UNIVERSIDADE ESTADUAL DE MARINGÁ

CENTRO DE CIÊNCIAS EXATAS

DEPARTAMENTO DE MATEMÁTICA

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

(Mestrado)

Um estudo de códigos abelianos sobre anel de cadeia a partir de elementos idempotentes

Júlio Atílio Dias de Mattos

Orientadora: Profa. Dra. Fernanda Diniz de Melo Hernandez

Maringá - PR

2023

[1]O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001 e com apoio do Ministério da Ciência, Tecnologia e Inovação - Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq - Brasil (443685/2020-7)

Júlio Atílio Dias de Mattos

Um estudo de códigos abelianos sobre anel de cadeia a partir de elementos idempotentes

Dissertação apresentada ao Programa de Pós-Graduação em Matemática do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de concentração: Álgebra

Orientadora: Profa. Dra. Fernanda Diniz de Melo Hernandez

Maringá - PR

2023

Dados Internacionais de Catalogação na Publicação (CIP)
(Biblioteca Setorial BSE-DMA-UEM, Maringá, PR, Brasil)

M444e

Mattos, Júlio Atílio Dias de
Um estudo de códigos abelianos sobre anel de cadeia a partir de elementos idempotentes / Júlio Atílio Dias de Mattos. -- Maringá, 2023.
54 f. : il.

Orientadora: Profª. Drª. Fernanda Diniz de Melo Hernandez.
Dissertação (mestrado) - Universidade Estadual de Maringá, Centro de Ciências Exatas, Programa de Pós-Graduação em Matemática - Área de Concentração: Álgebra, 2023.

1. Idempotentes. 2. Anéis de grupo. 3. Anéis de cadeia. 4. Códigos cíclicos. 5. Códigos de grupos. 6. Complemento Dual. 7. Códigos LCD. I. Hernandez, Fernanda Diniz de Melo, orient. II. Universidade Estadual de Maringá. Centro de Ciências Exatas. Programa de Pós-Graduação em Matemática - Área de Concentração: Álgebra. III. Título.

CDD 22.ed. 512.2

Edilson Damasio CRB9-1.123

JÚLIO ATÍLIO DIAS DE MATTOS

UM ESTUDO DE CÓDIGOS ABELIANOS SOBRE ANEL DE CADEIA A PARTIR DE ELEMENTOS IDEMPOTENTES

Dissertação apresentada ao Programa de Pós-Graduação em Matemática do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática tendo a Comissão Julgadora composta pelos membros:

COMISSÃO JULGADORA:

Profa. Dra. Fernanda Diniz de Melo Hernandez - UEM (Presidente)
Prof. Dr. Raul Antonio Ferraz - IME / USP
Prof. Dr. Laerte Bemm - UEM

Aprovado em: 28 de agosto de 2023.
Local de defesa: Bloco F67 – Auditório do Departamento de Matemática.

Agradecimentos

Agradeço a Deus, por iluminar minha trajetória até aqui.

Aos meus pais, Ilse e Sergio, que me ensinaram a lutar pelos meus objetivos e sempre me ampararam nos momentos difíceis. Agradeço minha madrinha Ires que sempre me deu os melhores conselhos e muitos livros de álgebra.

À minha orientadora Profa. Dra. Fernanda Diniz de Melo Hernandez pela paciência, por sempre prezar pelo meu crescimento profissional e por ser uma grande amiga. Ao Prof. Dr. Cesar Adolfo Hernandez Melo pelas perguntas instigantes que sempre me fizeram pensar além.

Agradeço meu namorado Diogo, que esteve ao meu lado a todo momento e me amparou nos momentos de tristeza e frustração.

Aos meus amigos, que me fizeram rir nos dias tristes.

Aos professores Dr. Raul Antonio Ferraz e Dr. Laerte Bemm, por aceitarem o convite para participarem da banca e se disporem a ler meu trabalho.

Por fim, agradeço a CNPq pelo apoio financeiro, sem o qual esse trabalho não seria possível.

Resumo

Neste trabalho estudaremos um método para encontrar os elementos idempotentes de um anel comutativo R a partir dos elementos idempotentes do anel quociente $\frac{R}{N}$, onde N pertence a uma coleção de ideais satisfazendo certas hipóteses. O método citado, chamado de levantamento de idempotentes, servirá como ferramenta para encontrar os elementos idempotentes de um anel de grupo RG, onde R é um anel de cadeia finito comutativo com unidade e G é um grupo abeliano finito. Com os elementos idempotentes de RG e o gerador do ideal maximal de R caracterizaremos os códigos abelianos de tal anel de grupo e, tomando algumas hipóteses adicionais, exibiremos uma fórmula para determinar o peso de um código cíclico de comprimento p^n. Por fim, usaremos a teoria de elementos idempotentes para identificar os códigos LCD sobre uma álgebra de grupo RG, para o caso onde R é um anel comutativo com unidade arbitrário.

Palavras-chave: Idempotentes, Levantamento de Idempotentes, Anéis de Grupo, Anéis de Cadeia, Códigos, Códigos Cíclicos, Códigos de Grupos, Complemento Dual, LCD.

