POLIANA LUZ MOREIRA

CÓDIGOS METACÍCLICOS

Dissertação apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós-Graduação em Matemática, para obtenção do título de *Magister Scientiae*.

VIÇOSA
MINAS GERAIS - BRASIL
2010

POLIANA LUZ MOREIRA

CÓDIGOS METACÍCLICOS

Dissertação apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós-Graduação em Matemática, para obtenção do título de *Magister Scientiae*.

APROVADA: 26 de fevereiro de 2010.

Alegria Gladys Chalom	Raul Antonio Ferraz
Paula Murgel Veloso	Ana Cristina Vieira (Co-orientadora)

Marinês Guerreiro
(Orientadora)

A Deus,

meu eterno e grande Amigo,
meu porto seguro, a razão de meu existir.

"Sim, grandes coisas fez o Senhor por nós, e por isso estamos alegres."
Sl 126,3.

Agradecimentos

A Deus pelo dom da vida, pelas bênçãos derramadas em todos os momentos e principalmente nos de maiores dificuldades ao longo dessa caminhada.

À Universidade Federal de Viçosa, pela possibilidade de realizar meus estudos da graduação e mestrado neste ambiente tranquilo e lindo.

À Fundação de Amparo à Pesquisa do Estado de Minas Gerais, FAPEMIG, pelo apoio financeiro.

Aos meus pais Francisco e Cida, com quem pude compartilhar minhas alegrias, conquistas, momentos de tristeza e que mesmo de longe me faziam sentir melhor com suas palavras, suas orações e pelo o amor incondicional que sentem por mim.

Aos meus irmãos e meu cunhado, Ana Kelly, Renato e Elias, pelas orações, pelo amor e pela torcida para que tudo desse certo nesta etapa da minha vida.

Ao meu sobrinho Davi, pelo sorriso e amor oferecidos a mim a cada visita e que sem saber me davam forças para voltar e continuar os estudos.

Ao meu namorado Marcos, pela paciência, pelo companheirismo, pela atenção e pelo amor dedicados durante esses anos que com certeza foram muito importantes.

Aos meus tios e primos, que sempre torcem por mim, pelas orações e pelo amor oferecido.

À minha orientadora Marinês, pela paciência e disponibilidade do tempo que tinha livre para me ajudar e direcionar meus estudos para que conseguisse concluir a dissertação.

Às co-orientadoras pela atenção quando foi possível.

À banca examinadora pela presença no dia da defesa e pelas sugestões feitas para melhorar a dissertação.

À minha turma de mestrado, Tatiana, Lílian, Vinícius, Marcos R., João, Luciano, Marcos B. e Diogo, pelos vários momentos de estudos no DMA, pelas ajudas quando necessitei, pelos apertos que passamos e pela alegria de ficarmos livres do exame de qualificação.

À Mara, secretária do Mestrado, que ajudou muito nos ouvindo nos momentos de tristeza e desânimo e nos incentivando sempre com suas palavras amigas e com suas orações.

A todos os meus amigos da graduação, pela convivência mesmo que de longe e pouca, sei da torcida de todos.

Aos amigos de Valadares, principalmente à Luana, pela preocupação de saber notícias, pelo carinho e pelas orações.

Aos professores e funcionários do DMA, pela formação acadêmica e pela amizade.

A todos que direta ou indiretamente contribuíram para que esse sonho se realizasse.

MUITO OBRIGADA!

Sumário

Resumo

MOREIRA, Poliana Luz, M.Sc., Universidade Federal de Viçosa, fevereiro, 2010. **Códigos Metacíclicos**. Orientadora: Marinês Guerreiro. Co-orientadoras: Sônia Maria Fernandes e Ana Cristina Vieira.

Neste trabalho, estudamos os códigos corretores de erros que são ideais na álgebra de grupo $\mathbb{F}G(M, N, R)$ sobre um corpo $\mathbb{F}$ de característica 2, onde o grupo subjacente é metacíclico, não abeliano, de ordem ímpar e possui a seguinte apresentação:

$$G(M, N, R) = \langle a, b : a^M = b^N = 1,\ ba = a^R b \rangle,$$

onde $mdc(M, R) = 1$, $R^N \equiv 1 (mod\, M)$ e $R \neq 1$. Utilizamos a teoria de representações dos grupos metacíclicos para encontrar os idempotentes geradores dos códigos centrais minimais de $\mathbb{F}G(M, N, R)$ e provamos que estes códigos são combinatorialmente equivalentes a certos códigos abelianos, cujas distâncias mínimas não são as melhores possíveis. No entanto, alguns destes códigos centrais minimais se decompõem em soma direta de ideais (códigos) minimais à esquerda, que possuem distâncias mínimas maiores que as dos códigos abelianos de comprimento e dimensão comparáveis. Desta maneira, o estudo de certos códigos metacíclicos minimais (à esquerda) se torna mais interessante. Uma descrição detalhada da teoria de representações dos grupos metacíclicos e alguns resultados sobre álgebras de grupo que auxiliam a determinação dos códigos metacíclicos são apresentados preliminarmente, bem como alguns resultados sobre códigos cíclicos.

Abstract

MOREIRA, Poliana Luz, M.Sc., Universidade Federal de Viçosa, February, 2010. **Metacyclic Codes**. Adviser: Marinês Guerreiro. Co-Advisers: Sônia Maria Fernandes and Ana Cristina Vieira.

In this work, we study the error-correction codes that are ideals in the group algebra $\mathbb{F}G(M, N, R)$ over a field $\mathbb{F}$ of characteristic 2, where the underlying group is a non-abelian metacyclic of odd order and has the following presentation:

$$G(M, N, R) = \langle a, b : a^M = b^N = 1,\ ba = a^R b \rangle,$$

where $gcd(M, R) = 1$, $R^N \equiv 1 (mod\, M)$ and $R \neq 1$. We use the theory of representations of the metacyclic groups to find the idempotent generators of the minimal central codes of $\mathbb{F}G(M, N, R)$ and prove that these codes are combinatorically equivalent to certain abelian codes whose minimum distances are not the best. However, some of these minimal central codes break down into direct sum of minimal left ideals (left codes), which have minimum distances greater than those abelian codes of comparable length and size. Thus, the study of certain metacyclic minimal (left) codes becomes more interesting. A detailed description of the theory of representations of metacyclic groups and some results on group algebras that support the determination of metacyclic codes are initially presented , as well as some results on cyclic codes.

Introdução

Os códigos corretores de erros participam do nosso cotidiano de inúmeras formas, estando presentes, por exemplo, sempre que fazemos uso de informações digitalizadas, tais como assistir a um programa de televisão, falar ao telefone, ouvir um CD de música, assistir a um filme em DVD, mandar um recado para alguém via *pager* ou navegar na Internet.

Um código corretor de erros é, em essência, um modo organizado de acrescentar algum dado adicional a cada informação que se queira transmitir ou armazenar, que permita, recuperar a informação, detectar e corrigir erros. A Teoria dos Códigos é um campo de investigação atual e muito ativo, tanto do ponto de vista científico quanto tecnológico, sendo pesquisado por diversas áreas do conhecimento como, Matemática, Computação, Engenharia Elétrica e Estatística entre outras.

Na década de 40, quando os computadores eram máquinas muito caras, apenas instituições de grande porte como o governo e as universidades tinham condições de mantê-los, usando-os para executar tarefas numéricas complexas, como calcular a órbita precisa de Marte. O Laboratório Bell de Tecnologia possuía tais computadores e Richard W. Hamming deparou-se com estas máquinas em 1947, cujo acesso era restrito aos fins de semanas. Nesta época, as máquinas paravam seu funcionamento quando detectavam um erro e o trabalho não podia ser concluído. Assim, Hamming ficou pensando nesta questão, embora este problema não fosse novo, pois já ocorria nas centrais telefônicas e de telégrafos.

Na Teoria de Códigos Corretores de Erros, um conjunto A finito qualquer com q elementos é chamado de **alfabeto**. Os elementos de A são chamados **letras** ou **dígitos**. Uma sequência de n elementos de A é chamada **palavra de comprimento** n. Um **código corretor de erros** é um subconjunto próprio qualquer de A^n, onde A^n é o conjunto de todas as palavras de comprimento n sobre A.

A pesquisa de Hamming tinha como objetivo principal a transmissão de uma cadeia de caracteres composta de 0 e 1, ou seja, o alfabeto do código era $\{0, 1\}$. Para exemplificar, consideremos o código $\mathcal{C}$ formado por todas as possíveis palavras

binárias de comprimento 3:

000	001	010	100
011	101	110	111

Se o canal de transmissão sofrer interferência, a palavra recebida pode ser diferente da palavra enviada. Por exemplo, se queremos enviar a palavra 010 pertencente ao código descrito acima e a enviamos por um canal onde ocorra um erro, então a palavra recebida pode ser, por exemplo, 011. Esta palavra pertence ao código e não será recebida como errada, pior ainda, esta palavra terá outro significado, que poderá alterar a mensagem.

Obter precisão num canal de transmissão que sofra interferências requer dígitos de redundância nas palavras e, portanto, palavras mais longas e isto diminui o fluxo de informação. Um dos objetivos da teoria dos códigos corretores de erros é desenvolver métodos para enviar mensagens rápidas de modo que seja possível detectar e corrigir erros. Por exemplo, em canais em que pode acontecer no máximo um erro por palavra, a concepção de "paridade"ajuda a detectar erros com rapidez e confiabilidade ao mesmo tempo.

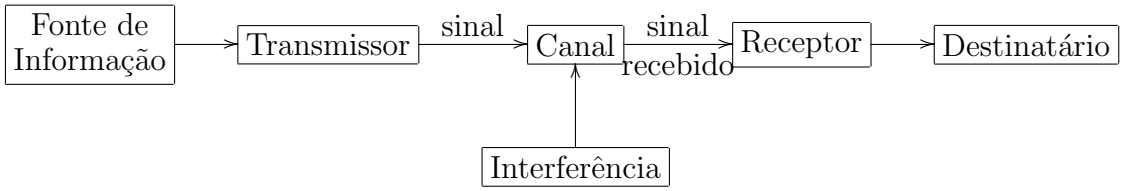
As comunicações entre máquinas e entre seus componentes internos estão sujeitas a interferências internas e externas. Hamming interessou-se pelos erros que ocorriam internamente nos computadores e desenvolveu um código corretor de erro único e códigos que detectam até dois erros e corrigem erro único, mas somente em abril de 1950 seu trabalho foi publicado no "The Bell System Technical Journal".

Durante os três anos de elaboração destes códigos e da publicação de seu trabalho, Hamming publicou alguns memorandos conforme sua pesquisa evoluía. Ele queria fazer um código mais eficiente e indagou se era possível construir um código corretor de um único erro, onde as palavras teriam quatro dígitos de informações e menos do que oito dígitos de redundâncias por palavra. Esta questão foi respondida indiretamente em outubro de 1948 por C. E. Shannon em seu artigo intitulado "A Mathematical Theory of Communication", publicado no "The Bell System Technical Journal". O artigo de C. E. Shannon deu início a um novo campo da Engenharia Elétrica, a Teoria da Informação, cuja ênfase era o estudo do canal de comunicação que recebia interferência durante as transmissões de dados, e um ramo dela chamou-se Códigos Corretores de Erros. A partir deste artigo, podemos dizer que houve um desenvolvimento contínuo e bastante significativo da Teoria dos Códigos.

Em seu artigo, Shannon enfatiza que o problema fundamental da comunicação

é a reprodução exata de cada caracter de modo como este foi enviado, pois cada mensagem tem um significado próprio.

O esquema de representação de um sistema de comunicação que Shannon propôs em seu trabalho é utilizado até hoje e, iremos reproduzi-lo a seguir:



Este esquema consiste essencialmente em cinco partes:

(1) **Fonte de Informação**: produz uma mensagem ou sequência de mensagens para serem transmitidas a um terminal receptor.

(2) **Transmissor ou codificador**: opera a mensagem produzindo um sinal para transmissão sobre um canal.

(3) **Canal**: meio usado para transmitir o sinal do transmissor para o receptor.

(4) **Receptor ou Decodificador**: desempenha a operação inversa feita pelo transmissor, reconstruindo a mensagem.

(5) **Destinatário**: pessoa (ou objeto) para quem a mensagem é destinada.

À medida que a Teoria de Códigos Corretores de Erros foi avançando, novas técnicas foram desenvolvidas incorporando estruturas algébricas mais elaboradas. Para nossos propósitos, consideramos **códigos lineares** que são subespaços próprios do espaço vetorial $\mathbb{F}_q^n$, onde o alfabeto escolhido é um corpo finito $\mathbb{F}_q$ com q elementos. Em particular, um código linear $\mathcal{C}$ é dito **cíclico** se, para qualquer palavra $(v_0, v_1, ..., v_{n-1})$ em $\mathcal{C}$, a palavra $(v_{n-1}, v_0, ..., v_{n-2})$ também está em $\mathcal{C}$. Os códigos cíclicos são muito utilizados por formarem uma classe de códigos lineares que possui bons algoritmos de codificação e de decodificação.

Observamos que o espaço vetorial $\mathbb{F}_q^n$ pode ser construído, por exemplo, através de um isomorfismo entre $\mathbb{F}_q^n$ e a álgebra de grupo $\mathbb{F}_q C_n$, onde C_n é o grupo cíclico de ordem n. Este isomorfismo estabelece uma correspondência entre os códigos cíclicos de $\mathbb{F}_q^n$ e os ideais do anel de grupo $\mathbb{F}_q C_n$. Desta maneira, os códigos cíclicos serão vistos como ideais na álgebra de grupo $\mathbb{F}_q C_n$.

Mais geralmente, se $\mathbb{F}$ é um corpo e G um grupo, ambos finitos, dizemos que um código em uma álgebra de grupo $\mathbb{F}G$ é um ideal desta álgebra. Estes são os chamados **códigos de grupo**.

Este trabalho tem como objetivo estudar os códigos de grupo metacíclicos, ou seja, os ideais da álgebra de grupo $\mathbb{F}G(M, N, R)$, onde o grupo $G(M, N, R)$ subjacente é metacíclico não abeliano de ordem ímpar e $\mathbb{F}$ é um corpo de característica 2. Um tal grupo é uma extensão de um grupo finito $\mathbb{Z}_M$ por um grupo finito $\mathbb{Z}_N$ e tem uma apresentação da forma:

$$\langle a, b : a^M = b^N = 1,\ ba = a^R b\rangle,$$

onde $mdc(M, R) = 1$, $R^N \equiv 1(mod\, M)$ e $R \neq 1$.

No Capítulo 1, apresentaremos noções básicas sobre módulos e álgebras e alguns resultados sobre semissimplicidade de anéis e álgebras, culminando no Teorema de Wedderburn-Artin (Teorema 1.3.26). Em seguida, apresentaremos as definições e principais resultados sobre anéis de grupo, demonstrando o Teorema de Maschke (Teorema 1.4.25) que estabelece condições necessárias e suficientes para que uma anel de grupo seja semissimples e, assim, se decomponha em uma soma direta de ideais minimais bilaterais.

Para o caso em que o grupo G é finito e $\mathbb{F}$ é um corpo tal que $car(\mathbb{F}) \nmid |G|$, a álgebra de grupo é semissimples e, como tal, pode ser decomposta em uma soma direta de ideais minimais bilaterais, cada um deles gerado por um idempotente central primitivo. Desta maneira para descrever os códigos de grupo, basta conhecermos os seus geradores idempotentes. Uma ferramenta importante para esta finalidade é a Teoria de Representações e Caracteres de Grupos, da qual apresentaremos, ao final do Capítulo 1, as definições básicas e principais resultados utilizados ao longo deste trabalho.

Como nosso foco são os códigos metacíclicos, descreveremos no Capítulo 2, a estrutura dos grupos metacíclicos e suas representações irredutíveis. Trabalharemos principalmente com grupos metacíclicos do tipo $G = G(M, N, R)$ cuja apresentação é dada por: $\langle a, b : a^M = 1, b^N = 1, ba = a^R b\rangle$, onde $mdc(M, R) = 1$, $R^N \equiv 1(mod\ M)$, $R \neq 1, N \neq 1$ e sobre corpos de característica 2, de modo que a álgebra $\mathbb{F}G$ seja semissimples. Primeiramente, trabalharemos sobre um corpo L que contenha suficientes raízes da unidade de modo que todas as representações de G sejam absolutamente irredutíveis sobre L. Depois utilizaremos essas representações absolutamente irredutíveis para descrever as representações irredutíveis de G sobre um subcorpo de L.

O Capítulo 3 é o principal deste trabalho. Iniciaremos com uma introdução à Teoria de Códigos Corretores de Erros, para estabelecer a linguagem utilizada nesta

teoria. Em seguida, descreveremos os códigos cíclicos como ideais na álgebra de grupo $\mathbb{F}_q C_n$ do grupo cíclico finito C_n de ordem $n > 1$ e, para os códigos cíclicos minimais, utilizaremos a estrutura de subgrupos do grupo cíclico para calcular os idempotentes centrais primitivos geradores desses códigos. Além disso, citaremos alguns resultados de Ferraz e Milies [18], que determinam sob que condições as álgebras de grupo abelianos sobre corpos finitos têm o mesmo número de componentes simples que as álgebras de grupo racionais de tais grupos.

Considerando a álgebra de grupo $\mathbb{F}G$ do grupo metacíclico $G = G(M, N, R)$ de ordem ímpar sobre um corpo $\mathbb{F}$ de característica 2, na sequência do trabalho, estabeleceremos uma correspondência biunívoca entre o conjunto dos códigos centrais minimais não isomorfos em $\mathbb{F}G$ e o conjunto das representações irredutíveis não equivalentes de G sobre $\mathbb{F}$. A partir deste resultado faremos a decomposição da álgebra de grupo $\mathbb{F}G$ em códigos centrais minimais utilizando um conjunto completo de representações irredutíveis não equivalentes de G.

Verificaremos ainda que existe uma equivalência combinatorial entre os códigos metacíclicos centrais e certos códigos abelianos. Para descrever os códigos metacíclicos centrais minimais em $\mathbb{F}G$, associaremos cada um destes códigos a um código cíclico e com esta correspondência obteremos mais informações sobre eles como, por exemplo, a qual código cada um destes códigos metacíclicos centrais minimais é combinatorialmente equivalente.

Uma vez que vários resultados sobre códigos abelianos já são conhecidos, estaremos interessados em códigos metacíclicos que não sejam combinatorialmente equivalentes a códigos abelianos, ou seja, em códigos metacíclicos centrais minimais que se decompõem em códigos minimais à esquerda. Esta decomposição em códigos minimais à esquerda primeiramente será feita com os códigos centrais minimais em LG, onde L é o corpo de decomposição de G sobre um corpo primo de característica 2 e depois apresentaremos um algoritmo para encontrar esta decomposição em $\mathbb{F}G$, onde $\mathbb{F}$ é um corpo finito (qualquer) de característica 2.

Apresentaremos dois exemplos de grupos metacíclicos: os diedrais de ordem $2n$ e os quatérnios generalizados de ordem $4n$. Para descrever os idempotentes centrais primitivos geradores dos códigos diedrais e quatérnios minimais, que possuem ordem par, não podemos utilizar as técnicas descritas nas seções anteriores, uma vez que a característica do corpo, neste caso, precisa ser ímpar. Descreveremos brevemente o trabalho de tese de doutorado de Dutra [9], no qual novas técnicas para encontrar os idempotentes geradores dos códigos diedrais e quatérnios são explicitadas e também desenvolvidas técnicas de codificação e de decodificação de tais códigos.

Capítulo 1

Preliminares

Neste capítulo apresentamos definições e resultados que são utilizados ao longo do trabalho. Optamos por omitir as demonstrações que podem ser encontradas em [3], [4], [10], [18] e [21].

1.1 Módulos e Álgebras

A noção de módulo, que introduzimos abaixo, é de fundamental importância no desenvolvimento da teoria de anéis de grupos e de representações de grupos. Todos os anéis citados neste trabalho possuem unidade. As demonstrações omitidas podem ser encontradas no Capítulo 2 da referência [4].

Definição 1.1.1 *Seja R um anel. Diz-se que um conjunto não vazio M é um* ***módulo à esquerda*** *sobre R (ou um R-**módulo à esquerda**) se M é um grupo abeliano em relação a uma operação, que indicaremos por $+$, e está definida uma lei de composição externa que a cada par $(a, m) \in R \times M$ associa um elemento $am \in M$ tal que, para todos $a, b \in R$ e para todos $m, m_1, m_2 \in M$, verifica-se:*

1. $(a + b)m = am + bm$,
2. $a(m_1 + m_2) = am_1 + am_2$,
3. $a(bm) = (ab)m$,
4. $1m = m$.

De forma análoga pode-se definir a noção de R-**módulo à direita**, considerando a multiplicação à direita por elementos do anel. Usaremos a expressão R-módulo para indicar R-módulo à esquerda.

Observamos que se $\mathbb{F}$ é um corpo, então o conceito de $\mathbb{F}$-módulos coincide com a noção de espaços vetoriais sobre o corpo $\mathbb{F}$.

Em particular, um anel é sempre um módulo sobre ele mesmo. Quando considerarmos um dado anel R como um módulo à esquerda ou à direita sobre ele mesmo, usaremos a notação ${}_RR$ e R_R, respectivamente.

Definição 1.1.2 *Seja R um anel comutativo. Um R-módulo A é dito uma R-**álgebra** se existe uma multiplicação definida em A tal que, com a adição dada em A e esta multiplicação, A é um anel e valem as seguintes condições:*

$$r(ab) = (ra)b = a(rb), \tag{1.1}$$

para todo $r \in R$ e para todos $a, b \in A$.

Se A, como um anel, possui uma unidade 1_A, então a condição (1.1) da definição acima implica que o conjunto $R \cdot 1_A$ (que é um anel isomorfo a R) está contido no centro de A.

Definição 1.1.3 *Seja M um módulo sobre um anel R. Um subconjunto não vazio $N \subset M$ é dito um R-**submódulo** de M se:*

1. *para todos $x, y \in N$, temos $x + y \in N$ e*
2. *para todo $r \in R$ e para todo $n \in N$, temos $rn \in N$.*

*Se R é comutativo e M é uma R-álgebra, dizemos que N é uma R-**subálgebra** de M se é um R-submódulo e um subanel de M.*

Definição 1.1.4 *Sejam R um anel comutativo e A e B dois R-módulos. Uma aplicação $f : A \to B$ é chamada R-**homomorfismo** se, para todos $a_1, a_2 \in A$ e $r \in R$, temos:*

1. *$f(a_1 + a_2) = f(a_1) + f(a_2)$ e*
2. *$f(ra_1) = rf(a_1)$.*

Observamos que se R é um anel comutativo e A e B são R-álgebras, então uma aplicação $f : A \to B$ é chamada **homomorfismo de R-álgebras** se é um homomorfismo de anéis e um R-homomorfismo. Quando o homomorfismo de R-álgebras f é bijetor, dizemos que f é um isomorfismo de R-álgebras e denotamos por $A \simeq B$. Denotamos por $Hom_R(A, B)$, o conjunto de todos os homomorfismos de R-álgebras $f : A \to B$.

Definição 1.1.5 *Um conjunto $S = \{s_i\}_{i \in I}$ de elementos de um R-módulo M é dito um **conjunto de geradores** de M se $M = RS$, isto é, se todo elemento de M pode ser escrito como uma combinação linear (finita) de elementos de S com coeficientes em R.*

Definição 1.1.6 *Um conjunto $S = \{s_i\}_{i \in I}$ de elementos de um R-módulo M é dito **linearmente independente** (ou, simplesmente, R-**livre**), se qualquer combinação linear (finita) de elementos de S com coeficientes em R tal que*

$$r_{i_1} s_{i_1} + r_{i_2} s_{i_2} + \cdots + r_{i_t} s_{i_t} = 0$$

implica $r_{i_1} = r_{i_2} = \cdots = r_{i_t} = 0$.

Definição 1.1.7 *Um conjunto $S = \{s_i\}_{i \in I}$ de elementos de um R-módulo M é dito uma **base** de M sobre R (ou, simplesmente, R-base) se é linearmente independente e é um conjunto de geradores de M.*

Nem todo R-módulo possui uma base como acontece com os espaços vetoriais. Quando um R-módulo possui uma base, recebe um nome especial que é dado a seguir.

Definição 1.1.8 *Um R-módulo M é dito **livre** se possui uma base.*

1.2 Produto Tensorial

Nesta seção apresentamos uma importante construção na Teoria de Módulos: o produto tensorial. As demonstrações dos resultados apresentados nesta seção serão omitidas e podem ser encontradas no Capítulo 2 da referência [4].

Definição 1.2.1 *Sejam R um anel, M um R-módulo à direita e N um R-módulo à esquerda. Seja A um grupo abeliano aditivo. Uma **aplicação balanceada** f do produto cartesiano $M \times N$ em A é uma aplicação que satisfaz:*

1. $f(m_1 + m_2, n) = f(m_1, n) + f(m_2, n)$,

2. $f(m, n_1 + n_2) = f(m, n_1) + f(m, n_2)$,

3. $f(m, rn) = f(mr, n)$,

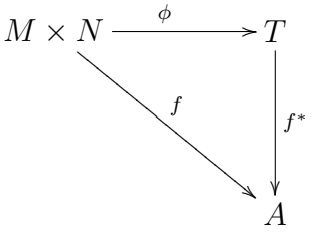
para todos $m, m_1, m_2 \in M, n, n_1, n_2 \in N, r \in R$.

O produto tensorial de módulos é usualmente definido via uma propriedade universal.

Definição 1.2.2 *Sejam M e N um R-módulo à direita e um R-módulo à esquerda, respectivamente. Um grupo abeliano T, juntamente com uma aplicação balanceada $\phi : M \times N \to T$, é dito um* ***produto tensorial*** *de M e N se valem as seguintes propriedades:*

1. *Os elementos da forma $\phi(m, n)$, para todos $m \in M, n \in N$ geram T (como um grupo aditivo).*

2. *Para qualquer grupo abeliano aditivo A e qualquer aplicação balanceada $f : M \times N \to A$, existe um homomorfismo $f^* : T \to A$ tal que $f = f^* \circ \phi$ (neste caso, chamamos f^** ***fator de*** *f por ϕ), isto é, tal que o seguinte diagrama é comutativo:*



Denotamos o produto tensorial T por $M \otimes_R N$, ou simplesmente $M \otimes N$ quando não for necessário especificar o anel R e $\phi(m, n) = m \otimes n$, para todo $m \in M$ e para todo $n \in N$.

Teorema 1.2.3 *Sejam M e N um R-módulo à direita e um R-módulo à esquerda, respectivamente. Então o produto tensorial de M e N existe e é único, a menos de isomorfismo.*

Nos resultados a seguir, listamos as principais propriedades do produto tensorial que serão utilizadas ao longo deste trabalho.

Proposição 1.2.4 *Seja M um R-módulo à direita e sejam N_1 e N_2 R-módulos à esquerda. Então*

$$M \otimes (N_1 \oplus N_2) \simeq (M \otimes N_1) \oplus (M \otimes N_2).$$

Teorema 1.2.5 *Seja N um R-módulo à esquerda. Então $R \otimes_R N \simeq N$.*

Definição 1.2.6 *Sejam R e S dois anéis. Um grupo aditivo M é dito um (R,S)-**bimódulo** se M é um R-módulo à esquerda e um S-módulo à direita e temos $r(ms) = (rm)s$, para todos $r \in R$, $s \in S$ e $m \in M$.*

Proposição 1.2.7 *Sejam M um R-módulo à direita, N um (R,S)-bimódulo e L um S-módulo à esquerda. Então*

$$M \otimes_R (N \otimes_S L) \simeq (M \otimes_R N) \otimes_S L.$$

Proposição 1.2.8 *Sejam M e N um R-módulo à direita e um R-módulo à esquerda, respectivamente, e assuma que S é um outro anel tal que M é um (S,R)-bimódulo. Então $M \otimes_R N$ é um S-módulo à esquerda, com a multiplicação dada por*

$$\lambda \left(\sum_i m_i \otimes n_i \right) = \sum_i \lambda m_i \otimes n_i, \text{ para } \lambda \in R.$$

Particularmente, se M e N são R-álgebras, então $M \otimes N$ é uma R-álgebra conforme o resultado a seguir.

Proposição 1.2.9 *Sejam M e N álgebras sobre um anel comutativo R (M também pode ser considerado um (R,R)-bimódulo de modo óbvio). Então $M \otimes N$ é uma álgebra sobre R com a multiplicação dada por*

$$\left(\sum_i m_i \otimes n_i \right) \left(\sum_j m_j \otimes n_j \right) = \sum_{i,j} m_i m_j \otimes n_i n_j.$$

Proposição 1.2.10 *Se M e N são R-módulos livres, com bases $\beta = \{m_i\}_{i \in I}$ e $\widetilde{\beta} = \{n_j\}_{j \in J}$, respectivamente, então $M \otimes N$ é um R-módulo livre com base $\beta \otimes \widetilde{\beta} = \{m_i \otimes n_j\}$, para todo $i \in I$ e para todo $j \in J$. Em particular, se β e $\widetilde{\beta}$ são finitas, então* $\dim(M \otimes N) = \dim M \cdot \dim N$.

1.3 Semissimplicidade e o Teorema de Wedderburn-Artin

Sabemos que todo subespaço de um espaço vetorial é um somando direto. Isto deixa de ser verdade quando se trata de módulos sobre anéis arbitrários, por exemplo, $\mathbb{Z}$ não é um somando direto de $\mathbb{Q}$ como um $\mathbb{Z}$-módulo. De agora em diante estaremos

interessados em módulos particulares que possuem esta propriedade. Nesta seção omitiremos algumas demonstrações que podem ser encontradas no Capítulo 2 da referência [4].

Definição 1.3.1 *Um R-módulo M é dito* ***simples*** *se $M \neq \{0\}$ e seus únicos submódulos são $\{0\}$ e M.*

Definição 1.3.2 *Um R-módulo M é dito* ***semissimples*** *se todo submódulo de M é um somando direto.*

Proposição 1.3.3 *Seja $N \neq \{0\}$ um submódulo de um módulo semissimples M. Então N é semissimples e contém um submódulo simples.*

Teorema 1.3.4 *Seja M um R-módulo. Então as seguintes condições são equivalentes:*

1. *M é semissimples.*
2. *M é uma soma direta de submódulos simples.*
3. *M é uma soma (não necessariamente direta) de submódulos simples.*

Corolário 1.3.5 *Seja $M = \oplus_{i \in I} M_i$ uma decomposição de um módulo semissimples M como uma soma direta de submódulos simples e seja N um submódulo de M. Então existe um subconjunto de índices $J \subset I$ tal que $N \simeq \oplus_{i \in J} M_i$.*

Definição 1.3.6 *Um anel R é dito* ***semissimples*** *se o módulo R_R é semissimples.*

Teorema 1.3.7 *Seja R um anel. Então as seguintes condições são equivalentes:*

1. *Todo R-módulo é semissimples.*
2. *R é um anel semissimples.*
3. *R é uma soma direta de um número finito de ideais minimais à esquerda.*

Teorema 1.3.8 *Seja R um anel. Então R é semissimples se, e somente se, todo ideal à esquerda de R é da forma $L = Re$, onde $e \in R$ é um idempotente.*

Teorema 1.3.9 *Seja $R = \oplus_{i=1}^{t} L_i$ uma decomposição de um anel semissimples como uma soma direta de ideais minimais à esquerda. Então existe uma família $\{e_1, \cdots, e_t\}$ de elementos de R tais que:*

1. *$e_i \neq 0$ é um idempotente, para $1 \leq i \leq t$.*

2. *Se* $i \neq j$, *então* $e_i e_j = 0$.

3. $1 = e_1 + \cdots + e_t$.

4. e_i *não pode ser escrito como* $e_i = e_i' + e_i''$, *onde* e_i', e_i'' *são idempotentes não nulos tais que* $e_i' e_i'' = 0$, *para* $1 \leq i \leq t$.

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

Definição 1.3.10 *Seja* R *um anel. Uma família de idempotentes* $\{e_1, \cdots, e_t\}$ *satisfazendo* (1), (2) *e* (3) *do teorema anterior é dita uma* ***família completa de idempotentes ortogonais****. Um idempotente satisfazendo* (4) *do teorema anterior é dito* ***primitivo****.*

Lema 1.3.11 *Seja* L *um ideal minimal à esquerda de um anel semissimples* R *e seja* M *um* R*-módulo simples. Então* $LM \neq \{0\}$ *se, e somente se,* $L \simeq M$ *como* R*-módulos e, neste caso,* $LM = M$.

Proposição 1.3.12 *Seja* $R = \oplus_{i=1}^{t} L_i$ *uma decomposição de um anel semissimples* R *como uma soma direta de ideais minimais à esquerda. Então todo* R*-módulo simples é isomorfo a um dos ideais* L_i *da decomposição dada.*

Lema 1.3.13 *Seja* L *um ideal minimal à esquerda de um anel semissimples* R. *Então a soma de todos os ideais de* R *isomorfos a* L *é um ideal bilateral de* R.

Lema 1.3.14 *Seja* I *um ideal bilateral, de um anel semissimples, que contém um ideal minimal à esquerda* L. *Então* I *contém todos os ideais à esquerda isomorfos a* L.

Proposição 1.3.15 *Seja* L *um ideal minimal à esquerda de um anel semissimples* R *e seja* B *a soma de todos os ideais à esquerda de* R *isomorfos a* L. *Então* B *é um ideal bilateral minimal de* R.

Dada uma decomposição de um anel semissimples R como uma soma direta de ideais minimais à esquerda , reordenando-os se necessário, podemos agrupar juntos os ideais à esquerda isomorfos da seguinte maneira:

$$R = \underbrace{L_{11} \oplus \cdots \oplus L_{1r_1}} \oplus \underbrace{L_{21} \oplus \cdots \oplus L_{2r_2}} \oplus \cdots \oplus \underbrace{L_{s1} \oplus \cdots \oplus L_{sr_s}},$$

onde, $L_{ij} \simeq L_{ik}$ e $L_{ij} L_{kh} = \{0\}$ se $i \neq k$, de acordo com o Lema 1.3.11. Da Proposição 1.3.12 segue que todos ideais minimais à esquerda são isomorfos a um dos ideais da decomposição de R dada acima.

Teorema 1.3.16 *Com a notação acima, seja A_i a soma de todos os ideais à esquerda isomorfos a L_{i1}, para todo $1 \leq i \leq s$. Então:*

1. *Cada A_i é um ideal minimal bilateral de R.*
2. *$A_iA_j = \{0\}$, se $i \neq j$.*
3. *$R = \oplus_{i=1}^{s} A_i$, onde s é o número de classes de isomorfismos de ideais minimais à esquerda de R.*

Definição 1.3.17 *Um anel R é chamado **simples** se seus únicos ideais bilaterais são $\{0\}$ e R.*

Corolário 1.3.18 *Os ideais A_i, para $1 \leq i \leq s$, definidos no Teorema 1.3.16, são anéis simples.*

Os ideais bilaterais construídos no Teorema 1.3.16 determinam completamente todos os ideais bilaterais de R.

