Códigos metacíclicos

Samir Assuena

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

Durante o desenvolvimento deste trabalho o autor recebeu auxílio financeiro do CNPq

São Paulo, outubro de 2013

Códigos metacíclicos

Este exemplar corresponde à redação
final da tese devidamente corrigida
e defendida por Samir Assuena
e aprovada pela Comissão Julgadora.

Banca Examinadora:

- Prof. Dr. Francisco César Polcino Milies (orientador) IME-USP
- Prof. Dr. Raul Antonio Ferraz IME-USP
- Prof^a. Dr^a. Ana Cristina Vieira UFMG
- Prof. Dr. Thierry Petit Lobão UFBA
- Prof. Dr. Antonio Paques UFRGS

Agradecimentos

Agradeço a Deus por ter me dado força para vencer mais este desafio da minha vida mas também por ter me dado os maiores presentes da minha vida meus filhos Mateus e Larissa.

Agradeço minha esposa Elis por todo amor, carinho, compreensão e apoio ao longo de todos esses anos.

Agradeço aos meus pais, João Alberto e Virgínia, por tudo que fizeram por mim e pelos meus irmãos.

Agradeço aos meus irmãos, Jorge e Vinícius e suas respectivas esposas, pela confiança e apoio.

Agradeço a toda minha família tios, tias, primos e primas.

Agradeço ao meu sogro, Eliseu, à minha sogra, Dona Telma.

Agradeço aos meus cunhados Edilson e Edmilson e suas esposas Monise e Fabiana.

Agradeço a UFSCar pela minha formação, ao Prof. Daniel Vendrscolo e aos amigos das turmas de 2000 e 2001.

Agradeço ao Instituto de Matemática e Estatística da USP, principalmente ao Prof. César Polcino Milies pela orientação e pela pessoa extraordinária que é.

Agradeço ao Instituto Mauá de Tecnologia e aos professores Thiago, Anderson, Samira, Marilda, Marim, Ivanildo, Jones, Muller, Paulo, Ana, Airton e Ivete.

Agradeço aos eternos amigos: Betão, Zuaneti, Bigode, Lê, Tica, Ricardo, Felippe e suas respectivas esposas e ainda a todos os outros amigos da CEC.!!!!

Resumo

Neste trabalho, consideramos álgebras de grupo semi-simples $\mathbb{F}_q G$ de grupos metacíclicos não abelianos que cindem sobre corpos finitos. Inicialmente, damos condições para que o número de componentes simples da álgebra $\mathbb{F}_q G$ seja minimal e encontramos os idempotentes centrais primitivos quando a ordem do grupo é igual a $p^m \ell^n$, onde p e ℓ são números primos distintos. Posteriomente, obtemos condições necessárias e suficientes para que o número de componentes simples da álgebra $\mathbb{F}_q G$ seja minimal no caso em que a ordem do grupo é igual a $2n$. Finalmente, quando $G = D_{p^m}$, o grupo diedral de ordem $2p^m$, obtemos duas decomposições da álgebra $\mathbb{F}_q D_{p^m}$ como soma direta de ideais à esquerda minimais, calculamos suas dimensões e pesos e mostramos que, em uma destas decomposições, os códigos à esquerda minimais não são equivalentes a códigos abelianos, dando uma resposta afirmativa para uma conjectura formulada por Sabin e Lomonaco em 1995.

Palavras-chave: Códigos Metacíclicos, Idempotentes Primitivos, Grupos Metacíclicos não Abelianos.

Abstract

We consider semisimple group algebras $\mathbb{F}_q G$ of non abelian split metacyclic groups over a finite field. First we give necessary and suficiente conditions for them to have a minimal number of simple components and find the primitive central idempotents of $\mathbb{F}_q G$ in the case when the order G is equals $p^m \ell^n$, where p and ℓ are different prime numbers. Then, we consider the special case when the order of G is $2n$. Finally, when $G = D_{p^m}$ the dihedral group of order $2p^m$, we obtain two decomposition of the algebra into direct sum of minimal left ideals, compute their dimensions and weights. We show that one of these decompositions gives raise to minimal codes that are not combinatorially equivalent to abelian codes giving an affirmative answer to a conjecture formulated by Sabin and Lomonaco in 1995.

Keywords: Metacyclic Codes, Primitive Idempotens, Non Abelian Metacyclic Groups.

Sumário

Introdução

A Teoria dos Códigos Corretores de Erros teve início com o trabalho de Richard Hamming intitulado *Error Detecting and Error Correcting Codes*. Desde então, esta teoria vem sendo aplicada em várias áreas de outras ciências (tais como Engenharia Elétrica, Computação, etc), em telefonia, em DVD, entre outras.

Basicamente, o objetivo da Teoria de Códigos Corretores de Erros é transmitir mensagens através de um canal de uma maneira segura, de tal forma que o código seja capaz de detectar e corrigir o maior número possível de erros que possam ocorrer durante tal transmissão.

Para tanto, tomamos um conjunto finito $\mathcal{A}$ com q elementos o qual chamamos de **alfabeto**. Uma palavra de comprimento n em $\mathcal{A}$ é uma n-upla $(v_0, v_1, \cdots, v_{n-1})$. Um **código de comprimento n** sobre $\mathcal{A}$ é um subconjunto próprio $\mathcal{C}$ do produto cartesiano $\mathcal{A}^n$, para algum $n \geq 1$.

Dados $x = (x_0, x_1, \cdots, x_{n-1})$ e $y = (y_0, y_1, \cdots, y_{n-1})$ duas palavras de $\mathcal{A}^n$, definimos a *distância de Hamming* entre x e y como

$$d(x, y) = |\{i,\ x_i \neq y_i,\ 0 \leq i \leq n-1\}|.$$

Sendo assim, definimos a distância mínima de um código $\mathcal{C}$ como

$$d(\mathcal{C}) = min\ \{d(x, y) \mid x, y \in \mathcal{C},\ x \neq y\}.$$

Se tomarmos $\mathcal{A}$ como sendo $\mathbb{F}_q$, o corpo finito com q elementos, então $\mathbb{F}_q^n$ é um $\mathbb{F}_q$-espaço vetorial. Os $\mathbb{F}_q$-subespaços de $\mathbb{F}_q^n$ são chamados *códigos lineares*. Dentre os códigos lineares, existe uma classe muito importante de códigos chamados *códigos cíclicos*. Mais explicitamente, um código linear diz-se *cíclico* se

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

Sejam $C_n = \langle g,\ g^n = 1 \rangle$ o grupo cíclico de ordem n e $\mathbb{F}_q C_n$ a álgebra do grupo C_n sobre $\mathbb{F}_q$. Prova-se que a imagem de um código cíclico através da função

$$\psi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q C_n$$

$$(x_0, \cdots, x_{n-1}) \longmapsto \textstyle\sum_{i=0}^{n-1} x_i g^i$$

é um ideal de $\mathbb{F}_q C_n$. Sendo assim, define-se um *código de grupo* como um ideal da álgebra $\mathbb{F}_q G$ com G um grupo finito.

Um grupo G diz-se **metacíclico** se G contém um subgrupo normal H cíclico tal que o grupo G/H também é cíclico. Pode-se provar que G, sendo metacíclico finito, possui a seguinte apresentação

$$G = \langle a, b \mid a^m = 1, b^n = a^s, bab^{-1} = a^i \rangle$$

onde a e b são tais que $H = \langle a \rangle$ e $G/H = \langle bH \rangle$. Quando $s = m$, dizemos que G é um grupo *metacíclico que cinde* e, neste caso, G é o produto semi-direto $G = \langle a \rangle \rtimes \langle b \rangle$.

O estudo dos códigos metacíclicos desenvolveu-se através dos seguintes trabalhos

- R. E. Sabin, *On Row-Cyclic Codes with Algebraic Structure* , Designs, Codes and Cryptography, 4, 145-155 (1994)
- R. E. Sabin, S. J. Lomonaco, *Metacyclic Error-Correcting Codes*, AAECC 6 (1995) 191-210.
- F. S. Dutra, R. A. Ferraz, C. Polcino Milies, *Semisimple group codes and dihedral codes*, Algebra and Disc. Math., 3 (2009) 28-4.

No artigo *Metacyclic Error-Correcting Codes*, Sabin e Lomonaco introduziram a noção de *equivalência combinatorial* que é uma bijeção entre álgebras de grupos obtida pela extensão linear de uma bijeção entre dois grupos finitos de mesma ordem. Mais detalhadamente, sejam G e $\mathcal{G}$ dois grupos finitos de mesma ordem e $\mathbb{F}$ um corpo, sejam $\mathbb{F}G$ e $\mathbb{F}\mathcal{G}$ suas correspondentes álgebras de grupo, uma **equivalência combinatorial** é um isomorfismo de espaços vetoriais $\phi : \mathbb{F}G \longrightarrow \mathbb{F}\mathcal{G}$ induzido por uma bijeção $\phi : G \longrightarrow \mathcal{G}$. Os códigos $\mathcal{C} \subset \mathbb{F}G$ e $\widehat{\mathcal{C}} \subset \mathbb{F}\mathcal{G}$ são **combinatorialmente equivalentes** se existe uma equivalência combinatorial $\phi : \mathbb{F}G \longrightarrow \mathbb{F}\mathcal{G}$ tal que $\phi(\mathcal{C}) = \widehat{\mathcal{C}}$.

No caso em que G é um grupo metacíclico, tal que $mdc(q, |G|) = 1$, a álgebra de grupo $\mathbb{F}_qG$ é semissimples, Sabin e Lomonaco, usando Teoria de Representações de Grupos, mostraram que códigos em $\mathbb{F}_qG$, gerados por idempotentes centrais são combinatorialmente equivalentes a códigos abelianos. Isso motivou a procura de códigos minimais à esquerda da álgebra $\mathbb{F}_qG$.

No capítulo 1, apresentamos as noções preliminares que serão utilizadas ao longo deste trabalho.

No capítulo 2, consideramos álgebras de grupos metacíclicos **não abelianos** que cindem sobre corpos finitos e encontramos uma condição necessária para que a álgebra $\mathbb{F}_qG$ tenha número mínimo de componentes simples. Isto acontece quando as álgebras $\mathbb{F}_qG$ e $\mathbb{Q}G$ têm o mesmo número de componentes simples. Finalizamos este capítulo obtendo os idempotentes centrais primitivos da álgebra $\mathbb{F}_qG$, no caso em que $|G| = p^m\ell^n$, sendo p e ℓ números primos.

No capítulo 3, apresentamos uma extensão do [4, Teorema 3.3] feito para grupos diedrais.

No capítulo 4, conhecendo os idempotentes centrais primitivos da álgebra $\mathbb{F}_qD_{p^m}$, onde D_{p^m} é o grupo diedral de ordem p^m, obtivemos duas decomposições da álgebra $\mathbb{F}_qD_{p^m}$ como soma direta de ideais à esquerda minimais, sendo que, em uma destas decomposições, tais ideais minimais são combinatorialmente equivalentes a códigos abelianos mas na outra decomposições, tais ideais minimais **não** são combinatorialmente equivalentes a códigos abelianos.

Capítulo 1

Preliminares

1.1 Grupos Metacíclicos

Definição 1.1.1. *Um grupo G diz-se* ***metacíclico*** *se G contém um subgrupo normal H cíclico tal que o grupo G/H também é cíclico.*

Exemplos de grupos metacíclicos são os grupo diedrais e os grupos cujos subgrupos de Sylow são cíclicos ([18, Teorema 10.1.10]).

Seja G um grupo metacíclico finito, escrevendo $H = \langle a \rangle$, seu subgrupo normal de ordem m, e $G/H = \langle bH \rangle$, podemos provar que G possui a seguinte apresentação

$$G = \langle a, b \mid a^m = 1, b^n = a^s, bab^{-1} = a^i \rangle$$

onde n é $|G/H|$. Além disto, os inteiros n, m, s, i se relacionam da seguinte maneira

$$s \mid m, \quad m \mid s(i-1) \quad , \quad i < m, \quad \text{mdc}(i, m) = 1.$$

Quando $s = m$, dizemos que G é um grupo *metacíclico que cinde* e, neste caso, G é o produto semi-direto $G = \langle a \rangle \rtimes \langle b \rangle$.

Teorema 1.1.2. [2, Teorema 47.10] *Seja G um grupo metacíclico com apresentação acima. Seu subgrupo comutador G' é cíclico, gerado por a^{i-1}. Consequentemente, $|G'| = m/mdc(m, i-1)$.*

Teorema 1.1.3. [10, Lema 2.1] *Se $G = \langle a \rangle \rtimes \langle b \rangle$ com $o(a) = m$ e $o(b) = n$, então o expoente de G é:*

$$exp(G) = mmc(m, n).$$

1.2 Anéis de Grupos

Sejam R um anel com unidade e G um grupo. Denotamos por RG o conjunto de todas as combinações lineares formais

$$\alpha = \sum_{g \in G} a_g g$$

onde $a_g \in R$ e somente um número finito de coeficientes a_g é diferente de zero. Neste sentido, todas as somas podem ser consideradas finitas, mesmo quando os índices do somatório percorrem um conjunto infinito.

Definição 1.2.1. *Seja $\alpha = \sum_{g \in G} a_g g$ um elemento de RG. Definimos o* **suporte** *de α como sendo o conjunto dos elementos $g \in G$ tal que $a_g \neq 0$ em $\alpha = \sum_{g \in G} a_g g$. Mais formalmente,*

$$supp(\alpha) = \{g \in G \mid a_g \neq 0\}. \tag{1.1}$$

Dois elementos $\alpha = \sum_{g \in G} a_g g$ e $\beta = \sum_{g \in G} b_g g$, pertencentes a RG, são iguais se e somente se $a_g = b_g$ para todo $g \in G$.

Dados dois elementos $\alpha = \sum_{g \in G} a_g g$ e $\beta = \sum_{g \in G} b_g g$, pertencentes a RG, definimos a soma e o produto de α e β da seguinte maneira:

$$\alpha + \beta = \left(\sum_{g \in G} a_g g\right) + \left(\sum_{g \in G} b_g g\right) = \sum_{g \in G} (a_g + b_g) g \tag{1.2}$$

$$\alpha\beta = \sum_{g,h\in G} (a_g b_h)(gh). \tag{1.3}$$

Verifica-se facilmente que o conjunto RG, munido das operações de soma e produto definidas em (1.2) e (1.3) é um anel com unidade. Além disso, podemos definir uma multiplicação de elementos de RG por elementos de R, de tal forma que RG seja um R-módulo e, se R for um anel comutativo, RG seja uma R-álgebra. Tal multiplicação é definida por

$$\lambda\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} (\lambda a_g) g. \tag{1.4}$$

Definição 1.2.2. *O conjunto RG, com as operações definidas acima, é chamado* **anel de grupo de** G **sobre** R. *Se R é comutativo, RG é também chamado de* **álgebra de grupo de** G **sobre** R.

Considere a função $i : G \to RG$ definida por $i(x) = \sum_{g\in G} a_g g$ onde $a_x = 1$ e $a_g = 0$ se $g \neq x$. Tal função é uma imersão de G em RG; portanto podemos considerar G como um subconjunto de RG e dizer que G é uma base de RG sobre R.

Por outro lado, a função $\nu : R \to RG$ dada por $\nu(r) = \sum_{g\in G} a_g g$ onde $a_{1_G} = r$ e $a_g = 0$ se $g \neq 1_G$ é um monomorfismo de anéis. Logo R pode ser considerado como um subanel de RG.

Definição 1.2.3. *Um anel R, com unidade, diz-se* ***semissimples****, se todo ideal à esquerda de R é um somando direto, isto é, para todo ideal à esquerda I de R, existe um ideal à esquerda J de R tal que $R = I \oplus J$.*

Teorema 1.2.4. *Seja R um anel com unidade. Então*

i) R é semissimples, se e somente se todo ideal à esquerda de R é gerado por um idempotente.

ii) Se R é semissimples, então R é uma soma direta finita de ideais minimais à esquerda.

Teorema 1.2.5. *Seja $R = \oplus_{i=1}^{t} L_i$ uma decomposição de um anel semissimples com unidade como soma direta da ideais minimais à esquerda. Então, existe uma família $\{e_1, \cdots, e_t\}$ de elementos de R tal que:*

i) $e_i \neq 0$ é um elemento idempotente, $1 \leq i \leq t$;

ii) Se $i \neq j$, então $e_i e_j = 0$;

iii) $1 = e_1 + \cdots + e_t$;

iv) e_i não pode ser escrito como soma de dois idempotentes não nulos cujo produto é zero, $1 \leq i \leq t$.

Reciprocamente, se existe uma família $\{e_1, \cdots, e_t\}$ de idempotentes de R satisfazendo as condições acima, então os ideais à esquerda $L_i = Re_i$ são minimais e $R = \oplus_{i=1}^{t} L_i$.

Definição 1.2.6. *Seja R um anel com unidade, uma família $\{e_1, \cdots, e_t\}$ de idempotentes de R satisfazendo as condições (i), (ii) e (iii) do Teorema acima é chamada* ***família completa de idempotentes ortogonais****. Um idempotente que satisfaz a condição (iv) chama-se* ***primitivo****.*

Proposição 1.2.7. *Seja R um anel com unidade semissimples. Então*

i) $R = \oplus_{i=1}^{s} A_i$, onde cada A_i é um ideal bilateral minimal;

ii) Todo ideal bilateral I de R pode ser escrito como $I = A_{i_1} \oplus \cdots \oplus A_{i_t}$, onde $1 \leq i_1 < \cdots < i_t \leq s$;

iii) Se $R = \oplus_{j=1}^{r} B_j$ é uma outra decomposição de R em soma direta de ideais bilaterais minimais, então $s = r$ e , após uma possível reordenação dos índices, $A_i = B_i$ para todo i.

Definição 1.2.8. *Os únicos ideais bilaterais minimais de um anel semissimples são chamados as* ***componentes simples*** *de R.*

Teorema 1.2.9. *Seja* $R = \oplus_{i=1}^{s} A_i$ *a decomposição de um anel com unidade semissimples, como soma direta de ideais bilaterais minimais. Então, existe uma família* $\{e_1, \cdots, e_t\}$ *de elementos de R tal que:*

i) $e_i \neq 0$ *é um idempotente central,* $1 \leq i \leq t$*;*

ii) Se $i \neq j$*, então* $e_i e_j = 0$*;*

iii) $1 = e_1 + \cdots + e_t$*;*

iv) e_i *não pode ser escrito como soma de dois idempotentes centrais não nulos cujo produto é zero,* $1 \leq i \leq t$*.*

Definição 1.2.10. *Os elementos* $\{e_1, \cdots, e_t\}$ *de R do Teorema acima são chamados de* ***idempotentes centrais primitivos*** *de R.*

Teorema 1.2.11 (**Wedderburn-Artin**)**.** *Um anel R com unidade é semissimples, se e somente se R é uma soma direta de anéis de matrizes sobre anéis com divisão:*

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

Em relação aos anéis de grupo, temos o seguinte

Teorema 1.2.12 (**Maschke**)**.** *Sejam G um grupo e R um anel com unidade. Então, o anel de grupo RG é semissimples, se e somente se valem as seguintes condições*

i) R é um anel semissimples;

ii) G é finito;

iii) $|G|$ *é invertível em R.*

Corolário 1.2.13. *Sejam G um grupo finito e K um corpo. Então, KG é semissimples, se e somente se* $\mathrm{car}(K) \nmid |G|$*.*

Vamos reunir alguns resultados sobre idempotentes centrais primitivos de algumas álgebras de grupo.

Definição 1.2.14. *Dado um anel de grupo RG e H um subgrupo finito do grupo G, tal que $|H|$ é invertível em R, denotaremos por $\widehat{H}$ o seguinte elemento de RG:*

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

Lema 1.2.15. [17, Lema 3.6.6] *Sejam R um anel com unidade e H um subgrupo de um grupo G. Se $|H|$ é invertível em R, então $\widehat{H}$ é um elemento idempotente de RG. Além disso, se $H \lhd G$, então $\widehat{H}$ é central.*

Lema 1.2.16. [8, Lema 7.1.2] *Sejam p um número primo e $A = \langle a \rangle$, um grupo cíclico de ordem p^m, $m \geqslant 1$. Seja*

$$A = A_0 \supseteq A_1 \supseteq \cdots \supseteq A_m = \{1\}$$

a cadeia descendente de todos os subgrupos de A, isto é, $A_i = \langle a^{p^i} \rangle$. Então, os idempotentes primitivos da álgebra de grupo $\mathbb{Q}A$ são:

$$e_0 = \widehat{A} \quad e \quad e_i = \widehat{A_i} - \widehat{A_{i-1}}, \ 1 \leq i \leq m.$$

Além disso, $(\mathbb{Q}A)e_i \cong \mathbb{Q}(\xi_{p^i})$, onde ξ_{p^i} denota uma raiz p^i-ésima primitiva da unidade.

Sejam G um grupo finito e $\mathbb{F}$ um corpo qualquer tal que $\mathrm{car}(\mathbb{F}) \nmid |G|$. Denote por e o expoente de G e considere ξ uma raiz e-ésima primitiva da unidade. Para cada $\theta \in \mathrm{Gal}(\mathbb{F}(\xi), \mathbb{F})$, temos que $\theta(\xi) = \xi^r$ para algum inteiro positivo r. Podemos então definir uma ação do grupo $\mathrm{Gal}(\mathbb{F}(\xi), \mathbb{F})$ em G, dada por $\theta(g) = g^r$.

Denotando por $\mathcal{C}(g)$ a classe de conjugação de g e $\Gamma_g = \sum_{x \in \mathcal{C}(g)} x$, então $\theta(\Gamma_g) = \Gamma_{\theta(g)}$. Duas classes de conjugação de G são $\mathbb{F}$-**conjugadas**, se elas se correspondem sob esta ação. Da mesma forma, dois elementos g_1 e g_2 de G são $\mathbb{F}$-**conjugados**, se existem $\theta \in \mathrm{Gal}(\mathbb{F}(\xi), \mathbb{F})$ e $h \in G$ tais que $g_1 = h(\theta(g_2))h^{-1}$.

Teorema 1.2.17 (Witt-Berman [2], Ferraz [5]). *Sejam G um grupo finito e $\mathbb{F}$ um corpo qualquer tal que* $\mathrm{car}(\mathbb{F}) \nmid |G|$. *Então o número de componentes simples da álgebra $\mathbb{F}G$ é igual ao número de classes de $\mathbb{F}$-conjugação.*

1.3 Códigos Corretores de Erros

Apresentaremos nesta seção os principais resultados da teoria de códigos corretores de erros que motivaram os nossos estudos neste trabalho.

Seja $\mathcal{A}$ um conjunto finito com q elementos que será chamado de **alfabeto** e cujos elementos chamaremos de **letras**. Uma sequência de n letras de $\mathcal{A}$ será chamada de **palavra de comprimento n**.

Consideremos, então, o conjunto

$$\mathcal{A}^n = \{(c_0, \cdots, c_{n-1}), \mid c_i \in \mathcal{A}\}$$

de todas as palavras de comprimento n sobre $\mathcal{A}$.

Definição 1.3.1. *Um **código de comprimento n** é um subconjunto não trivial de $\mathcal{A}^n$, para algum n.*

A Teoria dos Códigos Corretores de Erros tem como objetivo principal a transmissão de mensagens através de um canal, detectar e corrigir possíveis erros que venham a ocorrer nessa transmissão. Para tanto, precisamos formalizar alguns conceitos.

Definição 1.3.2. *Sejam $x = (x_0, \ldots, x_{n-1})$ e $y = (y_0, \ldots, y_{n-1})$ duas palavras de $\mathcal{A}^n$. Definimos a **distância de Hamming** entre x e y como sendo*

$$d(x, y) = |\{i \mid x_i \neq y_i, 0 \leq i \leq n-1\}|.$$

Em outras palavras, a distância de Hamming entre duas palavras de $\mathcal{A}^n$ é o número de coordenadas em que elas diferem.

*Sendo assim, dado um código $\mathcal{C} \subset \mathcal{A}^n$, definimos a **distância mínima de $\mathcal{C}$** como sendo*

$$d(\mathcal{C}) = min\{d(x,y) \mid x,y \in \mathcal{C},\ x \neq y\}.$$

A distância mínima de um código $\mathcal{C}$ é um parâmetro do código muito importante, pois, quanto maior ela for, mais erros o código será capaz de dectar e corrigir. Mais explicitamente, temos a seguinte:

Proposição 1.3.3. [14, Teorema 6.10] *Seja $\mathcal{C} \subset \mathcal{A}^n$ um código com distância mínima $d(\mathcal{C}) = d$. Então, $\mathcal{C}$ pode corrigir t erros se e somente se $d \geq 2t+1$ Em outras palavras, $\mathcal{C}$ pode corrigir até $\left\lfloor \frac{d-1}{2} \right\rfloor$ erros.*

Seja $\mathbb{F}_q$ um corpo finito com q elementos. Considerando $\mathbb{F}_q$ como o alfabeto e $\mathbb{F}_q^n$ o espaço de todas as palavras, um **código linear** é um subespaço vetorial de $\mathbb{F}_q^n$(e não apenas um subconjunto).

Dada $x = (x_0, \ldots, x_{n-1})$ uma palavra em $\mathbb{F}_q^n$, definimos o **peso** de x como sendo

$$w(x) = d(x,0) = |\{i \mid x_i \neq 0,\ 0 \leq i \leq n-1\}|.$$

Definição 1.3.4. *Dado um códogo linear $\mathcal{C}$ de $\mathbb{F}_q^n$, definimos o **peso** de $\mathcal{C}$ como sendo o número*

$$w(\mathcal{C}) = min\{w(c),\ c \in \mathcal{C},\ c \neq 0\}.$$

Com isso, temos a seguinte

Proposição 1.3.5. *Seja $\mathcal{C} \subset \mathbb{F}_q^n$ um código linear. Então*

i) Para cada $x, y \in \mathcal{C}$, temos que $d(x,y) = w(x-y)$,

ii) $d(\mathcal{C}) = w(\mathcal{C})$.

Uma família importante de códigos lineares são os chamados *códigos cíclicos*, que são os códigos $\mathcal{C} \subset \mathbb{F}_q$, tais que se $(x_0, \cdots, x_{n-1}) \in \mathcal{C}$ então $(x_{n-1}, \cdots, x_{n-2}) \in \mathcal{C}$.

Dado um grupo finito G de ordem n, a álgebra de grupo $\mathbb{F}_q G$ e $\mathbb{F}_q^n$ são isomorfos como $\mathbb{F}_q-$ espaços vetoriais.

Denotando por $C_n = \langle a \rangle$ o grupo cíclico de ordem n, temos

Teorema 1.3.6. *Um código $\mathcal{C} \subset \mathbb{F}_q^n$ sobre $\mathbb{F}_q$ é cíclico, se e somente se sua imagem pela aplicação*

$$\psi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q C_n$$

$$(x_0, \cdots, x_{n-1}) \longmapsto \sum_{i=0}^{n-1} x_i a^i$$

é um ideal de $\mathbb{F}_q C_n$.

Mais geralmente, um *código de grupo* é, por definição, um ideal da álgebra de grupo $\mathbb{F}_q G$ de um grupo finito. Dedicamos o resto deste trabalho ao estudo de **códigos metacíclicos**, isto é, códigos de grupos sobre grupos metacíclicos.

Capítulo 2

Álgebras de Grupos Metacíclicos sobre Corpos Finitos

2.1 Número de componentes simples

Ao longo desta seção, G indicará sempre um grupo metacíclico com a seguinte apresentação:

$$G = \langle a, b \mid a^m = 1 = b^n,\ \ bab^{-1} = a^i \rangle$$

e m e n denotarão sempre as ordens de a e b respectivamente. Ainda, $\mathbb{F}_q$ denotará um corpo finito com q elementos satisfazendo $mdc(q, |G|) = 1$.

Antes de iniciarmos nosso estudo sobre álgebra de grupo, vamos expor um resultado sobre grupos de Galois de corpos finitos.

Teorema 2.1.1. [11, Teorema 4.26] *Seja $\mathbb{F}_q$ um corpo finito com q elementos, $\mathbb{E}$ uma extensão de $\mathbb{F}_q$ com $[\mathbb{E} : \mathbb{F}_q] = n$. Então $\mathbb{E}$ é uma extensão cíclica sobre $\mathbb{F}_q$ com grupo de Galois $\langle \sigma \rangle$ onde σ é o $\mathbb{F}_q$-automorfismo de $\mathbb{E}$ definido por $\sigma(a) = a^q$, para todo $a \in \mathbb{E}$.*

Observação 2.1.2. Sabemos que dois elementos g_1 e g_2 de G são $\mathbb{F}_q$-conjugados em G, se existem $\theta \in \mathrm{Gal}(\mathbb{F}_q(\xi), \mathbb{F})$ e $h \in G$ tais que $g_1 = h(\theta(g_2))h^{-1}$. Em vista do Teorema 2.1.1, g_1 e g_2 são $\mathbb{F}_q$-conjugados em G, se e somente se existem $s \in \mathbb{Z}$ e $h \in G$, tais que $g_1 = hg_2^{q^s}h^{-1}$, uma vez que $\theta(\xi) = \sigma^s(\xi) = \xi^{q^s}$.

A seguir, vamos provar um Lema que será muito útil.

Lema 2.1.3. *Sejam H um grupo finito, x e y dois elementos de H. Seja $\mathbb{F}_q$ um corpo finito com q elementos tal que $mdc(q,|H|)=1$. Se x e y são $\mathbb{F}_q$-conjugados em H, então x e y são $\mathbb{Q}$-conjugados em H.*

Demonstração. Sejam e o expoente de H e ξ uma raiz e-ésima primitiva da unidade. Se x e y são $\mathbb{F}_q$-conjugados, existem $h \in H$ e $\varphi \in \mathrm{Gal}(\mathbb{F}_q(\xi), \mathbb{F}_q)$ tais que $y = h(\varphi(x))h^{-1}$. Pelo Teorema 2.1.1, existe $s \in \mathbb{Z}$, tal que $\varphi(\xi) = \xi^{q^s}$. Além disso, como $mdc(q, |H|) = 1$, então $mdc(q^s, e) = 1$. Podemos então definir $\varphi^* \in \mathrm{Gal}(\mathbb{Q}(\xi), \mathbb{Q})$ por $\varphi^*(\xi) = \xi^{q^s}$. Logo $y = h(\varphi^*(x))h^{-1}$ o que nos mostra que x e y são $\mathbb{Q}$-conjugados em H. ■

Corolário 2.1.4. *Seja H um grupo finito. Cada $\mathbb{Q}$-classe de H é uma união disjunta de $\mathbb{F}_q$-classes. Consequentemente se o número de $\mathbb{F}_q$-classes e de $\mathbb{Q}$-classes são iguais, então as $\mathbb{Q}$-classes e as $\mathbb{F}_q$-classes coincidem.*

Notemos que, pelo Lema 2.1.3, o número de componentes simples da álgebra $\mathbb{Q}G$ é menor ou igual ao número de componentes simples da álgebra $\mathbb{F}_qG$. Isto nos motiva a introduzir a seguinte

Definição 2.1.5. *Sejam G um grupo finito e $\mathbb{F}_q$ um corpo finito com q elementos, tais que $mdc(q, |G|) = 1$. Dizemos que o número de componentes simples da álgebra $\mathbb{F}_qG$ é minimal, se as álgebras $\mathbb{Q}G$ e $\mathbb{F}_qG$ têm o mesmo número de componentes simples.*

Ferraz e Simón-Pinero determinaram, em [7], o número de componentes simples da álgebra $\mathbb{Q}G$. Neste capítulo vamos determinar condições sobre os inteiros m e n para que a álgebra $\mathbb{F}_qG$ tenha um número mínimo de componentes simples.

Iniciaremos apresentando dois resultados cujas demonstrações podem ser encontradas em [7].

Lema 2.1.6. [7, Lema 2.4]

Sejam H um grupo finito , x e y elementos de H. Então x e y são $\mathbb{Q}$-conjugados em H, se e somente se existem $h \in H$ e $s \in \mathbb{Z}$, tais que $x^s = hyh^{-1}$ e os elementos x e y têm a mesma ordem.

Proposição 2.1.7. [7, Proposição 2.6] *Seja G um grupo metacíclico. Para cada inteiro k, existe um único divisor v de n, tal que os elementos b^k e b^v são $\mathbb{Q}$-conjugados em G. Esse divisor é $v = mdc(k, n)$.*

Consequentemente, tem-se também o seguinte:

Corolário 2.1.8. *Sejam H um grupo e k um inteiro satisfazendo $mdc(k, n) = 1$. Então os elementos b^k e b são $\mathbb{Q}$-conjugados em H.*

O Corolário 2.1.8 nos motiva a determinar condições sobre n para que, dado um inteiro k satisfazendo $mdc(k, n) = 1$, se tenha que b^k e b são $\mathbb{F}_q$-conjugados em G. Sendo assim, para corpos finitos, obtemos o seguinte resultado:

Lema 2.1.9. *Seja G um grupo metacíclico. Então os elementos b^k e b são $\mathbb{F}_q$-conjugados, para todo inteiro k com $mdc(k,n)=1$, se e somente se o grupo $\mathcal{U}(\mathbb{Z}_n)$ das unidades dos inteiros módulo n é cíclico, gerado por $\bar{q}$, a classe de q em $\mathbb{Z}_n$.*

Demonstração. Suponhamos que $\mathcal{U}(\mathbb{Z}_n) = \langle \bar{q} \rangle$. Então, para todo $\bar{k} \in \mathcal{U}(\mathbb{Z}_n)$, existe $s \in \mathbb{Z}$ tal que, $\bar{k} = \bar{q}^s$. Logo $b^k = b^{q^s}$, o que, pela Observação 2.1.2 nos mostra, que b^k e b são $\mathbb{F}_q$-conjugados.

Reciprocamente, se b^k e b são $\mathbb{F}_q$-conjugados, então $b^k = hb^{q^s}h^{-1}$ para algum $s \in \mathbb{Z}$ e algum $h \in G$. Escrevendo $h = a^t b^x$, então

$$b^k = a^t b^x b^{q^s} b^{-x} a^{-t} = a^t b^{q^s} a^{-t} = a^t a^{-i^{q^s}} b^{q^s}.$$

Este fato nos mostra que $b^{q^s}b^{-k} \in \langle a \rangle \cap \langle b \rangle$ consequentemente $b^{q^s} = b^k$ mostrando que $\bar{k} = \bar{q}^s$ em $\mathcal{U}(\mathbb{Z}_n)$. ■

Lema 2.1.10. *Sejam um inteiro k tal que mdc(k,n)=1 e n_1, um divisor positivo de n. Se b^k e b^{n_1} são $\mathbb{F}_q$-conjugados, então $n_1 = 1$. Analogamente, se $mdc(k, m) = 1$ e a^k e a^{m_1} são $\mathbb{F}_q$-conjugados com m_1 um divisor positivo de m, então $m_1 = 1$.*

Demonstração.

Se b^k e b^{n_1} são $\mathbb{F}_q$-conjugados, então existe $s \in \mathbb{Z}$ tal que

$$b^k = b^{q^s n_1}$$

assim $k = q^s n_1 + \alpha n = q^s n_1 + \alpha\beta n_1 = zn_1$. Logo $mdc(k, n) = mdc(zn_1, \beta n_1) = n_1 mdc(z, \beta) = 1$ mostrando que $n_1 = 1$. ■.

Proposição 2.1.11. *Sejam G um grupo metacíclico e $\mathbb{F}_q$ um corpo finito com q elementos, tal que mdc(q, |G|)=1. Se o número de componentes simples da álgebra $\mathbb{F}_qG$ é minimal, então o grupo $\mathcal{U}(\mathbb{Z}_n)$ é um grupo cíclico gerado por $\bar{q}$.*

Demonstração. Se o número de componentes simples da álgebra $\mathbb{F}_qG$ é minimal, pelo Corolário 2.1.4, dois elementos b^{k_1} e b^{k_2} são $\mathbb{Q}$-conjugados em G se e somente se b^{k_1} e b^{k_2} são $\mathbb{F}_q$-conjugados em G. Assim, pelo Corolário 2.1.7, para cada inteiro k existe um divisor v de n, tal que os elementos b^k e b^v são $\mathbb{Q}$-conjugados em G, e consequentemente b^k e b^v são $\mathbb{F}_q$-conjugados em G. Tomando um inteiro k tal que $mdc(k, n) = 1$, existe um divisor positivo m_1 de n tal que b^k e b^{m_1} são $\mathbb{F}_q$-conjugados. No entanto, pelo Lema 2.1.10, $m_1 = 1$, o que nos mostra que, para todo inteiro k satisfazendo $mdc(k, n) = 1$, tem-se que b^k e b são $\mathbb{F}_q$-conjugados em G. Assim, pelo Lema 2.1.9, $\mathcal{U}(\mathbb{Z}_n)$ é um grupo cíclico gerado por $\bar{q}$. ■

Sabendo que o número de componentes simples de $\mathbb{F}_qG$ é minimal, conseguimos determinar uma condição sobre n. Agora vamos tentar determinar condições sobre m. Para tanto, começamos com o seguinte:

Lema 2.1.12. *Seja $A = \langle a \rangle$. Dados dois elementos a^k e $a^j \in A$, então eles são $\mathbb{Q}$-conjugados em G se e somente se mdc(k,m)=mdc(j,m).*

Demonstração. Seja e o expoente de G. Por definição, a^k e a^j são $\mathbb{Q}$-conjugados em G se e somente se existem $h \in G$ e um inteiro r com $mdc(r, e) = 1$, tais que $a^j = ha^{kr}h^{-1}$. Pelo Teorema 1.1.3, $e = mmc(m, n)$ e então $mdc(r, m) = 1$. Seja $h = a^x b^y$. Temos

$$a^j = a^x b^y a^{kr} b^{-y} a^{-x} = a^{kri^y}.$$

Esta igualdade nos mostra que

$$j \equiv kri^y \ mod(m). \tag{2.1}$$

Sejam $d_k = mdc(k, m)$ e $d_j = mdc(j, m)$. Como d_j divide j e m então d_j divide kri^y. Sabemos que $i \in \mathcal{U}(\mathbb{Z}_m)$, da Definição 1.1.1. Ainda, como $mdc(r, m) = 1$ temos também que $r \in \mathcal{U}(\mathbb{Z}_m)$ donde $ri^y \in \mathcal{U}(\mathbb{Z}_m)$. Consequentemente, existem inteiros α e β tais que

$$1 = \alpha ri^y + \beta m \Rightarrow k = k\alpha ri^y + k\beta m.$$

Como $d_j \mid kri^y$ e $d_j \mid m$, podemos escrever $k = d_j k_1 + d_j k_2$, com $k_1, k_2 \in \mathbb{Z}$, que nos mostra que $d_j \mid d_k$. Reciprocamente, como $d_k \mid k$ e $d_k \mid m$, $d_k \mid kri^y$, segue de 2.1 que $d_k \mid j$, logo $d_k \mid d_j$, donde $d_j = d_k$.

Suponhamos que $mdc(k, m) = mdc(j, m)$. Então os ideais
$(d_k) = \{\alpha k + \beta m \mid \alpha, \beta \in \mathbb{Z}\}$ e $(d_j) = \{\alpha j + \beta m \mid \alpha, \beta \in \mathbb{Z}\}$ são iguais. Logo, existem $\alpha_0, \beta_0 \in \mathbb{Z}$ tais que $j = \alpha_0 k + \beta_0 m$. Com isso, $a^j = a^{\alpha_0 k}$ com o(a^j) =o(a^k) e o resultado segue do Lema 2.1.6. ■

Corolário 2.1.13. *Para cada $a^k \in G$, existe um único divisor v de m, tal que a^k e a^v são $\mathbb{Q}$-conjugados em G.*

Demonstração. Basta tomar $v = mdc(k, m)$ e aplicar o Lema 2.1.12.

Corolário 2.1.14. *Sejam a^{m_1} e a^{m_2} em G com $m_1, m_2 \in \mathbb{N}$ satisfazendo $m_1 \mid m$ e $m_2 \mid m$. Se a^{m_1} e a^{m_2} são $\mathbb{Q}$-conjugados em G, então $m_1 = m_2$.*

Dado um elemento a^j de G, como $b^x a^j b^{-x} = a^{ji^x}$ para todo $x \in \mathbb{Z}$, sua classe de conjugação é o conjunto

$$\Gamma_{a^j} = \{a^j, a^{ji}, a^{ji^2}, \cdots, a^{ji^{n-1}}\}.$$

Notemos, novamente que pelo Lema 2.1.6, para todo $k \in \mathbb{Z}$ com $mdc(k, m) = 1$, tem-se que a^k e a são $\mathbb{Q}$-conjugados. Sobre $\mathbb{F}_q$, temos o seguinte:

Lema 2.1.15. *Seja k um inteiro tal que mdc(k,m)=1. Então os elementos a e a^k são $\mathbb{F}_q$-conjugados em G se e somente se $\mathcal{U}(\mathbb{Z}_m) = \langle \bar{i} \rangle \langle \bar{q} \rangle$.*

Demonstração. Seja $k \in \mathbb{Z}$ tal que $mdc(k, m) = 1$. Suponhamos que a e a^k são $\mathbb{F}_q$-conjugados em G. Por definição, existem $h \in G$ e $s \in \mathbb{Z}$ satisfazendo $a^{kq^s} = hah^{-1}$, ou seja, o elemento a^{kq^s} pertence à classe de conjugação de a, o que implica que $a^{kq^s} = a^{i^t}$ para algum t, $0 \leq t \leq n-1$. Em outras palavras, $\bar{k}\bar{q}^s = \bar{i}^t$ em $\mathbb{Z}_m$ logo $\bar{k} = \bar{i}^t(\bar{q}^s)^{-1}$ o que mostra que $\mathcal{U}(\mathbb{Z}_m) = \langle \bar{i} \rangle \langle \bar{q} \rangle$.

Reciprocamente, se $\mathcal{U}(\mathbb{Z}_m) = \langle \bar{i} \rangle \langle \bar{q} \rangle$, então todo $\bar{k} \in \mathcal{U}(\mathbb{Z}_m)$ pode ser escrito como $\bar{k} = \bar{i}^t \bar{q}^s$ e, consequentemente, a e a^k são $\mathbb{F}_q$-conjugados em G. ■

Estamos em condições de provar o principal resultado desta seção.

Teorema 2.1.16. *Sejam G um grupo metacíclico e $\mathbb{F}_q$ um corpo finito com q elementos tal que mdc(q, |G|)=1. Se o número de componentes simples da álgebra $\mathbb{F}_q G$ é minimal, então $\mathcal{U}(\mathbb{Z}_n) = \langle \bar{q} \rangle$ e $\mathcal{U}(\mathbb{Z}_m) = \langle \bar{i} \rangle \langle \bar{q} \rangle$.*

Demonstração. Se o número de componentes simples da álgebra $\mathbb{F}_q G$ é minimal, então pela Proposição 2.1.11, $\mathcal{U}(\mathbb{Z}_n) = \langle \bar{q} \rangle$.

Dado k um inteiro, tal que $mdc(k, m) = 1$. Pelo Lema 2.1.12, temos que a e a^k são $\mathbb{Q}$-conjugados em G. Assim, por hipótese, a e a^k são $\mathbb{F}_q$-conjugados, portanto o

resultado segue pelo Lema 2.1.15. ■

Enunciaremos a seguir um resultado de Teoria dos Números que será necessário adiante.

Teorema 2.1.17. [13, Teorema 6.11] *Seja n um número inteiro. Então o grupo* $\mathcal{U}(\mathbb{Z}_n)$ *é cíclico se e somente se* $n = 1, 2, 4, p^m$ *ou* $2p^m$*, com p primo ímpar.*

Ferraz e Polcino Milies, em [6], provaram o seguinte

Teorema 2.1.18. [6, Teorema 2.2] *Sejam* $\mathbb{F}_q$ *um corpo finito com q elementos e A um grupo abeliano de expoente e, tal que mdc(q,|A|)=1. Então o número de componentes simples da álgebra* $\mathbb{F}_qA$ *é minimal se e somente se* $\mathcal{U}(\mathbb{Z}_e)$ *é um grupo cíclico gerado por* $\bar{q} \in \mathbb{Z}_e$.

Seja, agora, A um grupo abeliano finito de ordem mn, tal que $A = \langle x \rangle \times \langle y \rangle$, onde $o(x) = m$ e $o(y) = n$. Então, o expoente de A é $e = mmc(m, n)$. Portanto, pelo Teorema 2.1.18, se o número de componentes simples da álgebra $\mathbb{F}_qG$ é minimal, então $\mathcal{U}(\mathbb{Z}_e) = \langle \bar{q} \rangle$. Mais precisamente, pelo Teorema 2.1.17, temos os seguintes casos:

1. $e = 2$ e q ímpar.

   Neste caso, devemos ter $m = n = 2$, pois $e = mmc(m, n)$, logo $\mathcal{U}(\mathbb{Z}_m) = \langle \bar{q} \rangle$ e $\mathcal{U}(\mathbb{Z}_n) = \langle \bar{q} \rangle$.

2. $e = 4$ e $q \equiv 3 (\text{mod } 4)$.

   Neste caso, devemos ter $m = n = 4$ e novamente teremos $\mathcal{U}(\mathbb{Z}_m) = \langle \bar{q} \rangle$ e $\mathcal{U}(\mathbb{Z}_n) = \langle \bar{q} \rangle$.

3. $e = p^s$ e $\mathcal{U}(\mathbb{Z}_{p^s}) = \langle \bar{q} \rangle$.

   Neste caso, $m = p^s$ e $n = p^t$ com $t \leq s$, portanto $\mathcal{U}(\mathbb{Z}_m) = \langle \bar{q} \rangle$ e $\mathcal{U}(\mathbb{Z}_n) = \langle \bar{q} \rangle$.

4. $e = 2p^s$ e $\mathcal{U}(\mathbb{Z}_{2p^s}) = \langle \bar{q} \rangle$.

   Neste caso, $m = 2p^s$ e $n = 2p^t$ com $t \leq s$, portanto $\mathcal{U}(\mathbb{Z}_m) = \langle \bar{q} \rangle$ e $\mathcal{U}(\mathbb{Z}_n) = \langle \bar{q} \rangle$.

Assim, se o número de componentes simples da álgebra $\mathbb{F}_qA$ é minimal, então $\mathcal{U}(\mathbb{Z}_m) = \langle \bar{q} \rangle$ e $\mathcal{U}(\mathbb{Z}_n) = \langle \bar{q} \rangle$, exatamente o mesmo resultado obtido no Teorema 2.1.16, pois, neste caso, $i = 1$.

Observação 2.1.19. A recíproca do Teorema 2.1.16 não vale sempre. De fato, considerando um grupo abeliano $A = \langle x \rangle \times \langle y \rangle$, onde $\mathrm{o}(x) = p^m$ e $\mathrm{o}(y) = \ell^n$, de tal maneira que $\mathcal{U}(\mathbb{Z}_{p^m}) = \langle \bar{q} \rangle$ e $\mathcal{U}(\mathbb{Z}_{\ell^n}) = \langle \bar{q} \rangle$, então o expoente de A é $e = exp(A) = p^m\ell^n$. Assim,

$$\mathbb{Z}_e = \mathbb{Z}_{p^m\ell^n} \cong \mathbb{Z}_{p^m} \oplus \mathbb{Z}_{\ell^n}$$

donde

$$\mathcal{U}(\mathbb{Z}_e) \cong \mathcal{U}(\mathbb{Z}_{p^m}) \times \mathcal{U}(\mathbb{Z}_{\ell^n}).$$

Como $|\mathcal{U}(\mathbb{Z}_{p^m})|$ e $|\mathcal{U}(\mathbb{Z}_{\ell^n})|$ são ambos pares, este produto direto não é cíclico, o que nos mostra que o número de componentes simples da álgebra $\mathbb{F}_qA$ não é minimal.

2.2 Idempotentes Centrais Primitivos

Ao longo desta seção, G indicará sempre um grupo metacíclico **não abeliano** com a seguinte apresentação:

$$G = \left\langle a, b \mid a^{p^m} = 1 = b^{\ell^n},\ bab^{-1} = a^i \right\rangle$$

onde e p e ℓ são números primos ímpares distintos e $i \neq 1$. Seja, ainda, $\mathbb{F}_q$ um corpo finito com q elementos, tal que $\mathrm{mdc}(q, |G|)$=1.

Da nossa hipótese sobre G, sabemos que $i^{\ell^n} \equiv 1 \mathrm{mod}\ (p^m)$, logo $o(\bar{i}) = \ell^s$ em $\mathcal{U}(\mathbb{Z}_{p^m})$. Nosso objetivo é mostrar que, sob estas condições e $o(\bar{i}) = \ell^n$ em $\mathcal{U}(\mathbb{Z}_{p^m})$, vale a recíproca do Teorema 2.1.16, ou seja, se $\mathcal{U}(\mathbb{Z}_{p^m}) = \langle \bar{q} \rangle$ e $\mathcal{U}(\mathbb{Z}_{\ell^n}) = \langle \bar{q} \rangle$, então o número de componentes simples da álgebra $\mathbb{F}_qG$ é minimal. Tendo em mãos este resultado, vamos explicitar os idempotentes centrais primitivos $\mathbb{F}_qG$.

Para cada número natural $v,\ 0 \leq v \leq \ell^n - 1$, definimos

$$t_v = \text{mdc}(i^v - 1, p^m).$$

Denotando por ℓ^s a ordem de $\bar{i}$ em $\mathcal{U}(\mathbb{Z}_{p^m})$, obtemos o seguinte resultado

Lema 2.2.1. *Se $k < s$, então $mdc(i^{\ell^k} - 1, p^m) = 1$.*

Demonstração. Seja $d = mdc(i^{\ell^k} - 1, p^m)$. Então $d = p^t$ com $t \leq m$ e existe um número inteiro r tal que $i^{\ell^k} - 1 = rp^t$, donde $i^{\ell^k} = 1 + rp^t$. Mas

$$\begin{aligned} i^{\ell^s} = (i^{\ell^k})^{\ell^{s-k}} &= (1 + rp^t)^{\ell^{s-k}} \\ &= \sum \tbinom{\ell^{s-k}}{j} (rp^t)^{\ell^{s-k}-j} \\ &= (rp^t)^{\ell^{s-k}} + \cdots + \ell^{s-k} rp^t + 1. \end{aligned}$$

Da nossa suposição, $i^{\ell^s} - 1 = up^m$, para algum inteiro u. Então

$$up^m = (rp^t)^{\ell^{s-k}} + \cdots + \ell^{s-k} rp^t$$

e, dividindo por p^t, obtemos

$$up^{m-t} = r^{\ell^{s-k}} p^{\ell^{s-k}t-t} + \cdots + \ell^{s-k} r.$$

Se $0 < t < m$, então $p \mid r$ e, como $i^{\ell^k} - 1 = rp^t$ segue que $p^{t+1} \mid i^{\ell^k} - 1$ uma contradição pois $mdc(i^{\ell^k} - 1, p^m) = p^t$.

Se $t = m$, então $p^m \mid (i^{\ell^k} - 1)$, donde $\bar{i}^{\ell^k} = \bar{1}$ em $\mathcal{U}(\mathbb{Z}_{p^m})$, também uma contradição, pois $o(\bar{i}) = \ell^s$. Logo $t = 0$. ∎

No que segue, vamos precisar dos seguintes resultados de Ferraz e Simón-Pinero:

Lema 2.2.2. [7, Lema 2.3]

Sejam H um grupo de expoente e a e b elementos de H. Então a e b são $\mathbb{Q}$-conjugados em H se e somente se existem $h \in H$ e $\tau \in \mathbb{Z}$ com $mdc(\tau, o(a)) = 1$, tal que $a^\tau = hbh^{-1}$.

Proposição 2.2.3. [7, Proposição 2.6] *Seja H um grupo metacíclico com a seguinte apresentação:*

$$H = \langle a, b \mid a^m = 1,\ \ b^n = a^s,\ \ bab^{-1} = a^i \rangle.$$

Então, dado um elemento $a^x b^y \in H$, existe um único divisor v de n, tal que $a^x b^y$ é $\mathbb{Q}$-conjugado a $a^r b^v$ para algum r. Além disso, $v = mdc(y, n)$ e podemos escolher r, tal que $0 \leq r \leq t_v - 1$.

Corolário 2.2.4. [7, Corolário 2.7] *Seja H um grupo metacíclico com a seguinte apresentação:*

$$H = \langle a, b \mid a^m = 1,\ \ b^n = a^s,\ \ bab^{-1} = a^i \rangle.$$

Seja $t_v = mdc(i^v - 1, m)$. Definindo

$$D_v = \{a^r b^v \mid 0 \leq r \leq t_v - 1\}$$

tem-se que cada elemento de H é $\mathbb{Q}$-conjugado a um elemento em $\bigcup_{v|n} D_v$, e nenhum elemento em D_{v_1} pode ser $\mathbb{Q}$-conjugado a outro elemento de D_{v_2}, se $v_1 \neq v_2$.

Como, no nosso caso, ℓ é um número primo, temos que $\bigcup_{v|\ell^n} D_v = D_1 \cup \cdots \cup D_{\ell^n}$.

Seja $\mathbb{F}_q$ um corpo finito com q elementos, tal que $\mathrm{mdc}(q, |G|) = 1$. Suponhamos que $\mathcal{U}(\mathbb{Z}_{p^m}) = \langle \bar{q} \rangle$, $\mathcal{U}(\mathbb{Z}_{\ell^n}) = \langle \bar{q} \rangle$.

Suponhamos, ainda, que $o(\bar{i}) = \ell^n$ em $\mathcal{U}(\mathbb{Z}_{p^m})$. Pelo Lema 2.2.1,
$t_{\ell^k} = mdc(i^{\ell^k} - 1, p^m) = 1$, se $k < n$ donde

$$D_{\ell^k} = \{a^j b^{\ell^k} : 0 \leq j \leq t_{\ell^k} - 1\} = \{b^{\ell^k}\}.$$

Pelo Corolário 2.2.4, todo elemento de G da forma $a^x b^y$ é $\mathbb{Q}$-conjugado a b^{ℓ^k}, para algum inteiro k. Entretanto, pelo Lema 2.2.2, existem $\gamma \in \mathcal{U}(\mathbb{Z}_{\ell^n})$ e $h \in G$, tais que $(a^x b^y)^\gamma = h b^{\ell^k} h^{-1}$.

Dados dois elementos da forma $a^{x_1}b^{y_1}$ e $a^{x_2}b^{y_2}$ que são $\mathbb{Q}$-conjugados, então eles são $\mathbb{Q}$-conjugados ao mesmo elemento b^{ℓ^k}, $k < s$. Assim, $a^{x_1}b^{y_1}$ e $a^{x_2}b^{y_2}$ são $\mathbb{Q}$-conjugados, se e somente se $a^{x_1}b^{y_1}$ e $a^{x_2}b^{y_2}$ são $\mathbb{F}_q$-conjugados pois $\mathcal{U}(\mathbb{Z}_{\ell^n}) = \langle \bar{q} \rangle$.

Por fim, pelo Corolário 2.1.13, um elemento da forma a^j é $\mathbb{Q}$-conjugado a a^v com $v \mid p^m$. Além disto, dois elementos a^j e $a^k \in G$ são $\mathbb{Q}$-conjugados em G se e somente se existem $\gamma_1 \in \mathcal{U}(\mathbb{Z}_{p^m})$ e $g \in G$, tais que $(a^j)^{\gamma_1} = ga^kg^{-1}$ e isto acontece se e somente se a^j e a^k são $\mathbb{F}_q$-conjugados em G, uma vez que $\mathcal{U}(\mathbb{Z}_{p^m}) = \langle \bar{q} \rangle$.

Consequentemente, mostramos que dois elementos g_1 e g_2 de G são $\mathbb{Q}$-conjugados se e somente se eles são $\mathbb{F}_q$-conjugados, portanto o número de componentes simples da álgebra $\mathbb{F}_qG$ é minimal. Finalmente, o número de componentes simples da álgebra $\mathbb{F}_qG$ é igual ao número de divisores de p^m somado com o número de divisores de ℓ^n, logo o número de componentes simples da álgebra $\mathbb{F}_qG$ é $m + n + 1$.

Como p e ℓ são números primos, denotando $A = \langle a \rangle$ e $B = \langle b \rangle$, temos as seguintes cadeias de subgrupos:

$$A = A_0 \supseteq A_1 \supseteq \cdots \supseteq A_m = \{1\}$$

$$B = B_0 \supseteq B_1 \supseteq \cdots \supseteq B_n = \{1\}$$

com $A_i = \langle a^{p^i} \rangle$ e $B_j = \langle b^{\ell^j} \rangle$.

Considerando os idempotentes associados a estas cadeias, isto é,

$$e_0 = \widehat{A} \quad e \quad e_i = \widehat{A_i} - \widehat{A_{i-1}}, \ \ 1 \leq i \leq m$$

$$f_0 = \widehat{B} \quad e \quad f_j = \widehat{B_j} - \widehat{B_{j-1}}, \ \ 1 \leq j \leq n$$

podemos escrever:

$$1 = f_0e_0 + f_1e_0 + \cdots + f_ne_0 + e_1 + \cdots + e_m.$$

Os idempotentes acima construídos são centrais e existem exatamente $m + n + 1$ o que nos mostra que o conjunto

$$\{f_je_0, 0 \leq j \leq n\} \cup \{e_i, 1 \leq i \leq m\}$$

é o conjunto de idempotentes centrais primitivos da álgebra $\mathbb{F}_qG$.

Capítulo 3

Álgebras de Grupo de Alguns Grupos Metacíclicos Particulares

3.1 Resultados Preliminares

Dutra, Ferraz e Polcino Milies provaram em [4], Teorema 3.3, o seguinte resultado:

Teorema 3.1.1. *Sejam D_n um grupo diedral com a seguinte apresentação*

$$D_n = \langle a, b \mid a^n = 1 = b^2,\ \ bab = a^{-1} \rangle$$

e $\mathbb{F}_q$ um corpo finito com q elementos tal que $\mathrm{mdc}(q, 2n)=1$. *O número de componentes simples da álgebra $\mathbb{F}_q D_n$ é minimal se e somente se vale uma das seguintes condições:*

i) $n = 2$ *ou* 4 *e* q *ímpar;*

ii) $n = 2^m$ *com* $m \geq 3$ *e* q *congruente à 3 ou 5 módulo 8;*

iii) $n = p^m$ *com* p *primo ímpar e a classe* $\overline{q}$ *é um gerador de* $\mathcal{U}(\mathbb{Z}_{p^m})$;

iv) $n = p^m$ *com* p *primo ímpar e a classe* $\overline{q}$ *é um gerador do subgrupo* $\mathcal{U}^2(\mathbb{Z}_{p^m}) = \{x^2 \mid x \in \mathcal{U}(\mathbb{Z}_{p^m})\}$ *e* $\overline{-1}$ *não é um quadrado em* $\mathcal{U}(\mathbb{Z}_{p^m})$;

v) $n = 2p^m$ *e com* p *primo ímpar e a classe* $\overline{q}$ *é um gerador de* $\mathcal{U}(\mathbb{Z}_{2p^m})$;

vi) $n = 2p^m$ *com* p *primo ímpar e a classe* $\overline{q}$ *é um gerador do subgrupo* $\mathcal{U}^2(\mathbb{Z}_{2p^m}) = \{x^2 \mid x \in \mathcal{U}(\mathbb{Z}_{2p^m})\}$ *e* $\overline{-1}$ *não é um quadrado em* $\mathcal{U}(\mathbb{Z}_{2p^m})$*;*

vii) $n = 4p^m$ *com* p *primo ímpar,* q *e (-q) têm ordem* $\varphi(p^m)$ *módulo* $4p^m$*;*

viii) $n = p_1^{m_1}p_2^{m_2}$ *com* p_1 *e* p_2 *primos ímpares,* $\text{mdc}(\varphi(p_1^{m_1}), \varphi(p_2^{m_2})) = 2$*,* q *e (-q) têm ordem* $\varphi(p_1^{m_1})\varphi(p_2^{m_2})/2$ *em* $\mathcal{U}(\mathbb{Z}_{p_1^{m_1}p_2^{m_2}})$*;*

ix) $n = 2p_1^{m_1}p_2^{m_2}$ *com* p_1 *e* p_2 *primos ímpares,* $\text{mdc}(\varphi(p_1^{m_1}), \varphi(p_2^{m_2})) = 2$*,* q *e (-q) têm ordem* $\varphi(p_1^{m_1})\varphi(p_2^{m_2})/2$ *em* $\mathcal{U}(\mathbb{Z}_{2p_1^{m_1}p_2^{m_2}})$*.*

Neste capítulo, consideraremos grupos metacíclicos **não abelianos** com a apresentação:

$$G = \langle a, b \mid a^n = 1 = b^2,\ \ bab = a^i \rangle.$$

tendo como objetivo principal, estender o Teorema 3.1.1.

Vamos enunciar alguns resultados de teoria dos números que serão utilizados na demonstração do principal resultado deste capítulo.

Lema 3.1.2. [22, Corolário 4.2.7] *Seja* ξ *uma raiz n-ésima primitiva da unidade. Então* $\text{Gal}(\mathbb{Q}(\xi), \mathbb{Q}) \cong \mathcal{U}(\mathbb{Z}_n)$*.*

Definição 3.1.3. *Seja* n *um inteiro. Definimos a* ***função de Euler*** $\varphi(n)$ *como o número de inteiros* $a = 1, 2, \ldots, n$ *tais que mdc(a,n)=1.*

Lema 3.1.4. [13, Lema 5.4] *Se* $n = p^m$*, onde* p *é um número primo, então*

$$\varphi(p^m) = p^{m-1}(p-1).$$

Teorema 3.1.5. [13, Teorema 5.6] *Sejam* m *e* n *um números inteiros primos entre si. Então* $\varphi(mn) = \varphi(m)\varphi(n)$*.*

Teorema 3.1.6. [13, Teorema 6.11] *Seja* n *um número inteiro. Então o grupo* $\mathcal{U}(\mathbb{Z}_n)$ *é cíclico se e somente se* $n = 1, 2, 4, p^m$ *ou* $2p^m$ *com* p *primo ímpar.*

Lema 3.1.7. *Seja $m \geq 3$ um inteiro. Então*

$$5^{2^{m-3}} \equiv 2^{m-1} + 1 \ (mod\ 2^m)$$

$$-5^{2^{m-3}} \equiv 2^{m-1} - 1 \ (mod\ 2^m).$$

Demonstração. Sabe-se que 2^{m-1} é a maior potência de 2 que divide $5^{2^{m-3}} - 1$ ([13, Lema 6.9]). Logo

$$5^{2^{m-3}} - 1 = 2^{m-1}s$$

onde $s = 2k + 1$ é um inteiro ímpar. Assim,

$$5^{2^{m-3}} - 1 = 2^m k + 2^{m-1}$$

donde

$$5^{2^{m-3}} \equiv 2^{m-1} + 1 \ (mod\ 2^m).$$

Como $2^{m-1} \equiv -2^{m-1} \ (mod\ 2^m)$, a segunda afirmação segue imediatamente. ■

Teorema 3.1.8. [13, Teorema 6.10] *Se $m \geq 3$, então*

$$\mathcal{U}(\mathbb{Z}_{2^m}) = \{\pm\overline{5}^j \mid 0 \leq j \leq 2^{m-2}\}.$$

Em outras palavras, $\mathcal{U}(\mathbb{Z}_{2^m}) = \langle\overline{-1}\rangle \times \langle\overline{5}\rangle$. Além disto, as unidades de ordem 2 em $\mathbb{Z}_{2^m}$ são $\overline{-1}$, $\overline{2^{m-1}-1}$ e $\overline{2^{m-1}+1}$. Ainda, como $|\mathcal{U}(\mathbb{Z}_{2^m})| = 2^{m-1}$, então $o(\overline{5}) = 2^{m-2}$.

Definição 3.1.9. *Um elemento $x \in \mathcal{U}(\mathbb{Z}_n)$, diz-se* ***resíduo quadrático módulo n*** *se $x = s^2$ para algum $s \in \mathcal{U}(\mathbb{Z}_n)$. O subgrupo dos resíduos quadráticos módulo n será denotado por Q_n.*

Teorema 3.1.10. [13, Teorema 7.14] *Seja x um número inteiro ímpar. Então $x \in Q_4$ se e somente se $x \equiv 1\ mod\ 4$.*

Lema 3.1.11. [13, Lema 7.3] *Seja $n > 2$. Suponhamos que $\mathcal{U}(\mathbb{Z}_n)$ seja um grupo cíclico. Então Q_n é um grupo cíclico de ordem $\varphi(n)/2$, gerado por g^2, onde g é um gerador de $\mathcal{U}(\mathbb{Z}_n)$.*

Teorema 3.1.12. [13, Teorema 7.15] *Seja $n = n_1 n_2 \cdots n_k$ com n_j primos entre si. Então $x \in Q_n$ se e somente se $x \in Q_{n_j}$ para cada j.*

Lema 3.1.13. [19, Corolário 6.6] *Todo grupo abeliano finito A é um produto direto de grupos cíclicos $A = C_{m_1} \times C_{m_2} \times \cdots \times C_{m_t}$ com $m_1 \mid m_2 \mid \cdots \mid m_t$.*

Definição 3.1.14. *Dizemos que um grupo abeliano finito A possui **fatores invariantes** $(m_1, \cdots, m_t)$ se $A = C_{m_1} \times C_{m_2} \times \cdots \times C_{m_t}$ com $m_1 \mid m_2 \mid \cdots \mid m_t$..*

Lema 3.1.15. [19, Corolário 6.14]

1. *Dois grupos abelianos finitos são isomorfos se e somente se eles possuem os mesmos fatores invariantes.*

2. *Sejam A, B e C grupos abelianos finitos. Se $A \times B \cong A \times C$, então $B \cong C$.*

Para cada $m \in \mathbb{Z}$, definimos uma função:

$$\begin{aligned} f_m : G &\longrightarrow G \\ a^j b^k &\longmapsto a^{jm} b^k, \ k = 0, 1. \end{aligned}$$

É fácil verificar que f_m é um homomorfismo de grupos. Ainda, $f_m \circ f_n = f_{mn}$, donde $f_m \in \mathrm{Aut}(G)$ se $\overline{m} \in \mathcal{U}(\mathbb{Z}_n)$.

Esta construção nos permite enunciar a seguinte:

Proposição 3.1.16. *O grupo das unidades dos inteiros módulo n é isomorfo a um subgrupo do grupo Aut(G).*

Demonstração. Considere a seguinte função:

$$\psi : \mathcal{U}(\mathbb{Z}_n) \longrightarrow \mathrm{Aut}(G)$$

$$\overline{m} \longmapsto f_m.$$

Note que $f_m = I$ implica que, em particular, $a = a^m$, donde $a^{m-1} = 1$. Consequentemente, $m \equiv 1 \ (mod\ n)$. ■

Seja, agora, $\mathbb{F}_q$ um corpo finito com q elementos, tal que $mdc(q, |G|) = 1$. Como $|G| = 2n$, tem-se que $\overline{q} \in \mathcal{U}(\mathbb{Z}_n)$ e, portanto, $f_q \in \mathrm{Aut}(G)$. Seja e é o expoente do grupo G. Dada uma raiz e-ésima primitiva da unidade ξ, o grupo de Galois $\mathrm{Gal}(\mathbb{F}_q(\xi), \mathbb{F}_q)$ é cíclico, gerado pelo automorfismo de Frobenius $\sigma : \xi \mapsto \xi^q$.

Vamos mostrar que existe uma relação entre $\mathrm{Gal}(\mathbb{F}_q(\xi), \mathbb{F}_q)$ e o subgrupo de $\mathrm{Aut}(G)$ gerado por f_q. Mais precisamente, temos a seguinte resultado, que tem interesse em si mesmo, mas não será necessário adiante.

Proposição 3.1.17. *Seja e o expoente de G e seja ξ uma raiz primitiva e-ésima da unidade. Então os grupos* $\mathrm{Gal}(\mathbb{F}_q(\xi), \mathbb{F}_q)$ *e* $\langle f_q \rangle$ *são isomorfos.*

Demonstração. Definimos a seguinte aplicação:

$$\Phi : \mathrm{Gal}(\mathbb{F}_q(\xi), \mathbb{F}_q) \longrightarrow \langle f_q \rangle$$

$$\sigma^t \longmapsto f_{q^t}.$$

Notemos inicialmente que $\sigma^k(\xi) = \xi^{q^k}$.

1. Φ é um homomorfismo de grupos.

   $\sigma^{k_1}\sigma^{k_2} = \sigma^{k_1+k_2}$, portanto $\Phi(\sigma^{k_1}\sigma^{k_2}) = f_{q^{k_1+k_2}} = f_{q^{k_1}q^{k_2}} = f_{q^{k_1}} \circ f_{q^{k_2}} = \Phi(\sigma^{k_1})\Phi(\sigma^{k_2})$.

2. Φ é injetora.

   Seja $\sigma^k \in \ker(\Phi)$. Então $f_{q^k} = f_1$. Isto implica que $a = a^{q^k}$, logo $q^k = 1 + \beta n$, donde $\sigma^k(\xi) = \xi^{q^k} = \xi\xi^{\beta n}$.

   Se n é par então $n = exp(G)$, donde $\sigma^k(\xi) = \xi$. Se n é ímpar, então $exp(G) = 2n$. Como $mdc(q, 2n) = 1$, temos que q também é ímpar. Na equação $q^k = 1 + \beta n$, estes fatos implicam que β é par, isto é, $\beta = 2\beta'$. Então

   $$\sigma^k(\xi) = \xi\xi^{2\beta' n} = \xi.$$

   Em qualquer caso, $\sigma = Id$.

Claramente, Φ é sobrejetora, o que prova a Proposição. ■

3.2 A Estrutura da Álgebra

Vamos começar apresentando um Lema técnico.

Lema 3.2.1. *Sejam G um grupo metacíclico não abeliano com a seguinte apresentação*

$$G = \langle a, b \mid a^n = 1 = b^2,\ \ bab = a^i \rangle.$$

e $d = mdc(n, i-1)$. As classes de conjugação dos elementos não centrais de G são da forma $\mathcal{C}(a^m) = \{a^m, a^{mi}\}$ e $\mathcal{C}(a^j b) = a^j bG' = a^j b \langle a^{i-1} \rangle$, $0 \leq j \leq d-1$.

Demonstração.

A inclusão $\mathcal{C}(x) \subset xG'$ vale para grupos em geral. Só temos que provar que, no nosso caso, vale a inclusão contrária. De fato, dado $y \in a^j bG'$, temos que

$$y = a^j b(a^{i-1})^k = a^j ba^{ik}a^{-k} = a^j a^k ba^{-k} = a^k(a^j b)a^{-k}.$$

Logo $a^j bG' \subset \mathcal{C}(a^j b)$. ■

Queremos estender o Teorema 3.1.1 e isso significa determinar para quais valores de n a álgebra $\mathbb{F}_q G$ tem número mínimo de componentes simples.

Lema 3.2.2. *Sejam m_1 e m_2 divisores positivos de n. Se os elementos de G, a^{m_1} e a^{m_2}, são $\mathbb{F}_q$-conjugados em G, então $m_1 = m_2$.*

Demonstração. Sejam a^{m_1} e a^{m_2} elementos de G $\mathbb{F}_q$-conjugados. Existem $h \in G$ e $t_0 \in \mathbb{Z}$, tais que $a^{m_1} = h(a^{m_2})^{q^{t_0}}h^{-1}$, ou seja, $a^{m_1} = a^{m_2 q^{t_0}}$ ou $a^{m_1} = a^{m_2 i q^{t_0}}$. Isso implica que $m_1 = m_2 q^{t_0} + kn$ ou $m_1 = m_2 q^{t_0} i + kn$. Entretanto, m_2 divide n, então m_2 divide m_1. Analogamente, mostramos que m_1 divide m_2 e, como m_1 e m_2 são positivos, tem-se que $m_1 = m_2$. ■

Proposição 3.2.3. *Seja G um grupo metacíclico não abeliano com a seguinte apresentação:*

$$G = \langle a, b \mid a^n = 1 = b^2,\ \ bab = a^i \rangle.$$

Os elementos a e a^m, para todo m, tal que $\overline{m} \in \mathcal{U}(\mathbb{Z}_n)$, são $\mathbb{F}_q$-conjugados se e somente se $\overline{q}$ gera o grupo $\mathcal{U}(\mathbb{Z}_n)$, ou $\mathcal{U}(\mathbb{Z}_n) = \langle \overline{q} \rangle \times \langle \overline{i} \rangle$.

Demonstração. Suponhamos que a e a^m são $\mathbb{F}_q$-conjugados. Então, $a^m = a^{q^t}$ ou $a^m = a^{iq^t}$, para algum $t \in \mathbb{Z}$. Isto nos mostra que $\mathcal{U}(\mathbb{Z}_n) = \langle \overline{i} \rangle \langle \overline{q} \rangle$. Se $\overline{i} \in \langle \overline{q} \rangle$, então $\mathcal{U}(\mathbb{Z}_n) = \langle \overline{q} \rangle$, caso contrário, $\mathcal{U}(\mathbb{Z}_n) = \langle \overline{i} \rangle \times \langle \overline{q} \rangle$.

Reciprocamente, se $\mathcal{U}(\mathbb{Z}_n) = \langle \overline{q} \rangle$, então $a^m = a^{q^t}$ e estes elementos são $\mathbb{F}_q$-conjugados em G. Se $\overline{q}$ gera um subgrupo de índice 2 em $\mathcal{U}(\mathbb{Z}_n)$ e $\overline{i} \notin \langle \overline{q} \rangle$, então $\overline{m} \langle \overline{q} \rangle = \langle \overline{q} \rangle$ ou $\overline{m} \langle \overline{q} \rangle = \overline{i} \langle \overline{q} \rangle$. No primeiro caso, $m = q^k$ para algum k, donde $a^m = a^{q^k}$ e a e a^m são $\mathbb{F}_q$-conjugados. Se $\overline{m} \langle \overline{q} \rangle = \overline{i} \langle \overline{q} \rangle$, então $\overline{m} = \overline{i}\overline{q}^t$, para algum t donde $a^m = a^{iq^t}$ e, como a^i é conjugado a a, temos que a e a^m são $\mathbb{F}_q$-conjugados. ■

Sabemos, pelo Corolário 2.1.13, que, para cada $a^k \in G$, existe um único divisor v de n, tal que a^k e a^v são $\mathbb{Q}$-conjugados em G. Além disso, como $\text{mdc}(q, |G|) = 1$ se a^{m_1} e a^{m_2} são $\mathbb{F}_q$-conjugados em G, então a^{m_1} e a^{m_2} são $\mathbb{Q}$-conjugados em G. Esse fato nos permite enunciar o seguinte:

Teorema 3.2.4. *Sejam G um grupo metacíclico não abeliano com a seguinte apresentação:*

$$G = \langle a, b \mid a^n = 1 = b^2,\ \ bab = a^i \rangle$$

$\mathbb{F}_q$ um corpo finito com q elementos, tal que mdc*(q, 2n)=1. Se o número de componentes simples da álgebra $\mathbb{F}_q G$ é minimal, então $\overline{q}$ gera o grupo $\mathcal{U}(\mathbb{Z}_n)$ ou $\mathcal{U}(\mathbb{Z}_n) = \langle \overline{q} \rangle \times \langle \overline{i} \rangle$.*

Demonstração. A demonstração é análoga à do Teorema 2.1.16.

Lema 3.2.5. *Sejam G um grupo metacíclico não abeliano com a seguinte apresentação:*

$$G = \langle a, b \mid a^n = 1 = b^2,\ \ bab = a^i \rangle$$

$\mathbb{F}_q$ um corpo finito com q elementos tal que mdc*(q, 2n)=1. Suponhamos que $\overline{q}$ gera o grupo $\mathcal{U}(\mathbb{Z}_n)$ ou $\mathcal{U}(\mathbb{Z}_n) = \langle \overline{q} \rangle \times \langle \overline{i} \rangle$. As seguintes afirmações são equivalentes.*

1. *a^{m_1} e a^{m_2} são $\mathbb{F}_q$-conjugados em G*
2. *a^{m_1} e a^{m_2} são $\mathbb{Q}$-conjugados em G*

Demonstração. Notemos que, por hipótese, $mdc(q, n) = 1$, logo se a^{m_1} e a^{m_2} são $\mathbb{F}_q$-conjugados em G, pelo Lema 2.1.3, a^{m_1} e a^{m_2} são $\mathbb{Q}$-conjugados em G.

Suponhamos que a^{m_1} e a^{m_2} são $\mathbb{Q}$-conjugados. Se $\mathcal{U}(\mathbb{Z}_n) = \langle \overline{q} \rangle$, então $a^{m_1} = a^{m_2 q^t}$, e se $\mathcal{U}(\mathbb{Z}_n) = \langle \overline{i} \rangle \times \langle \overline{q} \rangle$, então $a^{m_1} = a^{m_2 q^t i}$. Em ambos os casos, a^{m_1} e a^{m_2} são $\mathbb{F}_q$-conjugados. ∎

Vamos provar um Lema técnico que nos será muito útil.

Lema 3.2.6. *Sejam G um grupo metacíclico não abeliano com a seguinte apresentação:*

$$G = \langle a, b \mid a^n = 1 = b^2,\ \ bab = a^i \rangle$$

$\mathbb{F}_q$ um corpo finito com q elementos, tal que mdc*(q, 2n)=1. Se $n = p_1^{m_1} p_2^{m_2}$, com p_1 e p_2 primos ímpares e $\overline{i} \neq \overline{1}$ em $\mathcal{U}(\mathbb{Z}_{p_j^{m_j}})$ para cada j, então* mdc*(n,i-1)=1. Consequentemente, o subgrupo G' de G é igual a $\langle a \rangle$.*

Demonstração. Seja $d = mdc(n, i-1)$. Por hipótese, $i \not\equiv 1 \ (mod\ p_j^{m_j})$, $j = 1, 2$, logo $d = p_1^{t_1} p_2^{t_2}$ com $t_1 \neq m_1$ e $t_2 \neq m_2$.

Como $d \mid (i-1)$, existe $\alpha \in \mathbb{Z}$, tal que $(i-1) = p_1^{t_1} p_2^{t_2} \alpha$, isto é, $i = p_1^{t_1} p_2^{t_2} \alpha + 1$. Assim, $i^2 = p_1^{2t_1} p_2^{2t_2} \alpha^2 + 2p_1^{t_1} p_2^{t_2} \alpha + 1$, donde $i^2 - 1 = p_1^{2t_1} p_2^{2t_2} \alpha^2 + 2p_1^{t_1} p_2^{t_2} \alpha$.

Como, da hipótese sobre G, $i^2 \equiv 1 \ (mod\ n)$ podemos escrever $i^2 - 1 = p_1^{m_1} p_2^{m_2} \beta$ e, substituindo, temos que $p_1^{m_1} p_2^{m_2} \beta - p_1^{2t_1} p_2^{2t_2} \alpha^2 - 2p_1^{t_1} p_2^{t_2} \alpha = 0$. Se $t_1 > 0$, podemos dividir esta igualdade por $p_1^{t_1} p_2^{t_2}$, donde $p_1^{m_1 - t_1} p_2^{m_2 - t_2} \beta - p_1^{t_1} p_2^{t_2} \alpha^2 - 2\alpha = 0$, logo p_1 divide α, consequentemente, o elemento $p_1^{t_1+1} p_2^{t_2}$ divide $(i-1)$ uma contradição mostrando que $t_1 = 0$. De modo análogo, motra-se que $t_2 = 0$. ■

Teorema 3.2.7. *Sejam G um grupo metacíclico não abeliano com a seguinte apresentação*

$$G = \langle a, b \mid a^n = 1 = b^2, \ \ bab = a^i \rangle$$

$\mathbb{F}_q$ um corpo finito com q elementos tal que mdc*$(q, 2n)=1$. O número de componentes simples da álgebra $\mathbb{F}_q G$ é minimal se e somente se vale uma das seguintes condições:*

i) $n = 4$ *e q ímpar;*

ii) $n = 2^m$ *com* $m \geq 3$ *e*
$$\begin{cases} q \equiv 3 \ (mod\ 8) & \text{e } \overline{i} = \overline{2^{m-1} + 1} \quad \text{ou } \overline{i} = \overline{-1} \\ q \equiv 5 \ (mod\ 8) & \text{e } \overline{i} = \overline{2^{m-1} - 1} \quad \text{ou } \overline{i} = \overline{-1} \end{cases}$$

iii) $n = p^m$ *com p primo ímpar e a classe $\overline{q}$ é um gerador de $\mathcal{U}(\mathbb{Z}_{p^m})$;*

iv) $n = p^m$ *com p primo ímpar e a classe $\overline{q}$ é um gerador do subgrupo $\mathcal{U}^2(\mathbb{Z}_{p^m}) = \{x^2 \mid x \in \mathcal{U}(\mathbb{Z}_{p^m})\}$ e $\overline{i}$ não é um quadrado em $\mathcal{U}(\mathbb{Z}_{p^m})$;*

v) $n = 2p^m$ *e com p primo ímpar e a classe $\overline{q}$ é um gerador de $\mathcal{U}(\mathbb{Z}_{2p^m})$;*

vi) $n = 2p^m$ *com p primo ímpar e a classe $\overline{q}$ é um gerador do subgrupo $\mathcal{U}^2(\mathbb{Z}_{2p^m}) = \{x^2 \mid x \in \mathcal{U}(\mathbb{Z}_{2p^m})\}$ e $\overline{i}$ não é um quadrado em $\mathcal{U}(\mathbb{Z}_{2p^m})$;*

vii) $n = 4p^m$ *com p primo ímpar, q e (iq) têm ordem $\varphi(p^m)$ módulo $4p^m$ com $\overline{i} = \overline{-1}$ ou $\overline{i} = \overline{2p^m + 1}$;*

viii) $n = p_1^{m_1}p_2^{m_2}$ *com* p_1 *e* p_2 *primos ímpares,* $\mathrm{mdc}(\varphi(p_1^{m_1}), \varphi(p_2^{m_2})) = 2$*,* q *e (iq) têm ordem* $\varphi(p_1^{m_1})\varphi(p_2^{m_2})/2$ *em* $\mathcal{U}(\mathbb{Z}_{p_1^{m_1}p_2^{m_2}})$ *com* $\bar{i} \neq \bar{1}$ *em* $\mathcal{U}(\mathbb{Z}_{p_j^{m_j}})$*,* $j = 1, 2$*;*

ix) $n = 2p_1^{m_1}p_2^{m_2}$ *com* p_1 *e* p_2 *primos ímpares,* $\mathrm{mdc}(\varphi(p_1^{m_1}), \varphi(p_2^{m_2})) = 2$*,* q *e (iq) têm ordem* $\varphi(p_1^{m_1})\varphi(p_2^{m_2})/2$ *em* $\mathcal{U}(\mathbb{Z}_{2p_1^{m_1}p_2^{m_2}})$ *com* $\bar{i} \neq \bar{1}$ *em* $\mathcal{U}(\mathbb{Z}_{p_j^{m_j}})$*,* $j = 1, 2$*.*

Demonstração. Suponhamos que o número de componentes simples da álgebra $\mathbb{F}_qG$ é minimal. Pelo Teorema 3.2.4, a ordem de $\overline{q}$ em $\mathcal{U}(\mathbb{Z}_n)$ deve ser $\varphi(n)$ ou $\varphi(n)/2$, onde φ denota a função de Euler.

Seja $n = 2^m p_1^{m_1}p_2^{m_2}\cdots p_t^{m_t}$, a decomposição de n como produto de potências de primos. Então

$$\mathbb{Z}_n = \mathbb{Z}_{2^m} \oplus \mathbb{Z}_{p_1^{m_1}} \cdots \oplus \mathbb{Z}_{p_t^{m_t}} \text{ e}$$

$$\mathcal{U}(\mathbb{Z}_n) = \mathcal{U}(\mathbb{Z}_{2^m}) \times \mathcal{U}(\mathbb{Z}_{p_1^{m_1}}) \cdots \times \mathcal{U}(\mathbb{Z}_{p_t^{m_t}}).$$

Vamos analisar em casos separados.

(a) A ordem de $\overline{q}$ *em* $\mathcal{U}(\mathbb{Z}_n)$ *é* $\varphi(n)$*.*

Neste caso, temos que $\mathcal{U}(\mathbb{Z}_n) = \langle\overline{q}\rangle$, portanto, pelo Teorema 3.1.6, devemos ter $n = 2, 4, p^m$ ou $2p^m$. Se $n = 2$, então $G = C_2 \times C_2$ o que não pode ocorrer pois G não é abeliano. Deste modo, ou *(i)* ou *(iii)* ou *(v)* ocorre. Além disso, no caso em que $n = 4$, deve-se ter que $q \equiv 3$ $(mod\ 4)$ para que $\overline{q}$ seja gerador.

(b) A ordem de $\overline{q}$ *em* $\mathcal{U}(\mathbb{Z}_n)$ *é* $\varphi(n)/2$ *com* $\mathcal{U}(\mathbb{Z}_n)$ *cíclico.*

Sendo assim, pelo Lema 3.1.11, o grupo Q_n dos resíduos quadráticos módulo n é cíclico de ordem $\varphi(n)/2$, portanto $Q_n = \langle\overline{q}\rangle$, mostrando que ocorre, ou *(iv)*, ou *(vi)* e ainda, *(i)* no caso em que $n = 4$ e $q \equiv 1$ $(mod\ 4)$.

(c) A ordem de $\overline{q}$ *em* $\mathcal{U}(\mathbb{Z}_n)$ *é* $\varphi(n)/2$ *com* $\mathcal{U}(\mathbb{Z}_n)$ *não cíclico.*

Neste caso, temos que $\mathcal{U}(\mathbb{Z}_n) = \langle\overline{q}\rangle \times \langle\overline{i}\rangle \cong C_{\varphi(n)/2} \times C_2$. Assim, $\varphi(n)/2$ é um número par pois se $\varphi(n)/2$ fosse ímpar, $\mathcal{U}(\mathbb{Z}_n)$ seria cíclico.

Como $C_{\varphi(n)/2}$ é um grupo cíclico de ordem par, então existe um único subgrupo de $C_{\varphi(n)/2}$ de ordem 2. Logo, o 2-subgrupo abeliano elementar maximal de $\mathcal{U}(\mathbb{Z}_n)$ é $C_2 \times C_2$.

Se $n = p_1^{m_1}p_2^{m_2}p_3^{m_3}$, então $\mathcal{U}(\mathbb{Z}_n) \cong \mathcal{U}(\mathbb{Z}_{p_1^{m_1}}) \times \mathcal{U}(\mathbb{Z}_{p_2^{m_2}}) \times \mathcal{U}(\mathbb{Z}_{p_3^{m_3}})$, donde $C_2 \times C_2 \times C_2$ seria um 2-subgrupo abeliano elementar de $\mathcal{U}(\mathbb{Z}_n)$, o que não pode ocorrer. Logo, devemos ter $n = 2^m$ com $m \geq 3$ ou $n = 4p^m$ ou $n = p_1^{m_1}p_2^{m_2}$ ou $n = 2p_1^{m_1}p_2^{m_2}$.

Analisaremos cada um destes casos separadamente.

(c-(i)) $n = 2^m, m \geq 3$.

Sabemos que $\overline{i} \notin \langle\overline{q}\rangle$, pelo Teorema 3.2.4 e que $\overline{i} = \overline{-1}$, $\overline{2^{m-1}-1}$ ou $\overline{2^{m-1}+1}$ pelo Teorema 3.1.8. Além disso, pelo Lema 3.1.7, temos $\overline{2^{m-1}+1} \in \langle\overline{5}\rangle$, $\overline{2^{m-1}-1} \in \langle\overline{-5}\rangle$.

Como $\overline{q} \in \mathcal{U}(\mathbb{Z}_{2^m})$, então devemos ter $\overline{q} = \overline{5}^j$ ou $\overline{q} = \overline{-5}^j$. Por outro lado, $o(\overline{5}) = o(\overline{-5}) = 2^{m-2} = \varphi(n)/2 = o(\overline{q})$, consequentemente, temos $\langle\overline{q}\rangle = \langle\overline{5}\rangle$ ou $\langle\overline{q}\rangle = \langle\overline{-5}\rangle$. Observemos que, em ambos os casos, j deve ser um número ímpar.

No caso em que $\langle\overline{q}\rangle = \langle\overline{5}\rangle$, então então $q \equiv 5^{2k+1}\ (mod\ 2^m)$ para algum inteiro k. Então $q \equiv 25^k \cdot 5\ (mod\ 2^m)$ donde $q \equiv 25^k \cdot 5 \equiv\ 5\ (mod\ 8)$. Ainda, deve se ter que $\overline{i} = \overline{-1}$ ou $\overline{i} = \overline{2^{m-1}-1}$.

Da mesma forma, se $\langle\overline{q}\rangle = \langle\overline{-5}\rangle$, então $q \equiv 3\ (mod\ 8)$ e $\overline{i} = \overline{-1}$ ou $\overline{i} = \overline{2^{m-1}+1}$.

(c-(ii)) $n = 4p^m$.

Como $|\mathcal{U}(\mathbb{Z}_{4p^m})| = \varphi(4p^m) = 2\varphi(p^m)$, tem-se que $o(\overline{q}) = \varphi(p^m)$. Queremos mostrar ainda que $o(\overline{iq}) = \varphi(p^m)$. Para tanto, seja $k = o(\overline{iq})$. Se k fosse ímpar, teríamos $\overline{iq}^k = \overline{i}\overline{q}^k = \overline{1}$, implicando que $\overline{i} \in \langle\overline{q}\rangle$, uma contradição. Consequentemente, k é par. Assim $\overline{iq}^k = \overline{q}^k = \overline{1}$, donde $k \mid \varphi(p^m)$. Finalmente, $\overline{i}^{\varphi(p^m)}\overline{q}^{\varphi(p^m)} = \overline{iq}^{\varphi(p^m)} = \overline{1}$, logo $k = \varphi(p^m)$.

(c-(iii)) $n = p_1^{m_1} p_2^{m_2}$.

Inicialmente, notemos que $\mathcal{U}(\mathbb{Z}_{p_1^{m_1} p_2^{m_2}}) \cong \mathcal{U}(\mathbb{Z}_{p_1^{m_1}}) \times \mathcal{U}(\mathbb{Z}_{p_2^{m_2}})$.

Como $\mid \mathcal{U}(\mathbb{Z}_{p_1^{m_1} p_2^{m_2}}) \mid = \varphi(p_1^{m_1})\varphi(p_2^{m_2})$, temos que $o(\overline{q}) = \frac{\varphi(p_1^{m_1})\varphi(p_2^{m_2})}{2}$ e um argumento análogo ao do caso anterior, prova que $o(\overline{iq}) = \frac{\varphi(p_1^{m_1})\varphi(p_2^{m_2})}{2}$.

Podemos escrever $\varphi(p_1^{m_1}) = 2 \cdot k_1$ e $\varphi(p_2^{m_2}) = 2 \cdot k_2$, donde

$$\begin{aligned}\mathcal{U}(\mathbb{Z}_{p_1^{m_1} p_2^{m_2}}) &\cong C_{\varphi(p_1^{m_1})} \times C_{\varphi(p_2^{m_2})} \\ &= C_{2k_1} \times C_{2k_2}\end{aligned}$$

Como, $\mathcal{U}(\mathbb{Z}_{p_1^{m_1} p_2^{m_2}}) \cong C_2 \times C_{\varphi(p_1^{m_1} p_2^{m_2})/2}$, esta é a decomposição do grupo $\mathcal{U}(\mathbb{Z}_{p_1^{m_1} p_2^{m_2}})$ como produto direto de grupos cíclicos. Em outras palavras, os grupos C_2 e $C_{\varphi(p_1^{m_1} p_2^{m_2})/2}$ são os faotres invariantes de $\mathcal{U}(\mathbb{Z}_{p_1^{m_1} p_2^{m_2}})$. Consequentemente, devemos ter $mmc(2k_1, 2k_2) = \varphi(p_1^{m_1} p_2^{m_2})/2 = 2k_1 k_2$, donde

$$mdc(\varphi(p_1^{m_1}), \varphi(p_2^{m_2})) = mdc(2k_1, 2k_2) = \frac{2k_1 2k_2}{mmc(2k_1, 2k_2)} = 2.$$

(c-(iv)) $n = 2p_1^{m_1} p_2^{m_2}$.

Análogo ao caso anterior, uma vez que $\varphi(2p_1^{m_1} p_2^{m_2}) = \varphi(p_1^{m_1} p_2^{m_2})$.

Reciprocamente, se **n=4**, então G é o grupo diedral de ordem 8 e o resultado segue do Teorema 3.1.1.

Se vale *(ii)*, $\mathbf{n = 2^m}$ e $q \equiv 3 \ (mod\ 8)$ ou $q \equiv 5 \ (mod\ 8)$, pelo Teorema 3.1.16

$$\mathcal{U}(\mathbb{Z}_{2^m}) = \{\pm\overline{5}^j \mid 0 \leq j \leq 2^{m-2}\};$$

logo $\overline{q} = \overline{5}^j$ ou $\overline{q} = \overline{-5}^j$.

Se j é par, como $5^2 \equiv 1 \ (mod\ 8)$ e $-5^2 \equiv 7 \ (mod\ 8)$, tem-se que $q \equiv 1 \ (mod\ 8)$ ou $q \equiv 7 \ (mod\ 8)$, uma contradição. Logo j deve ser ímpar, donde $\langle\overline{q}\rangle = \langle\overline{5}\rangle$ ou $\langle\overline{q}\rangle = \langle\overline{-5}\rangle$. Vamos considerar separadamente os casos possíveis.

(a) Se $q \equiv 3 \; mod \; 8$ e $i = 2^{m-1}+1$, então $\langle \overline{q} \rangle = \langle \overline{-5} \rangle$, o que nos mostra que $\mathcal{U}(\mathbb{Z}_{2^m}) = \langle \overline{q} \rangle \times \langle \overline{i} \rangle$. Assim, pelo Lema 3.2.5, os elementos a^{m_1} e a^{m_2} são $\mathbb{Q}$-conjugados em G se e somente se a^{m_1} e a^{m_2} são $\mathbb{F}_q$-conjugados em G. Precisamos provar que se $a^j b$ e $a^k b$ são $\mathbb{Q}$-conjugados, então $a^j b$ e $a^k b$ também são $\mathbb{F}_q$-conjugados.

Se $a^j b$ e $a^k b$ são $\mathbb{Q}$-conjugados, pelo Lema 3.1.2, existem $\overline{r} \in \mathcal{U}(\mathbb{Z}_{2^m})$ e $h \in G$, tais que $(a^j b)^r = h(a^k b)h^{-1}$.

Como $\mathcal{U}(\mathbb{Z}_{2^m}) = \langle \overline{q} \rangle \times \langle \overline{i} \rangle$, devemos ter $\overline{r} = \overline{i}\overline{q}^t$, para algum inteiro t e $(a^j b)^{iq^t} = h(a^k b)h^{-1}$.

Agora, $mdc(i-1, 2^m) = mdc(2^{m-1}, 2^m) = 2^{m-1}$, logo, pelo Lema 3.2.1, existem 2^{m-1} classes de conjugação de elementos da forma $a^j b$.

Afirmação 1: $(a^j b)^{2^k} = a^{2^{k-1}(j+ji)}$, para todo $k \geq 1$.

Notemos que $(a^j b)^2 = a^j a^{ji} = a^{j+ji}$, então $(a^j b)^{2^k} = (a^j b)^{2 \cdot 2^{k-1}} = (a^{(j+ji)})^{2^{k-1}} = (a^j)^{2^{k-1}(j+ji)}$ o que prova a Afirmação 1.

Afirmação 2: Para cada j positivo, tem-se que $a^{2^{m-2}(j+ji)} \in G'$.

Se $j = 2s$, então $2^{m-2}(2s + 2si) = 2^{m-1}(s + si) = (i-1)(s + si)$. Portanto, pelo Teorema 1.1.2, $a^{2^{m-2}(j+ji)} = (a^{(i-1)})^{(s+si)} \in G' = \langle a^{i-1} \rangle$.

Se $j = 2s + 1$, então

$2^{m-2}(j + ji) = 2^{m-2}(2s + 1 + 2si + i) = 2^{m-1}(s + si) + 2^{m-2}(1 + i)$.

Como, $i + 1 = 2^{m-1} + 2$, logo $2^{m-2}(i+1) = 2^{m-2}2^{m-1} + 2^{m-1} = (i-1)(2^{m-2}+1)$, consequentemente, $a^{2^{m-2}(j+ji)} = a^{(i-1)(s+si+2^{m-2}+1)} \in G' = \langle a^{i-1} \rangle$ provando a Afirmação 2.

Finalmente notemos que

$(a^j b)^i = (a^j b)^{2^{m-1}}(a^j b) = a^{2^{m-2}(j+ji)} a^j b = a^{(i-1)s} a^j b = a^j b a^{(i-1)si} \in a^j b G' = \mathcal{C}(a^j b)$. Isto nos mostra que $(a^j b)^{iq^t} = g(a^j b)^{q^t} g^{-1} = h(a^k b)h^{-1}$. Deste modo, $a^k b = h^{-1}[(a^j b)^i]^{q^t} h$, mas $(a^j b)^i = g(a^j b)g^{-1}$, consequentemente, $a^j b$ e $a^k b$ são $\mathbb{F}_q$-conjugados em G. Assim, quando $q \equiv 3 \; mod \; 8$ e $i = 2^{m-1} + 1$, o número de componentes simples da álgebra $\mathbb{F}_q G$ é minimal.

(b) Se $q \equiv 5\ mod\ 8$ e $i = 2^{m-1} - 1$, então $\langle \overline{q} \rangle = \langle \overline{5} \rangle$ e novamente $\mathcal{U}(\mathbb{Z}_{2^m}) = \langle \overline{q} \rangle \times \langle \overline{i} \rangle$ e os elementos a^{m_1} e a^{m_2} são $\mathbb{Q}$-conjugados em G se e somente se a^{m_1} e a^{m_2} são $\mathbb{F}_q$-conjugados em G.

Por outro lado, $mdc(i-1, 2^m) = mdc(2^{m-1}-2, 2^m) = 2\ mdc(2^{m-2}-1, 2^{m-1}) = 2$ uma vez $2^{m-2} - 1$ é um número ímpar. Isto nos mostra que existem duas classes de conjugação de elementos da forma $a^j b$ a saber $\mathcal{C}(b)$ e $\mathcal{C}(ab)$. No entanto, os elementos b e ab não são $\mathbb{Q}$-conjugados nem $\mathbb{F}_q$-conjugados em G, portanto no caso $q \equiv 5\ mod\ 8$ e $i = 2^{m-1} - 1$, o número de componentes simples da álgebra $\mathbb{F}_q G$ é minimal.

(c) Se $i = -1$, o grupo G é diedral e o resultado segue do Teorema 3.1.1.

Se $\mathbf{n = p^m}$ com p primo ímpar, então, pelo Lema 3.1.6, o grupo $\mathcal{U}(\mathbb{Z}_{p^m})$ é cíclico, donde existe um único elemento de ordem 2 em $\mathcal{U}(\mathbb{Z}_{p^m})$, a saber, $\overline{-1}$. Da nossa hipótese sobre G, temos $\overline{i}^2 = \overline{1}$ em $\mathcal{U}(\mathbb{Z}_{p^m})$, logo devemos ter $\overline{i} = \overline{-1}$, o que nos mostra que G é o grupo diedral D_{p^m} e resultado segue do Teorema 3.1.1. O mesmo acontece quando $\mathbf{n = 2p^m}$ com p primo ímpar.

Se vale *(vii)*, então $\mathbf{n = 4p^m}$, com p primo ímpar e as unidades de ordem 2 em $\mathbb{Z}_{4p^m}$ são $\overline{-1}$, $\overline{2p^m - 1}$ e $\overline{2p^m + 1}$.

$$\mathbb{Z}_{4p^m} \cong \mathbb{Z}_4 \times \mathbb{Z}_{p^m}$$

portanto,

$$\mathcal{U}(\mathbb{Z}_{4p^m}) \cong \mathcal{U}(\mathbb{Z}_4) \times \mathcal{U}(\mathbb{Z}_{p^m}).$$

Por hipótese, $o(\overline{q}) = \varphi(p^m)$. Vamos mostrar que $\overline{i} \notin \langle \overline{q} \rangle$. Suponhamos, por absurdo, que $\overline{i} \in \langle \overline{q} \rangle$, então $\overline{i} = \overline{q}^{\frac{\varphi(p^m)}{2}}$, pois $o(\overline{i}) = 2$ e existe um único elemento de ordem 2 em $\langle \overline{q} \rangle$. Além disso, $\frac{\varphi(p^m)}{2}$ deve ser par senão teríamos $(\overline{iq})^{\frac{\varphi(p^m)}{2}} = \overline{i}\overline{q}^{\frac{\varphi(p^m)}{2}} = \overline{i}^2 = \overline{1}$, o que não pode ocorrer, pois $o(\overline{iq}) = \varphi(p^m)$. Assim, existe um inteiro s tal que $\varphi(p^m)/2 = 2s$, donde $\varphi(p^m) = 4s$.

Podemos, então, escrever $\overline{i} = (\overline{q}^{\frac{\varphi(p^m)}{4}})^2$. No entanto, isso nos diz que i é um resíduo quadrático módulo $4p^m$ e, pelo Teorema 3.1.12, i é um resíduo quadrático módulo 4, portanto $i \equiv 1 \ mod \ 4$.

Se $\overline{i} = \overline{-1}$, então G é o grupo diedral e o resultado segue do Teorema 3.1.1.

Se $\mathbf{i = 2p^m + 1}$, então $2p^m+1 = 4k+1$, o que implicaria que $2 \mid p^m$ uma contradição.

Portanto, em ambos os casos, $\mathcal{U}(\mathbb{Z}_{4p^m}) = \langle \overline{q} \rangle \times \langle \overline{i} \rangle$, logo, pelo Lema 3.2.5, os elementos a^{m_1} e a^{m_2} são $\mathbb{Q}$-conjugados em G se e somente se a^{m_1} e a^{m_2} são $\mathbb{F}_q$-conjugados em G. Vamos provar que, se a^jb e a^kb são $\mathbb{Q}$-conjugados, então a^jb e a^kb também são $\mathbb{F}_q$-conjugados.

Se a^jb e a^kb são $\mathbb{Q}$-conjugados, pelo Lema 3.1.2, existem $\overline{r} \in \mathcal{U}(\mathbb{Z}_{4p^m})$ e $h \in G$, tais que $(a^jb)^r = h(a^kb)h^{-1}$. Como $\mathcal{U}(\mathbb{Z}_{4p^m}) = \langle \overline{q} \rangle \times \langle \overline{i} \rangle$, devemos ter $\overline{r} = \overline{i}\overline{q}^t$, para algum inteiro t e $(a^jb)^{iq^t} = h(a^kb)h^{-1}$.

Por fim, se $i = 2p^m + 1$, então $mdc(i-1, 4p^m) = 2p^m$ e

$(a^jb)^{2p^m+1} = (a^jb)(a^jb)^{2p^m} = (a^jb)(a^{j+ji})^{p^m} = (a^jb)(a^{j(i+1)p^m})$, mas

$(i+1)p^m = (2p^m+2)p^m = 2p^mp^m + 2p^m = 2p^m(p^m+1) = (i-1)(p^m+1)$, o que nos mostra que $(a^jb)^i \in a^jbG' = \mathcal{C}(a^jb)$. Portanto, $(a^jb)^{iq^t} = g(a^jb)^{q^t}g^{-1} = h(a^kb)h^{-1}$, consequentemente, a^jb e a^kb são $\mathbb{F}_q$-conjugados em G, logo o número de componentes simples da álgebra $\mathbb{F}_qG$ é minimal.

Se vale *(viii)*, então $\mathbf{n = p_1^{m_1}p_2^{m_2}}$ com p_1 e p_2 primos ímpares, $mdc(\varphi(p_1^{m_1}), \varphi(p_2^{m_2})) = 2$, q e (iq) têm ordem $\varphi(p_1^{m_1})\varphi(p_2^{m_2})/2$ módulo $p_1^{m_1}p_2^{m_2}$ com $\overline{i} \neq \overline{1}$ em $\mathcal{U}(\mathbb{Z}_{p_j^{m_j}}),\ j = 1, 2$, donde todas as classes de conjugação dos elementos da forma a^jb são iguais a $\mathcal{C}(b)$, uma vez que o Lema 3.2.6 nos diz que $mdc(i-1, p_1^{m_1}p_2^{m_2}) = 1$.

Por hipótese, $o(\overline{q}) = \frac{\varphi(p_1^{m_1})\varphi(p_2^{m_2})}{2}$, o que nos mostra que $\overline{q}$ gera um subgrupo de índice 2 em $\mathcal{U}(\mathbb{Z}_n)$. Além disso, sabemos que $mdc(\varphi(p_1^{m_1}), \varphi(p_2^{m_2})) = 2$, logo existem inteiros $t_1, t_2 \in \mathbb{Z}$, satisfazendo $\varphi(p_1^{m_1}) = 2t_1$, $\varphi(p_2^{m_2}) = 2t_2$, $mdc(t_1, t_2) = 1$. Consequentemente:

$$\begin{aligned}\mathcal{U}(\mathbb{Z}_n) &\cong C_{\varphi(p_1^{m_1})} \times C_{\varphi(p_2^{m_2})} \\ &= C_{2t_1} \times C_{2t_2} \\ &\cong C_2 \times C_{t_1} \times C_{2t_2} \\ &\cong C_2 \times C_{2t_1t_2} \\ &= C_2 \times C_{\frac{\varphi(p_1^{m_1})\varphi(p_2^{m_2})}{2}}.\end{aligned}$$

Suponhamos, por absurdo, que $\bar{i} \in \langle \overline{q} \rangle$, então devemos ter $\bar{i} = \overline{q}^{\frac{\varphi(p_1^{m_1})\varphi(p_2^{m_2})}{4}}$, pois $o(\bar{i}) = 2$. Agora, como $o(\overline{iq}) = \frac{\varphi(p_1^{m_1})\varphi(p_2^{m_2})}{2}$, então $\frac{\varphi(p_1^{m_1})\varphi(p_2^{m_2})}{4}$ é par, e assim, podemos escrever $\bar{i} = (\overline{q}^{\frac{\varphi(p_1^{m_1})\varphi(p_2^{m_2})}{8}})^2$ e concluímos que i é um resíduo quadrático módulo $p_1^{m_1}p_2^{m_2}$.

Pelo Teorema 3.1.12, i é resíduo quadrático módulo $p_j^{m_j}$ para $j = 1, 2$.

Sejam g_j geradores dos grupos $\mathcal{U}(\mathbb{Z}_{p_j^{m_j}})$, respectivamente. Pelo Lema 3.1.11, os subgrupos $Q_{p_j^{m_j}}$ são cíclicos de ordem $\varphi(p_j^{m_j})/2$ e gerados pelos elementos g_j^2.

Como, por hipótese, $i \not\equiv 1 \; mod \; p_j^{m_j}$ então $o(\bar{i}) = 2$ módulo $p_j^{m_j}$. Isso implica que $o(\bar{i}) = 2$ em $Q_{p_j^{m_j}}$, donde $\varphi(p_j^{m_j})/2$ é par. Com isso, existem inteiros s_1 e s_2, tais que $\varphi(p_1^{m_1})/2 = 2s_1$ e $\varphi(p_2^{m_2})/2 = 2s_2$, o que nos mostra que $\varphi(p_1^{m_1}) = 4s_1$ e $\varphi(p_2^{m_2}) = 4s_2$, uma contradição, pois $mdc(\varphi(p_1^{m_1}), \varphi(p_2^{m_2})) = 2$. Portanto $\bar{i} \notin \langle \overline{q} \rangle$.

Novamente, $\mathcal{U}(\mathbb{Z}_{p_1^{m_1}p_2^{m_2}}) = \langle \overline{q} \rangle \times \langle \bar{i} \rangle$, portanto, pelo Lema 3.2.5, os elementos a^{m_1} e a^{m_2} são $\mathbb{Q}$-conjugados em G se e somente se a^{m_1} e a^{m_2} são $\mathbb{F}_q$-conjugados em G e, portanto, o número de componentes simples da álgebra $\mathbb{F}_qG$ é minimal.

Se vale *(ix)*, então $\mathbf{n = 2p_1^{m_1}p_2^{m_2}}$ com p_1 e p_2 primos ímpares, $mdc(\varphi(p_1^{m_1}), \varphi(p_2^{m_2})) = 2$, q e (iq) têm ordem $\varphi(p_1^{m_1})\varphi(p_2^{m_2})/2$ módulo $p_1^{m_1}p_2^{m_2}$ com $\bar{i} \neq \overline{1}$ em $\mathcal{U}(\mathbb{Z}_{p_j^{m_j}})$, $j = 1, 2$, então existem duas classes de conjugação distintas de elementos da forma a^jb, a saber, $\mathcal{C}(ab)$ e $\mathcal{C}(b)$, pois $mdc(i-1, n) = 2$. Tais classes de conjugação não são $\mathbb{Q}$-conjugadas nem $\mathbb{F}_q$-conjugadas. Prova-se o resultado de maneira análoga ao caso anterior. ■

Finalizaremos este capítulo, exibindo dois exemplos que justificam as hipóteses assumidas sobre $\bar{i}$ nos itens *(vii)*, *(viii)* e *(ix)* do Teorema 3.2.7.

Exemplo 3.2.8. Quando $n = 4p^m$, as unidades de ordem 2 em $\mathbb{Z}_{4p^m}$ são $\overline{-1}$, $\overline{2p^m - 1}$ e $\overline{2p^m + 1}$. Vimos, no Teorema 3.2.7 *(vii)*, que se $\overline{i} = \overline{-1}$ ou $\overline{i} = \overline{2p^m + 1}$, então $\mathcal{U}(\mathbb{Z}_{4p^m}) = \langle\overline{q}\rangle \times \langle\overline{i}\rangle$. Vamos exibir um exemplo mostrando que, para o caso $\overline{i} = \overline{2p^m - 1}$, esse resultado não vale em geral.

Considere $n = 20 = 4.5$. Assim:

$$\mathcal{U}(\mathbb{Z}_{20}) = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}, \overline{11}, \overline{13}, \overline{17}, \overline{19}\}.$$

As unidades de ordem 4 em $\mathbb{Z}_{20}$ são $\overline{3}, \overline{7}, \overline{13}, \overline{17}$. Tomando $\overline{i} = \overline{2p^m - 1} = \overline{9}$, tem-se que $\overline{9} = \overline{3}^2 = \overline{7}^2 = \overline{13}^2 = \overline{17}^2$, ou seja, em nenhum dos casos podemos ter $\mathcal{U}(\mathbb{Z}_{20}) = \langle\overline{q}\rangle \times \langle\overline{i}\rangle$.

Exemplo 3.2.9. No item *(viii)*, do Teorema 3.2.7, estamos supondo que $\overline{i} \neq \overline{1}$ em $\mathcal{U}(\mathbb{Z}_{p_j^{m_j}})$, para $j = 1,\ 2$.

Seja $n = 15 = 3 \cdot 5$, então as unidades em $\mathbb{Z}_{15}$ são

$$\mathcal{U}(\mathbb{Z}_{15}) = \{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{18}, \overline{11}, \overline{13}, \overline{14}\}.$$

Devemos ter $\overline{i}^2 = \overline{1}$ e $o(\overline{q}) = o(\overline{iq}) = 4 = (\varphi(3)\varphi(5))/2$. As unidades de ordem 2 em $\mathcal{U}(\mathbb{Z}_{15})$ são $\overline{4},\ \overline{11},\ \overline{14}$ e as unidades de ordem 4 em $\mathcal{U}(\mathbb{Z}_{15})$ são $\overline{2},\ \overline{7},\ \overline{8},\ \overline{13}$.

Tomando $\overline{i} = \overline{4}$, então tem-se que $\overline{4} = \overline{2}^2 = \overline{7}^2 = \overline{8}^2 = \overline{13}^2$. Note ainda que $\overline{i} = \overline{4} = \overline{1}$ em $\mathcal{U}(\mathbb{Z}_3)$. Portanto, em nenhum dos casos podemos ter $\mathcal{U}(\mathbb{Z}_{15}) = \langle\overline{q}\rangle \times \langle\overline{i}\rangle$

Com esses dois exemplos, mostramos que, no caso em que $n = 20$ e $\overline{i} = \overline{2p^m - 1} = \overline{9}$ e, no caso em que $n = 15$ com $\overline{i} = \overline{4}$, não podemos ter $\mathcal{U}(\mathbb{Z}_n) = \langle\overline{q}\rangle \times \langle\overline{i}\rangle$ e, pelo Teorema 3.2.4, o número de componentes simples da álgebra $\mathbb{F}_q G$ não é minimal.

Capítulo 4

Códigos sobre Grupos Metacíclicos

4.1 Aspectos Gerais

Vamos reunir e explorar aqui algumas propriedades básicas da teoria de códigos de grupo.

Sejam $\mathbb{F}$ um corpo finito e G um grupo finito. Vimos que podemos identificar códigos cíclicos sobre $\mathbb{F}^n$ com ideais da álgebra de grupo $\mathbb{F}C_n$, sendo C_n o grupo cíclico de ordem n.

Assim como nos códigos cíclicos, definimos a **distância de Hamming** entre dois elementos $\alpha = \sum_{g\in G} \alpha_g g$ e $\beta = \sum_{g\in G} \beta_g g$ de $\mathbb{F}G$, como:

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

e o **peso** de um elemento α é $w(\alpha) = d(\alpha, 0) = |supp(\alpha)|$. Finalmente, o **peso** de um ideal $I \subset \mathbb{F}G$ é o número

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

Suponhamos que car($\mathbb{F}$) não divide $|G|$. Seja $H \subset G$ um subgrupo qualquer de G. Escrevendo $\widehat{H} = \frac{1}{|H|} \sum_{h\in H} h$, temos que:

- $\widehat{H}^2 = \widehat{H}$

- Se $h \in H$, então $(h-1)\widehat{H} = 0$
- Dados $g_1, g_2 \in G \setminus H$, então $(g_1-1)\widehat{H} = (g_2-1)\widehat{H} \Leftrightarrow g_1\widehat{H} - \widehat{H} = g_2\widehat{H} - \widehat{H} \Leftrightarrow g_1\widehat{H} = g_2\widehat{H} \Leftrightarrow g_1H = g_2H$
- Seja τ um transversal de H em G. Então, para cada $g \in G$, existe um único $t \in \tau$, tal que $g = th, h \in H$. Assim, $(g-1)\widehat{H} = (th-1)\widehat{H} = (t(h-1)+(t-1))\widehat{H} = (t-1)\widehat{H}$.
- Se $g \in G \setminus H$, então $g\widehat{H} \neq \widehat{H}$.

Definição 4.1.1. *Sejam R um anel com unidade e G um grupo. O homomorfismo $\epsilon : RG \longrightarrow R$ dado por*

$$\epsilon\left(\sum_{g\in G}\alpha_g g\right) = \sum_{g\in G}\alpha_g$$

*é chamado **aplicação aumento** de RG e seu núcleo, denotado por $\Delta(G)$, é chamado **ideal de aumento** de RG.*

Proposição 4.1.2. [17, Proposição 3.2.10] *O conjunto $\{g-1 \mid g \in G,\ g \neq 1\}$ é uma base de $\Delta(G)$ sobre R.*

Lema 4.1.3. [17, Corolário 3.6.9] *Sejam R um anel e G um grupo finito, tal que $|G|$ é invertível em R. Então, podemos escrever RG como soma direta de anéis*

$$RG \cong R \oplus \Delta(G).$$

O seguinte resultado pode ser deduzido a partir de [17, Proposição 3.3.3], mas damos a seguir uma demonstração direta.

Lema 4.1.4. *Com as notações acima,* $\dim_{\mathbb{F}}((\mathbb{F}G)\widehat{H}) = (G:H)$.

Demonstração. Considere o seguinte conjunto $\Delta(G)\widehat{H} = \{\alpha\widehat{H}, \alpha \in \Delta(G)\}$. Podemos definir uma multiplicação dos elementos de $\Delta(G)\widehat{H}$ por elementos de $\mathbb{F}$ como $\gamma \cdot \alpha\widehat{H} := (\gamma\alpha)\widehat{H}$. Como $\Delta(G)$ é um ideal de $\mathbb{F}G$, então esta operação está bem definida e o conjunto $\Delta(G)\widehat{H}$ torna-se um $\mathbb{F}$-espaço vetorial.

Afirmação 4.1.5. *O conjunto* $\beta = \{(t-1)\widehat{H}, t \in \tau,\ t \neq 1\}$ *é uma base de* $\Delta(G)\widehat{H}$.

De fato, se $\alpha \in \Delta(G)$, pela Proposição 4.1.2, podemos escrever $\alpha = \sum_{g_i \neq 1} \alpha_i(g_i - 1)$. Como τ é um transversal de H em G, podemos escrever $\alpha = \sum_{t_i \neq 1} \alpha_i(t_i h_j - 1)$ e, portanto, $\alpha\widehat{H} = \sum_{t_i \neq 1} \alpha_i(t_i - 1)\widehat{H}$, o que nos motra que β gera $\Delta(G)\widehat{H}$.

Por fim, seja $\sum_{t_i \neq 1} \alpha_i(t_i - 1)\widehat{H} = 0$ uma combinação linear nula de elementos de $\Delta(G)\widehat{H}$. Deste modo, $\sum_{t_i \neq 1} \alpha_i t_i \widehat{H} = \sum_{t_i \neq 1} \alpha_i \widehat{H}$, uma contradição, pois $t_i \notin H$, o que prova a Afirmação.

Afirmação 4.1.6. $(\mathbb{F}G)\widehat{H} \cong \mathbb{F}\widehat{H} \oplus \Delta(G)\widehat{H}$ *como espaços vetoriais.*

Notemos inicialmente que $\mathbb{F}\widehat{H} \cap \Delta(G)\widehat{H} = 0$. De fato, se existe $\gamma_1\widehat{H} = r\widehat{H} = \sum_{t_j \neq 1} r_j(t_j - 1)\widehat{H}$ implica que, para algum índice j, $t_j \in H$, uma contradição. Agora, pelo Lema 4.1.3, existe um isomorfismo $\Phi : \Delta(G) \oplus \mathbb{F} \longrightarrow \mathbb{F}G$, portanto, para cada $\alpha_1\widehat{H} + \alpha_2\widehat{H} \in \mathbb{F}\widehat{H} \oplus \Delta(G)\widehat{H}$, definimos $\Psi(\alpha_1\widehat{H} + \alpha_2\widehat{H}) = \alpha\widehat{H}$, onde $\alpha = \Phi(\alpha_1 + \alpha_2)$.

1. Ψ está bem definida.

   De fato, se $\alpha_1\widehat{H} + \alpha_2\widehat{H} = \beta_1\widehat{H} + \beta_2\widehat{H}$, então $\alpha_1\widehat{H} = \beta_1\widehat{H}$ e, como $\alpha_1, \beta_1 \in \mathbb{F}$, temos que $\alpha_1 = \beta_1$. Por outro lado, como $\alpha_2, \beta_2 \in \Delta(G)$, então $\alpha_2 = \sum_{t_j \neq 1} r_j(t_j h_i - 1)$ e $\beta_2 = \sum_{t_j \neq 1} s_j(t_j h_i - 1)$ e, assim, $\alpha_2\widehat{H} = \sum_{t_j \neq 1} r_j(t_j - 1)\widehat{H} = \sum_{t_j \neq 1} s_j(t_j - 1)\widehat{H} = \beta_2\widehat{H}$, o que implica que $\sum_{t_j \neq 1}(r_j - s_j)t_j\widehat{H} = \sum_{t_j \neq 1}(r_j - s_j)\widehat{H}$ e isto nos mostra que, para algum índice j_0, $t_{j_o} \in H$ e isto ocorre somente se $r_j = s_j$, consequentemente, $\alpha_2 = \beta_2$.

2. Ψ é um isomorfismo de $\mathbb{F}$-espaços.

   Como $\mathbb{F}$ é um corpo, temos que Φ é um isomorfismo de álgebras, logo Ψ é um $\mathbb{F}$-isomorfismo.

Consequentemente,

$$dim(\mathbb{F}G)\widehat{H} = dim\,\mathbb{F}\widehat{H} + dim\,\Delta(G)\widehat{H} = 1 + ((G:H) - 1) = (G:H).$$

■

Os resultados a seguir estão demonstrados em [4], no caso em que $H \triangleleft G$. Mostraremos que valem, mesmo quando H é um subgrupo qualquer.

Lema 4.1.7. *Seja G um grupo finito e $\mathbb{F}$ um corpo, tal que* $\mathrm{car}(\mathbb{F})$ *não divide a ordem de G. Sejam H, H^*, subgrupos quaisquer de G com $H \subset H^*$. Escrevendo, $e = \widehat{H} - \widehat{H^*}$ tem-se que:*

1. *$dim_{\mathbb{F}}(\mathbb{F}G)e = (G:H) - (G:H^*)$;*
2. *$w((\mathbb{F}G)e) = 2|H|$;*
3. *Se $\mathcal{A}$ é um transversal de H^* em G e τ um transversal de H em H^* contendo 1, então o conjunto*

$$\{r(1-t)\widehat{H} \mid r \in \mathcal{A}, t \in \tau \setminus \{1\}\}$$

é uma base de $(\mathbb{F}G)e$ sobre $\mathbb{F}$.

Demonstração.

(1). Pelo Lema 4.1.4, $dim(\mathbb{F}G)\widehat{H} = (G:H)$ e $dim(\mathbb{F}G)\widehat{H^*} = (G:H^*)$. Entretanto, $\widehat{H} = e + \widehat{H^*}$ e $e\widehat{H^*} = 0$, logo $(\mathbb{F}G)\widehat{H} = (\mathbb{F}G)e \oplus (\mathbb{F}G)\widehat{H^*}$, portanto
$dim_{\mathbb{F}}(\mathbb{F}G)e = (G:H) - (G:H^*)$.

(2). Notemos que $e\widehat{H} = (\widehat{H} - \widehat{H^*})\widehat{H} = e$. Sejam τ um transversal de H em G e $\beta \in (\mathbb{F}G)e$. Existe $\alpha \in \mathbb{F}G$, tal que $\beta = \alpha e$. Agora, $\beta\widehat{H} = \alpha e\widehat{H} = \alpha e = \beta$. Logo $\beta = \sum a_t th = \sum a_t th\widehat{H} = \sum a_t t\widehat{H}$. Se $w(\beta) = |H|$, então $\beta = at\widehat{H} = \alpha e$, implicando que $\widehat{H} \in (\mathbb{F}G)e$ uma contradição, consequentemente, $w(\beta) \geq 2|H|$.

Por fim, seja $h \in H^* \setminus H$. Assim:

$$(1-h)e = (1-h)(\widehat{H} - \widehat{H^*}) = \widehat{H} - \widehat{H^*} - h\widehat{H} + \widehat{H^*} = (1-h)\widehat{H}.$$

Como $supp(h\widehat{H}) \cap supp(\widehat{H}) = \emptyset$ temos que $w((1-h)e) = 2|H|$, o que nos mostra que $w((\mathbb{F}G)e) = 2|H|$.

(3). Sejam $\mathcal{A}$ é um transversal de H^* em G e τ um transversal de H em H^*, contendo 1. Se $r \in \mathcal{A}$ e $t \in \tau$, então $r(1-t)\widehat{H} = r(1-t)\widehat{H}e \in (\mathbb{F}G)e$ uma vez que $(1-t)\widehat{H^*} = 0$. Considere a combinação linear:

$$0 = \sum_{r,t\neq 1} x_{rt}(r(1-t))\widehat{H} = \sum_{r,t\neq 1} x_{rt} r\widehat{H} - \sum_{r,t\neq 1} x_{rt} rt\widehat{H}.$$

o que nos mostra que $\sum_{r,t\neq 1} x_{rt} r\widehat{H} = \sum_{r,t\neq 1} x_{rt} rt\widehat{H}$. No entanto, $t \notin H$ logo $x_{rt} = 0$, mostrando que os elementos de β são linearmente independentes.

Por outro lado,

$$\begin{aligned} |\beta| = |\mathcal{A}|(|\tau| - 1) &= (G : H^*)((H^* : H) - 1) \\ &= (G : H^*)((H^* : H)) - (G : H^*) \\ &= (G : H) - (G : H^*). \end{aligned}$$

■

Corolário 4.1.8. *Seja G um grupo finito e $\mathbb{F}$ um corpo, tal que* $\mathrm{car}(\mathbb{F})$ *não divide a ordem de G. Sejam H_1, H_1^* subgrupos normais de G com $H_1 \subset H_1^* = \{1\}$. Para todo subgrupo H de G, satisfazendo $H \cap H_1^*$ temos:*

1. $dim_{\mathbb{F}}(\mathbb{F}G)(\widehat{H}e) = (G : HH_1) - (G : HH_1^*)$;
2. $w((\mathbb{F}G)e) = 2|HH_1| = 2|H||H_1|$;
3. *Se $\mathcal{A}$ é um transversal de HH_1^* em G e τ um transversal de HH_1 em HH_1^* contendo* 1*, então o conjunto*

$$\{r(1-t)\widehat{HH_1} \mid r \in \mathcal{A}, t \in \tau \setminus \{1\}\}$$

é uma base de $(\mathbb{F}G)(\widehat{H}e)$ sobre $\mathbb{F}$.

Demonstração. Basta ver que $\widehat{H}(\widehat{H_1} - \widehat{H_1^*}) = \widehat{HH_1} - \widehat{HH_1^*}$.

4.2 Códigos Diedrais de Comprimento $2p^m$

Em toda esta seção D_{p^m} denotará o grupo diedral de ordem $2p^m$ e $\mathbb{F}_q$ um corpo finito com q elementos, tal que $\text{mdc}(2p^m, q) = 1$.

Nesta seção, vamos determinar duas decomposições da álgebra $\mathbb{F}_q D_{p^m}$, em soma direta de ideais minimais à esquerda, bem como calcular as dimensões desses ideais e seus respectivos pesos.

Suponhamos que $\mathcal{U}(\mathbb{Z}_{p^m}) = \langle \overline{q} \rangle$. Pelo Teorema 3.1.6, o número de componentes simples da álgebra $\mathbb{F}_q D_{p^m}$ é minimal

Escrevendo $A = \langle a \rangle$, seja

$$A = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_m = \{1\}$$

a cadeia descendente de todos os subgrupos de A, isto é, $H_j = \langle a^{p^j} \rangle$. Então, os idempotentes primitivos da álgebra de grupo $\mathbb{F}_q A$ são

$$e_0 = \widehat{A} \quad e \quad e_j = \widehat{H_j} - \widehat{H_{j-1}}, \ 1 \leq j \leq m.$$

Podemos escrever $e_0 = \widehat{\langle a \rangle}$ como a soma dos idempotentes

$$e_{11} = \left(\tfrac{1+b}{2}\right) e_0 \quad e \quad e_{22} = \left(\tfrac{1-b}{2}\right) e_0.$$

Sendo assim, temos o seguinte:

Teorema 4.2.1. *Sejam D_{p^m}, o grupo diedral e $\mathbb{F}_q$, um corpo finito com q elementos, tal que* $\text{mdc}(2p^m, q) = 1$. *Suponhamos que $\mathcal{U}(\mathbb{Z}_{p^m}) = \langle \overline{q} \rangle$.*

O conjunto dos idempotentes centrais primitivos da álgebra de grupo $\mathbb{F}_q D_{p^m}$ é:

$$\{e_{11}, e_{22}\} \cup \{e_j, \ 1 \leq j \leq m\}.$$

Existe uma equivalência entre códigos sobre grupos metacíclicos gerados por idempotente centrais e códigos abelianos. Esta equivalência, chamada **equivalência combinatorial**, foi introduzida por Sabin e Lomonaco, em [21], e vamos defini-la a seguir.

Definição 4.2.2. *Sejam G e $\mathcal{G}$, dois grupos finitos de mesma ordem e $\mathbb{F}$ um corpo. Sejam $\mathbb{F}G$ e $\mathbb{F}\mathcal{G}$ suas correspondentes álgebras de grupo. Uma* ***equivalência combinatorial*** *é um isomorfismo de espaços vetoriais $\phi : \mathbb{F}G \longrightarrow \mathbb{F}\mathcal{G}$, induzido por uma bijeção $\phi : G \longrightarrow \mathcal{G}$. Os códigos $\mathcal{C} \subset \mathbb{F}G$ e $\widehat{\mathcal{C}} \subset \mathbb{F}\mathcal{G}$, são* ***combinatorialmente equivalentes****, se existe uma equivalência combinatorial $\phi : \mathbb{F}G \longrightarrow \mathbb{F}\mathcal{G}$ tal que $\phi(\mathcal{C}) = \widehat{\mathcal{C}}$.*

Uma importante observação é que códigos combinatorialmente equivalentes possuem a mesma distribuição de peso.

Sejam G um grupo metacíclico com a seguinte apresentação:

$$G = \langle a, b \mid a^m = 1 = b^n,\ \ bab^{-1} = a^i \rangle$$

e $\mathbb{Z}_m \times \mathbb{Z}_n$, com geradores $\tilde{a}$ e $\tilde{b}$. Definimos a bijeção:

$$\begin{aligned} \phi : G &\longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n \\ \phi(a^i b^j) &\longmapsto \tilde{a}^i \tilde{b}^j. \end{aligned}$$

Para qualquer corpo $\mathbb{F}$, ϕ pode ser estendida para o isomorfismo de espaços vetoriais $\phi : \mathbb{F}G \longrightarrow \mathbb{F}(\mathbb{Z}_m \times \mathbb{Z}_n)$.

Lema 4.2.3. [21, Lema 6] *Se $c \in \mathcal{Z}(\mathbb{F}G)$, então $\gamma(\alpha c) = \gamma(\alpha)\gamma(c)$, para todo $\alpha \in \mathbb{F}G$.*

Teorema 4.2.4. [21, Teorema 1]

Considere a equivalência combinatorial:

$$\begin{aligned} \phi : G &\longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n \\ \phi(a^i b^j) &\longmapsto \tilde{a}^i \tilde{b}^j. \end{aligned}$$

Se $\mathcal{C}$ é um código gerado por um idempotente central em $\mathbb{F}G$, então $\phi(\mathcal{C})$ é um ideal da álgebra de grupo $\mathbb{F}(\mathbb{Z}_m \times \mathbb{Z}_n)$. Além disso, se e denota o único gerador idempotente de $\mathcal{C}$, então $\gamma(e)$ é o idempotente gerador de $\gamma(\mathcal{C})$.

Este Teorema mostra que todos os códigos metacíclicos gerados por idempotentes centrais são combinatorialmente equivalentes a códigos abelianos. Sendo assim, no mesmo trabalho [21], Sabin e Lomonaco dedicaram-se ao estudo de códigos à esquerda sobre a álgebra $\mathbb{F}_q G$ e conjecturaram que existem códigos à esquerda minimais na álgebra $\mathbb{F}_q G$, que não são combinatorialmente equivalentes a códigos abelianos. Nosso objetivo, agora, é provar a validade dessa conjectura, isto é, a existência de tais códigos.

Como mencionado anteriormente, vamos escrever os idempotentes primitivos centrais da álgebra $\mathbb{F}_q D_{p^m}$ como soma de idempotentes. O Teorema 4.2.1 nos diz que os idempotentes primitivos centrais são

$$\{e_{11}, e_{22}\} \cup \{e_j,\ 1 \leq j \leq m\}.$$

Podemos escrever cada idempotente primitivo central $e_j, 1 \leq j \leq m$, como

$$e_j = e_{11}^j + e_{22}^j$$

com $e_{11}^j = \left(\frac{1+b}{2}\right) e_j$ e $e_{22}^j = \left(\frac{1-b}{2}\right) e_j$ idempotentes ortogonais. Como e_j é primitivo e central, os idempotentes e_{11}^j e e_{22}^j não podem ser centrais.

Vamos provar que os idempotentes construídos acima são primitivos. É um fato conhecido em característica 0 [12]. Vamos provar que também vale para álgebras de grupos sobre corpos finitos. Para tanto, precisamos de alguns resultados.

Lema 4.2.5. *O centralizador C_b de b em $\mathbb{F}_q D_{p^m}$ é o conjunto:*

$$C_b = \{\gamma_1 + \gamma_2 b \mid \gamma_i \in \mathcal{Z}(\mathbb{F}_q D_{p^m}) \cap \mathbb{F}_q \langle a \rangle\}.$$

Demonstração. Seja $\beta \in C_b$. Como $\beta \in \mathbb{F}_q D_{p^m}$, podemos escrevê-lo da seguinte maneira:

$$\beta = \sum_{j=0}^{p^m} \alpha_j a^j + \sum_{k=0}^{p^m} \beta_k a^k b.$$

Por hipótese, $b\beta b = \beta$, logo multiplicando a equação acima por b em ambos os lados, obtemos:

$$\beta = \sum_{j=0}^{p^m} \alpha_j a^{-j} + \sum_{k=0}^{p^m} \beta_k a^{-k} b.$$

Agora, igualando as equações, tem-se que $\alpha_j = \alpha_{-j}$ e $\beta_k = \beta_{-k}$, consequentemente

$$\begin{aligned}\beta &= \sum_{j=0}^{p^m} \alpha_j (a^j + a^{-j}) + \sum_{k=0}^{p^m} \beta_k (a^k + a^{-k}) b \\ &= \sum_{j=0}^{p^m} \alpha_j \Gamma_{a^j} + \left(\sum_{k=0}^{p^m} \beta_k \Gamma_{a^k} \right) b \\ &= \gamma_1 + \gamma_2 b.\end{aligned}$$

Com isso, mostramos a inclusão $C_b \subseteq \{\gamma_1 + \gamma_2 b \mid \gamma_i \in \mathcal{Z}(\mathbb{F}_q D_{p^m}) \cap \mathbb{F}_q \langle a \rangle\}$. A outra inclusão é imediata, portanto temos a igualdade. ■

Proposição 4.2.6. [16, Proposição 12.1] *Seja B uma álgebra associativa simples. Então seu centro, $\mathcal{Z}(B)$, é um corpo.*

Proposição 4.2.7. *Para cada $j, 1 \leq j \leq m$, os idempotentes e_{11}^j e e_{22}^j são primitivos.*

Demonstração. Sejam $f_1, f_2 \in (\mathbb{F}_q D_{p^m}) e_{11}^j$ tais que $f_1^2 = f_1$, $f_2^2 = f_2$, $f_1 f_2 = 0$ e $e_{11}^j = f_1 + f_2$. Multiplicando à esquerda a igualdade $e_{11}^j = f_1 + f_2$ por f_2, obtemos que $f_2 f_1 = 0 = f_1 f_2$.

Como $(1-b)e_{11}^j = (1-b)f_1 + (1-b)f_2 = 0$, multiplicando esta igualdade, à direita, por f_1 e depois por f_2, obtemos que $(1-b)f_1 = 0 = (1-b)f_2$, o que nos mostra que $f_1 = bf_1$ e $f_2 = bf_2$.

No entanto, $e_{11}^j = \left(\frac{1+b}{2}\right) e_j$ logo $e_{11}^j(1-b) = 0$, uma vez que e_j é central. Podemos, então, concluir $bf_1 b = f_1$ e $bf_2 b = f_2$. Sendo assim, pelo Lema 4.2.5, existem $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathcal{Z}(\mathbb{F}_q D_{p^m})$, tais que $f_1 = \alpha_1 + \alpha_2 b$ e $f_2 = \beta_1 + \beta_2 b$.

Podemos assumir que $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathcal{Z}(\mathbb{F}_q D_{p^m}) e_j$, pois como $\mathbb{F}_q D_{p^m} = \oplus (\mathbb{F}_q D_{p^m}) e_j$, então $\mathcal{Z}(\mathbb{F}_q D_{p^m}) = \oplus \mathcal{Z}((\mathbb{F}_q D_{p^m}) e_j)$ e além disso, $f_1, f_2 \in (\mathbb{F}_q D_{p^m}) e_j$.

Por fim, temos que $f_1 f_2 = (\alpha_1\beta_1 + \alpha_2\beta_2) + (\alpha_1\beta_2 + \alpha_2\beta_1)b = 0$, consequentemente, $\alpha_1\beta_1 + \alpha_2\beta_2 = \alpha_1\beta_2 + \alpha_2\beta_1 = 0$, uma vez que $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathcal{Z}(\mathbb{F}_q D_{p^m}) e_j \cap \mathbb{F}_q \langle a \rangle$.

Somando estas duas igualdades, obtemos que $(\alpha_1 + \alpha_2)(\beta_1 + \beta_2) = 0$, isto implica que $\alpha_1 + \alpha_2 = 0$ ou $\beta_1 + \beta_2 = 0$. Finalmente, se $\alpha_1 + \alpha_2 = 0$, então $f_1 = \alpha_1 - \alpha_1 b = 0$,

pois $f_1 = f_1 e_{11}^j$. Agora, se $\beta_1 + \beta_2 = 0$, então $f_2 = \beta_1 - \beta_1 b = 0$, pelo mesmo motivo. ■

Queremos determinar os parâmetros dos códigos, à esquerda, minimais $I_{j_1} = (\mathbb{F}_q D_{p^m}) e_{11}^j$ e $I_{j_2} = (\mathbb{F}_q D_{p^m}) e_{22}^j$. Para cada j, $1 \leq j \leq m$, considere os subgrupos de $K_j = \langle b \rangle H_j$ e $K_j^* = \langle b \rangle H_{j-1}$. Temos que $K_j \subset K_j^*$ e os elementos $\widehat{K_j}$ e $\widehat{K_j^*}$ são idempotentes de $\mathbb{F}_q D_{p^m}$, podemos então aplicar o Lema 4.1.7 e concluir

$$\dim I_{j_1} = (D_{p^m} : K_j) - (D_{p^m} : K_j^*) = \varphi(p^j) \text{ e } w(I_{j_1}) = 2|K_j| = 4|H_j|.$$

Além disso, como $\dim(\mathbb{F}_q D_{p^m}) e_j = 2\varphi(p^j)$, tem-que $\dim I_{j_2} = \varphi(p^j)$. Falta-nos determinar o peso de I_{j_2}.

Teorema 4.2.8 ([6], Teorema 3.2)**.** *Sejam $\mathbb{F}$ um corpo finito com q elementos e $\mathcal{G}$ um grupo cíclico de ordem $2p^m$, p um primo ímpar, tal que $o(q)=\varphi(p^m)$ em $\mathcal{U}(\mathbb{Z}_{p^m})$. Escrevendo $\mathcal{G} = C \times A$, onde A é o p-subgrupo de Sylow de $\mathcal{G}$ e $C = \{1, t\}$, seu 2-subgrupo de Sylow. Se $\tilde{e}_j$, $1 \leq j \leq m$, denota o idempotente primitivo de $\mathbb{F}A$, então os idempotentes primitivos de $\mathbb{F}\mathcal{G}$ são*

$$\left(\tfrac{1+t}{2}\right) \tilde{e}_j \qquad e \qquad \left(\tfrac{1-t}{2}\right) \tilde{e}_j, \ 1 \leq j \leq m.$$

Vamos provar que estes códigos não centrais também são combinatorialmente equivalentes a códigos abelianos.

Proposição 4.2.9. *Considerando a equivalência combinatorial*

$$\begin{aligned} \gamma : \ D_{p^m} &\longrightarrow \mathcal{G} = A \times C_2 \\ \gamma(a^i b^j) &\longmapsto \tilde{a}^i t^j \end{aligned}$$

então

$$\gamma(I_{j_1}) = \mathbb{F}_q \mathcal{G} \left(\left(\tfrac{1+t}{2}\right) \tilde{e_j} \right) \ e \ \gamma(I_{j_2}) = \mathbb{F}_q \mathcal{G} \left(\left(\tfrac{1-t}{2}\right) \tilde{e_j} \right).$$

Demonstração. Dado $x = \sum_{g \in G} x_g g \left(\tfrac{1 \mp b}{2}\right) e_j \in I_{j_k}$. Então

$$\gamma(x) = \sum_{g \in G} x_g \gamma \left(g \left(\tfrac{1 \mp b}{2}\right) \right) \gamma(e_j) = \sum_{g \in G} x_g \gamma \left(g \left(\tfrac{1 \mp b}{2}\right) \right) \tilde{e_j}.$$

Basta mostrarmos que $\gamma\left(g\left(\frac{1\mp b}{2}\right)\right) = \gamma(g)\left(\frac{1\mp t}{2}\right)$. Vamos analisar em casos separados.

1. $g = a^s$.

$$\begin{aligned}\gamma\left(a^s\left(\tfrac{1\mp b}{2}\right)\right) &= \gamma\left(\tfrac{a^s \mp a^s b}{2}\right)\\ &= \gamma\left(\tfrac{a^s}{2}\right) \mp \gamma\left(\tfrac{a^s b}{2}\right)\\ &= \tfrac{\tilde{a}^s}{2} \mp \tfrac{\tilde{a}^s t}{2}\\ &= \tilde{a}^s\left(\tfrac{1\mp t}{2}\right).\end{aligned}$$

2. $g = a^s b$.

   Como $(a^s b)\left(\frac{1\mp b}{2}\right) = \frac{a^s \mp a^s b}{2}$, segue do caso anterior.

3. $g = b$.

   Assim, $b\left(\frac{1+b}{2}\right) = \left(\frac{1+b}{2}\right)$ e $\gamma\left(b\left(\frac{1+b}{2}\right)\right) = \gamma\left(\frac{1+b}{2}\right) = \frac{1+t}{2}$. Por fim, $b\left(\frac{1-b}{2}\right) = -\left(\frac{1-b}{2}\right)$ e portanto $\gamma\left(b\left(\frac{1-b}{2}\right)\right) = -\gamma\left(\frac{1-b}{2}\right) = -\left(\frac{1-t}{2}\right) = t\left(\frac{1-t}{2}\right)$. ■

Podemos usar este resultado para determinar os parâmetros destes códigos.

Pretendemos agora encontrar outros ideais, à esquerda, minimais que serão isomorfos como ideais aos anteriores, mas com parâmetros diferentes. Antes de prosseguirmos, vamos enunciar um resultado que pode ser encontrado em [17].

Definição 4.2.10. *Sejam G um grupo e G' seu subgrupo comutador. Denotamos por $\Delta(G : G')$ o ideal à esquerda de RG gerado pelo conjunto $\{g - 1 \ : g \in G'\}$.*

Proposição 4.2.11. [17, Proposição 3.6.11] *Seja RG uma álgebra de grupo semissimples. Se G' denota o subgrupo comutador de G e $e_{G'} = \frac{1}{|G'|}\sum_{h\in G'} h$, então podemos escrever:*

$$RG = RGe_{G'} \oplus \Delta(G : G'),$$

onde $RGe_{G'} \cong R(G/G')$ é a soma de todas as componentes simples comutativas de RG e $\Delta(G : G')$ é a soma de todas as outras. Além disso, $Ann(RGe_{G'}) = \Delta(G : G')$.

Agora, pelo Teorema 4.2.1, temos $e_{D'_{p^m}} = e_0$ e $e_j e_0 = 0$, para todo $j,\ 1 \leq j \leq m$, em outras palavras, $e_j \in Ann(\mathbb{F}_q D_{p^m} e_{D'_{p^m}}) = \Delta(D_{p^m} : D'_{p^m})$, consequentemente, para cada $j,\ 1 \leq j \leq m$ temos o isomorfismo:

$$(\mathbb{F}_q D_{p^m}) e_j \cong \mathrm{M}_2(K_j)$$

com K_j um corpo finito contendo $\mathbb{F}_q$.

O próximo Lema nos diz quem é o isomorfismo.

Lema 4.2.12. *Seja R um anel contendo um conjunto de elementos $e_{ij},\ 1 \leq i, j, \leq n$ que satisfazem as seguintes relações:*

$$1 = \sum_{i=1}^{n} e_{ii}, \quad e_{ij}e_{jk} = e_{ik}, \quad e_{ij}e_{lk} = 0, \text{ se } l \neq j.$$

Então $R \cong \mathrm{M_n}(S)$, onde S é o centralizador de $e_{ij},\ 1 \leq i, j, \leq n$ e $S \cong e_{11}Re_{11}$.

Demonstração.A função

$$\sigma : \mathrm{M_n}(S) \longrightarrow R$$

dada por $\sigma((c_{ij})) = \sum c_{ij}e_{ij}$, é um isomorfismo de anéis. ■

Observação 4.2.13. Seja $u \in (\mathbb{F}_q D_{p^m}) e_j$ um elemento idempotente. Sua imagem pelo isomorfismo acima é um idempotente em $\mathrm{M}_2(S)$, logo seu polinômio minimal divide o polinômio $p(x) = x(x-1)$, consequentemente $\sigma^{-1}(u)$ é uma matriz semelhante a matriz $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, logo u é conjugado a e_{11}^j em $(\mathbb{F}_q D_{p^m}) e_j$.

Para cada $j, 1 \leq j \leq m$, considere o seguinte elemento $e_{12}^j = \left(\frac{1+b}{2}\right) a \left(\frac{1-b}{2}\right) e_j$ de $(\mathbb{F}_q D_{p^m}) e_j$.

Lema 4.2.14. *O elemento* $e_{12}^j = \left(\frac{1+b}{2}\right) a \left(\frac{1-b}{2}\right) e_j$ *é diferente de zero.*

Demonstração. Primeiramente, vamos mostrar que o elemento $(a-a^{-1})^2$ é central em $\mathbb{F}_q D_{p^m}$. De fato, $(a-a^{-1})^2 = a^2 - 2 + a^{-2}$ e claramente, $(a-a^{-1})^2$ comuta com a. Assim,

$$\begin{aligned} b(a-a^{-1})^2 b &= ba^2b - 2bb + ba^{-2}b \\ &= a^{-2} - 2 + a^2 \\ &= (a-a^{-1})^2. \end{aligned}$$

Suponhamos que $\left(\frac{1+b}{2}\right) a \left(\frac{1-b}{2}\right) e_j = 0$, então

$$\begin{aligned} (1+b)a(1-b)e_j &= ((a+a^{-1}b)(1-b))e_j \\ &= (a - ab + a^{-1}b - a^{-1})e_j \\ &= ((a-a^{-1})(1-b))e_j \\ &= 0. \end{aligned}$$

Multiplicando esta igualdade por $(a-a^{-1})$, obtemos que $((a-a^{-1})^2(1-b))e_j = 0$. Como $(a-a^{-1})^2$ é central, então $(a-a^{-1})^2 e_j \in \mathcal{Z}(\mathbb{F}_q D_{p^m} e_j)$ o qual é um corpo, portanto teremos que $(1-b)e_j = 0$, o que é uma contradição. ■

Usando o elemento e_{12}^j, vamos definir uma unidade em $(\mathbb{F}_q D_{p^m})e_j$, de fato, sejam $\alpha^j = e_{11}^j + e_{12}^j + e_{22}^j$ e $\beta^j = e_{11}^j - e_{12}^j + e_{22}^j$, então $\alpha^j\beta^j = \beta^j\alpha^j = e_j$, ou seja, $\alpha^j \in \mathcal{U}(\mathbb{F}_q D_{p^m} e_j)$.

A partir de agora, vamos trabalhar dentro da componente simples não comutativa $(\mathbb{F}_q D_{p^m} e_j)$, para tanto vamos omitir o índice j na expressão dos idempotentes.

Conjugando e_{11} por α, dá-nos o elemento $(\alpha)e_{11}(\alpha^{-1}) = e_{11} - e_{12}$, o qual é um idempotente de $(\mathbb{F}_q D_{p^m} e)$, uma vez que a conjugação é um automorfismo. Queremos então determinar os parâmetros do código $I = \mathbb{F}_q D_{p^m}(e_{11} - e_{12})$.

Proposição 4.2.15. *(i) A dimensão do código* $\mathbb{F}_q D_{p^m}(e_{11} - e_{12})$ *é* $\varphi(p^j)$,

(ii) Se, $j \geq 2$, *então o peso do código* $\mathbb{F}_q D_{p^m}(e_{11} - e_{12})$ *é*

$$w(\mathbb{F}_q D_{p^m}(e_{11} - e_{12})) = 12|H_j|.$$

(iii) Se $\mathcal{A}$ é um transversal de $K_j^* = \langle b\rangle H_{j-1}$ em G e τ um transversal de $K_j = \langle b\rangle H_j$ em K^* contendo 1, então o conjunto

$$\{\left(1 + \left(\tfrac{1+b}{2}\right) a \left(\tfrac{1-b}{2}\right)\right) \left(r(1-t)\widehat{K_j} - \tfrac{1}{2}r(1-t)\widehat{K_j}a + \tfrac{1}{2}r(1-t)\widehat{K_j}a^{-1}\right)\}$$

onde $r \in \mathcal{A}$ e $t \in \tau \setminus 1$, é uma base de $\mathbb{F}_q D_{p^m}(e_{11} - e_{12})$ sobre $\mathbb{F}_q$.

Demonstração.

(i). Como a conjugação é um automorfismo e $\alpha e_{11}\alpha^{-1} = e_{11} - e_{12}$, então $dim((\mathbb{F}_q D_{p^m}))e_{11} = dim(\mathbb{F}_q D_{p^m}(e_{11} - e_{12})) = \varphi(p^j)$.

(ii) Inicialmente, como os idempotentes e_{11} e $(e_{11} - e_{12})$ são primitivos, os ideais, à esquerda, $\mathbb{F}_q D_{p^m} e_{11}$ e $\mathbb{F}_q D_{p^m}(e_{11} - e_{12})$, são minimais, portanto devemos ter $\mathbb{F}_q D_{p^m} e_{11} \cap \mathbb{F}_q D_{p^m}(e_{11} - e_{12}) = 0$ ou $\mathbb{F}_q D_{p^m} e_{11} \cap \mathbb{F}_q D_{p^m}(e_{11} - e_{12}) = \mathbb{F}_q D_{p^m}(e_{11} - e_{12})$. Se a última igualdade ocorrer, então $e_{11} - e_{12} = z e_{11}$ e multiplicando por e_{22}, tem-se que $e_{12} = 0$, uma contradição, o que nos mostra que $\mathbb{F}_q D_{p^m} e_{11} \cap \mathbb{F}_q D_{p^m}(e_{11} - e_{12}) = 0$.

Seja $\gamma \in \mathbb{F}_q D_{p^m}(e_{11} - e_{12})$ um elemento não nulo. Existe $\beta \in \mathbb{F}_q D_{p^m}$ tal que

$$\begin{aligned}
\gamma &= \beta(e_{11} - e_{12}) \\
&= \beta e_{11} - \beta e_{12} \\
&= \beta e_{11} - \beta e_{11}\left(\tfrac{a}{2} - \tfrac{ba^{-1}}{2}\right) \\
&= \beta e_{11}\left(1 - \tfrac{a}{2} + \tfrac{a^{-1}}{2}\right).
\end{aligned}$$

Assim sendo, existe um elemento $\tilde{\beta} \in \mathbb{F}_q D_{p^m} e_{11}$, tal que $\gamma = \tilde{\beta}\left(1 - \tfrac{a}{2} + \tfrac{a^{-1}}{2}\right)$. Pelo Corolário 4.1.8, e denotando $K_j = \langle b\rangle H$ e $K_j^* = \langle b\rangle H_{j-1}$, o conjunto

$$\{r(1-t)\widehat{K_j} \mid r \in \mathcal{A}, t \in \tau \setminus \{1\}\},$$

onde $\mathcal{A}$ é um transversal de K_j^* em D_{p^m} e τ um transversal de K_j em K_j^* contendo 1, é uma base de $(\mathbb{F}_q D_{p^m})e_{11}$ sobre $\mathbb{F}_q$, logo podemos escrever γ como a seguinte soma:

$$\begin{aligned}\gamma &= \left(\sum_{k,s}\alpha_{ks}r_k(1-t_s)\widehat{K_j}\right)\left(1-\tfrac{a}{2}+\tfrac{a^{-1}}{2}\right)\\ &= \sum_{k,s}\alpha_{ks}r_k(1-t_s)\widehat{K_j}-\tfrac{1}{2}\sum_{k,s}\alpha_{ks}r_k(1-t_s)\widehat{K_j}a+\tfrac{1}{2}\sum_{k,s}\alpha_{ks}r_k(1-t_s)\widehat{K_j}a^{-1}.\end{aligned}$$

Como $\widehat{K_j}=\left(\frac{1+b}{2}\right)\widehat{H_j}$, então

$$\begin{aligned}\gamma &= \sum_{k,s}\alpha_{ks}r_k(1-t_s)\left(\tfrac{1+b}{2}\right)\widehat{H_j}-\tfrac{1}{2}\sum_{k,s}\alpha_{ks}r_k(1-t_s)\left(\tfrac{1+b}{2}\right)a\widehat{H_j}+\\ &+\tfrac{1}{2}\sum_{k,s}\alpha_{ks}r_k(1-t_s)\left(\tfrac{1+b}{2}\right)a^{-1}\widehat{H_j}\\ &= [\tfrac{1}{2}\sum_{k,s}\alpha_{ks}r_k(1-t_s)+\tfrac{1}{2}\sum_{k,s}\alpha_{ks}r_k(1-t_s)b-\tfrac{1}{4}\sum_{k,s}\alpha_{ks}r_k(1-t_s)a-\\ &-\tfrac{1}{4}\sum_{k,s}\alpha_{ks}r_k(1-t_s)a^{-1}b+\tfrac{1}{4}\sum_{k,s}\alpha_{ks}r_k(1-t_s)a^{-1}+\tfrac{1}{4}\sum_{k,s}\alpha_{ks}r_k(1-t_s)ab]\widehat{H_j}\\ &= [\tfrac{1}{2}\sum_{k,s}\alpha_{ks}r_k(1-t_s)-\tfrac{1}{4}\sum_{k,s}\alpha_{ks}r_k(1-t_s)a+\tfrac{1}{4}\sum_{k,s}\alpha_{ks}r_k(1-t_s)a^{-1}\\ &+\tfrac{1}{2}\sum_{k,s}\alpha_{ks}r_k(1-t_s)b+\tfrac{1}{4}\sum_{k,s}\alpha_{ks}r_k(1-t_s)ab-\tfrac{1}{4}\sum_{k,s}\alpha_{ks}r_k(1-t_s)a^{-1}b]\widehat{H_j}.\end{aligned}$$

Escrevendo $\gamma_1=\frac{1}{2}\sum_{k,s}\alpha_{ks}r_k(1-t_s)$, podemos escrever

$$\gamma=[\gamma_1-\tfrac{1}{2}\gamma_1a+\tfrac{1}{2}\gamma_1a^{-1}+\gamma_1b+\tfrac{1}{2}\gamma_1ab-\tfrac{1}{2}\gamma_1a^{-1}b]\widehat{H_j}.$$

Vamos analisar em casos separados.

Caso 1: $\gamma_1=\frac{1}{2}\sum_{k,s}\alpha_{ks}r_k(1-t_s)$ com $t_s\neq t_u$ se $s\neq u$.

Sejam t_{s_1} e $t_{s_2}\in supp(\gamma)$. Assim, os elementos $r_{s_1}t_{s_1}, r_{s_1}t_{s_1}a, r_{s_1}t_{s_1}a^{-1}, r_{s_2}t_{s_2}, r_{s_2}t_{s_2}a$ e $r_{s_2}t_{s_2}a^{-1}$ são todos distintos entre si e distintos dos demais elementos do $supp(\gamma)$. De fato, como $r_s\in\mathcal{A}$ então $r_{s_1}t_{s_1}\neq r_{s_2}t_{s_2}$, uma vez que $t_{s_1}\neq t_{s_2}$.

Se $r_{s_1}t_{s_1}=r_{s_2}a$, então $t_{s_1}=r_{s_1}^{-1}r_{s_2}a$. Como a ordem do elemento $r_{s_1}^{-1}r_{s_2}a$ é p^m, então a ordem de t_{s_1} é p^m, o que não pode ocorrer, pois, por hipótese, $t_{s_1}\in H_{j-1}$ e $j\geq 2$ donde $|H_{j-1}|=p^{m-(j-1)}<p^m$.

O caso $r_{s_1}t_{s_1}=r_{s_2}a^{-1}$ prova-se de maneira análoga.

Se tivéssemos $r_{s_1}t_{s_1}=r_{s_2}t_{s_2}a$, então a ordem do elemento $t_{s_1}t_{s_2}^{-1}$ seria p^m, pois a ordem do elemento a^2 é p^m.

O caso $r_{s_1}t_{s_1}=r_{s_2}t_2a^{-1}$ prova-se e maneira análoga.

Acabamos de provar que, nesse caso, existem pelo menos seis elementos pertencentes ao $supp(\gamma_1-\frac{1}{2}\gamma_1a+\frac{1}{2}\gamma_1a^{-1})$, que são distintos de todos os outros elementos do

$supp(\gamma_1 - \frac{1}{2}\gamma_1 a + \frac{1}{2}\gamma_1 a^{-1})$. Isso implica que existem pelo menos seis elementos pertencentes ao $supp(\gamma_1 b - \frac{1}{2}\gamma_1 ab + \frac{1}{2}\gamma_1 a^{-1}b)$, que são distintos de todos os outros elementos do $supp(\gamma_1 b - \frac{1}{2}\gamma_1 ab + \frac{1}{2}\gamma_1 a^{-1}b)$, donde $w(\gamma) \geq 12|H_j|$.

Caso 2: $\gamma_1 = \frac{1}{2}\sum_k \alpha_k r_k(1-t)$

Neste caso, podemos escrever:

$$\gamma_1 - \tfrac{1}{2}\gamma_1 a + \tfrac{1}{2}\gamma_1 a^{-1} = \left(\sum_k \tfrac{\alpha_k}{2} r_k - \sum_k \tfrac{\alpha_k}{4} r_k a + \sum_k \tfrac{\alpha_k}{4} r_k a^{-1}\right)(1-t).$$

Se $r_{k_1} = r_{k_2} a$, então $r_{k_1} a^{-1} = r_{k_2}$, donde

$\gamma_1 - \frac{1}{2}\gamma_1 a + \frac{1}{2}\gamma_1 a^{-1} =$

$$= \left(\left(\tfrac{\alpha_{k_1}}{2} - \tfrac{\alpha_{k_2}}{4}\right) r_{k_1} - \tfrac{\alpha_{k_1}}{4} r_{k_1} a + \left(\tfrac{\alpha_{k_1}}{2} + \tfrac{\alpha_{k_2}}{4}\right) r_{k_2} + \tfrac{\alpha_{k_2}}{4} r_{k_2} a^{-1}\right)(1-t) +$$

$$+ \left(\sum_{k \neq k_1, k_2} \frac{\alpha_k}{2} r_k - \sum_{k \neq k_1, k_2} \frac{\alpha_k}{4} r_k a + \sum_{k \neq k_1, k_2} \frac{\alpha_k}{4} r_k a^{-1}\right)(1-t).$$

Os elementos $r_{k_1}, r_{k_1} a, r_{k_2}$ e $r_{k_2} a^{-1}$ são distintos. De fato, se $r_{k_1} = r_{k_2} a^{-1}$, então $r_{k_2} a = r_{k_2} a^{-1}$, donde $a^2 = 1$, o que não pode ocorrer. Pelo mesmo motivo, não podemos ter a igualdade $r_{k_2} = r_{k_1} a$.

Por fim, se $\alpha_{k_2} = 2\alpha_{k_1}$, então o coeficiente do elemento r_{k_1} é zero, mas os coeficientes dos elementos $r_{k_1} a, r_{k_2}$ e $r_{k_2} a^{-1}$ são não nulos, o que prova que, se $r_{k_1} = r_{k_2} a$, existem pelos menos três distintos em $supp(\gamma_1 - \frac{1}{2}\gamma_1 a + \frac{1}{2}\gamma_1 a^{-1})$.

Se $r_{k_1} = r_{k_2} a$ e $r_{k_1} = r_{k_3} a^{-1}$, então:

$\gamma_1 - \frac{1}{2}\gamma_1 a + \frac{1}{2}\gamma_1 a^{-1} =$

$= \left(\left(\tfrac{\alpha_{k_1}}{2} - \tfrac{\alpha_{k_2}}{4} + \tfrac{\alpha_{k_3}}{4}\right) r_{k_1} + \left(-\tfrac{\alpha_{k_1}}{4} - \tfrac{\alpha_{k_3}}{4}\right) r_{k_1} a + \left(\tfrac{\alpha_{k_1}}{4} + \tfrac{\alpha_{k_2}}{2}\right) r_{k_2} + \tfrac{\alpha_{k_2}}{4} r_{k_2} a^{-1} + \tfrac{\alpha_{k_3}}{4} r_{k_3}\right)(1-t) + \left(\sum_{k \neq k_1, k_2, k_3} \tfrac{\alpha_k}{2} r_k - \sum_{k \neq k_1, k_2, k_3} \tfrac{\alpha_k}{4} r_k a + \sum_{k \neq k_1, k_2, k_3} \tfrac{\alpha_k}{4} r_k a^{-1}\right)(1-t).$

Resolvendo um sistema linear, prova-se que existem pelos menos três elementos distintos em:

$$\left(\left(\tfrac{\alpha_{k_1}}{2} - \tfrac{\alpha_{k_2}}{4} + \tfrac{\alpha_{k_3}}{4}\right) r_{k_1} + \left(-\tfrac{\alpha_{k_1}}{4} - \tfrac{\alpha_{k_3}}{4}\right) r_{k_1} a + \left(\tfrac{\alpha_{k_1}}{4} + \tfrac{\alpha_{k_2}}{2}\right) r_{k_2} + \tfrac{\alpha_{k_2}}{4} r_{k_2} a^{-1} + \tfrac{\alpha_{k_3}}{4} r_{k_3}\right).$$

Sendo assim, esses elementos distintos multiplicados por $(1-t)$ e por $(1-t)b$ serão distintos e existirão pelo menos 12 elementos distintos de todos os outros elementos do $supp(\gamma)$ donde $w(\gamma) \geq 12|H_j|$.

Se $r_{k_1} = r_{k_2}a$ e $r_{k_1}a = r_{k_4}$, então Se $r_{k_1} = r_{k_4}a^{-1}$ e, neste caso, prova de maneira análoga ao caso anterior, que $w(\gamma) \geq 12|H_j|$.

Se $r_{k_1} = r_{k_2}a$ e $r_{k_1}a = r_{k_4}a^{-1}$, então

$\gamma_1 - \frac{1}{2}\gamma_1 a + \frac{1}{2}\gamma_1 a^{-1} =$

$= \left(\left(\frac{\alpha_{k_1}}{2} - \frac{\alpha_{k_4}}{4}\right) r_{k_1} + \left(\frac{-\alpha_{k_1}}{4} - \frac{\alpha_{k_4}}{4}\right) r_{k_1}a + \left(\frac{\alpha_{k_2}}{2} + \frac{\alpha_{k_1}}{4}\right) r_{k_2} + \frac{\alpha_{k_2}}{4} r_{k_2}a^{-1} - \frac{\alpha_{k_4}}{4} r_{k_2}a + \frac{\alpha_{k_4}}{2} r_{k_4}\right).$

Novamente, existem pelo menos três elementos distintos em $supp(\gamma_1 - \frac{1}{2}\gamma_1 a + \frac{1}{2}\gamma_1 a^{-1})$, donde existem pelo menos 12 elementos distintos em $supp(\gamma)$ logo $w(\gamma) \geq 12|H_j|$.

Por fim, se $r_{k_1} = r_{k_2}a$ e $r_{k_2} = r_{k_3}a$ ou $r_{k_2} = r_{k_3}a^{-1}$ e se $r_{k_1} = r_{k_2}a$ e $r_{k_2}a = r_{k_3}a^{-1}$, segue dos casos anteriores que $w(\gamma) \geq 12|H_j|$.

Caso 3: $\gamma_1 = \frac{1}{2}\left(\sum_k \alpha_k r_k(1-t_1) + \sum_s \alpha_s r_s(1-t_2)\right)$ com $t_1 \neq t_2$.

Pelo Caso 2, existem pelos menos três elementos distintos pertencentes ao $supp(\frac{1}{2}\left(\sum_k \alpha_k r_k(1-t_1)\right)$, da forma $r_{k_1}t_1$ ou $r_{k_2}t_1 a$ ou $r_{k_3}t_1 a^{-1}$. Da mesma maneira, existem pelos menos três elementos distintos pertencentes ao $supp(\frac{1}{2}\left(\sum_k \alpha_k r_k(1-t_2)\right)$, da forma $r_{k_4}t_2$ ou $r_{k_5}t_2 a$ ou $r_{k_6}t_2 a^{-1}$. Como, neste caso, $t_1 \neq t_2$, segue do Caso 1, que os elementos $r_{k_1}t_1$, $r_{k_2}t_1 a$, $r_{k_3}t_1 a^{-1}$, $r_{k_4}t_2$, $r_{k_5}t_2 a$ e $r_{k_6}t_2 a^{-1}$ são todos distintos entre si e distintos dos demais elementos do $supp(\gamma)$, donde $w(\gamma) \geq 12|H_j|$.

Caso 4: $\gamma_1 = \frac{1}{2}r(1-t)$.

Por hipótese, $j \geq 2$, donde $a, a^{-1} \notin H_{j-1}$, consequentemente os elementos r, rt, ra, ra^{-1}, rta, rta^{-1}, são todos distintos, uma vez que $t \in H_{j-1}$ e $a \neq a^{-1}$. Logo, se $j \geq 2$, então o peso de γ é $w(\gamma) = 12|H_j|$.

(iii). Novamente, aplicando Corolário 4.1.8 e denotando $K_j = \langle b \rangle H_j$ e

$K_j^* = \langle b \rangle H_{j-1}$, o conjunto:

$$\{r(1-t)\widehat{K_j} \mid r \in \mathcal{A}, t \in \tau \setminus \{1\}\},$$

onde $\mathcal{A}$ é um transversal de K^* em D_{p^m} e τ um transversal de K_j em K_j^* contendo 1, é uma base de $(\mathbb{F}_q D_{p^m})e_{11}$ sobre $\mathbb{F}_q$.

Por fim, como a conjugação é um automorfismo de $(\mathbb{F}_q D_{p^m})e$, o conjunto:

$$\{\alpha(r(1-t)\widehat{K_j})\alpha^{-1} \mid r \in \mathcal{A}, t \in \tau \setminus \{1\}\}$$

onde $\mathcal{A}$ é um transversal de K_j^* em D_{p^m} e τ um transversal de K_j em K_j^* contendo 1, é uma base de $(\mathbb{F}_q D_{p^m})(e_{11} - e_{12})$ sobre $\mathbb{F}_q$. Vamos agora desmembrar o produto $\alpha(r(1-t)\widehat{K_j})\alpha^{-1}$. Primeiramente, notemos que

$\widehat{K_j}e_{11} = \left(\frac{1+b}{2}\right)\widehat{H_j}e_{11} = e_{11}$,

$\widehat{K_j}e_{22} = \left(\frac{1+b}{2}\right)\widehat{H_j}e_{22} = 0$,

$\widehat{K_j}e_{12} = \left(\frac{1+b}{2}\right)\widehat{H_j}\left(\frac{1+b}{2}\right)a\left(\frac{1-b}{2}\right)e = \left(\frac{1+b}{2}\right)a\left(\frac{1-b}{2}\right)\widehat{H_j}e = \left(\frac{1+b}{2}\right)a\left(\frac{1-b}{2}\right)e = e_{12}$.

Portanto, temos que $\widehat{K_j}\alpha^{-1} = \widehat{K_j}(e_{11} - e_{12} + e_{22}) = e_{11} - e_{12}$ e o produto

$$\begin{aligned}\alpha(r(1-t))\widehat{K_j}\alpha^{-1} &= \alpha(r(1-t))(e_{11} - e_{12}) \\ &= e_{11}(r(1-t))e_{11} - e_{11}(r(1-t))e_{12} + e_{12}(r(1-t))e_{11} - \\ &\quad - e_{12}(r(1-t))e_{12} + e_{22}(r(1-t))e_{11} - e_{22}(r(1-t))e_{12}.\end{aligned}$$

Podemos tomar $r, t \in \langle a \rangle$, pois se $r = a^s b$, então $r\widehat{K_j} = a^s\widehat{K_j}$. Assim $(1-t)e = (1-t)\widehat{H_j}$, logo:

- $r(1-t)e_{11} = r(1-t)e\left(\frac{1+b}{2}\right) = r(1-t)\widehat{H_j}\left(\frac{1+b}{2}\right) = r(1-t)\widehat{K_j}$,
- $r(1-t)e_{12} = r(1-t)e\left(\frac{1+b}{2}\right)a\left(\frac{1-b}{2}\right) = r(1-t)\widehat{K_j}a\left(\frac{1-b}{2}\right)$,
- $e_{11}(r(1-t))e_{11} = \left(\frac{1+b}{2}\right)r(1-t)\widehat{K_j}$,
- $e_{12}(r(1-t))e_{11} = \left(\frac{1+b}{2}\right)a\left(\frac{1-b}{2}\right)r(1-t)\widehat{K_j}$,
- $e_{22}(r(1-t))e_{11} = \left(\frac{1-b}{2}\right)r(1-t)\widehat{K_j}$,
- $e_{11}(r(1-t))e_{12} = \left(\frac{1+b}{2}\right)r(1-t)\widehat{K_j}a\left(\frac{1-b}{2}\right)$,

- $e_{12}(r(1-t))e_{12} = \left(\frac{1+b}{2}\right) a \left(\frac{1-b}{2}\right) r(1-t)\widehat{K_j}a \left(\frac{1-b}{2}\right)$,
- $e_{22}(r(1-t))e_{12} = \left(\frac{1-b}{2}\right) r(1-t)\widehat{K_j}a \left(\frac{1-b}{2}\right)$.

Com isso,

- $e_{11}(r(1-t))e_{11}+e_{12}(r(1-t))e_{11}+e_{22}(r(1-t))e_{11} = \left(1 + \left(\frac{1+b}{2}\right) a \left(\frac{1-b}{2}\right)\right) r(1-t)\widehat{K_j}$,
- $e_{11}(r(1-t))e_{12}+e_{12}(r(1-t))e_{12}+e_{22}(r(1-t))e_{12} = \left(1 + \left(\frac{1+b}{2}\right) a \left(\frac{1-b}{2}\right)\right) r(1-t)\widehat{K_j}a \left(\frac{1-b}{2}\right)$.

Consequentemente,
$\alpha(r(1-t)\widehat{K_j})\alpha^{-1} = \left(1 + \left(\frac{1+b}{2}\right) a \left(\frac{1-b}{2}\right)\right) \left(r(1-t)\widehat{K_j} - \frac{1}{2}r(1-t)\widehat{K_j}a + \frac{1}{2}r(1-t)\widehat{K_j}a^{-1}\right)$.

■

Finalizaremos este capítulo mostrando que se, $m \geq 2$, então os códigos $\mathbb{F}_q D_{p^m}(e_{11} - e_{12})$, não são combinatorialmente equivalentes a nenhum código abeliano de comprimento $2p^m$. Utilizaremos uma técnica desenvolvida por Ferraz e Polcino Milies em [6].

Seja A um p-grupo abeliano. Para cada subgrupo H de A, tal que $A/H \neq \{1\}$ é cíclico, vamos construir um idempotente de $\mathbb{F}_q A$. Como A/H é cíclico de ordem p^k, existe um único subgrupo H^* de A contendo H, tal que $|H^*/H| = p$. Definimos $e_H = \widehat{H} - \widehat{H^*}$.

Sendo assim, temos os seguintes

Teorema 4.2.16. [6, Lema 5 e Teorema 4.] *Sejam p um primo ímpar e A um p-grupo abeliano de expoente p^r. Suponhamos que $\mathcal{U}(\mathbb{Z}_{p^r}) = \langle \bar{q} \rangle$, então os elementos e_H definidos acima, juntamente com $e_A = \widehat{A}$, formam o conjunto de idempotentes primitivos de $\mathbb{F}_q A$.*

Teorema 4.2.17. [6, Teorema 4.2] *Sejam p um primo ímpar e A, um grupo abeliano de expoente $2p^r$. Escreva $A = E \times B$, onde E é um 2-grupo abeliano elementar e B é um p-grupo. Então os idempotentes primitivos de $\mathbb{F}_q A$ são produtos da forma $e.f$, onde e é um idempotente primitivo de $\mathbb{F}_q E$ e f é um idempotente primitivo de $\mathbb{F}_q B$.*

Estamos trabalhando sob a hipótese $\mathcal{U}(\mathbb{Z}_{p^m}) = \langle \bar{q} \rangle$. Seja A um grupo abeliano de ordem $2p^m$. Novamente, escrevendo $A = C_2 \times B$, sendo $C_2 = \langle t \rangle$ o grupo cíclico de ordem 2 e B um p-grupo. Os idempotentes primitivos de $\mathbb{F}_q A$ são da forma $e = \left(\frac{1+t}{2}\right) e_H$ ou $e = \left(\frac{1-t}{2}\right) e_H$ com $e_H = \widehat{H} - \widehat{H^*}$, onde H é um subgrupo de B, tal que B/H é cíclico de ordem p^i.

O seguinte resultado está implícito em [6].

Teorema 4.2.18. *Denotando $I_e = (\mathbb{F}_q A)e$, temos*

i) dim $I_e = \varphi(p^i)$

ii) $w(I_e) = 4|H|$.

Vamos denotar o ideal $\mathbb{F}_q D_{p^m}(e_{11} - e_{12})$ por I. Suponhamos então que I seja combinatorialmente equivalente a um código J de $\mathbb{F}_q A$. Existem dois casos possíveis:

1. $J = \oplus_{k=1}^{s} I_{e_{H_{i_k}}}$

   Neste caso, $\dim J = \sum_{k=1}^{s} \varphi(p^{i_k}) = \dim I = \varphi(p^j)$. Se existir algum expoente $i_k > j$, então teremos $\dim J > \dim I$, uma contradição. Assim $i_k < j$ para todo k. Entretanto,

   $$\sum_{k=0}^{s} \varphi(p^{i_k}) = (p^{i_1-1} + p^{i_2-1} + \cdots + p^{i_s-1})(p-1) = p^{j-1}(p-1).$$

   Isto implica que

   $$p^{i_1-1} + p^{i_2-1} + \cdots + p^{i_s-1} = p^{j-1}.$$

   Seja $i_t = \min\{i_1, \cdots, i_s\}$. Dividindo a igualdade acima por p^{i_t}, tem-se que

   $p^{i_1-i_t} + \cdots + 1 + \cdots + p^{i_s-i_t} = p^{j-i_t}$, o que implica que $p \mid 1$, uma contradição.

2 $J = I_e$

   Neste caso, devemos ter $w(J) = w(I_e) = 4|H| = w(I)$, mas, pela Proposição 4.2.15, sabemos que $w(I) = 12|H|$, consequentemente, I não é combinatorialmente equivalente a nenhum código abeliano.

Assim, temos provado o seguinte:

Teorema 4.2.19. *Seja D_{p^m} o grupo diedral com a apresentação:*

$$D_{p^m} = \langle a, b \mid a^{p^m} = 1 = b^2,\ \ bab = a^{-1} \rangle.$$

e $\mathbb{F}_q$ um corpo finito com q elementos, tal que $\mathrm{mdc}(2p^m, q) = 1$ *e $\mathcal{U}(\mathbb{Z}_{p^m}) = \langle \bar{q} \rangle$.*

Então, dentro de cada componente simples não comutativa da álgebra $\mathbb{F}_q D_{p^m}$, existe um código à esquerda minimal que não é combinatorialmente equivalente a códigos abelianos.

4.3 Uma família de exemplos

Sejam D_{p^m} o grupo diedral de ordem $2p^m$ e $\mathbb{F}_q$ um corpo finito com q elementos, tal que $\mathrm{mdc}(2p^m, q) = 1$. Vimos, na seção anterior que, se $\mathcal{U}(\mathbb{Z}_{p^m}) = \langle \overline{q} \rangle$, então os idempotentes centrais primitivos da álgebra $\mathbb{F}_q D_{p^m}$ são

$$\{e_{11}, e_{22}\} \cup \{e_j,\ 1 \leq j \leq m\},$$

onde

$$e_0 = \widehat{A} \quad e \quad e_j = \widehat{H_j} - \widehat{H_{j-1}},\ \ 1 \leq j \leq m$$

e

$$e_{11} = \left(\tfrac{1+b}{2}\right) e_0 \quad e \quad e_{22} = \left(\tfrac{1-b}{2}\right) e_0.$$

Posteriormente, para cada $j,\ 1 \leq j \leq m$, construímos os idempotentes $e_{11}^j - e_{12}^j$, que foram obtidos através da conjugação dos idempotentes primitivos não centrais e_{11}^j pelos elementos $\alpha = e_{11}^j + e_{12}^j + e_{22}^j$, onde

$$e_{11}^j = \left(\tfrac{1+b}{2}\right) e_j, \quad e_{12}^j = \left(\tfrac{1+b}{2}\right) a \left(\tfrac{1-b}{2}\right) e_j \ \text{ e } \ e_{22}^j = \left(\tfrac{1-b}{2}\right) e_j.$$

No endereço eletrônico, *www.codetables.de*, encontram-se registros dos códigos mais eficientes conhecidos. Fixados o comprimento e a dimensão, estão descritos os códigos lineares sobre $\mathbb{F}_q$com maiores pesos conhecidos, nos casos em que $q = 2, 3, 4, 5, 7, 8, 9$.

Quando o comprimento do código é 18 e a dimensão é 2, os maiores pesos conhecidos são:

- 12 sobre $\mathbb{F}_2$;
- 13 sobre $\mathbb{F}_3$;
- 14 sobre $\mathbb{F}_4$;
- 15 sobre $\mathbb{F}_5$;
- 15 sobre $\mathbb{F}_7$;
- 16 sobre $\mathbb{F}_8$ e
- 16 sobre $\mathbb{F}_9$.

Em cada um desses casos, se exibe o código particular que atinge esse peso, um para cada caso.

Vamos mostrar, a seguir, que, se a característica do corpo é diferente de 2, 3, 5 e 7, podemos encontrar códigos de comprimento 18 e dimensão 2 cujo peso é 15. Para tanto, utilizaremos o idempotente $e_{11}^1 - e_{12}^1$. O interessante desse exemplo é que uma **mesma construção** descreve todos os códigos sobre esta família infinita de corpos.

Sejam D_9, o grupo diedral de ordem 18, e $\mathbb{F}_q$ um corpo de característica diferente de 2, 3, 5 e 7. Considere o subgrupo normal H_1 de D_9, gerado pelo elemento a^3. Mais explicitamente, $H_1 = \{1, a^3, a^6\}$. Pela Proposição 4.2.15, o conjunto $\{(1-a), (1-a^2)\}$ é uma base do ideal $\mathbb{F}_q D_9(e_{11}^1)$ sobre $\mathbb{F}_q$, uma vez que, neste caso, $\mathcal{A} = \{1\}$ e $\tau = \{1, a, a^2\}$.

Seja γ um elemento não nulo do ideal $\mathbb{F}_q D_9(e_{11}^1 - e_{12}^1)$. Vimos, na demonstração da Proposição 4.2.15, que podemos escrever o elemento γ como

$$\gamma = (\gamma_1 - \tfrac{1}{2}\gamma_1 a + \tfrac{1}{2}\gamma_1 a^{-1} + \gamma_1 b + \tfrac{1}{2}\gamma_1 ab - \tfrac{1}{2}\gamma_1 a^{-1}b)\widehat{H_1},$$

onde, neste caso, $\gamma_1 = \frac{1}{2}(\alpha(1-a)+\beta(1-a^2))$. Como $a^{-1} = a^8$ e, $\gamma_1 = \frac{1}{2}\left((\alpha+\beta) - \alpha a - \beta a^2\right)$, então

$$2\gamma_1 - \gamma_1 a + \gamma_1 a^8 = (\alpha+2\beta) + (-3\alpha-2\beta)a + (-2\beta+\alpha)a^2 + \beta a^3 + (\alpha+\beta)a^8.$$

Consequentemente:

$$\begin{aligned}(2\gamma_1 - \gamma_1 a + \gamma_1 a^8)\widehat{H_1} &= (\alpha+2\beta)\widehat{H_1} + (-3\alpha-2\beta)a\widehat{H_1} + (-2\beta+\alpha)a^2\widehat{H_1} + \beta a^3\widehat{H_1} \\ &\quad + (\alpha+\beta)a^8\widehat{H_1} \\ &= (\alpha+3\beta)\widehat{H_1} + (-3\alpha-2\beta)a\widehat{H_1} + (2\alpha-\beta)a^2\widehat{H_1},\end{aligned}$$

uma vez que $a^3\widehat{H_1} = \widehat{H_1}$ e $a^8\widehat{H_1} = a^2\widehat{H_1}$.

Por fim,

$$\left((2\gamma_1 + \gamma_1 a - \gamma_1 a^8)b\right)\widehat{H_1} = (3\alpha+\beta)b\widehat{H_1} + (-\alpha+2\beta)ab\widehat{H_1} + (-2\alpha-3\beta)a^2b\widehat{H_1}.$$

Assim,

$$\gamma = \left((\alpha+3\beta) + (-3\alpha-2\beta)a + (2\alpha-\beta)a^2 + (3\alpha+\beta)b + (-\alpha+2\beta)ab + (-2\alpha-3\beta)a^2b\right)\widehat{H_1}.$$

Um cálculo direto mostra que, se a característica do corpo $\mathbb{F}_q$ for diferente de 2, 3, 5 e 7, então no máximo um dos coeficientes do elemento acima pode ser zero. Logo, o peso de γ é $w(\gamma) \geq 15$. Temos , então, provado a seguinte:

Proposição 4.3.1. *Sejam $\mathbb{F}_q$ um corpo finito com q elementos e D_9 o grupo diedral de ordem 18. Se a característica de $\mathbb{F}_q$ for diferente de 2, 3, 5 e 7, então:*

1. *A dimensão do código $\mathbb{F}_q D_9(e_{11}^1 - e_{12}^1)$ é $\varphi(3) = 2$;*

2. *O peso do código $\mathbb{F}_q D_9(e_{11}^1 - e_{12}^1)$ é $w(\mathbb{F}_q D_9(e_{11}^1 - e_{12}^1)) = 15$.*

Capítulo 5

Conclusões

Sejam $\mathbb{F}_q$ um corpo finito com q elementos e G um grupo finito, tal que $mdc(q, |G|) = 1$. Neste trabalho, verificamos, inicialmente, que se G é um grupo metacíclico que cinde, não abeliano, de ordem $p^m\ell^n$, onde p e ℓ são números primos ímpares, então o número de componentes simples da álgebra $\mathbb{F}_qG$ é minimal e os idempotentes centrais primitivos podem ser obtidos a partir da estrutura do grupo G.

Sejam D_{p^m} o grupo diedral finito de ordem $2p^m$, com p primo ímpar, e $\mathbb{F}_q$ um corpo finito com q elementos, tal que $mdc(q, 2p^m) = 1$. Verificamos alguns ideais à esquerda minimais da álgebra $\mathbb{F}_qD_{p^m}$ produzem códigos mais eficiêntes que códigos abelianos minimais de comprimento $2p^m$, respondendo, assim, uma conjectura de Sabin e Lomonaco de 1995.

Referências Bibliográficas

[1] G. K. Bakshi, M. Raka, *Minimal cyclic codes of lenght p^nq*, Finite Fields and Their Applications, 9 (2003), 432-448.

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

[3] F. S. Dutra, *Sobre Códigos Diedrais e Quatérnios*, Tese de Doutorado.

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

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

[6] R. A. Ferraz, C. Polcino Milies, *Idempotents in group algebras and minimal abelian codes*, Finite Fields and Their Applications, 13 (2007), 382-393.

[7] R. A. Ferraz, J. J. Simón-Pinero, *Central Units in Metacyclic Integral Group Rings*, Communications in Algebra, 36:10, (2008), 3708-3722.

[8] E.G. Goodaire, E. Jespers, C. Polcino Milies, *Alternative loop rings*, North Holland Math. Studies n.184, Amsterdam, 1996.

[9] M. Grassl, *Bounds on the minimum distance of linear codes*. Disponível *on line* em http://www.codetables.de, consultado em 27/09/2013.

[10] C.E. Hempel, *Metacyclic Groups*, Communications in Algebra, 28:8, (2000), 3865-3897.

[11] N. Jacobson, *Basic Algebra I*, Second Edition, W. H. Freeman and Company, New York, 1985.

[12] E. Jespers, G. Leal, C. Polcino Milies, *Units of Integral Group Rings of some Metacyclic Groups*, Canad. Math. Bull., 37 (2) (1994), 228-237.

[13] G. A. Jones, J. M. Jones, *Elementary Number Theory*, Springer undergraduate mathematics series, Springer-Verlag, London, 1998.

[14] G. A. Jones, J. M. Jones, *Information and Coding Theory*, Springer undergraduate mathematics series, Springer-Verlag, London, 2000.

[15] D. S. Passman, *The Algebraic Structure of Group Rings*, Wiley-Intersciense, New York, 1977.

[16] R. S. Pierce, *Associative Algebras*, Springer-Verlag, New York, 1982.

[17] C. Polcino Milies, S.K. Sehgal, *An Introduction to Group Rings*, Kluwer Academic Publishers, Dordrecht, Boston, London, 2001.

[18] D. J. S. Robinson, *A Course in the Theory of Groups*, Springer-Verlag, New York, 1996.

[19] J.J. Rotman, *An Introduction to the Theory of Groups*, Fourth Edition, Springer-Verlag, New York, 1995.

[20] R. E. Sabin, *On Row-Cyclic Codes with Algebraic Structure* , Designs, Codes and Cryptography, 4, 145-155, (1994).

[21] R. E. Sabin, S. J. Lomonaco, *Metacyclic Error-Correcting Codes*, AAECC 6 (1995), 191-210.

[22] S. H. Wientraub, *Galois Theory*, Springer-Verlag, New York, 2006.