Abstract

In this work we will study a method to find the idempotent elements of a commutative ring R from the idempotent elements of the quotient ring $\frac{R}{N}$, where N belongs to a collection of ideals satisfying certain assumptions. The aforementioned method, called idempotent lifting, will be used as a tool to find the idempotent elements of a group ring RG, where R is a commutative finite chain ring with unity and G is a finite abelian group. With the idempotent elements of RG and the generator of the maximal ideal of R we will characterize the abelian codes of such a group ring and, taking some additional assumptions, we will obtain a formula to determine the weight of a cyclic code of length p^n. Finally, we will use the theory of idempotent elements to identify the LCD codes on a group algebra RG, for the case where R is an arbitrary commutative ring with unity.

Keywords: Idempotents, Idempotent lifting, Group Rings, Chain Ring, Codes, Cyclic Codes, Group Codes, Dual Complement, LCD.

Sumário

Introdução

O Matemático Benjamin Peirce foi o primeiro a introduzir os nomes "nilpotente"e "idempotente"em 1870, enquanto estudava álgebras comutativas. Também foi ele quem desenvolveu a Decomposição de Pierce de módulos semissimples. Desde então, os elementos idempotentes foram amplamente usados por diversas áreas de pesquisa além da matemática, dentre elas temos física e química teórica e economia. A Teoria de Informação não é exceção, principalmente na Teoria de Códigos Corretores de Erros, veja [1, 2, 7, 9, 14, 15, 23, 20].

Encontrar elementos idempotentes de um anel arbitrário pode ser uma tarefa difícil. Na tentativa de encontrar esses elementos desenvolveram-se diversos trabalhos que buscam idempotentes sob distintas condições. Como exemplo temos o trabalho de R. A. Ferraz e C. P. Milies [9] no qual encontraram uma família de idempotentes primitivos ortogonais das álgebras de grupo $\mathbb{F}_qG$, onde $\mathbb{F}_q$ é um corpo finito de q elementos e G é um p-grupo, em que q e p satisfazem certas hipóteses. Tal família de idempotentes primitivos ortogonais é determinada a partir do reticulado de subgrupos de G.

O objetivo deste trabalho é estudar o método desenvolvido por F. D. Melo Hernández, C. A. Hernández Melo e H. Tapia-Recillas em [19] para encontrar idempotentes de um anel comutativo R a partir de elementos idempotentes de um anel quociente $\frac{R}{N}$, onde N é um ideal próprio de uma família de ideais de R que satisfazem o que chamaremos de condição CNC. Tal método será chamado de Levantamento de Idempotentes e veremos como podemos aplicá-lo na Teoria de Códigos Corretores de Erros e estudar as propriedades que os códigos encontrados com esses idempotentes possuem.

O estudo dos códigos corretores de erros tiveram início na primeira metade do século XIX, com o matemático americano R. W. Hamming, enquanto trabalhava no *Bell Telephone Laboratories*. Naquela época, os computadores eram muito lentos e capazes apenas de detectar um erro e quando isso acontecia o computador parava de processar o

programa que executava, pois não era capaz de corrigi-lo, por isso muitos trabalhos eram perdidos. Empenhado em resolver tal problema, em 1950, Hamming publicou um artigo [10], onde ele descreve um código capaz de detectar dois erros e corrigir um, se for único.

Hamming seguiu se perguntando se poderia encontrar códigos melhores, mas foi um colega de trabalho, chamado C. E. Shannon, quem conseguiu encontrar tal código. Shannon publicou um artigo [24] em 1948, no qual descreveu um código mais eficiente e o atribuiu ao próprio Hamming. Tal trabalho possibilitou a criação de duas teorias amplamente estudadas atualmente, a **Teoria dos Códigos Corretores de Erros** e a **Teoria da Informação**.

A Teoria dos Códigos Corretores de Erros juntamente com suas aplicações torna a Matemática Pura e a Aplicada cada vez mais próximas. A fim de se obter uma teoria matemática de Códigos Corretores de Erros, os Códigos Lineares, os quais são a classe de códigos mais estudadas, foram inicialmente definidos como subespaços vetoriais de um espaço vetorial $\mathbb{F}^n$, onde $\mathbb{F}$ é um corpo finito e representa o alfabeto do código. Porém, trabalhos como [6, 11, 23], que estudam códigos lineares sobre $\mathbb{Z}_4$, tem motivado os estudo de códigos sobre anéis mais gerais.

Como uma extensão natural de $\mathbb{Z}_4$, A. R. Calderbank e N. J. A. Sloane, em [3], determinaram a estrutura de códigos cíclicos, os quais são uma classe de códigos lineares, sobre $\mathbb{Z}_{p^m}$, onde p é um número primo e $m \geq 1$. Em 1997, P. Kanwar e S. R. López-Permouth em [14], estudaram códigos cíclicos sobre $\mathbb{Z}_{p^m}$ do ponto de vista de anéis de polinômios. Mais tarde tais resultados foram estendidos para códigos cíclicos sobre anéis de Galois por Z. Wan em [26].

Tanto os anéis $\mathbb{Z}_{p^m}$ quanto os anéis de Galois, são exemplos de anéis de cadeia assim, em 1999, G. H. Norton e A. Sălăgean, em [22], estenderam os resultados de [3] e [14] para códigos sobre anéis de cadeia finitos. Mais recentemente, em 2004, H. Q. Dinh e S. R. López-Permouth em [8], demonstraram os mesmos resultados de [22] usando anéis de polinômios.