Proposição 1.3.19 *Seja $R = \oplus_{i=1}^{s} A_i$ a decomposição de um anel semissimples R como uma soma direta de ideais minimais bilaterais. Então*

1. *Todo ideal bilateral I de R pode ser escrito na forma $I = A_{i_1} \oplus \cdots \oplus A_{i_t}$, onde $1 \leq i_1 < \cdots < i_t \leq s$.*
2. *Se $R = \oplus_{j=1}^{r} B_j$ é outra decomposição de R em uma soma direta de ideais minimais bilaterais, então $r = s$ e, após uma possível renumeração dos índices, $A_i = B_i$, para todo $i \in \{1, 2, ..., r\}$.*

Definição 1.3.20 *Os únicos ideais minimais bilaterais de um anel semissimples R são chamados de **componentes simples** de R.*

Teorema 1.3.21 *Seja $R = \oplus_{i=1}^{s} A_i$ uma decomposição de um anel semissimples como soma direta de ideais minimais bilaterais. Então existe uma família $\{e_1, \cdots, e_s\}$ de elementos de R tal que:*

1. *$e_i \neq 0$ é um idempotente central de R, para $1 \leq i \leq s$.*
2. *Se $i \neq j$, então $e_ie_j = 0$.*
3. *$1 = e_1 + \cdots + e_s$.*

4. *e_i não pode ser escrito como $e_i = e_i' + e_i''$, onde e_i', e_i'' são idempotentes centrais não nulos tais que $e_i' e_i'' = 0,\ 1 \leq i \leq s$.*

Definição 1.3.22 *Os elementos $\{e_1, \cdots, e_s\}$ do teorema acima são chamados de* ***idempotentes centrais primitivos*** *de R.*

Lema 1.3.23 *Seja R um anel e sejam $M = M_1 \oplus \cdots \oplus M_r$ e $N = N_1 \oplus \cdots \oplus N_s$ dois R-módulos escritos como uma soma direta de submódulos. Sejam $\varepsilon_j : M_j \to M$ as inclusões de cada M_j em M e $\pi_i : N \to N_i$ os R-homomorfismos naturais de N em suas componentes.*

1. *Assuma que, para cada par de índices i, j, temos um R-homomorfismo $\phi_{ij} \in Hom_R(M_j, N_i)$. Então a aplicação $\phi : M \to N$ definida por:*

$$\begin{aligned}\phi(m_1 + \cdots + m_r) &= \begin{pmatrix} \phi_{11} & \cdots & \phi_{1r} \\ \cdots & \cdots & \cdots \\ \phi_{s1} & \cdots & \phi_{sr} \end{pmatrix} \begin{pmatrix} m_1 \\ \cdots \\ m_r \end{pmatrix} \\ &= \underbrace{\phi_{11}(m_1) + \cdots + \phi_{1r}(m_r)}_{\in N_1} + \cdots + \underbrace{\phi_{s1}(m_1) + \cdots + \phi_{sr}(m_r)}_{\in N_s},\end{aligned}$$

   é um R-homomorfismo. Para indicar que ϕ é dado da forma acima, escreveremos simplesmente $\phi = (\phi_{ij})$.

2. *Reciprocamente, se $\phi \in Hom_R(M, N)$, então $\phi_{ij} = \pi_i \circ \phi \circ \varepsilon_j \in Hom_R(M_j, N_i)$ e $\phi = (\phi_{ij})$.*

3. *Para $\phi = (\phi_{ij})$ e $\psi = (\psi_{ij})$, temos $\phi + \psi = (\phi_{ij} + \psi_{ij})$.*

4. *$Hom_R(M^n, M^n) \simeq M_n(Hom_R(M, M))$, como anéis, onde $M^n = \underbrace{M \times \cdots \times M}_{n \text{ vezes}}$.*

Lema 1.3.24 ***(Lema de Schur)*** *Seja R um anel e sejam M e N dois R-módulos simples. Seja $f : M \to N$ um homomorfismo não nulo. Então f é um isomorfismo.*

Corolário 1.3.25 *Seja R um anel e sejam M, N R-módulos simples. Então temos:*

1. *Se $M \not\simeq N$, então $Hom_R(M, N) = \{0\}$.*

2. *$Hom_R(M, N)$ é um anel de divisão.*

Teorema 1.3.26 ***(Teorema de Wedderburn-Artin)*** *Um anel R é semissimples se, e somente se, ele é uma soma direta de álgebras de matrizes sobre anéis de divisão, isto é, se*

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

Teorema 1.3.27 *Seja R um anel semissimples e assuma que*

$$R \simeq M_{n_1}(D_1) \oplus \cdots \oplus M_{n_s}(D_s) \simeq M_{m_1}(D'_1) \oplus \cdots \oplus M_{m_r}(D'_r),$$

onde D_i e D'_j, para $1 \leq i \leq s$ e $1 \leq j \leq r$ são anéis de divisão. Então $r = s$ e, após uma conveniente permutação de índices, temos $n_i = m_i$ e $D_i \simeq D'_i$.

1.4 Anéis de Grupos

Nesta seção introduzimos a definição de um anel de grupo RG de um grupo G sobre um anel com unidade R. Definimos a aplicação de aumento e o ideal de aumento, o núcleo desta aplicação que é um importante ideal de um anel de grupo. Além disso, discutimos condições sobre o grupo G e sobre o anel R para que o anel de grupo RG seja semissimples, demonstrando o Teorema de Maschke. Ao final da seção apresentamos algumas álgebras de grupo de grupos abelianos. As demonstrações omitidas podem ser encontradas no Capítulo 3 da referência [4].

Seja G um grupo (não necessariamente finito) e R um anel. Denote por RG o conjunto de todas as "combinações lineares"da forma

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

onde $a_g \in R$ e $a_g = 0$, para quase todo $g \in G$, isto é, somente um número finito de coeficientes são diferentes de 0 em cada soma. Quando conveniente, também escrevemos α na forma:

$$\alpha = \sum_{g \in G} a(g) g.$$

Dado um elemento $\alpha = \sum_{g \in G} a_g g$, definimos o **suporte** de α como sendo o subconjunto de elementos de G que efetivamente aparecem na expressão de α, isto é:

$$supp(\alpha) = \{g \in G : a_g \neq 0\}. \tag{1.2}$$

Segue da definição que, dados dois elementos, $\alpha = \sum_{g \in G} a_g g$ e $\beta = \sum_{g \in G} b_g g \in RG$, temos $\alpha = \beta$ se, e somente se, $a_g = b_g$, para todo $g \in G$.

Definimos a **soma** de dois elementos em RG componente a componente, isto é,

$$\left(\sum_{g \in G} a_g g\right) + \left(\sum_{g \in G} b_g g\right) = \sum_{g \in G} (a_g + b_g) g. \tag{1.3}$$

Também, dados dois elementos $\alpha = \sum_{g\in G} a_g g$ e $\beta = \sum_{g\in G} b_g g \in RG$, definimos o **produto** deles por

$$\alpha\beta = \sum_{g,h\in G} a_g b_h gh. \tag{1.4}$$

Reordenando os termos na fórmula acima, podemos escrever o produto $\alpha\beta$ como

$$\alpha\beta = \sum_{u\in G} c_u u, \tag{1.5}$$

onde

$$c_u = \sum_{gh=u} a_g b_h.$$

É fácil verificar que, com as operações acima, RG é um anel que possui como unidade o elemento $1 = \sum_{g\in G} u_g g$, onde o coeficiente correspondente ao elemento neutro do grupo é igual a 1 e $u_g = 0$, para todos os outros elementos de G.

Definimos ainda um produto de elementos em RG por elementos $\lambda \in R$ por

$$\lambda\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} (\lambda a_g) g. \tag{1.6}$$

É fácil verificar que RG é um R-módulo. Na verdade, se R é comutativo, então RG é uma álgebra sobre R.

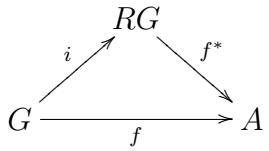
Definição 1.4.1 *O conjunto RG, com as operações definidas acima, é chamado de* ***anel de grupo de*** *G* ***sobre*** *R. No caso em que R for comutativo, RG é chamado de* ***álgebra de grupo de*** *G* ***sobre*** *R.*

Podemos definir uma imersão $i : G \to RG$ fixando, para cada elemento $x \in G$, o elemento $i(x) = \sum_{g\in G} a_g g$, onde $a_x = 1$ e $a_g = 0$, se $g \neq x$. Desta maneira, consideramos G como um subconjunto de RG. Com esta identificação em mente, vemos que RG é um R-módulo livre com base G.

Também podemos considerar uma aplicação $\nu : R \to RG$ 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 fácil verificar que ν é um monomorfismo de anel e, assim, podemos considerar R como um subanel de RG.

Dadas as identificações acima e dados $r \in R$ e $g \in G$, é claro que $rg = gr$ em RG. Portanto, se R for comutativo, temos $R \subset Z(RG)$, o centro de RG.

Proposição 1.4.2 *Sejam G um grupo e R um anel. Dado qualquer anel A tal que $R \subset A$ e qualquer aplicação $f : G \to A$ tal que $f(gh) = f(g)f(h)$, para todos $g, h \in G$, existe um único homomorfismo de anel $f^* : RG \to A$, que é R-linear, tal que $f^* \circ i = f$, onde $i : G \to RG$ é a inclusão dada acima, isto é, tal que o seguinte diagrama comuta:*



Além disso, se R é central em A (e assim A é uma R-álgebra), então f^* é um homomorfismo de R-álgebras.

Corolário 1.4.3 *Seja $f : G \to H$ um homomorfismo de grupos. Existe um único homomorfismo de anéis $f^* : RG \to RH$ tal que $f^*(g) = f(g)$, para todo $g \in G$. Se R é comutativo, então f^* é um homomorfismo de R-álgebras. Além disso, se f é um epimorfismo (monomorfismo), então f^* é também um epimorfismo (monomorfismo).*

Observe que se $H = \{1\}$, então o Corolário 1.4.3 mostra que a aplicação trivial $G \to \{1\}$ induz a um homomorfismo de anéis $\varepsilon : RG \to R$ tal que

$$\varepsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g.$$

Definição 1.4.4 *O homomorfismo $\varepsilon : RG \to R$ dado por*

$$\varepsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g$$

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

Note que se um elemento $\alpha = \sum_{g\in G} a_g g$ pertence a $\Delta(G)$, então $\varepsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g = 0$. Logo podemos escrever α na forma:

$$\alpha = \sum_{g\in G} a_g g - \sum_{g\in G} a_g = \sum_{g\in G} a_g(g-1).$$

Claramente todos os elementos da forma $g-1$, $g \in G$, pertencem a $\Delta(G)$. A observação acima mostra que $\{g-1 : g \in G, g \neq 1\}$ é um conjunto de geradores de $\Delta(G)$ sobre R. Observe também que este conjunto é linearmente independente.

Proposição 1.4.5 *O conjunto $\{g-1 : g \in G, g \neq 1\}$ é uma base de $\Delta(G)$ sobre R. Logo podemos escrever*

$$\Delta(G) = \left\{ \sum_{g \in G} a_g(g-1) : g \in G,\ g \neq 1,\ a_g \in R \right\}$$

onde, como sempre, assumimos que somente um número finito de coeficientes a_g são diferentes de 0.

Particularmente, se R é comutativo e G finito, então $\Delta(G)$ é um R-módulo livre de posto $|G|-1$.

Proposição 1.4.6 *Sejam R um anel comutativo e G,H grupos. Então*

$$R(G \times H) \simeq (RG)H \simeq RG \otimes_R RH.$$

Prova: Defina o homomorfismo $\overline{\varphi}$ do grupo $G \times H$ no grupo das unidades de $(RG)H$, dado por $\overline{\varphi}((g,h)) = gh$.

Mostremos que $\overline{\varphi}$ é um homomorfismo injetor de grupos multiplicativos. De fato:

- Sejam (g_1,h_1), $(g_2,h_2) \in G \times H$. Daí $\overline{\varphi}((g_1,h_1)\cdot(g_2,h_2)) = g_1g_2h_1h_2$. Por outro lado, $\overline{\varphi}((g_1,h_1)) \cdot \overline{\varphi}((g_2,h_2)) = g_1h_1g_2h_2 = g_1g_2h_1h_2$, pela observação feita após a Definição 1.4.1.

  Suponhamos $\overline{\varphi}((g_1,h_1)) = \overline{\varphi}((g_2,h_2))$ e daí $g_1h_1 = g_2h_2$. Como g_1h_1, $g_2h_2 \in (RG)H$, segue que $g_1 = g_2$ e consequentemente $h_1 = h_2$.

Estendemos $\overline{\varphi}$ linearmente da seguinte maneira:

$$\begin{array}{rccc} \varphi\ : & R(G\times H) & \longrightarrow & (RG)H \\ & \displaystyle\sum_{g\in G,\, h\in H} \alpha_{gh}(g,h) & \longmapsto & \displaystyle\sum_{h\in H}\left(\sum_{g\in G}\alpha_{gh}g\right)h. \end{array}$$

Provemos que φ assim definida é um isomorfismo de álgebras de grupo. De fato:

- Sejam $\alpha,\ \beta \in R(G\times H)$. Daí $\alpha = \sum\limits_{g\in G,\, h\in H} \alpha_{gh}(g,h)$ e $\beta = \sum\limits_{j\in G,\, k\in H} \alpha_{jk}(j,k)$.

  Assim, $\varphi(\alpha\cdot\beta) = \varphi(\sum \alpha_{gh}\beta_{jk}(gj,hk)) = \sum\limits_{h,\,k\in H}\Big(\sum\limits_{g,\,j\in G}\alpha_{gh}\beta_{jk}gj\Big)hk.$

  Por outro lado,
  $$\begin{aligned}\varphi(\alpha)\cdot\varphi(\beta) &= \varphi(\textstyle\sum \alpha_{gh}(g,h))\cdot\varphi(\sum \beta_{jk}(j,k)\\ &= \sum_{h\in H}\Big(\sum_{g\in G}\alpha_{gh}g\Big)h\cdot\sum_{k\in H}\Big(\sum_{j\in G}\beta_{jk}j\Big)k\\ &= \sum_{h,\,k\in H}\Big(\sum_{g,\,j\in G}\alpha_{gh}\beta_{jk}gj\Big)hk.\end{aligned}$$
  Logo $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$.

- Sejam $\alpha,\ \eta \in R(G\times H)$ tais que $\alpha = \sum \alpha_{gh}(g,h)$ e $\eta = \sum \eta_{gh}(g,h)$. Assim,
  $$\begin{aligned}\varphi(\alpha+\eta) &= \varphi((\textstyle\sum \alpha_{gh}+\eta_{gh})(g,h))\\ &= \sum_{h\in H}\Big(\sum_{g\in G}(\alpha_{gh}+\eta_{gh})g\Big)h\\ &= \sum_{h\in H}\Big(\sum_{g\in G}\alpha_{gh}g\Big)h + \sum_{h\in H}\Big(\sum_{g\in G}\beta_{gh}g\Big)h\\ &= \varphi(\alpha)+\varphi(\eta).\end{aligned}$$

- Sejam $r\in R$ e $\alpha = \sum\limits_{g\in G,\, h\in H}\alpha_{gh}(g,h) \in R(G\times H)$. Daí

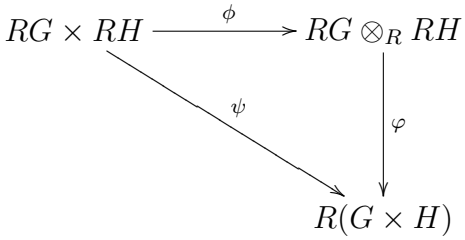
  $\varphi(r\cdot\alpha) = \varphi(\sum r\alpha_{gh}(g,h)) = \sum\limits_{h\in H}\Big(\sum\limits_{g\in G} r\alpha_{gh}g\Big)h = r\Big(\sum\limits_{h\in H}\Big(\sum\limits_{g\in G}\alpha_{gh}g\Big)h\Big) =$
  $r\cdot\varphi(\alpha)$.

- Sejam $\alpha = \sum \alpha_{gh}gh,\ \ \eta = \sum \eta_{gh}gh \in R(G\times H)$ tais que $\varphi(\alpha) = \varphi(\beta)$. Assim,
  $$\begin{aligned}\varphi(\alpha)=\varphi(\eta) &\Rightarrow \sum_{h\in H}\Big(\sum_{g\in G}\alpha_{gh}g\Big)h = \sum_{h\in H}\Big(\sum_{g\in G}\eta_{gh}g\Big)h\\ &\Rightarrow \sum_{h\in H}\Big(\sum_{g\in G}\alpha_{gh}g\Big)h - \sum_{h\in H}\Big(\sum_{g\in G}\eta_{gh}g\Big)h = 0\\ &\Rightarrow \sum_{h\in H}\Big(\sum_{g\in G}(\alpha_{gh}-\eta_{gh})g\Big)h = 0\\ &\Rightarrow \Big(\sum_{g\in G}(\alpha_{gh}-\eta_{gh})g\Big) = 0\\ &\Rightarrow \alpha_{gh} = \eta_{gh}, \text{ para todo } g\in G \text{ e para todo } h\in H.\end{aligned}$$
  O que mostra que φ é injetora.

- Vemos que $GH \subset Im\overline{\varphi} \subset Im\varphi$. Os elementos de $(RG)H$ são do tipo $\sum_{h\in H}\left(\sum_{g\in G}\alpha_{gh}g\right)h$, ou seja, GH gera $(RG)H$ sobre R. Portanto, considerando a extensão linear φ, temos $(RG)H \subset Im\varphi$. Logo φ é sobrejetora.

Agora vamos utilizar a Propriedade Universal do Produto Tensorial para mostrar que $\psi : RG \otimes_R RH \longrightarrow R(G \times H)$ dada por $\psi\left(\sum_{i=0}^{n} r_i g_i \otimes \sum_{j=0}^{m} s_j h_j\right) = \sum r_i s_j (g_i, h_j)$ é um isomorfismo de álgebras.

Considere o seguinte diagrama:



A função $\psi : RG \times RH \longrightarrow R(G \times H)$ dada por $\psi\left(\sum_{i=0}^{n} r_i g_i, \sum_{j=0}^{m} s_j h_j\right) = \sum r_i s_j (g_i, h_j)$ é uma aplicação balanceada. De fato:

Sejam $\alpha, \beta \in RG$, $\gamma, \eta \in RH$ tais que $\alpha = \sum r_i g_i$, $\beta = \sum s_i g_i$, $\gamma = \sum t_j h_j$, $\eta = \sum v_j h_j$ e $r \in R$. Daí

- $\psi(\alpha+\beta, \gamma) = \psi(\sum(r_i+s_i)g_i, \sum t_j h_j) = \sum(r_i+s_i)t_j(g_i,h_j) = \sum r_i t_j(g_i,h_j) + \sum s_i t_j(g_i,h_j) = \psi(\alpha, \gamma) + \psi(\beta, \gamma)$.
- $\psi(\alpha, \gamma+\eta) = \psi(\sum r_i g_i, \sum(t_j+v_j)h_j) = \sum r_i(t_j+v_j)(g_i,h_j) = \sum r_i t_j(g_i,h_j) + \sum r_i v_j(g_i,h_j) = \psi(\alpha, \gamma) + \psi(\alpha, \eta)$.
- $\psi(r\alpha, \gamma) = \psi(\sum r r_i g_i, \sum t_j h_j) = \sum r r_i t_j(g_i,h_j) = r\sum r_i t_j(g_i,h_j) = r(\psi(\alpha, \gamma))$.
- $\psi(\alpha, r\gamma) = \psi(\sum r_i g_i, \sum r t_j h_j) = \sum r_i r t_j(g_i,h_j) = r\sum r_i t_j(g_i,h_j) = r(\psi(\alpha, \gamma))$.

Pela Propriedade Universal do Produto Tensorial, existe único homomorfismo de álgebras $\psi : RG \otimes_R RH \longrightarrow R(G \times H)$ dada por $\psi\left(\sum_{i=0}^{n} r_i g_i \otimes \sum_{j=0}^{m} s_j h_j\right) = \sum r_i s_j (g_i, h_j)$ que faz o diagrama acima comutar.

Mostremos que ψ é um homomorfismo. De fato:

Sejam $x, y \in RG \otimes_R RH$ tais que $x = \sum r_i g_i \otimes \sum t_j h_j$, $y = \sum s_i g_i \otimes \sum v_j h_j$ e $r \in R$.

- $\varphi(x) + \varphi(y) = \sum (r_i t_j + s_i v_j)(g_i, h_j) = \varphi(\sum (r_i t_j + s_i v_j) g_i \otimes h_j) = \varphi(x + y)$.
- $\varphi(xy) = \varphi(\sum r_i s_i g_i^2 \otimes \sum t_j v_j h_j^2) = \sum r_i s_i t_j v_j (g_i^2, h_j^2) = \varphi(x)\varphi(y)$.
- $\varphi(rx) = \varphi(\sum r r_i g_i \otimes \sum t_j h_j) = \sum r r_i t_j (g_i, h_j) = r(\sum r_i t_j (g_i, h_j)) = r\varphi(x)$.

Seja $\widetilde{\varphi} : R(G \times H) \longrightarrow RG \otimes_R RH$ definida por $\widetilde{\varphi}(\sum r_{ij}(g_i, h_j)) = \sum r_{ij} g_i \otimes h_j$. Observe que $\varphi(\widetilde{\varphi}(\sum r_{ij}(g_i, h_j))) = \varphi(\sum r_{ij} g_i \otimes h_j) = \sum r_{ij}(g_i, h_j) = Id_{\widetilde{\varphi}}$.

Por outro lado,
$\widetilde{\varphi}(\varphi(\sum r_i g_i \otimes \sum s_j h_j)) = \widetilde{\varphi}(\sum r_i s_j (g_i, h_j)) = \sum r_i s_j g_i \otimes h_j = \sum r_i g_i \otimes \sum s_j h_j = Id_{\varphi}$.

Assim, $\widetilde{\varphi}$ e φ são inversas uma da outra. Logo φ é bijetora. Portanto, $RG \otimes_R RH$ e $R(G \times H)$ são isomorfos.

■

Vamos agora encontrar condições sobre R e G que nos permitam decompor RG como uma soma direta de certos subanéis. O nosso maior interesse é determinar quando RG é um anel semissimples e escrevê-lo como uma soma direta de ideais minimais.

Começaremos estudando as relações entre subgrupos de G e ideais de RG. Esta relação é muito útil no estudo de muitos problemas envolvendo a estrutura e propriedades de RG.

Dados um grupo G e um anel R, denotamos por $\mathcal{S}(G)$ o conjunto de todos os subgrupos de G e por $\mathcal{I}(RG)$ o conjunto de todos os ideais à esquerda de RG.

Definição 1.4.7 *Para um subgrupo $H \in \mathcal{S}(G)$, denotamos por $\Delta_R(G, H)$ o ideal à esquerda de RG gerado pelo conjunto $\{h - 1 : h \in H\}$, isto é,*

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

Para um anel fixo R, omitimos o subscrito e denotamos $\Delta_R(G, H)$ simplesmente por $\Delta(G, H)$. Observe que $\Delta(G, G) = \Delta(G)$.

Lema 1.4.8 *Seja H um subgrupo de um grupo G e seja S um conjunto de geradores de H. O conjunto $\{s-1 : s \in S\}$ é um conjunto de geradores de $\Delta(G,H)$ como um ideal à esquerda de RG.*

Para uma melhor descrição de $\Delta_R(G,H)$, denotamos por $\mathcal{T} = \{q_i\}_{i\in I}$ um conjunto completo de representantes das classes laterais à esquerda de H em G, isto é, um **transversal** de H em G e vamos sempre escolher, como representante da classe H em $\mathcal{T}$, o elemento identidade de G. Pela definição de transversal, todo elemento $g \in G$ pode ser escrito de maneira única na forma $g = q_i h_j$, onde $q_i \in \mathcal{T}$ e $h_j \in H$.

Proposição 1.4.9 *O conjunto $B_H = \{q(h-1) : q \in \mathcal{T},\, h \in H,\, h \neq 1\}$ é uma base de $\Delta_R(G,H)$ sobre R.*

Se $H \lhd G$, então o homomorfismo canônico $\omega : G \to G/H$ pode ser estendido ao epimorfismo $\omega^* : RG \to R(G/H)$ tal que

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

Proposição 1.4.10 *Seja H um subgrupo normal de um grupo G. Então, com a notação acima, $Ker(\omega^*) = \Delta(G,H)$.*

Corolário 1.4.11 *Seja H um subgrupo normal de um grupo G. Então $\Delta(G,H)$ é um ideal bilateral de RG e*

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

Logo $\Delta(G)$ é núcleo do epimorfismo ε induzido pela aplicação trivial

$$G \to G/G = \{1\}.$$

Assim, podemos construir uma aplicação de $\mathcal{S}(G)$ sobre $\mathcal{I}(RG)$ tal que os subgrupos normais de G são levados em ideais bilaterais de RG.

Dado um ideal à esquerda $I \in \mathcal{I}(RG)$, consideremos o conjunto

$$\nabla(I) = \{g \in G : g - 1 \in I\},$$

isto é,

$$\nabla(I) = G \cap (1 + I).$$

Afirmamos que $\nabla(I)$ é um subgrupo de G. De fato, se $g, h \in \nabla(I)$, então $gh - 1 = g(h-1) + g - 1 \in \nabla(I)$. Logo $gh \in \nabla(I)$. Também, se $g \in \nabla(I)$, então $g^{-1} - 1 = -g^{-1}(g-1) \in \nabla(I)$. Portanto, $g^{-1} \in \nabla(I)$. É fácil verificar que se I é um ideal bilateral de RG, então $\nabla(I)$ é um subgrupo normal em G.

Proposição 1.4.12 *Se $H \in \mathcal{S}(G)$, então $\nabla(\Delta(G,H)) = H$.*

As aplicações ∇ e Δ, ao contrário do que parece, não são inversas uma da outra. De fato, dado um ideal $I \in \mathcal{I}(RG)$, é fácil ver que $\Delta(G, \nabla(I)) \subset I$. Mas a igualdade pode não ser verdade. Se $I = RG$, então $\nabla(RG) = \{g \in G : g - 1 \in RG\} = G$. Mas, $\Delta(G, \nabla(RG)) = \Delta(G) \neq RG$.

Definição 1.4.13 *Dados um anel de grupo RG e um subconjunto finito X do grupo G, denotaremos por $\widehat{X}$ o seguinte elemento de RG:*

$$\widehat{X} = \sum_{x \in X} x.$$

Lema 1.4.14 *Seja R um anel com unidade e seja H um subgrupo de um grupo G. Se $|H|$ é invertível em R então $e_H = \dfrac{1}{|H|}\widehat{H}$ é um idempotente de RG. Além disso, se $H \lhd G$, então e_H é central.*

Proposição 1.4.15 *Seja R um anel e seja H um subgrupo normal de um grupo G. Se $|H|$ é invertível em R, tomando $e_H = \dfrac{1}{|H|}\widehat{H}$ temos uma soma direta de anéis*

$$RG = RGe_H \oplus RG(1 - e_H),$$

onde

$$RGe_H \simeq R(G/H) \ \text{ e } \ RG(1 - e_H) = \Delta(G, H).$$

Definição 1.4.16 *Seja R um anel e seja G um grupo finito tal que $|G|$ é invertível em R. O idempotente $e_G = \dfrac{1}{|G|}\widehat{G}$ é chamado **idempotente principal** de RG.*

Como uma consequência imediata do resultado acima, usando o idempotente principal de RG, podemos mostrar que álgebras de grupo semissimples sempre contêm pelo menos uma componente simples que é isomorfa ao anel dos coeficientes.

Corolário 1.4.17 *Seja R um anel e seja G um grupo finito tal que $|G|$ é invertível em R. Então podemos escrever RG como uma soma direta de anéis*

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

Lema 1.4.18 *Seja R um anel comutativo e seja I um ideal da álgebra de grupo RG. O anel quociente RG/I é comutativo se, e somente se, $\Delta(G, G') \subset I$, onde G' denota o subgrupo comutador de G.*

Proposição 1.4.19 *Seja RG uma álgebra de grupo semissimples. Então temos*

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

onde $RGe_{G'} \simeq R(G/G')$ é a soma de todas as componentes simples comutativas de RG e $\Delta(G, G')$ é soma de todas as outras.

Agora vamos determinar condições necessárias e suficientes sobre R e G para que o anel de grupo RG seja semissimples. Veremos primeiro algumas técnicas e resultados sobre anuladores.

Definição 1.4.20 *Seja X um subconjunto de um anel de grupo RG. O* ***anulador à esquerda*** *de X é o conjunto*

$$Ann_l(X) = \{\alpha \in RG : \alpha x = 0, \, \forall x \in X\}.$$

Do mesmo modo definimos o ***anulador à direita*** *de X como:*

$$Ann_r(X) = \{\alpha \in RG : x\alpha = 0, \, \forall x \in X\}.$$

Lema 1.4.21 *Seja H um subgrupo de um grupo G e seja R um anel. O $Ann_r(\Delta(G, H)) \neq 0$ se, e somente se, H é finito. Neste caso, temos*

$$Ann_r(\Delta(G, H)) = \widehat{H} \cdot RG.$$

Além disso, se $H \lhd G$, então o elemento $\widehat{H}$ é central em RG e temos

$$Ann_r(\Delta(G, H)) = Ann_l(\Delta(G, H)) = RG \cdot \widehat{H}.$$

Corolário 1.4.22 *Seja G um grupo finito. Então:*

1. $Ann_l(\Delta(G)) = Ann_r(\Delta(G)) = R \cdot \widehat{G}$.
2. $Ann_r(\Delta(G)) \cap \Delta(G) = \{a\widehat{G} : a \in R, \, a|G| = 0\}$.

Lema 1.4.23 *Seja I um ideal bilateral de um anel R. Suponha que exista um ideal à esquerda J tal que $R = I \oplus J$ (como R-módulos à esquerda). Então $J \subset Ann_r(I)$.*

Lema 1.4.24 *Se o ideal de aumento $\Delta(G)$ é um somando direto de RG, como um RG-módulo, então G é finito e $|G|$ é invertível em R.*

O seguinte teorema determina condições necessárias e suficientes sobre R e G para que o anel de grupo RG seja semissimples.

Teorema 1.4.25 ***(Teorema de Maschke)*** *Seja G um grupo. O anel de grupo RG é semissimples se, e somente se, valem as seguintes condições:*

1. *R é um anel semissimples.*
2. *G é finito.*
3. *$|G|$ é invertível em R.*

Prova: Suponha que RG é semissimples. Pelo Corolário 1.4.11, $R \simeq RG/\Delta(G)$. Já que o quociente de um anel semissimples é semissimples, segue que R é semissimples. Como a semissimplicidade de RG implica que $\Delta(G)$ é um somando direto, o Lema 1.4.24 mostra que as condições (2) e (3) são verdadeiras.

Reciprocamente, suponha que as condições (1), (2) e (3) são verdadeiras e seja M um RG-submódulo de RG. Já que R é semissimples, segue pelo Teorema 1.3.7, que RG é semissimples como um R-módulo. Portanto, existe um R-submódulo N de RG tal que

$$RG = M \oplus N.$$

Seja $\pi : RG \to M$ a projeção canônica associada a esta soma direta. Definimos $\pi^* : RG \to M$ por uma média

$$\pi^*(x) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gx), \text{ para todo } x \in RG.$$

Se provarmos que π^* é um RG-homomorfismo tal que $(\pi^*)^2 = \pi^*$ e $Im(\pi^*) = M$, então $Ker(\pi^*)$ é um RG-submódulo tal que $RG = M \oplus Ker(\pi^*)$ e o teorema está provado.

Já que π^* é um R-homomorfismo, para mostrar que ele é também um RG-homomorfismo é suficiente mostrar que

$$\pi^*(ax) = a\pi^*(x), \text{ para todo } x \in G \text{ e para todo } a \in G.$$

Temos

$$\pi^*(ax) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gax) = \frac{a}{|G|} \sum_{g \in G} (ga)^{-1}\pi((ga)x).$$

Quando g percorre sobre todos os elementos em G, o produto ga também percorre sobre todos os elementos em G. Logo

$$\pi^*(ax) = a\frac{1}{|G|}\sum_{t\in G} t^{-1}\pi(tx) = a\pi^*(x).$$

Já que π é uma projeção sobre M, sabemos que $\pi(m) = m$, para todo $m \in M$. Como M é um RG-módulo, temos que $gm \in M$, para todo $g \in G$. Portanto,

$$\pi^*(m) = \frac{1}{|G|}\sum_{g\in G} g^{-1}\pi(gm) = \frac{1}{|G|}\sum_{g\in G} g^{-1}gm = m.$$

Dado um elemento $x \in RG$, temos $\pi(gx) \in M$, portanto, $\pi^*(x) \in M$ e segue que $Im(\pi^*) \subset M$. Consequentemente, $\pi^*(\pi^*(x)) = \pi^*(x)$, para todo $x \in RG$, ou seja, $(\pi^*)^2 = \pi^*$.

O fato que $\pi^*(m) = m$, para todo $m \in M$, também mostra que $M \subset Im(\pi^*)$ e segue o teorema.

■

O caso em que $R = \mathbb{F}$ é um corpo é de grande importância. Neste caso, $\mathbb{F}$ é sempre semissimples e $|G|$ é invertível em $\mathbb{F}$ se, e somente se, $|G| \neq 0$ em $\mathbb{F}$, isto é, se e somente se $car(\mathbb{F}) \nmid |G|$.

Corolário 1.4.26 *Seja G um grupo finito e seja $\mathbb{F}$ um corpo. Então $\mathbb{F}G$ é semissimples se, e somente se, $car(\mathbb{F}) \nmid |G|$.*

Veremos agora uma adaptação do Teorema de Wedderburn-Artin que nos dá muitas informações sobre a estrutura de uma álgebra de grupo.

Teorema 1.4.27 *Seja G um grupo finito e seja $\mathbb{F}$ um corpo tal que $car(\mathbb{F}) \nmid |G|$. Então:*

1. *$\mathbb{F}G$ é uma soma direta de um número finito de ideais bilaterais minimais $\{B_i\}_{1\leq i\leq r}$, as componentes simples de $\mathbb{F}G$. Cada B_i é um anel simples.*
2. *Qualquer ideal bilateral de $\mathbb{F}G$ é uma soma direta de alguns dos membros da família $\{B_i\}_{1\leq i\leq r}$.*
3. *Cada componente simples B_i é isomorfa a um anel de matrizes completo da forma $M_{n_i}(D_i)$, onde D_i é um anel de divisão contendo uma cópia de $\mathbb{F}$ em seu centro, e o isomorfismo*

$$\mathbb{F}G \overset{\phi}{\simeq} \oplus_{i=1}^{r} M_{n_i}(D_i)$$

é um isomorfismo de $\mathbb{F}$-álgebras.

4. *Em cada matriz $M_{n_i}(D_i)$, o conjunto*

$$I_i = \left\{ \begin{pmatrix} x_1 & 0 & \cdots & 0 \\ x_2 & 0 & \cdots & 0 \\ & & \cdots & \\ x_{n_i} & 0 & \cdots & 0 \end{pmatrix} : x_1, x_2, \cdots, x_{n_i} \in D_i \right\} \simeq D_i^{n_i}$$

é um ideal minimal à esquerda.

Dado $x \in \mathbb{F}G$, consideramos $\phi(x) = (\alpha_1, \cdots, \alpha_r) \in \oplus_{i=1}^r M_{n_i}(D_i)$ e definimos o produto de x por um elemento $m_i \in I_i$ por $xm_i = \alpha_i m_i$. Com esta definição I_i torna-se um $\mathbb{F}G$-módulo simples.

5. *$I_i \not\simeq I_j$, se $i \neq j$.*

6. *Qualquer $\mathbb{F}G$-módulo simples é isomorfo a algum I_i, para $1 \leq i \leq r$.*

Corolário 1.4.28 *Seja G um grupo finito e seja $\mathbb{F}$ um corpo algebricamente fechado tal que $car(\mathbb{F}) \not| |G|$. Então:*

$$\mathbb{F}G \simeq \oplus_{i=1}^r M_{n_i}(\mathbb{F})$$

e $n_1^2 + n_2^2 + \cdots + n_r^2 = |G|$.

Não existe um método geral para se determinar os ideais à esquerda de uma álgebra de grupo $\mathbb{F}G$, no entanto, existem alguns resultados que estabelecem o número de componentes simples de $\mathbb{F}G$, utilizando a estrutura intrínseca do grupo. Listamos alguns desses resultados a seguir, para posterior referência.

Teorema 1.4.29 *([3], Teorema 27.22) Seja G um grupo finito e seja $\mathbb{F}$ um corpo algebricamente fechado tal que $car(\mathbb{F}) \nmid |G|$. O número de componentes simples de $\mathbb{F}G$ é igual ao número de classes de conjugação de G.*

Notemos que se o corpo $\mathbb{F}$ não for algebricamente fechado e $car(F) \nmid |G|$, o número de componentes simples de $\mathbb{F}G$ será sempre menor ou igual ao número de classes de conjugação do grupo G. O Corolário 39.5 e Teorema 42.8 (de Berman-Witt) encontrados em [3] são outros exemplos de resultados desta natureza.

Em [18], Ferraz e Milies apresentaram um método geral para calcular o número de componentes simples de uma álgebra de grupo semissimples sem utilizar a Teoria de Caracteres. No caso de álgebras de grupo de grupos abelianos finitos, existe uma maneira mais simples de se determinar este número.

Nos próximos resultados desta seção, usaremos as notações abaixo.

Sejam $\mathbb{F}$ um corpo finito com $|\mathbb{F}| = q$ elementos, A um grupo abeliano finito tal que $mdc(q, |A|) = 1$. Então $\mathbb{F}A$ é semissimples e, se $\{e_1, e_2, ..., e_r\}$ é o conjunto de idempotentes centrais primitivos de $\mathbb{F}A$ temos

$$\mathbb{F}A = \oplus_{i=1}^{r}(\mathbb{F}A)e_i \cong \oplus_{i=1}^{r}\mathbb{F}_i,$$

onde $\mathbb{F}_i \cong (\mathbb{F}A)e_i$, $1 \leq i \leq r$, são corpos que são extensões finitas de $\mathbb{F}$.

Seja $\mathcal{D} = \oplus_{i=1}^{r}\mathbb{F}e_i$. Note que $\mathbb{F}e_i \simeq \mathbb{F}$ como corpos na forma natural e, portanto, o número r de componentes simples de $\mathbb{F}A$ é também a dimensão de $\mathcal{D}$ como espaço vetorial sobre $\mathbb{F}$.

Lema 1.4.30 *([18], Lema 1) Seja α um elemento de $\mathbb{F}A$. Então $\alpha \in \mathcal{D}$ se, e somente se, $\alpha^q = \alpha$.*

Definição 1.4.31 *Seja h um elemento do grupo abeliano finito A. A* ***q-classe ciclotômica*** *de h em A é o conjunto*

$$S_h = \{h^{q^j} \ : \ 0 \leq j \leq t_h - 1\},$$

onde t_h é o menor inteiro positivo tal que

$$q^{t_h} \equiv 1 (mod\, o(h))$$

e $o(h)$ denota a ordem de h.

Segue diretamente da Definição 1.4.31 que se $S_h \neq S_k$, então $S_h \cap S_k = \emptyset$.

Lema 1.4.32 *([21], Lema 2.1.3) Seja α um elemento de $\mathcal{D}$. Se $\alpha = \sum_{h \in A} \alpha_h h$, então $\alpha_h = \alpha_{h^q} = \alpha_{h^{q^2}} = ... = \alpha_{h^{q^{t_h - 1}}}$, para cada $h \in A$.*

Teorema 1.4.33 *([18], Teorema 2.1) O número de componentes simples de $\mathbb{F}A$ é igual ao número de q-classes ciclotômicas de A.*

Vamos adaptar a Definição 1.4.31 para o caso em que o grupo é cíclico finito que utilizaremos na subseção 2.2.3.

Definição 1.4.34 *Seja $H = \langle c \rangle$ um grupo cíclico de ordem j. Assim, todo elemento de $g \in H$ é da forma $g = c^s$. A q-****classe ciclotômica de*** *s é o conjunto dos inteiros dado por*

$$\Omega_s = \{s, sq, sq^2, ..., sq^{r_s - 1}\},$$

onde cada sq^t é reduzido módulo j e r_s é o menor inteiro positivo r_i tal que $sq^{r_i} \equiv s (mod\ j)$.

Na seção seguinte, vamos descrever álgebras de grupos de grupos cíclicos e abelianos, utilizando os resultados acima.

1.5 Álgebras de Grupo de Grupos Abelianos

Nesta seção descrevemos álgebras de grupo de grupos abelianos finitos sobre corpos de característica relativamente prima com a ordem do grupo, isto é, de modo que as hipóteses do Teorema 1.4.27 estejam satisfeitas e a álgebra de grupo seja semissimples.

Primeiramente, seja G um grupo cíclico finito com apresentação dada por $G = \langle a : a^n = 1\rangle$ e $\mathbb{F}$ um corpo tal que $car(\mathbb{F})$ não divide n. Para $\mathbb{F}[x]$ o anel de polinômios sobre $\mathbb{F}$ na indeterminada x, considere a aplicação

$$\begin{array}{rccc} \psi & : & \mathbb{F}[x] & \longrightarrow & \mathbb{F}G \\ & & f & \longmapsto & f(a) \end{array}.$$

É fácil verificar que ψ é um epimorfismo de anéis e, pelo Primeiro Teorema do Homomorfismo para anéis,

$$\mathbb{F}G \simeq \frac{\mathbb{F}[x]}{Ker(\psi)},$$

onde $Ker(\psi) = \{f \in \mathbb{F}[x] : f(a) = 0\}$.

Já que $\mathbb{F}[x]$ é um domínio de ideais principais, $Ker(\psi)$ é o ideal gerado pelo polinômio f_0, de menor grau, tal que $f_0(a) = 0$. É importante observar que, sob este isomorfismo, a imagem do elemento a é a classe $x + \langle f_0\rangle \in \dfrac{\mathbb{F}[x]}{\langle f_0\rangle}$.

Como $a^n = 1$, segue que $x^n - 1 \in Ker(\psi)$. Note que se $f = \displaystyle\sum_{i=0}^{r} k_i x^i$ é um polinômio de grau $r \leq n$, então temos $f(a) = \displaystyle\sum_{i=0}^{r} k_i a^i \neq 0$, pois os elementos $\{1, a, a^2, \cdots, a^r\}$ são linearmente independentes sobre $\mathbb{F}$. Logo $Ker(\psi) = \langle x^n - 1\rangle$, e assim,

$$\mathbb{F}G \simeq \frac{\mathbb{F}[x]}{\langle x^n - 1\rangle}.$$

Seja $x^n - 1 = f_1 f_2 \cdots f_t$ a decomposição de $x^n - 1$ como um produto de polinômios irredutíveis em $\mathbb{F}[x]$. Como estamos assumindo que $car(\mathbb{F}) \nmid n$, o polinômio $x^n - 1$

é separável sobre $\mathbb{F}$ e, assim, $f_i \neq f_j$ se $i \neq j$. Usando o Teorema Chinês do Resto, podemos escrever:

$$\mathbb{F}G \simeq \frac{\mathbb{F}[x]}{\langle f_1 \rangle} \oplus \frac{\mathbb{F}[x]}{\langle f_2 \rangle} \oplus \cdots \oplus \frac{\mathbb{F}[x]}{\langle f_t \rangle}.$$

Sob este isomorfismo, o gerador a é aplicado no elemento

$$(x + \langle f_1 \rangle, \cdots, x + \langle f_t \rangle).$$

Se ζ_i denota uma raiz de f_i, para $1 \leq i \leq t$, então temos $\dfrac{\mathbb{F}[x]}{\langle f_i \rangle} \simeq \mathbb{F}(\zeta_i)$. Consequentemente,

$$\mathbb{F}G \simeq \mathbb{F}(\zeta_1) \oplus \mathbb{F}(\zeta_2) \oplus \cdots \oplus \mathbb{F}(\zeta_t).$$

Como todos os elementos ζ_i, para $1 \leq i \leq t$, são raízes de $x^n - 1$, temos $\mathbb{F}G$ isomorfo a uma soma direta de extensões ciclotômicas de $\mathbb{F}$. Sob este isomorfismo, o elemento a é levado no elemento $(\zeta_1, \zeta_2, \cdots, \zeta_t)$.

A seguir, descrevemos outra maneira de decompor a álgebra de grupo de um grupo cíclico que nos possibilitará generalizar o resultado para grupos abelianos finitos.

Lembramos que, para um dado inteiro d, o d-ésimo **polinômio ciclotômico**, denotado por Φ_d, é o produto $\Phi_d = \Pi_j(x - \zeta_j)$, onde ζ_j percorre todas as d-ésimas raízes primitivas da unidade. Também sabemos que $x^n - 1 = \Pi_{d|n}\Phi_d$, o produto de todos os polinômios ciclotômicos Φ_d em $\mathbb{F}[x]$, onde d é um divisor de n. Para cada d, seja $\Phi_d = \Pi_{i=1}^{a_d} f_{d_i}$ a decomposição de Φ_d como um produto de polinômios irredutíveis em $\mathbb{F}[x]$.

Logo a decomposição de $\mathbb{F}G$ pode ser escrita na forma:

$$\mathbb{F}G \simeq \oplus_{d|n} \oplus_{i=1}^{a_d} \frac{\mathbb{F}[x]}{\langle f_{d_i} \rangle} \simeq \oplus_{d|n} \oplus_{i=1}^{a_d} \mathbb{F}(\zeta_{d_i}),$$

onde ζ_{d_i} denota uma raiz de f_{d_i}, para $1 \leq i \leq a_d$. Para um d fixo, todos os elementos ζ_{d_i} são raízes n-ésimas primitivas da unidade. Portanto, todos os corpos da forma $\mathbb{F}(\zeta_{d_i})$, $1 \leq i \leq a_d$, são iguais uns aos outros e podemos sempre escrever

$$\mathbb{F}G \simeq \oplus_{d|n} a_d \mathbb{F}(\zeta_d),$$

onde ζ_d é uma raiz primitiva de ordem d e $a_d\mathbb{F}(\zeta_d)$ denota a soma direta de a_d corpos diferentes, todos eles isomorfos a $\mathbb{F}(\zeta_d)$.

Já que $\partial(f_{d_i}) = [\mathbb{F}(\zeta_d) : \mathbb{F}]$, onde $\partial(f_{d_i})$ é o grau do polinômio f_{d_i}, temos que os polinômios f_{d_i}, para $1 \leq i \leq a_d$, possuem o mesmo grau. Assim, considerando os graus na decomposição de Φ_d, temos

$$\phi(d) = a_d[\mathbb{F}(\zeta_d) : \mathbb{F}],$$

onde ϕ denota a função de Euler, a saber,

$$\phi(d) = |\{n \in \mathbb{Z} : 1 \leq n < d,\ mdc(n, d) = 1\}|.$$

Como G é um grupo cíclico de ordem n, para cada divisor d de n, o número de elementos de ordem d em G, que denotamos por n_d, é precisamente $\phi(d)$. Portanto, podemos escrever

$$a_d = \frac{n_d}{[\mathbb{F}(\zeta_d) : \mathbb{F}]}.$$

A descrição obtida acima pode ser estendida a anéis de grupo de grupos abelianos finitos, conforme o teorema a seguir, cuja demonstração é feita por indução e utiliza o Teorema de Estrutura dos Grupos Abelianos Finitos (Teorema 1.3.9 em [4]).

Teorema 1.5.1 ***(Perlis-Walker, [20])****([4], Teorema* 3.5.4*) Seja G um grupo abeliano finito de ordem n e seja $\mathbb{F}$ um corpo tal que $car(\mathbb{F}) \nmid n$. Então*

$$\mathbb{F}G \simeq \oplus_{d|n} a_d \mathbb{F}(\zeta_d),$$

onde ζ_d denota uma raiz primitiva da unidade de ordem d e $a_d = \frac{n_d}{[\mathbb{F}(\zeta_d) : \mathbb{F}]}$. Nesta fórmula, n_d denota o número de elementos de ordem d em G.

Corolário 1.5.2 *Seja G um grupo abeliano finito de ordem n. Então*

$$\mathbb{Q}G \simeq \oplus_{d|n} a_d \mathbb{Q}(\zeta_d),$$

onde ζ_d denota uma raiz primitiva da unidade de ordem d e a_d é o número de subgrupos cíclicos (ou fatores cíclicos) de G.

Corolário 1.5.3 *Seja G um grupo abeliano finito de ordem n e seja $\mathbb{F}$ um corpo tal que $car(\mathbb{F}) \nmid n$. Se $\mathbb{F}$ contém uma raiz primitiva da unidade de ordem n, então*

$$\mathbb{F}G \simeq \underbrace{\mathbb{F} \oplus \cdots \oplus \mathbb{F}}_{n \text{ vezes}}.$$

1.6 Representações e Caracteres de Grupos

Nesta seção apresentamos alguns resultados sobre representações e caracteres de grupos, que serão fortemente utilizados nos demais capítulos deste trabalho.

Definição 1.6.1 *Sejam G um grupo, R um anel comutativo e V um R-módulo livre de posto finito. Uma* ***representação de*** *G* ***sobre*** *R, com espaço representação V, é um homomorfismo de grupos $\mathcal{T} : G \to GL(V)$, onde $GL(V)$ denota o grupo de R-automorfismos de V. O posto de V é chamado* ***grau*** *da representação $\mathcal{T}$ e vamos denotá-lo por $\partial(\mathcal{T})$.*

Dada uma representação $\mathcal{T}$ de um grupo G sobre um anel comutativo R, o espaço representação V se torna um RG-módulo sob a ação

$$g \cdot v = \mathcal{T}(g)v \text{ , para todos } g \in G \text{ , } v \in V,$$

estendida linearmente a todos os elementos de RG. Reciprocamente, dado um RG-módulo W (livre de posto finito), definimos uma representação de G sobre R da seguinte maneira:

$$\begin{array}{rccl} \varphi & : & G & \longrightarrow & GL(W) \\ & & g & \longmapsto & \varphi(g)w = g \cdot w, \end{array}$$

para todo $g \in G$ e para todo $w \in W$.

Proposição 1.6.2 *([4], Proposição* 4.2.1*) Seja G um grupo e seja R um anel comutativo com unidade. Existe uma bijeção entre as representações de G sobre R e os RG-módulos que são livres e de posto finito sobre R.*

Desta maneira, todo resultado sobre representação de um grupo G sobre um anel comutativo R tem um análogo para RG-módulo e vice-versa.

Para um dado elemento $g \in G$, denotamos por $\mathcal{T}_g : V \to V$ o automorfismo correspondente sob $\mathcal{T}$. Portanto, se $g, h \in G$, temos $\mathcal{T}_{gh} = \mathcal{T}_g \circ \mathcal{T}_h$ e $\mathcal{T}_1 = I$.

Se fixarmos uma R-base de V, podemos definir um isomorfismo ϕ de $GL(V)$ no grupo $GL(n, R)$ das matrizes invertíveis $n \times n$ com coeficientes em R, associando cada automorfismo $\mathcal{T}_g \in GL(V)$ a sua matriz com respeito à base dada.

Definição 1.6.3 *Seja G um grupo e seja R um anel comutativo. Uma* ***representação matricial*** *de G sobre R de grau n é um homomorfismo de grupos $\overline{\mathcal{T}} : G \to GL(n, R)$, onde $GL(n, R)$ denota o grupo das matrizes $n \times n$ invertíveis sobre o anel R.*

Se $\mathcal{T} : G \to GL(V)$ é uma representação de G sobre R com espaço representação V e consideramos o isomorfismo $\phi : GL(V) \to GL(n, R)$ associado, em relação a uma base dada como acima, então $\phi \circ \mathcal{T} : G \to GL(n, R)$ é uma representação matricial de G. Do mesmo modo, dada uma representação matricial $\mathcal{T} : G \to GL(n, R)$, temos $\phi^{-1} \circ \mathcal{T} : G \to GL(V)$ uma representação de G sobre R.

Por este fato, dada uma representação de um grupo sobre um anel temos uma representação matricial associada a ela e vice-versa. Usaremos algumas vezes neste trabalho, a notação $\mathcal{T}$ no lugar da representação matricial $\overline{\mathcal{T}}$.

Definição 1.6.4 *Duas representações $\mathcal{T}$ e $\mathcal{T}'$ com espaços representação V e V', respectivamente, são ditas* ***equivalentes*** *se existe um $\mathbb{F}$-isomorfismo $\varphi : V \to V'$ tal que $\mathcal{T}'(g)\varphi = \varphi\mathcal{T}(g)$, para todo $g \in G$.*

Observação 1.6.5 *Duas representações de grau 1 são equivalentes se, e somente se, são iguais.*

Definição 1.6.6 *Duas representações matriciais $\overline{\mathcal{T}}_1 : G \to GL(n, R)$ e $\overline{\mathcal{T}}_2 : G \to GL(n, R)$ de um grupo G sobre R são* ***equivalentes*** *se existe uma matriz invertível $\mathcal{U} \in GL(n, R)$ tal que $\overline{\mathcal{T}}_1(x) = \mathcal{U}\overline{\mathcal{T}}_2(x)\mathcal{U}^{-1}$, para todo $x \in G$.*

Definição 1.6.7 *Uma* ***representação monomial*** *é uma representação matricial $\overline{\mathcal{T}}$ de G tal que, para cada $g \in G$, $\overline{\mathcal{T}}(g)$ tem exatamente uma entrada não nula em cada linha e em cada coluna.*

Definição 1.6.8 *Seja $\mathcal{T} : G \to GL(V)$ uma representação de G sobre R. Um subespaço V' de V é dito* ***invariante*** *sob $\mathcal{T}$ (ou G-**invariante**) se $\mathcal{T}_{(x)}(V') \subset V'$, para todo $x \in G$.*

Observe que todo subespaço invariante sob $\mathcal{T}$ é um RG-submódulo do RG-módulo V no qual está contido.

Definição 1.6.9 *Uma representação $\mathcal{T} : G \to GL(V)$ é dita* ***irredutível*** *se os únicos subespaços de V que são invariantes sob $\mathcal{T}$ são $\{0\}$ e V. Caso contrário, dizemos que a representação $\mathcal{T}$ é* ***redutível****.*

Teorema 1.6.10 *([10], Proposição 9.5) As representações irredutíveis de um grupo abeliano finito sobre um corpo algebricamente fechado são todas de grau 1.*

Definição 1.6.11 *Seja G um grupo e seja V um espaço vetorial de dimensão finita sobre um corpo $\mathbb{F}$. Seja $\mathcal{T} : G \to GL(V)$ uma representação de G sobre $\mathbb{F}$. O* ***caracter*** *χ de G* ***associado à representação*** *$\mathcal{T}$ é a aplicação $\chi : G \to \mathbb{F}$ dada por $\chi(g) = tr(\mathcal{T}_g)$, para todo $g \in G$. Se a representação $\mathcal{T}$ é irredutível, então χ é um* ***caracter irredutível****.*

Se χ denota o caracter associado a uma representação $\mathcal{T} : G \to GL(V)$, o grau da representação também é chamado de **grau** do caracter χ, isto é,

$$\partial(\chi) = [V : \mathbb{F}].$$

Observe que se $car(\mathbb{F}) = 0$, então temos

$$\chi(1_G) = tr(\mathcal{T}_{1_G}) = tr(I) = [V : \mathbb{F}] = \partial(\chi).$$

Vemos no próximo teorema como caracterizar os idempotentes utilizando os caracteres de grupo.

Teorema 1.6.12 *([4], Teorema* 5.1.11*) Sejam G um grupo finito e $\mathbb{F}$ um corpo tal que $car(\mathbb{F}) \nmid |G|$. Os idempotentes centrais primitivos de $\mathbb{F}G$ são da seguinte forma*

$$e_i = \frac{1}{|G|} \sum_{x \in G} \chi_i(1)\chi(x^{-1})x.$$

Definição 1.6.13 *Sejam A uma $\mathbb{F}$-álgebra e V um A-módulo irredutível. V é dito* ***absolutamente irredutível*** *se $V^L = V \otimes_{\mathbb{F}} L$ é um $A^L = A \otimes_{\mathbb{F}} L$ módulo irredutível para toda extensão de corpo L sobre $\mathbb{F}$. Dizemos que L é um* ***corpo de decomposição*** *de A se todo A^L-módulo irredutível é absolutamente irredutível.*

Definição 1.6.14 *Seja $\mathbb{F}$ um corpo. Dizemos que uma representação irredutível $\mathcal{T}$ sobre $\mathbb{F}$ é* ***absolutamente irredutível*** *se $\mathcal{T}$ é irredutível sobre qualquer extensão de $\mathbb{F}$.*

Definição 1.6.15 *Seja G um grupo. Dizemos que L é um* ***corpo de decomposição*** *do grupo G, se todo LG-módulo irredutível é absolutamente irredutível, ou seja, se toda representação irredutível de G sobre L é absolutamente irredutível.*

Pelo Teorema 29.20, encontrado em [3], temos:

Observação 1.6.16 *Seja G um grupo finito, $\mathbb{F}$ um corpo de característica $car(\mathbb{F}) \nmid |G|$ e $\overline{\mathbb{F}}$ o fecho algébrico de $\mathbb{F}$. Então existe um corpo L tal que $\mathbb{F} \subset L \subset \overline{\mathbb{F}}$, com $[L : \mathbb{F}]$ finito, que é um corpo de decomposição de G.*

Finalizamos acrescentando que existe uma segunda definição para corpo de decomposição de um grupo, dada a seguir, que é equivalente à Definição 1.6.15 quando a ordem do grupo G é finita e o corpo de decomposição L é tal que $car(L) \nmid |G|$.

Definição 1.6.17 *Seja G um grupo finito. Dizemos que um corpo L tal que $car(L) \nmid |G|$ é um* ***corpo de decomposição*** *de G se*

$$LG \simeq \oplus_{i=1}^{r} M_{n_i}(L).$$

1.6.1 Representações Induzidas e Módulos Induzidos

Seja H um subgrupo de um grupo finito G, e seja $\mathbb{F}$ um corpo qualquer. Assumimos nesta subseção que todos os módulos são espaços vetoriais sobre $\mathbb{F}$ de dimensão finita. Como $\mathbb{F}H$ é uma subálgebra de $\mathbb{F}G$, todo $\mathbb{F}G$-módulo L é também um $\mathbb{F}H$-módulo, o qual vamos denotar por L_H. Assim, L_H tem o mesmo espaço vetorial que L, mas o domínio de operadores à esquerda é $\mathbb{F}H$ em vez de $\mathbb{F}G$. Uma representação matricial $\overline{\mathcal{T}}_H$ de H associada a L_H é obtida de uma representação matricial $\overline{\mathcal{T}}$ de G associada a L definindo

$$\overline{\mathcal{T}}_H = \overline{\mathcal{T}}|H.$$

Nosso objetivo é descrever uma construção, a qual associa a cada $\mathbb{F}H$-módulo M um $\mathbb{F}G$-módulo induzido M^G. Esta construção é um dos instrumentos básicos de toda a Teoria de Representações de Grupos.

Definição 1.6.18 *Seja H um subgrupo de G e seja M um $\mathbb{F}H$-módulo à esquerda. Então $\mathbb{F}G$ é um $(\mathbb{F}G, \mathbb{F}H)$-bimódulo e formamos o $\mathbb{F}G$-módulo $M^G = \mathbb{F}G \otimes_{\mathbb{F}H} M$ que é chamado **módulo induzido** por M. A representação de G associada a M^G é chamada **representação induzida**.*

Para encontrar M^G, começamos com a decomposição de G em uma união disjunta das classes laterais, ou seja,

$$G = g_1H \cup g_2H \cup ... \cup g_tH,$$

onde t=[G:H] e $g_1 = 1$. Todo elemento de G é expresso como um produto g_ih, para algum $1 \leq i \leq t$ e para algum $h \in H$, e então todo elemento de $\mathbb{F}G$ é expresso unicamente como

$$\sum_{i=1}^{t} g_ib_i,\ b_i \in \mathbb{F}H.$$

Assim, temos

$$\mathbb{F}G = g_1\mathbb{F}H \oplus g_2\mathbb{F}H \oplus ... \oplus g_t\mathbb{F}H,$$

tal que $\mathbb{F}G$ é um $\mathbb{F}H$-módulo à direita livre com base $\{g_1, g_2, ..., g_t\}$.

Pela Proposição 1.2.4, obtemos

$$M^G = (g_1\mathbb{F}H \otimes_{\mathbb{F}H} M) \oplus (g_2\mathbb{F}H \otimes_{\mathbb{F}H} M) \oplus ... \oplus (g_t\mathbb{F}H \otimes_{\mathbb{F}H} M),$$

o qual pode ser reescrito pelo Teorema 1.2.5 como uma soma direta de $\mathbb{F}H$-módulos:

$$M^G = (g_1 \otimes M) \oplus (g_2 \otimes M) \oplus ... \oplus (g_t \otimes M), \tag{1.7}$$

pela fórmula $g_i b \otimes m = g_i \otimes bm$, para todo $b \in \mathbb{F}H$ e $m \in M$.

Em (1.7), temos uma decomposição de M^G em $\mathbb{F}$-subespaços os quais são, em geral, nem $\mathbb{F}G$-submódulos, nem $\mathbb{F}H$-submódulos de M^G. Notemos que $g_i\mathbb{F}H \simeq \mathbb{F}H$ como submódulos à direita, com o isomorfismo sendo dado por $g_i b \mapsto b$, $b \in \mathbb{F}H$. Portanto, pelo Teorema 1.2.5,

$$g_i\mathbb{F}H \otimes_{\mathbb{F}H} M \simeq \mathbb{F}H \otimes_{\mathbb{F}H} M \simeq M.$$

Assim, temos um $\mathbb{F}$-isomorfismo $g_i\mathbb{F}H \otimes_{\mathbb{F}H} M \simeq M$ que é dado por $g_i b \otimes m \mapsto bm$, para todo $b \in \mathbb{F}H$ e para todo $m \in M$. Logo a dimensão do espaço vetorial M^G sobre $\mathbb{F}$ é dada por

$$[M^G : \mathbb{F}] = [G : H][M : \mathbb{F}],$$

onde $[G : H]$ é o número de classes laterais à esquerda distintas de H em G. E concluímos também que todo elemento de M^G pode ser expresso como $\sum g_i \otimes u_i$ com $u_1, u_2, ..., u_t$ unicamente determinados. Segue disto que se $\{m_1, m_2, ..., m_r\}$ é uma $\mathbb{F}$-base de M, então os elementos

$$\{g_i \otimes m_j : 1 \leq i \leq t, 1 \leq j \leq r\} \tag{1.8}$$

formam uma $\mathbb{F}$-base para M^G.

Agora dada uma representação matricial $\overline{\mathcal{T}}$ associada a M relativa a uma $\mathbb{F}$-base $\{m_1, m_2, ..., m_r\}$ de M tal que

$$hm_i = \sum \alpha_{ij}(h)m_j, \ \ \overline{\mathcal{T}}(h) = (\alpha_{ij}(h)), \ h \in H,$$

determina-se uma representação matricial $\overline{\mathcal{U}}$ associada a M^G, relativa a $\mathbb{F}$-base (1.8) de M^G, da seguinte maneira: expressamos $g(g_i \otimes m_j)$ como uma combinação linear dos elementos da base $\mathbb{F}$-base (1.8), escrevendo

$$gg_i = g_k h, \tag{1.9}$$

para algum $h \in H$ e para algum k, $1 \leq k \leq t$. Daí

$$g(g_i \otimes m_j) = gg_i \otimes m_j = g_k \otimes hm_j = \sum \alpha_{sj}(h)g_k \otimes m_s.$$

Agora por, (1.9), temos $h = g_k^{-1}gg_i$. Estendemos o domínio de definição de α_{sj} de H para G definindo $\alpha_{sj}(x) = 0$, para todo $x \in G$, $x \notin H$, e assim temos

$$g(g_i \otimes m_j) = \sum_{s=1}^{r}\sum_{k=1}^{t} \alpha_{sj}(g_k^{-1}gg_i) \cdot g_k \otimes m_s. \tag{1.10}$$

Organizamos os elementos da base (1.8) na ordem

$$g_1 \otimes m_1, ..., g_1 \otimes m_r, g_2 \otimes m_1, ..., g_2 \otimes m_r, ..., g_t \otimes m_1, ..., g_t \otimes m_r,$$

e pela equação (1.10) temos, para cada $g \in G$,

$$\overline{\mathcal{U}}(g) = \begin{array}{c} \begin{array}{ccc} & (i,1), ..., (i,r) & \\ \end{array} \\ \left(\begin{array}{c|c|c} * & * & * \\ \hline * & \overline{\mathcal{T}}(g_j^{-1} g g_i) & * \\ \hline * & * & * \end{array}\right) \begin{array}{l} (j,1) \\ \vdots \\ (j,r) \end{array} \end{array} ,$$

onde $\overline{\mathcal{T}}$ é estendida para todo elemento de G, definindo $\overline{\mathcal{T}}(x) = 0$, para todo $x \in G$, $x \notin H$. Assim, $\overline{\mathcal{U}}(g)$ é particionada em uma matriz $t \times t$ com blocos $r \times r$ e o bloco na j-ésima linha-bloco e i-ésima coluna-bloco é $\overline{\mathcal{T}}(g_j^{-1} g g_i)$.

$$\text{Assim, } \overline{\mathcal{U}}(g) = \begin{pmatrix} \overline{\mathcal{T}}(g_1^{-1} g g_1) & \dots & \overline{\mathcal{T}}(g_1^{-1} g g_t) \\ \vdots & \dots & \vdots \\ \overline{\mathcal{T}}(g_t^{-1} g g_1) & \dots & \overline{\mathcal{T}}(g_t^{-1} g g_t) \end{pmatrix}.$$

Como já sabemos calcular as representações induzidas de um grupo e módulos induzidos, podemos citar o próximo teorema que será utilizado no Capítulo 2.

Teorema 1.6.19 *([10], Teorema* 17.11*) As representações de grau* 1 *de um grupo G são exatamente as representações irredutíveis de $\frac{G}{G'}$ levantadas à G, onde G' é o subgrupo comutador de G. Em particular, o número de representações distintas de grau* 1 *de G é igual a $\left|\frac{G}{G'}\right|$, e assim divide $|G|$.*

Definição 1.6.20 *Uma cadeia descendente*

$$M = M_1 \supset M_2 \supset ... \supset M_{n-1} \supset M_n = 0$$

de submódulos é chamada uma ***série de decomposição*** *do módulo M. Os módulos quocientes $\frac{M_i}{M_{i+1}}$ são chamados* ***fatores de decomposição*** *da série.*

Definição 1.6.21 *Dois $\mathbb{F}G$-módulos(ou representações) L_1 e L_2 são ditos* ***disjuntos*** *se eles não possuem fatores de decomposição em comum.*

Os teoremas a seguir serão utilizados na demonstração dos Lemas 2.2.1 e 2.2.2.

Teorema 1.6.22 *([3], Corolário* 45.5*) Seja $H \lhd G$ e seja $\mathcal{T}$ uma representação irredutível de H. Então a representação induzida $\mathcal{T}^G$ é irredutível se, e somente se, para todo $x \notin H$, as representações de H, $\mathcal{T}$ e $\mathcal{T}^{(x)}$, onde $\mathcal{T}^{(x)}(h) = xhx^{-1}$ são disjuntas.*

Teorema 1.6.23 *([3], Teorema* 45.6*) Seja $\mathbb{F}$ um corpo algebricamente fechado tal que $car(\mathbb{F}) \nmid |G|$. Sejam H_1 e H_2 subgrupos de G, e sejam L_i $\mathbb{F}H_i$-módulos irredutíveis, $i \in \{1, 2\}$, tais que cada módulo induzido L_i^G é irredutível. Então L_1^G e L_2^G não são $\mathbb{F}G$-isomorfos se, e somente se, para todo $x \in G$, os $\mathbb{F}H^{(x)}$-módulos $x \otimes L_1$ e L_2 são disjuntos, onde $H^{(x)} = xH_1x^{-1} \cap H_2$.*

Capítulo 2

Grupos Metacíclicos e suas Representações

Neste capítulo, apresentamos fatos básicos sobre grupos metacíclicos finitos e representações irredutíveis sobre corpos de característica que não dividem a ordem do grupo metacíclico $G(M, N, R)$.

2.1 A Estrutura de um Grupo Metacíclico

Definição 2.1.1 *Um* ***grupo metacíclico*** G *é um grupo que contém um subgrupo normal cíclico* H *tal que* $\dfrac{G}{H}$ *é cíclico.*

Seja G um grupo metacíclico finito contendo um subgrupo cíclico normal $H = \langle a \rangle$ de ordem M e com um grupo quociente $\dfrac{G}{H} = \langle bH \rangle$ de ordem N. Assim, existe um inteiro t que $b^N = a^t$ e, para algum inteiro R, $bab^{-1} = a^R$. Ainda, como $\sigma : a^i \mapsto ba^ib^{-1}$ é um automorfismo de H, as potências de σ são determinadas por

$$\sigma^k(a) = b^k a b^{-k} = a^{R^k}. \tag{2.1}$$

Se σ tem ordem u, então

$$\begin{cases} R^k - 1 \not\equiv 0 \pmod{M} \\ R^u - 1 \equiv 0 \pmod{M}. \end{cases} \quad , \text{ para } 1 \leq k \leq u-1,$$

Os inteiros M, N, R, u, t devem satisfazer as seguintes condições adicionais:

$$\begin{aligned} &i) \quad mdc(M,R) = 1; \\ &ii) \quad M|t(R-1); \\ &iii) \quad u|N \text{ e, em particular, } R^N \equiv 1(mod\ M). \end{aligned} \tag{2.2}$$

De fato:

i) Como $R^u - 1 \equiv 0(mod\ M)$ temos:
$M|R^u - 1 \Rightarrow R^u - 1 = zM \Rightarrow mdc(R^u, M) = 1 \Rightarrow mdc(R, M) = 1.$

ii) Temos $a^t = b^N$. Daí
$(a^t)^R = \sigma(a^t) = ba^tb^{-1} = bb^Nb^{-1} = a^t \Rightarrow a^{tR} = a^t \Rightarrow a^{tR-t} = e \Rightarrow a^{t(R-1)} = e \Rightarrow M|t(R-1).$

iii) Temos $\sigma^N(a) = a^{R^N} = b^Nab^{-N} = (a^t)^Na(a^{-t})^N = a$. Portanto, $o(\sigma)|N \Rightarrow u|N$. Em particular, $a^{R^N-1} = e \Rightarrow M|R^N - 1 \Rightarrow R^N - 1 \equiv 0(mod\ M)$.

Desta maneira, os números M, N e R caracterizam o grupo metacíclico G e isto sugere a notação $G = G(M, N, R)$.

Usando as propriedades $i), ii)$ e $iii)$ verifica-se que os elementos de G podem ser escritos na forma

$$g = a^ib^j, \text{ para } 0 \leq i \leq M-1\,,\ 0 \leq j \leq N-1.$$

De agora em diante, denotaremos o grupo metacíclico $G(M, N, R)$ por G e consideraremos somente os grupos metacíclicos não abelianos de ordem ímpar, ou seja, aqueles cuja apresentação é

$$\langle a, b : a^M = 1, b^N = 1, ba = a^Rb\rangle, \tag{2.3}$$

onde $mdc(M, R) = 1$ e $R^N \equiv 1(mod\ M)\,,\ R \neq 1, N \neq 1$.

Lema 2.1.2 *O subgrupo comutador G' do grupo metacíclico G dado por (2.3) é o subgrupo $\langle a^{R-1}\rangle$ de ordem $\dfrac{M}{mdc(R-1, M)}$.*

Prova: Como todo subgrupo de um grupo cíclico é cíclico e, dada uma ordem para o subgrupo, ele é único, então é característico. Assim, todos os subgrupos de $\langle a \rangle$ são normais em G já que $\langle a \rangle \lhd G$. Portanto, podemos considerar o grupo quociente $\dfrac{G}{\langle a^{R-1} \rangle}$ e seja ν o homomorfismo natural $\nu : G \longrightarrow \dfrac{G}{\langle a^{R-1} \rangle}$. Aplicando ν à $bab^{-1} = a^R$ temos:

$$\nu(bab^{-1}) = \nu(a^R) = \nu(a \cdot a^{R-1}) = \nu(a)\nu(a^{R-1}) = \nu(a).$$

Daí $\nu(b)\nu(a)\nu(b^{-1}) = \nu(a)$ e, portanto, $\nu(b)\nu(a) = \nu(a)\nu(b)$. Logo $\dfrac{G}{\langle a^{R-1} \rangle}$ é abeliano e daí $G' \subset \langle a^{R-1} \rangle$.

Por outro lado, temos que $[b, a] \in G'$ é tal que:

$$[b, a] = bab^{-1}a^{-1} = a^R a^{-1} = a^{R-1}.$$

Portanto, $G' = \langle a^{R-1} \rangle$ e, como a ordem de a é M, segue que $|\langle a^{R-1} \rangle| = \dfrac{M}{mdc(R-1, M)}$.

■

2.2 As Representações dos Grupos Metacíclicos

Seja G um grupo metacíclico finito apresentado como em (2.3). Vamos ver mais adiante (Corolário 2.2.4) que quando N é primo, as representações irredutíveis de G sobre um corpo algebricamente fechado $\mathbb{K}$, são de grau 1 ou de grau N. Por este motivo, vamos falar destas representações absolutamente irredutíveis grau 1 e de grau N.

2.2.1 Representações Absolutamente Irredutíveis de Grau 1

Seja G' o subgrupo comutador de G. Pelo Lema 2.1.2, G' é o subgrupo cíclico $\langle a^{R-1} \rangle$ e tem ordem $P = \dfrac{M}{mdc(M, R-1)}$. Assim, $\dfrac{G}{G'}$ é isomorfo ao grupo abeliano $\mathbb{Z}_K \times \mathbb{Z}_N$, onde $K = \dfrac{M}{P} = mdc(M, R-1)$.

Como $\frac{G}{G'}$ é abeliano, segue das Proposições 1.6.10 e 1.6.2 que as representações de $\frac{G}{G'}$ são unidimensionais. Para cada representação irredutível $\mathfrak{U}_i$ de $\frac{G}{G'}$ da forma

$$\begin{array}{rccc} \mathfrak{U}_i & : & \frac{G}{G'} & \longrightarrow & GL(\mathbb{K}) \cong \mathbb{K}^* \\ & & gG' & \longmapsto & \mathfrak{U}_i(gG') \end{array},$$

definimos uma representação do grupo metacíclico G por $\mathcal{T}_i : G \to \mathbb{F}^*$ tal que

$$\mathcal{T}_i(g) = \begin{cases} 1, & \text{se} \quad g \in G' \\ \mathfrak{U}_i(gG'), & \text{se} \quad g \notin G' \end{cases}.$$

Pelo Teorema 1.6.19 existem KN representações unidimensionais distintas de G, onde $K = mdc(M, R-1)$. Logo as representações $\mathcal{T}_i$ são as KN representações absolutamente irredutíveis de grau 1 de G.

2.2.2 Representações Absolutamente Irredutíveis de Grau N

Para o subgrupo $H = \langle a \rangle$ do grupo metacíclico G existem exatamente M $\mathbb{K}H$-módulos unidimensionais não isomorfos, pela Proposição 1.6.10, já que esse subgrupo é abeliano. Denotaremos esses módulos por $L_i = \mathbb{K}l_i$, para $1 \leq i \leq M$. Seja ξ uma raiz M-ésima primitiva da unidade. A ação de a sobre L_i é dada por

$$al_i = \xi^i l_i, \text{ para cada } 1 \leq i \leq M.$$

Para calcular os módulos induzidos $L_i^G = \mathbb{K}G \otimes_{\mathbb{K}H} L_i$, notemos primeiro que as classes laterais à esquerda, $1H, bH, ..., b^{N-1}H$ são distintas, pois a ordem de $\frac{G}{H}$ é igual a N. Assim, L_i^G tem uma base sobre $\mathbb{K}$ dada por $\{1 \otimes l_i, b \otimes l_i, ..., b^{N-1} \otimes l_i\}$. As ações de a e b sobre os elementos da base são definidas por

$$b(b^k \otimes l_i) = b^{k+1} \otimes l_i, 0 \leq k < N-1,$$

$$b(b^{N-1} \otimes l_i) = 1 \otimes a^t l_i = \xi^{it}(1 \otimes l_i)$$

e por (2.1) temos:

$$a(b^k \otimes l_i) = b^k \otimes a^{R^k} l_i = \xi^{iR^k}(b^k \otimes l_i).$$

Seja $\overline{\mathcal{T}}_i$ a representação matricial de H dada por $\overline{\mathcal{T}}_i(a) = \xi^i$. Então a representação matricial induzida $\overline{\mathcal{T}}_i^G$ de G calculada com respeito à base $\{b^k \otimes l_i\}_{0\leq k\leq N-1}$ de L_i^G é dada por:

$$a \mapsto \overline{\mathcal{T}}_i^G(a) = \begin{pmatrix} \xi^i & 0 & 0 & \cdots & 0 \\ 0 & \xi^{iR} & 0 & \cdots & 0 \\ 0 & 0 & \xi^{iR^2} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \xi^{iR^{N-1}} \end{pmatrix},$$

$$b \mapsto \overline{\mathcal{T}}_i^G(b) = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & \xi^{it} \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 0 \end{pmatrix}.$$

Lema 2.2.1 *A representação matricial induzida $\mathcal{T}_l^G$ de G sobre $\mathbb{K}$ é irredutível se, e somente se, $R^j l \not\equiv l(mod\ M)$, para todo $1 \leq j \leq N-1$.*

Prova: Pelo Teorema 1.6.22 e pela Observação 1.6.5, a representação induzida $\mathcal{T}_l^G$ de G sobre $\mathbb{K}$ é irredutível se, e somente se, para todo $g = a^l b^j \notin \langle a \rangle$ temos $\mathcal{T}_l(a) \neq \mathcal{T}_l(gag^{-1})$, ou seja, $\xi^l \neq \mathcal{T}_l(a^l b^j a b^{-j} a^{-l}) = \mathcal{T}_l(a^{R^j}) = \xi^{lR^j}$, para todo $1 \leq j \leq N-1$. Por outro lado,
$\xi^l = \xi^{lR^j} \Leftrightarrow \xi^l(\xi^{lR^j - l} - 1) = 0 \Leftrightarrow \xi^{lR^j - l} = 1 \Leftrightarrow M | lR^j - l \Leftrightarrow lR^j - l \equiv 0(mod\ M)$
$\Leftrightarrow lR^j \equiv l(mod\ M)$.

Assim, como $\xi^l \neq \xi^{lR^j}$ para todo $1 \leq j \leq N-1$, segue que $R^j l \not\equiv l(mod\ M)$, para todo $1 \leq j \leq N-1$.

■

Lema 2.2.2 *Sejam $\overline{\mathcal{T}}_r^G$ e $\overline{\mathcal{T}}_s^G$ representações matriciais induzidas irredutíveis de G sobre $\mathbb{K}$. Então $\overline{\mathcal{T}}_r^G$ e $\overline{\mathcal{T}}_s^G$ são não equivalentes se, e somente se, temos $R^j r \not\equiv s(mod\ M)$, para todo $1 \leq j \leq N-1$.*

Prova: Pelo Teorema 1.6.23 e pela Observação 1.6.5, as representações matriciais induzidas $\overline{\mathcal{T}}_r^G$ e $\overline{\mathcal{T}}_s^G$ são não equivalentes se, e somente se, para todo $g \in G$, temos $\overline{\mathcal{T}}_s(a) \neq \overline{\mathcal{T}}_r(gag^{-1})$. Como $g = a^r b^j$, temos $\xi^s \neq \overline{\mathcal{T}}_r(a^r b^j a b^{-j} a^{-r}) = \overline{\mathcal{T}}_r(a^{R^j}) = \xi^{rR^j}$, para todo $1 \leq j \leq N-1$.

Por outro lado,

$$\xi^{rR^j} = \xi^s \Leftrightarrow \xi^s(\xi^{rR^j-s} - 1) = 0 \Leftrightarrow \xi^{rR^j-s} = 1 \Leftrightarrow M|rR^j - s \Leftrightarrow$$
$$\Leftrightarrow rR^j - s \equiv 0(mod\ M) \Leftrightarrow rR^j \equiv s(mod\ M).$$

Portanto, como $\xi^s \neq \xi^{rR^j}$ para todo $1 \leq j \leq N-1$, segue que $R^j r \not\equiv s(mod\ M)$, para todo $1 \leq j \leq N-1$.

■

Teorema 2.2.3 *Toda representação matricial irredutível de um grupo metacíclico G sobre $\mathbb{K}$ é ou unidimensional ou equivalente a uma das representações monomiais $\overline{T}_i^G$, para $1 \leq i \leq M$, se, e somente se, para cada i e j, $1 \leq i \leq M$, $1 \leq j \leq N-1$,*

$$R^j i \equiv i(mod\ M) \Rightarrow Ri \equiv i(mod\ M). \tag{2.4}$$

Prova: Suponha primeiro que, para cada i e j, $1 \leq i \leq M$, $1 \leq j \leq N-1$, $R^j i \equiv i(mod\ M)$ implica $Ri \equiv i(mod\ M)$.

Sejam $X = \{1, 2, 3, ..., M\}$ e a aplicação

$$\begin{array}{rccc} \varphi & : & X & \longrightarrow & X \\ & & x & \longmapsto & \varphi(x) = Rx(mod\ M). \end{array}$$

Assim, para cada j, $1 \leq j \leq N-1$, as aplicações φ e φ^j deixam os mesmos símbolos fixados pois, sejam $A = \{x \in X : \varphi(x) = x\}$ e $B = \{y \in X : \varphi^j(y) = y\}$ os conjuntos de elementos fixados por φ e φ^j, respectivamente. Temos $A \subset B$ e por hipótese, $\varphi^j(y) = R^j y \equiv y(mod\ M)$ implica $Ry = \varphi(y) \equiv y(mod\ M)$, ou seja, $B \subset A$.

Se P é o grupo gerado por φ, então por (2.2), P é um grupo finito cuja ordem divide N. Se φ tem ordem 1, então $\varphi = Id$. Suponhamos $\varphi \neq Id$ e $|\varphi| = t < N$. Assim, $\varphi^t(x) = R^t x = x$, para todo $x \in X$. Mas, por hipótese, isto implica $\varphi(x) = Rx = x$, para todo $x \in X$, ou seja, $\varphi = Id$, o que é uma contradição. Portanto, concluímos que a ordem de φ é ou 1 ou N.

Se φ tem ordem 1, então $R \equiv 1(mod\ M)$ e como $bab^{-1} = a$ segue que G é abeliano. Daí pelas Proposições 1.6.10 e 1.6.2, todas as representações irredutíveis de G são unidimensionais e assim, o teorema está provado.

Suponha agora que φ tenha ordem N. Particionamos o conjunto X em órbitas relativas à ação do grupo P. Como dois elementos x e y que estão em uma mesma P-órbita são equivalentes temos

$$x \sim_P y \Leftrightarrow \exists\, k \text{ tal que } \varphi^k(x) = y.$$

A hipótese implica que todo elemento que é fixado por qualquer potência de φ também é fixado em particular por φ e como as P-órbitas dos elementos fixados pela φ são unitárias, então os elementos fixados por potências de φ estão nas P-órbitas unitárias. Já os elementos que não são fixados por nenhuma potência de φ formam uma P-órbita com os N elementos $1, \varphi(x), \varphi^2(x), ..., \varphi^{N-1}(x)$. Portanto, toda P-órbita de X tem ou 1 ou N elementos.

Assim os Lemas 2.2.1 e 2.2.2 recebem a seguinte interpretação em termos destas P-órbitas:

1. O Lema 2.2.1 estabelece que a representação matricial induzida $\overline{\mathcal{T}}_i^G$ é irredutível se, e somente se, a órbita contendo i contém N elementos distintos, pois $\overline{\mathcal{T}}_i^G$ é irredutível se, e somente se, $R^j i \not\equiv i (mod\ M)$, para todo $1 \leq j \leq N-1$. Logo i não é fixado por nenhuma potência de φ e assim i não é fixado por φ e, portanto, i está numa órbita com N elementos.

2. O Lema 2.2.2 afirma que se i e i' pertencem à órbitas contendo N elementos cada, então $\overline{\mathcal{T}}_i^G$ e $\overline{\mathcal{T}}_{i'}^G$ são não equivalentes se, e somente se, estas órbitas são disjuntas.

Assim, o número de representações matriciais induzidas irredutíveis não equivalentes entre as $\overline{\mathcal{T}}_i^G$ é igual ao número de órbitas contendo N elementos. Este número será $\dfrac{M-K}{N}$, onde $K = mdc(R-1, M)$. Logo o número de representações matriciais induzidas irredutíveis entre as $\overline{\mathcal{T}}_i^G$, para todo $1 \leq i \leq M$, é exatamente $\dfrac{M-K}{N}$ e a soma dos quadrados dos graus destas representações é $\dfrac{(M-K)N^2}{N}$.

Por outro lado, o número de representações unidimensionais distintas pelo Teorema 1.6.19, é a ordem de $\dfrac{G}{G'}$ a qual é dada pelo Lema 2.1.2 e é igual a KN.

Assim, a soma dos quadrados dos graus das representações matriciais irredutíveis não equivalentes de G encontradas até agora é igual a

$$\frac{(M-K)N^2}{N} + KN = MN = |G|.$$

Portanto, do Corolário 1.4.28 segue que estas são todas as representações irredutíveis de G.

Reciprocamente, suponha que todas as representações irredutíveis de G ou têm grau 1 ou são equivalentes a uma das representações matriciais induzidas $\overline{\mathcal{T}}_i^G$, para

cada $1 \leq i \leq M$. Então, pelo Lema 2.1.2, existem KN representações unidimensionais distintas. Como antes, existem exatamente $K = mdc(R-1, M)$ órbitas unitárias em X. Para que $\frac{(M-K)N^2}{N} + KN = MN = |G|$, os elementos restantes devem se decompor em $\frac{M-K}{N}$ órbitas distintas, cada uma contendo N elementos distintos e isto implica a relação (2.4).

■

Corolário 2.2.4 *Seja G um grupo metacíclico com geradores a e b satisfazendo as relações*

$$bab^{-1} = a^R\,,\; b^N = a^t\,,\; a^M = 1,$$

onde M é a ordem de a, $mdc(M,R) = 1$, $m|t(R-1)$ e N é primo. Então todas as representações matriciais irredutíveis de G de sobre um corpo algebricamente fechado são ou unidimensionais ou representações monomiais $\overline{\mathcal{T}}^G$, onde $\overline{\mathcal{T}}$ é uma representação unidimensional do subgrupo $H = \langle a \rangle$ de G.

Prova: Por (2.2), a ordem do automorfismo

$$\begin{array}{rccc} \varphi \;:\; H & \longrightarrow & H \\ a^i & \longmapsto & ba^ib^{-1} \end{array}$$

é um fator de N e como N é primo, ou este automorfismo é a identidade e daí G é abeliano ou a ordem do grupo cíclico $P = \langle \varphi \rangle$ é igual a N. Sabemos que o número de elementos na órbita contendo x é igual a $[P : F_x]$, onde $F_x = \{\varphi^j \in P : \varphi^j(x) = x\}$. Assim, como N é primo ou F_x tem N elementos ou F_x tem 1 elemento.

Se F_x tem N elementos, então qualquer potência de φ fixa $x \in H$ e, em particular, φ fixa x. Se F_x tem 1 elemento, então φ não fixa x. Assim, $R^j i \equiv i(mod\ M)$ implica $Ri \equiv i(mod\ M)$. Portanto, pelo Teorema 2.2.3, segue o resultado.

■

Corolário 2.2.5 *Seja G um grupo metacíclico satisfazendo as hipóteses do Corolário 2.2.4. O número de representações irredutíveis distintas de G sobre um corpo algebricamente fechado é igual a*

$$NK + \frac{M-K}{N},$$

onde $K = mdc(M, R-1)$.

De modo geral, mesmo que N não seja primo temos o seguinte resultado:

Teorema 2.2.6 *Se G é um grupo metacíclico satisfazendo as hipóteses (2.3), então os módulos irredutíveis de G são ou unidimensionais ou componentes do módulo L^G, onde L é um módulo unidimensional de um subgrupo A de G.*

Prova: Considere o subgrupo $G_1 = \{e\}$ de G, e seja L_1 o único G_1-módulo unidimensional. Então por um lado, L_1^G é isomorfo ao módulo regular à esquerda ${}_{\mathbb{K}G}\mathbb{K}G$ e tal que todos os G-módulos são componentes de L_1^G. Por outro lado, pelo Teorema 38.4 em [3], temos

$$L_1^G \cong (L_1^A)^G.$$

Então $L_1^A = \oplus M_i$, onde os M_i são todos os A-módulos irredutíveis (e portanto, são unidimensionais). Pela Proposição 1.2.4, temos $L_1^G = \oplus M_i^G$, e o resultado segue da teoria de módulos completamente redutíveis. ■

Pelo teorema a seguir, vemos que todas as representações irredutíveis de G sobre um corpo algebricamente fechado são monomiais.

Teorema 2.2.7 *([3], Teorema 52.2) Seja G um grupo finito com um subgrupo normal abeliano H tal que $\frac{G}{H}$ é abeliano e seja $\mathbb{K}$ um corpo algebricamente fechado cuja característica não divide $|G|$. Então toda representação irredutível de G sobre $\mathbb{K}$ é monomial.*

Corolário 2.2.8 *Seja $G = G(M, N, R)$ um grupo metacíclico satisfazendo as hipóteses (2.3). O número de representações irredutíveis de G sobre um corpo algebricamente fechado $\mathbb{K}$ é dada por*

$$NK + \frac{M-K}{N},$$

onde $K = mdc(M, R-1)$.

Prova: Pelo Teorema 2.2.6, uma representação irredutível de G sobre $\mathbb{K}$ é ou unidimensional ou componente de um módulo L^G, onde L é um módulo unidimensional de um subgrupo de G. Pelo Teorema 1.6.19, o número de representações unidimensionais de G sobre $\mathbb{K}$ é NK, onde $K = mdc(M, R-1)$. Temos $|G| = MN$ e assim, $|G| - NK = (M-K)N$.

Para $H = \langle a \rangle$, temos $\dim L_i^G = N$, para cada $\mathbb{K}H$-módulo $L_i = \mathbb{K}l_i$, para cada $1 \leq i \leq M$. Estas representações são monomiais. Pelo Teorema 2.2.7 e pela demonstração do Teorema 2.2.3, existem $\frac{M-K}{N}$ representações irredutíveis deste tipo.

Como $|G| = MN = KN + \dfrac{(M-K)}{N}N^2$, as representações irredutíveis unidimensionais e as representações do tipo L_i^G formam um conjunto completo de representações irredutíveis de G sobre $\mathbb{K}$.

■

Exemplo 2.2.9 *Considere o grupo metacíclico $G = G(9,3,4)$, daí $G' \simeq \mathbb{Z}_3$ e $\dfrac{G}{G'} \cong \mathbb{Z}_3 \times \mathbb{Z}_3$. O Corolário 2.2.5 nos diz que existem 11 representações absolutamente irredutíveis de G sobre o fecho algébrico $\overline{\mathbb{F}}_2$ do corpo $\mathbb{F}_2$, as quais podem ser expressas sobre o corpo de decomposição de G, $L = \mathbb{F}_{2^6}$.*

Seja ω uma raiz cúbica primitiva da unidade.

As representações absolutamente irredutíveis de grau 1 são dadas por:

$$\overline{\mathcal{T}}_i(a) = \omega^{i(mod\,3)}, \overline{\mathcal{T}}_i(b) = \omega^j$$

para $0 \leq i < 9$ e $j = \left[\dfrac{i}{3}\right]$, onde $[\,]$ é a função maior inteiro.

Seja δ uma raiz nona primitiva da unidade.

Existem duas representações absolutamente irredutíveis não equivalentes de grau 3, já que o número de representações matriciais usuais é dada por $\dfrac{M-K}{N}$, onde $K = mdc(R-1, M)$. Estas representações são dadas por: $\overline{\mathcal{T}}_j(a) = (t_{rc})$, onde

$$t_{rc} = \begin{cases} \delta^{R^{r-1}}, & se\ \ r = c\ \ e\ \ j = 9 \\ \delta^{8R^{r-1}}, & se\ \ r = c\ \ e\ \ j = 10 \\ 0, & se\ \ r \neq c \end{cases}$$

e $\overline{\mathcal{T}}_j(b) = (t_{rc})$, onde

$$t_{rc} = \begin{cases} 1, & se\ \ r - 1 \equiv c(mod\ N) \\ 0, & se\ \ r - 1 \not\equiv c(mod\ N). \end{cases}$$

Exemplo 2.2.10 *Considere o grupo metacíclico $G = G(11,5,3)$, daí $G' \simeq \mathbb{Z}_{11}$. Pelo Corolário 2.2.5, existem 7 representações absolutamente irredutíveis de G sobre o fecho algébrico $\overline{\mathbb{F}}_2$ do corpo $\mathbb{F}_2$, as quais podem ser expressas sobre o corpo de decomposição de G, $L = \mathbb{F}_{2^{10}}$.*

Seja ω uma raiz quinta primitiva da unidade.

As representações absolutamente irredutíveis de grau 1 são dadas por:

$$\overline{\mathcal{T}}_i(a) = \omega^{i(mod\,5)}, \overline{\mathcal{T}}_i(b) = \omega^j$$

para $0 \leq i < 5$ *e* $j = \left[\frac{i}{5}\right]$, *onde* [ ] *é a função maior inteiro.*

Seja δ *uma raiz* 11*-ésima primitiva da unidade.*

Existem duas representações absolutamente irredutíveis não equivalentes de grau 5*, já que o número de representações matriciais usuais é dada por* $\frac{M-K}{N}$*, onde* $K = mdc(R-1, M)$*. Estas representações são dadas por*

$$\overline{\mathcal{T}}_5(a) = \begin{pmatrix} \delta^5 & 0 & 0 & 0 & 0 \\ 0 & \delta^4 & 0 & 0 & 0 \\ 0 & 0 & \delta & 0 & 0 \\ 0 & 0 & 0 & \delta^3 & 0 \\ 0 & 0 & 0 & 0 & \delta^9 \end{pmatrix}, \overline{\mathcal{T}}_6(a) = \begin{pmatrix} \delta^6 & 0 & 0 & 0 & 0 \\ 0 & \delta^7 & 0 & 0 & 0 \\ 0 & 0 & \delta^{10} & 0 & 0 \\ 0 & 0 & 0 & \delta^8 & 0 \\ 0 & 0 & 0 & 0 & \delta^2 \end{pmatrix}$$

$$e\ \overline{\mathcal{T}}_5(b) = \overline{\mathcal{T}}_6(b) = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

2.2.3 Representações Irredutíveis de $G = G(M, N, R)$ sobre um Subcorpo de um Corpo de Decomposição de G

Seja L um corpo de decomposição de $G = G(M, N, R)$ e $\mathbb{F} = \mathbb{F}_q$ um subcorpo de L com q elementos.

Observação 2.2.11 *De acordo com o Corolário* 9.23*, encontrado em [12], qualquer representação irredutível de* G *sobre* $\mathbb{F}$ *é uma soma direta de representações absolutamente irredutíveis* $\mathcal{T}_i$ *de* G *sobre* L*, onde as representações* $\mathcal{T}_i$ *são do mesmo grau; conforme veremos no Lema 3.4.14.*

Para calcular as representações irredutíveis de G sobre $\mathbb{F}$ que são formadas por somas de representações absolutamente irredutíveis sobre L de grau 1, escreveremos o par $\overline{\mathcal{T}}_i(a)$, $\overline{\mathcal{T}}_i(b)$ como (ξ^j, ω^t), onde ξ é uma raiz K-ésima primitiva da unidade e ω é uma raiz N-ésima primitiva da unidade. Assim formamos o conjunto

$$\mathfrak{L} = \{(\xi^l, \omega^m) : \exists h \,\text{tal que}\, l = q^h j (mod K) \,\text{e}\, \exists f \,\text{tal que}\, m = q^f t (mod K)\}.$$

Em outras palavras, um par (ξ^l, ω^m) pertence a $\mathfrak{L}$ se e somente se l é um elemento da q-classe ciclotômica que contém j e m é um membro da q-classe ciclotômica que contém t.

Os elementos de $\mathfrak{L}$ são representações de G. A soma de algumas destas representações produzem representações irredutíveis sobre $\mathbb{F}$.

Para determinar as representações absolutamente irredutíveis de grau N que deverão ser somadas, usaremos as representações matriciais usuais. Seja

$$\overline{\mathcal{T}}_i(a) = \begin{pmatrix} \delta^i & 0 & 0 & \cdots & 0 \\ 0 & \delta^{iR} & 0 & \cdots & 0 \\ 0 & 0 & \delta^{iR^2} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \delta^{iR^{N-1}} \end{pmatrix},$$

onde δ é uma raiz M-ésima primitiva da unidade e para $0 \leq i \leq M-1$. Os expoentes $i, iR, ..., iR^{N-1}$ formarão um conjunto para cada representação absolutamente irredutível de grau N. Este conjunto será chamado de **conjunto de potências associadas à** $\overline{\mathcal{T}}_i$.

Determinamos agora as q-classes ciclotômicas do conjunto dos inteiros módulo M. Particionamos o conjunto de todos os conjuntos de potências acima tais que a união das potências encontradas nos conjuntos agrupados é uma q-classe ciclotômica de $\{0, 1, ..., M-1\}$ ou uma união de tais classes. As representações cujos conjuntos de tais potências associadas foram combinadas são somandos diretos de uma representação que é irredutível sobre $\mathbb{F}$.

Como cada uma destas representações é uma soma direta de representações que podem ser expressas sobre L, cada representação está relacionada a uma representação matricial na qual as representações absolutamente irredutíveis são inseridas em sua diagonal. Assim, todas as entradas das representações matriciais estão em L. Alternativamente, representações matriciais podem ser encontradas nas quais todas as entradas são elementos de $\mathbb{F}$.

Exemplo 2.2.12 *Seja* $G = G(9, 3, 4)$. *Sejam* ω *uma raiz terceira primitiva da unidade e* δ *uma raiz nona primitiva da unidade. Representamos as* 9 *representações absolutamente irredutíveis usuais de grau* 1, $\overline{\mathcal{T}}_i$, *encontradas no Exemplo* 2.2.9 *como pares* $(\omega^{i(mod3)}, \omega^j)$, *onde* $j = \left[\frac{i}{3}\right]$ *para todo* i, $0 \leq i < 9$.

Estas representações absolutamente irredutíveis são agrupadas em 5 *conjuntos* $\mathfrak{L}_i$, $0 \leq i \leq 4$, *onde* $\mathfrak{L}_0 = \{(\omega^0, \omega^0)\}$, $\mathfrak{L}_1 = \{(\omega^1, \omega^0), (\omega^2, \omega^0)\}$, $\mathfrak{L}_2 = \{(\omega^0, \omega^1), (\omega^0, \omega^2)\}$, $\mathfrak{L}_3 = \{(\omega^1, \omega^1), (\omega^2, \omega^2)\}$, $\mathfrak{L}_4 = \{(\omega^2, \omega^1), (\omega^1, \omega^2)\}$.

Assim, as 5 *representações irredutíveis sobre* $\mathbb{F}_2$ *resultam em :*

$$\overline{\mathcal{D}}_0 = \overline{\mathcal{T}}_0\,,\ \overline{\mathcal{D}}_0(a) = 1\,,\ \overline{\mathcal{D}}_0(b) = 1,$$

$$\overline{\mathcal{D}}_1 = \overline{\mathcal{T}}_1 \oplus \overline{\mathcal{T}}_2\,,\ \overline{\mathcal{D}}_1(a) = \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix},\ \overline{\mathcal{D}}_1(b) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$\overline{\mathcal{D}}_2 = \overline{\mathcal{T}}_3 \oplus \overline{\mathcal{T}}_6\,,\ \overline{\mathcal{D}}_2(a) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ \overline{\mathcal{D}}_2(b) = \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix},$$

$$\overline{\mathcal{D}}_3 = \overline{\mathcal{T}}_4 \oplus \overline{\mathcal{T}}_8\,,\ \overline{\mathcal{D}}_3(a) = \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix},\ \overline{\mathcal{D}}_3(b) = \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix},$$

$$\overline{\mathcal{D}}_4 = \overline{\mathcal{T}}_5 \oplus \overline{\mathcal{T}}_7\,,\ \overline{\mathcal{D}}_4(a) = \begin{pmatrix} \omega^2 & 0 \\ 0 & \omega \end{pmatrix},\ \overline{\mathcal{D}}_4(b) = \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}.$$

Ambas as representações absolutamente irredutíveis de grau $N = 3$, $\overline{\mathcal{T}}_9$ e $\overline{\mathcal{T}}_{10}$, devem ser somadas, já que o conjunto das potências associadas com cada uma são $\{1, 4, 7\}$ e $\{8, 5, 2\}$ respectivamente e sua união é uma 2-classe ciclotômica de 9. Resultando em uma única representação irredutível sobre $\mathbb{F}_2$.

$$\overline{\mathcal{D}}_5 = \overline{\mathcal{T}}_9 \oplus \overline{\mathcal{T}}_{10}\,,\ \overline{\mathcal{D}}_5(a) = \begin{pmatrix} \delta & 0 & 0 & 0 & 0 & 0 \\ 0 & \delta^4 & 0 & 0 & 0 & 0 \\ 0 & 0 & \delta^7 & 0 & 0 & 0 \\ 0 & 0 & 0 & \delta^8 & 0 & 0 \\ 0 & 0 & 0 & 0 & \delta^5 & 0 \\ 0 & 0 & 0 & 0 & 0 & \delta^2 \end{pmatrix}, \overline{\mathcal{D}}_5(b) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Exemplo 2.2.13 *Seja $G = G(11, 5, 3)$. Sejam ω uma raiz quinta primitiva da unidade e δ uma raiz onze-ésima primitiva da unidade. Representamos as 5 representações absolutamente irredutíveis usuais de grau 1, $\overline{\mathcal{T}}_i$, encontradas no Exemplo 2.2.10 como pares $(\omega^{i(mod5)}, \omega^j)$, onde $j = \left[\frac{i}{5}\right]$ para todo i, $0 \leq i < 5$.*

Estas representações absolutamente irredutíveis são agrupadas em 2 conjuntos $\mathfrak{L}_i$, $0 \leq i \leq 2$, onde $\mathfrak{L}_0 = \{(\omega^0, \omega^0)\}$, $\mathfrak{L}_1 = \{(\omega^1, \omega^0), (\omega^2, \omega^0), (\omega^3, \omega^0), (\omega^4, \omega^0)\}$.

Assim, as 2 representações irredutíveis sobre $\mathbb{F}_2$ resultam em :

$$\overline{\mathcal{D}}_0 = \overline{\mathcal{T}}_0\,,\ \overline{\mathcal{D}}_0(a) = 1\,,\ \overline{\mathcal{D}}_0(b) = 1,$$

$$\overline{\mathcal{D}}_1 = \overline{\mathcal{T}}_1 \oplus \overline{\mathcal{T}}_2 \oplus \overline{\mathcal{T}}_3 \oplus \overline{\mathcal{T}}_4\,,\ \overline{\mathcal{D}}_1(a) = \begin{pmatrix} \omega & 0 & 0 & 0 \\ 0 & \omega^2 & 0 & 0 \\ 0 & 0 & \omega^3 & 0 \\ 0 & 0 & 0 & \omega^4 \end{pmatrix},\ \overline{\mathcal{D}}_1(b) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Ambas as representações absolutamente irredutíveis de grau $N = 5$, $\overline{\mathcal{T}}_5$ e $\overline{\mathcal{T}}_6$, devem ser somadas, já que o conjunto das potências associadas com cada uma são

$\{5,4,1,3,9\}$ *e* $\{6,7,10,8,2\}$ *respectivamente e sua união é uma* 2*-classe ciclotômica de* 11*. Resultando em uma única representação irredutível sobre* $\mathbb{F}_2$.

$$\overline{\mathcal{D}}_2 = \overline{\mathcal{T}}_5 \oplus \overline{\mathcal{T}}_6\,,\ \overline{\mathcal{D}}_2(a) = \begin{pmatrix} \delta^5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \delta^4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \delta & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \delta^3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \delta^9 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \delta^6 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \delta^7 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \delta^{10} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \delta^8 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \delta^2 \end{pmatrix},$$

$$\overline{\mathcal{D}}_2(b) = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Capítulo 3

Códigos de Grupo de Grupos Metacíclicos

Este é o principal capítulo deste trabalho. Como vimos na introdução, um **código de grupo** é simplesmente um ideal em uma álgebra de grupo $\mathbb{F}G$, onde $\mathbb{F}$ é um corpo e G é um grupo, ambos finitos. O nosso principal interesse é estudar os códigos corretores de erros metacíclicos que são ideais em álgebras de grupo do grupo metacíclico $G(M, N, R)$ de ordem ímpar, apresentado como em (2.3), sobre corpos de característica 2.

Iniciamos este capítulo com uma introdução à Teoria de Códigos Corretores de Erros, para estabelecer a linguagem utilizada nesta teoria e, em seguida, apresentamos os códigos lineares. Uma importante classe de códigos lineares é a dos códigos cíclicos que normalmente, na literatura introdutória, é apresentada utilizando-se a estrutura de anéis de polinômios, onde os códigos cíclicos são descritos como ideais no anel quociente $\frac{\mathbb{F}_q[x]}{\langle x^n - 1\rangle}$, com $\mathbb{F}_q$ um corpo finito que possui q elementos e n é um número natural que indica o comprimento do código.

Na seção 3.3, através de um isomorfismo entre o anel $\frac{\mathbb{F}_q[x]}{\langle x^n - 1\rangle}$ e a álgebra de grupo $\mathbb{F}_qC_n$ do grupo cíclico finito C_n de ordem n, fica estabelecida uma correspondência biunívoca entre os ideais no anel quociente de polinômios e os ideais da álgebra $\mathbb{F}_qC_n$. Desta maneira, descrevemos os códigos cíclicos como ideais na álgebra de grupo $\mathbb{F}_qC_n$.

De modo geral, pela Teoria de Anéis de Grupos, utilizando o Teorema de Maschke e o Teorema 1.3.21, um ideal ou código (minimal) de uma álgebra de grupo semissimples é gerado por um idempotente (primitivo). Para alguns códigos cíclicos,

utilizamos a estrutura de subgrupos do grupo cíclico para calcular os idempotentes centrais primitivos da álgebra de grupo geradores desses códigos. Além disso, citamos alguns resultados de Ferraz e Milies [18], que determinam sob que condições as álgebras de grupo abelianos sobre corpos finitos têm o mesmo número de componentes simples que as álgebras de grupo racionais de tais grupos.

Na seção 3.4, considerando a álgebra de grupo $\mathbb{F}G$ do grupo metacíclico $G = G(M, N, R)$ de ordem ímpar sobre um corpo $\mathbb{F}$ de característica 2, estabelecemos uma correspondência biunívoca entre o conjunto dos códigos centrais minimais distintos em $\mathbb{F}G$ e o conjunto das representações irredutíveis não equivalentes de G sobre $\mathbb{F}$. A partir deste resultado fazemos a decomposição da álgebra de grupo $\mathbb{F}G$ em códigos centrais minimais utilizando um conjunto completo de representações irredutíveis não equivalentes de G.

Verificamos ainda que existe uma equivalência combinatorial entre os códigos metacíclicos centrais e certos códigos abelianos e, particularmente, os códigos metacíclicos centrais minimais e os códigos cíclicos são combinatorialmente equivalentes.

Uma vez que vários resultados sobre códigos abelianos já são conhecidos, estamos interessados em códigos metacíclicos que não sejam combinatorialmente equivalentes a códigos abelianos, ou seja, em códigos centrais minimais que se decompõem em códigos minimais à esquerda. Esta decomposição em códigos minimais à esquerda primeiramente é feita com os códigos centrais minimais em LG, onde L é o corpo de decomposição de G e depois apresentamos um algoritmo para encontrar esta decomposição em $\mathbb{F}G$, onde $\mathbb{F}$ é um corpo finito de característica 2.

Apresentamos, na seção 3.6, dois exemplos de grupos metacíclicos: os diedrais de ordem $2n$ e os quatérnios generalizados de ordem $4n$. Para descrever os idempotentes centrais primitivos geradores dos códigos diedrais e quatérnios minimais, que possuem ordem par, não podemos utilizar as técnicas descritas nas seções anteriores, uma vez que a característica do corpo, neste caso, precisa ser ímpar. Descrevemos brevemente o trabalho de tese de doutorado de Dutra [9], no qual novas técnicas para encontrar os idempotentes geradores dos códigos diedrais e quatérnios são explicitadas e também desenvolvidas técnicas de codificação e de decodificação de tais códigos.

3.1 Noções da Teoria de Códigos Corretores de Erros

Seja $\mathcal{A}$ um conjunto finito qualquer que chamamos de **alfabeto**. O número de elementos de $\mathcal{A}$ é denotado por q.

Os elementos de $\mathcal{A}$ são chamados de **letras** ou **dígitos**. Uma sequência de elementos de $\mathcal{A}$ é dita uma **palavra**. O **comprimento** de uma palavra é o número de letras que compõem a palavra.

Consideramos $\mathcal{A}^n$ o conjunto de todas as palavras de comprimento n sobre $\mathcal{A}$, isto é, $\mathcal{A}^n = \{(c_0, c_1, ..., c_{n-1}) : c_i \in \mathcal{A}, 0 \leq i \leq n-1\}$.

Definição 3.1.1 *Um **código** é um subconjunto próprio qualquer de $\mathcal{A}^n$, para algum número natural n.*

Às vezes, para enfatizarmos o fato de que $\mathcal{A}$ tem q elementos, dizemos que um código $\mathcal{C} \subset \mathcal{A}^n$ é um **código de bloco q-ário**.

Exemplo 3.1.2 *Seja $\mathcal{A} = \{0, 1\}$. Considere o conjunto*

$$\mathcal{C} = \{00000, 01011, 10110, 11101\} \subset \mathcal{A}^5.$$

Pela definição, $\mathcal{C}$ é um código de bloco binário.

Definição 3.1.3 *Dados dois elementos x, y pertencentes a $\mathcal{A}^n$, a **distância de Hamming** entre x e y é o número de coordenadas em que x e y diferem, ou seja,*

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

Exemplo 3.1.4 *Se $x = 01011$ e $y = 11101$, então $d(x, y) = 3$.*

Definição 3.1.5 *Seja $\mathcal{C}$ um código. A **distância mínima** de $\mathcal{C}$ é o número*

$$d = min\{d(u, v) : u, v \in \mathcal{C} \, e \, u \neq v\}.$$

Exemplo 3.1.6 *Vamos encontrar a distância mínima de $\mathcal{C} = \{00000, 01011, 10110, 11101\}$. Assim,*

$$\begin{array}{lll} d(00000, 01011) = 3, & d(00000, 10110) = 3, & d(00000, 11101) = 4, \\ d(01011, 10110) = 4, & d(01011, 11101) = 3, & d(10110, 11101) = 3. \end{array}$$

Portanto, a distância mínima de $\mathcal{C}$ é 3.

A distância mínima d de um código é importante, pois ela nos fornece a capacidade de correção do código.

Definição 3.1.7 *Seja $\mathcal{C}$ um código com distância mínima d, chamamos de* ***capacidade de correção*** *de $\mathcal{C}$ ao número*

$$k = \left[\frac{d-1}{2}\right],$$

onde $[x]$ representa a parte inteira do número real x.

Teorema 3.1.8 *([2], Teorema 1) Seja $\mathcal{C}$ um código com distância mínima d. Então $\mathcal{C}$ pode detectar até $d-1$ erros e corrigir até $k = \left[\frac{d-1}{2}\right]$ erros.*

Um código sobre um alfabeto $\mathcal{A}$ possui três parâmetros fundamentais (n, m, d), que são respectivamente, o seu comprimento (o número n corresponde à dimensão do espaço ambiente $\mathcal{A}^n$ onde $\mathcal{C}$ se encontra), o seu número de elementos e a sua distância mínima.

O objetivo dos códigos corretores de erros é acrescentar dados adicionais à mensagem que iremos transmitir ou armazenar de forma que nos permita recuperá-la detectando e corrigindo possíveis erros. O processo de adicionar dados à mensagem é chamado de **codificação**. E o processo de recuperação da mensagem é chamado de **decodificação**.

3.2 Códigos Lineares

Os códigos interessantes são aqueles cujo espaço ambiente possui alguma estrutura algébrica. Para isto, começamos escolhendo o alfabeto como um corpo finito $\mathbb{F}_q$ com q elementos e o código será um conjunto de palavras que forma um subespaço vetorial não trivial de $\mathbb{F}_q^n$. Um tal código será chamado **código linear**.

Definição 3.2.1 *Dada uma palavra $u = (u_0, u_1, ..., u_{n-1})$ de $\mathbb{F}_q^n$ definimos o* ***peso*** *de u como sendo o seu número de coordenadas não nulas, isto é,*

$$\omega(u) = |\{i : u_i \neq 0\,,\, 0 \leq i \leq n-1\}|.$$

Em outras palavras, temos

$$\omega(u) = d(u, 0),$$

onde d é a distância de Hamming de $\mathcal{C}$.

Definição 3.2.2 *O* ***peso de um código linear*** $\mathcal{C}$ *é o inteiro*

$$\omega(\mathcal{C}) = min\{\omega(u) : u \in \mathcal{C} \, e \, u \neq 0\}.$$

Proposição 3.2.3 *([2], Proposição 1) Se* $\mathcal{C} \subset \mathbb{F}_q^n$ *é um código linear com distância mínima* d*, então*

i) para todos $x, y \in \mathcal{C}, d(x, y) = \omega(x - y)$,

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

3.3 Códigos Cíclicos

Os códigos cíclicos são muito utilizados por formarem uma classe de códigos lineares que possui bons algoritmos de codificação e de decodificação.

Definição 3.3.1 *Um código linear* $\mathcal{C} \subset \mathbb{F}_q^n$ *é chamado* ***código cíclico*** *se, para todo* $c = (c_0, c_1, ..., c_{n-1})$ *pertencente a* $\mathcal{C}$*, a palavra* $(c_{n-1}, c_0, ..., c_{n-2})$ *também pertence a* $\mathcal{C}$*.*

Observamos que o espaço vetorial $\mathbb{F}_q^n$ pode ser construído de diversas maneiras. Apresentamos duas delas.

Seja R_n o anel das classes residuais em $\mathbb{F}_q[x]$ módulo $x^n - 1$, isto é, $R_n = \dfrac{\mathbb{F}_q[x]}{\langle x^n - 1 \rangle}$.

Um elemento de R_n é, portanto, um conjunto da forma

$$\overline{f(x)} = \{f(x) + g(x)(x^n - 1) : g(x) \in \mathbb{F}_q[x]\}.$$

Assim, R_n é um $\mathbb{F}_q$-espaço vetorial de dimensão n com base $\{\overline{1}, \overline{x}, ..., \overline{x^{n-1}}\}$ e daí $\mathbb{F}_q^n$ é isomorfo a R_n através da transformação linear

$$\begin{array}{rccc} \nu : & \mathbb{F}_q^n & \longrightarrow & R_n \\ & (a_0, a_1, ..., a_{n-1}) & \longmapsto & \overline{a_0} + \overline{a_1 x} + ... + \overline{a_{n-1} x^{n-1}} \end{array} .$$

Então todo código linear $\mathcal{C} \subset \mathbb{F}_q^n$ pode ser transportado para R_n pelo isomorfismo ν e aí estudado. A vantagem de R_n sobre $\mathbb{F}_q^n$ é que, no primeiro temos, além da estrutura de espaço vetorial, uma estrutura adicional de anel.

Assim, pelo Teorema 1 em [2], p. 111, um código cíclico é visto como um ideal de R_n.

Dado um ideal I de R_n, sabemos que existe um único polinômio mônico g de $\mathbb{F}_q[x]$, que é um divisor de $x^n - 1$, cuja classe em R_n gera I. Este polinômio é chamado **polinômio gerador** de I.

Além disso, o polinômio $h = \dfrac{x^n - 1}{g}$ é tal que sua classe módulo R_n anula o ideal I e por essa razão é chamado de **polinômio teste** de I.

Portanto, se $mdc(q, n) = 1$, então g e h são primos entre si e existem polinômios $r, s \in \mathbb{F}_q[x]$ tais que $rg + sh = 1$. Ainda temos $I = \langle \overline{e} \rangle = R_n\overline{e}$ e $\overline{e}^2 = \overline{e}$, onde $\overline{x}\,\overline{e} = \overline{x}$, para todo $\overline{x} \in I$, isto é, todo ideal I de R_n é gerado por um idempotente que é a identidade de I.

Assim, se um dos polinômios g ou e são conhecidos, então o outro pode ser encontrado de acordo com as fórmulas $e = rg$ e $g = mdc(x^n - 1, e)$. Daí podemos descrever os ideais em R_n.

Se denotamos por $C_n = \langle a : a^n = 1 \rangle$ o grupo cíclico de ordem n, temos

$$R_n \cong \mathbb{F}_q C_n,$$

onde $\mathbb{F}_q C_n$ é a álgebra de grupo do grupo C_n sobre $\mathbb{F}_q$.

Neste isomorfismo, os elementos de $\mathbb{F}_q C_n$ correspondentes a g, h e e de R_n são dados por $g(a), h(a)$ e $e(a)$, onde a é um gerador de C_n.

Assim, códigos cíclicos (de comprimento n) são definidos também como ideais da álgebra de grupo $\mathbb{F}_q C_n$.

A vantagem de se trabalhar com álgebra de grupo $\mathbb{F}_q C_n$ ao invés de R_n é que evitamos fazer quociente de polinômios, o que é muito trabalhoso.

Pelo Corolário 1.4.26, quando o $mdc(q, n) = 1$ a álgebra de grupo $\mathbb{F}_q C_n$ é semissimples, ou seja, é escrita como uma soma direta de ideais bilaterais minimais e todos os outros ideais desta álgebra são determinados como uma soma destes ideais minimais.

Assim, dizemos que um **código cíclico minimal** é um ideal minimal da álgebra de grupo semissimples $\mathbb{F}_q C_n$. E para conhecermos os geradores dos códigos cíclicos minimais, basta conhecermos os idempotentes centrais primitivos de $\mathbb{F}_q C_n$.

Os idempotentes centrais primitivos de $\mathbb{F}_q C_n$ podem ser encontrados através dos idempotentes centrais primitivos de LC_n, onde L é o corpo de decomposição

de C_n. Para isto, consideremos a representação $\mathcal{T}_i : C_n \to GL(1, L)$ definida por $\mathcal{T}_i(a^j) = \xi^{ij}$, para todo $1 \leq i \leq n$, onde ξ é uma raiz n-ésima primitiva da unidade em L e $L = \mathbb{F}_q(\xi)$.

Observe que $L = \mathbb{F}_q(\xi) \subset \overline{\mathbb{F}}_q$ e $\mathbb{F}_q(\xi)$ é o corpo de decomposição de C_n. Assim, as representações $\mathcal{T}_i$ são absolutamente irredutíveis sobre L.

Observamos também que as diferentes representações de C_n sobre L de grau 1 são irredutíveis e não equivalentes, duas a duas. De fato, sejam $\overline{\mathcal{T}_i}$ e $\overline{\mathcal{T}_j}$ representações matriciais de C_n sobre L de grau 1, para $i, j = 1, 2, ..., n$. Se $\overline{\mathcal{T}_i}$ e $\overline{\mathcal{T}_j}$ são equivalentes, então existe um escalar $\alpha \in L$ tal que $\overline{\mathcal{T}_i}(x) = \alpha\overline{\mathcal{T}_j}(x)\alpha^{-1}$, isto é, $\overline{\mathcal{T}_i} = \overline{\mathcal{T}_j}$, para todo $x \in C_n$. Como C_n tem no máximo $|C_n| = n$ representações irredutíveis não equivalentes, segue que estas são todas as possíveis representações irredutíveis de C_n sobre L e são todas de grau 1.

Logo os caracteres irredutíveis de C_n sobre $\mathbb{F}_q$ são as funções $\chi_i : C_n \to L$ definidas por

$$\chi_i(a^j) = \xi^{ij} \text{ , para todo } 1 \leq i \leq n.$$

Assim, pelo Teorema 1.6.12 e como $\chi_i(y^{-j}) = \xi^{-ij}$, para todo $y \in C_n$ e $\chi_i(1) = 1$, podemos escrever os idempotentes centrais primitivos de LC_n na seguinte forma:

$$e_i = \frac{1}{n}\sum_{j=0}^{n-1}(\xi^i)^{-j}a^j \text{ , para todo } 0 \leq i \leq n-1.$$

Seja $E = \{e_i : 0 \leq i \leq n-1\}$ o conjunto dos idempotentes centrais primitivos de LC_n. Seja o grupo $J = Aut_{\mathbb{F}_q}(\mathbb{F}_q(\xi))$ que é gerado pelo automorfismo de Frobenius

$$\begin{array}{rccc} \sigma & : & \mathbb{F}_q(\xi) & \longrightarrow & \mathbb{F}_q(\xi). \\ & & \xi & \longmapsto & \xi^q \end{array}$$

A ação de J sobre E, particiona E em órbitas disjuntas. É fácil ver que a soma dos elementos de cada órbita é um idempotente e provemos que essa soma é fixada pela ação de J sobre LC_n. De fato, suponha que $l + 1$ seja a ordem de J. Daí $J = \{e, \sigma, \sigma^2, ..., \sigma^l\}$.

Sejam $\sigma(e_i) = \sum \sigma(\xi^{ij})a^j = \xi^{qij}a^j$, $\sigma^2(e_i) = \sum \sigma^2(\xi^{ij})a^j = \xi^{q^2ij}a^j, ...,$ $\sigma^l(e_i) = \sum \sigma^l(\xi^{ij})a^j = \xi^{q^lij}a^j$.

Considere a órbita do e_i, $orb(e_i) = \{e_i = \sigma^{l+1}(e_i), \sigma(e_i), ..., \sigma^l(e_i)\}$. Daí

$$\begin{aligned} \sigma(e_i + \sigma(e_i) + \sigma^2(e_i) + ... + \sigma^l(e_i)) &= e_i + \sigma(e_i) + \sigma^2(e_i) + ... + \sigma^l(e_i) \\ &= \sum(\xi^{ij} + \xi^{qij} + \xi^{q^2ij} + ... + \xi^{q^lij})a^j. \end{aligned}$$

Assim, a soma dos idempotentes primitivos numa órbita é fixada pela σ.

Os coeficientes de cada um desses elementos fixados pela σ são também fixados pela ação de σ em $\mathbb{F}_q(\xi) = L$. Assim, os coeficientes de cada um desses elementos fixados são expressões nas potências de ξ que estão no corpo $\mathbb{F}_q$.

Portanto, cada idempotente central primitivo de $\mathbb{F}_qC_n$ é formado pela soma dos idempotentes centrais primitivos de LC_n que estão numa mesma órbita.

Como no caso dos ideais, todos os códigos cíclicos estarão determinados a partir dos códigos cíclicos minimais. Devido a essa identificação entre códigos e ideais, todas as definições de peso e distância mínima feitas para códigos lineares podem ser atribuídas aos ideais.

Observação 3.3.2 *O número de componentes simples da álgebra de grupo do grupo cíclico C_n sobre os racionais é menor ou igual ao número de componentes simples da álgebra de grupo $\mathbb{F}_qC_n$, para qualquer corpo finito $\mathbb{F}_q$ tal que $car(\mathbb{F}_q) \nmid n$.*

De fato:

Se $\mathbb{E}$ é um corpo qualquer tal que $car(\mathbb{E}) \nmid n$ e $f_1, f_2, ..., f_t$ são os polinômios irredutíveis de $\mathbb{E}[x]$ tais que $x^n - 1 = f_1(x)f_2(x)...f_t(x)$, então estes polinômios são distintos, separáveis e não possuem raízes em comum e, pelo Teorema Chinês do Resto, temos

$$\mathbb{E}C_n \simeq \frac{\mathbb{E}[x]}{\langle x^n - 1\rangle} \simeq \frac{\mathbb{E}[x]}{\langle f_1\rangle} \oplus \frac{\mathbb{E}[x]}{\langle f_2\rangle} \oplus ... \oplus \frac{\mathbb{E}[x]}{\langle f_t\rangle},$$

de modo que $\mathbb{E}C_n$ tem t componentes simples. Se $\mathbb{E} = \mathbb{Q}$, então t é igual ao número de divisores de n, já que os fatores irredutíveis de $x^n - 1$ sobre $\mathbb{Q}$ são os polinômios ciclotômicos. Se $\mathbb{E} = \mathbb{F}_q$, um corpo finito com q elementos, então algum dos polinômios ciclotômicos pode ser redutível sobre $\mathbb{F}_q$, fazendo com que a álgebra de grupo $\mathbb{F}_qC_n$ possa ter mais componentes simples que a álgebra de grupo $\mathbb{Q}C_n$.

Agora, damos a descrição dos idempotentes centrais primitivos de $\mathbb{Q}C_n$ e em seguida vemos quais são as álgebras de grupo de grupos cíclicos sobre corpos finitos que utilizam a mesma fórmula para o cálculo de seus idempotentes.

O próximo lema nos auxilia na determinação dos idempotentes centrais primitivos geradores de alguns códigos cíclicos, utilizando a estrutura dos subgrupos do grupo cíclico de ordem p^m, onde p é um número primo.

Lema 3.3.3 *([5], Lema 1.2) Seja C_{p^m} o grupo cíclico de ordem p^m gerado por a, $m \geq 1$. Considere*

$$C_{p^m} = A_0 \supset A_1 \supset ... \supset A_m = 1$$

a cadeia descendente de subgrupos cíclicos de C_{p^m}, onde $A_i = \langle a^{p^i} \rangle$. Então os idempotentes centrais primitivos de $\mathbb{Q}C_{p^m}$ são

$$e_0 = \widehat{A}_0 \ \ e \ \ e_i = \widehat{A}_i - \widehat{A}_{i-1}, \ para \ 1 \leq i \leq m,$$

onde $\widehat{A}_j = \dfrac{1}{|A_j|} \sum_{x \in A_j} x$. Além disso, $\mathbb{Q}C_{p^m}(e_i) \simeq \mathbb{Q}(\xi_{p^i})$, onde ξ_{p^i} denota uma raiz primitiva da unidade.

Teorema 3.3.4 *([5], Teorema 1.4(2)) Seja G um grupo abeliano finito escrito como produto direto de p_i-subgrupos de Sylow G_i de G, isto é, $G = G_1 \times G_2 \times ... \times G_t$, para primos distintos $p_1, p_2, ..., p_t$. Então os idempotentes centrais primitivos de $\mathbb{Q}C_n$ são produtos da forma $e_1 e_2 ... e_t$, onde e_i é um idempotente central primitivo de $\mathbb{Q}G_i$.*

Quando $\mathbb{F}_q C_n$ é semissimples e possui o mesmo número de componentes simples que a álgebra de grupo $\mathbb{Q}C_n$, os idempotentes centrais primitivos de $\mathbb{F}_q C_n$ serão dados pela mesma fórmula que os idempotentes centrais primitivos de $\mathbb{Q}C_n$ (com os coeficientes entendidos como elementos de $\mathbb{F}_q$).

No caso em que n é uma potência de um primo p, um idempotente e é uma diferença da forma $\widehat{H} - \widehat{H}^*$, onde H e H^* são subgrupos de C_n com $\left|\dfrac{H^*}{H}\right| = p$ ou simplesmente $e = \widehat{H}$, com $H = C_n$. De qualquer modo, o idempotente $\widehat{H}$ pode ter seus coeficientes entendidos como elementos de $\mathbb{F}_q$, pois todos os coeficientes deste idempotente são iguais a $\dfrac{1}{|H|}$ e $|H|$ divide n que é relativamente primo com a característica do corpo $\mathbb{F}_q$.

O novo conjunto de idempotentes ainda continua contendo elementos centrais, dois a dois ortogonais, somam 1 e nenhum deles pode ser escrito como soma de dois idempotentes centrais ortogonais e não nulos, pois caso contrário, também o seriam sobre $\mathbb{Q}$.

Assim, nessas condições, diremos que os idempotentes de $\mathbb{F}_q C_n$ e $\mathbb{Q}C_n$ são os mesmos.

Exemplo 3.3.5 *Vamos encontrar os idempotentes de $\mathbb{F}_3 C_8$.*

Os subgrupos de C_8 são: $C_8 = \langle a \rangle, C_4 = \langle a^2 \rangle, C_2 = \langle a^4 \rangle$ e $C_1 = \langle a^8 \rangle = \{1\}$.

Temos $\left|\dfrac{C_8}{C_4}\right| = \left|\dfrac{C_4}{C_2}\right| = \left|\dfrac{C_2}{C_1}\right| = 2$.

Assim, pelo que vimos acima, os idempotentes de $\mathbb{F}_3 C_8$ são:

$$e_1 = \widehat{C_8} = 2 + 2a + 2a^2 + 2a^3 + 2a^4 + 2a^5 + 2a^6 + 2a^7,$$
$$e_2 = \widehat{C_4} - \widehat{C_8} = 2 + a + 2a^2 + a^3 + 2a^4 + a^5 + 2a^6 + a^7,$$
$$e_3 = \widehat{C_2} - \widehat{C_4} = 1 + 2a^2 + a^4 + 2a^6 \; e$$
$$e_4 = \widehat{C_1} - \widehat{C_2} = 2 + a^4.$$

Estamos interessados em saber agora sob que condições sobre q e n as álgebras de grupos $\mathbb{F}_q C_n$ e $\mathbb{Q}C_n$ têm o mesmo número de componentes simples. Em [18], Ferraz e Milies garantem quando álgebras de grupos abelianos sobre corpos finitos têm o mesmo número de componentes simples que as álgebras de grupos racionais de tais grupos. A seguir fazemos um breve resumo deste trabalho, enfatizando o resultado sobre os grupos cíclicos.

Relembramos que a **q-classe ciclotômica** de h em A, onde A é um grupo abeliano finito, é o conjunto

$$S_h = \{h^{q^j} \; : \; 0 \leq j \leq t_h - 1\},$$

onde t_h é o menor inteiro positivo tal que

$$q^{t_h} \equiv 1 (mod\, o(h))$$

e $o(h)$ denota a ordem de h.

Note que se $x \in S_h$, então $x = h^{q^j}$, para algum j. Como $mdc(q, o(h)) = 1$ segue que o subgrupo $\langle x \rangle = \langle h \rangle$. Portanto, cada q-classe ciclotômica S_h é um subconjunto do conjunto $\mathcal{G}_h$ de todos os geradores do grupo cíclico $\langle h \rangle$.

Pelo Corolário 1.5.2, o número de componentes simples da álgebra de grupo racional de um grupo abeliano finito A é igual ao número de subgrupos cíclicos de A. Assim, o número de subgrupos cíclicos de A é uma cota inferior para o número de componentes simples e esta cota é obtida se, e somente se, $S_h = \mathcal{G}_h$, para todo $h \in A$.

Para inteiros positivos r e m, denotaremos por $\overline{r} \in \mathbb{Z}_m$ a imagem de r no anel dos inteiros módulo m. Então,

$$\mathcal{G}_h = \{h^r / mdc(r, o(h)) = 1\} = \{h^r / \overline{r} \in \mathcal{U}(\mathbb{Z}_{o(h)})\}.$$

Definição 3.3.6 *O* ***expoente*** *de um grupo G é o menor inteiro positivo m tal que $g^m = e$, para todo $g \in G$, onde e é o elemento neutro do grupo.*

Teorema 3.3.7 *([18], Teorema 2.2) Sejam $\mathbb{F}$ um corpo finito com $|\mathbb{F}| = q$ elementos e A um grupo abeliano finito de expoente e, tal que $mdc(q, |A|) = 1$. Então $S_h = \mathcal{G}_h$, para todo $h \in A$ se e somente se $\mathcal{U}(\mathbb{Z}_e)$ é um grupo cíclico gerado por $\overline{q} \in \mathbb{Z}_e$.*

Teorema 3.3.8 *([14] , Teorema 21) O grupo $\mathcal{U}(\mathbb{Z}_e)$ é cíclico se, e somente se, $e = 2, 4, p^n$ ou $2p^n$, onde p é um inteiro primo ímpar e n é um inteiro positivo.*

Corolário 3.3.9 *([18], Corolário 2) Sejam $\mathbb{F}$ um corpo finito com $|\mathbb{F}| = q$ elementos, A um grupo abeliano finito de expoente e, tal que $mdc(q, |A|) = 1$. Então $S_h = \mathcal{G}_h$, para todo $h \in A$ se, e somente se, uma das afirmações acontece:*

i) $e = 2$ *e* q *é ímpar;*

ii) $e = 4$ *e* $q \equiv 3(mod 4)$;

iii) $e = p^n$ *e* $o(q) = \phi(p^n)$ *em* $\mathcal{U}(\mathbb{Z}_{p^n})$*, onde* ϕ *é a função de Euler;*

iv) $e = 2p^n$ *e* $o(q) = \phi(p^n)$ *em* $\mathcal{U}(\mathbb{Z}_{2p^n})$.

Encerramos esta seção com a definição de códigos de grupo.

Definição 3.3.10 *Se $\mathbb{F}$ um corpo finito e G um grupo finito. Um* ***código de grupo*** *é um ideal na álgebra de grupo $\mathbb{F}G$. Um* ***código central (minimal)*** *é um ideal bilateral (minimal) desta álgebra.*

Quando o grupo considerado é abeliano (metacíclico), dizemos que o código é **abeliano (resp. metacíclico)**.

3.4 Códigos Metacíclicos

Nesta primeira subseção vemos resultados gerais sobre códigos centrais minimais de $\mathbb{F}H$ para H um grupo finito qualquer e $\mathbb{F}$ um corpo tal que $car(\mathbb{F}) \nmid |H|$. A segunda subseção é dedicada aos códigos metacíclicos não abelianos de ordem ímpar que são apresentados como em (2.3).

Na última subseção estudamos os códigos à esquerda (ideais à esquerda), os quais são combinatorialmente equivalentes a códigos não abelianos.

3.4.1 Decomposição de $\mathbb{F}H$ em Códigos Centrais Minimais

Nesta subseção determinamos a decomposição de $\mathbb{F}H$, onde H é um grupo finito qualquer e $\mathbb{F}$ é um corpo tal que $car(\mathbb{F}) \nmid |H|$ em códigos centrais minimais utilizando resultados sobre representações dos grupos, apresentados no Capítulo 1.

Pelo Corolário 1.4.26, $\mathbb{F}H$ é semissimples e unicamente decomposta em uma soma direta de códigos centrais minimais. Esta decomposição de $\mathbb{F}H$ pode ser determinada por um conjunto de representações irredutíveis conforme o resultado a seguir. Para este resultado, precisamos saber que uma representação $\mathcal{T}$ de H com espaço representação V é estendida a uma representação $\mathcal{T}'$ de $\mathbb{F}H$ com espaço representação V da seguinte maneira:

$$\mathcal{T}'\Big(\sum_{g\in H}\alpha_g g\Big) = \sum_{g\in H}\alpha_g \mathcal{T}(g).$$

Lema 3.4.1 *Seja $\{\mathcal{T}_0, \mathcal{T}_1, ..., \mathcal{T}_{h-1}\}$ um conjunto completo de representações irredutíveis não equivalentes de H sobre $\mathbb{F}$. Para todo i, $0 \leq i < h$, o conjunto $\mathfrak{C}_i$ definido por*

$$\mathfrak{C}_i = \{c \in \mathbb{F}H : \mathcal{T}_j(c) = 0, \text{ para todo } j,\ 0 \leq j \leq h-1\,, j \neq i\} \tag{3.1}$$

é um código central minimal em $\mathbb{F}H$.

Prova: O conjunto $\mathfrak{C}_i$ é não vazio, pois como $0 = 0\cdot g_0 + 0\cdot g_1 + 0\cdot g_2 + ... + 0\cdot g_n \in \mathbb{F}H$ e $\mathcal{T}_j(0) = \mathcal{T}_j(0\cdot g_0 + 0\cdot g_1 + 0\cdot g_2 + ... + 0\cdot g_n) = 0\cdot\mathcal{T}_j(g_0) + 0\cdot\mathcal{T}_j(g_1) + 0\cdot\mathcal{T}_j(g_2) + ... + 0\cdot\mathcal{T}_j(g_n) = 0$, já que $\mathcal{T}_j$ é uma representação de álgebra de grupo para todo j, $0 \leq j \leq h-1$.

Sejam $c, d \in \mathfrak{C}_i$. Daí $c, d \in \mathbb{F}H$, $\mathcal{T}_j(c) = 0$ e $\mathcal{T}_j(d) = 0$, para todo j, $0 \leq j \leq h-1$, $j \neq i$. Logo $\mathcal{T}_j(c-d)(v) = \mathcal{T}_j(c)(v) - \mathcal{T}_j(d)(v) = 0\cdot v - 0\cdot v = 0$, para todo $v \in V$, ou seja, $c - d \in \mathfrak{C}_i$.

Sejam $t \in \mathbb{F}H$ e $c \in \mathfrak{C}_i$. Daí $c \in \mathbb{F}H$ e $\mathcal{T}_j(c) = 0$, para todo j, $0 \leq j \leq h-1$, $j \neq i$. Assim,

$$\mathcal{T}_j(tc) = \mathcal{T}_j\Big(\Big(\sum_{g\in H} t_g g\Big)\Big(\sum_{h\in H} s_h h\Big)\Big) = \mathcal{T}_j\Big(\sum t_g s_h gh\Big) = \sum t_g s_h \mathcal{T}_j(gh) =$$

$$\sum t_g s_h \mathcal{T}_j(g)\mathcal{T}_j(h) = \Big(\sum t_g \mathcal{T}_j(g)\Big)\Big(\sum s_h \mathcal{T}_j(h)\Big) = \Big(\sum t_g \mathcal{T}_j(g)\Big)\cdot 0 = 0.$$

Logo $tc \in \mathfrak{C}_i$.

Analogamente, $\mathcal{T}_j(ct) = 0$. Logo $\mathfrak{C}_i$ é ideal bilateral em $\mathbb{F}H$.

Provemos que $\mathfrak{C}_i$ é minimal. De fato, seja M um ideal contido em $\mathfrak{C}_i$ e sejam os V_j os espaços representação das representações irredutíveis $\mathcal{T}_j$. Se $x \in M \subset \mathfrak{C}_i$, então $\mathcal{T}_0(x)(v) = 0$, para todo $v \in V_0$, $\mathcal{T}_1(x)(v) = 0$, para todo $v \in V_1, ...,$ $\mathcal{T}_{i-1}(x)(v) = 0$, para todo $v \in V_{i-1}$, $\mathcal{T}_i(x)(v) = 0$, para todo $v \in V_i$, $\mathcal{T}_{i+1}(x)(v) = 0$, para todo $v \in V_{i+1}, ...,$ $\mathcal{T}_{h-1}(x)(v) = 0$, para todo $v \in V_{h-1}$. Lembre que $\mathcal{T} = \oplus_{j=0}^{h-1}\mathcal{T}_j$ é a representação irredutível regular à esquerda de H. Assim, se $\mathcal{T}_i(x)(v) = 0$, para todo $v \in V_i$ e para todo $0 \leq i \leq h-1$, então $\mathcal{T}(x) = 0$, o que implica $x = 0$. Logo $M = 0$. Se existir $0 \neq y \in M$ tal que $\mathcal{T}_i(y)(v) \neq 0$, para algum $v \in V_i$, então $0 \neq \mathcal{T}_i(M)$ é um $\mathbb{F}H$-submódulo de $\mathcal{T}_i(\mathfrak{C}_i) = \mathcal{T}_i(\mathbb{F}H)$, que é um submódulo simples, pois $\mathbb{F}H$ é semissimples. Assim, $\mathcal{T}_i(\mathfrak{C}_i)$ é semissimples e isto implica que $\mathcal{T}_i(\mathfrak{C}_i) = \mathcal{T}_i(M)$. Se existir $h \in \mathfrak{C}_i \setminus M$, então $\mathcal{T}_i(h) = \mathcal{T}_i(x)$, para algum $x \in M$. Logo $\mathcal{T}_i(h-x) = 0$. Daí $h - x = 0$, o que implica $h = x$ e isto é um absurdo. Portanto, $M = \mathfrak{C}_i$.

■

Dizemos que o código minimal $\mathfrak{C}_i$ definido por (3.1) **corresponde** a representação irredutível $\mathcal{T}_i$ de H. Esta correspondência pode ser estendida a todos os códigos do seguinte modo. Cada código central em $\mathbb{F}H$ é uma soma direta única de códigos centrais minimais em $\mathbb{F}H$, isto é, para qualquer código central $\mathfrak{C}$ existe um conjunto $P \subseteq \{0, 1, ..., h-1\}$ tal que $\mathfrak{C} = \oplus_{i \in P}\mathfrak{C}_i$, onde $\mathfrak{C}_i$ é minimal, pois $\mathbb{F}H$ é semissimples. Então $\mathfrak{C}$ corresponde a $\mathcal{T} = \oplus_{i \in P}\mathcal{T}_i$.

Pela Proposição 1.6.2 e pelo Teorema 1.3.7, toda representação de H sobre $\mathbb{F}$ é equivalente a uma soma de representações irredutíveis sobre $\mathbb{F}$ e, portanto, segue o lema:

Lema 3.4.2 *Existe uma correspondência biunívoca entre o conjunto dos códigos centrais não isomorfos em $\mathbb{F}H$ e o conjunto das representações não equivalentes de H sobre $\mathbb{F}$.*

Para relacionar a dimensão de um código com o grau de sua representação correspondente, primeiro examinamos códigos em LH, onde L é um corpo de decomposição de H contendo $\mathbb{F}$.

Pela Definição 1.6.15, segue que as representações irredutíveis de H sobre L são absolutamente irredutíveis. Pelo Teorema 1.4.27, sabemos que um código central minimal em LH é isomorfo a uma álgebra de matrizes $n \times n$ sobre um anel de divisão D contendo L.

Por outro lado, a Definição 1.6.17, que é equivalente à Definição 1.6.15, diz que $LH \simeq \oplus M_{n_i}(L)$. Juntando estas informações temos o seguinte resultado:

Lema 3.4.3 *Seja L um corpo de decomposição de H e seja $\mathcal{T}$ uma representação irredutível de H sobre L. Se o código central minimal $\mathcal{C} \subset LH$ corresponde a $\mathcal{T}$, então* $\dim \mathcal{C} = (\partial\mathcal{T})^2$.

Prova: Pelo que observamos acima, no caso em que L é corpo de decomposição de H, temos que o anel de divisão D é igual a L.

Assim, cada código central minimal $\mathcal{C}$ em LH é isomorfo a uma álgebra de matrizes $n \times n$ sobre L, onde n é o grau da representação correspondente ao código. Segue que $\dim \mathcal{C} = (\partial\mathcal{T})^2$, onde $\mathcal{T}$ é a representação irredutível de H sobre L correspondente ao código $\mathcal{C}$.

■

Agora, pela Observação 1.6.16, $\mathbb{F}$ sempre pode ser considerado como um subcorpo de algum corpo de decomposição L para H.

Pelo Lema 3.4.2 e pelo Corolário 9.23, encontrado em [12], um código central minimal $\mathfrak{C}$ em $\mathbb{F}H$ corresponde a uma representação irredutível sobre $\mathbb{F}$ que é a soma de representações absolutamente irredutíveis as quais podem ser expressas sobre L. O código $\mathfrak{C}$ é então o subcódigo subcorpo sobre $\mathbb{F}$ de algum código central $\mathcal{C}$ em LH. Denotamos então $\mathfrak{C} = \mathcal{C}|\mathbb{F}$.

Podemos determinar a dimensão de um código central qualquer em $\mathbb{F}H$, utilizando o teorema a seguir.

Teorema 3.4.4 *Sejam L um corpo de decomposição de H e um subcorpo $\mathbb{F} \subseteq L$. Seja $\{\mathcal{T}_0, \mathcal{T}_1, ..., \mathcal{T}_{h-1}\}$ um conjunto completo de representações irredutíveis não equivalentes de H sobre L. Seja $\mathcal{T}$ a representação irredutível de H sobre $\mathbb{F}$, onde $\mathcal{T} = \oplus_{i\in P}\mathcal{T}_i$, para algum $P \subseteq \{0, 1, ..., h-1\}$. Se o código central minimal $\mathfrak{C}$ em $\mathbb{F}H$ corresponde a $\mathcal{T}$, então* $\dim \mathfrak{C} = \sum_{i\in P}(\partial\mathcal{T}_i)^2$.

Prova: Seja $\{\mathcal{T}_0, \mathcal{T}_1, ..., \mathcal{T}_{h-1}\}$ um conjunto completo de representações irredutíveis de H sobre L com códigos centrais minimais $\mathcal{C}_0, \mathcal{C}_1, ..., \mathcal{C}_{h-1}$ em LH.

Pelo Lema 3.4.3, o código $\mathcal{C} = \oplus_{i\in P}\mathcal{C}_i \subset LH$ corresponde à representação $\mathcal{T} = \oplus_{i\in P}\mathcal{T}_i$ e $\dim(\mathcal{C}) = \sum_{i\in P}(\partial\mathcal{T}_i)^2$.

Assim, $\dim(\mathfrak{C}) \leq \dim(\mathcal{C})$.

Suponha $\dim(\mathfrak{C}) < \dim(\mathcal{C})$. Então a base de $\mathfrak{C}$ sobre $\mathbb{F}$ (que também pode ser vista sobre L), gera um código central $\mathcal{C}' \subset \mathcal{C} \subset LH$. E o código $\mathcal{C}'$ contém um ou mais elementos não nulos de $\mathbb{F}H$. Então $\mathcal{C}'$ contém um subcódigo subcorpo $\mathfrak{C}'$ sobre

$\mathbb{F}$, onde $\mathfrak{C}'$ é um código central e $\mathfrak{C}' \subset \mathfrak{C}$. Isto contradiz a minimalidade de $\mathfrak{C}$ em $\mathbb{F}H$.

■

Pelo Teorema 1.3.8 e pelo Teorema 3.25, encontrado em [19], se $\mathbb{F}H$ é semissimples, então cada código central $\mathfrak{C}$ é gerado por um único elemento idempotente de $\mathbb{F}H$. Este elemento idempotente pode ser determinado a partir da representação correspondente de $\mathfrak{C}$, como no lema a seguir.

Lema 3.4.5 *Se $\mathfrak{C}$ é um código central em $\mathbb{F}H$ com representação irredutível correspondente $\mathcal{T}$ sobre $\mathbb{F}$, então $\mathfrak{C}$ tem um único gerador dado por* $e = \dfrac{1}{|H|}\sum_{g\in H} tr(1)tr(\mathcal{T}(g^{-1}))g$.

Prova: Sejam $\{\mathcal{T}_0, \mathcal{T}_1, ..., \mathcal{T}_{h-1}, \}$ um conjunto completo de representações irredutíveis não equivalentes de H sobre L, onde L é um corpo de decomposição de H, $\mathbb{F} \subseteq L$ e $\mathcal{T}$ uma representação irredutível de H sobre $\mathbb{F}$ correspondente ao código $\mathfrak{C}$. Daí $\mathcal{T} = \oplus_{i\in P}\mathcal{T}_i$ para algum $P \subseteq \{0, 1, ..., h-1\}$.

Seja $\{e_1, e_2, ..., e_r\}$ o conjunto completo de idempotentes centrais primitivos de $\mathbb{F}H$. Cada componente e_i pode ser escrito como $e_i = \sum_{g\in H} a_i(g)g$ para todo $1 \leq i \leq r$.

Sejam $\chi_i(g) = tr(\mathcal{T}_i(g))$ para todo $g \in H$ e o caracter regular ρ dado por $\rho = \sum \chi_i(1)\chi_i$. Assim, $\rho(1) = |H|$ e se $g \neq 1$, então $\rho(g) = 0$.

Aplicando o caracter regular ρ em e_i temos

$$\rho(e_i) = \sum_{g\in H} a(g)\rho(g) = a_i(1)|H|. \tag{3.2}$$

Assim, para um elemento $x \in H$ temos

$$\rho(x^{-1}e_i) = \sum a_i(xg)\rho(g) = a_i(x)|H|.$$

Por (3.2), temos

$$a_i(x)|H| = \rho(x^{-1}e_i) = \sum_{j=1}^{r} \chi_j(1)\chi_j(x^{-1}e_i).$$

Como $\chi_i(e_i) = \partial\mathcal{T}_i$ e $\chi_i(e_j) = 0$ se $i \neq j$, temos $\mathcal{T}_j(x^{-1}e_i) = \mathcal{T}_j(x^{-1})\mathcal{T}_j(e_i) = 0$ e $\mathcal{T}_i(x^{-1}e_i) = \mathcal{T}_i(x^{-1})\mathcal{T}_i(e_i) = \mathcal{T}_i(x^{-1})$. Assim, $\chi_j(x^{-1}e_i) = 0$ e $\chi_i(x^{-1}e_i) = \chi_i(x^{-1})$.

Consequentemente, $a_i(x) = \frac{1}{|H|}\chi_i(1)\xi_i(x^{-1})$ para todo $x \in H$.

Substituindo em $e_i = \sum_{g\in H} a(g)g$, temos $e_i = \frac{1}{|H|}\sum_{g\in H}\chi_i(1)\chi_i(g^{-1})g$. ■

Finalizamos a seção com um corolário do resultado anterior aplicado a grupos metacíclicos.

Corolário 3.4.6 *Se G é um grupo metacíclico de ordem ímpar e apresentado como em (2.3), então o código central $\mathfrak{C}$ com representação irredutível $\mathcal{T}$ tem um único gerador dado por $e = \sum_{g\in G} tr(\mathcal{T}(g^{-1}))g$.*

Prova: Sabemos que $\chi_i(g) = tr(\mathcal{T}_i(g))$ para todo $g \in G$, onde $\mathcal{T}_i$ é uma representação irredutível e que as representações irredutíveis de G são ou de grau 1 ou de grau N, pelo Teorema 2.2.3. Assim, $\chi_i(1)$ é uma matriz identidade ou de ordem 1 ou de ordem N. Como $|G|$ é ímpar, N é a ordem de um dos geradores de G e estamos sobre o corpo $\mathbb{F}$ de característica 2, $\chi_i(1) = 1$ e $|G| = 1$.

Portanto, pelo Lema 3.4.5, temos $e_i = \sum_{g\in G}\chi_i(g^{-1})g$, para todo $g \in G$.

■

3.4.2 A Estrutura dos Códigos Metacíclicos Centrais

Nesta subseção G é um grupo metacíclico finito não abeliano de ordem ímpar como apresentado em (2.3), $\mathbb{F}$ é um corpo tal que $car(\mathbb{F}) \nmid |G|$ e L é um corpo de decomposição de G tal que $\mathbb{F} \subset L \subset \overline{\mathbb{F}}$.

Notemos que como uma representação irredutível $\mathcal{T}$ de G sobre L é absolutamente irredutível, então $\mathcal{T}$ é irredutível sobre $\overline{\mathbb{F}}$ e assim, usando o Corolário 2.2.4, $\mathcal{T}$ tem grau 1 ou N. Esta informação será efetivamente usada daqui para frente.

Utilizamos a seguinte notação para descrever os elementos da álgebra $\mathbb{F}G(M, N, R)$: Cada elemento $c \in \mathbb{F}G$ é escrito de modo único em termos de a e b como $c = c(a, b) = \sum_{j=0}^{N-1}\sum_{i=0}^{M-1} f_{ij}a^i b^j$, onde $f_{ij} \in \mathbb{F}$. Para descrever c como uma MN-upla de elementos de $\mathbb{F}$, ordenamos os elementos de G (a base de $\mathbb{F}G$) lexicograficamente da seguinte maneira:

$$a^i b^j < a^k b^l \text{ quando } j < l \text{ ou quando } j = l \text{ e } i < k$$

e escrevemos $c = (f_{00}, f_{10}, f_{20}, ..., f_{(M-1)0}, f_{01}, f_{11}, f_{21}, ..., f_{(M-1)1}, ..., f_{0(N-1)}, f_{1(N-1)}, ..., f_{(M-1)(N-1)})$. Fazendo $c_i = (f_{0i}, f_{1i}, ..., f_{(M-1)i})$, a notação $c_0|c_1|...|c_{N-1}$ também será usada para denotar c como uma sequência de N blocos, cada bloco uma M-upla sobre $\mathbb{F}$.

Exemplo 3.4.7 *Seja $c = 3a^5 + 2b - a^4b - 15a^3b^2$ um elemento em $\mathbb{F}G(9, 3, 4)$. A representação por 9-upla de c é dada por:*

$$000003000|2000(-1)0000|000(-15)00000.$$

Se enumerarmos as representações irredutíveis de G sobre L e as representações irredutíveis sobre $\mathbb{F}$ um corpo tal que $car(\mathbb{F}) \nmid |G|$, como no Capítulo 2, podemos usar os lemas anteriores para determinar a decomposição única a menos de isomorfismo de $\mathbb{F}G$ em códigos centrais minimais.

Veremos que as representações de G estão relacionadas com as representações do grupo abeliano $\mathbb{Z}_M \times \mathbb{Z}_N$. Assim, existe uma relação entre os códigos centrais em $\mathbb{F}G$ e certos códigos abelianos em $\mathbb{F}(\mathbb{Z}_M \times \mathbb{Z}_N)$ e esta relação é uma relação de equivalência.

Definição 3.4.8 *Sejam H e $\widetilde{H}$ grupos finitos de mesma ordem e seja $\mathbb{F}$ um corpo. Sejam $\mathbb{F}H$ e $\mathbb{F}\widetilde{H}$ as álgebras de grupo correspondentes aos grupos H e $\widetilde{H}$, respectivamente. Uma* ***equivalência combinatorial*** *é um $\mathbb{F}$-isomorfismo de espaço vetorial, $\gamma : \mathbb{F}H \to \mathbb{F}\widetilde{H}$, induzido por uma bijeção $\gamma : H \to \widetilde{H}$. Os códigos $\mathfrak{C} \subseteq \mathbb{F}H$ e $\widetilde{\mathfrak{C}} \subseteq \mathbb{F}\widetilde{H}$ são ditos* ***combinatorialmente equivalentes*** *se existe uma equivalência combinatorial $\gamma : \mathbb{F}H \to \mathbb{F}\widetilde{H}$ tal que $\gamma(\mathfrak{C}) = \widetilde{\mathfrak{C}}$.*

Em outras palavras, se $\mathfrak{C}$ e $\widetilde{\mathfrak{C}}$ são combinatorialmente equivalentes, qualquer palavra de um dos códigos é simplesmente uma permutação fixa dos elementos do corpo que constituem uma palavra do outro código. Assim, códigos combinatorialmente equivalentes devem ter as mesmas distribuições de peso.

Exemplo 3.4.9 *Sejam $G = \{g_1, g_2, ..., g_s\}$ e $\widetilde{G} = \{h_1, h_2, ..., h_s\}$ dois grupos e considere a bijeção*

$$\begin{array}{rccc} \gamma & : & G & \longrightarrow & \widetilde{G} \\ & & g_i & \longmapsto & h_{\sigma(i)}, \end{array}$$

onde $\sigma \in S_s$, o grupo de permutações com s elementos, é tal que $\sigma(i) = i + 1$ para todo $i \in \{1, 2, ..., s-1\}$ e $\sigma(s) = 1$.

Logo a equivalência combinatorial é dada por

$$\begin{array}{rccc} \gamma & : & \mathbb{F}G & \longrightarrow & \mathbb{F}\widetilde{G} \\ & & \alpha_1 g_1 + \alpha_2 g_2 + ... + \alpha_s g_s & \longmapsto & \alpha_1 h_2 + \alpha_2 h_3 + ... + \alpha_s h_1. \end{array}$$

Se escrevemos os elementos das álgebras de grupo na forma de s-uplas, γ induz a bijeção de $\mathbb{F}^s$, $\overline{\gamma}:\mathbb{F}^s \longrightarrow \mathbb{F}^s$, dada por $\overline{\gamma}(\alpha_1,\alpha_2,...,\alpha_s)=(\alpha_s,\alpha_1,\alpha_2,...,\alpha_{s-2},\alpha_{s-1})$.

Seja G o grupo metacíclico com geradores a e b conforme em (2.3) e seja $\widetilde{G}=\mathbb{Z}_M\times\mathbb{Z}_N$, com geradores $\widetilde{a}$ e $\widetilde{b}$. Defina a bijeção $\gamma: G\to\widetilde{G}$ dada por $\gamma(a^ib^j)=\widetilde{a}^i\widetilde{b}^j$. Como G é base de $\mathbb{F}G$ e $\widetilde{G}$ é base de $\mathbb{F}\widetilde{G}$, γ é um $\mathbb{F}$-isomorfismo de espaços vetoriais. Logo γ é uma equivalência combinatorial.

Lema 3.4.10 *Se $c\in Z(\mathbb{F}G)$, então para todo $p\in\mathbb{F}G$, $\gamma(pc)=\gamma(p)\gamma(c)$.*

Prova: Seja $c=\displaystyle\sum_{j=0}^{N-1}\Big(\sum_{i=0}^{M-1}f_{ij}a^i\Big)b^j$.

Para todo $k\,,\,0\le k<M$ e para todo $l\,,\,0\le l<N$, é suficiente mostrarmos que $\gamma(a^kb^lc)=\gamma(a^kb^l)\gamma(c)$, pois dado $p\in\mathbb{F}G\,,\,p=d_1g_1+d_2g_2+...+d_kg_k$ temos $\gamma(pc)=\gamma((d_1g_1+d_2g_2+...+d_kg_k)c)=\gamma(d_1g_1c+d_2g_2c+...+d_kg_kc)=d_1\gamma(g_1c_1)+d_2\gamma(g_2c_2)+...+d_k\gamma(g_kc_k)$, onde cada $d_i\in\mathbb{F}$ e cada $g_i\in G$. Daí $\gamma(a^kb^lc)=\gamma(a^kcb^l)$, já que c pertence ao centro de $\mathbb{F}G$.

$$\begin{aligned}
\text{Assim, } \gamma(a^kcb^l) &= \gamma\Big(a^k\Big(\sum_{j=0}^{N-1}\Big(\sum_{i=0}^{M-1}f_{ij}a^i\Big)b^j\Big)b^l\Big)\\
&= \gamma\Big(\sum_{j=0}^{N-1}\Big(\sum_{i=0}^{M-1}f_{ij}a^{k+i}\Big)b^{j+l}\Big)\\
&= \sum_{j=0}^{N-1}\Big(\sum_{i=0}^{M-1}f_{ij}\widetilde{a}^{k+i}\Big)\widetilde{b}^{j+l}\\
&= \widetilde{a}^k\widetilde{b}^l\Big(\sum_{j=0}^{N-1}\Big(\sum_{i=0}^{M-1}f_{ij}\widetilde{a}^i\Big)\widetilde{b}^j\Big)\\
&= \gamma(a^kb^l)\gamma(c).
\end{aligned}$$

Logo para qualquer $p\in\mathbb{F}G$, pela linearidade de γ, $\gamma(pc)=\gamma(p)\gamma(c)$.

■

Teorema 3.4.11 *Seja $\gamma:\mathbb{F}G\to\mathbb{F}(\mathbb{Z}_M\times\mathbb{Z}_N)$ a equivalência combinatorial definida por $\gamma(a^ib^j)=\widetilde{a}^i\widetilde{b}^j$ como anteriormente. Se $\mathfrak{C}$ é um código central em $\mathbb{F}G$, então $\gamma(\mathfrak{C})$ é um ideal na álgebra comutativa $\mathbb{F}(\mathbb{Z}_M\times\mathbb{Z}_N)$. Além disso, se e denota o único gerador idempotente de $\mathfrak{C}$, então $\gamma(e)$ é o gerador idempotente de $\gamma(\mathfrak{C})$.*

Prova: O conjunto $\gamma(\mathfrak{C})=\{\gamma(c):\,c\in\mathfrak{C}\}$ é não vazio, pois $\gamma(0^i0^j)=\widetilde{0}^i\widetilde{0}^j=0$, já que $\mathfrak{C}$ é ideal e assim $0^i0^j=0\in\mathfrak{C}$. Sejam $\alpha\,\text{e}\,\beta\in\gamma(\mathfrak{C})$. Então $\alpha=\gamma(c_1)\,,\,\beta=\gamma(c_2)$,

para algum $c_1 \in \mathfrak{C}$ e algum $c_2 \in \mathfrak{C}$. Assim, $\alpha - \beta = \gamma(c_1) - \gamma(c_2) = \gamma(c_1 - c_2) \in \mathfrak{C}$, já que $c_1 - c_2 \in \mathfrak{C}$, pois $\mathfrak{C}$ é ideal.

Sejam $d \in \mathbb{F}(\mathbb{Z}_M \times \mathbb{Z}_N)$ e $\gamma(c_1) \in \gamma(\mathfrak{C})$. Daí $d\gamma(c_1) = \gamma(\overline{d})\gamma(c_1)$, pois γ é uma bijeção e pelo fato que $c_1 \in \mathfrak{C}$ e $\mathfrak{C}$ é um código central em $\mathbb{F}G$. Pelo Lema 3.4.10, $\gamma(\overline{d})\gamma(c_1) = \gamma(\overline{d}c_1) \in \gamma(\mathfrak{C})$, já que $\overline{d}c_1 \in \mathfrak{C}$, pois $\mathfrak{C}$ é ideal. Logo $\gamma(\mathfrak{C})$ é ideal em $\mathbb{F}(\mathbb{Z}_M \times \mathbb{Z}_N)$.

Mostraremos agora que se e denota o único gerador idempotente de $\mathfrak{C}$, então $\gamma(e)$ é o gerador idempotente de $\gamma(\mathfrak{C})$. De fato, por hipótese, $\mathfrak{C} = \{pe : p \in \mathbb{F}G\} = \langle e \rangle$. Assim, $\gamma(\mathfrak{C}) = \{\gamma(pe) : p \in \mathbb{F}G\}$, pelo Lema 3.4.10, temos $\{\gamma(p)\gamma(e) : p \in \mathbb{F}G\} = \{\widetilde{p}\gamma(e) : \widetilde{p} \in \mathbb{F}(\mathbb{Z}_M \times \mathbb{F}\mathbb{Z}_N)\} = \langle \gamma(e) \rangle$, um código abeliano.

Além disso, $\gamma(e)$ é idempotente. De fato, $\gamma(e) = \gamma(ee)$, pois e é idempotente e como pertence ao centro de $\mathbb{F}G$, pelo Lema 3.4.10, segue que $\gamma(ee) = \gamma(e)\gamma(e) = [\gamma(e)]^2$.

■

O Teorema 3.4.11 nos diz que todos os códigos metacíclicos centrais são combinatorialmente equivalentes a códigos abelianos.

Exemplo 3.4.12 *Consideremos o grupo metacíclico* $G(9,3,4)$ *e sejam* $p(a) = \sum_{i=0}^{M-1} a^i$ *e* $q(b) = \sum_{j=0}^{N-1} b^j$. *Sejam* ω *uma raiz cúbica primitiva da unidade e* δ *uma raiz nona primitiva da unidade.*

i) Seja $L = \mathbb{F}_{2^6}$. *Daí* $LG = \oplus_{i=0}^{10} \mathcal{C}_i$, *onde cada* $\mathcal{C}_i$ *é gerado por um único idempotente* e_i.

Para $0 \leq i \leq 8$, *temos* $e_i = p(\omega^{i(mod3)}a)q(\omega^j b)$, *onde* $j = \left[\frac{i}{3}\right]$, $e_9 = p(\delta a) + p(\delta^4 a) + p(\delta^7 a)$ *e* $e_{10} = p(\delta^8 a) + p(\delta^5 a) + p(\delta^2 a)$.

Neste exemplo, $\mathcal{C}_8$ *é gerado por*

$$e_8 = \left(\sum_{i=0}^{8} (\omega^2 a)^i\right)\left(\sum_{j=0}^{2} (\omega^2 b)^j\right),$$

ou seja,

$$e_8 = (1 + \omega^2 a + \omega a^2 + a^3 + \omega^2 a^4 + \omega a^5 + a^6 + \omega^2 a^7 + \omega a^8)(1 + \omega^2 b + \omega b^2)$$

que na notação que estabelecemos na página 69 pode ser escrito como $1\omega^2\omega 1\omega^2\omega 1\omega^2\omega|\omega^2\omega 1\omega^2\omega 1\omega^2\omega 1|\omega 1\omega^2\omega 1\omega^2\omega 1\omega^2$.

Pelo Lema 3.4.3, $\dim \mathcal{C}_i = 1$ *, para* $0 \leq i \leq 8$ *e* $\dim \mathcal{C}_i = 9$ *, para* $9 \leq i \leq 10$.

ii) Seja $\mathbb{F} = \mathbb{F}_2$. *Daí* $\mathbb{F}G = \oplus_{i=0}^{5} \mathfrak{C}_i$. *Cada* $\mathfrak{C}_i$ *é gerado por um único idempotente* x_i. *Cada um desses idempotentes é a soma de geradores idempotentes de códigos centrais minimais em* LG *como a seguir:*

$$x_0 = e_0 \, , \, x_1 = e_1 + e_2 \, , \, x_2 = e_4 + e_5 \, , \, x_3 = e_7 + e_8 \, ,$$

$$x_4 = e_3 + e_6 \, , \, x_5 = e_9 + e_{10}.$$

Neste exemplo, $\mathfrak{C}_1$ *é gerado pelo idempotente* $011011011|011011011|011011011$ *e* $\mathfrak{C}_5$ *é gerado pelo idempotente* $000100100|\boldsymbol{0}|\boldsymbol{0}$.

Pelo Teorema 3.4.4, $\dim \mathfrak{C}_0 = 1$, $\dim \mathfrak{C}_i = 2$ *, para* $1 \leq i \leq 4$ *e* $\dim \mathfrak{C}_5 = 18$.

Códigos Cíclicos Associados a Códigos Centrais Minimais

Para descrever e classificar os códigos centrais em $\mathbb{F}G$, onde $\mathbb{F}$ é um corpo tal que $car(\mathbb{F}) \nmid |G|$, primeiramente vamos associar a cada código central um código cíclico. Denotamos por $\mathbb{Z}_M$ o subgrupo normal de G gerado por a. Sob esta identificação, $\mathbb{F}\mathbb{Z}_M$ é uma subálgebra de $\mathbb{F}G$. Um ideal nesta subálgebra pode ser associado a um ideal na álgebra maior.

Definição 3.4.13 *Seja* $c \in \mathbb{F}G$, *onde* $c = c_0|c_1|...|c_{N-1}$. *Para o código* $\mathfrak{C} \subseteq \mathbb{F}G$, $\mathcal{A} = \{c_0 : c = c_0|c_1|...|c_{N-1} \in \mathfrak{C}\}$ *é o* ***código cíclico associado*** *a* $\mathfrak{C}$. *O código* $\mathcal{A}$ *é um ideal de* $\mathbb{F}\mathbb{Z}_M$.

Em outras palavras, $\mathcal{A}$ é um código cíclico consistindo de todas as primeiras M-uplas das palavras do código $\mathfrak{C}$ em $\mathbb{F}G$.

Nosso principal interesse são os códigos cíclicos associados aqueles códigos centrais metacíclicos que contêm códigos à esquerda. O próximo lema nos permite estabelecer uma partição dos códigos centrais minimais de $\mathbb{F}G$ em dois conjuntos. A demonstração deste lema depende fortemente da estrutura das representações absolutamente irredutíveis de $G(M, N, R)$ apresentada no Capítulo 2.

Lema 3.4.14 *Seja* L *um corpo de decomposição de* G *tal que* $\mathbb{F} \subset L \subset \overline{\mathbb{F}}$. *Se* $\mathfrak{C}$ *é um código central minimal em* $\mathbb{F}G$ *com representação irredutível correspondente* $\mathcal{T}$ *sobre* $\mathbb{F}$, *então* $\mathcal{T}$ *é unicamente decomposta (a menos de equivalência) em uma soma direta de representações absolutamente irredutíveis sobre* L, *as quais são todas de*

mesmo grau. Na decomposição, todas as representações constituintes são ou de grau 1 *ou de grau* N.

Prova: Pela demonstração do Teorema 2.2.3, as representações absolutamente irredutíveis de G sobre L são ou de grau 1 ou de grau N. Seja $G^{'}$ o subgrupo comutador de G. Pelo Lema 2.1.2, $G^{'} \subseteq \mathbb{Z}_M$ e $\dfrac{G}{G^{'}} \simeq \mathbb{Z}_K \times \mathbb{Z}_N$. As representações absolutamente irredutíveis de G de grau um são as representações absolutamente irredutíveis de $\mathbb{Z}_K \times \mathbb{Z}_N$. Estas KN representações são unicamente particionadas em somas diretas para formar representações de $\mathbb{Z}_K \times \mathbb{Z}_N$ (e assim de G) que são irredutíveis sobre $\mathbb{F}$.

Pelo Lema 9.18, encontrado em [12], toda representação irredutível de G sobre L deve ser incluída como somando direto em exatamente uma representação irredutível de G sobre $\mathbb{F}$, podemos concluir que representações absolutamente irredutíveis de grau N são igualmente somadas para formar representações irredutíveis sobre $\mathbb{F}$.

■

Definição 3.4.15 *Seja* $\mathfrak{C}$ *um código central minimal em* $\mathbb{F}G$ *com representação correspondente* $\mathcal{T}$. *O código* $\mathfrak{C}$ *é dito de* ***grau*** 1 ***(grau*** N***)*** *se as representações absolutamente irredutíveis constituintes de* $\mathcal{T}$ *são de grau* 1 *(resp. de grau* N*).*

Em LG, os códigos centrais minimais de grau N correspondem a representações absolutamente irredutíveis de G e, pelo Lema 3.4.3, têm dimensão N^2. Se $\mathbb{F}$ é um subcorpo de L, segue do Teorema 3.4.4 que um código central de grau N tem uma dimensão que é um múltiplo de N^2. Podemos descrever completamente um tal código em termos de seus códigos cíclicos associados, a partir do lema a seguir.

Lema 3.4.16 *Se* $\mathfrak{C}$ *é um código central minimal em* $\mathbb{F}G$ *de grau* N *com código cíclico associado* $\mathcal{A}$, *então o gerador idempotente de* $\mathfrak{C}$ *é* $e|\boldsymbol{0}|\boldsymbol{0}|...|\boldsymbol{0}$, *onde* e *é o gerador idempotente de* $\mathcal{A}$.

Prova: Seja $\{\mathcal{T}_0, \mathcal{T}_1, ..., \mathcal{T}_{h-1}\}$ um conjunto de representações absolutamente irredutíveis de G não equivalentes. Seja $\mathcal{T}$ a representação (irredutível sobre $\mathbb{F}$) correspondente a $\mathfrak{C}$, onde $\mathcal{T} = \oplus_{i \in P} \mathcal{T}_i$ e $P \subseteq \{0, 1, ..., h-1\}$. Pelo Lema 3.4.14, para todo $i \in P$, $\mathcal{T}_i$ é de grau N.

Para todo $g \in G$, onde $g = a^i b^j$ e $0 < j < N$, $tr\mathcal{T}_i(g) = 0$, para todo $i \in P$, pois as representações matriciais $\mathcal{T}_i(a)$ são diagonais e as representações matriciais $\mathcal{T}_i(b)$ possuem diagonal principal nula, como vimos na página 43 e portanto, o produto destas representações é uma matriz com diagonal nula. Assim, $tr\mathcal{T}(g) = 0$, para todo $g \notin \mathbb{Z}_M$. Então, pelo Corolário 3.4.6, $\mathfrak{C}$ tem um gerador idempotente $e^{,}$, onde $e^{,} = e|\mathbf{0}|\mathbf{0}|...\mathbf{0}$.

Se $c = c_0|c_1|...|c_{N-1} \in \mathfrak{C}$, então $ce' = c_0e|c_1e|...|c_{N-1}e = c$, pelo Teorema 1.3.8. Assim, $c_0e = c_0$, para todo c_0, ou seja, para todos os elementos de $\mathcal{A}$. Pelo Corolário 3.4.6, tal elemento é único.

■

O próximo teorema, que segue do Lema 3.4.16 e do Teorema 3.4.11, descreve todo código central minimal de grau N como um código produto direto. A equivalência combinatorial γ é como definida previamente.

Teorema 3.4.17 *Seja $\mathfrak{C}$ um código central minimal em $\mathbb{F}G$ de grau N com código cíclico associado $\mathcal{A}$. Então $\mathfrak{C}$ é combinatorialmente equivalente a $\mathcal{A} \otimes \mathbb{F}\mathbb{Z}_N$.*

Prova: Seja $\mathfrak{C}$ um código central minimal de $\mathbb{F}G$ de grau N. Pelo Lema 3.4.16, o gerador idempotente de $\mathfrak{C}$ é uma combinação linear de potências de a, pois $\mathfrak{C} = \langle e|\mathbf{0}|\mathbf{0}|...|\mathbf{0}\rangle$, onde $\mathcal{A} = \langle e\rangle$, sendo e idempotente em $\mathbb{F}\langle a\rangle$. Note que $e = \sum_{i=0}^{M-1} d_i a^i$, com $d_i \in \mathbb{F}$.

Pelo Teorema 3.4.11, como $\mathfrak{C} = \langle e|\mathbf{0}|\mathbf{0}|...|\mathbf{0}\rangle$ é um ideal central minimal, então $\gamma(\langle e|\mathbf{0}|\mathbf{0}|...|\mathbf{0}\rangle)$ é um ideal central em $\mathbb{F}\mathbb{Z}_M \otimes \mathbb{F}\mathbb{Z}_N$, pois pela Proposição 1.4.6, $\psi : \mathbb{F}(\mathbb{Z}_M \times \mathbb{Z}_N) \longrightarrow \mathbb{F}\mathbb{Z}_M \otimes \mathbb{F}\mathbb{Z}_N$ é um isomorfismo de álgebra de grupo. Além disso, temos

$$\begin{array}{rccc} \gamma & : & \mathbb{F}G & \longrightarrow & \mathbb{F}\mathbb{Z}_M \otimes \mathbb{F}\mathbb{Z}_N \\ & & \sum_{j=0}^{N-1}\sum_{i=0}^{M-1} d_{ij}a^ib^j & \longmapsto & \sum_{j=0}^{N-1}\sum_{i=0}^{M-1} d_{ij}\widetilde{a}^i \otimes \widetilde{b}^j, \end{array}$$

um isomorfismo de espaços vetoriais. Assim, $\mathfrak{C} = \{p(e|\mathbf{0}|\mathbf{0}|...|\mathbf{0}) : p \in \mathbb{F}G\}$ e

$$\gamma(\mathfrak{C}) = \{\gamma(p(e|\mathbf{0}|\mathbf{0}|...|\mathbf{0})) : p \in \mathbb{F}G\} = \{\gamma(p\cdot e|p\cdot\mathbf{0}|p\cdot\mathbf{0}|...|p\cdot\mathbf{0}) : p \in \mathbb{F}G\}$$
$$= \{\gamma(p\cdot e|\mathbf{0}|\mathbf{0}|...|\mathbf{0}) : p \in \mathbb{F}G\} = \{\gamma(p)\gamma(e) : p \in \mathbb{F}G\}$$
$$= \{\widetilde{p}\gamma(e) : \widetilde{p} \in \mathbb{F}(\mathbb{Z}_M \times \mathbb{Z}_N)\} = \left\{\widetilde{p}\sum d_i\widetilde{a}^i\widetilde{b}^0 : \widetilde{p} \in \mathbb{F}(\mathbb{Z}_M \times \mathbb{Z}_N)\right\}$$
$$= \left\{\psi(\widetilde{p})\sum d_i\widetilde{a}^i\otimes\widetilde{b}^0 : \psi(\widetilde{p}) \in \mathbb{F}(\mathbb{Z}_M\otimes\mathbb{F}\mathbb{Z}_N)\right\} = \left\{q\sum d_i\widetilde{a}^i\otimes\widetilde{b}^0 : q \in \mathbb{F}(\mathbb{Z}_M\otimes\mathbb{F}\mathbb{Z}_N)\right\}$$
$$= \left\{\left(\sum_{i,j} d_{ij}\widetilde{a}^i\widetilde{b}^j\right)\left(\sum_i d_i\widetilde{a}^i\widetilde{b}^0\right) : d_{ij} \in \mathbb{F}\right\} = \left\{\sum d_i\widetilde{a}^i \otimes \sum d_j\widetilde{b}^j\widetilde{b}^0 : d_{ij} \in \mathbb{F}\right\}$$
$$= \left\{\sum d_i\widetilde{a}^i \otimes \sum d_{ij}\widetilde{b}^j : d_{ij} \in \mathbb{F}\right\} = \mathcal{A} \otimes \mathbb{F}\mathbb{Z}_N.$$

■

Corolário 3.4.18 *Seja $\mathfrak{C}$ um código central minimal em $\mathbb{F}G$ de grau N com código cíclico associado $\mathcal{A}$. Se $\mathfrak{C}$ tem dimensão kN^2 então $\mathcal{A}$ tem dimensão kN.*

Prova: Pelo Teorema 3.4.17, $\mathfrak{C}$ é combinatorialmente equivalente a $\mathcal{A} \otimes \mathbb{F}\mathbb{Z}_N$. Logo $\dim(\mathfrak{C}) = \dim(\mathcal{A} \otimes \mathbb{F}\mathbb{Z}_N) = \dim(\mathcal{A}) \cdot \dim(\mathbb{F}\mathbb{Z}_N)$. Por hipótese, $\dim(\mathfrak{C}) = kN^2$ e como $\dim(\mathbb{F}\mathbb{Z}_N) = N$, temos $kN^2 = \dim(\mathcal{A}) \cdot N$, ou seja, $\dim(\mathcal{A}) = kN$.

■

Exemplo 3.4.19 *Seja o grupo metacíclico $G = G(9, 3, 4)$. Sejam ω uma raiz cúbica primitiva da unidade e δ uma raiz nona primitiva da unidade.*

i) Considere $L = \mathbb{F}_{2^6}$. Assim, $\mathcal{C}_9$ que é gerado por
$e_9 = 1+(\delta+\delta^4+\delta^7)a+(\delta^2+\delta^5+\delta^8)a^2+\delta^3a^3+(\delta+\delta^4+\delta^7)a^4+(\delta^2+\delta^5+\delta^8)a^5+\delta^6a^6$
$+ (\delta + \delta^4 + \delta^7)a^7 + (\delta^2 + \delta^5 + \delta^8)a^8$
é combinatorialmente equivalente a $A_9 \otimes \mathbb{F}\mathbb{Z}_3$, onde $A_9 \subset \mathbb{F}\mathbb{Z}_9$. Como δ é uma raiz nona primitiva da unidade, temos δ, δ^4, δ^7, δ^8, δ^5 e δ^2 não nulos e A_9 gerado pelo idempotente $100\omega^2 00\omega 00$, onde $\omega = \delta^6$.

Temos também $\mathcal{C}_{10}$ que é gerado por
$e_{10} = 1 + (\delta^2 + \delta^5 + \delta^8)a + (\delta + \delta^4 + \delta^7)a^2 + \delta^6a^3 + (\delta^2 + \delta^5 + \delta^8)a^4$
$+ (\delta + \delta^4 + \delta^7)a^5 + \delta^3a^6 + (\delta^2 + \delta^5 + \delta^8)a^7 + (\delta + \delta^4 + \delta^7)a^8$
é combinatorialmente equivalente a $A_{10} \otimes \mathbb{F}\mathbb{Z}_3$, onde $A_{10} \subset \mathbb{F}\mathbb{Z}_9$. Como δ é uma raiz nona primitiva da unidade, temos δ, δ^4, δ^7, δ^8, δ^5 e δ^2 não nulos e A_{10} gerado pelo idempotente $100\omega 00\omega^2 00$, onde $\omega = \delta^6$.

ii) Considere $\mathbb{F} = \mathbb{F}_2$. Assim, $\mathfrak{C}_5$ que é gerado por $x_5 = e_9 + e_{10} = 001001000|\boldsymbol{0}|\boldsymbol{0}$ é combinatorialmente equivalente a $\mathcal{A} \otimes \mathbb{F}\mathbb{Z}_3$, onde $\mathcal{A} \subset \mathbb{F}\mathbb{Z}_9$. Como δ é uma raiz nona primitiva da unidade, temos δ, δ^4, δ^7, δ^8, δ^5 e δ^2 não nulos e $\mathcal{A}$ gerado pelo idempotente 000100100 e $\mathcal{A} = (A_9 \oplus A_{10})|\mathbb{F}$.

3.4.3 Códigos à Esquerda

Estamos interessados em estudar os códigos metacíclicos unilaterais em $\mathbb{F}G$ que são não abelianos, pois os códigos metacíclicos centrais não nos fornecem nenhum resultado diferente dos já conhecidos para códigos abelianos. Escolhemos estudar os ideais à esquerda, os quais são chamados **códigos à esquerda**, apesar de todos os resultados serem aplicados igualmente aos ideais à direita.

Os dois teoremas a seguir não serão demonstrados.

Teorema 3.4.20 *Se $\mathfrak{C}$ é um código central minimal em $\mathbb{F}G$ de grau 1, então $\mathfrak{C}$ não contém subcódigos à esquerda não triviais.*

Entretanto, os códigos centrais minimais de grau N se decompõem.

Teorema 3.4.21 *Se $\mathfrak{C}$ é um código central minimal em $\mathbb{F}G$ de grau N e dimensão kN^2, então $\mathfrak{C}$ é a soma direta de N códigos minimais à esquerda, cada um de dimensão kN.*

Esta decomposição de um código minimal em $\mathbb{F}G$ de grau N e dimensão kN^2 não é única, pelo Teorema 4, p.16, e pelo Corolário 1, p.16, em [13] . Este fato torna o estudo de códigos metacíclicos mais interessante que o estudo de códigos abelianos. Para determinar as decomposições possíveis, examinamos mais de perto as representações irredutíveis, as quais correspondem aos códigos centrais minimais de grau N. Pelo Lema 3.4.14, tais representações são somas diretas de representações absolutamente irredutíveis de grau N. Começamos examinando as representações absolutamente irredutíveis e seus códigos correspondentes.

3.4.4 Códigos Minimais à Esquerda em $LG(M, N, R)$

Seja L um corpo de decomposição de G com característica 2.

Os códigos centrais minimais em LG correspondem a representações absolutamente irredutíveis ou de grau 1 ou grau N e são desta forma, ou de grau 1 (e de dimensão 1) ou de grau N (e de dimensão N^2). Pelo Teorema 3.4.21, um código central minimal de grau N e dimensão N^2 pode ser decomposto em uma soma direta de N códigos minimais à esquerda cada um de dimensão N. Os N códigos somandos em qualquer decomposição são isomorfos como espaços vetoriais e como códigos, entretanto, eles não precisam ser combinatorialmente equivalentes.

A partir de agora $\langle e \rangle_{\mathcal{L}}$ indicará o ideal à esquerda gerado pelo elemento e do anel de grupo LG.

Dadas uma representação absolutamente irredutível $\mathcal{T}$ de grau N e uma representação matricial particular $\overline{\mathcal{T}}$, relacionada a $\mathcal{T}$, queremos determinar os códigos minimais à esquerda que são somandos do código minimal central correspondente a $\mathcal{T}$.

O teorema a seguir nos permite identificar um gerador idempotente para cada um dos códigos componentes.

Teorema 3.4.22 *Seja $\mathcal{C}$ um código central minimal em LG de grau N correspondente à representação irredutível $\mathcal{T}$. Se $\overline{\mathcal{T}}$ é uma representação matricial relacionada a $\mathcal{T}$, então $\mathcal{C} = \oplus_{i=1}^{N} W_i$ e cada W_i é um código minimal à esquerda gerado pelo idempotente $e_i = \sum_{g \in G} (\tau_{ii}(g^{-1}))g$, onde $\tau_{ii}(g^{-1})$ é a entrada (i,i) na matriz $\overline{\mathcal{T}}(g^{-1})$.*

Prova: Para cada $1 \leq i \leq N$, defina um operador projeção p_i em $\mathcal{C}$ dado por:

$$p_i = \frac{N}{|G|} \sum_{g \in G} \tau_{ii}(g^{-1}) \cdot R(g),$$

onde R é uma representação regular à direita por g, isto é, $R : G \longrightarrow GL(LG)$ e $R(g)$ é a multiplicação à direita de g. Pelo Teorema 8 em [13], p.21, $p_i : \mathcal{C} \longrightarrow W_i$, onde W_i é um subespaço de $\mathcal{C}$ e $\mathcal{C} = \oplus_{i=1}^{N} W_i$. Mas p_i^{-1} é a transposta da matriz geradora (irredutível) de um ideal em LG com gerador $e_i = \frac{N}{|G|} \sum_{g \in G} (\tau_{ii}(g^{-1}))g$. Como $|G|$ é ímpar e N é a ordem de um dos geradores de G, sobre um corpo de característica 2, temos $e_i = \sum_{g \in G} (\tau_{ii}(g^{-1}))g$.

Desta forma, este código (o espaço coluna de p_i) é W_i. Assim, para todo $c \in \mathcal{C}$, $p_i(c) = c \cdot e_i$. Mas pela demonstração do Teorema 8 em [13], p.21, $p_i : W_i \longrightarrow W_i$ é a aplicação identidade. Portanto, para cada $c \in W_i$, $p_i(c) = c = c \cdot e_i$. Assim, e_i é a identidade à direita em W_i. Logo é um idempotente. ■

Como cada escolha de uma base para o espaço representação de uma representação $\mathcal{T}$, define uma representação matricial $\overline{\mathcal{T}}$ relacionada a $\mathcal{T}$, o Teorema 3.4.22 garante que, tomando uma base particular para o espaço representação, selecionamos um conjunto de N códigos minimais à esquerda cuja soma direta é um código central minimal $\mathcal{C}$. Cada código minimal à esquerda é gerado por um idempotente definido pelo Teorema 3.4.22. O interessante aqui é que estes idempotentes geradores dos códigos minimais à esquerda não são únicos, o que os difere do caso abeliano.

Definição 3.4.23 *Seja $\mathcal{C}$ o código central minimal de grau N correspondente à representação irredutível $\mathcal{T}$. Se $\overline{\mathcal{T}}$ é uma representação matricial relacionada a $\mathcal{T}$, então $\overline{\mathcal{T}}$* ***determina*** *a decomposição $\mathcal{C} = \oplus_{i=1}^{N} W_i$ e* ***define*** *um gerador idempotente e_i para cada código minimal à esquerda W_i. O conjunto $E = \{e_1, e_2, ..., e_N\}$ é o* ***conjunto definido*** *de geradores onde $W_i = \langle e_i \rangle_{\mathcal{L}}$, para todo $i, 1 \leq i \leq N$.*

Além disso, pela página 108 da referência [19], o conjunto definido $E = \{e_1, e_2, ..., e_N\}$, $e_i e_j = 0$, para todo $i \neq j$ e $\sum_{i=1}^{N} e_i = e$, onde e é o gerador idempotente de $\mathcal{C}$. O

conjunto E é o conjunto completo de idempotentes mutuamente ortogonais. Apesar desses geradores serem mutuamente ortogonais, os códigos à esquerda em geral, não se anulam com outro código à esquerda, isto é, se $c_1 \in \langle e_i \rangle_{\mathcal{L}}$ e $c_2 \in \langle e_j \rangle$, para $i \neq j$, $c_1 \cdot c_2$ não precisa ser zero. Isto é verdade porque esses códigos à esquerda têm geradores que não estão no centro de G.

Exemplo 3.4.24 *Sejam* $LG = \mathbb{F}_{2^3}G(7,3,2)$ *e o código minimal central* $\mathcal{C}_3 = \langle 1110100|\boldsymbol{0}|\boldsymbol{0}\rangle$. *Queremos encontrar duas decomposições em códigos minimais à esquerda em* LG *para* $\mathcal{C}_3$.

Este código corresponde à representação irredutível $\mathcal{T}_3$, *a qual é relacionada com a representação matricial usual* $\overline{\mathcal{T}}_3$, *onde* $\overline{\mathcal{T}}_3(a) = \begin{pmatrix} \xi & 0 & 0 \\ 0 & \xi^2 & 0 \\ 0 & 0 & \xi^4 \end{pmatrix}$, $\overline{\mathcal{T}}_3(b) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ *e* ξ *é uma raiz sétima primitiva da unidade.*

Assim, pelo Teorema 3.4.22, o código $\mathcal{C}_3$ *tem uma decomposição em códigos minimais à esquerda dada por* $\mathcal{C}_3 = \oplus_{i=1}^{3} W_i$, *onde*

$$W_1 \, tem \, 1\xi^6\xi^5\xi^4\xi^3\xi^2\xi^1|\boldsymbol{0}|\boldsymbol{0} \, como \, gerador \, idempotente,$$

$$W_2 \, tem \, 1\xi^5\xi^3\xi^1\xi^6\xi^4\xi^2|\boldsymbol{0}|\boldsymbol{0} \, como \, gerador \, idempotente \, e$$

$$W_3 \, tem \, 1\xi^3\xi^6\xi^2\xi^5\xi^1\xi^4|\boldsymbol{0}|\boldsymbol{0} \, como \, gerador \, idempotente.$$

Seja $\mathcal{T}^*$ *uma representação matricial equivalente à* $\overline{\mathcal{T}}_3$. *Assim, a representação irredutível* $\mathcal{T}_3$ *também está relacionada a* $\mathcal{T}^*$, *onde* $\mathcal{T}^*(a) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ *e* $\mathcal{T}^*(b) = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$.

Portanto, pelo Teorema 3.4.22, $\mathcal{C}_3$ *tem uma outra decomposição em códigos minimais à esquerda dada por* $\mathcal{C}_3 = \oplus_{i=1}^{3} W_i^{'}$, *onde*

$$W_1^{'} \, tem \, 1110100|1101001|0100111 \, como \, gerador \, idempotente,$$

$$W_2^{'} \, tem \, 1001110|0100111|1101001 \, como \, gerador \, idempotente \, e$$

$$W_3^{'} \, tem \, 1001110|1001110|1001110 \, como \, gerador \, idempotente.$$

3.4.5 Códigos Minimais à Esquerda em $\mathbb{F}G(M, N, R)$

Seja L um corpo de decomposição de $G = G(M, N, R)$ de característica 2, e seja $\mathbb{F}$ um subcorpo de L. Em $\mathbb{F}G$ como em LG, os Teoremas 3.4.20 e 3.4.21 nos direcionam a examinar os códigos centrais minimais de grau N na busca por códigos não abelianos. Estes códigos, com seus correspondentes em LG, podem ser decompostos em uma soma direta de N códigos minimais à esquerda, os quais são isomorfos como espaços vetoriais, mas não necessariamente combinatorialmente equivalentes. Novamente a decomposição não é única. Desejamos determinar os códigos minimais à esquerda de uma decomposição particular encontrando seus geradores idempotentes. Infelizmente, os métodos usados para se chegar no Teorema 3.4.22 não podem ser usados quando a representação envolvida não é absolutamente irredutível. Veremos que podemos identificar os geradores idempotentes dos códigos minimais à esquerda, mas para isto devemos produzir representações matriciais de uma maneira particular.

Seja $\{\mathcal{T}_0, \mathcal{T}_1, ..., \mathcal{T}_{h-1}\}$ um conjunto completo de representações absolutamente irredutíveis distintas de G . Seja $\mathfrak{C} \subset \mathbb{F}G$ um código central minimal de grau N correspondente à representação irredutível $\mathcal{T}$ sobre $\mathbb{F}$. Então $\mathcal{T} = \oplus_{i\in P}\mathcal{T}_i$, onde $P \subseteq \{0, 1, ..., h-1\}$ e, para todo $i \in P$, $\mathcal{T}_i$ é de grau N. Seja $\mathcal{C}_i$ o código central minimal em LG correspondente à $\mathcal{T}_i$. Como L é uma extensão de $\mathbb{F}$, $\mathfrak{C}$ é um subcódigo subcorpo sobre $\mathbb{F}$ da soma direta $\oplus_{i\in P}\mathcal{C}_i$, ou seja, se x é uma palavra do código $\mathfrak{C}$, então x é uma palavra do código $\oplus_{i\in P}\mathcal{C}_i$. Existe também uma relação entre os códigos cíclicos associados. Se $\mathfrak{C}$ tem um código cíclico associado $\mathcal{A}$ em $\mathbb{F}\mathbb{Z}_M$, e cada $\mathcal{C}_i$ tem um código cíclico associado A_i em $L\mathbb{Z}_M$, então $\mathcal{A}$ é um subcódigo subcorpo sobre $\mathbb{F}$ de $\oplus_{i\in P}A_i$. Denote $\mathcal{A} = \oplus_{i\in P}A_i|\mathbb{F}$.

Buscamos decompor um código central minimal $\mathfrak{C}$ de $\mathbb{F}G$ em códigos minimais à esquerda. Para fazer isto, primeiro decompomos cada $\mathcal{C}_i$ (em LG) de tal maneira que somas de códigos minimais à esquerda, um de cada $\mathcal{C}_i$, contenham um código minimal à esquerda distinto em $\mathbb{F}G$ como um subcódigo subcorpo. De outro modo, procuramos uma representação matricial $\overline{\mathcal{T}}$ relacionada a $\mathcal{T}$ a qual é uma soma direta de representações matriciais $\overline{\mathcal{T}}_i$ cujos elementos da diagonal correspondentes têm soma em $\mathbb{F}$. Então, usando o Teorema 3.4.22, podemos encontrar os idempotentes geradores dos somandos minimais à esquerda de cada $\mathcal{C}_i$. Adicionando k (o número de elementos de P) idempotentes correspondentes, um de cada $\mathcal{C}_i$, produzimos o idempotente gerador de um código minimal à esquerda em $\mathbb{F}G$.

O algoritmo a seguir, determina uma tal composição.

3.4.6 Algoritmo para determinar Códigos Minimais à Esquerda em $\mathbb{F}G(M, N, R)$

Sejam $\mathcal{T}$ a representação irredutível sobre $\mathbb{F}$ correspondente ao código central minimal $\mathfrak{C}$ de grau N em $\mathbb{F}G$ com código cíclico associado $\mathcal{A}$ em $\mathbb{F}\mathbb{Z}_M$ e $\mathcal{T} = \oplus_{i\in P}\mathcal{T}_i$, onde, para todo $i \in P$, $\mathcal{T}_i$ é absolutamente irredutível sobre L e corresponde ao código central minimal $\mathcal{C}_i$ de grau N em LG. Seja A_i em $L\mathbb{Z}_M$ o código cíclico associado a $\mathcal{C}_i$. Assim, $\mathcal{A} = \oplus_{i\in P}A_i|\mathbb{F}$.

Seja t_i o gerador idempotente de A_i.

1. Escolha N vetores linearmente independentes em $\mathcal{A} : d_1, d_2, ..., d_N$.

2. Para cada $i \in P$ e j , $1 \leq j \leq N$, projete d_j da seguinte maneira: $t_i.d_j = c_{ij}$ em $L\mathbb{Z}_M$.

   Para cada $i \in P$, $\{c_{ij} : 1 \leq j \leq N\}$ é um conjunto de vetores linearmente independentes e assim, forma uma possível base para o espaço representação de $\mathcal{T}_i$.

3. Para cada $i \in P$, troque a base do espaço representação de cada uma das representações matriciais usuais $\overline{\mathcal{T}}_i$ para a base $c_{i1}, c_{i2}, ..., c_{iN}$:

a) Expresse cada elemento c_{ij} da nova base como uma combinação linear dos componentes da base original, $\{p(\delta^{-j}a), p(\delta^{-j}a^R)b, p(\delta^{-j}a^{R^2})b^2, ..., p(\delta^{-j}a^{R^{N-1}})b^{N-1}\}$, onde $e_j = p(\delta^{-j}a)$, pelo que foi visto na Seção 3.3, é o gerador idempotente de um código cíclico particular unidimensional em $L\mathbb{Z}_M$ e δ é uma raiz M-ésima primitiva da unidade.

b) Encontre uma matriz mudança de base M na qual a i-ésima coluna contém os coeficientes de $p(\delta^{-j}a), p(\delta^{-j}a^R)b, p(\delta^{-j}a^{R^2})b^2, ..., p(\delta^{-j}a^{R^{N-1}})b^{N-1}$ usados para representar c_{ij}. A matriz M é invertível.

c) Encontre a representação matricial $\mathcal{T}_i^*$ alterada, equivalente à representação matricial irredutível $\overline{\mathcal{T}}_i$. Para todo $g \in G$,

$$\mathcal{T}^*(g) = M^{-1}\overline{\mathcal{T}}(g)M.$$

   Assim, as representações matriciais $\mathcal{T}_i^*$, $1 \leq i < N$ são encontradas.

4. Para cada $i \in P$, $\mathcal{C}_i = \oplus_{j=1}^N W_{ij}$. Aplique o Teorema 3.4.22 para determinar e_{ij}, o gerador idempotente de W_{ij}. Então para cada j , $1 \leq j \leq N$, $e_j = \sum_{i\in P} e_{ij}$ gera um código em LG que contém um código minimal à esquerda $\mathcal{W}_j \subset \mathbb{F}G$ como subcódigo subcorpo. E assim, $\mathfrak{C} = \oplus_{j=1}^N \mathcal{W}_j$, onde $\mathcal{W}_j = \langle e_j \rangle_{\mathcal{L}}$.

Exemplo 3.4.25 *Considere o grupo metacíclico $G = G(9,3,4)$ e seja $\mathbb{F} = \mathbb{F}_2$ o corpo primo de característica 2. Pelo exemplo 2.2.12, $\mathfrak{C}_5$ é de grau $N = 3$ e corresponde à representação $\mathcal{T} = \mathcal{T}_9 \oplus \mathcal{T}_{10}$. Sejam $\mathcal{T}_9$ e $\mathcal{T}_{10}$ representações correspondentes aos códigos centrais minimais $\mathcal{C}_9$ e $\mathcal{C}_{10}$ em $\mathbb{F}_{2^6}G$, com códigos cíclicos associados A_9 e A_{10}. Além disso, $\mathfrak{C}_5$ tem código cíclico associado $\mathcal{A}$ com gerador idempotente* 000100100. *Assim, produzimos duas decomposições em ideais minimais à esquerda de $\mathfrak{C}_5$ sobre $\mathbb{F}G$.*

De fato:

1. *Selecione de $\mathcal{A}$ as três palavras linearmente independentes* 000100100, 000010010, 000001001. *Altere a representação matricial usual, $\overline{\mathcal{T}}_9$, usando como nova base de vetores*

$$100\delta^6 00\delta^3 00, 0100\delta^6 00\delta^3 0 \, e \, 00100\delta^6 00\delta^3$$

(as três palavras de $\mathcal{A}$ projetadas sobre A_9).

Assim, encontramos uma representação semelhante $\mathcal{T}_9^*$, onde $\mathcal{T}_9^*(a) = \begin{pmatrix} 0 & 0 & \delta^3 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ *e* $\mathcal{T}_9^*(b) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \delta^3 & 0 \\ 0 & 0 & \delta^6 \end{pmatrix}$.

Alterando a representação matricial usual $\overline{\mathcal{T}}_{10}$, usando como nova base de vetores

$$100\delta^3 00\delta^6 00, 0100\delta^3 00\delta^6 0, \, e \, 00100\delta^3 00\delta^6$$

(as três palavras de $\mathcal{A}$ projetadas sobre A_{10}), encontramos uma representação semelhante $\mathcal{T}_{10}^*$, onde $\mathcal{T}_{10}^*(a) = \begin{pmatrix} 0 & 0 & \delta^6 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ *e* $\mathcal{T}_{10}^*(b) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \delta^6 & 0 \\ 0 & 0 & \delta^3 \end{pmatrix}$.

Os ideais minimais à esquerda em códigos centrais minimais $\mathcal{C}_i \subset \mathbb{F}_{2^6}G$ têm geradores idempotentes e_{ij}, $9 \leq i \leq 10$ e $1 \leq i \leq 3$ descritos a seguir:

$$\begin{aligned}
e_{9,1} &= 100\delta^6 00\delta^3 00|100\delta^6 00\delta^3 00|100\delta^6 00\delta^3 00, \\
e_{9,2} &= 100\delta^6 00\delta^3 00|\delta^6 00\delta^3 00100|\delta^3 00100\delta^6 00, \\
e_{9,3} &= 100\delta^6 00\delta^3 00|\delta^3 00100\delta^6 00|\delta^6 00\delta^3 00100, \\
e_{10,1} &= 100\delta^3 00\delta^6 00|100\delta^3 00\delta^6 00|100\delta^3 00\delta^6 00, \\
e_{10,2} &= 100\delta^3 00\delta^6 00|\delta^3 00\delta^6 00100|\delta^6 00100\delta^3 00, \\
e_{10,3} &= 100\delta^3 00\delta^6 00|\delta^6 00100\delta^3 00|\delta^3 00\delta^6 00100.
\end{aligned}$$

Em $\mathbb{F}_2 G$, encontramos os códigos minimais à esquerda $\mathcal{W}_i, 1 \leq i \leq 3$, somandos de $\mathfrak{C}_5$ com geradores idempotentes $e_i = e_{9,i} + e_{10,i}$ descritos a seguir:

- *O código* $\mathcal{W}_1$ *tem gerador idempotente* $e_1 = 000100100|000100100|000100100$ *e é um* $(27, 6, 6)$ *código.*
- *O código* $\mathcal{W}_2$ *tem gerador idempotente* $e_2 = 000100100|100100000|100000100$ *e é um* $(27, 6, 6)$ *código.*
- *O código* $\mathcal{W}_3$ *tem gerador idempotente* $e_3 = 000100100|100000100|100100000$ *e é um* $(27, 6, 6)$ *código.*

2. *Selecione de* $\mathcal{A}$ *as três palavras linearmente independentes* 000111111, 000110110, 000011011. *Altere a representação matricial usual* $\overline{\mathcal{T}}_9$, *usando como nova base de vetores*

$$111\delta^6\delta^6\delta^6 00\delta^3\delta^3\delta^3, 110\delta^6\delta^6 0\delta^3\delta^3 0 \, e \, 011\delta^6\delta^6 0\delta^3\delta^3$$

(as três palavras de $\mathcal{A}$ *projetadas sobre* A_9*).*

Assim, encontramos uma representação semelhante $\mathcal{T}_9'$, *onde* $\mathcal{T}_9'(a) = \begin{pmatrix} \delta^3 & 0 & \delta^6 \\ 0 & 0 & 1 \\ \delta^6 & 1 & \delta^3 \end{pmatrix}$ *e* $\mathcal{T}_9'(b) = \begin{pmatrix} 0 & \delta^6 & 1 \\ 1 & \delta^3 & 1 \\ \delta^6 & \delta^6 & \delta^3 \end{pmatrix}$.

Alterando a representação matricial usual $\overline{\mathcal{T}}_{10}$, *usando como nova base de vetores* $111\delta^3\delta^3\delta^3\delta^6\delta^6\delta^6, 110\delta^3\delta^3 0\delta^6\delta^6 0$, *e* $010\delta^3\delta^3 0\delta^6\delta^6 0$ *(as três palavras de* $\mathcal{A}$ *projetadas sobre* A_{10}*), encontramos uma representação semelhante* $\mathcal{T}_9'$, *onde* $\mathcal{T}_{10}'(a) = \begin{pmatrix} \delta^6 & 0 & \delta^3 \\ 0 & 0 & 1 \\ \delta^3 & 1 & \delta^6 \end{pmatrix}$ *e* $\mathcal{T}_{10}'(b) = \begin{pmatrix} 0 & \delta^3 & 1 \\ 1 & \delta^6 & 1 \\ \delta^3 & \delta^3 & \delta^6 \end{pmatrix}$.

Os ideais minimais à esquerda nos códigos centrais minimais $\mathcal{C}_i \subset \mathbb{F}_{2^6}G$ *têm geradores idempotentes* e_{ij}, $9 \leq i \leq 10$ *e* $1 \leq i \leq 3$ *descritos a seguir:*

$$e_{9,1} = 1\delta^6 1\delta^6\delta^3\delta^6\delta^3 1\delta^3|0\delta^6\delta^3 0\delta^3 101\delta^6|01\delta^3 0\delta^6 10\delta^3\delta^6,$$

$$e_{9,2} = 1\delta^6 0\delta^6\delta^3 0\delta^3 10|\delta^6 1\delta^6\delta^3\delta^6\delta^3 1\delta^3 1|\delta^3\delta^3\delta^6 11\delta^3\delta^6\delta^6 1,$$

$$e_{9,3} = 101\delta^6 0\delta^6\delta^3 0\delta^3|\delta^6\delta^3 1\delta^3 1\delta^6 1\delta^6\delta^3|\delta^3\delta^6 11\delta^3\delta^6\delta^6 1\delta^3,$$

$$e_{10,1} = 1\delta^3 1\delta^3\delta^6\delta^3\delta^6 1\delta^6|0\delta^3\delta^6 0\delta^6 101\delta^3|01\delta^6 0\delta^3 10\delta^6\delta^3,$$

$$e_{10,2} = 1\delta^3 0\delta^3\delta^6 0\delta^6 10|\delta^3 1\delta^3\delta^6\delta^3\delta^6 1\delta^6 1|\delta^6\delta^6\delta^3 11\delta^6\delta^3\delta^3 1,$$

$$e_{10,3} = 101\delta^3 0\delta^3\delta^6 0\delta^6|\delta^3\delta^6 1\delta^6 1\delta^3 1\delta^3\delta^6|\delta^6\delta^3 11\delta^6\delta^3\delta^3 1\delta^6.$$

Em $\mathbb{F}_2G$, *encontramos os códigos minimais à esquerda* $\mathcal{W}_i, 1 \leq i \leq 3$, *somandos de* $\mathfrak{C}_5$ *com geradores idempotentes* $e_i = e_{9,i} + e_{10,i}$ *descritos a seguir:*

- *O código* $\mathcal{W}_1$ *tem gerador idempotente* $e_1 = 010111101|011010001|001010011$ *e é um* $(27, 6, 12)$ *código.*

- *O código* $\mathcal{W}_2$ *tem gerador idempotente* $e_2 = 010110100|101111010|111001110$ *e é um* $(27, 6, 12)$ *código.*
- *O código* $\mathcal{W}_3$ *tem gerador idempotente* $e_3 = 000101101|110101011|110011101$ *e é um* $(27, 6, 12)$ *código.*

3.5 Limites e Resultados

Como indicado acima, códigos metacíclicos minimais à esquerda que são subcódigos de um mesmo código central não precisam ser combinatorialmente equivalentes e podem ter distâncias mínimas muito diferentes. Se o código central minimal $\mathfrak{C}$ em $\mathbb{F}G$ tem um código cíclico associado o qual é minimal em $\mathbb{F}\mathbb{Z}_M$, a distância mínima de qualquer subcódigo de $\mathfrak{C}$ pode ser limitada.

Seja $\mathcal{C}$ um código central minimal em LG de grau N correspondente à representação irredutível $\mathcal{T}$. Se $\overline{\mathcal{T}}$ é uma representação matricial relacionada a $\mathcal{T}$, então $\mathcal{C} = \oplus_{i=1}^{N} W_i$ e cada W_i é um código minimal à esquerda.

Lema 3.5.1 *Seja* $\mathfrak{C}$ *um código central minimal em* $\mathbb{F}G(M, N, R)$ *de grau* N *com código cíclico associado* $\mathcal{A}$ *minimal em* $\mathbb{F}\mathbb{Z}_M$ *e seja* $\mathcal{W}$ *um código minimal à esquerda em* $\mathfrak{C}$. *Se* $c = c_0|c_1|...|c_{N-1} \in \mathcal{W}$ *e* $c \neq 0$, *então* $c_i \neq 0$ *para todo* i, $0 \leq i < N$.

Prova: Seja $\mathbb{F} = \mathbb{F}_{2^q}$. Pelos Teoremas 3.4.17 e 3.4.21, ambos $\mathcal{W}$ e $\mathcal{A}$ têm dimensão kN para algum $k \geq 1$. Assim, ambos $\mathcal{W}$ e $\mathcal{A}$ contêm $(2^q)^{kN}$ elementos. Assuma, sem perda de generalidade, que para algum $c \in \mathcal{W}$, $c_0 \neq \mathbf{0}$ e $c_{N-1} = \mathbf{0}$. Pela Definição 3.4.13, $c_0 \in \mathcal{A}$. Considere $\mathcal{A} \subset \mathbb{F}G$. Para todo $x \in \mathcal{A}$, $xc \in \mathcal{W}$ e

$$xc = xc_0|xc_1|...|xc_{N-1} = xc_0|xc_1|...|\mathbf{0}.$$

Como $\mathcal{A}$ é minimal, c_0 gera $\mathcal{A}$. Assim, para cada $x \in \mathcal{A}$ distinto, xc é um elemento distinto de $\mathcal{W}$. Existem $(2^q)^{kN}$ tais elementos. Assim, cada elemento de $\mathcal{W}$ deve ser desta forma, e cada elemento não nulo de $\mathcal{W}$ tem uma primeira M-upla não nula. Entretanto, supondo que $x = \alpha_0 + \alpha_1 a + \alpha_2 a^2 + ... + \alpha_{M_{-1}} a^{M-1}$ e $c = \beta_{00} + \beta_{10} a + \beta_{20} a^2 + ... + \beta_{(M-1)0} a^{M-1} + \beta_{01} b + \beta_{12} ab + ... + \beta_{(M-1)1} a^{M-1} b + ... + \beta_{0(N-1)} b^{N-1} + \beta_{1(N-1)} ab^{N-1} + ... + \beta_{(M-1)(N-1)} a^{M-1} b^{N-1}$, temos:

$$bc = \beta_{00} b + \beta_{10} a^R b + \beta_{20} a^{2R} b + ... + \beta_{(M-1)0} a^{R(M-1)} b + \beta_{01} b^2 + \beta_{11} a^R b^2 + ...+$$

$$+\beta_{(M-1)1} a^{R(M-1)} b^2 + ... + \beta_{0(N-1)} a^{R(N-1)} b + \beta_{1(N-1)} a^R + ... + \beta_{(M-1)(N-1)} a^{R(M-1)}.$$

Reorganizando estes fatores de acordo com a ordem da base (os elementos de G) e utilizando a notação definida na página 69, temos

$$bc = bc_{N-1}|bc_0|...|bc_{N-2} = \mathbf{0}|bc_0|...|bc_{N-2} \in \mathcal{W}.$$

Isto contradiz a conclusão prévia que a primeira M-upla de um elemento em $\mathcal{W}$ ser $\mathbf{0}$ somente quando o elemento for $\mathbf{0}$.

Portanto, a suposição de que $c_{N-1} = \mathbf{0}$ é falsa.

■

Usaremos $Avg(\mathfrak{C})$ para indicar a média aritmética dos pesos das palavras não nulas do código linear $\mathfrak{C}$. Claramente, a distância mínima de qualquer código-bloco linear $\mathfrak{C}$, $d_{min}(\mathfrak{C})$, deve estar limitada por $[Avg(\mathfrak{C})]$ acima.

Agora, limitamos a distância mínima de certos códigos minimais à esquerda usando a média aritmética do peso das palavras não nulas de códigos cíclicos associados e a distância mínima destes códigos cíclicos. Para limitarmos esta distância mínima precisaremos da seguinte observação.

Observação 3.5.2 *Seja* $c = \beta_{00}\beta_{10}\beta_{20}...\beta_{(M-1)0}|\beta_{01}\beta_{12}...\beta_{(M-1)1}|...|\beta_{0(N-1)}\beta_{1(N-1)}...\beta_{(M-1)(N-1)} = c_0|c_1|...|c_{N-1}$ *uma palavra não nula de um código* $\mathcal{C}$.

Assim,
$ac = \beta_{(M-1)0}\beta_{00}\beta_{10}\beta_{20}...\beta_{(M-2)0}|\beta_{(M-1)1}\beta_{01}\beta_{12}...\beta_{(M-2)1}|...|\beta_{(M-1)(N-1)}\beta_{0(N-1)}\beta_{1(N-1)}$
$...\beta_{(M-2)(N-1)}$
$a^2c = \beta_{(M-2)0}\beta_{(M-1)0}\beta_{00}\beta_{10}...\beta_{(M-3)0}|\beta_{(M-2)1}\beta_{(M-1)1}\beta_{01}...\beta_{(M-3)1}|...|\beta_{(M-2)(N-1)}$
$\beta_{(M-1)(N-1)}\beta_{0(N-1)}...\beta_{(M-3)(N-1)}$
$\vdots$
$a^jc = \beta_{(M-j)0}...\beta_{(M-1)0}\beta_{00}\beta_{10}...\beta_{[M-(j+1)]0}|\beta_{(M-j)1}...\beta_{(M-1)1}\beta_{01}...\beta_{[M-(j+1)]1}|...|$
$\beta_{(M-j)(N-1)}...\beta_{(M-1)(N-1)}\beta_{0(N-1)}...\beta_{[M-(j+1)](N-1)}$, *para todo* $1 \leq j \leq M-1$.

Logo multiplicar qualquer potência de a por uma palavra de um código permuta os coeficientes dos N-blocos desta palavra.

Agora, como em um grupo metacíclico dado por (2.3) temos $ba = a^Rb$, *multiplicar qualquer potência de b por uma palavra não nula de um código significa que temos uma permutação cíclica dos N-blocos de cada palavra do código, ou seja,*
$bc = c_{N-1}|c_0|c_1|...|c_{N-2}$
$b^2c = c_{N-2}|c_{N-1}|c_0|...|c_{N-3}$
$\vdots$
$b^tc = c_{N-t}|...|c_0|...|c_{N-(t+1)}$, *para todo* $1 \leq t \leq N-1$.

Exemplo 3.5.3 *Considere o código central minimal* $\mathfrak{C}_3 = \langle x_3 \rangle$ *do Exemplo 3.4.12. Seja* $c = 011011011|0\omega^2\omega^2 0\omega^2\omega^2 0\omega^2\omega^2|0\omega\omega 0\omega\omega 0\omega\omega$ *uma palavra do código* $\mathfrak{C}_3$*. Daí temos:*
$ac = 101101101|\omega^2 0\omega^2\omega^2 0\omega^2\omega^2 0\omega^2|\omega 0\omega\omega 0\omega\omega 0\omega,$
$a^5c = 110110110|\omega^2\omega^2 0\omega^2\omega^2 0\omega^2\omega^2 0|\omega\omega 0\omega\omega 0\omega\omega 0,$
$bc = 0\omega\omega 0\omega\omega 0\omega\omega|011011011|0\omega^2\omega^2 0\omega^2\omega^2 0\omega^2\omega^2$ *e*
$b^2c = 0\omega^2\omega^2 0\omega^2\omega^2 0\omega^2\omega^2|0\omega\omega 0\omega\omega 0\omega\omega|011011011.$

Teorema 3.5.4 *Seja* $\mathfrak{C}$ *um código central minimal em* $\mathbb{F}G$ *de grau* N *com código cíclico associado* $\mathcal{A}$ *minimal à esquerda em* $\mathfrak{C}$*, então*

$$Nd_{min}(\mathcal{A}) \leq d_{min}(\mathcal{W}) \leq [N \cdot Avg(\mathcal{A})],$$

onde $Avg(\mathcal{A})$ *é a média aritmética dos pesos das palavras não nulas em* $\mathcal{A}$*.*

Prova: O limite inferior de $d_{min}(\mathcal{W})$ segue diretamente do Lema 3.5.1.

Pelo Teorema 3.4.21, $\mathcal{W}$ tem dimensão kN. Listamos todas as $(2^q)^{kN}$ palavras não nulas de $\mathcal{W}$ como:

$$\begin{array}{rcl} c_1 & = & c_{11}|c_{12}|...|c_{1N} \\ c_2 & = & c_{21}|c_{22}|...|c_{2N} \\ \vdots & & \\ c_h & = & c_{h1}|c_{h2}|...|c_{hN} \end{array} .$$

onde $h = (2^q)^{kN} - 1$.

O Lema 3.5.1 nos diz que para uma palavra não nula em $\mathcal{W}$, todas os N-blocos são não nulos, ou seja, para todo i , $1 \leq i \leq h$, $c_{ij} \neq 0$ para todo j , $1 \leq j \leq N$. Além disso, a diferença $c_i - c_j \in \mathcal{W}$ para todos i, j, $1 \leq i, j \leq N$, pois $\mathcal{W}$ é um código. Assim, pelo Lema 3.5.1, para todo f, $1 \leq f \leq N$, $c_{if} \neq c_{jf}$.

Seja $\mathcal{A}^1 = \{c_{i1} : 1 \leq i \leq h\}$ o conjunto de todas a primeiras M-uplas das palavras não nulas de $\mathcal{W}$. Para todo f, $1 \leq f \leq h$, conjunto de todas as f-ésimas M-uplas $\mathcal{A}^f = \{c_{if} : 1 \leq i \leq h\}$ é igual a $\mathcal{A}^1$. De fato:

Note que para cada $1 \leq s \leq M-1$, $\{a^s c_j : j = 1, ..., h\} = \{c_j : j = 1, ..., h\} = \mathcal{W}^*$ e para cada $1 \leq t \leq N-1$, $\{b^t c_j : j = 1, ..., h\} = \mathcal{W}^*$, ou seja, multiplicar o conjunto $\{c_j : j = 1, ..., h\}$ por algum elemento da álgebra de grupo $\mathbb{F}G$, permuta estes elementos entre si.

Pela observação acima, temos $a^j\mathcal{A}^t = \mathcal{A}^1$, pois multiplicando todas as palavras não nulas de um código com qualquer potência de a há uma permutação entre os coeficientes de cada bloco das palavras e também pelo fato que $c_{if} \neq c_{jf}$, para todo f.

Temos também que

$$\begin{array}{rcl} d_{1f} = b^{N-f+1}c_1 & = & c_{1f}|c_{1-f+1}|...|c_{1N}|c_{11}|...|c_{1f-1} \\ d_{2f} = b^{N-f+1}c_2 & = & c_{2f}|c_{2-f+1}|...|c_{2N}|c_{21}|...|c_{2f-1} \\ \vdots & & \\ d_{hf} = b^{N-f+1}c_h & = & c_{hf}|c_{h-f+1}|...|c_{hN}|c_{h1}|...|c_{hf-1} \end{array} .$$

Mas, $\{d_{1f}, d_{2f}, ..., d_{hf}\} = \{c_1, c_2, ..., c_h\} = \mathcal{W}^*$. Assim, $b^{N-f+1}\mathcal{W}^* = \mathcal{W}^*$.

Logo mostramos que $b^{N-f+1}\mathcal{A}^1 = \mathcal{A}^f$. Portanto, $\mathcal{A}^f = \mathcal{A}^1$.

Seja $\mathbf{w}_i$ o número de palavras de peso i. Se $\mathcal{W}$ tem distribuição de peso $\mathbf{w}_0, \mathbf{w}_1, ..., \mathbf{w}_{MN}$ e $\mathcal{A}$ tem distribuição de peso $\mathbf{w}_0^{'}, \mathbf{w}_1^{'}, ..., \mathbf{w}_M^{'}$, então

$$\sum_{i=1}^{MN} \mathbf{w}_i \cdot i = N \sum_{i=1}^{M} \mathbf{w}_i^{'} \cdot i,$$

$$\sum_{i=1}^{MN} \mathbf{w}_i \cdot \frac{i}{h} = N \sum_{i=1}^{M} \mathbf{w}_i^{'} \cdot \frac{i}{h},$$

onde $h = (2^q)^{kN} - 1$.

Assim, $Avg(\mathcal{W}) = Avg(\mathcal{A})$. Daí $d_{min}(\mathcal{W}) \leq Avg(\mathcal{W}) \leq N \cdot Avg(\mathcal{A})$.

■

Lema 3.5.5 *Se todas as palavras de um código linear $\mathcal{C}$ de comprimento n e dimensão k sobre um corpo $\mathbb{F}$ de q elementos são organizadas como linhas de uma matriz $q^k \times n$ de modo que nenhuma coluna da matriz é nula, então cada elemento do corpo $\mathbb{F}$ aparece q^{k-1} vezes em cada coluna.*

Prova: Com j fixado, considere $W = \{x = (x_1, x_2, ..., x_{j-1}, 0, x_{j+1}, ..., x_n) : x \in \mathcal{C}\}$ o conjunto de todas as palavras do código $\mathcal{C}$ que possuem a j-ésima entrada nula.

Afirmamos que W é um subespaço vetorial de $\mathcal{C}$. De fato:

- $W \neq \emptyset$, pois a palavra $(0, 0, ..., 0, 0, 0, ..., 0) \in \mathcal{C}$, já que 0 está na j-ésima posição.
- Sejam $x, y \in \mathcal{C}$. Daí $x = (x_1, x_2, ..., x_{j-1}, 0, x_{j+1}, ..., x_n)$ e $y = (y_1, y_2, ..., y_{j-1}, 0, y_{j+1}, ..., y_n)$. Assim,

  $$x + y = (x_1 + y_1, x_2 + y_2, ..., x_{j-1} + y_{j-1}, 0, x_{j+1} + y_{j+1}, ..., x_n + y_n)$$

  e, portanto, $x + y \in \mathcal{C}$.

- Sejam $z \in \mathbb{F}$ e $x = (x_1, x_2, ..., x_{j-1}, 0, x_{j+1}, ..., x_n)$. Daí $z \cdot x = (z \cdot x_1, z \cdot x_2, ..., z \cdot x_{j-1}, z \cdot 0, z \cdot x_{j+1}, ..., z \cdot x_n) = (zx_1, zx_2, ..., zx_{j-1}, 0, zx_{j+1}, ..., zx_n)$. Portanto, $z \cdot x \in \mathcal{C}$.

Considere as classes laterais de W em $\mathcal{C}$, ou seja, $y+W = (y_1, y_2, ..., y_{j-1}, y_j, y_{j+1}, ..., y_n) + W$, onde $y \in \mathcal{C}$.

Se $\mathbb{F}_q = \{0, a_1, a_2, ..., a_{q-1}\}$, então podemos tomar como representantes das classes laterais distintas de W em $\mathcal{C}$ os elementos: $(0, 0, ..., 0)$ e $\overline{a}_i = (0, ..., a_i, 0, ..., 0)$, com a_i na posição j, para cada $1 \leq i \leq q-1$.

Como as classes laterais são disjuntas e sua união nos fornece o código todo, temos:

$$\mathcal{C} = W \cup (\overline{a}_1 + W) \cup (\overline{a}_2 + W) \cup ... \cup (\overline{a}_{q-1} + W).$$

Pelo Teorema de Lagrange, as classes laterais são equipotentes, assim:

$$|\mathcal{C}| = |W| + |(\overline{a}_1 + W)| + |(\overline{a}_2 + W)| + ... + |(\overline{a}_{q-1} + W)| = q|W|.$$

Por outro lado, $|\mathcal{C}| = q^k$. Portanto, $|W| = q^{k-1}$. E assim, segue o resultado.

■

Lema 3.5.6 *Considerando as hipóteses do Lema 3.5.5, a soma de todos os pesos das palavras do código $\mathcal{C}$ é $n(q-1)q^{k-1}$.*

Prova: Pelo Lema 3.5.5, cada elemento do corpo $\mathbb{F}$ aparece q^{k-1} vezes em cada coluna. Para calcular o peso de uma palavra, descartamos as q^{k-1} vezes em que o 0 aparece em cada coluna. Assim, temos $q-1$ elementos não nulos do corpo que aparecem q^{k-1} vezes em cada coluna. Como a matriz formada pelas palavras do código $\mathcal{C}$ possui n colunas, a soma de todos os pesos das palavras do código é $n(q-1)q^{k-1}$.

■

Como qualquer código-bloco $\mathfrak{C}$ de comprimento n e dimensão k sobre um corpo $\mathbb{F} = \mathbb{F}_{2^q}$ possui $2^{q^k} - 1$ elementos com peso não nulo, pelos Lemas 3.5.5 e 3.5.6, concluímos que a $Avg(\mathfrak{C}) = \dfrac{n \cdot (2^q - 1)(2^q)^{k-1}}{2^{q^k} - 1}$. Assim, os limites do Teorema 3.5.4 podem ser reescritos.

Corolário 3.5.7 *Seja $\mathfrak{C}$ um código central minimal em $\mathbb{F}_{2^q}G$ de grau N com dimensão kN^2 e código cíclico associado $\mathcal{A}$ minimal em $\mathbb{F}\mathbb{Z}_M$. Se $\mathcal{W}$ é um código minimal à esquerda em $\mathfrak{C}$, então*

$$Nd_{min}(\mathcal{A}) \leq d_{min}(\mathcal{W}) \leq \left[N \cdot M\frac{(2^q-1)(2^q)^{kN-1}}{2^{q^{kN}}-1}\right].$$

O limite inferior da distância mínima é sempre alcançado por um código minimal à esquerda que é uma repetição do código cíclico associado. Um tal código é combinatorialmente equivalente ao código abeliano $\mathcal{A} \otimes \mathfrak{C}$, onde $\mathfrak{C}$ é o código unidimensional em $\mathbb{F}\mathbb{Z}_N$ gerado por $\sum_{i=0}^{N-1} b^i$. Muitos códigos minimais à esquerda são equivalentes a códigos não abelianos e excedem este limite inferior.

O limite superior da distância mínima é muito bom, já que frequentemente ultrapassa a distância mínima do melhor código linear encontrado para um comprimento e uma dimensão comparáveis. Claro que não temos a garantia de que um código minimal à esquerda com tal distância mínima exista. Na prática, entretanto, encontramos códigos com distâncias mínimas que satisfazem o limite superior. Em alguns casos, o código tem distância mínima que é igual ao melhor código-bloco linear de comprimento e dimensão comparáveis.

Observação 3.5.8 *Nos próximos exemplos, utilizamos o Sistema Octal para simplificar a apresentação dos geradores dos códigos minimais à esquerda em $\mathbb{F}G$. Assim, apresentamos agora a conversão do Sistema Binário para o Sistema Octal e vice-versa.*

Para realizar a conversão do Sistema Binário para o Octal, separamos o número binário em grupos de três em três dígitos a partir da direita. Depois fazemos a divisão do número formado em cada grupo por 8, e o número octal encontrado é o resto desta divisão. Caso o último grupo não tenha três dígitos, chegamos a este valor completando o grupo com zeros à esquerda.

Exemplo 3.5.9 *O número binário 100111 é transformado em 47 no Sistema Octal, pois 100 tem resto 4 na divisão por 8 e 111 tem resto 7 na divisão por 8.*

Para realizar a conversão do Sistema Octal para o Binário, basta converter cada dígito do número em octal no seu correspondente binário.

Exemplo 3.5.10 *O número octal 76 é transformado em 111110 no Sistema Binário, pois 7 corresponde a 111 no Sistema Binário e 6 corresponde a 110 no Sistema Binário.*

No próximo exemplo mostramos uma aplicação do Teorema 3.5.4 e descrevemos alguns geradores dos códigos minimais à esquerda em duas álgebras de grupo.

Exemplo 3.5.11 1. *Em* $\mathbb{F}_2G(9,3,4)$ *considere o código central minimal* $\mathfrak{C}$ *com código cíclico associado* $\mathcal{A} = \langle 000100100\rangle$, $d_{min}(\mathcal{A}) = 2$ *e* $Avg(\mathcal{A}) = 4,57$.

Se $\mathcal{W} \subset \mathfrak{C}$ *é um código minimal à esquerda de* $\mathcal{C}$, *então* $3 \cdot 2 \leq d_{min}(\mathcal{W}) \leq [3 \cdot 4,57]$, *isto é,* $6 \leq d_{min}(\mathcal{W}) \leq 13$. *Com geradores apresentados no Sistema Octal, temos:*

a) O código $\mathcal{W}_1 = \langle 044|044|044\rangle_{\mathcal{L}}$ *tem distância mínima* 6 *e é combinatorialmente equivalente à repetição de* $\mathcal{A}$ *(*3 *vezes). De fato, para provar que a distância mínima de* $\mathcal{W}_1$ *é* 6, *observamos primeiro que a distância mínima de* $\mathcal{A}$ *é* 2.

Como $\mathcal{A} = \langle a^3 + a^6\rangle_{\mathcal{L}}$ *e* $\omega(a^3 + a^6) = 2$, *temos* $\omega(\mathcal{A}) \leq \omega(a^3 + a^6) = 2$.

Agora, todo elemento do código cíclico $\mathcal{A}$ *é dado por:*

$$\begin{aligned}\beta &= \left(\sum_{i=0}^{8} \alpha_i a^i\right)(a^3 + a^6)\\ &= (\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \alpha_3 a^3 + \alpha_4 a^4 + \alpha_5 a^5 + \alpha_6 a^6 + \alpha_7 a^7 + \alpha_8 a^8)(a^3 + a^6)\\ &= \alpha_0 a^3 + \alpha_1 a^4 + \alpha_2 a^5 + \alpha_3 a^6 + \alpha_4 a^7 + \alpha_5 a^8 + \alpha_6 + \alpha_7 a + \alpha_8 a^2 + \alpha_0 a^6 + \alpha_1 a^7 + \\ &\alpha_2 a^8 + \alpha_3 + \alpha_4 a + \alpha_5 a^2 + \alpha_6 a^3 + \alpha_7 a^4 + \alpha_8 a^5\\ &= (\alpha_3 + \alpha_6) + (\alpha_7 + \alpha_4)a + (\alpha_8 + \alpha_5)a^2 + (\alpha_0 + \alpha_6)a^3 + (\alpha_1 + \alpha_7)a^4 + (\alpha_2 + \\ &\alpha_8)a^5 + (\alpha_3 + \alpha_0)a^6 + (\alpha_4 + \alpha_1)a^7 + (\alpha_5 + \alpha_2)a^8.\end{aligned}$$

Como $\omega(\mathcal{A}) \leq \omega(a^3+a^6) = 2$, *devemos ter* $\omega(\mathcal{A}) = 1$ *ou* $\omega(\mathcal{A}) = 2$. *Se* $\omega(\mathcal{A}) = 1$, *então deve existir um elemento de* $\mathcal{A}$ *que tenha um único coeficiente não nulo.*

Observemos que os coeficientes destes elementos são somas de coeficientes com índices distintos e cada α_i *aparece somente em dois coeficientes de* β.

Por causa desta observação podemos supor, sem perda de generalidade, que $\alpha_3 + \alpha_6$ *é este coeficiente não nulo. Como estamos sobre* $\mathbb{F}_2$, $\alpha_3 = 1$ *e* $\alpha_6 = 0$ *ou* $\alpha_3 = 0$ *e* $\alpha_6 = 1$.

Se $\alpha_3 = 1$ *e* $\alpha_6 = 0$, *então o coeficiente de* a^6 *também será não nulo, o que é uma contradição com a hipótese de que* $\omega(\mathcal{A}) = 1$.

Se $\alpha_3 = 0$ *e* $\alpha_6 = 1$, *então o coeficiente de* a^3 *também será não nulo, o que é uma contradição com a hipótese de que* $\omega(\mathcal{A}) = 1$.

Portanto, $\omega(\mathcal{A}) = d_{min}(\mathcal{A}) = 2$.

Uma palavra no código minimal à esquerda $\mathcal{W}_1$ é da forma:

$$v = \left(\sum_{j=0}^{2}\sum_{i=0}^{8}\alpha_{ij}a^ib^j\right)(a^3+a^6)(1+b+b^2) = \left(\sum_{j=0}^{2}\sum_{i=0}^{8}\alpha_{ij}a^ib^j\right)(1+b+b^2)(a^3+a^6),$$

pois $(a^3+a^6)(1+b+b^2) = (1+b+b^2)(a^3+a^6)$.

Primeiro escrevemos o elemento $u = \left(\sum_{j=0}^{2}\sum_{i=0}^{8}\alpha_{ij}a^ib^j\right)(1+b+b^2)$ *da seguinte maneira:*

$$u = \sum \alpha_{ij}a^ib^j + \sum \alpha_{ij}a^ib^{j+1} + \sum \alpha_{ij}a^ib^{j+2} =$$
$$= \{(\alpha_{00}+\alpha_{01}+\alpha_{02}) + (\alpha_{10}+\alpha_{12}+\alpha_{11})a + (\alpha_{20}+\alpha_{22}+\alpha_{21})a^2 +$$
$$+(\alpha_{30}+\alpha_{32}+\alpha_{31})a^3 + (\alpha_{40}+\alpha_{42}+\alpha_{41})a^4 + (\alpha_{50}+\alpha_{52}+\alpha_{51})a^5 +$$
$$+(\alpha_{60}+\alpha_{62}+\alpha_{61})a^6 + (\alpha_{70}+\alpha_{72}+\alpha_{71})a^7 + (\alpha_{80}+\alpha_{82}+\alpha_{81})a^8\}b^0$$
$$+\{(\alpha_{01}+\alpha_{00}+\alpha_{02}) + (\alpha_{11}+\alpha_{10}+\alpha_{12})a + (\alpha_{21}+\alpha_{20}+\alpha_{22})a^2 +$$
$$+(\alpha_{31}+\alpha_{30}+\alpha_{32})a^3 + (\alpha_{41}+\alpha_{40}+\alpha_{42})a^4 + (\alpha_{51}+\alpha_{50}+\alpha_{52})a^5 +$$
$$+(\alpha_{61}+\alpha_{60}+\alpha_{62})a^6 + (\alpha_{71}+\alpha_{70}+\alpha_{72})a^7 + (\alpha_{81}+\alpha_{80}+\alpha_{82})a^8\}b^1 +$$
$$+\{(\alpha_{02}+\alpha_{01}+\alpha_{00}) + (\alpha_{12}+\alpha_{11}+\alpha_{10})a + (\alpha_{22}+\alpha_{21}+\alpha_{20})a^2 +$$
$$+(\alpha_{32}+\alpha_{31}+\alpha_{30})a^3 + (\alpha_{42}+\alpha_{41}+\alpha_{40})a^4 + (\alpha_{52}+\alpha_{51}+\alpha_{50})a^5 +$$
$$+(\alpha_{62}+\alpha_{61}+\alpha_{60})a^6 + (\alpha_{72}+\alpha_{71}+\alpha_{70})a^7 + (\alpha_{82}+\alpha_{81}+\alpha_{80})a^8\}b^2.$$

E observamos que os três blocos de coeficientes deste elemento que acompanham b^0, b^1 *e* b^2, *respectivamente, são iguais. Assim, para calcularmos o peso deste elemento é suficiente verificarmos o que acontece com o primeiro bloco de coeficientes quando multiplicamos por* a^3+a^6. *Fazendo* $d = \{(\alpha_{00}+\alpha_{01}+\alpha_{02}) + (\alpha_{10}+\alpha_{12}+\alpha_{11})a + (\alpha_{20}+\alpha_{22}+\alpha_{21})a^2 + (\alpha_{30}+\alpha_{32}+\alpha_{31})a^3 + (\alpha_{40}+\alpha_{42}+\alpha_{41})a^4 + (\alpha_{50}+\alpha_{52}+\alpha_{51})a^5 + (\alpha_{60}+\alpha_{62}+\alpha_{61})a^6 + (\alpha_{70}+\alpha_{72}+\alpha_{71})a^7 + (\alpha_{80}+\alpha_{82}+\alpha_{81})a^8\}b^0$, *obtemos:*

$$Y = d(a^3+a^6) = (\alpha_{60}+\alpha_{62}+\alpha_{61}+\alpha_{30}+\alpha_{32}+\alpha_{31}) + (\alpha_{70}+\alpha_{72}+\alpha_{71}+\alpha_{40}+\alpha_{42}+\alpha_{41})a + (\alpha_{80}+\alpha_{82}+\alpha_{81}+\alpha_{50}+\alpha_{52}+\alpha_{51})a^2 + (\alpha_{00}+\alpha_{01}+\alpha_{02}+\alpha_{60}+\alpha_{61}+\alpha_{62})a^3 + (\alpha_{10}+\alpha_{12}+\alpha_{11}+\alpha_{70}+\alpha_{72}+\alpha_{71})a^4 + (\alpha_{20}+\alpha_{22}+\alpha_{21}+\alpha_{80}+\alpha_{81}+\alpha_{82})a^5 + (\alpha_{30}+\alpha_{32}+\alpha_{31}+\alpha_{00}+\alpha_{01}+\alpha_{02})a^6 + (\alpha_{40}+\alpha_{42}+\alpha_{41}+\alpha_{10}+\alpha_{12}+\alpha_{11})a^7 + (\alpha_{50}+\alpha_{52}+\alpha_{51}+\alpha_{20}+\alpha_{22}+\alpha_{21})a^8.$$

Note que cada soma $(\alpha_{i0}+\alpha_{i2}+\alpha_{i3})$ *aparece somente duas vezes como parcela de coeficiente em* Y, *similarmente ao que aconteceu no caso do elemento* β *do código cíclico. Este fato se repete nos três blocos de coeficientes. Isto não é surpresa, uma vez que* $\mathcal{W}_1$ *é combinatorialmente equivalente a três cópias de* $\mathcal{A}$. *Assim, sendo*

em Y se um coeficiente for não nulo , pelo menos mais um de seus coeficientes será não nulo. Logo Y tem peso maior ou igual a 2 e como este fato se repete nos outros dois blocos, o peso de v será pelo menos 6. Daí $\omega(\mathcal{W}_1) \geq 6$, mas como $\omega(\mathcal{W}_1) \leq \omega(\langle 044|044|044\rangle_{\mathcal{L}}) = 6$, concluímos que $\omega(\mathcal{W}_1) = 6$, ou seja, $d_{min}(\mathcal{W}_1) = 6$.

b) O código $\mathcal{W}_2 = \langle 264|572|716\rangle_{\mathcal{L}}$ tem distância mínima 12.

2. *Em $\mathbb{F}_2G(11, 5, 3)$ considere o código central minimal $\mathfrak{C}$ com código cíclico associado $\mathcal{A} = \langle 01111111111\rangle$, $d_{min}(\mathcal{A}) = 2$ e $Avg(\mathcal{A}) = 5, 5$.*

Se $\mathcal{W} \subset \mathfrak{C}$, então $5 \cdot 2 \leq d_{min}(\mathcal{W}) \leq [5 \cdot 5, 5]$, isto é, $10 \leq d_{min}(\mathcal{W}) \leq 27$. Com geradores apresentados no Sistema Octal, temos:

a)O código $\mathcal{W}_1 = \langle 1777|1777|1777|1777|1777\rangle_{\mathcal{L}}$ tem distância mínima 10 e é combinatorialmente equivalente à repetição de $\mathcal{A}$.

b) O código $\mathcal{W}_2 = \langle 1777|0404|0305|2362|3314\rangle_{\mathcal{L}}$ tem distância mínima 20 e é combinatorialmente equivalente a um código não abeliano de comprimento 55.

3.6 Códigos Diedrais e Quatérnios Minimais

Nesta seção consideramos dois grupos metacíclicos: os diedrais de ordem $2n$, que têm a apresentação dada por

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

e os quatérnios generalizados de ordem $4n$, que têm a seguinte apresentação

$$Q_n = \langle a, b : a^{2n} = 1,\, b^2 = a^n,\, b^{-1}ab = a^{-1}\rangle,$$

onde $n \geq 2$. Quando $n = 2$, Q_2 é dito simplesmente o grupo dos quatérnios.

Como estes grupos possuem ordem par, eles não satisfazem as hipóteses dos resultados apresentados nas seções anteriores. Assim, para descrever os idempotentes centrais primitivos geradores dos códigos diedrais minimais e dos códigos quatérnios minimais, devem ser aplicadas outras técnicas. Na tese de doutorado de Flaviana Dutra [9], sob algumas hipóteses sobre a característica do corpo, é exibida uma técnica para se descrever esses idempotentes.

Primeiramente, Dutra observa que o número de componentes simples da álgebra semissimples $\mathbb{F}_qD_n$ é maior ou igual ao número de componentes simples da álgebra de grupo racional $\mathbb{Q}D_n$. O teorema principal da tese de Dutra, determina para

quais valores de n o conjunto de idempotentes centrais primitivos pode ser obtido de maneira natural, ou seja, sob que condições $\mathbb{F}_q D_n$ e $\mathbb{Q}D_n$ têm o mesmo número de componentes simples e, nestes casos, descreve os idempotentes que são dados pelas mesmas fórmulas de $\mathbb{Q}D_n$, exceto pelo fato que os coeficientes são tomados como elementos de $\mathbb{F}_q$ no lugar de $\mathbb{Q}$. Para provar esse teorema, Dutra utilizou os resultados de Ferraz e Milies em [18], citados na seção 3.3 e outras propriedades inerentes ao grupo diedral.

Para estudar os códigos quatérnios minimais, Dutra utiliza a decomposição de Wedderburn da álgebra de grupo racional $\mathbb{Q}Q_n$ do grupo dos quatérnios generalizados para estabelecer em que condições a álgebra semissimples $\mathbb{F}_q Q_n$ tem o mesmo número de componentes simples que tal álgebra racional, restrita ao caso $n = 2^m$. Isto é feito de duas maneiras diferentes. Primeiramente, Dutra compara as decomposições de $\mathbb{F}_q Q_n$ e $\mathbb{F}_q D_n$ e depois utiliza o método de contagem de Ferraz estabelecido em [17].

Para os códigos diedrais minimais e para os casos de códigos quatérnios minimais apresentados em sua tese, Dutra determina as bases do código e calcula suas dimensões e distâncias mínimas, utilizando muitas propriedades da estrutura dos referidos grupos e seus subgrupos.

3.7 Considerações Finais

Na busca por melhores códigos, estudamos o caso dos códigos metacíclicos da álgebra de grupo do grupo metacíclico não abeliano de ordem ímpar apresentado em (2.3) sobre um corpo de característica 2, já que os códigos lineares, cíclicos e abelianos já são conhecidos. Observamos que os códigos metacíclicos centrais eram combinatorialmente equivalentes aos códigos abelianos. Procuramos então encontrar códigos metacíclicos que não tivessem essa equivalência. Assim, observamos que os códigos metacíclicos à esquerda (unilaterais) possuíam distância mínima maiores que os códigos abelianos de dimensão e comprimento comparáveis.

Outras técnicas para encontrar melhores códigos metacíclicos foram apresentadas por Dutra em sua tese de doutorado [9], para os grupos metacíclicos diedrais e quatérnios e Piret em [15] estudou códigos quase-cíclicos com geradores da forma $d|c_1|...|c_n$ onde d é o gerador idempotente de um código cíclico em $\mathbb{F}\mathbb{Z}_M$ e, para todo i , c_i é uma palavra de tal código. Em vários casos, os códigos quase-cíclicos estudados eram de fato códigos metacíclicos.

A tabela a seguir lista vários dos melhores códigos metacíclicos encontrados. A última coluna, as melhores d_{min}, foram descritas em [1]. Estão incluídos vários

códigos de comprimento par cujos geradores foram identificados usando técnicas similares mas não idênticas às descritas acima.

N	k	G	Gerador(octal)	d_{min}	Melhor d_{min}
14	6	$(7, 2, 6)$	164|113	4	5
14	7	$(7, 2, 6)$	013|064	4	4
(código	anterior	aumentado)			
21	6	$(7, 3, 2)$	072|072|047	8	8
27	6	$(9, 3, 4)$	356|055|365	12	12
27	8	$(9, 3, 4)$	275|456|654	10	10
127	19	$(9, 3, 4)$	dual do código anterior	4	4
55	10	$(11, 5, 3)$	0033|2026|1224|0305|0603	20	23
55	11	$(11, 5, 3)$	3710|1751|2553|3475|3174	20	22
(código	anterior	aumentado)			
55	20	$(11, 5, 3)$	0363|1001|3514|2031|1147	16	16
55	45	$(11, 5, 3)$	2350|3027|2730|2334|1744	4	4
63	3	$(21, 3, 4)$	3164723|2351647|7235164	36	36
63	12	$(21, 3, 4)$	2607663|2143455|3575316	24	24
93	15	$(31, 3, 5)$	13410237634|10702646457|17335771337	32	36
93	16	$(31, 3, 5)$	04367540143|07075131320|00442006440	32	34
(código	anterior	aumentado)			
93	77	$(31, 3, 5)$	dual do código anterior	6	6
110	10	$(11, 10, 7)$	1777|0126|0402|2272|1205|3342|0776|3063|0716|1576	48	49

Referências Bibliográficas

[1] A. E. Brouwer and T. Verhoff, *An updated table of minimum-distance bounds for binary linear codes*, IEEE Trans. Inform. Theory **39** (1993), 662-677.

[2] A. Hefez e M. L. T. Vilela,*Códigos Corretores de Erros*, IMPA, Rio de Janeiro, 2002.

[3] C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Interscience, New York, 1962.

[4] C. P. Milies and S. K. Sehgal, *An Introduction to Group Rings*, Kluwer Academic Publishers, Dodrecht, 2002.

[5] E. Goodaire, E. Jespers and C. P. Milies, *Alternative Loop Rings*, North-Holland Math. Studies, vol. 184, Elsevier, Amsterdam, 1996.

[6] E. Jespers, G. Leal and C. P. Milies, *Units of integral group rings of some metacyclic groups*, Canad. Math. Bull. **37**,2 (1994), 228-237.

[7] F. J. MacWilliams, *Codes and ideals in group algebras*, in C. R. Bose and T. A. Dowling (eds) Proc. of Conf. on Combinatorial Mathematics and Its Applications, 1967, N. C. Chapel Hill: U. of N. C. Press, 1969.

[8] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correting codes*, New York, North-Holland, 1977.

[9] F. S. Dutra, *Sobre Códigos Diedrais e Quatérnios*, Tese de Doutoramento, ICEX-UFMG, Belo Horizonte, 2006.

[10] G. James and M. Liebeck, *Representations and characters of groups*, Cambridge University Press, 1993.

[11] H. Domingues e G. Iezzi, *Álgebra Moderna*, Editora Atual, São Paulo, 2003.

[12] I. M. Isaacs, *Character Theory of Finite Groups*, Dover Publications, New York, 1976.

[13] J.-P. Serre, *Linear representations of finite groups*, Springer, Berlin, Heidelberg, New York, 1977.

[14] P. A. Martin, *Introdução à Teoria dos Grupos e à Teoria de Galois*, IME-USP, São Paulo, 1998.

[15] P. Piret, *Good block codes derived from cyclic codes*, Electronics Lettes **10** (1974), 391-392.

[16] R. E. Sabin and S. J. Lomonaco, *Metacyclic error-correcting codes*, AAECC **6** (1995), 191-210.

[17] R. A. Ferraz, *Simple components and central units in group algebras*, Journal of Algebra **279** (2004), 191-203.

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

[19] R. Keown, *An introduction to group representation theory*, Academic Press, New York, 1975.

[20] S. Perlis and G. Walker, *Abelian group algebras of finite order*, Trans. Amer. Math. Soc. **68** (1950), 420-426.

[21] V. O. Luchetta, *Códigos Cíclicos como ideais em álgebras de grupos*, Dissertação de Mestrado, IME-USP, São Paulo, 2005.

[22] Y. Cheng and N. J. A. Sloane, *Codes from symmetry groups, and a* $[32, 17, 8]$ *code*, SIAM J. Disc. Math. **2** (1989), 28-37.

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo