer of the elements in D_8 are

$$C_{D_8}(a^ib^j) = \begin{cases} D_8 & \text{if } (i,j) = (0,0) \text{ or } (i,j) = (4,0); \\ \langle a \rangle & \text{if } (i,j) = (i,0) \text{ for } i \neq 4; \\ \langle a^ib \rangle \times \langle a^{i+4}b \rangle & \text{if } (i,j) = (i,1). \end{cases}$$

A direct computation shows that $\alpha(a^ib^j, y) = \alpha(y, a^ib^j)$ for any $y \in C_{D_8}(a^ib^j)$. Then, every element of D_8 is α-regular. Notice that α is not a normal cocycle because $a \in D_8$ is a α-regular element and $\alpha(b,a) = 2 \neq 1 = \alpha(bab,b)$.

As every element of D_8 is α-regular, it follows that the α-regular conjugacy classes of D_8 are the conjugacy classes of G, that is,

$$\{1\}, \{a^4\}, \{a, a^7\}, \{a^2, a^6\}, \{a^3, a^5\},$$
$$\{b, a^2b, a^4b, a^6b\}, \{ab, a^3b, a^5b, a^7b\}.$$

Let us denote by T_{ij} the left tranversal of $C_{D_8}(a^ib^j)$ in D_8. Then

$$T_{ij} = \begin{cases} \{1\} & \text{if } (i,j) = (0,0) \text{ or } (i,j) = (4,0); \\ \{1, b\} & \text{if } (i,j) = (i,0) \text{ for } i \neq 4; \\ \{1, a, a^2, a^3\} & \text{if } (i,j) = (i,1). \end{cases}$$

It follows from last theorem that

$$C_{00}^+ = \bar{1}$$
$$C_{40}^+ = \sum_{t \in T_{40}} \bar{t}\overline{a^4}(\bar{t})^{-1} \qquad C_{30}^+ = \sum_{t \in T_{30}} \bar{t}\overline{a^3}(\bar{t})^{-1}$$
$$C_{10}^+ = \sum_{t \in T_{10}} \bar{t}\bar{a}(\bar{t})^{-1} \qquad C_{01}^+ = \sum_{t \in T_{01}} \bar{t}\bar{b}(\bar{t})^{-1}$$
$$C_{20}^+ = \sum_{t \in T_{20}} \bar{t}\overline{a^2}(\bar{t})^{-1} \qquad C_{11}^+ = \sum_{t \in T_{11}} \bar{t}\overline{ab}(\bar{t})^{-1}$$

constitute a basis of $\mathcal{Z}(\mathbb{F}_3^\alpha D_8)$ over $\mathbb{F}_3$.

Recall that $e = exp(G)$, $\gamma \in Z^2(G, \mathbb{F}^*)$ is normal, $\ell = min\{k \in \mathbb{N} : \gamma(x,y)^k = 1,\ x, y \in G\}$, $n = \ell.e$ and θ a primitive root of unity of order n. With the notations of previous Theorem, the set $\{C_{\bar{g}}^+ | g \in T_\gamma\}$ is a $\mathbb{F}(\theta)$-basis of $\mathcal{Z}(\mathbb{F}(\theta)^\gamma G)$.

For each σ in the Galois group $Gal(\mathbb{F}(\theta)/\mathbb{F})$ and $(\alpha_1, \cdots, \alpha_r)$ in $\oplus_{i=1}^{r}\mathbb{F}(\theta)$, we can define

$$\sigma.(\alpha_1, \cdots, \alpha_r) := (\sigma(\alpha_1), \cdots, \sigma(\alpha_r)).$$

Set $\sigma^{\psi} = \psi^{-1}\sigma\psi$ and denote $\bar{g}^{\sigma} = \bar{g}^{m(\sigma)}$, where $\sigma(\theta) = \theta^{m(\sigma)}$ for $\sigma \in Gal(\mathbb{F}(\theta)/\mathbb{F})$. For any $\sigma \in Gal(\mathbb{F}(\theta)/\mathbb{F})$ denote by $r(\sigma)$ the remainder in the division of $m(\sigma)$ by e and denote $\mu(\sigma) = m(\sigma) - r(\sigma)$.

Notice that $\bar{g}^e = u(g).\bar{1}$ for each $g \in G$ where $u(g) = \prod_{i=0}^{e-1}\gamma(g, g^i)$. Since $u(g)$ is a ℓth root of unity, we can take $v(g) \in \mathbb{F}(\theta)$ such that $v(g)^e = u(g)$. Since $\mu(\sigma) = m(\sigma) - r(\sigma) = ej$ for some positive integer j, we get that $v(g)^{\mu(\sigma)} = v(g)^{ej} = u(g)^j \in \mathbb{F}$.

Recall that $\psi : \mathbb{F}(\theta)^{\gamma}G \to \oplus_{i=1}^{r}M_{n_i}(\mathbb{F}(\theta))$ is an isomorphism of $\mathbb{F}(\theta)$-algebras. Let $\pi_i : \oplus_{j=1}^{r}M_{n_j}(\mathbb{F}(\theta)) \to M_{n_i}(\mathbb{F}(\theta))$ be the projection of the i-th component, $1 \leq i \leq r$. We consider $T_i = \pi_i\psi$, $1 \leq i \leq r$, the irreducible representations of $\mathbb{F}(\theta)^{\gamma}G$, and χ_i the characters of T_i, respectively.

Theorem 3.1.7. *For any $\sigma \in Gal(\mathbb{F}(\theta)/\mathbb{F})$ denote by $r(\sigma)$ the remainder in the division of $m(\sigma)$ by e and denote $\mu(\sigma) = m(\sigma) - r(\sigma)$. Then, for each $g \in T_{\gamma}$,*

$$\sigma^{\psi}(C_{\bar{g}}^{+}) = v(g)^{\mu(\sigma)}C_{\bar{g}^{r(\sigma)}}^{+},$$

for all $\sigma \in Gal(\mathbb{F}(\theta)/\mathbb{F})$.

Proof. Let $\lambda_1, \cdots, \lambda_t$ be the eigenvalues of $T_i(\bar{g})$ with $g \in T_{\gamma}$. Since $\bar{g}^e = u(g)\bar{1}$, we have $(T_i(\bar{g}))^e = T_i(\bar{g}^e) = u(g)I_{n_i}$, where I_{n_i} is the identity matrix of $M_{n_i}(\mathbb{F}(\theta))$. Then, the polynomial $X^e - u(g) \in \mathbb{F}[X]$ annihilates $T_i(\bar{g})$. As the minimal polynomial $p(x)$ of $T_i(\bar{g})$ divides $X^e - u(g)$ in $\mathbb{F}[X]$ and $X^e - u(g)$ has no repeated roots, we have that $p(x)$ has no repeated roots. Furthermore, the elements $v(g)\theta^{\ell k} \in \mathbb{F}(\theta)$, $0 \leq k < e$, are all roots of $X^e - u(g)$, which implies that $p(x)$ splits over $\mathbb{F}(\theta)$. By [20, Theorem 6.6], we

have that $T_i(\bar{g})$ is diagonalizable and so $t = n_i$. Since $p(x)$ divides $X^e - u(g)$, we get that $\lambda_j = v(g)\theta^{\ell k_j}$, for some $0 \leq k_j < e$. Then

$$\begin{aligned}
\sigma(\chi_i(\bar{g})) &= \sigma\left(\sum_{j=1}^{n_i} \lambda_j\right) \\
&= \sum_{j=1}^{n_i} \left(v(g)\theta^{\ell k_j}\right)^{m(\sigma)} \\
&= v(g)^{\mu(\sigma)} v(g)^{-\mu(\sigma)} \sum_{j=1}^{n_i} \left(v(g)\theta^{\ell k_j}\right)^{m(\sigma)} \\
&= v(g)^{\mu(\sigma)} \sum_{j=1}^{n_i} v(g)^{m(\sigma)-\mu(\sigma)} \theta^{\ell k_j m(\sigma)} \\
&= v(g)^{\mu(\sigma)} \sum_{j=1}^{n_i} v(g)^{r(\sigma)} \theta^{\ell k_j r(\sigma)} \\
&= v(g)^{\mu(\sigma)} \sum_{j=1}^{n_i} \lambda_j^{r(\sigma)}.
\end{aligned}$$

where $\theta^{\ell k_j m(\sigma)} = \theta^{\ell k_j r(\sigma)}$ because e divides $\mu(\sigma) = m(\sigma) - r(\sigma)$.

On the other hand, if we denote by $tr(A)$ the trace of the square matrix A, then

$$\begin{aligned}
\chi_i(\bar{g}^{r(\sigma)}) &= tr\left(T_i(\bar{g}^{r(\sigma)})\right) \\
&= tr\left(T_i(\bar{g})^{r(\sigma)}\right) \\
&= \sum_{j=1}^{n_i} \lambda_j^{r(\sigma)}.
\end{aligned}$$

Hence $\sigma(\chi_i(\bar{g})) = v(g)^{\mu(\sigma)}\chi_i(\bar{g}^{r(\sigma)})$. As $C^+_{\bar{g}} \in \mathcal{Z}(\mathbb{F}(\theta)^\gamma G)$ and T_i is a homomorphism, we have that $T_i(C^+_{\bar{g}}) = \alpha I_{n_i}$. Then, $\chi_i(C^+_{\bar{g}}) = tr\left(T_i(C^+_{\bar{g}})\right) = n_i\alpha$ implying that $T_i(C^+_{\bar{g}}) = (\chi_i(C^+_{\bar{g}})/n_i)I_{n_i}$. We conclude that

$$\begin{aligned}
\sigma\psi(C^+_{\bar{g}}) &= \sigma\left(\sum_{i=1}^{r}\pi_i\right)\psi(C^+_{\bar{g}}) \\
&= \sigma\sum_{i=1}^{r}\pi_i\psi(C^+_{\bar{g}}) \\
&= \sigma\sum_{i=1}^{r}T_i(C^+_{\bar{g}}) \\
&= \sum_{i=1}^{r}\sigma(\chi_i(C^+_{\bar{g}}))/n_i \\
&= \sum_{i=1}^{r}v(g)^{\mu(\sigma)}\chi_i(C^+_{\bar{g}^{r(\sigma)}})/n_i \\
&= v(g)^{\mu(\sigma)}\sum_{i=1}^{r}\pi_i\psi(C^+_{\bar{g}^{r(\sigma)}})/n_i \\
&= v(g)^{\mu(\sigma)}\psi(C^+_{\bar{g}^{r(\sigma)}}).
\end{aligned}$$

□

For each $g \in T_\gamma$, we shall call

$$S_g = \{v(g)^{\mu(\sigma)}C^+_{\bar{g}^{r(\sigma)}} \,|\, \sigma \in Gal(\mathbb{F}(\theta)/\mathbb{F}), \mu(\sigma) = m(\sigma) - r(\sigma)\}$$

the *cyclotomic γ-classes of g*.

Example 3.1.9. We continue with Examples 3.1.3 and 3.1.6. Since $G = C_2 \times C_6 = \langle g_1\rangle \times \langle g_2\rangle$, we have the exponent $e = 6$ of the group G. It follows from Example 3.1.6 that $\mathbb{F}_5(\theta) = \mathbb{F}_{5^2}$, where θ is a root of the irreducible polynomial $f(x) = x^2 + x + 1 \in \mathbb{F}_5[x]$ and $f(x)$ divides $x^{12} - 1$. Then, the Galois group $Gal(\mathbb{F}_{5^2}/\mathbb{F}_5) = \{Id, \sigma\}$, where Id is the identity map of $\mathbb{F}_{5^2}$ and $\sigma : \mathbb{F}_{5^2} \to \mathbb{F}_{5^2}$ is defined by $\sigma(a + b\theta) = a + b\theta^5$ with $a, b \in \mathbb{F}_5$. Since $T_\gamma = \{1, g_2^2, g_2^4\}$, we conclude that the cyclotomic γ-classes of G are

$$S_1 = \{\bar{1}\} \quad \text{and} \quad S_2 = \{\bar{g}_2^2, \bar{g}_2^4\}.$$

We have to prove that the elements of $S_{\bar{g}}$ are central in $\mathbb{F}^\gamma G$. We begin with the following technical result.

Lemma 3.1.8. *If $g \in G$ is a γ-regular element and m is a positive integer then*

$$\gamma(h, g^m) = \gamma(g^m, h)$$

for all $h \in C_G(g)$.

Proof. We shall proceed by induction on m. If $m = 1$ then, since g is γ-regular, we obtain $\gamma(h, g) = \gamma(g, h)$, for all $h \in C_G(g)$. Assume that $\gamma(h, g^{m-1}) = \gamma(g^{m-1}, h)$ for all $h \in C_G(g)$. Using the cocycle identity $\gamma(x, y)\gamma(xy, z) = \gamma(y, z)\gamma(x, yz)$ for $x = g$, $y = g^{m-1}$, $z = h$, we get

$$\gamma(g, g^{m-1})\gamma(g^m, h) = \gamma(g^{m-1}, h)\gamma(g, g^{m-1}h).$$

Since g is γ-regular and $g^{m-1}h \in C_G(g)$, we have $\gamma(g, g^{m-1}h) = \gamma(g^{m-1}h, g)$. By the induction hypothesis $\gamma(g^{m-1}, h) = \gamma(h, g^{m-1})$ for all $h \in C_G(g)$. Then

$$\gamma(g, g^{m-1})\gamma(g^m, h) = \gamma(h, g^{m-1})\gamma(hg^{m-1}, g).$$

Again, using the cocycle identity $\gamma(x, y)\gamma(xy, z) = \gamma(y, z)\gamma(x, yz)$ for $x = h$, $y = g^{m-1}$, $z = g$, we get

$$\gamma(h, g^{m-1})\gamma(hg^{m-1}, g) = \gamma(g^{m-1}, g)\gamma(h, g^m).$$

As $\gamma(g, g^{m-1}) = \gamma(g^{m-1}, g)$, we conclude that $\gamma(h, g^m) = \gamma(g^m, h)$, for all $h \in C_G(g)$. □

Since $\gamma \in Z^2(G, \mathbb{F}^*)$, we identify the center $\mathcal{Z}(\mathbb{F}^\gamma G)$ with the subalgebra of $\mathcal{Z}(\mathbb{F}(\theta)^\gamma G)$ which is obtained by restriction of coefficients, i.e., we identify the center of $\mathcal{Z}(\mathbb{F}^\gamma G)$ with a subalgebra of $\mathcal{Z}(\mathbb{F}(\theta)^\gamma G)$ via the map

$$\iota\left(\sum_{g \in T_\gamma} a_g C_{\bar{g}}^+\right) = \sum_{g \in T_\gamma} a_g C_{\bar{g}}^+.$$

Theorem 3.1.9. *Let T be the full set of representatives of the cyclotomic γ-classes of G, V_g the $\mathbb{F}$-linear space of $\mathcal{Z}(\mathbb{F}^\gamma G)$ spanned by S_g and*

$$\mathcal{A} = \{\alpha \in \mathcal{Z}(\mathbb{F}^\gamma G) | \sigma^\psi(\alpha) = \alpha \text{ for all } \sigma \in Gal(\mathbb{F}(\theta)/\mathbb{F})\}.$$

For $\alpha \in \mathcal{Z}(\mathbb{F}^\gamma G)$, denote by $p_\alpha(x)$ the minimal polynomial of α over $\mathbb{F}$. Then

1. $\mathcal{Z}(\mathbb{F}^\gamma G) = \oplus_{g \in T} V_g$.

2. *The set* $\{\eta_g\}_{g\in T_0}$, *with* $\eta_g = \sum_{\Gamma\in S_g} \Gamma$ *and* $T_0 = \{g \in T : \eta_g \neq 0\}$, *is a* $\mathbb{F}$*-basis of* $\mathcal{A}$.

3. $\mathcal{A} = \{\alpha \in \mathcal{Z}(\mathbb{F}^\gamma G) |\ p_\alpha(x)$ *splits over* $\mathbb{F}\}$.

Proof. 1. Let m be a positive integer with $gcd(m, o(g)) = 1$. Then there exist $s, t \in \mathbb{Z}$ such that $1 = sm + to(g)$. If $h \in C_G(g^m)$ then $h^{-1}g^m h = g^m$, which implies that $g = g^{sm} = h^{-1}g^{sm}h = h^{-1}gh$, so $h \in C_G(g)$. As $C_G(g) \subseteq C_G(g^m)$, we get that $C_G(g) = C_G(g^m)$. By Lemma 3.1.8 we conclude that g^m is γ-regular. Since for all $\sigma \in Gal(\mathbb{F}(\theta)/\mathbb{F})$ it is true that $gcd(m(\sigma), o(g)) = 1$, we have that g^σ is γ-regular implying that $v(g)^{\mu(\sigma)}C^+_{\bar{g}^{r(\sigma)}}$ is central in $\mathbb{F}^\gamma G$. Then $S_g \subset \mathcal{Z}(\mathbb{F}^\gamma G)$, which implies that $V_g \subset \mathcal{Z}(\mathbb{F}^\gamma G)$. As $V_g = Span_{\mathbb{F}}(S_g)$, and $\cup_{g\in T} S_g$ is a $\mathbb{F}$-basis of $\mathcal{Z}(\mathbb{F}^\gamma G)$, we get that $\oplus_{g\in T} V_g \subseteq \mathcal{Z}(\mathbb{F}^\gamma G)$. Since $\oplus_{g\in T} V_g$ and $\mathcal{Z}(\mathbb{F}^\gamma G)$ are vector spaces of the same dimension over $\mathbb{F}$ the result holds.

2. By definition $\mathcal{A} \subset \mathcal{Z}(\mathbb{F}^\gamma G)$ and by the first part we already know that $\cup_{g\in T} S_g$ is a basis of $\mathcal{Z}(\mathbb{F}^\gamma G)$ over $\mathbb{F}$. Let $\alpha = \sum_{g,\sigma} a_{g,\sigma} v(g)^{\mu(\sigma)} C^+_{g^{r(\sigma)}} \in \mathcal{A}$, where $a_{g,\sigma} \in \mathbb{F}$. Then

$$\sum_{g,\sigma} a_{g,\sigma} v(g)^{\mu(\sigma)} C^+_{\bar{g}^{r(\sigma)}} = \sum_{g,\sigma} a_{g,\sigma} v(g)^{\mu(\tau\sigma)} C^+_{\bar{g}^{r(\tau\sigma)}}$$

for every $\tau \in Gal(\mathbb{F}(\theta)/\mathbb{F})$. Then $a_{g,\sigma} = a_{g,\tau\sigma}$, for all $\tau \in Gal(\mathbb{F}(\theta)/\mathbb{F})$ and $g \in T$, which implies that $\alpha = \sum_{g\in T} a_g \eta_{\bar{g}}$. Because $\{\eta_g\}_{g\in T_0} = \{\eta_g\}_{g\in T} \setminus \{0\}$ and $\{\eta_g\}_{g\in T_0}$ is linearly independent over $\mathbb{F}$, we get that $\{\eta_{\bar{g}}\}_{g\in T_0}$ is a basis of $\mathcal{A}$ and we are done.

3. Since $\alpha \in \mathcal{A}$ if and only if $\sigma^\psi(\alpha) = \alpha$ for all $\sigma \in Gal(\mathbb{F}(\theta)/\mathbb{F})$, we have that $\sigma(\psi(\alpha)) = \psi(\alpha)$, for all $\sigma \in Gal(\mathbb{F}(\theta)/\mathbb{F})$. Then, we conclude that $\alpha \in \mathcal{A}$ if and only if $\psi(\alpha) \in \oplus_{i=1}^r \mathbb{F}$. Because ψ is an isomorphism, we have that α and $\psi(\alpha)$ have the same minimal polynomial, and this polynomial splits over $\mathbb{F}$ if and only if $\psi(\alpha) \in \oplus_{i=1}^r \mathbb{F}$.

□

Definition 3.1.10. The cyclotomic γ-classes of g, where $g \in T_0$, are called *regular cyclotomic γ-classes.*

Example 3.1.10. Let $G = C_2 \times C_6 = \langle g_1\rangle \times \langle g_2\rangle$. With notations of examples 3.1.3, 3.1.6 and 3.1.9, we have by Example 3.1.9 that the cyclotomic γ-classes of G are

$$S_1 = \{\bar{1}\} \quad \text{and} \quad S_2 = \{\bar{g_2}^2, \bar{g_2}^4\}.$$

Since $\eta_{\bar{1}} = \bar{1} \neq 0$ and $\eta_{\bar{g_2}^2} = \bar{g_2}^2 + \bar{g_2}^4 \neq 0$, we conclude that $1, g_2^2 \in T_0$ and by definition, S_1 and S_2 are regular cyclotomic γ-classes.

Since $p = char(\mathbb{F})$ does not divide $|G|$, there is an isomorphism

$$\varphi : \mathbb{F}^\gamma G \to \oplus_{i=1}^m M_{d_i}(D_i)$$

where m and d_i are positive integers and D_i is a division algebra over $\mathbb{F}$, $1 \leq i \leq m$.

Theorem 3.1.11. *The number of simple components of $\mathbb{F}^\gamma G$ is equal to the number of regular cyclotomic γ-classes of G.*

Proof. With the notations above, let $\mathbb{F}_i$ be the center of D_i, $1 \leq i \leq m$. We know that $\mathcal{Z}(\mathbb{F}^\gamma G) \cong \oplus_{i=1}^m \mathbb{F}_i$. Since φ is an isomorphism and $\mathcal{A} = \{\alpha \in \mathcal{Z}(\mathbb{F}^\gamma G) | p_\alpha(x) \text{ splits over } \mathbb{F}\}$, we have

$$\varphi(\mathcal{A}) = \{\varphi(\alpha) \in \varphi(\mathcal{Z}(\mathbb{F}^\gamma G)) | p_{\varphi(\alpha)}(x) \text{ splits over } \mathbb{F}\} = \oplus_{i=1}^m \mathbb{F}.$$

From part 2 of Theorem 3.1.9, we have that $\{\varphi(\eta_g)\}_{g \in T_0}$ is a $\mathbb{F}$-basis of $\varphi(\mathcal{A})$. We conclude that $|T_0| = dim_{\mathbb{F}}(\varphi(\mathcal{A})) = m$. □

Example 3.1.11. Let $G = C_2 \times C_6 = \langle g_1 \rangle \times \langle g_2 \rangle$ and $\gamma : G \times G \to \mathbb{F}_5$ defined by

$$\gamma(g_1^{i_1} g_2^{i_2}, g_1^{j_1} g_2^{j_2}) = 4^{i_2 j_1}.$$

By the last example (Example 3.1.10), we have

$$S_1 = \{\bar{1}\} \quad \text{and} \quad S_2 = \{\bar{g_2}^2, \bar{g_2}^4\}.$$

and by Example 3.1.6, we have

$$\mathbb{F}_5^\gamma G \cong M_2(\mathbb{F}_5) \oplus M_2(\mathbb{F}_{5^2}).$$

T

Since we are interested in codes in twisted group algebras, we assume that the field $\mathbb{F}$ and the group G are finite. Then, for some positive integer ℓ, we have that $(\gamma(x,y))^\ell = 1$ holds for every 2-cocycle γ. Let C_n be the cyclic group of order n and $\mathbb{F}$ a field with q elements. By Lemma 3.1.1 we have that $H^2(C_n, \mathbb{F}^*) \cong \mathbb{F}^*/(\mathbb{F}^*)^n$ which is a cyclic group of order $k = gcd(q-1, n)$.

Finally, we give an important consequence of the Theorem 3.1.11.

Corollary 3.1.12. *Let γ be a 2-cocycle in $Z^2(C_n, \mathbb{F}^*)$. Then the number of irreducible factors of the polynomial $x^n - \lambda \in \mathbb{F}[x]$, where $\lambda = \prod_{i=0}^{n-1} \gamma(g, g^i)$, is equal to the number of regular cyclotomic γ-classes of C_n.*

Proof. By Lemma 3.1.1 we have that γ is cohomologous to γ_λ with $\lambda \in \mathbb{F}^*$. Note that $\lambda = \prod_{i=0}^{n-1} \gamma_\lambda(g, g^i) = \prod_{i=0}^{n-1} \gamma(g, g^i)$. Since $x^n - \lambda$ is separable, we have

$$\mathbb{F}^\gamma C_n \cong \mathbb{F}^{\gamma_\lambda} C_n \cong \mathbb{F}[x]/\langle x^n - \lambda \rangle \cong \oplus_{i=1}^r \mathbb{F}[x]/\langle p_i(x) \rangle,$$

where $x^n - \lambda = \prod_{i=1}^{r} p_i(x)$. Since $\mathbb{F}[x]/\langle p_i(x) \rangle$ are fields for $1 \leq i \leq r$, it follows that r is the number of simple components of $\mathbb{F}^\gamma C_n$ so, using Theorem 3.1.11, we get that r is the number of regular cyclotomic γ-classes of C_n and we are done. □

Example 3.1.12. Let $\mathbb{F}_7$ be the field with 7 elements and C_4 the cyclic group of order 4. Then $k = |H^2(C_4, \mathbb{F}_7^*)| = gcd(6, 4) = 2$. As $(\mathbb{F}_7^*)^4 = \{1, 2\}$, we have that γ_6 is not cohomologous to γ_1, so, in this case $H^2(C_4, \mathbb{F}_7^*) = \{[\gamma_1], [\gamma_6]\}$. Let θ be a primitive root of unity of order 8. Then, the Galois group of $\mathbb{F}_7(\theta)$ over $\mathbb{F}_7$ is $\{I, \sigma\}$, where $\sigma(\theta) = \theta^7$. Note that every element of G is γ_6-regular, because γ_6 is symmetric. The cyclotomic γ_6-classes are

$$S_1 = \{\bar{1}\}, \quad S_{g^2} = \{\bar{g}^2, 6\bar{g}^2\}, \quad S_g = \{\bar{g}, \bar{g}^3\}.$$

Since $\eta_{g^2} = \bar{g}^2 + 6\bar{g}^2 = 0$ and $\eta_1, \eta_g \neq 0$ we get that the regular cyclotomic γ_6-classes are

$$S_{\bar{1}} = \{\bar{1}\} \quad \textit{and} \quad S_{\bar{g}} = \{\bar{g}, \bar{g}^3\}.$$

Then $\mathbb{F}_7^{\gamma_6} C_4$ has two simple components. This agrees with the usual polynomial approach, because $x^4 - 6 = p_1(x)p_2(x)$, where $p_1(x) = x^2 + 3x + 1$ and $p_2(x) = x^2 + 4x + 1$ are irreducible over $\mathbb{F}_7$. Thus

$$\frac{\mathbb{F}[x]}{\langle x^4 - 6 \rangle} \cong \frac{\mathbb{F}[x]}{\langle p_1(x) \rangle} \oplus \frac{\mathbb{F}[x]}{\langle p_2(x) \rangle} \cong \mathbb{F}_{7^2} \oplus \mathbb{F}_{7^2}.$$

3.2 MINIMAL IDEMPOTENTS OF $\mathbb{F}^\gamma C_n$

The following result is easy to prove.

Lemma 3.2.1. *Let $\mathcal{A}$ be a semisimple commutative $\mathbb{F}$-algebra with unity. Assume that $\mathcal{B}$ is a semisimple subalgebra of $\mathcal{A}$ with the same unity and for which every minimal idempotent of $\mathcal{B}$ is a minimal idempotent of $\mathcal{A}$. Then $\mathcal{B}$ and $\mathcal{A}$ have the same complete set of minimal idempotents.*

Let n be a positive integer with prime factorization $n = \prod_{i=1}^{r} p_i^{a_i}$. Let $\mathbb{F}$ be a finite field with q elements and $C_n = C_{p_1^{a_1}} \times \cdots \times C_{p_r^{a_r}}$ a cyclic group of order n generated by an element g, where $C_{p_i^{a_i}}$ is a cyclic group of order $p_i^{a_i}$ generated by $g_i = g^{n/p_i^{a_i}}$ for $1 \leq i \leq r$. We wish to find formulas for the minimal idempotents of a twisted group algebra $\mathbb{F}^{\gamma}C_n$, where $\gamma \in Z^2(C_n, \mathbb{F}^*)$.

Consider $\mathbb{F}^*$ as trivial C_n-module. From the proof of Lemma 3.1.1, we have that $\gamma_\lambda, \gamma_{\lambda'} \in Z^2(C_n, \mathbb{F}^*)$ are cohomologous if and only if $\lambda = \lambda'.N(a)$ for some $a \in \mathbb{F}^*$, where N is the norm map. Since the action of C_n in $\mathbb{F}^*$ is trivial, we have that $a^{g^i} = a$, for all $0 \leq i \leq n-1$, and so,

$$N(a) = \prod_{i=0}^{n-1} a^{g^i} = a^n.$$

By [22, Lemma 2.1.1], the C_n-graded $\mathbb{F}$-algebras $\mathbb{F}^{\gamma_\lambda}C_n$ and $\mathbb{F}^{\gamma_{\lambda'}}C_n$ are isomorphic, if and only if γ_λ and $\gamma_{\lambda'}$ are cohomologous. We conclude that $\mathbb{F}^{\gamma_\lambda}C_n$ and $\mathbb{F}^{\gamma_{\lambda'}}C_n$ are isomorphic as C_n-graded $\mathbb{F}$-algebras if and only if $\lambda = \lambda'.a^n$, for some $a \in \mathbb{F}^*$. Again by the proof of Lemma 3.1.1, if $\gamma \in Z^2(C_n, \mathbb{F}^*)$ and $\lambda = \prod_{k=0}^{n-1} \gamma(g, g^k)$, then

$$\mathbb{F}^{\gamma}C_n \cong \mathbb{F}^{\gamma_\lambda}C_n$$

as C_n-graded $\mathbb{F}$-algebras.

Assume that first $r = 2$. Set $\lambda = \lambda_1\lambda_2$ with $\lambda_1, \lambda_2 \in \mathbb{F}^*$. Consider $\gamma_{\lambda_i} \in Z^2(C_{p_i^{a_i}}, \mathbb{F}^*)$, with $i = 1, 2$. Set $\tilde{\gamma} = \gamma_{\lambda_1} \times \gamma_{\lambda_2} \in Z^2(C_n, \mathbb{F}^*)$. Since

$$\prod_{k=0}^{n-1} \tilde{\gamma}(g, g^k) = \prod_{i=0}^{p_1^{a_1}-1} \gamma_{\lambda_1}(g_1, g_1^i) \prod_{j=0}^{p_2^{a_2}-1} \gamma_{\lambda_2}(g_2, g_2^j) = \lambda_1\lambda_2 = \lambda$$

we conclude that $\tilde{\gamma}$ is cohomologous to $\gamma_\lambda \in Z^2(C_n, \mathbb{F}^*)$.

Proposition 3.2.2. *Let $\lambda = \lambda_1\lambda_2 \in \mathbb{F}^*$, $\gamma_\lambda \in Z^2(C_n, \mathbb{F}^*)$ and $\gamma_{\lambda_i} \in Z^2(C_{p_i^{a_i}}, \mathbb{F}^*)$, with $i = 1, 2$. Then*

$$\mathbb{F}^{\gamma_\lambda}C_n \cong \left(\mathbb{F}^{\gamma_{\lambda_1}}C_{p_1^{a_1}}\right) \otimes \left(\mathbb{F}^{\gamma_{\lambda_2}}C_{p_2^{a_2}}\right).$$

Proof. Define $\psi : \mathbb{F}^{\gamma_\lambda}C_n \to \left(\mathbb{F}^{\gamma_{\lambda_1}}C_{p_1^{a_1}}\right) \otimes \left(\mathbb{F}^{\gamma_{\lambda_2}}C_{p_2^{a_2}}\right)$ by $\psi(\overline{g_1g_2}) = \bar{g}_1 \otimes \bar{g}_2$. It is easy to see that ψ is an isomorphism of $\mathbb{F}$-algebras and the result follows. □

Corollary 3.2.3. *Let $\gamma_\lambda \in Z^2(C_n, \mathbb{F}^*)$ and $\gamma_{\lambda_i} \in Z^2(C_{p_i^{a_i}}, \mathbb{F}^*)$, with $i = 1, 2$. If $\lambda = \lambda_1 = \lambda_2$ then*

$$\mathbb{F}^{\gamma_\lambda} C_n \cong \left(\mathbb{F}^{\gamma_\lambda} C_{p_1^{a_1}}\right) \otimes \mathbb{F}C_{p_2^{a_2}} \cong \mathbb{F}C_{p_1^{a_1}} \otimes \left(\mathbb{F}^{\gamma_\lambda} C_{p_2^{a_2}}\right).$$

An easy consequence is the next result.

Corollary 3.2.4. *Let $n = \prod_{i=1}^{r} p_i^{a_i}$. Let $\gamma_\lambda \in Z^2(C_n, \mathbb{F}^*)$ and $\gamma_{\lambda_i} \in Z^2(C_{p_i^{a_i}}, \mathbb{F}^*)$, for some $1 \leq i \leq r$. Then*

$$\mathbb{F}^{\gamma_\lambda} C_n \cong \mathbb{F}C_{p_1^{a_1}} \otimes \cdots \otimes \left(\mathbb{F}^{\gamma_\lambda} C_{p_i^{a_i}}\right) \otimes \cdots \otimes \mathbb{F}C_{p_r^{a_r}}.$$

The following results will be very useful in the sequel.

Theorem 3.2.5. *[7, Theorem 3.1] Let $\lambda \in \mathbb{F}^*$ with order e. Then the binomial $X^t - \lambda$ is irreducible in $\mathbb{F}[X]$ if and only if the integer $t \geq 2$ satisfies the following conditions:*

1. *$gdc(t, (q-1)/e) = 1$;*
2. *each prime factor of t divides e;*
3. *if $4|t$ then $4|(q-1)$.*

Let $f(X), g(X) \in \mathbb{F}[X]$, and let $P(X) = \sum_{i=0}^{n} c_i X^i \in \mathbb{F}[X]$ of degree n. Then the following composition

$$P(f/g) = g(X)^n P(f(X)/g(X)) = \sum_{i=0}^{n} c_i f(X)^i g(X)^{n-i}$$

is again a polynomial in $\mathbb{F}[X]$.

Theorem 3.2.6. *[7, Theorem 3.7] Let $f(X), g(X) \in \mathbb{F}[X]$, and let $P(X) \in \mathbb{F}[X]$ be irreducible of degree n. Then $P(f/g) = g^n(X) P(f(X)/g(X))$ is irreducible over $\mathbb{F}$ if and only if $f(X) - \lambda g(X)$ is irreducible over $\mathbb{F}_{q^n}$ for some root $\lambda \in \mathbb{F}_{q^n}$ of $P(X)$.*

Let d be an integer and θ_d a primitive root of unity of order d. For any integer s denote by $(\mathbb{F}^*)^{(s)}$ the subgroup $\{a^s : a \in \mathbb{F}^*\}$ of $\mathbb{F}^*$. For a positive integer n and $\lambda \in \mathbb{F}^*$ we define

$$h_{n,q}(\lambda) = max\left\{s \in \mathbb{N} : s|n \text{ and } \lambda \in (\mathbb{F}^*)^{(s)}\right\}.$$

Let $\mathcal{O}_d(x)$ be the multiplicative order of x modulo the positive integer d.

Theorem 3.2.7. *Let $\gamma = \gamma_\lambda \in Z^2(C_n, \mathbb{F}^*)$ for $\lambda \in \mathbb{F}^*$. Let $h = h_{n,q}(\lambda)$ and $\lambda = b^h$, with $b \in \mathbb{F}^*$. Denote $\tilde{g} = b^{-1}\bar{g}^{n/h}$ and $\tilde{C}_h = \langle \tilde{g} \rangle$. Then, for any $d|h$, we have*

1. *$gdc\left((n/h), (q^{\mathcal{O}_d(q)} - 1)/\tilde{d}\right) = 1$;*
2. *each prime factor of n/h divides $\tilde{d}$;*
3. *if $4|(n/h)$ then $4|(q^{\mathcal{O}_d(q)} - 1)$,*

where $\tilde{d}$ is the multiplicative order of $b\theta_d$ in $\mathbb{F}^*_{q^{\mathcal{O}_d(q)}}$, if and only if the set of minimal idempotents of the twisted group algebra $\mathbb{F}^\gamma C_n$ coincides with the set of minimal idempotents of the group algebra $\mathbb{F}\tilde{C}_h$.

Proof. Since $\{\bar{g}^i : 0 \leq i \leq n-1\} \subset \mathbb{F}^\gamma C_n$ is linearly independent over $\mathbb{F}$, we have that $\tilde{C}_h$ is linearly independent over $\mathbb{F}$. As $\tilde{g}^h = b^{-h}\bar{g}^n = \lambda^{-1}\lambda = 1$ it follows that $\tilde{C}_h$ is a cyclic group of order h.

Let e be a minimal idempotent of $\mathbb{F}\tilde{C}_h$. By Perlis-Walker Theorem (See [37, Theorem 3.5.4]) we have that $(\mathbb{F}\tilde{C}_h)e \overset{\varphi}{\cong} \mathbb{F}(\theta_d)$ for some $d|h$ with $\varphi(\tilde{g}e) = \theta_d$ and $P_d(X)$ the minimal polynomial of $\tilde{g}e$ over $\mathbb{F}$. Now, we wish to prove that $(\mathbb{F}^\gamma C_n)e$ is a field.

Consider the homomorphism of $\mathbb{F}$-algebras $\psi : \mathbb{F}[X] \to (\mathbb{F}^\gamma C_n)e$ defined by $\psi(X) = \bar{g}e$. Let $f_d(X) = P_d(b^{-1}X^{n/h})$. Then

$$f_d(\bar{g}e) = P_d(b^{-1}\bar{g}^{n/h}e) = P_d(\tilde{g}e) = 0$$

and so, $f_d(X) \in Ker(\psi)$. By Theorem 3.2.6, $f_d(X)$ is irreducible over $\mathbb{F}$ if and only if $b^{-1}X^{n/h} - \theta_d \in \mathbb{F}_{q^{\mathcal{O}_d(q)}}[X]$ is irreducible, where θ_d is a root of $P_d(X)$. From Theorem 3.2.5, the polynomial $b^{-1}X^{n/h} - \theta_d = b^{-1}(X^{n/h} - b\theta_d)$ is irreducible if and only if the conditions 1, 2 and 3 are satisfied. Then, $f_d(X)$ is irreducible if and only if these conditions holds. Since $(\mathbb{F}^\gamma C_n)e$ is a field if and only if $f_d(X)$ is irreducible, the result follows. □

The above theorem is a natural generalization of the following result.

Proposition 3.2.8. *[29, Theorem 3.1] Let $\mathbb{F} = \mathbb{F}(\theta_4)$, let $G = \langle g \rangle$ be a cyclic group of order 2^n and let $\mathbb{F}^\gamma G$ be the twisted group algebra of G over $\mathbb{F}$ defined by equality $\bar{g}^{2^n} = \lambda \in \mathbb{F}^*$. Let $h_{n,q}(\lambda) = 2^s$ and $\lambda = b^{2^s}$, $b \in \mathbb{F}^*$. Let us denote $h = b^{-1}\bar{g}^{2^{n-s}}$. Then*

1. *$H = \langle h \rangle$ is a group of order 2^s and the elements of this group are linearly independent over $\mathbb{F}$, i.e., the group algebra $\mathbb{F}H$ is a subalgebra of $\mathbb{F}^\gamma G$.*

2. *The set of minimal idempotents of $\mathbb{F}^{\gamma}G$ coincides with the set of minimal idempotents of $\mathbb{F}H$.*

For a subset X of the cyclic group C_n such that $char(\mathbb{F})$ does not divide $|X|$, we shall denote by $\widehat{X}$ the following element of $\mathbb{F}C_n$:

$$\widehat{X} = \frac{1}{|X|}\sum_{x\in X} x.$$

Let p be a rational odd prime and $\gamma = \gamma_\lambda \in Z^2(C_{p^m}, \mathbb{F}^*)$. Assume that $h_{p^m}(\lambda) = p^s$, $\lambda = b^{p^s}$, for some $b \in \mathbb{F}^*$, and the conditions 1, 2 and 3 of the Theorem 3.2.7 holds. Then, we have the following result.

Theorem 3.2.9. *Let*

$$\tilde{C}_{p^s} = A_0 \supset A_1 \supset \cdots \supset A_s = \{1\}$$

be the descending chain of all subgroups of $\tilde{C}_{p^s} = \langle \tilde{g} \rangle$, where $\tilde{g} = b^{-1}\bar{g}^{p^{m-s}}$. If $\mathcal{O}_{p^s}(q) = \Phi(p^s)$ then the set of minimal idempotents of $\mathbb{F}^{\gamma}C_n$ are

$$e_0 = \frac{1}{p^s}\left(\sum_{a\in A_0} a\right) \tag{14}$$

and

$$e_i = \widehat{A_i} - \widehat{A_{i-1}}, \quad 1 \leq i \leq s. \tag{15}$$

Proof. By Theorem 3.2.7, the set of minimal idempotents of $\mathbb{F}^{\gamma}C_{p^m}$ are the set of minimal idempotents of $\mathbb{F}\tilde{C}_{p^s}$. Since $\mathcal{O}_{p^s}(q) = \Phi(p^s)$, we have by [39, Theorem 3.5] the formulas for the idempotents. □

Let $\lambda \in \mathbb{F}^*$ and n a positive integer such that $h = h_n(\lambda) = 2p^s$, where p is a rational odd prime integer. Then, $\lambda = b^h$ for some $b \in \mathbb{F}^*$.

Theorem 3.2.10. *Assume that the conditions 1, 2 and 3 of the Theorem 3.2.7 are satisfied. In addition, suppose that $\mathcal{O}_{p^s}(q) = \Phi(p^s)$. Let $\tilde{g}_1 = b^{-2}\bar{g}^{n/p^s}$, $\tilde{g}_2 = b^{-p^s}\bar{g}^{n/2}$ and $\tilde{C}_1 = \langle \tilde{g}_1 \rangle$, $\tilde{C}_2 = \langle \tilde{g}_2 \rangle = \{1, \tilde{g}_2\}$. Let*

$$\tilde{C}_1 = A_0 \supset A_1 \supset \cdots \supset A_s = \{1\}$$

be the descending chain of all subgroups of $\tilde{C}_1$. Then the complete set of minimal idempotents of $\mathbb{F}^{\gamma}C_n$ is $\{e_i f_j : 0 \leq i \leq s,\ j = 0, 1\}$ where

$$e_0 = \frac{1}{p^s}\left(\sum_{a\in A_0} a\right), \quad f_0 = \frac{1}{2}(1 + \tilde{g}_2), \quad f_1 = 1 - f_0 \tag{16}$$

and

$$e_i = \widehat{A_i} - \widehat{A_{i-1}}, \quad 1 \leq i \leq s. \tag{17}$$

Proof. First notice that $\tilde{C}_h = \tilde{C}_1 \times \tilde{C}_2$, where $\tilde{C}_n = \langle \tilde{g} \rangle$, $\tilde{g} = b^{-1}\bar{g}^{n/h}$ and $|\tilde{C}_1| = p^s$, $|\tilde{C}_2| = 2$. By Theorem 3.2.7, the complete set of minimal idempotents of $\mathbb{F}^\gamma C_n$ is the complete set of minimal idempotents of $\mathbb{F}\tilde{C}_h$.

Let $\mathbb{F}\tilde{C}_1 \cong \oplus_{i=1}^{t_1} \mathbb{F}_{d_i}$, where $d_i = [\mathbb{F}_{d_i} : \mathbb{F}]$, and $\mathbb{F}\tilde{C}_2 \cong \mathbb{F} \oplus \mathbb{F}$. Then

$$\mathbb{F}\tilde{C}_h \cong \mathbb{F}\tilde{C}_1 \otimes_{\mathbb{F}} \mathbb{F}\tilde{C}_2 \cong \left(\oplus_{i=1}^{t_1} \mathbb{F}_{d_i}\right) \otimes_{\mathbb{F}} (\mathbb{F} \oplus \mathbb{F}) \cong \oplus_{i=1}^{t_1} 2\mathbb{F}_{d_i}.$$

Thus $2t_1$ is the number of minimal idempotents of $\mathbb{F}\tilde{C}_h$. Notice that, if $e \in \mathbb{F}\tilde{C}_1$ and $f \in \mathbb{F}\tilde{C}_2$ are minimal idempotents, then $(\mathbb{F}\tilde{C}_h)ef \cong (\mathbb{F}\tilde{C}_1)e \otimes_{\mathbb{F}} (\mathbb{F}\tilde{C}_2)f$ which is a field. Then, the product of minimal idempotents of $\mathbb{F}\tilde{C}_1$ and $\mathbb{F}\tilde{C}_2$ forms a complete set of minimal idempotents of $\mathbb{F}\tilde{C}_h$. Since $\mathcal{O}_{p^s}(q) = \Phi(p^s)$ by [39, Theorem 3.5] we get that formulas for the minimal idempotents of $\mathbb{F}\tilde{C}_1$ and $\mathbb{F}\tilde{C}_2$ are given by equations 16 and 17. □

We shall now determine the minimum distance and dimension of minimal codes in twisted group algebras of cyclic groups of order p^m. Let $\gamma = \gamma_\lambda \in Z^2(C_{p^m}, \mathbb{F}^*)$ with $\lambda \in \mathbb{F}^*$ and $h_{p^m}(\lambda) = p^s$. Suppose that all assumptions of Theorem 3.2.9 are satisfied. Then, the set of minimal idempotents of $\mathbb{F}^\gamma C_{p^m}$ is $\{e_i : 0 \leq i \leq s\}$ where e_i are given by equations 14 and 15.

Note that $\{\tilde{g}^i\bar{g}^e : 0 \leq i < p^s, 0 \leq e < p^{m-s}\}$ is a basis of $\mathbb{F}^\gamma C_n$ over $\mathbb{F}$. Let τ_i be a transversal A_{i-1} in $\tilde{C}_{p^m}$. As A_{i-1}/A_i is a cyclic group of order p we have that $A_{i-1} =< a_i, A_i >$. Since $\mathcal{B}_0 = \{t(1-a_i)\widehat{A_i} : t \in \tau_i\}$ is a basis of $(\mathbb{F}\tilde{C}_{p^m})e_i$ over $\mathbb{F}$ (See [?, Proposition 2.1]), we get that

$$\mathcal{B} = \{v\bar{g}^e : v \in \mathcal{B}_0,\ 0 \leq e < p^{m-s}\}$$

is a basis of $\mathbb{F}^\gamma C_{p^m} e_i$ over $\mathbb{F}$. Then, we conclude that the minimum distance of $\mathbb{F}^\gamma C_{p^m} e_i$ is

$$w((\mathbb{F}^\gamma C_{p^m})e_i) = 2p^{m-i}$$

and the dimension is

$$dim_{\mathbb{F}}((\mathbb{F}^\gamma C_{p^m})e_i) = p^{m-s}\Phi(p^i),$$

where Φ is the Euler's totient function.

3.3 AN EXAMPLE

For each positive integer n, prime power q and $\lambda \in \mathbb{F}^*$, we shall use the following function in GAP [17] to compute $h_{n,q}(\lambda)$.

```
h:=function(q, n, lambda)
local L1, field, L3, UnitsField, UnitsFd, D, d, i, j;
L1:=[];
field:=AsList(GF(q));
L3:=[];
UnitsField:=field[2..q];
D:=DivisorsInt(n);
for d in D do
UnitsFd:=[];
for i in [1..(q-1)] do
Add(UnitsFd, UnitsField[i]^d);
od;
Add(L1, UnitsFd);
od;
for j in [1..Length(D)] do
if lambda in L1[j] and lambda in field then Add(L3, D[j]); fi;
od;
return Maximum(L3);
end;
```

For any $\alpha \in \mathbb{F}^*$ denote by $o(\alpha)$ the multiplicative order of α. Now, we shall proceed with the examples.

Example 3.3.1. Let $n = 65$, $C_n = \langle g \rangle$, $q = 27$ and let λ be a generator of $\mathbb{F}^*$. Then, $h = h_{65,27}(\lambda) = 5$ and $n/h = 13$. Since $1 = 26 + (-5).5$ and $-5 \equiv 21 \ (mod\ 26)$, we have that $b = \lambda^{21}$ satisfies $\lambda = b^5$.

If $d = 1$ then $\tilde{d} = o(b) = 26$. The conditions of Theorem 3.2.7 are satisfied:

1. $gdc\left((n/h), (q^{\mathcal{O}_d(q)} - 1)/\tilde{d}\right) = gdc(13, (27-1)/26) = 1$;
2. each prime factor of $n/h = 13$ divides $\tilde{d} = 26$;

3. This condition is trivially true, because $4 \nmid 13$.

If $d = 5$ then $\tilde{d} = o(b\theta_5) = 130$. Again, the conditions of Theorem 3.2.7 are satisfied:

1. $gdc\left((n/h), (q^{\mathcal{O}_d(q)} - 1)/\tilde{d}\right) = gdc(13, (27^4 - 1)/130) = gdc(13, 4088) = 1$;
2. each prime factor of $n/h = 13$ divides $\tilde{d} = 130$;
3. This condition is trivially true, because $4 \nmid 13$.

By Theorem 3.2.7, we conclude that the minimal idempotents of $\mathbb{F}_{27}^{\gamma_\lambda} C_{65}$ are the minimal idempotents of $\mathbb{F}_{27}\langle\tilde{g}\rangle$, where $\tilde{g} = \lambda^5 \bar{g}^{13}$. Since $\langle\tilde{g}\rangle$ is cyclic of order 5, we have that

$$e_0 = (1/2) \sum_{k=0}^{4} (\lambda^5 \bar{g}^{13})^k \quad \text{and} \quad e_1 = 1 - (1/2) \sum_{k=0}^{4} (\lambda^5 \bar{g}^{13})^k$$

are the minimal idempotents of $\mathbb{F}_{27}^{\gamma_\lambda} C_{65}$.

BIBLIOGRAPHY

[1] G. K. Bakshi, M. Raka, A Class of Constacyclic Codes over a Finite Field, Finite Fields Their Appl. , **182** 362-377 (2012).

[2] E. R. Berlekamp, Algebraic Coding Theory, Laguna Hills, CA: Aegean Park Press (1984).

[3] E. R. Berlekamp, Negacyclic Codes for the Lee Metric, chap. 17 in Bose, Dowling (eds), "Proceedings of the Conference on Combinatorial Mathematics and Its Applications (April 1967)", The University of Carolina Press, Chapel Hill, published 1969.

[4] J. J. Bernal, A. del Río and J. J. Simón, An Intrinsical Description of Group Codes, Des. Codes Cryptogr., **51**(3) 289-300 (2009).

[5] S. D. Berman, On the theory of group codes, Cybern Syst Anal **3** 25–31 (1967).

[6] I. F. Blake, Codes Over Certain Rings, Information and Control **20** 396-404 (1972).

[7] I. F. Blake, X. Gao, R. C. Mullin, S. A. Vanstone, T. Yaghoobian, Applications of finite fields, Springer (1993).

[8] C. Gladys, R. A. Ferraz, C. Polcino, Essential Idempotents and Simplex Codes, Algebra Comb. Discrete Appl. **4**(2) 181–188 (2016).

[9] P. Charpin. Les codes de Reed-Solomon en tant qu'idéaux d'une algèbre modulaire. C.R. Acad. Sci. Paris, t.294, Série I:597-600 (1982).

[10] B. Chen, Y. Fan, L. Lin, H. Liu, Constacyclic Codes over Finite Fields, Finite Fields Their Appl., **18**(6) 1217-1231 (2012).

[11] B. Chen, H. Q. Dinh, H. Liu, L. Wang, Constacyclic Codes of Length $2p^s$ over $\mathbb{F}_p^m + u\mathbb{F}_p^m$, Finite Fields Their Appl. ,**37** 108-130 (2016).

[12] H. Q. Dinh, Constacyclic Codes of Length p^s over $\mathbb{F}_p^m + u\mathbb{F}_p^m$, Journal of Algebra, **324**(5) 940-950 (2010).

[13] L. Esteban, R. Tapia-Rojo, A. Sancho, L. J. Boya, Groups of order less than 32, revisited, Rev. Real Academia de Ciencias. Zaragoza. **66** 63–104, (2011)

[14] R. A. Ferraz, Simple Components and Central Units in Group Algebras, Journal of Algebra, **279**(1) 191-203 (2004).

[15] R. A. Ferraz, C. Polcino Milies, Idempotents in Group Algebras and Minimal Abelian Codes, Finite Fields Their Appl., **13**2 382-393 (2007).

[16] A. B. Fontaine and W. W. Peterson, "Group code equivalence and optimum codes", IEEE Trans. Inf. Theory, vol. IT-5, **5** 60-70 (1959).

[17] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.5.6; 2012. (http://www.gap-system.org).

[18] M. J. E. Golay, Notes on digital coding, Proceedings of the IRE 37, **657** (1949).

[19] R. W. Hamming, Error detecting and error correcting codes , Bell System Technical Journal **29** 147-160 (1950).

[20] K. Hoffman, R. Kunze, Linear Algebra, 2nd ed., Prentice-Hall, New Jersey (1971).

[21] E. Jespers, G. Leal , A. Paques, Central Idempotents in the Rational Group Algebra of a Finite Nilpotent Group, J of Algebra and Its Appl. **2** 57-62 (2003).

[22] G. Karpilovsky, Group representations Vol. 2, North-Holland Mathematics Studies (1993).

[23] G. Karpilovsky, Group Representations Vol. 3, North-Holland Mathematics Studies (1994).

[24] P. Landrock and O. Manz, Classical Codes as Ideals in Group Algebras, Designs, Codes and Cryptography, **2** 273-285 (1992).

[25] R. Lidl, , H.Niederreiter, Finite Fields 2nd ed., Encyclopedia of Mathematics and its Applications, Cambridge: Cambridge University (1996).

[26] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.

[27] H. F. Mattson and G. Solomon, A new treatment of Bose-Chaudhuri codes, J. Soc. Ind. Appl. Math **9** 654-669 (1961).

[28] B. R. McDonald, Finite rings with identity, M. Dekker (1974).

[29] T. Zh. Mollov, N. A. Nachev, Minimal Idempotents of Twisted Group Algebras of cyclic 2-groups, South. Asian Bulletin of Mathematics, **26**(4) 593-601 (2002).

[30] G. Nebe, A.Schäfer, A Nilpotent non Abelian Group Code, Algebra and Discrete Mathematics , **18**(2) (2014).

[31] G. Olteanu and I. Van Gelder, Construction of minimal non-abelian left group codes, Designs Codes and Cryptography (2013).

[32] D. S.Passman, *Infinite Crossed Products*, Pure and applied mathematics v. 135.

[33] D. S. Passman, The Algebraic Structure of Group Rings, John Wiley and Sons, New York, 1985.

[34] W. W. Peterson and D. T. Brown, Cyclic Codes for Error Detection, in Proceedings of the IRE, **49** 228-235, (1961).

[35] W. W. Peterson, Error Correcting Codes, MIT Press, Cambridge Massachusetts (1961).

[36] C. G. Pillado, S. Gonzales and C. Martínez, V. Markov and A. Nechaev, GROUP CODES OVER NON-ABELIAN GROUP, Journal of Algebra and Its Applications Vol. 12, No. 7 (2013).

[37] C. Polcino Milies, S.K. Sehgal, An Introduction to Group Rings, Kluwer Academic Publishers, Dordrecht, Boston, London (2002).

[38] E. Prange, Cyclic Error-Correcting Codes in Two Symbols. AFCRC-TN-57-103, Air Force Cambridge Research Center, Cambridge, Mass. (1957).

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

[40] S. Roman, Coding and Information Theory, New York, NY (1992).

[41] W. F. Reynolds, Twisted Group Algebras over Arbitrary Fields, Illinois J. of Mathematics , **15** 91-103 (1971).

[42] D. J. S. Robinson, A Course in the Theory of Groups, Second Edition, Springer (1996).

[43] J. J. Rotman, An Introduction to Homological Algebra, 2nd ed., Universitext Berlin, Springer (2009).

[44] P. Shankar, On BCH codes over arbitrary integer rings, IEEE Trans. Inform. Theory, IT-25 **4** 480-483 (1979).

[45] C. E. Shannon, A Mathematical Theory of Communication, The Bell System Technical Journal Vol. XXVII **3** (1948).

[46] D. Slepian, A class of binary signalling alphabets, Bell System Technica Journal, **35** 203-234 (1956).

[47] E. Spiegel, Codes over $\mathbb{Z}_m$, Information and Control **35** 48-51 (1977).

[48] A. W. Tucker, A Combinatorial Equivalence of Matrices, presented at Symposium on Combinatorial Design and Analysis (1958).

[49] E. Witt, Die algebraische Struktur des Gruppenringes einer endlichen Gruppe über einem Zahlkörper, J. für die reine und ang. Mathematik **1952**(190) (1952).