Em 2012, A. T. Silva, em [25] mostrou os mesmo resultados de [8] para códigos cíclicos, mas agora usando uma abordagem de anéis de grupo ao invés de usar a linguagem polinomial empregada por Dinh e López-Permouth. No presente, trabalho usaremos o levantamento de idempotentes e as mesmas técnicas que Silva usou em [25] para descrever os códigos abelianos sobre um anel de cadeia finito.

No primeiro capítulo deste trabalho veremos alguns conceitos que serão usados ao longo do texto. Iniciaremos relembrando alguns resultados da Teoria de Módulos Semissimples e Anéis de Grupos, definiremos Códigos Lineares e mostraremos que podemos ver os códigos como ideais de um anel de grupo e então enunciaremos resultados sobre Anéis de Cadeia.

No capítulo 2 veremos o método de levantamento de idempotentes. Iniciaremos com o resultado que nos motivou a buscar elementos idempotentes de um anel R a partir dos elementos idempotentes do anel quociente $\frac{R}{N}$, onde N é um ideal nil de R. Mostraremos que o processo de levantamento preserva propriedades dos idempotentes do quociente para o anel R. Quando R é comutativo podemos garantir a unicidade do idempotente levantado e exibir uma fórmula para determinar os idempotentes obtidos pelo levantamento. Ainda neste capítulo definiremos a condição CNC, que nos permitirá determinar os elementos idempotentes de R a partir de uma sequência de levantamentos passando por uma cadeia de homomorfismos de anéis. Encerraremos o capítulo determinando os idempotentes de um anel de grupo RG em que R possui uma coleção de ideais satisfazendo a condição CNC.

Com o Levantamento de Idempotentes como ferramenta, no terceiro capítulo, caracterizaremos os códigos abelianos sobre um anel de grupo RG, onde R é um anel de cadeia finito comutativo com unidade e G é um grupo abeliano finito, a partir dos idempotentes levantados e do gerador do ideal maximal de R. Tal caracterização nos permite determinar quantos códigos podemos obter no anel RG. O peso de um código é uma informação fundamental, pois com ele é possível determinar a capacidade de correção de erros de um código. Assim, após caracterizarmos os códigos sobre anéis de cadeia, poderemos calcular o peso de códigos cíclicos de comprimento p^n, onde p é um número primo. Para tal, consideraremos as hipóteses sobre a quantidade de elementos de R e p descritas em [9] por Ferraz e Milies. Nestas condições podemos determinar a cardinalidade de cada código cíclico.

Outra classe de códigos lineares são os códigos com complemento dual, conhecidos como código LCD. Tais códigos foram introduzidos por J. L. Massey em [16] no ano de 1992, onde foi mostrado que existem códigos LCD assintoticamente bons, ou seja, existem códigos LCD que atingem algumas das cotas que relaciona peso e dimensão dos códigos. Os códigos LCD tiveram uma aplicação recém-descoberta em criptografia, e assim o interesse em códigos desse tipo foi renovado. Em particular, foi demonstrado que

os códigos LCD binários desempenham um papel importante nas implementações contra problemas como "side-channel attacks"e "fault injection attacks", veja [4, 5].

Em 2018, J. de La Cruz e W. Willems, mostraram em [7] que os códigos de grupo LCD de $\mathbb{F}G$, onde $\mathbb{F}$ é corpo e G é um grupo finito, são gerados por certos elementos idempotentes. No Capítulo 4, baseado em [7], mostraremos que é possível estender os resultados de La Cruz e Willems para códigos LDC em RG, para o caso mais geral em que R é um anel comutativo com unidade. Por fim, caracterizaremos os códigos LCD determinados pelos elementos idempotentes estudados por Ferraz e Milies em [9] de um anel RG para o caso em que R é um anel de cadeia finito comutativo com unidade e G um grupo cíclico de ordem p^n.

Capítulo 1

Conceitos Preliminares

O objetivo deste trabalho é estudar formas de encontrar idempotentes de anéis comutativos. Aqui exibiremos alguns resultados que serão usados para o desenvolvimento da teoria. De forma geral, os resultados apresentados nesse capítulo não serão demonstrados, mas indicaremos a referência caso se faça necessária a consulta.

1.1 Módulos Semissimples e Anéis de Grupo

Definição 1.1.1. Seja R um anel. Um grupo abeliano M (aditivo) é chamado de **R-módulo** se para cada $a \in R$ e cada $m \in M$ temos $am \in M$ tal que:

1. $(a+b)m = am + bm$, $\forall a, b \in R,\ \forall m \in M$;
2. $a(m_1 + m_2) = am_1 + am_2$ $\forall a \in R,\ \forall m_1, m_2 \in M$;
3. $a(bm) = (ab)m$ $\forall a, b \in R,\ \forall m \in M$;
4. Se R tem unidade, então $1m = m$ $\forall m \in M$.

Sejam R é um anel comutativo com unidade e A um R-módulo. Dizemos que A é uma **R-álgebra** se tem uma multiplicação, definida em A tal que, com a adição de A e essa multiplicação, A seja um anel tal que a seguinte condição aconteça:

$$r(ab) = (ra)b = a(rb),$$

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

Definição 1.1.2. Seja M um módulo sobre R. Um subconjunto não vazio $N \subset M$ é chamado de R**-submódulo** de M se as seguintes condições acontecem:

1. Para todos $x, y \in N$, $x + y \in N$;

2. Para todo $r \in R$ e todo $n \in N$, $rn \in N$.

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

Definição 1.1.3. Um R-módulo M é chamado **semissimples** se todo submódulo de M for um somando direto.

Definição 1.1.4. Um anel R sempre é um módulo sobre si mesmo e quando R é um módulo semissimples então R é chamado de **anel semissimples**.

Teorema 1.1.5. [21] Seja R um anel. Então as condições a seguir são equivalentes:

1. Todo R-módulo é semissimples.

2. R é um anel semissimples

3. R é soma direta de um número finito de ideais minimais à esquerda.

Definição 1.1.6. Seja R um anel. Dizemos que um elemento $e \in R$ é **idempotente** se $e^2 = e$. Uma família de idempotentes $\{e_1, \ldots, e_t\}$ satisfazendo:

ii. Se $i \neq j$ então e_i e e_j são ortogonais, ou seja, $e_i e_j = 0$.

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

iv. e_i é primitivo, ou seja, não pode ser escrito como $e_i = e_i' + e_i''$, em que e_i', e_i'' são idempotentes tais que $e_i', e_i'' \neq 0$ e $e'e'' = 0$, com $1 \leq i \leq t$.

é chamado de família de **idempotentes ortogonais primitivos**.

Podemos usar idempotentes para caracterizar a decomposição de anéis semissimples como soma direta de ideais minimais à esquerda. Esta é chamada de decomposição de Peirce.

Teorema 1.1.7. [21] Seja $R = \oplus_{i=1}^{t} L_i$ uma decomposição de um anel R semissimples como soma direta de ideias minimais à esquerda. Então, existe uma família $\{e_1; \cdots ; e_t\}$ de elementos idempotentes ortogonais primitivos de R tais que $L_i = Re_i$, para todo $i = 1, 2, \ldots, t$. Reciprocamente, se exite uma família de elementos idempotentes ortogonais primitivos $\{e_1, \cdots , e_t\}$, então o ideal à esquerda $L_i = Re_i$ é minimal e $R = \oplus_{i=1}^{t} L_i$.

Neste trabalho usaremos ativamente os anéis de grupo e suas propriedades, aqui daremos algumas definições e resultados básicos. Em [21] essa estrutura é estudada com mais detalhes.

Definição 1.1.8. Sejam R um anel e G um grupo. O conjunto denotado por RG e formado pelas somas formais do tipo

$$\sum_{g \in G} x_g g,$$

onde $x_g \in R$ e $x_g = 0$ exceto para um número finito de índices $g \in G$, com as operações de soma e multiplicação definidas por:

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g;$$

$$\sum_{g \in G} a_g g \cdot \sum_{g \in G} b_g g = \sum_{g,h \in G} a_g b_h gh$$

é um anel. O anel RG é chamado de **anel de grupo** de G sobre R.

Denotando o elemento neutro do grupo G por 1_G. Considere o homomorfismo injetor de anéis $\nu : R \to RG$ dada por $\nu(r) = \sum_{g \in G} a_g g$, onde $a_{1_G} = r$ e $a_g = 0$ se $g \neq 1_G$. Com essa identificação podemos dizer que R é um subanel de RG. Geralmente escrevemos $\nu(r)$ apenas por r em RG. Assim, quando R possui unidade, denotada por 1_R, então RG também possui unidade dada por $1 = \nu(1_R)$.

Suponha R um anel com unidade. Podemos definir uma imersão $i : G \to RG$ atribuindo a cada elemento $x \in G$ o elemento $i(x) = \sum_{g \in G} a_g g$, onde $a_x = 1_R$ e $a_g = 0$ se $g \neq x$. Podemos, portanto, considerar G um subconjunto de RG. Para todo $g \in G$ denotamos $i(g)$ apenas por g.

O anel de grupo RG possui estrutura de R-módulo com a operação

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

Note que se R for comutativo segue que RG é uma álgebra sobre R chamada de **álgebra de grupo** de G sobre R. Considerando a imerção i, podemos dizer que G gera os elementos de RG, ou seja, G é uma base para RG. Quando $|G|$ é finito dizemos que RG tem dimensão $|G|$.

Definição 1.1.9. Dado um elemento $\alpha = \sum_{g\in G} a_g g$ de um anel de grupo RG. O **suporte** de α é o subconjunto de elementos de G que aparecem efetivamente na expressão de α, ou seja,

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

Proposição 1.1.10. Seja N é ideal de R, então $NG = \left\{\sum_{g\in G} n_g g \in RG;\ n_g \in N, \forall g \in G\right\}$ é ideal de RG, e mais

$$\frac{RG}{NG} \simeq \left(\frac{R}{N}\right) G.$$

Demonstração. Sejam $\sum_{g\in G} n_g g$ e $\sum_{g\in G} m_g g$ elementos de NG, uma vez que N é ideal de R, segue que $n_g - m_g \in N$, para todo $g \in G$, logo

$$\sum_{g\in G} n_g g - \sum_{g\in G} m_g g = \sum_{g\in G}(n_g - m_g)g\ \in NG.$$

Dado $\sum_{g\in G} a_g g \in RG$, temos

$$\sum_{g\in G} a_g g \cdot \sum_{g\in G} n_g g = \sum_{g,h\in G} a_g n_h gh \in NG,$$

e

$$\sum_{g\in G} n_g g \cdot \sum_{g\in G} a_g g = \sum_{g,h\in G} n_g a_h hg \in NG,$$

pois $a_g \in R$, para todo $g \in G$. Por fim, basta considerarmos o homomorfismo sobrejetor de anéis $f : RG \to \left(\frac{R}{N}\right) G$ definido por $f\left(a_g g\right) = (a_g + N)g$, cujo $Ker(f) = NG$. ■

Se H é subgrupo finito de G e R é um anel com unidade, podemos escrever

$$|H| = \underbrace{1 + 1 + \cdots + 1}_{|H|} \in RG.$$

E, caso $|H|$ seja inversível em RG, denotaremos por $\frac{1}{|H|}$ ou por $|H|^{-1}$ o inverso de $|H|$ em RG.

Proposição 1.1.11. Seja R um anel com unidade e H um subgrupo finito de um grupo G. Se $|H|$ é invertível em R, então

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

é um idempotente de RG.

Demonstração. Note que, como H é finito, então $h' \sum\limits_{h \in H} h = \sum\limits_{h \in H} h$ para qualquer $h' \in H$. Assim

$$\begin{aligned}
\widehat{H}^2 &= \left(\frac{1}{|H|} \sum_{h \in H} h \right)^2 \\
&= \frac{1}{|H|^2} \left(\sum_{h \in H} h \right) \left(\sum_{h \in H} h \right) \\
&= \frac{1}{|H|^2} |H| \sum_{h \in H} h \\
&= \frac{1}{|H|} \sum_{h \in H} h \\
&= \widehat{H}
\end{aligned}$$

■

Proposição 1.1.12. [21] Sejam R um anel com unidade e H um subgrupo normal de um grupo G. Se $|H|$ é inversível em R, então

$$RG\widehat{H} \simeq R\left(\frac{G}{H}\right).$$

Também é fácil ver que, se τ é uma transversal de H em G, então $\{tH \mid t \in \tau\}$ é uma

base de $RG\widehat{H}$. Daí, um elemento α em tal ideal é da forma

$$\alpha = \sum_{t\in\tau} \alpha_t t\widehat{H}, \quad \alpha_t \in R.$$

Agora, vejamos sob quais condições um anel de grupo é um anel semissimples.

Teorema 1.1.13. [21, Teorema de Maschke] Seja G um grupo. Então, o anel de grupo RG é semissimples se, e somente se, as seguintes condições são satisfeitas:

1. R é um anel semissimples.

2. G é finito.

3. $|G|$ é invertível em R.

O caso onde $R = \mathbb{K}$ é um corpo é um caso particular importante do Teorema de Maschke. Neste caso, $\mathbb{K}$ é sempre semissimples e $|G|$ é invertível em $\mathbb{K}$ se, e somente se, $|G| \neq 0$ em $\mathbb{K}$, ou seja, $char(\mathbb{K}) \nmid |G|$.

Corolário 1.1.14. [21] Seja G um grupo finito e seja $\mathbb{K}$ um corpo. Então, $\mathbb{K}G$ é semissimples se, e somente se, $char(\mathbb{K}) \nmid |G|$.

1.2 Códigos Lineares

Chamaremos um conjunto finito $\mathcal{A}$ de **alfabeto** e denotaremos o número de elementos de $\mathcal{A}$ por $|\mathcal{A}|$. Um **código corretor de erros** é um subconjunto próprio qualquer de $\mathcal{A}^n = \mathcal{A} \times \cdots \times \mathcal{A}$, para algum número natural n, em que seus elementos são chamados de **palavras**.

Dentre os vários tipos de códigos corretores de erros, os códigos lineares são os mais conhecidos e usados.

Considere R um anel finito com q elementos como alfabeto e o R-módulo R^n.

Definição 1.2.1. um **código linear** de comprimento n é um R-submódulo $\mathcal{C}$ de R^n. Podemos notar que se a dimensão do código $\mathcal{C}$ for k, então $|\mathcal{C}| = q^k$, ou seja, $\mathcal{C}$ tem q^k palavras.

Dadas duas palavras $u = (u_1, \ldots, u_n)$ e $v = (v_1, \ldots, v_n)$ do código $\mathcal{C}$ podemos definir a distância entre estas palavras sendo o número de coordenadas distintas de u e v. Em símbolos

$$d(u, v) = |\{i \ ; \ u_i \neq v_i, \ 1 \leq i \leq n\}|.$$

Essa distância é conhecida como **distância de Hamming**.

Um conceito muito importante da Teoria de Códigos é a **distância mínima** de um código $\mathcal{C}$ definida por

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

Definição 1.2.2. Dada uma palavra $u = (u_1, \ldots, u_n)$ de um código $\mathcal{C}$ definimos o seu **peso** sendo o número inteiro

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

O peso do código $\mathcal{C}$ é definido como

$$\omega(\mathcal{C}) = min\{\omega(u); \ u \in \mathcal{C} - \{0\}\}.$$

Temos que $d(u, v) = \omega(u - v)$, para quaisquer u e v em $\mathcal{C}$ e $d(\mathcal{C}) = \omega(\mathcal{C})$.

Dentre os códigos lineares a classe dos códigos cíclicos se destacam e mostram ser de grande utilidade, principalmente ao estudarmos codificação e decodificação quando tomamos o alfabeto como sendo um corpo finito (veja [12]).

Definição 1.2.3. Seja R um anel finito. Um código linear $\mathcal{C}$ de R^n é chamado de **código cíclico** se quando $(c_0, c_1, \ldots, c_{n-1})$ é uma palavra do código $\mathcal{C}$, então a palavra $(c_{n-1}, c_0, c_1, \ldots, c_{n-2})$, obtida a partir da troca cíclica de coordenadas $i \to i + 1$, tomada módulo n, também pertence a $\mathcal{C}$, ou seja,

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

1.3 Códigos Cíclicos em Anéis de Grupo

Nesta seção veremos que podemos estudar os códigos cíclicos como ideais de um anel de grupo sobre um grupo cíclico. Desta maneira, podemos estender estes conceitos para códigos sobre anéis de grupo sobre um grupo qualquer.

Tomando R um anel finito comutativo com unidade e C_n um grupo cíclico de ordem n gerado por a e considerando o anel de grupo RC_n, podemos definir o seguinte isomorfismo de R-módulos:

$$\begin{array}{rccc} \varphi: & R^n & \to & RC_n \\ & (c_0, c_1, \ldots, c_{n-1}) & \mapsto & \sum_{i=0}^{n-1} c_i a^i. \end{array}$$

Assim, sendo $\mathcal{C} \subset R^n$ um código cíclico, sabemos que se $c = (c_0, c_1, \ldots, c_{n-1})$ é uma palavra de $\mathcal{C}$ então $\overline{c} = (c_{n-1}, c_0, c_1, \ldots, c_{n-2})$ também está em $\mathcal{C}$. Com isso podemos observar que

$$\varphi(\overline{c}) = \sum_{i=0}^{n-1} c_i a^{i+1} = a \cdot \sum_{i=0}^{n-1} c_i a^i = a\varphi(c).$$

Logo, uma troca cíclica em R^n é equivalente a multiplicar pelo gerador de C_n em RC_n. E mais, $a^i\varphi(c) \in \varphi(\mathcal{C})$, para todo $i = 0, 1, \ldots, n-1$.

Proposição 1.3.1. Sejam $\mathcal{C} \subset R^n$ um código linear e C_n um grupo cíclico de ordem n gerado por a. Então $\mathcal{C}$ é um código cíclico se, e somente se, $\varphi(\mathcal{C})$ é um ideal de RC_n.

Demonstração. Seja $\mathcal{C}$ um código cíclico de R^n, então para todo $c \in \mathcal{C}$ temos que $\overline{c} \in \mathcal{C}$, onde $\overline{c}$ denota a palavra obtida pela troca cíclica das coordenadas de c. Logo, $\varphi(c) \in \varphi(\mathcal{C})$ e $a\varphi(c) = \varphi(\overline{c}) \in \varphi(\mathcal{C})$. Agora, como $\mathcal{C}$ é submódulo, para quaisquer $\varphi(x), \varphi(y) \in \varphi(\mathcal{C})$ temos $\varphi(x) - \varphi(y) = \varphi(x-y) \in \varphi(\mathcal{C})$, pois $x, y \in \mathcal{C}$, logo $x - y \in \mathcal{C}$. Seja $\sum_{i=0}^{n-1} h_i a^i \in RC_n$, logo

$$\begin{aligned} \sum_{i=0}^{n-1} h_i a^i \cdot \varphi(x) &= h_0 a^0 \varphi(x) + h_1 a^1 \varphi(x) + \cdots + h_{n-1} a^{n-1} \varphi(x) \\ &= a^0 \varphi(h_0 x) + a^1 \varphi(h_1 x) + \cdots + a^{n-1} \varphi(h_{n-1} x). \end{aligned}$$

Como, para todo $i = 0, 1, \ldots, n-1$, temos $h_i \in R$ e $\mathcal{C}$ é fechado para a multiplicação por escalar, temos que $h_i x \in \mathcal{C}$, logo $\varphi(h_i x) \in \varphi(\mathcal{C})$. Assim, $a^i\varphi(h_i x) \in \varphi(\mathcal{C})$, para todo $i = 0, 1, \ldots, n-1$. Portanto $\sum_{i=0}^{n-1} h_i a^i \cdot \varphi(x) \in \varphi(\mathcal{C})$, o que mostra que $\varphi(\mathcal{C})$ é ideal de RC_n.

Reciprocamente, suponha que $\varphi(\mathcal{C})$ é ideal de RC_n. Tomando $a = 1_R a \in RC_n$, temos que $a\varphi(c) \in \varphi(\mathcal{C})$, para todo $c \in \mathcal{C}$. Seja $x \in \mathcal{C}$. Denotando por $\overline{x} \in R^n$ a palavra obtida pela troca cíclica das coordenadas de x, temos que $\varphi(\overline{x}) = a\varphi(x)$. Logo, $\overline{x} = \varphi^{-1}(a\varphi(x)) \in \mathcal{C}$, pois $a\varphi(x) \in \varphi(\mathcal{C})$. Portanto $\mathcal{C}$ é um código cíclico. ■

Devido a essa equivalência, é comum dizermos que um código cíclico $\mathcal{C}$ é um ideal de anel de grupo RC_n.

Inspirado nessa caracterização temos a seguinte definição.

Definição 1.3.2. Seja R um anel e G um grupo. Um subconjunto $\mathcal{C}$ de RG é dito ser um **código de grupo à direita (esquerda)** se $\mathcal{C}$ é um ideal à direita (esquerda) de RG. Se $\mathcal{C}$ é um ideal de RG, então é chamado de **código de grupo**. Quando G é abeliano, o código de grupo $\mathcal{C}$ é chamado de **código abeliano**.

Observação 1.3.3. Pela definição anterior, temos que todo código cíclico é um código abeliano.

Observação 1.3.4. Podemos adaptar a distância de Hamming para anéis de grupo, basta notar que dados $\alpha, \beta \in RG$, então $d(\alpha, \beta) = |supp(\alpha - \beta)|$. Desta forma, o peso de α é dado por $\omega(\alpha) = |supp(\alpha)|$ e se $\mathcal{C}$ é um código de grupo de RG, então

$$\omega(\mathcal{C}) = min\{\omega(\alpha);\ \alpha \in \mathcal{C} - \{0\}\}.$$

1.4 Anéis de Cadeia

Definição 1.4.1. Um anel R é dito **anel de cadeia** se o conjunto de todos os seus ideais formam uma cadeia sob a inclusão.

Definição 1.4.2. Um anel R é chamado de **anel local** se possui um único ideal maximal.

Proposição 1.4.3. [8] Seja R um anel comutativo finito com unidade. As seguintes afirmações são equivalentes:

1. R é um anel local e o ideal maximal M de R é principal.
2. R é um anel local de ideais principais.
3. R é um anel de cadeia.

Observação 1.4.4. Seja R é um anel de cadeia finito comutativo com unidade e denote por $M = \langle a \rangle$ o ideal maximal de R gerado por a. Então a é um elemento nilpotente e denotemos seu índice de nilpotência por t. Assim os ideais de R formam a cadeia

$$R = \langle a^0 \rangle \supsetneq \langle a^1 \rangle \supsetneq \cdots \supsetneq \langle a^{t-1} \rangle \supsetneq \langle a^t \rangle = 0.$$

Proposição 1.4.5. [17] Sejam R um anel de cadeia finito e comutativo com unidade, com ideal maximal $M = \langle a \rangle$, t o índice de nilpotência de a em R e $\overline{R} = \frac{R}{M}$. Então:

1. Para algum primo q e inteiros positivos k e l, tais que $k \geq l$, temos $|R| = q^k$, $|\overline{R}| = q^l$ e as características de R e $\overline{R}$ são potencias de q.

2. Para $i = 0, 1, \ldots, t$ temos $|\langle a^i \rangle| = |\overline{R}|^{t-i}$. Em particular, $|R| = |\overline{R}|^t$, ou seja, $k = lt$.

Proposição 1.4.6. [17] Seja e um idempotente não nulo de um anel R. As seguintes condições são equivalentes:

1. e é primitivo.

2. eRe é um anel local.

3. Re é indecomponível.

Como consequência direta da última proposição temos o seguinte corolário:

Corolário 1.4.7. Sejam R um anel comutativo e G um grupo comutativo. Seja e é um idempotente da álgebra de grupo RG. São equivalentes:

1. e é primitivo.

2. RGe é um anel local.

3. RGe é indecomponível.

Capítulo 2

Idempotentes de Anéis Comutativo

Neste capítulo estudaremos alguns resultados apresentados em [19]. Veremos como obter os elementos idempotentes de um anel R a partir dos idempotentes do anel quociente $\frac{R}{N}$, onde N é um ideal nil de R, através de um processo aqui chamado de levantamento de idempotentes. Destacaremos o caso em que R é um anel comutativo, onde podemos garantir a unicidade dos idempotentes levantados.

Aqui definiremos quando uma coleção de ideais de um anel comutativo satisfaz a condição CNC. Com essa caracterização, quando um anel comutativo R possuir uma coleção de ideais $\{N_1, N_2, \ldots, N_k\}$ satisfazendo tal condição, poderemos obter os elementos idempotentes de R a partir de uma série de levantamentos desde o anel $\frac{R}{N_1}$ até chegarmos novamente no anel R.

Por fim, veremos como obter os idempotentes de um anel de grupo RG, onde R é anel comutativo que possui uma coleção de ideais satisfazendo a condição CNC e G é um grupo comutativo.

2.1 Levantamento de Idempotentes

O primeiro resultado dessa seção é o que nos motiva a buscar os idempotentes de um anel quociente e tentar, a partir destes, encontrar os idempotentes do anel quocientado. Esta proposição se encontra em [13, Proposição 7.14], e partir dele nos é permitido estudar as propriedades preservadas ao levantarmos os idempotentes.

Lembrando que um ideal nil N de um anel R é um ideal em que todos os seus elementos são nilpotentes, ou seja, se $a \in N$, então existe um inteiro positivo t tal que $a^t = 0$.

Proposição 2.1.1. Sejam R um anel com unidade, N um ideal nil de R e $\overline{f} = f + N$ um elemento idempotente do anel quociente $\frac{R}{N}$. Então existe um elemento idempotente e em R tal que $\overline{e} = \overline{f}$ em $\frac{R}{N}$. Além disso, se R for comutativo, então e é único.

Demonstração. Sendo $\overline{f}$ idempotente em $\frac{R}{N}$, então $\overline{f} = \overline{f}^2$ se, e somente se, $\overline{f - f^2} = \overline{0}$ logo $f - f^2 \in N$. Como N é um ideal nil, então existe um inteiro positivo n tal que $(f - f^2)^n = 0$. Assim, se tomarmos $g = 1 - f$ teremos que $(fg)^n = (f - f^2)^n = 0$ e $fg = f(1-f) = f - f^2 = (1-f)f = gf$. Logo $0 = (fg)^n = f^n g^n$. Agora, como $1 = f + g$ segue que

$$1 = 1^{2n+1} = (f+g)^{2n+1} = h + e,$$

onde

$$h = \sum_{i=0}^{n-1} \binom{2n-1}{i} f^i g^{2n-1-i} \quad \text{e} \quad e = \sum_{i=n}^{2n-1} \binom{2n-1}{i} f^i g^{2n-1-i}$$

Como $f^n g^n = 0$ e pelo que já vimos f comuta com g então $eh = he = 0$. Com isso e do fato de $h + e = 1$, temos

$$e = e1 = e(h+e) = eh + e^2 = e^2$$
$$h = h1 = h(h+e) = h^2 + he = h^2.$$

Logo h e e são elementos idempotentes de R. Além disso, como $fg \in N$ e

$$e = \sum_{i=n}^{2n-2} \binom{2n-1}{i} f^i g^{2n-1-i} + \underbrace{\binom{2n-1}{2n-1}}_{1} f^{2n-1} \underbrace{g^0}_{1}$$
$$\Leftrightarrow e - f^{2n-1} = \sum_{i=n}^{2n-2} \binom{2n-1}{i} f^i g^{2n-1-i},$$

então $e - f^{2n-1} \in N$. Assim $e \equiv f^{2n-1} \bmod N$. E mais, como

$$f \equiv f^2 \equiv \cdots \equiv f^{2n-1} \bmod N,$$

então $e \equiv f \bmod N$, ou ainda, $\overline{e} = \overline{f}$.

Por fim, assumindo que R é um anel comutativo, vamos mostrar que e é único elemento idempotente de R tal que $\overline{e} = \overline{f}$. De fato, suponha que existe $x \in R$ um idempotente tal que $x \equiv f \equiv e \bmod N$, então $x - e = z \in N$, ou seja, z é nilpotente com índice de

nilpotência t e $x = e + z$. Note que,

$$e + z = (e + z)^2 = e^2 + 2ez + z^2 = e + 2ez + z^2$$
$$\Rightarrow z^2 = (1 - 2e)z.$$

Disso temos que $z^3 = (1-2e)z^2 = (1-2e)^2 z$. Por indução, obtemos que $z^n = (1-2e)^{n-1}z$. Sendo $(1 - 2e)^2 = 1 - 4e + 4e = 1$, segue que $z^n = (1 - 2e)^{n-1}z = z$ para todo inteiro positivo n. Como $z^t = 0$, segue que $z = 0$. Portanto $x = e$. ■

Definição 2.1.2. Seja R um anel comutativo com unidade e N um ideal nil de R. Dado um elemento idempotente $\overline{f}$ de $\frac{R}{N}$, chamaremos o elemento e de R, unicamente determinado na Proposição 2.1.1, de **idempotente levantado** de $\overline{f}$.

Observação 2.1.3. As observações a seguir são consequências diretas da Proposição 2.1.1 quando R é comutativo.

1. Se $\overline{f}$ e $\overline{h}$ são idempotentes ortogonais de $\frac{R}{N}$ então os respectivos idempotentes levantados e e k de R também são ortogonais. De fato, sendo $(ek)^2 = e^2k^2 = ek$ segue que ek é idempotente de R. Agora, como $\overline{f} = \overline{e}$ e $\overline{h} = \overline{k}$ então $\overline{ek} = \overline{fh} = \overline{0}$, logo $ek \in N$. Uma vez que ek é um idempotente em um ideal nil N, então $ek = 0$.

2. Se $\overline{f}$ é um idempotente primitivo, então o idempotente levantado e também é primitivo em R. De fato, suponha que existem idempotentes ortogonais $g, h \in R$ tais que $e = g + h$. Assim temos $\overline{f} = \overline{e} = \overline{g} + \overline{h}$, com $\overline{g}$ e $\overline{h}$ idempotentes ortogonais em $\frac{R}{N}$, pois $\overline{g}\overline{h} = \overline{gh} = \overline{0}$. Como $\overline{f}$ é primitivo, então $\overline{g} = \overline{0}$ ou $\overline{h} = \overline{0}$, isto é, $g \in N$ ou $h \in N$ e, desde que N é ideal nil, segue que $g = 0$ ou $h = 0$.

3. Da afirmação anterior segue que se $\{\overline{f_1}, \overline{f_2}, \ldots, \overline{f_r}\}$ é um conjunto de idempotentes ortogonais primitivos de $\frac{R}{N}$, então o conjunto correspondente $\{e_1, e_2, \ldots, e_r\}$ de idempotentes levantados de R tem as mesmas propriedades.

4. