# Idempotentes geradores de códigos minimais

Janete do Prado

Tese apresentada
ao
Instituto de Matemática e Estatística
da
Universidade de São Paulo
para
obtenção do título
de
Doutor em Ciências

Programa: Matemática

Orientador: Prof. Dr. Francisco César Polcino Milies

São Paulo, 12 de abril de 2010

# Idempotentes geradores de códigos minimais

Esta versão definitiva da tese contém as correções e alterações sugeridas pela Comissão Julgadora durante a defesa realizada por Janete do Prado em 4/3/2010.

Comissão Julgadora:

- Prof. Dr. Francisco César Polcino Milies (orientador) - IME-USP
- Prof. Dr. Raul Antonio Ferraz - IME-USP
- Profa. Dra. Marinês Guerreiro - UFV
- Prof. Dr. Guilherme Augusto de La Rocque Leal - UFRJ
- Prof. Dr. Thierry Corrêa Petit Lobão - UFBA

"O ser humano não pode deixar de cometer erros;
é com erros que os homens de bom senso aprendem
a sabedoria para o futuro."

*Plutarco*

Ao meu marido,
Danilo

*dedico.*

# Agradecimentos

Agradeço:

A Deus.

Ao meu marido, Danilo Carlos da Graça Silva, que sempre me incentivou com amor, carinho e compreensão.

À minha família: Zeny Urdiali e Paulo do Prado, meus pais, e minha irmã Márcia Cristina do Prado; por todo apoio e pelo que fizeram ao longo da minha vida.

Aos meus sogros: Maria A. da Graça Silva e Carlos Pereira da Silva; por sempre estarem ao meu lado me apoiando e incentivando.

Ao Prof. Dr. Francisco César Polcino Milies, que me orientou durante este trabalho com paciência, amizade e dedicação.

À banca examinadora.

Aos professores do Departamento de Matemática do IME - USP que de alguma forma contribuíram para este trabalho, em especial para Raul Ferraz por sugestões importantes dadas enquanto este trabalho estava em andamento.

Aos professores da graduação, da FCT - UNESP, e aos do mestrado, do IBILCE - UNESP, por terem auxiliado no meu processo de aprendizagem.

# Resumo

Seja F um corpo de característica prima ímpar $p$. Neste trabalho exibimos uma família de $m+1$ idempotentes na álgebra de grupo $\mathrm{F}C_{2^m}$, uma base para os ideais (códigos) gerados por estes idempotentes, a dimensão e a distância mínima dos códigos correspondentes. Dessa forma, foram determinados códigos cíclicos minimais de comprimento $2^m$ em termos de seus idempotentes primitivos, e estes resultados foram estendidos, via levantamento de idempotentes, para alguns grupos abelianos finitos G tal que $\mathrm{G} \supset C_{2^m}$.

**Palavras-chave:** idempotentes, dimensão, distância mínima, levantamento de idempotentes.

# Abstract

Let F be a finite field of odd prime charateristic $p$. In this work we exhibit a family of $m+1$ idempotents in the group algebra $\mathrm{F}C_{2^m}$, bases for the ideals (codes) generated by these idempotents, and compute the dimension and minimum distance of the corresponding codes. Cyclic minimal codes of length $2^m$ are determined in terms of the primitive idempotents, and these results are extended, by lifting idempotents, to some finite abelian groups G such that $\mathrm{G} \supset C_{2^m}$.

**Keywords:** idempotents, dimension, minimum distance, lifting idempotents.

# Sumário

# Introdução

O objetivo principal deste trabalho foi estudar códigos corretores de erros utilizando técnicas de Álgebras de Grupo. Nesta perspectiva, um código é um ideal de uma álgebra de grupo finita. Para estudar códigos da álgebra vamos nos restringir aos códigos minimais. Assim, procuramos determinar os idempotentes primitivos de uma determinada álgebra, bem como a dimensão, a distância mínima e uma base para os códigos gerados por estes idempotentes.

Os idempotentes geradores de códigos cíclicos vem sendo estudados sistematicamente há bastante tempo. Em 1997, Arora e Pruthi estudaram códigos cíclicos de comprimento $p^n$ (com $p$ primo) [14] e, dois anos mais tarde, códigos de comprimento $2p^n$ [1].

Mudando o ponto de vista e usando técnicas de Álgebras de Grupo, Ferraz e Polcino Milies obtiveram estes mesmos resultados de forma bem mais simples e os estenderam para códigos abelianos. Essa mesma abordagem permitiu a F.S. Dutra obter geradores idempotentes para códigos minimais em Álgebras de Grupo Dihedrais e de Quatérnios [4] (Veja também Dutra, Ferraz e Polcino Milies [5]).

Ainda, Pruthi determinou geradores idempotentes para códigos cíclicos de comprimento $2^m$, embora estes idempotentes não sejam primitivos [13].

O ponto de partida desta tese foi tratar os resultados de Pruthi do ponto de vista das Álgebras de Grupo e, a partir destas ideias, determinar conjuntos completos de idempotentes primitivos.

O Capítulo 1 consiste numa revisão de conceitos e resultados da Teoria de Álgebras de Grupo, da Teoria de Códigos Corretores de Erros e sobre resíduos quadráticos, que usaremos ao longo deste trabalho. Em particular, são muito importantes resultados sobre levantamento

de idempotentes e sobre o número de componentes simples de uma álgebra de grupo, pois estes serão utilizados no desenvolvimento do Capítulo 3, principal capítulo deste trabalho.

No Capítulo 2, obtemos resultados sobre os códigos cíclicos gerados por idempotentes numa álgebra de grupo semisimples, de um grupo cíclico de ordem $2^m$. Determinamos a dimensão e a distância mínima destes códigos de um modo bem mais simples do que foi feito por Pruthi [13], que usou métodos polinomiais para estudar esses códigos. Além disso, exibimos uma base para tais códigos. Bases semelhantes foram obtidas em [5] para ideais gerados por idempotentes de uma determinada forma, em Álgebras de Grupo semisimples. Porém, as bases que obtivemos têm uma expressão mais simples do que as conhecidas.

Em [6], foram estudados códigos cíclicos minimais no caso em que o expoente do grupo G é $p^n$ ou $2p^n$, sobre um corpo $\mathrm{F}_q$ de ordem $q$ tal que $(q, |\mathrm{G}|) = 1$. Neste caso, os idempotentes primitivos são parecidos com os idempotentes obtidos no Capítulo 2.

O Capítulo 3 foi desenvolvido com o objetivo de explicitar os idempotentes primitivos da álgebra de grupo $\mathrm{F}_q\mathrm{G}$, onde $\mathrm{F}_q$ é um corpo tal que $q$ é uma potência de um primo ímpar $p$ e G é um grupo cíclico de ordem $2^m$.

Nos casos estudados, determinamos ainda os parâmetros importantes dos códigos correspondentes, isto é, obtivemos a dimensão e a distância mínima. Mais ainda, nestes casos demos também uma descrição explícita de uma base do ideal, o que permite, se desejado, descrever facilmente o processo de codificação correspondente. Os resultados deste capítulo são novos e não se encontram na literatura.

O Capítulo 4 apresenta resultados sobre ideais principais nilpotentes de uma álgebra de grupo de um grupo comutativo, que foram feitos por Poli [12] usando anéis de polinômios em várias variáveis. Neste trabalho, mostramos como resultados podem ser obtidos de maneira bem mais simples usando a Teoria de Álgebra de Grupo.

Além disso, mostramos como se pode efetuar de fato o levantamento de idempotentes em alguns casos, em que os resultados dos capítulos anteriores são utilizados.

# Capítulo 1

# Preliminares

Neste capítulo, veremos alguns conceitos e resultados que foram necessários para o desenvolvimento deste trabalho. Apesar da maioria das definições e resultados serem válidas para um anel R, não necessariamente um corpo, todo capítulo foi adaptado para uma álgebra de grupo FG, para um corpo F, pois todos os resultados obtidos neste trabalho, o foram no contexto de álgebra de grupo sobre corpos.

## 1.1 Álgebra de Grupo

O conteúdo desta seção pode ser encontrado em [10]. Sejam F um corpo finito com $|\mathrm{F}| = q$ elementos, sendo $q$ uma potência de um primo $p$, G um grupo abeliano finito de ordem $n$ e FG a álgebra de grupo correspondente.

**Definição 1.1.1** *O homomorfismo* $\epsilon : \mathrm{FG} \longrightarrow \mathrm{F}$ *dado por* $\epsilon\left(\sum_{g\in \mathrm{G}} \alpha_g g\right) = \sum_{g\in \mathrm{G}} \alpha_g$ *é dito a aplicação de aumento de* FG *e seu núcleo* $Ker(\epsilon) = \left\{\sum_{g\in \mathrm{G}} \alpha_g(g-1) : g \in \mathrm{G}, g \neq 1\right\}$, *denotado por* $\Delta(\mathrm{G})$, *é chamado o ideal de aumento de* FG.

**Proposição 1.1.1** *Se* H *é um subgrupo de* G *então*

$$\Delta(\mathrm{G},\mathrm{H}) = \left\{\sum_{h,t} \alpha_{ht} t(h-1) : h \in \mathrm{H}, h \neq 1, t \in \tau\right\}$$

*é um ideal de* FG, *onde* $\tau$ *é um transversal de* H *em* G.

**Corolário 1.1.1** *Se* H *é um subgrupo normal de* G, *então* $\dfrac{\mathrm{FG}}{\Delta(\mathrm{G},\mathrm{H})} \cong \mathrm{F}\left(\dfrac{\mathrm{G}}{\mathrm{H}}\right)$.

**Teorema 1.1.1** *Se* H *é um subgrupo normal de* G, *então* $\widehat{\mathrm{H}} = \dfrac{1}{|\mathrm{H}|}\sum_{h\in\mathrm{H}} h$ *é um idempotente central de* FG *e tem-se*

$$(\mathrm{FG})\widehat{\mathrm{H}} \cong \mathrm{F}\left(\frac{\mathrm{G}}{\mathrm{H}}\right).$$

**Teorema 1.1.2** *(Maschke) Sejam* G *um grupo finito e* F *um corpo. Então a álgebra de grupo* FG *é semisimples se, e somente se,* $car(\mathrm{F}) \nmid |\mathrm{G}|$.

**Teorema 1.1.3** *(Perlis-Walker) Sejam* G *um grupo abeliano finito de ordem* $n$ *e* F *um corpo tal que* $car(\mathrm{F}) \nmid n$. *Então* $\mathrm{FG} \cong \oplus_{d|n} a_d \mathrm{F}(\zeta_d)$, *onde* $\zeta_d$ *é raiz* $d$*-ésima primitiva da unidade,* $a_d = \dfrac{n_d}{[\mathrm{F}(\zeta_d):\mathrm{F}]}$ *e* $n_d$ *denota o número de elementos de ordem* $d$ *em* G.

A seguir veremos alguns fatos sobre o radical de uma álgebra, com o objetivo de estabelecer quando o ideal $\Delta(\mathrm{G},\mathrm{H})$ coincide com o radical de FG.

**Definição 1.1.2** *Seja* FG *uma álgebra de grupo. O radical de Jacobson de* FG, *denotado por* J(FG), *é a interseção de todos os ideais maximais de* FG.

**Definição 1.1.3** *Um ideal* I *de* FG *é dito nilpotente se existe um inteiro positivo* $n$ *tal que* $\mathrm{I}^n = (0)$.

**Proposição 1.1.2** *Todo ideal nilpotente de* FG *está contido no seu radical de Jacobson.*

**Teorema 1.1.4** *(Hopkins) Se* FG *é um anel artiniano, então* J(FG) *é um ideal nilpotente de* FG.

**Teorema 1.1.5** *Seja* FG *semisimples. Então* FG *é um anel artiniano e vale uma das seguintes condições equivalentes:*

(i) FG *não contém ideais bilaterais nilpotentes não nulos;*

(ii) FG *não contém ideais à esquerda nilpotentes não nulos;*

(iii) $\mathrm{J}(\mathrm{FG}) = (0)$.

*Por outro lado, se* FG *é um anel artiniano e uma das condições acima vale, então* FG *é semisimples.*

**Teorema 1.1.6** *Seja* FG *a álgebra de grupo de um grupo finito sobre um corpo* F *de característica* $p \geq 0$. *Então* FG *tem um ideal nilpotente não nulo se, e somente se,* $p > 0$ *e* $p \mid |G|$.

**Teorema 1.1.7** *(Coleman) Sejam* F *um corpo de característica* $p \geq 0$ *e* G *um grupo. Então o ideal de aumento* $\Delta(G)$ *de* FG *é nilpotente se, e somente se,* $p > 0$ *e* G *é um p-grupo finito.*

**Corolário 1.1.2** *Se* G *tem um p-subgrupo normal finito* P, *onde* $0 < p$ *é a característica de* F, *então* $\Delta(G, P)$ *é nilpotente.*

Como consequência, temos que se $G = P \times B$, onde P é um $p-$subgrupo e B é um $p'-$subgrupo, então, pelo Corolário 1.1.1, $\frac{FG}{\Delta(G,P)} \cong FB$ é semisimples, e daí, pelo Teorema 1.1.5, $\Delta(G,P) = J(FG)$.

## 1.2 Levantamento de Idempotentes

O fato do radical ser nilpotente, nos permitirá investigar álgebras não semisimples via levantamento de idempotentes módulo o radical. Nesta seção, veremos alguns resultados sobre levantamento de idempotentes (veja [3, capítulo 3 (seção 3.2)]).

**Definição 1.2.1** *Um idempotente* $e$ *é dito minimal ou primitivo, se ele não pode ser escrito na forma* $e = e' + e''$, *com* $e'$ *e* $e''$ *idempotentes ortogonais não nulos.*

**Lema 1.2.1** *Sejam* I *um ideal nilpotente de uma álgebra de grupo de dimensão finita* FG *e* $u \in FG$ *tal que* $u^2 \equiv u \ (mod\ I)$. *Então existe um idempotente* $e \in FG$ *tal que* $e \equiv u \ (mod\ I)$.

O Lema 1.2.1, nos dá uma caracterização das álgebras de grupo cujo módulo regular é indecomponível.

**Teorema 1.2.1** *São equivalentes:*

(i) *O* FG*-módulo regular é indecomponível;*

(ii) $\frac{\mathrm{FG}}{\mathrm{J(FG)}}$ *é uma álgebra com divisão;*

(iii) *Existe um único ideal maximal na álgebra* FG*;*

(iv) *Os elementos não inversíveis da álgebra* FG *formam um ideal de* FG.

As álgebras de grupo que satisfazem as condições do Teorema 1.2.1, são chamadas *locais.*

**Corolário 1.2.1** *Um* FG *- módulo é indecomponível se, e somente se, sua álgebra de endomorfismos é local.*

**Proposição 1.2.1** *Um idempotente* $e \in \mathrm{FG}$ *é minimal se, e somente se, o idempotente* $\overline{e} = e + \mathrm{J(FG)}$ *da álgebra de grupo quociente* $\overline{\mathrm{FG}} = \frac{\mathrm{FG}}{\mathrm{J(FG)}}$ *é minimal.*

Esta Proposição nos diz que existe uma correspondência um a um entre os idempotentes primitivos de FG e os da álgebra quociente $\frac{\mathrm{FG}}{\mathrm{J(FG)}}$. No entanto, no caso abeliano, todos os idempotentes primitivos de FG são exatamente os mesmos de FG módulo radical.

## 1.3 Códigos

Nesta seção enunciaremos alguns conceitos fundamentais da Teoria de Códigos Corretores de Erros.

Considere F um corpo finito com $q$ elementos, sendo $q$ uma potência de um primo $p$, G um grupo cíclico de ordem $n$ gerado por $g$, e FG a álgebra de grupo correspondente.

**Definição 1.3.1** *Um código linear é um subespaço próprio de* $\mathrm{F}^n$*, onde* F *é um corpo finito. Códigos de grupo são ideais (próprios) de* FG*. Se* G *é um grupo cíclico ou abeliano, então dizemos que os ideais de* FG *são códigos cíclicos ou abelianos, respectivamente. Ainda, os ideais minimais de* FG *são ditos códigos minimais.*

**Definição 1.3.2** *Sejam* I *um ideal de* FG *e* $\alpha = \sum_{g \in \mathrm{G}} \alpha_g g, \beta = \sum_{g \in \mathrm{G}} \beta_g g \in \mathrm{I}$*. A distância de Hamming entre* $\alpha$ *e* $\beta$ *é o número de elementos do suporte de* $\alpha - \beta$ *em que os coeficientes diferem, isto é,*

$$d(\alpha, \beta) = |\{g | \alpha_g \neq \beta_g, g \in \mathrm{G}\}|.$$

*O peso ou distância mínima do ideal* I *é definido por*

$$w(\mathrm{I}) = min\{d(\alpha, \beta) | \alpha \neq \beta, \alpha, \beta \in \mathrm{I}\}.$$

*O peso de um elemento* $\alpha \in \mathrm{I}$ *é dado por* $w(\alpha) = d(\alpha, 0)$.

Um código de FG é um ideal, portanto, ele é, em particular, um espaço vetorial de dimensão finita sobre o corpo finito F. Então ele possui uma base.

**Definição 1.3.3** *Considere* B *uma base de um código de grupo* I. *Dizemos que* B *é visível se, para todo subconjunto* B′ *de* B, *o peso do subespaço gerado por* B′ *é o peso de algum elemento de* B′.

**Definição 1.3.4** *Sejam* I *um ideal e* $x \in \mathrm{I}$. *Dizemos que* $s$ *é o índice de nilpotência de* $x$ *se* $x^s = 0$ *e* $x^{s-1} \neq 0$.

## 1.4 O número de componentes simples de FG

Considere $\mathrm{G} = \langle a \mid a^{2^m} = 1 \rangle$ o grupo cíclico de ordem $2^m$ gerado por $a$ e F um corpo finito com $q$ elementos, sendo $q$ uma potência de um primo ímpar. Seja $\zeta$ uma raiz $2^m$-ésima primitiva da unidade. O grupo de Galois $Gal(\mathrm{F}(\zeta), \mathrm{F})$ é gerado pelo automorfismo de Frobenius, $\zeta \longmapsto \zeta^q$. Chama-se a *F-classe correspondente a um elemento* $g \in \mathrm{G}$, ou também a *q - classe ciclotômica de g*, ao conjunto $\{g, g^q, g^{q^2}, \dots\}$. Por outro lado, o grupo de Galois $Gal(\mathbb{Q}(\zeta), \mathbb{Q})$ é isomorfo ao grupo $\mathcal{U} = \mathcal{U}(\mathbb{Z}_{2^m})$ das unidades dos inteiros módulo $2^m$ e, neste caso, chama-se a $\mathbb{Q}$ - classe correspondente a um elemento $g \in \mathrm{G}$ ao conjunto $\{g, g^3, g^5, \dots\}$ das potências ímpares de $g$. Note que este conjunto é precisamente o conjunto de todos os geradores do subgrupo cíclico $\langle g \rangle$. Assim, o número de $\mathbb{Q}$ - classes de G é o número de subgrupos cíclicos de G. Agora, dado $g \in \mathrm{G} = \langle a \rangle$, existe $r \in \mathbb{N}$ tal que $g = a^r$, logo a F - classe de $a^r$ denotada por $\mathcal{C}_{\mathrm{F}}(a^r)$ e a $\mathbb{Q}$ - classe de $a^r$ denotada por $\mathcal{C}_{\mathbb{Q}}(a^r)$ são, respectivamente, $\{a^r, a^{rq}, a^{rq^2}, \dots\}$ e $\{a^r, a^{3r}, a^{5r}, \dots\}$.

Sabemos que o número de componentes simples de FG é igual ao número de F - classes de FG (veja [6, Teorema 2.1]).

Os próximos resultados estão em [7], no entanto, vamos incluir uma demonstração para preservar a unidade da exposição.

**Lema 1.4.1** *Para todo inteiro $r \geq 3$ e todo inteiro ímpar $q$, a ordem de $q$ $(mod\ 2^r)$ é menor ou igual a $2^{r-2}$. Se $q \equiv 3\ (mod\ 8)$, então a ordem de $q$ é precisamente $2^{r-2}$.*

Demonstração: Sabemos que o grupo das unidades $\mathbb{Z}_{2^r}$ é $C_2 \times C_{2^{r-2}}$ e que se $q \equiv 5\ (mod\ 8)$, então $\overline{q}$ tem ordem no máximo $2^{r-2}$ (veja [8, Proposição 4.2.2]). Assim, a importância desse Lema é que se $q \equiv 3\ (mod\ 8)$, então $q$ tem ordem $2^{r-2}$ módulo $2^m$. Veremos que é suficiente provar para $q \equiv 5\ (mod\ 8)$, pois o caso $q \equiv 3\ (mod\ 8)$ segue desse fato.

Considere $A = \{5^{2i+1}\ (mod\ 2^r) \mid i = 0, 1, 2, \ldots\}$ e $B = \{a \in \mathbb{Z} \mid 1 \leq a < 2^r,\ a \equiv 5\ (mod\ 8)\}$. Como $5^{2i+1} = 25^i.5 \equiv 5\ (mod\ 8)$, temos $A \subseteq B$. Além disso, $|A| = \frac{1}{2}.2^{r-2} = 2^{r-3}$ pois 5 tem ordem $2^{r-2}$ $(mod\ 2^r)$. Por outro lado, existe um único inteiro congruente a 5 $(mod\ 2^r)$ em cada um dos intervalos $[1, 8)$, $[8, 16)$, $[16, 24), \ldots, [2^3(2^{r-3} - 1), 2^r)$, assim $|B| = 2^{r-3}$. Logo $A = B$ e concluímos que se $q \equiv 5\ (mod\ 8)$, então $q$ tem ordem $2^{r-2}$ $(mod\ 2^r)$. Em particular, todo $q \equiv -3\ (mod\ 8)$ tem ordem $2^{r-2}$ $(mod\ 2^r)$ e, portanto, todo $q \equiv 3\ (mod\ 8)$ tem esta ordem pois $q^{2^l} = (-q)^{2^l}$, para $l \geq 1$. □

**Lema 1.4.2** *Sejam G um grupo cíclico de ordem $2^m$, F um corpo com $q$ elementos, sendo $q$ uma potência de um primo ímpar, $\mathcal{U}_{2^r}$ o grupo das unidades de $\mathbb{Z}_{2^r}$ e denote por $\overline{q}$ a imagem de $q$ em $\mathcal{U}_{2^r}$, sob a aplicação natural. Seja $g \in G$ um elemento de ordem $2^r$, ou seja, $g = a^{2^{m-r}}$.*

**(i)** *Se $r = 0$ ou $r = 1$, então $\mathcal{C}_{\mathbb{Q}}(g) = \mathcal{C}_F(g)$.*

**(ii)** *Se $r = 2$, quando $q \equiv 1\ (mod\ 4)$, $\mathcal{C}_{\mathbb{Q}}(g)$ se divide em duas F - classes e quando $q \equiv 3\ (mod\ 4)$, então $\mathcal{C}_{\mathbb{Q}}(g) = \mathcal{C}_F(g)$.*

**(iii)** *Se $r = 3$, então $\mathcal{C}_{\mathbb{Q}}(g)$ se divide em pelo menos duas F - classes.*

**(iv)** *Se $r > 3$, então $\mathcal{C}_{\mathbb{Q}}(g)$ se divide na união disjunta de $[\mathcal{U}_{2^r} : \langle\overline{q}\rangle] > 1$ F - classes, cada uma com $o(\overline{q})$ elementos. Em particular, se $q \equiv 3\ (mod\ 8)$, então $\mathcal{C}_{\mathbb{Q}}(g)$ se divide em duas F - classes.*

Demonstração: **(i)** Se $r = 0$, então $g = 1$ e a afirmação é trivial. Se $r = 1$, então $g^k = g$ para todo inteiro ímpar $k$, assim $\mathcal{C}_{\mathbb{Q}}(g) = \mathcal{C}_F(g) = \{g\}$.

**(ii)** Considere $r = 2$. Se $q \equiv 1 \ (mod\ 4)$, então $\mathcal{C}_{\mathbb{Q}}(g) = \{g, g^3\}$, $\mathcal{C}_{\mathrm{F}}(g) = \{g\}$ e $\mathcal{C}_{\mathrm{F}}(g^3) = \{g^3\}$, isto é, a $\mathbb{Q}$ - classe de $g$ se divide em duas F - classes. Se $q \equiv 3 \ (mod\ 4)$, então $g^q = g^3$ e $q^2 \equiv 1 \ (mod\ 4)$. Portanto, $\mathcal{C}_{\mathbb{Q}}(g) = \{g, g^3\} = \mathcal{C}_{\mathrm{F}}(g)$.

**(iii)** Seja $r = 3$. Temos que $\mathcal{C}_{\mathbb{Q}}(g) = \{g, g^3, g^5, g^7\}$. Quando $q \equiv 1 \ (mod\ 4)$, então $\mathcal{C}_{\mathrm{F}}(g) = \{g\}$, se $q \equiv 1 \ (mod\ 8)$, e $\mathcal{C}_{\mathrm{F}}(g) = \{g, g^5\}$, se $q \equiv 5 \ (mod\ 8)$. Portanto, $\mathcal{C}_{\mathbb{Q}}(g)$ se divide em pelo menos duas F - classes.

Quando $q \equiv 3 \ (mod\ 4)$, então $\mathcal{C}_{\mathrm{F}}(g) = \{g, g^3\}$ se $q \equiv 3 \ (mod\ 8)$ e $\mathcal{C}_{\mathrm{F}}(g) = \{g, g^7\}$ se $q \equiv 7 \ (mod\ 8)$. Portanto, $\mathcal{C}_{\mathbb{Q}}(g)$ se divide em pelo menos duas F - classes.

**(iv)** Suponha $r > 3$. Então $\mathcal{C}_{\mathbb{Q}}(g) = \{g, g^3, \ldots, g^{2^{r-1}}\}$ e $\mathcal{C}_{\mathrm{F}}(g) = \{g, g^q, \ldots, g^{q^{k-1}}\}$, onde $k$ é o menor inteiro positivo tal que $g^{q^k} = g$. Como $q^{o(\overline{q})} \equiv 1 \ (mod\ 2^r)$, e $o(\overline{q})$ é o menor inteiro que satisfaz isso, então $k = o(\overline{q})$. Em particular, $k \leq 2^{r-2}$, pelo Lema 1.4.1, assim $k < 2^{r-1}$ e existe $g^s \in \mathcal{C}_{\mathbb{Q}}(g) - \mathcal{C}_{\mathrm{F}}(g)$. Temos $\mathcal{C}_{\mathrm{F}}(g^s) = \{g^s, g^{sq}, \ldots, g^{sq^{l-1}}\}$, onde $l$ é o menor natural tal que $g^{sq^l} = g^s$. Assim, $sq^l \equiv s \ (mod\ 2^r)$ e, como $s$ é ímpar, $q^l \equiv 1 \ (mod\ 2^r)$. Logo, $l = o(\overline{q}) = k$. Portanto, a F - classe de $g$ tem $o(\overline{q})$ elementos e $\mathcal{C}_{\mathbb{Q}}(g)$ é a união de $[\mathcal{U}_{2^r} : \langle\overline{q}\rangle]$ F - classes. Note que se $q \equiv 3 \ (mod\ 8)$, então, pelo Lema 1.4.1, $o(\overline{q}) \ (mod\ 2^r) = 2^{r-2}$. Portanto, $\mathcal{C}_{\mathbb{Q}}(g)$ se divide em $\dfrac{2^{r-1}}{2^{r-2}} = 2$ F - classes. □

**Proposição 1.4.1** *Seja* G $= \langle a \rangle$ *um grupo cíclico de ordem* $2^m$. *Se* $m = 1$, *então, para qualquer corpo* F, *existem duas* F- *classes em* G. *Se* $m > 1$, *o número de* F - *classes de* G *é* $m + 1$ *se* F $= \mathbb{Q}$ *e é pelo menos* $2m - 1$, *para qualquer corpo finito* F. *Este número mínimo é obtido se* F *tem ordem* $q \equiv 3 \ (mod\ 8)$.

Demonstração: Claramente temos $\mathcal{C}_{\mathrm{F}}(1) = \{1\}$, para qualquer corpo F. Se $m = 1$, então G $= \{1, a\}$ e $\mathcal{C}_{\mathrm{F}}(a) = \{a\}$, pois $a^s = a$, se $s$ é ímpar, isto é, sempre existem duas F - classes em G. Seja $m > 1$. Se $i$ é ímpar, então $a^i \in \mathcal{C}_{\mathbb{Q}}(a)$, a $\mathbb{Q}$ - classe de $a = a^{2^0}$. Se $i$ é par, então escreva $i = 2^{i_0}.i_1$, com $i_1$ ímpar. Então, para todo $j$ ímpar, temos $(a^i)^j = a^{2^{i_0}.i_1.j}$ com $i_1.j$ ímpar. Assim $a^i \in \mathcal{C}_{\mathbb{Q}}\left(a^{2^{i_0}}\right)$. Disto segue que as $\mathbb{Q}$ - classes de G consistem das potências ímpares de $a^{2^i}$, com $0 \leq i \leq m$, e temos

$$\mathcal{C}_0 = \mathcal{C}_{\mathbb{Q}}(a) = \left\{a, a^3, a^5, a^7, \ldots, a^{2^m-1}\right\}$$

$$\mathcal{C}_1 = \mathcal{C}_{\mathbb{Q}}\left(a^2\right) = \left\{a^2, a^6, a^{10}, a^{14}, \ldots, a^{2.(2^{m-1}-1)}\right\}$$

$$\mathcal{C}_2 = \mathcal{C}_{\mathbb{Q}}\left(a^4\right) = \left\{a^4, a^{12}, a^{20}, a^{28}, \ldots, a^{4.(2^{m-2}-1)}\right\}$$

$$\vdots$$

$$\mathcal{C}_i = \mathcal{C}_{\mathbb{Q}}\left(a^{2^i}\right) = \left\{a^{2^i}, a^{3.2^i}, a^{5.2^i}, a^{7.2^i}, \ldots, a^{2^i.(2^{m-i}-1)}\right\}$$

$$\vdots$$

$$\mathcal{C}_{m-3} = \mathcal{C}_{\mathbb{Q}}\left(a^{2^{m-3}}\right) = \left\{a^{2^{m-3}}, a^{3.2^{m-3}}, a^{5.2^{m-3}}, a^{7.2^{m-3}}\right\}$$

$$\mathcal{C}_{m-2} = \mathcal{C}_{\mathbb{Q}}\left(a^{2^{m-2}}\right) = \left\{a^{2^{m-2}}, a^{3.2^{m-2}}\right\} = \left\{a^{2^{m-2}}, a^{2^{m-1}}.a^{2^{m-2}}\right\}$$

$$\mathcal{C}_{m-1} = \mathcal{C}_{\mathbb{Q}}\left(a^{2^{m-1}}\right) = \left\{a^{2^{m-1}}\right\}$$

$$\mathcal{C}_m = \mathcal{C}_{\mathbb{Q}}\left(a^{2^m}\right) = \{1\}.$$

As duas últimas $\mathbb{Q}$ - classes são claramente F - classes, para qualquer corpo F. Assim, se $F = \mathbb{Q}$, existem $m+1$ F - classes. Se F é um corpo finito e $q \equiv 3 \ (mod\ 8)$, então, pelo Lema 1.4.2 (ii), $\mathcal{C}_{\mathbb{Q}}\left(a^{2^{m-2}}\right) = \mathcal{C}_{F}\left(a^{2^{m-2}}\right)$, pois $a^{2^{m-2}}$ tem ordem $2^2$. Por outro lado, pelo Lema 1.4.2, todas as outras $\mathbb{Q}$ - classes se dividem em pelo menos duas F - classes, resultando num total de pelo menos $2.(m-2)+3 = 2m-1$ F - classes. □

**Corolário 1.4.1** *Sob as hipóteses da Proposição 1.4.1, no caso em que* $q \equiv 5 \ (mod\ 8)$, *o número de* F - *classes de* FG *é* $2m$.

Demonstração: Precisamos verificar que cada uma das primeiras $m-1$ $\mathbb{Q}$ - classes da Proposição 1.4.1, se divide em exatamente duas F - classes. Pelo Lema 1.4.1, que $q$ tem ordem $2^{r-2}$ $(mod\ 2^r)$ e assim cada uma destas $\mathbb{Q}$ - classes se divide em $[\mathcal{U}_{2^r} : \langle\overline{q}\rangle] = \dfrac{2^{r-1}}{2^{r-2}} = 2$ F - classes, pelo Lema 1.4.2 (iv). Portanto, temos exatamente $2m$ F - classes em FG. □

## 1.5 Resíduos Quadráticos

Os resultados e definições desta seção, podem ser vistos em [15, capítulo 5]. Seja $F_q$ um corpo finito, onde $q$ é uma potência de um primo ímpar $p$. O nosso objetivo é utilizarmos

os resultados aqui citados para concluirmos que, se $q \equiv 3 \ (mod\ 8)$, então $-2$ é um quadrado em $\mathrm{F}_q$ e que, se $q \equiv 5 \ (mod\ 8)$, então $-1$ é um quadrado em $\mathrm{F}_q$.

**Definição 1.5.1** *Para $p$ um primo ímpar e $a$ um inteiro não divisível por $p$, definimos o Símbolo de Legendre $\left(\frac{a}{p}\right)$ por*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{se } a \text{ é um resíduo quadrático módulo } p \\ -1, & \text{se } a \text{ não é um resíduo quadrático módulo } p. \end{cases}$$

**Teorema 1.5.1** *O Símbolo de Legendre é uma função completamente multiplicativa de $a$, isto é,*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

*para $a$ e $b$ inteiros não divisíveis por $p$.*

O Teorema 1.5.1 nos diz que o produto de dois números que não são resíduos quadráticos é um resíduo quadrático.

**Teorema 1.5.2** *Para $p$ um primo ímpar, temos*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{se } p \equiv 1 \ (mod\ 4) \\ -1, & \text{se } p \equiv -1 \ (mod\ 4). \end{cases}$$

**Teorema 1.5.3** *Para $p$ um primo ímpar, temos*

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{se } p \equiv \pm 1 \ (mod\ 8) \\ -1, & \text{se } p \equiv \pm 3 \ (mod\ 8). \end{cases}$$

**Definição 1.5.2** *Para um inteiro positivo $a$ relativamente primo com o inteiro ímpar $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_t^{\alpha_t}$ o Símbolo de Jacobi, denotado por $\left[\frac{a}{n}\right]$, é definido por:*

$$\left[\frac{a}{n}\right] = \left[\frac{a}{p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_t^{\alpha_t}}\right] = \left(\frac{a}{p_1}\right)^{\alpha_1}\left(\frac{a}{p_2}\right)^{\alpha_2} \ldots \left(\frac{a}{p_t}\right)^{\alpha_t}$$

*onde os símbolos à direita da última igualdade são Símbolos de Legendre.*

**Teorema 1.5.4** *O Símbolo de Jacobi satisfaz*

$$\left[\frac{-1}{n}\right] = (-1)^{(n-1)/2}$$

*onde $n$ é um inteiro ímpar e positivo.*

**Problema 1.5.1** *Se $n$ é um inteiro ímpar e positivo, então*

$$\left[\frac{2}{n}\right] = (-1)^{(n^2-1)/8}.$$

Esse Problema 1.5.1 encontra-se resolvido em [15, Problema 5.2, p.113].

Com base nestes resultados, mostraremos que em $F_q$, onde $q = p^s$ e $p$ é um primo ímpar, $-2$ é um resíduo quadrático módulo $q$ se $q \equiv 3 \ (mod\ 8)$ e $-1$ é um resíduo quadrático módulo $q$, se $q \equiv 5 \ (mod\ 8)$.

Temos, pelo Teorema 1.5.2, $\left(\frac{-1}{p}\right) = -1$, isto é, $-1$ não é um resíduo quadrático módulo $p$ e, pelo Teorema 1.5.3, temos $\left(\frac{2}{p}\right) = -1$, isto é, 2 não é um resíduo quadrático módulo $p$. Portanto, pelo Teorema 1.5.1, $\left(\frac{-2}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-1}{p}\right) = -1.(-1) = 1$, e assim $-2$ é um resíduo quadrático módulo $p$, se $p \equiv 3 \ (mod\ 8)$. Para concluir, vamos avaliar o Símbolo de Legendre considerando-o como Símbolo de Jacobi, para que possamos utilizar o fato de que este símbolo também satisfaz a lei de Reciprocidade Quadrática. Pelos Teorema 1.5.4 e Problema 1.5.1 temos

$$\left(\frac{-2}{q}\right) = \left[\frac{-2}{q}\right] = \left[\frac{-1}{q}\right]\left[\frac{2}{q}\right] = (-1)^{(q-1)/2}.(-1)^{(q^2-1)/8} = (-1)^{(q-1)(q+5)/8} = 1.$$

Logo podemos afirmar:

**Lema 1.5.1** *Se $q \equiv 3 \ (mod\ 8)$, então $-2$ é um quadrado módulo $q$.*

Sabemos, pelo Teorema 1.5.4, que $\left[\frac{-1}{q}\right] = (-1)^{(q-1)/2}$, então se $q \equiv 5 \ (mod\ 8)$ segue

$$\left(\frac{-1}{q}\right) = \left[\frac{-1}{q}\right] = 1.$$

Assim, podemos concluir:

**Lema 1.5.2** *Se $q \equiv 5 \ (mod\ 8)$, então $-1$ é um quadrado módulo $q$.*

**Lema 1.5.3** *Se $q \equiv 7$ ou $9 \ (mod\ 16)$, então 2 é um quadrado módulo $q$.*

Demonstração: Pelo Problema 1.5.1, temos $\left[\frac{2}{q}\right] = (-1)^{(q^2-1)/8}$. Assim, se $q \equiv \pm 1 \ (mod\ 8)$, temos

$$\left(\frac{2}{q}\right) = \left[\frac{2}{q}\right] = 1.$$

Portanto, 2 é um resíduo quadrático módulo $q$. □

**Lema 1.5.4** *Se $q \equiv 9 \ (mod\ 16)$, então $-2$ é um quadrado módulo $q$.*

Demonstração: Pelo Lema 1.5.3, 2 é um quadrado módulo $q$. Como $\left[\frac{-1}{q}\right] = (-1)^{(q-1)/2}$, pelo Teorema 1.5.1, então

$$\left(\frac{-2}{q}\right) = \left[\frac{-2}{q}\right] = \left[\frac{2}{q}\right]\left[\frac{-1}{q}\right] = 1.$$

Logo $-2$ é um quadrado módulo $q$. □

**Observação 1.5.1** *Segue do Lema 1.5.4, que se $q \equiv 9 \ (mod\ 16)$, então $\mathrm{F}_q$ possui uma raiz oitava primitiva da unidade.*

# Capítulo 2

# Uma Família de Códigos Cíclicos de $\mathrm{F}_q C_{2^m}$

Neste capítulo exibiremos uma família de $m+1$ idempotentes na álgebra de grupo FG, quando G é um grupo cíclico de ordem $2^m$ e F um corpo finito de característica ímpar. Também determinamos a distância mínima e a dimensão dos códigos cíclicos que são gerados por esses idempotentes. Esses resultados foram obtidos por Pruthi [13], usando métodos polinomiais. Os mesmos idempotentes são obtidos aqui, de um modo talvez mais natural, usando Teoria de Álgebras de Grupo. Isso nos permitirá determinar a dimensão e a distância mínima, de uma forma mais simples do que em [13]. Além disso, será possível explicitar uma base para tais códigos, o que não acontece em [13].

Considere $\mathrm{G} = \langle a \mid a^{2^m} = 1 \rangle$ o grupo cíclico de ordem $2^m$ gerado por $a$, e seja F um corpo finito com $q$ elementos, sendo $q$ uma potência de um primo tal que $mdc(q, |\mathrm{G}|) = 1$.

## 2.1 Cálculo dos Idempotentes

Seja H um subgrupo do grupo G. Considere

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

Como $|H|$ divide $|G|$ e $mdc(q, |G|) = 1$, segue que $\widehat{H}$ está bem definido. Claramente $\widehat{H}$ é um idempotente de FG.

**Lema 2.1.1** *Seja* $G = \langle a \rangle$ *um grupo cíclico de ordem* $2^m$, $m \geq 1$. *Considere*

$$G = G_0 \supset G_1 \supset \cdots \supset G_m = \{1\}$$

*a cadeia descendente de todos os subgrupos de* G, *onde* $G_i = \langle a^{2^i} \rangle$ *e* $|G_i| = 2^{m-i}$. *Então os elementos* $e_0 = \widehat{G}$ *e* $e_i = \widehat{G_i} - \widehat{G_{i-1}}$ *com* $1 \leq i \leq m$, *formam um conjunto de idempotentes dois a dois ortogonais de* FG *tal que* $e_0 + e_1 + \cdots + e_m = 1$.

Demonstração: Primeiramente, observamos que se $1 \leq i \leq j$, então $G_i \supset G_j$ e assim

$$\widehat{G_i}\widehat{G_j} = \left(\frac{1}{|G_i|}\sum_{x \in G_i} x\right)\left(\frac{1}{|G_j|}\sum_{y \in G_j} y\right) = \frac{1}{|G_i||G_j|}|G_j|\sum_{x \in G_i} x = \frac{1}{|G_i|}\sum_{x \in G_i} x = \widehat{G_i}.$$

Precisamos verificar que estes elementos são idempotentes. Temos

$$e_0 e_0 = \widehat{G}\widehat{G} = \left(\frac{1}{|G|}\sum_{g \in G} g\right)\widehat{G} = \frac{1}{|G|}\sum_{g \in G}(g\widehat{G}) = \frac{1}{|G|}\sum_{g \in G}\widehat{G} = \widehat{G} = e_0.$$

Analogamente,

$$e_i e_i = (\widehat{G_i} - \widehat{G_{i-1}})(\widehat{G_i} - \widehat{G_{i-1}}) = \widehat{G_i}\widehat{G_i} - \widehat{G_i}\widehat{G_{i-1}} - \widehat{G_{i-1}}\widehat{G_i} + \widehat{G_{i-1}}\widehat{G_{i-1}} =$$

$$\widehat{G_i} - \widehat{G_{i-1}} - \widehat{G_{i-1}} + \widehat{G_{i-1}} = \widehat{G_i} - \widehat{G_{i-1}} = e_i.$$

Seja $i \neq j$ e suponha, sem perda de generalidade, que $i < j$. Temos

$$e_i e_j = (\widehat{G_i} - \widehat{G_{i-1}})(\widehat{G_j} - \widehat{G_{j-1}}) = \widehat{G_i}\widehat{G_j} - \widehat{G_i}\widehat{G_{j-1}} - \widehat{G_{i-1}}\widehat{G_j} + \widehat{G_{i-1}}\widehat{G_{j-1}} =$$

$$\widehat{G_i} - \widehat{G_{i-1}} - \widehat{G_i} + \widehat{G_{i-1}} = 0.$$

Temos ainda

$$e_0 e_i = \widehat{G}(\widehat{G_i} - \widehat{G_{i-1}}) = \widehat{G}\widehat{G_i} - \widehat{G}\widehat{G_{i-1}} = \widehat{G} - \widehat{G} = 0.$$

Assim, estes são idempotentes dois a dois ortogonais de FG.

Da expressão destes idempotentes, temos

$$e_0 + e_1 + \cdots + e_m = \widehat{G} + (\widehat{G_1} - \widehat{G_0}) + (\widehat{G_2} - \widehat{G_1}) + \cdots + (\widehat{G_m} - \widehat{G_{m-1}}) = \widehat{G_m} = 1.$$

□

O idempotente $e_0 = \widehat{\mathrm{G}}$ é dito o *idempotente principal*, e ele é primitivo. Isto segue do fato que $\mathrm{FG}e_0 \cong \mathrm{F}$, donde $e_0$ é indecomponível em soma de outros dois idempotentes.

## 2.2 Dimensão e Distância Mínima

Considere os idempotentes do Lema 2.1.1. Sejam $\mathrm{I}_i = \mathrm{FG}(e_i)$, com $0 \leq i \leq m$, ideais de FG, isto é, seus códigos cíclicos. O nosso objetivo é determinar a dimensão e a distância mínima de $\mathrm{I}_i$, para cada $i = 0, \ldots, m$.

**Lema 2.2.1** *Sejam* $\mathrm{I}_i = \mathrm{FG}(e_i)$, *com* $0 \leq i \leq m$, *ideais de* FG, *onde* $e_i$ *são os idempotentes do Lema 2.1.1. Então*

$$dim(\mathrm{I}_0) = 1,\ w(\mathrm{I}_0) = |\mathrm{G}| = 2^m,$$

$$dim(\mathrm{I}_i) = 2^{i-1} \text{ e } w(\mathrm{I}_i) = 2^{m-i+1},\ 1 \leq i \leq m.$$

Demonstração: Note que para $\mathrm{I}_i = \mathrm{FG}(e_i)$, com $i = 1, \ldots, m$, temos $e_i = \widehat{\mathrm{G}_i} - \widehat{\mathrm{G}_{i-1}}$, onde $\mathrm{G}_i$ é um subgrupo cíclico de G de ordem $2^{m-i}$ tal que $\mathrm{G}/\mathrm{G}_i$ é cíclico de ordem $2^i$ e $\mathrm{G}_{i-1}$ é o único subgrupo de G tal que $[\mathrm{G}_{i-1} : \mathrm{G}_i] = 2$.

Se $\mathrm{G} = \langle a \rangle$, então $\mathrm{G}_i = \langle a^{2^i} \rangle$, onde

$$o(a^{2^i}) = \frac{o(a)}{mdc(o(a), o(a^{2^{m-i}}))} = \frac{2^m}{mdc(2^m, 2^i)} = \frac{2^m}{2^i} = 2^{m-i}.$$

Note que

$$(1 - a^{2^{i-1}})\widehat{\mathrm{G}_i} = (1 - a^{2^{i-1}})(e_i + \widehat{\mathrm{G}_{i-1}}) = (1 - a^{2^{i-1}})e_i \in \mathrm{I}_i.$$

Como $a^{2^{i-1}} \notin \mathrm{G}_i$, é claro que $supp((1 - a^{2^{i-1}})\widehat{\mathrm{G}_i}) = \mathrm{G}_i \dot{\cup} a^{2^{i-1}}\mathrm{G}_i$ e o peso deste elemento é $w((1 - a^{2^{i-1}})\widehat{\mathrm{G}_i}) = 2.|\mathrm{G}_i| = 2.2^{m-i} = 2^{m-i+1}$. Assim, $w(\mathrm{I}_i) \leq 2^{m-i+1}$. Como $\mathrm{G} = \mathrm{G}_i \dot{\cup} a\mathrm{G}_i \dot{\cup} \ldots \dot{\cup} a^{2^i-1}\mathrm{G}_i$, pois $\{1, a, \ldots, a^{2^i-1}\}$ é um transversal de $\mathrm{G}_i$ em G, temos que todo elemento de FG pode ser escrito da seguinte forma

$$\alpha = \sum_{j=0}^{2^i-1} \alpha_j a^j, \text{ com } \alpha_j \in \mathrm{FG}_i.$$

Agora se $y \in \mathrm{G}_i$, então $y = a^{s2^i}$, com $s \in \mathbb{N}$. Assim, $ye_i = a^{s2^i}(\widehat{\mathrm{G}_i} - \widehat{\mathrm{G}_{i-1}}) = a^{s2^i}\widehat{\mathrm{G}_i} - a^{s2^i}\widehat{\mathrm{G}_{i-1}} = \widehat{\mathrm{G}_i} - \widehat{\mathrm{G}_{i-1}} = e_i$. Logo, $\alpha_j e_i = k_j e_i$, onde $k_j \in \mathrm{F}$ e $0 \leq j \leq 2^i - 1$.

Como $\mathrm{I}_i = (\mathrm{FG})e_i \subset (\mathrm{FG})\widehat{\mathrm{G}_i}$, então um elemento $0 \neq \gamma \in (\mathrm{FG})e_i = \mathrm{I}_i$ pode ser escrito da forma

$$\gamma = \alpha\widehat{\mathrm{G}_i} = (k_0 + k_1 a + \cdots + k_{2^{i-1}} a^{2^{i-1}})\widehat{\mathrm{G}_i}, \text{ com } k_j \in \mathrm{F}, j = 0, \ldots, 2^i - 1.$$

Como $\gamma \neq 0$, temos pelo menos um coeficiente $k_j \neq 0$. Mas, se $\gamma = k_j a^j \widehat{\mathrm{G}_i}$, então $\widehat{\mathrm{G}_i} \in (\mathrm{FG})e_i$, uma contradição. Logo, pelo menos dois coeficientes $k_j, k_{j'}$ são não nulos para todo $\gamma \in \mathrm{I}_i$ e, assim,

$$w(\mathrm{I}_i) = 2|\mathrm{G}_i| = 2^{m-i+1}, \text{ para } i = 1, \ldots, m.$$

Note que $\widehat{\mathrm{G}_i} = \widehat{\mathrm{G}_{i-1}} + e_i$ e que $\widehat{\mathrm{G}_{i-1}}e_i = 0$, assim $(\mathrm{FG})\widehat{\mathrm{G}_i} = (\mathrm{FG})\widehat{\mathrm{G}_{i-1}} \oplus (\mathrm{FG})e_i$. Assim, $dim_{\mathrm{F}}((\mathrm{FG})e_i) = dim_{\mathrm{F}}(\mathrm{FG})\widehat{\mathrm{G}_i} - dim_{\mathrm{F}}(\mathrm{FG})\widehat{\mathrm{G}_{i-1}}$. Temos $(\mathrm{FG})\widehat{\mathrm{G}_i} \cong \mathrm{F}(\mathrm{G}/\mathrm{G}_i)$, pelo Teorema 1.1.1, logo

$$dim_{\mathrm{F}}((\mathrm{FG})e_i) = dim_{\mathrm{F}}\mathrm{F}[\mathrm{G}/\mathrm{G}_i] - dim_{\mathrm{F}}\mathrm{F}[\mathrm{G}/\mathrm{G}_{i-1}] \tag{2.1}$$

e, claramente,

$$dim_{\mathrm{F}}\mathrm{F}[\mathrm{G}/\mathrm{G}_i] = |\mathrm{G}/\mathrm{G}_i| \text{ e } dim_{\mathrm{F}}\mathrm{F}[\mathrm{G}/\mathrm{G}_{i-1}] = |\mathrm{G}/\mathrm{G}_{i-1}|.$$

Portanto, segue da equação 2.1 que

$$dim_{\mathrm{F}}(\mathrm{I}_i) = dim_{\mathrm{F}}((\mathrm{FG})e_i) = 2^{i-1}.$$

Ainda, uma base para $\mathrm{I}_0 = (\mathrm{FG})e_0 = (\mathrm{FG})\widehat{\mathrm{G}} = \mathrm{F}\widehat{\mathrm{G}}$ é $\widehat{\mathrm{G}}$ e, portanto,

$$dim_{\mathrm{F}}\mathrm{I}_0 = 1.$$

Como todo elemento de $\mathrm{I}_0$ é um múltiplo escalar de $\widehat{\mathrm{G}}$ e $w(\widehat{\mathrm{G}}) = |\mathrm{G}|$, temos

$$w(\mathrm{I}_0) = |\mathrm{G}|.$$

□

## 2.3 Base

Consideremos os ideais $\mathrm{I}_i = \mathrm{FG}(e_i)$ de FG, onde

$$e_i = \widehat{\mathrm{G}_i} - \widehat{\mathrm{G}_{i-1}} = \frac{1}{2^{m-i+1}}(1 - a^{2^{i-1}} + a^{2^i} - a^{3.2^{i-1}} + a^{2^{i+1}} - \cdots + a^{2^m-2^i} - a^{2^m-2^{i-1}}),$$

para $1 \leq i \leq m$, e

$$e_0 = \widehat{\mathrm{G}_0} = \frac{1}{2^m}(1 + a + a^2 + \cdots + a^{2^m-1}).$$

Como $(\mathrm{FG})e_0 = (\mathrm{FG})\widehat{\mathrm{G}} \cong \mathrm{F}$ é de dimensão 1, segue imediatamente que $\mathrm{B}_0 = \{e_0\}$ é uma base de $\mathrm{I}_0$.

Já sabemos que $dim(\mathrm{I}_i) = 2^{i-1}$, para $1 \leq i \leq m$, pelo Lema 2.2.1.

Em [5, Proposição 2.2], se exibe uma base para ideais semelhantes aos aqui estudados. Entretanto, os elementos da base que exibimos a seguir, diferente dessa, têm uma expressão mais simples.

**Proposição 2.3.1** *Sob as hipóteses do Lema 2.2.1, o conjunto*

$$\mathrm{B}_i = \{e_i, ae_i, a^2e_i, \ldots, a^{2^{i-1}-1}e_i\}$$

*é uma base visível de* $\mathrm{I}_i$, *para* $1 \leq i \leq m$.

Demonstração: Para provarmos este fato, veremos que os elementos de $\mathrm{B}_i$ têm suportes disjuntos e, assim, são linearmente independentes.

Note que cada elemento de $\mathrm{B}_i$ é da forma

$$a^l e_i = \frac{a^l}{2^{m-i+1}}(1 - a^{2^{i-1}} + a^{2^i} - a^{3.2^{i-1}} + a^{2^{i+1}} - \cdots + a^{2^m-2^i} - a^{2^m-2^{i-1}}),$$

com $0 \leq l \leq 2^{i-1} - 1$, e que se $l \neq k$, $supp(a^l e_i) \subset a^l\langle a^{2^{i-1}}\rangle$ e $supp(a^k e_i) \subset a^k\langle a^{2^{i-1}}\rangle$. Seja $x \in supp(a^l e_i) \cap supp(a^k e_i) = a^l\langle a^{2^{i-1}}\rangle \cap a^k\langle a^{2^{i-1}}\rangle$, com $l \neq k$. Então

$$x = a^{l+r.2^{i-1}} = a^{k+s.2^{i-1}}.$$

Logo

$$a^{l-k+(r-s)2^{i-1}} = 1 \Longrightarrow 2^m \mid (l - k + (r - s)2^{i-1}).$$

Como $2^{i-1} \mid 2^m$, isto implica que

$$2^{i-1} \mid (l-k).$$

Mas $0 \leq l, k \leq 2^{i-1}-1$, logo $l-k=0$, uma contradição. Assim, $supp(a^l e_i) \cap supp(a^k e_i) = \emptyset$ e, portanto, o conjunto $\mathrm{B}_i$ é linearmente independente.

Como $|\mathrm{B}_i| = 2^{i-1}$, então $\mathrm{B}_i$ é uma base de $\mathrm{I}_i$, para $1 \leq i \leq m$.

Podemos notar também, que todo elemento de $\mathrm{B}_i$ tem peso $2^{m-i+1} = |\mathrm{G}_{i-1}| = w(\mathrm{I}_i)$, logo a base $\mathrm{B}_i$ é visível e, particularmente bem comportada, pois todos os seus elementos têm todos o mesmo peso que é exatamente o peso do ideal gerado por $\mathrm{B}_i$. □

# Capítulo 3

# Idempotentes Primitivos em $\mathrm{F}_qC_{2^m}$

Em todo este capítulo, F denotará um corpo com $q$ elementos, sendo $q$ uma potência de um primo ímpar $p$, $\mathrm{G} = \langle a \mid a^{2^m} = 1 \rangle$ o grupo cíclico gerado por $a$ de ordem $2^m$ e FG a álgebra de grupo correspondente. O nosso objetivo é determinar os idempotentes primitivos de FG, isto é, os idempotentes geradores dos ideais minimais de FG, o peso do código correspondente a cada um deles, a dimensão desses ideais e, mais ainda, de cada um deles exibiremos uma base.

Como veremos, temos quatro possibilidades a considerar: $q \equiv 1 \ (mod\ 8)$, $q \equiv 3 \ (mod\ 8)$, $q \equiv 5 \ (mod\ 8)$, ou $q \equiv 7 \ (mod\ 8)$, pois, em cada um destes casos, a ordem de $q \ (mod\ 2^m)$ bem como o número de componentes simples de FG é variável, o que modifica o cálculo dos idempotentes.

Os casos $q \equiv 3 \ (mod\ 8)$ e $q \equiv 5 \ (mod\ 8)$ apresentam regularidade suficiente para nos permitir fazer uma discussão completa de cada um destes casos. Já nos outros dois casos, isto não ocorre e nos limitaremos a ilustrar estas situações com exemplos particulares.

Seja $\theta$ uma raiz primitiva $2^m$- ésima da unidade em uma extensão de F. Então, pelo "Teorema de Brauer", para característica $p \neq 0$ [9, Corolário 9.15, p.151] temos que $\mathrm{F}(\theta)$ é um corpo de decomposição para G e os caracteres irredutíveis de G sobre $\mathrm{F}(\theta)$ são as aplicações

$$\begin{array}{rccc} \chi_i : & \mathrm{G} & \longrightarrow & \mathrm{F}(\theta) \\ & a^j & \longmapsto & \theta^{ij} \end{array}, \text{ com } 1 \leq i \leq 2^m.$$

É bem conhecido que os idempotentes de F($\theta$)G são da seguinte forma

$$e_i = \frac{1}{|\mathrm{G}|}\sum_{g\in \mathrm{G}} \chi_i(1)\chi_i(g^{-1})g = \frac{1}{2^m}\sum_{j=0}^{2^m-1}(\theta^i)^j a^j,$$

com $0 \leq i \leq 2^m - 1$ (veja [10, Teorema 5.1.11]). Como F é finito, $Gal(\mathrm{F}(\theta) : \mathrm{F}) =< \sigma >$, isto é, é cíclico gerado pelo automorfismo $\sigma : \mathrm{F}(\theta) \longrightarrow \mathrm{F}(\theta)$ definido por $x \longmapsto x^q$. É fácil ver que se $r = 2^{m-2} = [\mathrm{F}_q(\theta) : \mathrm{F}]$, então $o(\sigma) = r$. Além disso, os idempotentes primitivos de FG são da forma $e_i + \sigma(e_i) + \cdots + \sigma^{2^{m-2}-1}(e_i)$, pelo [2, Teorema 70.15].

Aplicando este método seria possível determinar os idempotentes em função de $\theta$. Porém, nós vamos dar expressões gerais (independentes de $\theta$) para esses idempotentes utilizando outro caminho, inspirado pelos idempotentes determinados a partir da estrutura de subgrupos de G, obtidos no capítulo anterior.

## 3.1 Caso $q \equiv 3 \ (mod\ 8)$

Suponha $q \equiv 3 \ (mod\ 8)$. Neste caso, o número de componentes simples de FG é $2m - 1$, pela Proposição 1.4.1. Além disso, $-2$ é um quadrado em F pelo Lema 1.5.1. Assim, seja $\alpha \in \mathrm{F}$ um elemento tal que $\alpha^2 = -2$. No próximo resultado temos explicitados todos os idempotentes primitivos de FG, para $q \equiv 3 \ (mod\ 8)$.

**Proposição 3.1.1** *Sejam* F *um corpo com q elementos, sendo q uma potência de um primo ímpar p tal que* $q \equiv 3 \ (mod\ 8)$ *e* $\mathrm{G} = \langle a \mid a^{2^m} = 1\rangle$ *o grupo cíclico gerado por a de ordem* $2^m$. *Os elementos*

$$\epsilon_0 = \frac{1 + a + a^2 + \cdots + a^{2^m-1}}{2^m},$$

$$\epsilon_1 = \frac{1 - a + a^2 - \cdots - a^{2^m-1}}{2^m},$$

$$\epsilon_2 = \frac{1 - a^2 + a^4 - \cdots - a^{2^m-2}}{2^{m-1}},$$

$$\epsilon_3 = (1 - a^4)\frac{(1 + a^{2^3} + \cdots + a^{2^m-2^3})(2 + \alpha a + \alpha a^3)}{2^m},$$

$$\epsilon_3' = (1 - a^4)\frac{(1 + a^{2^3} + \cdots + a^{2^m-2^3})(2 - \alpha a - \alpha a^3)}{2^m},$$

$$\epsilon_4 = (1-a^8)\frac{(1+a^{2^4}+\cdots+a^{2^m-2^4})(2+\alpha a^2+\alpha a^{3.2})}{2^{m-1}},$$

$$\epsilon_4' = (1-a^8)\frac{(1+a^{2^4}+\cdots+a^{2^m-2^4})(2-\alpha a^2-\alpha a^{3.2})}{2^{m-1}},$$

$$\cdots,$$

$$\epsilon_{m-1} = (1-a^{2^{m-2}})\frac{(1+a^{2^{m-1}})(2+\alpha a^{2^{m-4}}+\alpha a^{3.2^{m-4}})}{2^4},$$

$$\epsilon_{m-1}' = (1-a^{2^{m-2}})\frac{(1+a^{2^{m-1}})(2-\alpha a^{2^{m-4}}-\alpha a^{3.2^{m-4}})}{2^4},$$

$$\epsilon_m = (1-a^{2^{m-1}})\frac{(2+\alpha a^{2^{m-3}}+\alpha a^{3.2^{m-3}})}{2^3},$$

$$\epsilon_m' = (1-a^{2^{m-1}})\frac{(2-\alpha a^{2^{m-3}}-\alpha a^{3.2^{m-3}})}{2^3}$$

*formam um conjunto completo de idempotentes primitivos de* FG.

Demonstração: Claramente $\epsilon_0, \epsilon_1$ e $\epsilon_2$ são idempotentes dois a dois ortogonais, pois eles coincidem com os idempotentes do Lema 2.1.1.

De um modo geral, podemos escrever os idempotentes $\epsilon_j$ e $\epsilon_j'$, com $3 \leq j \leq m$, da seguinte forma

$$\epsilon_j = (1-a^{2^{j-1}})\frac{(1+a^{2^j}+\cdots+a^{2^m-2^j})(2+\alpha a^{2^{j-3}}+\alpha a^{3.2^{j-3}})}{2^{m-j+3}} \text{ e}$$

$$\epsilon_j' = (1-a^{2^{j-1}})\frac{(1+a^{2^j}+\cdots+a^{2^m-2^j})(2-\alpha a^{2^{j-3}}-\alpha a^{3.2^{j-3}})}{2^{m-j+3}}.$$

Os elementos $\epsilon_j$, com $3 \leq j \leq m$, são idempotentes, pois

$$\epsilon_j^2 = \left(1-a^{2^{j-1}}\right)^2 \frac{\left(1+a^{2^j}+\cdots+a^{2^m-2^j}\right)^2\left(2+\alpha a^{2^{j-3}}+\alpha a^{3.2^{j-3}}\right)^2}{2^{2m-2j+6}} =$$

$$\left(1-a^{2^{j-1}}\right)\left(1+a^{2^j}+\cdots+a^{2^m-2^j}\right)\left(2+\alpha a^{2^{j-3}}+\alpha a^{3.2^{j-3}}\right)^2 .$$

$$\frac{\left(1-a^{2^{j-1}}+a^{2^j}-a^{3.2^{j-i}}+a^{2^{j+1}}-a^{5.2^{j-1}}+\cdots+a^{2^m-2^j}-a^{2^m-2^{j-1}}\right)}{2^{2m-2j+6}} =$$

$$\left(1+a^{2^j}+\cdots+a^{2^m-2^j}\right).\left(2+\alpha a^{2^{j-3}}+\alpha a^{3.2^{j-3}}\right)^2 .$$

$$\frac{2.\left(1-a^{2^{j-1}}+a^{2^j}-a^{3.2^{j-i}}+a^{2^{j+1}}-a^{5.2^{j-1}}+\cdots+a^{2^m-2^j}-a^{2^m-2^{j-1}}\right)}{2^{2m-2j+6}} =$$

$$\left(1-a^{2^{j-1}}\right)\frac{\left(1+a^{2^j}+\cdots+a^{2^m-2^j}\right)^2\left(2+\alpha a^{2^{j-3}}+\alpha a^{3.2^{j-3}}\right)^2}{2^{2m-2j+5}}=$$

$$\left(1-a^{2^{j-1}}\right)\frac{2^{m-j}.\left(1+a^{2^j}+\cdots+a^{2^m-2^j}\right)\left(2+\alpha a^{2^{j-3}}+\alpha a^{3.2^{j-3}}\right)^2}{2^{2m-2j+5}}=$$

$$\left(1-a^{2^{j-1}}\right)\frac{\left(1+a^{2^j}+\cdots+a^{2^m-2^j}\right)\left(2+\alpha a^{2^{j-3}}+\alpha a^{3.2^{j-3}}\right)^2}{2^{m-j+5}}=$$

$$\left(1-a^{2^{j-1}}\right)\frac{\left(1+a^{2^j}+\cdots+a^{2^m-2^j}\right)\left(4+4\alpha a^{2^{j-3}}-2a^{2^{j-2}}+4\alpha a^{3.2^{j-3}}-4a^{2^{j-1}}-2a^{3.2^{j-2}}\right)}{2^{m-j+5}}=$$

$$\left(1-a^{2^{j-1}}+a^{2^j}-a^{3.2^{j-i}}+a^{2^{j+1}}-a^{5.2^{j-1}}+\cdots+a^{2^m-2^j}-a^{2^m-2^{j-1}}\right).$$

$$\frac{\left(4+4\alpha a^{2^{j-3}}-2a^{2^{j-2}}+4\alpha a^{3.2^{j-3}}-4a^{2^{j-1}}-2a^{3.2^{j-2}}\right)}{2^{m-j+5}}=$$

$$\frac{\left(1-a^{2^{j-1}}+a^{2^j}-a^{3.2^{j-i}}+a^{2^{j+1}}-a^{5.2^{j-1}}+\cdots+a^{2^m-2^j}-a^{2^m-2^{j-1}}\right)}{2^{m-j+5}}.$$

$$2^2.\left(2+\alpha a^{2^{j-3}}+\alpha a^{3.2^{j-3}}\right)=$$

$$\frac{\left(1-a^{2^{j-1}}\right)\left(1+a^{2^j}+\cdots+a^{2^m-2^j}\right)\left(2+\alpha a^{2^{j-3}}+\alpha a^{3.2^{j-3}}\right)}{2^{m-j+3}}=\epsilon_j.$$

Analogamente, prova-se que os elementos $\epsilon'_j$, com $3 \leq j \leq m$, também são idempotentes.

Vamos verificar que todos esses idempotentes são dois a dois ortogonais. Considere $\epsilon_j$ e $\epsilon_k$, com $j \neq k$ e $3 \leq j,k \leq m$. Suponha, sem perda de generalidade, que $k > j$. Para provarmos que

$$\epsilon_j\epsilon_k=(1-a^{2^{j-1}})\frac{(1+a^{2^j}+\cdots+a^{2^m-2^j})(2+\alpha a^{2^{j-3}}+\alpha a^{3.2^{j-3}})}{2^{m-j+3}}.$$

$$(1-a^{2^{k-1}})\frac{(1+a^{2^k}+\cdots+a^{2^m-2^k})(2+\alpha a^{2^{k-3}}+\alpha a^{3.2^{k-3}})}{2^{m-k+3}}=0,$$

basta notarmos que $(1+a^{2^j}+\cdots+a^{2^m-2^j}).(1-a^{2^{k-1}})=0$ pois $k-1 \geq j$.

Isto segue do fato que $a^{2^{k-1}}.(1+a^{2^j}+\cdots+a^{2^m-2^j})=(1+a^{2^j}+\cdots+a^{2^m-2^j})$. Portanto, $\epsilon_j$ e $\epsilon_k$ são ortogonais, para todos $j \neq k$. Analogamente conclui-se que $\epsilon'_j$ e $\epsilon'_k$ e $\epsilon_j$ e $\epsilon'_k$ são ortogonais para todos $j \neq k$.

Note que $\epsilon_0.\epsilon_j=0$ e $\epsilon_0.\epsilon'_j=0$, pois $(1-a^{2^{j-1}}).(1+a+a^2+\cdots+a^{2^m-1})=0$, para $3 \leq j \leq m$. Temos ainda $\epsilon_1.\epsilon_j=0$ e $\epsilon_1.\epsilon'_j=0$, pois

$$(1-a^{2^{j-1}}).(1-a+a^2-\cdots-a^{2^m-1})=$$

$$1-a+a^2-\cdots+a^{2^{j-1}}-a^{2^{j-1}+1}+\cdots-a^{2^m-1}-a^{2^{j-1}}+a^{2^{j-1}+1}-\cdots+a^{2^m-1}-1+a-\cdots+a^{2^{j-1}-1}=0.$$

Ainda $\epsilon_2.\epsilon_j = 0$ e $\epsilon_2.\epsilon'_j = 0$, pois

$$(1-a^{2^{j-1}}).(1-a^2+a^4-\cdots-a^{2^m-2}) =$$

$$1-a^2+a^4-\cdots+a^{2^{j-1}}-a^{2^{j-1}+2}+\cdots-a^{2^m-2}-a^{2^{j-1}}+a^{2^{j-1}+2}-\cdots+a^{2^m-2}-1+a^2-\cdots+a^{2^{j-1}-2}=0.$$

Agora

$$\epsilon_j.\epsilon'_j = \frac{1}{2^{2m-2j+6}}\left(1-a^{2^{j-1}}\right)^2\left(1+a^{2^j}+\cdots+a^{2^m-2^j}\right)^2.$$

$$\left(4-2\alpha a^{2^{j-3}}-2\alpha a^{3.2^{j-3}}+2\alpha a^{2^{j-3}}-\alpha^2 a^{2^{j-2}}-\alpha^2 a^{2^{j-1}}+2\alpha a^{3.2^{j-3}}-\alpha^2 a^{2^{j-1}}-\alpha^2 a^{3.2^{j-2}}\right) =$$

$$\frac{1}{2^{2m-2j+6}}\left(1-a^{2^{j-1}}\right)^2\left(1+a^{2^j}+\cdots+a^{2^m-2^j}\right)^2\left(4+4a^{2^{j-1}}+2a^{2^{j-2}}+2a^{3.2^{j-2}}\right) =$$

$$\frac{1}{2^{2m-2j+5}}\left(1-a^{2^{j-1}}\right)^2\left(1+a^{2^j}+\cdots+a^{2^m-2^j}\right)^2\left(2+a^{2^{j-2}}\right)\left(1+a^{2^{j-1}}\right).$$

Como $(1-a^{2^{j-1}}).(1+a^{2^{j-1}}) = 1-a^{2^j}$ e $(1-a^{2^j}).(1+a^{2^j}+\cdots+a^{2^m-2^j}) = 0$, segue que $\epsilon_j.\epsilon'_j = 0$.

Assim como no Lema 2.1.1, cada par de idempotentes ortogonais $\epsilon_j$ e $\epsilon'_j$, com $3 \leq j \leq m$, é tal que $\epsilon_j + \epsilon'_j = e_j = \widehat{G_j} - \widehat{G_{j-1}}$. Portanto a soma de todos estes idempotentes é igual a 1.

Eles são primitivos, pois existem exatamente $2m-1$ idempotentes nesta família, o mesmo número de componentes simples de FG, pela Proposição 1.4.1. □

O nosso objetivo agora, é determinar a dimensão e a distância mínima (ou peso) dos ideais minimais de $FC_{2^m}$ que são os ideais descritos de uma das seguintes formas: $I_i = (FC_{2^m})\epsilon_i$, $i = 0, 1, 2$, $J_j = (FC_{2^m})\epsilon_j$, ou $L_j = (FC_{2^m})\epsilon'_j$, com $j = 3, \ldots, m$.

**Proposição 3.1.2** *Sob as hipóteses da Proposição 3.1.1, considere os ideais minimais* $I_i = (FC_{2^m})\epsilon_i$, *com* $i = 0, 1, 2$. *Então:*

(i) $dim(I_i) = 1$ *e* $w(I_i) = 2^m$, *para* $i = 0, 1$;

(ii) $dim(I_2) = 2$ *e* $w(I_2) = 2^{m-1}$.

Demonstração: Podemos observar que os idempotentes $\epsilon_i$, com $i = 0, 1, 2$, coincidem com os idempotentes do Lema 2.1.1 e, portanto, os resultados seguem do Lema 2.2.1. □

**Proposição 3.1.3** *Sob as hipóteses da Proposição 3.1.1, considere os ideais minimais* $\mathrm{J}_j = (\mathrm{F}C_{2^m})\epsilon_j$, *com* $3 \leq j \leq m$. *Então,*

$$dim(\mathrm{J}_j) \geq 2^{j-2} \ e$$

$$w(\mathrm{J}_j) \leq w(\epsilon_j) = 3.2^{m-j+1}.$$

Demonstração: Mostraremos que, para $j = 3, \ldots, m$,

$$\mathrm{B}_j = \left\{\epsilon_j, a\epsilon_j, a^2\epsilon_j, \ldots, a^{2^{j-3}-1}\epsilon_j, a^{2^{j-2}}\epsilon_j, a^{2^{j-2}+1}\epsilon_j, a^{2^{j-2}+2}\epsilon_j, \ldots, a^{2^{j-2}+2^{j-3}-1}\epsilon_j\right\}$$

é um subconjunto linearmente independente de $\mathrm{J}_j$ e, portanto, teremos $dim(\mathrm{J}_j) \geq 2^{j-2}$. Para provarmos este fato, veremos que os elementos de $\mathrm{B}_j$ têm suportes disjuntos e, assim, são linearmente independentes.

Note que cada elemento de $\mathrm{B}_j$ é da forma $a^l\epsilon_j$ ou $a^{2^{j-2}+k}\epsilon_j$, com $0 \leq l, k \leq 2^{j-3} - 1$, e que $supp(a^l\epsilon_j) \subset a^l\langle a^{2^{j-3}}\rangle$ e $supp(a^{2^{j-2}+k}\epsilon_j) \subset a^{2^{j-2}+k}\langle a^{2^{j-3}}\rangle$. Seja $x \in supp(a^l\epsilon_j) \cap supp(a^{2^{j-2}+k}\epsilon_j) = a^l\langle a^{2^{j-3}}\rangle \cap a^{2^{j-2}+k}\langle a^{2^{j-3}}\rangle$, com $l \neq k$. Então

$$x = a^{l+r.2^{j-3}} = a^{2^{j-2}+k+s.2^{j-3}}.$$

Logo

$$a^{(l-k)+(r-s+2)2^{j-3}} = 1 \Longrightarrow 2^m \mid [(l-k) + (r-s+2)2^{j-3}].$$

Como $2^{j-3} \mid 2^m$, temos que

$$2^{j-3} \mid (l-k).$$

Assim, $l - k = 0$, pois $0 \leq l, k \leq 2^{j-3} - 1$, contradizendo a hipótese.

Portanto, $supp(a^l\epsilon_j) \cap supp(a^{2^{j-2}+k}\epsilon_j) = \emptyset$, e portanto o conjunto $\mathrm{B}_i$ é linearmente independente, o que implica $dim(\mathrm{J}_j) \geq 2^{j-2}$, para cada $j = 3, \ldots, m$.

Finalmente, para $3 \leq j \leq m$, como $\epsilon_j \in \mathrm{B}_j$ e $w(\epsilon_j) = 3.2^{m-j+1}$, temos $w(\mathrm{J}_j) \leq 3.2^{m-j+1}$.

□

**Proposição 3.1.4** *Sob as hipóteses da Proposição 3.1.1, considere os ideais minimais* $\mathrm{L}_j = (\mathrm{F}C_{2^m})\epsilon'_j$, *com* $3 \leq j \leq m$. *Então*

$$dim(\mathrm{L}_j) \geq 2^{j-2} \ e$$

$$w(\mathrm{L}_j) \leq w(\epsilon'_j) = 3.2^{m-j+1}.$$

Demonstração: A prova é semelhante à demonstração da Proposição 3.1.3, trocando-se $\epsilon_j$ por $\epsilon'_j$. □

**Lema 3.1.1** *Sob as hipóteses da Proposição 3.1.1, e considerando* $\mathrm{J}_j$ *e* $\mathrm{L}_j$*, como nas Proposições 3.1.3 e 3.1.4, para* $3 \leq j \leq m$*, temos*

$$dim(\mathrm{J}_j) = dim(\mathrm{L}_j) = 2^{j-2}.$$

Demonstração: Notemos o seguinte:

$$\sum_{i=0}^{2} dim(\mathrm{I}_i) + \sum_{j=3}^{m}(dim(\mathrm{J}_j) + dim(\mathrm{L}_j)) \geq 1+1+2+2.(2+4+\cdots+2^{m-2}) = 2^m = dim(\mathrm{FG}).$$

Portanto, vale a igualdade, e podemos concluir que $dim(\mathrm{J}_j) = dim(\mathrm{L}_j) = 2^{j-2}$. □

**Corolário 3.1.1** *Sob as hipóteses da Proposição 3.1.1, os conjuntos*

$$\mathrm{B}_j = \left\{\epsilon_j, a\epsilon_j, a^2\epsilon_j, \ldots, a^{2^{j-3}-1}\epsilon_j, a^{2^{j-2}}\epsilon_j, a^{2^{j-2}+1}\epsilon_j, a^{2^{j-2}+2}\epsilon_j, \ldots, a^{2^{j-2}+2^{j-3}-1}\epsilon_j\right\} \text{ e}$$

$$\mathrm{B}'_j = \left\{\epsilon'_j, a\epsilon'_j, a^2\epsilon'_j, \ldots, a^{2^{j-3}-1}\epsilon'_j, a^{2^{j-2}}\epsilon'_j, a^{2^{j-2}+1}\epsilon'_j, a^{2^{j-2}+2}\epsilon'_j, \ldots, a^{2^{j-2}+2^{j-3}-1}\epsilon'_j\right\}$$

*são bases visíveis de* $\mathrm{J}_j$ *e* $\mathrm{L}_j$*, respectivamente, e*

$$w(\mathrm{J}_j) = w(\mathrm{L}_j) = 3.2^{m-j+1}.$$

Demonstração: Segue do Lema 3.1.1, que $\mathrm{B}_j$ e $\mathrm{B}'_j$ são bases de $\mathrm{J}_j$ e $\mathrm{L}_j$, respectivamente. Ainda, como os elementos de $\mathrm{B}_j$ e $\mathrm{B}'_j$ têm suportes disjuntos, respectivamente, temos $w(x) \geq 3.2^{m-j+1}$, para todo $x \in \mathrm{J}_j$ ou $x \in \mathrm{L}_j$. Assim, $w(\mathrm{J}_j) = w(\mathrm{L}_j) = 3.2^{m-j+1}$. Como todos os elementos de $\mathrm{B}_j$ e de $\mathrm{B}'_j$ têm o mesmo peso, que é igual ao peso do ideal, resulta que estas bases são visíveis. □

## 3.2 Caso $q \equiv 5 \ (mod\ 8)$

Suponha $q \equiv 5 \ (mod\ 8)$. Neste caso, pelo Corolário1.4.1, o número de componentes simples de FG é $2m$ e pelo Lema 1.5.2, $-1$ é um quadrado em F. Assim, seja $\alpha \in \mathrm{F}$ um elemento tal que $\alpha^2 = -1$. No próximo resultado temos explicitados todos os idempotentes primitivos de FG, para $q \equiv 5 \ (mod\ 8)$.

**Proposição 3.2.1** *Sejam* F *um corpo com* $q$ *elementos, sendo* $q$ *uma potência de um primo ímpar* $p$ *tal que* $q \equiv 5 \pmod 8$ *e* $G = \langle a \mid a^{2^m} = 1 \rangle$ *o grupo cíclico gerado por* $a$ *de ordem* $2^m$. *Os elementos*

$$\epsilon_0 = \frac{1 + a + a^2 + \cdots + a^{2^m-1}}{2^m},$$

$$\epsilon_1 = \frac{1 - a + a^2 - \cdots - a^{2^m-1}}{2^m},$$

$$\epsilon_2 = (1 - a^2)\frac{(1 + a^4 + a^8 + \cdots + a^{2^m-2^2})(1 + \alpha a)}{2^m},$$

$$\epsilon_2' = (1 - a^2)\frac{(1 + a^4 + a^8 + \cdots + a^{2^m-2^2})(1 - \alpha a)}{2^m},$$

$$\epsilon_3 = (1 - a^4)\frac{(1 + a^8 + a^{16} + \cdots + a^{2^m-2^3})(1 + \alpha a^2)}{2^{m-1}},$$

$$\epsilon_3' = (1 - a^4)\frac{(1 + a^8 + a^{16} + \cdots + a^{2^m-2^3})(1 - \alpha a^2)}{2^{m-1}},$$

$$\cdots,$$

$$\epsilon_{m-1} = (1 - a^{2^{m-2}})\frac{(1 + a^{2^m-2^{m-1}})(1 + \alpha a^{2^{m-3}})}{2^3},$$

$$\epsilon_{m-1}' = (1 - a^{2^{m-2}})\frac{(1 + a^{2^m-2^{m-1}})(1 - \alpha a^{2^{m-3}})}{2^3},$$

$$\epsilon_m = (1 - a^{2^{m-1}})\frac{(1 + \alpha a^{2^{m-2}})}{2^2},$$

$$\epsilon_m' = (1 - a^{2^{m-1}})\frac{(1 - \alpha a^{2^{m-2}})}{2^2}$$

*formam um conjunto completo de idempotentes primitivos de* FG.

Demonstração: Claramente temos que $\epsilon_0$ e $\epsilon_1$ são idempotentes dois a dois ortogonais, pois eles coincidem com os idempotentes do Lema 2.1.1.

De um modo geral, podemos escrever os idempotentes $\epsilon_j$ e $\epsilon_j'$, com $2 \leq j \leq m$, da seguinte forma

$$\epsilon_j = (1 - a^{2^{j-1}})\frac{(1 + a^{2^j} + \cdots + a^{2^m-2^j})(1 + \alpha a^{2^{j-2}})}{2^{m-j+2}} \text{ e}$$

$$\epsilon_j' = (1 - a^{2^{j-1}})\frac{(1 + a^{2^j} + \cdots + a^{2^m-2^j})(1 - \alpha a^{2^{j-2}})}{2^{m-j+2}}.$$

Os elementos $\epsilon_j$, com $2 \leq j \leq m$, são idempotentes, pois

$$\epsilon_j^2 = \left(1 - a^{2^{j-1}}\right)^2 \frac{\left(1 + a^{2^j} + \cdots + a^{2^m-2^j}\right)^2 \left(1 + \alpha a^{2^{j-2}}\right)^2}{2^{2m-2j+4}} =$$

$$\left(1-a^{2^{j-1}}\right)\left(1+a^{2^j}+\cdots+a^{2^m-2^j}\right).$$

$$\frac{\left(1-a^{2^{j-1}}+a^{2^j}-a^{3.2^{j-i}}+a^{2^{j+1}}-a^{5.2^{j-1}}+\cdots+a^{2^m-2^j}-a^{2^m-2^{j-1}}\right)\left(1+\alpha a^{2^{j-2}}\right)^2}{2^{2m-2j+4}}=$$

$$\left(1+a^{2^j}+\cdots+a^{2^m-2^j}\right).\left(1+\alpha a^{2^{j-2}}\right)^2.$$

$$\frac{2.\left(1-a^{2^{j-1}}+a^{2^j}-a^{3.2^{j-i}}+a^{2^{j+1}}-a^{5.2^{j-1}}+\cdots+a^{2^m-2^j}-a^{2^m-2^{j-1}}\right)}{2^{2m-2j+4}}=$$

$$\left(1+a^{2^j}+\cdots+a^{2^m-2^j}\right).\left(1+\alpha a^{2^{j-2}}\right)^2.$$

$$\frac{\left(1-a^{2^{j-1}}\right)\left(1+a^{2^j}+\cdots+a^{2^m-2^j}\right)}{2^{2m-2j+3}}=$$

$$\left(1-a^{2^{j-1}}\right)\frac{\left(1+a^{2^j}+\cdots+a^{2^m-2^j}\right)^2\left(1+\alpha a^{2^{j-2}}\right)^2}{2^{2m-2j+3}}=$$

$$\left(1-a^{2^{j-1}}\right)\frac{2^{m-j}.\left(1+a^{2^j}+\cdots+a^{2^m-2^j}\right)\left(1+\alpha a^{2^{j-2}}\right)^2}{2^{2m-2j+3}}=$$

$$\left(1-a^{2^{j-1}}\right)\frac{\left(1+\alpha a^{2^{j-2}}\right)^2}{2^{m-j+3}}=$$

$$\left(1-a^{2^{j-1}}\right)\frac{\left(1+a^{2^j}+\cdots+a^{2^m-2^j}\right)\left(1+2\alpha a^{2^{j-2}}-a^{2^{j-1}}\right)}{2^{m-j+3}}=$$

$$\left(1-a^{2^{j-1}}+a^{2^j}-a^{3.2^{j-i}}+a^{2^{j+1}}-a^{5.2^{j-1}}+\cdots+a^{2^m-2^j}-a^{2^m-2^{j-1}}\right).$$

$$\frac{\left(1+2\alpha a^{2^{j-2}}-a^{2^{j-1}}\right)}{2^{m-j+3}}=$$

$$\frac{\left(1-a^{2^{j-1}}+a^{2^j}-a^{3.2^{j-i}}+a^{2^{j+1}}-a^{5.2^{j-1}}+\cdots+a^{2^m-2^j}-a^{2^m-2^{j-1}}\right)}{2^{m-j+3}}.2.\left(1+\alpha a^{2^{j-2}}\right)=$$

$$\frac{\left(1-a^{2^{j-1}}\right)\left(1+a^{2^j}+\cdots+a^{2^m-2^j}\right)\left(1+\alpha a^{2^{j-2}}\right)}{2^{m-j+2}}=\epsilon_j.$$

Analogamente prova-se que os elementos $\epsilon'_j$, para $2 \leq j \leq m$, são idempotentes.

Vamos verificar que todos esses idempotentes são dois a dois ortogonais. Considere $\epsilon_j$ e $\epsilon_k$, com $j \neq k$ e $2 \leq j,k \leq m$. Suponha, sem perda de generalidade, que $k > j$. Para provarmos a igualdade

$$\epsilon_j\epsilon_k = (1-a^{2^{j-1}})\frac{(1+a^{2^j}+\cdots+a^{2^m-2^j})(1+\alpha a^{2^{j-2}})}{2^{m-j+2}}.$$

$$(1-a^{2^{k-1}})\frac{(1+a^{2^k}+\cdots+a^{2^m-2^k})(1+\alpha a^{2^{k-2}})}{2^{m-k+2}}=0,$$

basta notarmos que $(1+a^{2^j}+\cdots+a^{2^m-2^j})\cdot(1-a^{2^{k-1}})=0$, pois $k-1\geq j$.

Isto segue de $a^{2^{k-1}}.(1+a^{2^j}+\cdots+a^{2^m-2^j})=(1+a^{2^j}+\cdots+a^{2^m-2^j})$. Portanto, $\epsilon_j$ e $\epsilon_k$ são ortogonais, para todos $2\leq j\neq k\leq m$. Analogamente, conclui-se que $\epsilon'_j$ e $\epsilon'_k$ e, $\epsilon_j$ e $\epsilon'_k$ são ortogonais para todos $2\leq j\neq k\leq m$.

Note que $\epsilon_0.\epsilon_j=0$ e $\epsilon_0.\epsilon'_j=0$, pois $(1-a^{2^{j-1}}).(1+a+a^2+\cdots+a^{2^m-1})=0$, para todo $2\leq j\leq m$. Temos também $\epsilon_1.\epsilon_j=0$ e $\epsilon_1.\epsilon'_j=0$, pois

$$(1-a^{2^{j-1}}).(1-a+a^2-\cdots-a^{2^m-1})=$$

$$1-a+a^2-\cdots+a^{2^{j-1}}-a^{2^{j-1}+1}+\cdots-a^{2^m-1}-a^{2^{j-1}}+a^{2^{j-1}+1}-\cdots+a^{2^m-1}-1+a-\cdots+a^{2^{j-1}-1}=0.$$

Temos ainda

$$\epsilon_j.\epsilon'_j=\frac{1}{2^{2m-2j+4}}\left(1-a^{2^{j-1}}\right)^2\left(1+a^{2^j}+\cdots+a^{2^m-2^j}\right)^2.\left(1-\alpha a^{2^{j-2}}+\alpha a^{2^{j-2}}-\alpha^2 a^{2^{j-1}}\right)=$$

$$\frac{1}{2^{2m-2j+4}}\left(1-a^{2^{j-1}}\right)^2\left(1+a^{2^j}+\cdots+a^{2^m-2^j}\right)^2\left(1+a^{2^{j-1}}\right).$$

Como $(1-a^{2^{j-1}}).(1+a^{2^{j-1}})=1-a^{2^j}$ e $(1-a^{2^j}).(1+a^{2^j}+\cdots+a^{2^m-2^j})=0$, segue que $\epsilon_j.\epsilon'_j=0$.

Cada par de idempotentes ortogonais $\epsilon_j$ e $\epsilon'_j$, com $2\leq j\leq m$, é tal que $\epsilon_j+\epsilon'_j=e_j=\widehat{G_j}-\widehat{G_{j-1}}$, assim como no Lema 2.1.1. Portanto a soma de todos estes idempotentes é igual a 1.

Eles são primitivos, pois existem exatamente $2m$ idempotentes nesta família, o mesmo número de componentes simples de FG, pelo Corolário 1.4.1. □

O nosso objetivo agora, é determinar a dimensão e a distância mínima dos ideais minimais de $FC_{2^m}$ que são de uma das seguintes formas: $I_i=(FC_{2^m})\epsilon_i$, $i=0,1$, $J_j=(FC_{2^m})\epsilon_j$ ou $L_j=(FC_{2^m})\epsilon'_j$, com $j=2,\ldots,m$.

**Proposição 3.2.2** *Sob as hipóteses da Proposição 3.2.1, considere os ideais minimais* $I_i=(FC_{2^m})\epsilon_i$, *com* $i=0,1$. *Então, para* $i=0,1$,

$$dim(I_i)=1 \text{ e } w(I_i)=2^m.$$

Demonstração: Podemos observar que os idempotentes $\epsilon_i$, com $i = 0, 1$, coincidem com os idempotentes do Lema 2.1.1 e, portanto, os resultados seguem do Lema 2.2.1. □

**Proposição 3.2.3** *Sob as hipóteses da Proposição 3.2.1, considere os ideais minimais* $\mathrm{J}_j = (\mathrm{F}C_{2^m})\epsilon_j$, *com* $2 \leq j \leq m$. *Então*

$$dim(\mathrm{J}_j) \geq 2^{j-2} \text{ e}$$

$$w(\mathrm{J}_j) \leq w(\epsilon_j) = 2^{m-j+2}.$$

Demonstração: Mostraremos que, para $j = 2, \ldots, m$,

$$\mathrm{B}_j = \left\{\epsilon_j, a\epsilon_j, a^2\epsilon_j, \ldots, a^{2^{j-3}-1}\epsilon_j, a^{2^{j-2}}\epsilon_j, a^{2^{j-2}+1}\epsilon_j, a^{2^{j-2}+2}\epsilon_j, \ldots, a^{2^{j-2}+2^{j-3}-1}\epsilon_j\right\}$$

é um subconjunto linearmente independente de $\mathrm{J}_j$ e, portanto, $dim(\mathrm{J}_j) \geq 2^{j-2}$. Para provarmos este fato, veremos que os elementos de $\mathrm{B}_j$ têm suportes disjuntos e, portanto, são linearmente independentes.

Note que cada elemento de $\mathrm{B}_j$ é da forma $a^l\epsilon_j$ ou $a^{2^{j-1}+k}\epsilon_j$, com $0 \leq l, k \leq 2^{j-3} - 1$, e que $supp(a^l\epsilon_j) \subset a^l\langle a^{2^{j-3}}\rangle$ e $supp(a^{2^{j-2}+k}\epsilon_j) \subset a^{2^{j-2}+k}\langle a^{2^{j-3}}\rangle$. Seja $x \in supp(a^l\epsilon_j) \cap supp(a^{2^{j-2}+k}\epsilon_j) = a^l\langle a^{2^{j-3}}\rangle \cap a^{2^{j-2}+k}\langle a^{2^{j-3}}\rangle$, com $l \neq k$. Então

$$x = a^{l+r.2^{j-3}} = a^{2^{j-2}+k+s.2^{j-3}}.$$

Logo

$$a^{(l-k)+(r-s+2)2^{j-3}} = 1 \Longrightarrow 2^m \mid [(l-k) + (r-s+2)2^{j-3}].$$

Como $2^{j-3} \mid 2^m$, temos que

$$2^{j-3} \mid (l-k).$$

Assim, $l - k = 0$, pois $0 \leq l, k \leq 2^{j-3} - 1$, contradizendo a hipótese.

Portanto, $supp(a^l\epsilon_j) \cap supp(a^{2^{j-2}+k}\epsilon_j) = \emptyset$ e daí o conjunto $\mathrm{B}_i$ é linearmente independente, o que implica que para cada $j = 2, \ldots, m$, tem-se $dim(\mathrm{J}_j) \geq 2^{j-2}$.

Finalmente, como $\epsilon_j \in \mathrm{B}_j$ e $w(\epsilon_j) = 2^{m-j+2}$, temos $w(\mathrm{J}_j) \leq 2^{m-j+2}$. □

**Proposição 3.2.4** *Sob as hipóteses da Proposição 3.2.1, considere os ideais minimais* $\mathrm{L}_j = (\mathrm{F}C_{2^m})\epsilon'_j$, *com* $2 \leq j \leq m$. *Então*

$$dim(\mathrm{L}_j) \geq 2^{j-2} \text{ e}$$

$$w(\mathrm{L}_j) \leq w(\epsilon'_j) = 2^{m-j+2}.$$

Demonstração: A prova é semelhante à demonstração da Proposição 3.2.3, trocando-se $\epsilon_j$ por $\epsilon'_j$. □

**Lema 3.2.1** *Sob as hipóteses da Proposição 3.2.1, e considerando* $\mathrm{J}_j$ *e* $\mathrm{L}_j$*, como nas Proposições 3.2.3 e 3.2.4, para* $2 \leq j \leq m$*, temos*

$$dim(\mathrm{J}_j) = dim(\mathrm{L}_j) = 2^{j-2}.$$

Demonstração: Somando as dimensões do ideais, temos:

$$\sum_{i=0}^{1} dim(\mathrm{I}_i) + \sum_{j=2}^{m}(dim(\mathrm{J}_j) + dim(\mathrm{L}_j)) \geq 1 + 1 + 2.(1 + 2 + \cdots + 2^{m-2}) = 2^m = dim(\mathrm{FG}).$$

Portanto, vale a igualdade e podemos concluir que $dim(\mathrm{J}_j) = dim(\mathrm{L}_j) = 2^{j-2}$. □

**Corolário 3.2.1** *Sob as hipóteses da Proposição 3.2.1, os conjuntos*

$$\mathrm{B}_j = \left\{\epsilon_j, a\epsilon_j, a^2\epsilon_j, \ldots, a^{2^{j-3}-1}\epsilon_j, a^{2^{j-2}}\epsilon_j, a^{2^{j-2}+1}\epsilon_j, a^{2^{j-2}+2}\epsilon_j, \ldots, a^{2^{j-2}+2^{j-3}-1}\epsilon_j\right\} \text{ e}$$

$$\mathrm{B}'_j = \left\{\epsilon'_j, a\epsilon'_j, a^2\epsilon'_j, \ldots, a^{2^{j-3}-1}\epsilon'_j, a^{2^{j-2}}\epsilon'_j, a^{2^{j-2}+1}\epsilon'_j, a^{2^{j-2}+2}\epsilon'_j, \ldots, a^{2^{j-2}+2^{j-3}-1}\epsilon'_j\right\}$$

*são bases visíveis de* $\mathrm{J}_j$ *e* $\mathrm{L}_j$*, respectivamente, e*

$$w(\mathrm{J}_j) = w(\mathrm{L}_j) = 2^{m-j+2}.$$

Demonstração: Segue do Lema 3.2.1, que $\mathrm{B}_j$ e $\mathrm{B}'_j$ são bases de $\mathrm{J}_j$ e $\mathrm{L}_j$, respectivamente. Ainda, como os elementos de $\mathrm{B}_j$ e $\mathrm{B}'_j$ têm suportes disjuntos, respectivamente, temos $w(x) \geq 2^{m-j+2}$, para todo $x \in \mathrm{J}_j$ ou $x \in \mathrm{L}_j$. Assim, $w(\mathrm{J}_j) = w(\mathrm{L}_j) = 2^{m-j+2}$. Como todos os elementos de $\mathrm{B}_j$ e de $\mathrm{B}'_j$ têm o mesmo peso, que é igual ao peso do ideal, resulta que estas bases são visíveis. □

## 3.3 Apêndice

Estudaremos, em alguns casos particulares, o número de componentes simples e os idempotentes primitivos, como anteriormente.

### 3.3.1 Caso $q \equiv 1 \ (mod\ 8)$

O caso $q \equiv 1 \ (mod\ 8)$ não apresenta uma regularidade como encontramos nos dois primeiros casos, pois não é possível expressar a ordem de $q$ em função de $m$, de modo geral.

**Exemplo 3.3.1** *Considere $q \equiv 1 \ (mod\ 8)$, onde $q$ é uma potência de um primo ímpar. Temos que não há uma regularidade na ordem de $q$, mod $2^m$.*

De fato: Considere $q = 17$ e $q = 9$. Note que $o(17) = 1 \ (mod\ 2^4)$ e $o(9) = 2 \ (mod\ 2^4)$, isto é, não existe uma expressão geral da ordem de $q$ para todo $q \equiv 1 \ (mod\ 8)$, como ocorre no Lema 1.4.1 para os casos em que $q \equiv 3$ ou $5 \ (mod\ 2^m)$.

Vamos considerar o caso particular em que $q \equiv 9 \ (mod\ 16)$. Neste caso, obtemos uma expressão geral para a ordem de $q$.

**Lema 3.3.1** *Se $q \equiv 9 \ (mod\ 16)$, então $o(q) = 2^{m-3} \ (mod\ 2^m)$, com $m \geq 3$.*

Demonstração: Façamos por indução sobre $m$.

Se $m = 3$, então $2^m = 8$ e, como $q \equiv 1 \ (mod\ 8)$, temos $o(q) = o(9) = 1 = 2^0 \ (mod\ 8)$.

Ainda, se $m = 4$ temos $9^{2^{m-3}} = 9^2 \equiv 1 \ (mod\ 2^4)$ e $9^{2^{m-4}} = 9 \not\equiv 1 \ (mod\ 2^4)$.

Vamos supor, por hipótese de indução, que $9^{2^{m-4}} \equiv 1 \ (mod\ 2^{m-1})$ e mostraremos que $9^{2^{m-3}} \equiv 1 \ (mod\ 2^m)$.

Temos

$$9^{2^{m-3}} - 1 = (9^{2^{m-4}})^2 - 1 = (9^{2^{m-4}} + 1)(9^{2^{m-4}} - 1).$$

Pela hipótese de indução, $2^{m-1} \mid (9^{2^{m-4}} - 1)$, e $2 \mid (9^{2^{m-4}} + 1)$, donde

$$9^{2^{m-3}} - 1 \equiv 0 \ (mod\ 2^m).$$

Veremos ainda que $9^{2^{m-4}} \not\equiv 1 \ (mod\ 2^m)$, o que completará a demonstração.

Suponha, por absurdo, $9^{2^{m-4}} \equiv 1 \ (mod\ 2^m)$. Equivalentemente, $3^{2^{m-3}} \equiv 1 \ (mod\ 2^m)$, o que contradiz o Lema 1.4.1, pois a ordem de 3 é $2^{m-2} \ (mod\ 2^m)$. Portanto, a ordem de $q$ é $2^{m-3} \ (mod\ 2^m)$. □

Precisamos notar alguns fatos sobre o número de componentes simples de uma álgebra de grupo neste caso.

**Proposição 3.3.1** *Seja* $G = \langle a \rangle$ *um grupo cíclico de ordem* $2^m$ *e* $q \equiv 9 \ (mod\ 16)$. *Se* $m = 1$, *então existem duas* F - *classes em* G. *Se* $m \geq 2$, *o número de* F - *classes é* $4(m-1)$.

Demonstração: Se $m = 1$, o resultado segue da Proposição 1.4.1. Suponha $m \geq 2$. Considere as $\mathbb{Q}$ - classes da Proposição 1.4.1, dadas por

$$C_0 = C_{\mathbb{Q}}(a) = \left\{a, a^3, a^5, a^7, \ldots, a^{2^m-1}\right\}$$

$$C_1 = C_{\mathbb{Q}}\left(a^2\right) = \left\{a^2, a^6, a^{10}, a^{14}, \ldots, a^{2.(2^{m-1}-1)}\right\}$$

$$C_2 = C_{\mathbb{Q}}\left(a^4\right) = \left\{a^4, a^{12}, a^{20}, a^{28}, \ldots, a^{4.(2^{m-2}-1)}\right\}$$

$$\vdots$$

$$C_i = C_{\mathbb{Q}}\left(a^{2^i}\right) = \left\{a^{2^i}, a^{3.2^i}, a^{5.2^i}, a^{7.2^i}, \ldots, a^{2^i.(2^{m-i}-1)}\right\}$$

$$\vdots$$

$$C_{m-3} = C_{\mathbb{Q}}\left(a^{2^{m-3}}\right) = \left\{a^{2^{m-3}}, a^{3.2^{m-3}}, a^{5.2^{m-3}}, a^{7.2^{m-3}}\right\}$$

$$C_{m-2} = C_{\mathbb{Q}}\left(a^{2^{m-2}}\right) = \left\{a^{2^{m-2}}, a^{3.2^{m-2}}\right\} = \left\{a^{2^{m-2}}, a^{2^{m-1}}.a^{2^{m-2}}\right\}$$

$$C_{m-1} = C_{\mathbb{Q}}\left(a^{2^{m-1}}\right) = \left\{a^{2^{m-1}}\right\}$$

$$C_m = C_{\mathbb{Q}}\left(a^{2^m}\right) = \{1\}.$$

Temos que as duas últimas $\mathbb{Q}$ - classes são claramente F - classes e, ainda,

$$C_{\mathbb{Q}}\left(a^{2^{m-2}}\right) = \left\{a^{2^{m-2}}, a^{3.2^{m-2}}\right\},$$

$$C_{\mathrm{F}}\left(a^{2^{m-2}}\right) = \left\{a^{2^{m-2}}, a^{q.2^{m-2}}\right\} = \left\{a^{2^{m-2}}\right\} \text{ e}$$

$$\mathcal{C}_{\mathrm{F}}\left(a^{3.2^{m-2}}\right)=\left\{a^{3.2^{m-2}}\right\},$$

isto é, a penúltima $\mathbb{Q}$ - classe se divide em duas F - classes. Falta verificar que para $0 \leq i \leq m-3$, as outras $\mathbb{Q}$ - classes se dividem em quatro F - classes cada. Para $i=0$, temos

$$\mathcal{C}_{\mathrm{F}}(a)=\left\{a^{0.2^3+1}, a^{1.2^3+1}, a^{2.2^3+1}, a^{3.2^3+1}, \ldots, a^{(2^{m-3}-1).2^3+1}\right\}=\left\{a^j \mid j \equiv 1 \text{ ou } 9 \ (mod\ 16)\right\},$$

$$\mathcal{C}_{\mathrm{F}}\left(a^3\right)=\left\{a^{0.2^3+3}, a^{1.2^3+3}, a^{2.2^3+3}, a^{3.2^3+3}, \ldots, a^{(2^{m-3}-1).2^3+3}\right\}=\left\{a^j \mid j \equiv 3 \text{ ou } 11 \ (mod\ 16)\right\},$$

$$\mathcal{C}_{\mathrm{F}}\left(a^5\right)=\left\{a^{0.2^3+5}, a^{1.2^3+5}, a^{2.2^3+5}, a^{3.2^3+5}, \ldots, a^{(2^{m-3}-1).2^3+5}\right\}=\left\{a^j \mid j \equiv 5 \text{ ou } 13 \ (mod\ 16)\right\} \text{ e}$$

$$\mathcal{C}_{\mathrm{F}}\left(a^7\right)=\left\{a^{0.2^3+7}, a^{1.2^3+7}, a^{2.2^3+7}, a^{3.2^3+7}, \ldots, a^{(2^{m-3}-1).2^3+7}\right\}=\left\{a^j \mid j \equiv 7 \text{ ou } 15 \ (mod\ 16)\right\},$$

isto é, a $\mathbb{Q}$ - classe de $a$ se divide em quatro F - classes. Temos ainda que cada $\mathbb{Q}$ - classe $\mathcal{C}_i=\mathcal{C}_{\mathbb{Q}}\left(a^{2^i}\right)=\left\{a^{2^i}, a^{3.2^i}, a^{5.2^i}, a^{7.2^i}, \ldots, a^{2^i.(2^{m-i}-1)}\right\}$, para $1 \leq i \leq m-3$, se divide nas seguintes F - classes

$$\left\{a^{(0.8+1)2^i}, a^{(1.8+1)2^i}, a^{(2.8+1)2^i}, \ldots, a^{[(2^{m-3}-1)2^3+1]2^i}\right\}=\left\{a^{j.2^i} \mid j \equiv 1 \ (mod\ 8)\right\},$$

$$\left\{a^{(0.8+3)2^i}, a^{(1.8+3)2^i}, a^{(2.8+3)2^i}, \ldots, a^{[(2^{m-3}-1)2^3+3]2^i}\right\}=\left\{a^{j.2^i} \mid j \equiv 3 \ (mod\ 8)\right\},$$

$$\left\{a^{(0.8+5)2^i}, a^{(1.8+5)2^i}, a^{(2.8+5)2^i}, \ldots, a^{[(2^{m-3}-1)2^3+5]2^i}\right\}=\left\{a^{j.2^i} \mid j \equiv 5 \ (mod\ 8)\right\} \text{ e}$$

$$\left\{a^{(0.8+7)2^i}, a^{(1.8+7)2^i}, a^{(2.8+7)2^i}, \ldots, a^{[(2^{m-3}-1)2^3+7]2^i}\right\}=\left\{a^{j.2^i} \mid j \equiv 7 \ (mod\ 8)\right\},$$

e isto segue do fato que $o(q)=2^{m-3}\ (mod\ 2^m)$. Portanto, temos $4(m-1)$ componentes simples em $\mathrm{F}C_{2^m}$, para $m \geq 2$. □

No caso em que $q \equiv 9\ (mod\ 16)$, pela Observação 1.5.1, que existe $\beta \in \mathrm{F}_q$ uma raiz oitava primitiva da unidade. No próximo resultado temos explicitados todos os idempotentes primitivos de FG, para $q \equiv 9\ (mod\ 16)$.

**Proposição 3.3.2** *Sejam* F *um corpo com* $q$ *elementos, sendo* $q$ *uma potência de um primo ímpar* $p$ *tal que* $q \equiv 9\ (mod\ 16)$ *e* $\mathrm{G}=\langle a \mid a^{2^m}=1\rangle$ *o grupo cíclico gerado por* $a$ *de ordem* $2^m$. *Os elementos*

$$\epsilon_0=\frac{1+a+a^2+\cdots+a^{2^m-1}}{2^m},$$

$$\epsilon_0'=\frac{1-a+a^2-\cdots-a^{2^m-1}}{2^m},$$

$$\epsilon_{2^{m-2}} = \frac{1}{2^m}\left(1+a^{2^{m-1}}\right)\left(1-a^2+a^4-\cdots-a^{2^{m-1}-2}\right)\left(1+\beta^2 a\right),$$

$$\epsilon_{3.2^{m-2}} = \frac{1}{2^m}\left(1+a^{2^{m-1}}\right)\left(1-a^2+a^4-\cdots-a^{2^{m-1}-2}\right)\left(1-\beta^2 a\right),$$

$$\epsilon_{11} = \frac{1}{8}\left(1-a^{2^{m-1}}\right)\left(1+\beta a^{2^{m-3}}+\beta^2 a^{2^{m-2}}+\beta^3 a^{3.2^{m-3}}\right),$$

$$\epsilon_{12} = \frac{1}{8}\left(1-a^{2^{m-1}}\right)\left(1+\beta^3 a^{2^{m-3}}-\beta^2 a^{2^{m-2}}+\beta a^{3.2^{m-3}}\right),$$

$$\epsilon_{13} = \frac{1}{8}\left(1-a^{2^{m-1}}\right)\left(1-\beta a^{2^{m-3}}+\beta^2 a^{2^{m-2}}-\beta^3 a^{3.2^{m-3}}\right),$$

$$\epsilon_{14} = \frac{1}{8}\left(1-a^{2^{m-1}}\right)\left(1-\beta^3 a^{2^{m-3}}-\beta^2 a^{2^{m-2}}-\beta a^{3.2^{m-3}}\right),$$

$$\epsilon_{j1} = \frac{1}{2^{m-(j-2)}}\left(1-a^{2^j}+a^{2^{j+1}}-a^{3.2^j}+\cdots-a^{2^m-2^j}\right)\left(1+\beta a^{2^{j-2}}+\beta^2 a^{2^{j-1}}+\beta^3 a^{3.2^{j-2}}\right),$$

$$\epsilon_{j2} = \frac{1}{2^{m-(j-2)}}\left(1-a^{2^j}+a^{2^{j+1}}-a^{3.2^j}+\cdots-a^{2^m-2^j}\right)\left(1+\beta^3 a^{2^{j-2}}-\beta^2 a^{2^{j-1}}+\beta a^{3.2^{j-2}}\right),$$

$$\epsilon_{j3} = \frac{1}{2^{m-(j-2)}}\left(1-a^{2^j}+a^{2^{j+1}}-a^{3.2^j}+\cdots-a^{2^m-2^j}\right)\left(1-\beta a^{2^{j-2}}+\beta^2 a^{2^{j-1}}-\beta^3 a^{3.2^{j-2}}\right),$$

$$\epsilon_{j4} = \frac{1}{2^{m-(j-2)}}\left(1-a^{2^j}+a^{2^{j+1}}-a^{3.2^j}+\cdots-a^{2^m-2^j}\right)\left(1-\beta^3 a^{2^{j-2}}-\beta^2 a^{2^{j-1}}-\beta a^{3.2^{j-2}}\right),$$

*para* $2 \leq j \leq m-2$, *formam um conjunto completo de idempotentes primitivos de* FG.

Demonstração: Claramente $\epsilon_0$ e $\epsilon_0'$ são idempotentes ortogonais, pois eles coincidem com os idempotentes do Lema 2.1.1. Para concluirmos que os elementos $\epsilon_{1i}$, com $1 \leq i \leq 4$, são idempotentes, faremos a demonstração para o caso particular de $\epsilon_{11}$. A prova para os outros elementos é análoga. Temos

$$\epsilon_{11}^2 = \frac{1}{64}\left(1-a^{2^{m-1}}\right)^2\left(1+\beta a^{2^{m-3}}+\beta^2 a^{2^{m-2}}+\beta^3 a^{3.2^{m-3}}\right)^2 =$$

$$\frac{1}{64}\left(2-2a^{2^{m-1}}\right)\left(1+2\beta a^{2^{m-3}}+3\beta^2 a^{2^{m-2}}+4\beta^3 a^{3.2^{m-3}}-3a^{2^{m-1}}-2\beta a^{5.2^{m-3}}-\beta^2 a^{3.2^{m-2}}\right) =$$

$$\frac{1}{32}\left(4+4\beta a^{2^{m-3}}+4\beta^2 a^{2^{m-2}}+4\beta^3 a^{3.2^{m-3}}-4a^{2^{m-1}}-4\beta a^{5.2^{m-3}}-4\beta^2 a^{3.2^{m-2}}-4\beta^3 a^{7.2^{m-3}}\right) =$$

$$\epsilon_{11}.$$

O elemento $\epsilon_{2^{m-2}}$ também é idempotente, pois

$$\epsilon_{2^{m-2}}^2 = \frac{1}{2^{2m}}\left(1+a^{2^{m-1}}\right)^2\left(1-a^2+a^4-\cdots-a^{2^{m-1}-2}\right)^2\left(1+\beta^2 a\right)^2 =$$

$$\frac{1}{2^{2m}}\left(1+a^{2^{m-1}}\right)\left(1-a^2+a^4-\cdots-a^{2^{m-1}-2}\right)\left(1+2\beta^2 a+\beta^4 a^2\right).$$

$$\left(1-a^2+a^4-a^6+\cdots-a^{2^{m-1}-2}+a^{2^{m-1}}-a^{2^{m-1}+2}+\cdots-a^{2^m-2}\right)=$$

$$\frac{1}{2^{2m}}2^{m-2}\left(1-a^2+a^4-a^6+\cdots-a^{2^{m-1}-2}+a^{2^{m-1}}-a^{2^{m-1}+2}+\cdots-a^{2^m-2}\right).$$

$$\left(1+a^{2^{m-1}}\right)\left(1+2\beta^2a-a^2\right)=$$

$$\frac{1}{2^{m+2}}\left(1+a^{2^{m-1}}\right)\left(1-a^2+a^4-a^6+\cdots-a^{2^{m-1}-2}+a^{2^{m-1}}-a^{2^{m-1}+2}+\cdots-a^{2^m-2}\right).$$

$$\left(2+2\beta^2a\right)=$$

$$\frac{1}{2^{m+1}}\left(1+a^{2^{m-1}}\right)^2\left(1-a^2+a^4-\cdots-a^{2^{m-1}-2}\right)\left(1+\beta^2a\right)=\epsilon_{2^{m-2}}.$$

Analogamente, prova-se que $\epsilon_{3.2^{m-2}}$ é idempotente.

Falta mostrar que os elementos $\epsilon_{ji}$, com $1\leq i\leq 4$ e $2\leq j\leq m-2$, são idempotentes. Faremos a demonstração para $\epsilon_{j1}$ e, analogamente, obtém-se os mesmos resultados para os outros elementos deste tipo. Temos

$$\epsilon_{j1}^2=\frac{1}{2^{2m-2j+4}}\left(1-a^{2^j}+a^{2^{j+1}}-a^{3.2^j}+\cdots-a^{2^m-2^j}\right)^2\left(1+\beta a^{2^{j-2}}+\beta^2a^{2^{j-1}}+\beta^3a^{3.2^{j-2}}\right)^2=$$

$$\frac{1}{2^{2m-2j+4}}.2^{m-j}\left(1-a^{2^j}+a^{2^{j+1}}-a^{3.2^j}+\cdots-a^{2^m-2^j}\right).$$

$$\left[\left(1-3a^{2^j}\right)+\left(2\beta-2\beta a^{2^j}\right)a^{2^{j-2}}+\left(3\beta^2-\beta^2a^{2^j}\right)a^{2^{j-1}}+4\beta^3a^{3.2^{j-2}}\right]=$$

$$\frac{1}{2^{m-j+4}}\left(1-a^{2^j}+a^{2^{j+1}}-a^{3.2^j}+\cdots-a^{2^m-2^j}\right).$$

$$\left[\left(1-3a^{2^j}\right)+2\beta\left(1-a^{2^j}\right)a^{2^{j-2}}+\beta^2\left(3-a^{2^j}\right)a^{2^{j-1}}+4\beta^3a^{3.2^{j-2}}\right]=$$

$$\frac{1}{2^{m-j+4}}.4\left(1-a^{2^j}+a^{2^{j+1}}-a^{3.2^j}+\cdots-a^{2^m-2^j}\right)+$$

$$\frac{1}{2^{m-j+4}}.4\beta a^{2^{j-2}}\left(1-a^{2^j}+a^{2^{j+1}}-a^{3.2^j}+\cdots-a^{2^m-2^j}\right)+$$

$$\frac{1}{2^{m-j+4}}.4\beta^2a^{2^{j-1}}\left(1-a^{2^j}+a^{2^{j+1}}-a^{3.2^j}+\cdots-a^{2^m-2^j}\right)$$

$$\frac{1}{2^{m-j+4}}.4\beta^3a^{3.2^{j-2}}\left(1-a^{2^j}+a^{2^{j+1}}-a^{3.2^j}+\cdots-a^{2^m-2^j}\right)=$$

$$\frac{1}{2^{m-j+2}}\left(1-a^{2^j}+a^{2^{j+1}}-a^{3.2^j}+\cdots-a^{2^m-2^j}\right)\left(1+\beta a^{2^{j-2}}+\beta^2a^{2^{j-1}}+\beta^3a^{3.2^{j-2}}\right)=\epsilon_{j1}.$$

Vamos verificar que estes idempotentes são dois a dois ortogonais. Claramente, $\epsilon_{2^{m-2}}$ e

$\epsilon_{3.2^{m-2}}$ são ortogonais aos idempotentes $\epsilon_{1i}$, com $1 \leq i \leq 4$, pois $(1-a^{2^{m-1}})(1+a^{2^{m-1}}) = 0$. E também $\epsilon_{2^{m-2}}$ e $\epsilon_{3.2^{m-2}}$ são ortogonais a $\epsilon_0$ e $\epsilon_0'$, pois

$$\left(1-a^2+a^4-\cdots-a^{2^{m-1}-2}\right)\left(1+a+a^2+\cdots+a^{2^{m-1}}\right)=0 \text{ e}$$

$$\left(1-a^2+a^4-\cdots-a^{2^{m-1}-2}\right)\left(1-a+a^2-\cdots-a^{2^{m-1}}\right)=0.$$

Precisamos mostrar que $\epsilon_{1i}.\epsilon_{1k} = 0$, se $i \neq k$ com $1 \leq i,k \leq 4$. Faremos um caso e o restante segue analogamente. Temos $\epsilon_{11}.\epsilon_{13} = 0$, pois

$$\left(1+\beta a^{2^{m-3}}+\beta^2 a^{2^{m-2}}+\beta^3 a^{3.2^{m-3}}\right)\left(1-\beta a^{2^{m-3}}+\beta^2 a^{2^{m-2}}-\beta^3 a^{3.2^{m-3}}\right)=$$

$$\left(1+\beta^2 a^{2^{m-2}}+a^{2^{m-1}}+\beta^2 a^{3.2^{m-2}}\right) \text{ e}$$

$$\left(1+\beta^2 a^{2^{m-2}}+a^{2^{m-1}}+\beta^2 a^{3.2^{m-2}}\right)\left(1-a^{2^{m-1}}\right)=0.$$

Para verificar que $\epsilon_{1i}$ é ortogonal a $\epsilon_{jl}$, com $1 \leq i,l \leq 4$ e $2 \leq j \leq m-2$, basta notarmos que $\left(1-a^{2^{m-1}}\right)\left(1-a^{2^j}+a^{2^{j+1}}-a^{3.2^j}+\cdots-a^{2^m-2^j}\right)=0$. Além disso, os elementos $\epsilon_{2^{m-2}}$ e $\epsilon_{3.2^{m-2}}$ são ortogonais aos idempotentes $\epsilon_{jl}$, com $1 \leq l \leq 4$ e $2 \leq j \leq m-2$, pois $\left(1-a^{2^j}\right)\left(1-a^2+a^4-a^6+\cdots-a^{2^{m-1}-2}+a^{2^{m-1}}-a^{2^{m-1}+2}+\cdots-a^{2^m-2}\right)=0$.

Precisamos verificar que $\epsilon_{jl}.\epsilon_{tk} = 0$, com $2 \leq j,t \leq m-2$, $1 \leq l,k \leq 4$, $l \neq k$ ou $j \neq t$. Faremos isso, em particular, para $\epsilon_{j1}$ e $\epsilon_{j2}$ e o restante segue analogamente. Note que

$$\left(1+\beta a^{2^{j-2}}+\beta^2 a^{2^{j-1}}+\beta^3 a^{3.2^{j-2}}\right)\left(1+\beta^3 a^{2^{j-2}}-\beta^2 a^{2^{j-1}}+\beta a^{3.2^{j-2}}\right)\left(1-a^{2^j}\right)=$$

$$\left(1+(\beta^3+\beta)a^{2^{j-2}}+(\beta+\beta^3)a^{5.2^{j-2}}-a^{2^{j-1}}+a^{2^j}-a^{3.2^{j-1}}\right)\left(1-a^{2^j}\right)=$$

$$\left(1+(\beta^3+\beta)a^{2^{j-2}}+(\beta+\beta^3)a^{9.2^{j-2}}-a^{2^{j-1}}+a^{2^{j+1}}-a^{5.2^{j-1}}\right)=$$

$$\left(1-a^{2^{j+1}}\right)\left(1+(\beta^3+\beta)a^{2^{j-2}}-a^{2^{j-1}}\right)$$

e, como $\left(1-a^{2^{j+1}}\right)\left(1+a^{2^{j+1}}+a^{2^{j+2}}+\cdots+a^{2^m-2^{j+1}}\right)=0$, segue o resultado.

Note que estes idempotentes ortogonais $\epsilon_{j1}, \epsilon_{j2}, \epsilon_{j3}$ e $\epsilon_{j4}$, com $1 \leq j \leq m-2$, são tais que $\epsilon_{j1}+\epsilon_{j2}+\epsilon_{j3}+\epsilon_{j4} = e_{j+1}$ e $\epsilon_{2^{m-2}}+\epsilon_{3.2^{m-2}} = e_2$, assim como no Lema 2.1.1. Portanto, a soma de todos estes idempotentes é igual a 1.

Eles são primitivos, pois existem exatamente $4(m-1)$ idempotentes nesta família, pela Proposição 3.3.1. □

### 3.3.2 Caso $q \equiv 7 \ (mod\ 8)$

Como nos casos anteriores, o caso $q \equiv 7 \ (mod\ 8)$ não apresenta uma regularidade facilmente perceptível, pois não podemos expressar a ordem de $q \ (mod\ 2^m)$ de modo geral.

**Exemplo 3.3.2** *Considere $q \equiv 7 \ (mod\ 8)$, onde $q$ é uma potência de um primo ímpar. Veremos que não há uma regularidade na ordem de $q$*

De fato: Considere $q = 7$ e $q = 31$. Note que $o(7) = 4 \ (mod\ 2^5)$ e $o(31) = 2 \ (mod\ 2^5)$, isto é, não existe uma expressão geral da ordem de $q$ para todo $q \equiv 7 \ (mod\ 8)$, como ocorre no Lema 1.4.1 para os casos em que $q \equiv 3$ ou $5 \ (mod\ 2^m)$.

Vamos considerar o caso particular em que $q \equiv 7 \ (mod\ 16)$. Neste caso, obtemos uma expressão geral para a ordem de $q$.

**Lema 3.3.2** *Se $q \equiv 7 \ (mod\ 16)$, então $o(q) = 2^{m-3} \ (mod\ 2^m)$ , com $m \geq 3$.*

Demonstração: Note que se $q \equiv 7 \ (mod\ 16)$, então $q \equiv -9 \ (mod\ 16)$. Logo, $q^{2^{m-3}} \equiv (-9)^{2^{m-3}} \equiv (-1)^{2^{m-3}} 9^{2^{m-3}} \equiv 1 \ (mod\ 2^m)$, pela Proposição 3.3.1.

Precisamos verificar ainda que $q^{2^{m-4}} \not\equiv 1 \ (mod\ 2^m)$. Suponha $7^{2^{m-4}} \equiv 1 \ (mod\ 2^m)$ para $m \geq 4$. Então, $(-9)^{2^{m-4}} \equiv 1 \ (mod\ 2^m)$, implicando em $3^{2^{m-3}} = (-1)^{2^{m-4}} 3^{2^{m-4}} \equiv 1 \ (mod\ 2^m)$, uma contradição com o Lema 1.4.2. Portanto, segue o resultado. □

Precisamos notar alguns fatos sobre o número de componentes simples de uma álgebra de grupo neste caso.

**Proposição 3.3.3** *Seja $\mathrm{G} = \langle a \rangle$ um grupo cíclico de ordem $2^m$ e $q \equiv 7 \ (mod\ 16)$. Se $m = 1$, então existem duas* F - *classes em* G. *Se $m = 2$, então existem três* F - *classes em* G. *Se $m \geq 3$, então o número de* F - *classes é $4m - 7$.*

Demonstração: Se $m = 1$, o resultado segue da Proposição 1.4.1. Se $m = 2$, então $C_{\mathrm{F}}(a) = \{a, a^3\} = C_{\mathbb{Q}}(a)$, $C_{\mathrm{F}}(1) = \{1\} = C_{\mathbb{Q}}(1)$ e $C_{\mathrm{F}}(a^2) = \{a^2\} = C_{\mathbb{Q}}(a^2)$. Suponha $m \geq 3$. Considere as $\mathbb{Q}$ - classes da Proposição 1.4.1, dadas por

$$C_0 = C_{\mathbb{Q}}(a) = \left\{a, a^3, a^5, a^7, \ldots, a^{2^m-1}\right\}$$

$$\mathcal{C}_1 = \mathcal{C}_{\mathbb{Q}}\left(a^2\right) = \left\{a^2, a^6, a^{10}, a^{14}, \ldots, a^{2.(2^{m-1}-1)}\right\}$$

$$\mathcal{C}_2 = \mathcal{C}_{\mathbb{Q}}\left(a^4\right) = \left\{a^4, a^{12}, a^{20}, a^{28}, \ldots, a^{4.(2^{m-2}-1)}\right\}$$

$$\vdots$$

$$\mathcal{C}_i = \mathcal{C}_{\mathbb{Q}}\left(a^{2^i}\right) = \left\{a^{2^i}, a^{3.2^i}, a^{5.2^i}, a^{7.2^i}, \ldots, a^{2^i.(2^{m-i}-1)}\right\}$$

$$\vdots$$

$$\mathcal{C}_{m-3} = \mathcal{C}_{\mathbb{Q}}\left(a^{2^{m-3}}\right) = \left\{a^{2^{m-3}}, a^{3.2^{m-3}}, a^{5.2^{m-3}}, a^{7.2^{m-3}}\right\}$$

$$\mathcal{C}_{m-2} = \mathcal{C}_{\mathbb{Q}}\left(a^{2^{m-2}}\right) = \left\{a^{2^{m-2}}, a^{3.2^{m-2}}\right\} = \left\{a^{2^{m-2}}, a^{2^{m-1}}.a^{2^{m-2}}\right\}$$

$$\mathcal{C}_{m-1} = \mathcal{C}_{\mathbb{Q}}\left(a^{2^{m-1}}\right) = \left\{a^{2^{m-1}}\right\}$$

$$\mathcal{C}_m = \mathcal{C}_{\mathbb{Q}}\left(a^{2^m}\right) = \{1\}.$$

Observamos que as duas últimas $\mathbb{Q}$ - classes são claramente F - classes e, ainda,

$$\mathcal{C}_{\mathrm{F}}\left(a^{2^{m-2}}\right) = \left\{a^{2^{m-2}}, a^{q.2^{m-2}}\right\} = \left\{a^{2^{m-2}}, a^{3.2^{m-2}}\right\} = \mathcal{C}_{\mathbb{Q}}\left(a^{2^{m-2}}\right).$$

Portanto, as três últimas $\mathbb{Q}$ - classes são iguais às F - classes. Precisamos verificar que a $\mathbb{Q}$ - classe de $a^{2^{m-3}}$ se divide em duas F - classes. De fato, pois

$$\mathcal{C}_{\mathrm{F}}\left(a^{2^{m-3}}\right) = \left\{a^{2^{m-3}}, a^{7.2^{m-3}}\right\} \text{ e}$$

$$\mathcal{C}_{\mathrm{F}}\left(a^{3.2^{m-3}}\right) = \left\{a^{3.2^{m-3}}, a^{5.2^{m-3}}\right\}.$$

Falta verificar que todas as primeiras $m-4$ $\mathbb{Q}$ - classes se dividem em quatro F - classes cada. Para $i = 0$, temos

$$\mathcal{C}_{\mathrm{F}}(a) = \left\{a^{0.2^3+1}, a^{1.2^3-1}, a^{2.2^3+1}, a^{3.2^3-1}, \ldots, a^{(2^{m-3}-1).2^3-1}\right\} = \left\{a^j \mid j \equiv 1 \text{ ou } 7 \ (mod\ 16)\right\},$$

$$\mathcal{C}_{\mathrm{F}}\left(a^3\right) = \left\{a^{0.2^3+3}, a^{1.2^3-3}, a^{2.2^3+3}, a^{3.2^3-3}, \ldots, a^{(2^{m-3}-1).2^3-3}\right\} = \left\{a^j \mid j \equiv 3 \text{ ou } 5 \ (mod\ 16)\right\},$$

$$\mathcal{C}_{\mathrm{F}}\left(a^9\right) = \left\{a^{0.2^3+3^2}, a^{1.2^3-3^2}, a^{2.2^3+3^2}, a^{3.2^3-3^2}, \ldots, a^{(2^{m-3}-1).2^3-3^2}\right\} =$$

$$\left\{a^j \mid j \equiv 9 \text{ ou } 15 \ (mod\ 16)\right\} \text{ e}$$

$$\mathcal{C}_{\mathrm{F}}\left(a^{27}\right) = \left\{a^{0.2^3+3^3}, a^{1.2^3-3^3}, a^{2.2^3+3^3}, a^{3.2^3-3^3}, \ldots, a^{(2^{m-3}-1).2^3-3^3}\right\} =$$

$$\left\{a^j \mid j \equiv 11 \text{ ou } 13 \ (mod\ 16)\right\},$$

isto é, a $\mathbb{Q}$ - classe do $a$ se divide em quatro F - classes. Ainda, para $1 \leq i \leq m-2$, cada $\mathbb{Q}$ - classe $C_i = C_{\mathbb{Q}}\left(a^{2^i}\right) = \left\{a^{2^i}, a^{3.2^i}, a^{5.2^i}, a^{7.2^i}, \ldots, a^{2^i.(2^{m-i}-1)}\right\}$ se divide nas seguintes F - classes:

$$\left\{a^{(0.8+1)2^i}, a^{(1.8-1)2^i}, a^{(2.8+1)2^i}, \ldots, a^{[(2^{m-i-3}-1)8-1]2^i}\right\} = \left\{a^{j.2^i} \mid j \equiv 1 \text{ ou } 7 \ (mod\ 16)\right\},$$

$$\left\{a^{(0.8+3)2^i}, a^{(1.8-3)2^i}, a^{(2.8+3)2^i}, \ldots, a^{[(2^{m-i-3}-1)8-1]2^i}\right\} = \left\{a^{j.2^i} \mid j \equiv 3 \text{ ou } 5 \ (mod\ 16)\right\},$$

$$\left\{a^{(1.8+1)2^i}, a^{(2.8-1)2^i}, a^{(3.8+1)2^i}, \ldots, a^{(2^{m-i-3}.2^3-1)2^i}\right\} = \left\{a^{j.2^i} \mid j \equiv 9 \text{ ou } 15 \ (mod\ 16)\right\} \text{ e}$$

$$\left\{a^{(1.8+3)2^i}, a^{(2.8-3)2^i}, a^{(3.8+3)2^i}, \ldots, a^{(2^{m-i-3}.2^3-3)2^i}\right\} = \left\{a^{j.2^i} \mid j \equiv 11 \text{ ou } 13 \ (mod\ 16)\right\},$$

e isto segue de $o(q) = 2^{m-3}\ (mod\ 2^m)$. Com isto, concluímos que existem $4m-7$ componentes simples em $FC_{2^m}$ se $m \geq 3$. □

# Capítulo 4

# Ideais em uma Álgebra de Grupo Abeliana Modular

Este capítulo contém simplificações dos resultados de Poli [12], para obter de forma mais clara e rápida a descrição dos ideais principais nilpotentes a partir da estrutura da álgebra de um determinado grupo abeliano. Nesse artigo, o autor trabalha com ideais de anéis de polinômios em várias variáveis. É precisamente o fato de utilizar a estrutura de grupo que permite simplificar muito e tornar mais claros os resultados.

## 4.1 Ideais nilpotentes de dimensão máxima

Consideremos $F_q$ um corpo, onde $q$ é uma potência de um primo $p$ e G um grupo abeliano finito. Podemos escrever G como produto direto $G = P \times H$, onde P é o $p$ - subgrupo de Sylow de G e $(|H|, p) = 1$. Escrevemos P na forma:

$$P =< a_1 > \times \cdots \times < a_n >= C_{q_1} \times \cdots \times C_{q_n} \tag{4.1}$$

onde $a_i^{q_i} = 1$, $i = 1, \ldots, n$, com $q_i = p^{r_i}$, para algum $r_i \in \mathbb{N}$. Convencionaremos que $q_1 \leq q_2 \leq \cdots \leq q_n$. Como $(|H|, p) = 1)$, temos por Perlis-Walker 1.1.3, que

$$FG \cong F(P \times H) \cong (FH)P \cong \left( \bigoplus_{i=1}^{t} K_i \right) P \cong K_1P \oplus \cdots \oplus K_tP,$$

com $K_i = F(\zeta_i)$ e $car(K_i) = p$.

Assim, consideraremos a álgebra de grupo $C = KP$, onde P é o subgrupo descrito acima e K é um corpo de característica $p$. Denotaremos por J o radical de Jacobson de KP. Sabe-se que $J = J(KP) = \Delta(P)$ (veja [10, Teoremas 2.7.16 e 6.3.1]).

**Proposição 4.1.1** *(Poli, [12, Proposição 1]) Sejam $\gamma \in KP = C$ com índice de nilpotência $s$ e $\langle\gamma\rangle$ o ideal gerado por $\gamma$. Então,*

(i) $dim\langle\gamma\rangle \leq \dfrac{s-1}{s}|P|$;

(ii) (a) $dim\langle\gamma\rangle = \dfrac{s-1}{s}|P| \iff Ann\gamma^i = \langle\gamma^{s-i}\rangle$, *para* $1 \leq i \leq s-1$;

(b) $dim\langle\gamma\rangle < \dfrac{s-1}{s}|P| \iff Ann\gamma^i \neq \langle\gamma^{s-i}\rangle$, *para* $1 \leq i \leq s-1$.

Demonstração: A demonstração que reproduzimos a seguir é a demonstração original de [12].

(i) Sejam $\varphi_{\gamma^i}$, com $1 \leq i \leq s-1$, endomorfismos de C, induzidos pela multiplicação por $\gamma^i$. Seja $f_i$ a restrição de $\varphi_{\gamma^i}$ ao ideal $\langle\gamma\rangle$ de C, com $1 \leq i \leq s-1$. Como $dim[Im(f_i)] + dim[Ker(f_i)] = dim\langle\gamma\rangle$, temos

$$dim\langle\gamma^{i+1}\rangle + dim(\langle\gamma\rangle \cap Ann\langle\gamma^i\rangle) = dim\langle\gamma\rangle.$$

Por outro lado, $dim[Ann\langle\gamma^i\rangle] + dim[Im(\varphi_{\gamma^i})] = dimC$ implica $dim(\langle\gamma\rangle \cap Ann\langle\gamma^i\rangle) \leq dim[Ann\langle\gamma^i\rangle] = dimC - dim[Im(\varphi_{\gamma^i})] = |P| - dim\langle\gamma^i\rangle$.

Portanto,

$$dim\langle\gamma\rangle \leq dim\langle\gamma^{i+1}\rangle + |P| - dim\langle\gamma^i\rangle.$$

Para $1 \leq i \leq s-1$, obtemos $dim\langle\gamma\rangle \leq \dfrac{s-1}{s}|P|$.

(ii) Para todo $r \in \{1, \ldots, s-2\}$, temos que $Ann\gamma^r = \langle\gamma^{s-r}\rangle$ se, e somente se, $Ann\gamma^{r-1} = \langle\gamma^{s-r+1}\rangle$. De fato, considere $Ann\gamma^r = \langle\gamma^{s-r}\rangle$. Claramente $\langle\gamma^{s-r+1}\rangle \subset Ann\gamma^{r-1}$, pois se $\alpha\gamma^{s-r+1} \in \langle\gamma^{s-r+1}\rangle$, então $\alpha\gamma^{s-r+1}\gamma^{r-1} = \alpha\gamma^s = 0$. Por outro lado, se $x \in Ann\gamma^{r-1}$, então $x\gamma^{r-1} = 0$, implicando que $x\gamma^{-1} \in \langle\gamma^{s-r}\rangle$. Logo $x = \beta\gamma^{s-r+1} \in \langle\gamma^{s-r+1}\rangle$. Analogamente prova-se a outra implicação.

Assim, temos $Ann\gamma^i = \langle\gamma^{s-i}\rangle$ ou $Ann\gamma^i \neq \langle\gamma^{s-i}\rangle$, para $1 \leq i \leq s-1$. Além disso, de acordo com a prova da afirmação $(i)$, temos que se $dim\langle\gamma\rangle = \dfrac{s-1}{s}|P|$, então $Ann\gamma^{s-1} = \langle\gamma\rangle$.

E, se $dim\langle\gamma\rangle \neq \frac{s-1}{s}|\mathrm{P}|$, então $Ann\gamma^{s-1} \neq \langle\gamma\rangle$. O resultado segue da equivalência anterior.

□

Os próximos resultados também encontram-se em [12], porém procuramos demonstrá-los de forma mais simples usando teoria de Álgebra de Grupo.

**Lema 4.1.1** *Se* $\gamma \in \mathrm{KP}$ *gera um ideal nilpotente de dimensão máxima em* KP, *então* $\gamma^{q_n-1} \neq 0$ *e* $dim\langle\gamma\rangle = (q_n - 1)q_1 \ldots q_{n-1}$.

Demonstração: Como $q_n \geq q_{n-1} \geq \cdots \geq q_1$ em , então $exp(\mathrm{P}) = q_n$ e, assim, para todo $g \in \mathrm{P}$, tem-se $g^{q_n} = 1$. Como $\{g-1|g \in \mathrm{P}, g \neq 1\}$ é uma base de $\Delta(\mathrm{P})$ e $(g-1)^{q_n} = 0$, então $\Delta(\mathrm{P})^{q_n} = 0$, logo o índice de nilpotência de $\Delta(\mathrm{P})$ é exatamente $q_n$, pois existe $a_n - 1 \in \Delta(\mathrm{P})$, com índice de nilpotência $q_n$.

Claramente, se $\gamma$ gera um ideal de índice de nilpotência máximo, então devemos ter $\gamma^{q_n} = 0$ e $\gamma^{q_n-1} \neq 0$.

Pela parte (ii) da Proposição 4.1.1, temos

$$dim\langle\gamma\rangle = \frac{s-1}{s}|\mathrm{P}|,$$

onde $s = q_n$. Logo

$$dim\langle\gamma\rangle = \frac{q_n - 1}{q_n} q_1 \ldots q_{n-1} q_n = (q_n - 1)q_1 \ldots q_{n-1}.$$

□

**Lema 4.1.2** *Se* $\gamma \in \mathrm{J}^2$, *então* $Ann\gamma^{s-1} \neq < \gamma >$ .

Demonstração: Seja $\gamma \in \mathrm{J}^2$. Se $p = 2$, então $\gamma^{\frac{q_n}{2}} = \gamma^{2^{r_n-1}} \in \mathrm{J}^{q_n} = \Delta(\mathrm{P})^{q_n} = 0$. Logo $\gamma$ não tem índice de nilpotência máximo.

Se $p$ é primo ímpar, então $\gamma^{\frac{q_n+1}{2}} \in \mathrm{J}^{q_n+1} = 0$ e, novamente, o índice de nilpotência não é máximo. Logo, pela Proposição 4.1.1, segue que $Ann\gamma^{s-1} \neq \langle\gamma\rangle$. □

**Teorema 4.1.1** *Seja* $\langle\gamma\rangle$ *um ideal nilpotente de dimensão máxima em* KP. *Então:*

(i) $\gamma \in \mathrm{J} - \mathrm{J}^2$;

(ii) $\gamma$ *contém um termo linear em* $a_j$, *para algum* $j$, *e os ideais nestas condições são todos isomorfos.*

Demonstração: (i) Se $\langle\gamma\rangle$ é um ideal nilpotente de dimensão máxima, então pelo Lema 4.1.1, $dim\langle\gamma\rangle = (q_n - 1)q_1 \dots q_{n-1}$. Pela Proposição 4.1.1, temos $Ann\gamma^{s-1} = \langle\gamma\rangle$. Portanto, pelo Lema 4.1.2, $\gamma \in \mathrm{J} - \mathrm{J}^2$.

(ii) Vamos verificar que os ideais de dimensão máxima em KP são todos isomorfos a $\langle a_n\rangle$. Seja $\gamma \in \mathrm{J} - \mathrm{J}^2$ um gerador de um ideal nilpotente de dimensão máxima, isto é, $dim\langle\gamma\rangle = (q_n - 1)q_1 \dots q_{n-1}$.

Sabemos que $\Delta(\mathrm{P})$ tem como base $\left\{ a_1^{j_1} \dots a_n^{j_n} - 1 \mid 0 \leq j_i \leq q_i - 1,\ 1 \leq i \leq n,\ \sum_{i=1}^{n} \geq 1 \right\}$. Como $a_1^{j_1} \dots a_n^{j_n} - 1 = (a_1^{j_1} - 1)(a_2^{j_2} \dots a_n^{j_n} - 1) + (a_1^{j_1} - 1) + (a_2^{j_2} \dots a_n^{j_n} - 1)$, então, por indução sobre n, $\left\{ \prod_{i=1}^{n}(a_i^{j_i} - 1) \mid 0 \leq j_i \leq q_i - 1,\ \sum_{i=1}^{n} j_i \geq 1 \right\}$ também é uma base de $\Delta(\mathrm{P})$. Se $\gamma$ tiver um termo da forma $a_i^k - 1 = (a_i - 1)(a_i^{k-1} - 1) + (a_i - 1) + (a_i^{k-1} - 1)$, podemos escrever $a_i^k - 1 = \alpha(a_i - 1) + r$, onde $r \in \Delta(\mathrm{P})^2 = \mathrm{J}^2$ e $\alpha \in \mathrm{K}$. Logo podemos supor $\gamma = \sum_{i=1}^{n} \alpha_i(a_i - 1) + \gamma'$, com $\gamma' \in \mathrm{J}^2$ e $\alpha_i \in \mathrm{K}$, para $1 \leq i \leq n$. Sejam $l$ o maior índice tal que $\alpha_l \neq 0$ e $q_l$ o índice de nilpotência de $a_l - 1$. Logo $(a_i - 1)^{q_l} = 0$, para $i \leq l$. Assim, $\gamma^{q_l} = \gamma'^{q_l}$. Se $q_l < q_n$, então temos $\gamma^{q_l} \neq 0$ e $\langle\gamma'^{q_n - q_l}\rangle = \langle\gamma^{q_n - q_l}\rangle = Ann\gamma^{q_l} = Ann\gamma'^{q_l}$, contradizendo o fato de $\gamma'$ pertencer a $\mathrm{J}^2$. Assim suponha $\gamma = \alpha(a_k - 1) + \gamma'$, com $\gamma' \in \mathrm{J}^2$ e $\alpha \in \mathrm{K}^*$. Precisamos ter $(a_k - 1)^{q_n - 1} \neq 0$, pois, caso contrário, teremos $\gamma^{q_n - 1} = \gamma'^{q_n - 1}$.

Considere $\varphi$ o automorfismo de KP dado por $\varphi(a_k) = \alpha(a_k - 1) + \gamma' = \gamma$ e $\varphi(a_i) = a_i$, para $i \neq k$. Então $\varphi(\langle a_k\rangle) = \langle\gamma\rangle$, donde segue que $\langle a_k\rangle \cong \langle\gamma\rangle$. □

## 4.2 Levantamento de idempotentes

Seja F um corpo de característica prima $p$. Em [11] A. Poli considera ideais de álgebras do tipo $\mathrm{A} = \dfrac{\mathrm{F}[x_1, \dots, x_n]}{(t_1(x_1), \dots, t_n(x_n))}$ que incluem as álgebras de grupo comutativas e mostra como efetuar o levantamento de idempotentes módulo um ideal nilpotente.

Mostraremos aqui que, no caso de grupos abelianos finitos G tais que $car(\mathrm{F}) \nmid |\mathrm{G}|$, este

levantamento, módulo o radical, pode ser feito de forma muito natural.

Sejam $p$ um número primo e G um grupo abeliano finito tal que $p \mid |G|$. Podemos considerar $G = P \times H$, onde P é o $p$ - subgrupo de Sylow de G e $p \nmid |H|$. Se projetamos FG módulo o seu radical, que na verdade coincide com o ideal de aumento $\Delta(G,P)$, teremos $\frac{FG}{\Delta(G,P)} \cong FH$ que é semisimples. Note que ao projetarmos a álgebra de grupo módulo o seu radical, restam apenas como ideais minimais de FG os que são gerados por idempotentes primitivos, pois sendo FH semisimples, este não possui ideais nilpotentes não nulos. Portanto, se determinamos os idempotentes de FH, então, segue da Proposição 1.2.1, que estes idempotentes são os idempotentes primitivos de FG, via levantamento. Além disso, neste caso também conhecemos, da seção anterior, os ideais principais nilpotentes de dimensão máxima.

Sejam $e_1, e_2, \ldots, e_n$ os idempotentes primitivos de FH. Temos a seguinte projeção

$$FG = F(P \times H) \longrightarrow F\left(\frac{G}{P}\right) \cong FH.$$

Os idempotentes $e_i$ de FH estão em FG (identificados), e pela Proposição 1.2.1, eles são os levantamentos de $e_i$.

### 4.2.1 Alguns Exemplos

**(1)** Seja H é um $p_1$ - grupo abeliano de expoente $p_1^n$, onde $p_1$ é primo ímpar e $o(q) = \Phi(p_1^n)$ em $U(\mathbb{Z}_{p_1^n})$.

Os idempotentes de FH foram determinados em [6].

Se $H = \langle a \rangle$ é um grupo de ordem $p_1^n$, então pelo Teorema 3.1 [6], os idempotentes primitivos de FH são $e_0 = \widehat{H}, e_i = \widehat{H_i} - \widehat{H_{i-1}}$, com $1 \leq i \leq n$ e $H_i = \langle a^{p_1^i} \rangle$.

Portanto, para qualquer $p$ - grupo abeliano P, os idempotentes de FG, quando $G = P \times H$, são os mesmos de FH.

Se H não é cíclico, então pelo Teorema 4.1 [6], os idempotentes primitivos de FH são $e_H = \widehat{H}, e_N = \widehat{N} - \widehat{N^*}$, para cada N subgrupo de H tal que $\frac{H}{N} \neq \{1\}$ é cíclico de ordem potência de $p_1$, sendo $N^*$ o único subgrupo de H contendo N tal que $\left|\frac{N^*}{N}\right| = p_1$.

Portanto, para qualquer $p$ - grupo abeliano P, os idempotentes de FG, quando G = P × H, são os mesmos de FH.

**(2)** Se H é um grupo abeliano de expoente $2p_1^n$, com a condição que $o(q) = \Phi(p_1^n)$ em $U(\mathbb{Z}_{p_1^n})$, podemos escrever H = E × B, onde E é um 2 - grupo abeliano elementar e B é um $p_1$ - grupo. Então segue do Teorema 4.2 [6], que os idempotentes primitivos de FH são da forma $ef$, onde $f$ são os idempotentes citados acima e os idempotentes $e$ são da forma $e = e_1 \dots e_r$, onde $e_i = \dfrac{1 \pm a_i}{2}$, sendo que $E = \langle a_1 \rangle \times \cdots \times \langle a_r \rangle$ é um produto de grupos cíclicos de ordem 2.

Portanto, para qualquer $p$ - grupo abeliano P, os idempotentes de FG, quando G = P × H, são os mesmos de FH.

**(3)** Se H = $C_{2^m}$ e $q \equiv 3 \ (mod\ 8)$, $q \equiv 5 \ (mod\ 8)$ ou $q \equiv 9 \ (mod\ 16)$, sabemos que os idempotentes primitivos de FH são, pelo Capítulo 3, em cada caso, respectivamente:

$$\epsilon_0 = \frac{1 + a + a^2 + \cdots + a^{2^m-1}}{2^m},$$

$$\epsilon_1 = \frac{1 - a + a^2 - \cdots - a^{2^m-1}}{2^m},$$

$$\epsilon_2 = \frac{1 - a^2 + a^4 - \cdots - a^{2^m-2}}{2^{m-1}};$$

$$\epsilon_3 = (1 - a^4)\frac{(1 + a^{2^3} + \cdots + a^{2^m-2^3})(2 + \alpha a + \alpha a^3)}{2^m},$$

$$\epsilon_3' = (1 - a^4)\frac{(1 + a^{2^3} + \cdots + a^{2^m-2^3})(2 - \alpha a - \alpha a^3)}{2^m};$$

$$\epsilon_4 = (1 - a^8)\frac{(1 + a^{2^4} + \cdots + a^{2^m-2^4})(2 + \alpha a^2 + \alpha a^{3.2})}{2^{m-1}},$$

$$\epsilon_4' = (1 - a^8)\frac{(1 + a^{2^4} + \cdots + a^{2^m-2^4})(2 - \alpha a^2 - \alpha a^{3.2})}{2^{m-1}},$$

$$\cdots;$$

$$\epsilon_{m-1} = (1 - a^{2^{m-2}})\frac{(1 + a^{2^{m-1}})(2 + \alpha a^{2^{m-4}} + \alpha a^{3.2^{m-4}})}{2^4},$$

$$\epsilon_{m-1}' = (1 - a^{2^{m-2}})\frac{(1 + a^{2^{m-1}})(2 - \alpha a^{2^{m-4}} - \alpha a^{3.2^{m-4}})}{2^4},$$

$$\epsilon_m = (1 - a^{2^{m-1}})\frac{(2 + \alpha a^{2^{m-3}} + \alpha a^{3.2^{m-3}})}{2^3},$$

$$\epsilon'_m = (1 - a^{2^{m-1}})\frac{(2 - \alpha a^{2^{m-3}} - \alpha a^{3.2^{m-3}})}{2^3},$$

onde $\alpha$ é um elemento tal que $\alpha^2 = -2$;

$$\epsilon_0 = \frac{1 + a + a^2 + \cdots + a^{2^m-1}}{2^m},$$

$$\epsilon_1 = \frac{1 - a + a^2 - \cdots - a^{2^m-1}}{2^m},$$

$$\epsilon_2 = (1 - a^2)\frac{(1 + a^4 + a^8 + \cdots + a^{2^m-2^2})(1 + \alpha a)}{2^m},$$

$$\epsilon'_2 = (1 - a^2)\frac{(1 + a^4 + a^8 + \cdots + a^{2^m-2^2})(1 - \alpha a)}{2^m},$$

$$\epsilon_3 = (1 - a^4)\frac{(1 + a^8 + a^{16} + \cdots + a^{2^m-2^3})(1 + \alpha a^2)}{2^{m-1}},$$

$$\epsilon'_3 = (1 - a^4)\frac{(1 + a^8 + a^{16} + \cdots + a^{2^m-2^3})(1 - \alpha a^2)}{2^{m-1}},$$

$$\cdots;$$

$$\epsilon_{m-1} = (1 - a^{2^{m-2}})\frac{(1 + a^{2^m-2^{m-1}})(1 + \alpha a^{2^{m-3}})}{2^3},$$

$$\epsilon'_{m-1} = (1 - a^{2^{m-2}})\frac{(1 + a^{2^m-2^{m-1}})(1 - \alpha a^{2^{m-3}})}{2^3},$$

$$\epsilon_m = (1 - a^{2^{m-1}})\frac{(1 + \alpha a^{2^{m-2}})}{2^2},$$

$$\epsilon'_m = (1 - a^{2^{m-1}})\frac{(1 - \alpha a^{2^{m-2}})}{2^2},$$

onde $\alpha$ é um elemento tal que $\alpha^2 = -1$;

$$\epsilon_0 = \frac{1 + a + a^2 + \cdots + a^{2^m-1}}{2^m},$$

$$\epsilon'_0 = \frac{1 - a + a^2 - \cdots - a^{2^m-1}}{2^m},$$

$$\epsilon_{2^{m-2}} = \frac{1}{2^m}\left(1 + a^{2^{m-1}}\right)\left(1 - a^2 + a^4 - \cdots - a^{2^{m-1}-2}\right)\left(1 + \beta^2 a\right),$$

$$\epsilon_{3.2^{m-2}} = \frac{1}{2^m}\left(1 + a^{2^{m-1}}\right)\left(1 - a^2 + a^4 - \cdots - a^{2^{m-1}-2}\right)\left(1 - \beta^2 a\right),$$

$$\epsilon_{11} = \frac{1}{8}\left(1 - a^{2^{m-1}}\right)\left(1 + \beta a^{2^{m-3}} + \beta^2 a^{2^{m-2}} + \beta^3 a^{3.2^{m-3}}\right),$$

$$\epsilon_{12} = \frac{1}{8}\left(1 - a^{2^{m-1}}\right)\left(1 + \beta^3 a^{2^{m-3}} - \beta^2 a^{2^{m-2}} + \beta a^{3.2^{m-3}}\right),$$

$$\epsilon_{13} = \frac{1}{8}\left(1 - a^{2^{m-1}}\right)\left(1 - \beta a^{2^{m-3}} + \beta^2 a^{2^{m-2}} - \beta^3 a^{3.2^{m-3}}\right),$$

$$\epsilon_{14} = \frac{1}{8}\left(1 - a^{2^{m-1}}\right)\left(1 - \beta^3 a^{2^{m-3}} - \beta^2 a^{2^{m-2}} - \beta a^{3.2^{m-3}}\right),$$

$$\epsilon_{j1} = \frac{1}{2^{m-(j-2)}}\left(1 - a^{2^j} + a^{2^{j+1}} - a^{3.2^j} + \cdots - a^{2^m - 2^j}\right)\left(1 + \beta a^{2^{j-2}} + \beta^2 a^{2^{j-1}} + \beta^3 a^{3.2^{j-2}}\right),$$

$$\epsilon_{j2} = \frac{1}{2^{m-(j-2)}}\left(1 - a^{2^j} + a^{2^{j+1}} - a^{3.2^j} + \cdots - a^{2^m - 2^j}\right)\left(1 + \beta^3 a^{2^{j-2}} - \beta^2 a^{2^{j-1}} + \beta a^{3.2^{j-2}}\right),$$

$$\epsilon_{j3} = \frac{1}{2^{m-(j-2)}}\left(1 - a^{2^j} + a^{2^{j+1}} - a^{3.2^j} + \cdots - a^{2^m - 2^j}\right)\left(1 - \beta a^{2^{j-2}} + \beta^2 a^{2^{j-1}} - \beta^3 a^{3.2^{j-2}}\right),$$

$$\epsilon_{j4} = \frac{1}{2^{m-(j-2)}}\left(1 - a^{2^j} + a^{2^{j+1}} - a^{3.2^j} + \cdots - a^{2^m - 2^j}\right)\left(1 - \beta^3 a^{2^{j-2}} - \beta^2 a^{2^{j-1}} - \beta a^{3.2^{j-2}}\right),$$

para $2 \leq j \leq m-2$, onde $\beta$ é uma raiz oitava da unidade em F.

(4) Se H $= C_{2^m}$ e $q \equiv 3\ (mod\ 8)$, $q \equiv 5\ (mod\ 8)$ ou $q \equiv 9\ (mod\ 16)$, tal como no caso do exemplo anterior, podemos determinar os idempotentes primitivos de FG, quando G $=$ P $\times C_{2^m}$, para todo $p$ - grupo abeliano P.

# Referências Bibliográficas


[1] S.K. Arora and M. Pruthi, *Minimal cyclic codes of length* $2p^n$ , Finite Field and Appl., 5 (1999), 177-187.

[2] C. Curtis e I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, John Wiley, New York, 1962.

[3] Y. A. Drodz e V. V. Kirichenko, *Finite Dimensional Algebras*, Springer-Verlag, Berlin, 1991.

[4] F. S. Dutra, *Sobre Códigos diedrais e quatérnios*, tese de doutorado, Instituto de Ciências Exatas, UFMG, Belo Horizonte, 2006.

[5] F. S. Dutra, R. A. Ferraz and C. Polcino Milies, *Semisimple Group Codes and Dihedral Codes*, Algebra and Discrete Mathematics,a aparecer.

[6] R. Ferraz e C. P. Milies, *Idempotents in Group Algebras and Minimal Abelian Codes*, Finite Fields and Appl.,**13** (2007), 382-393.

[7] R. Ferraz, E. G. Goodaire and C. P. Milies, *Some classes of semisimple group (and loop) algebras over finite fields*, preprint.

[8] K. Ireland and M. Rosen, *A Classical Introduction to Number Theory*, Graduate Texts in Mathematics, Vol. 84, Springer-Verlag, New York, 1982.

[9] M. I. Isaacs, *Character Theory of Finite Groups*, Academic Press, New York, 1976.

[10] C. P. Milies e S. K. Sehgal, *An Introduction to Group Rings*, Kluwer Academic P., Dordrecht, 2002.

[11] A. Poli, *Construction of Primitive Idempotents for n Variable Codes*, Lecture Notes in Computer Science, **228** (1986), 25-35.

[12] A. Poli, *Ideaux Principaux Nilpotents de Dimension Maximale dans l'Algebre* $F_q[X]$

*d'un Groupe Abelien Fini* G, Commun. Algebra, **12** (1984), 391-401.

[13] M. Pruthi, *Cyclic Codes of Length* $2^m$, Proc. Indian Acad. Sci.(Math. Sci.), **111** (2001), 371-379.

[14] M. Pruthi and S.K. Arora, *Minimal codes of prime power length*, Finite Field and Appl., **3** (1997), 93-113.

[15] J. P. O. Santos, *Introdução à Teoria dos Números*, Associação Instituto Nacional de Matemática Pura e Aplicada, Rio de Janeiro, 2003.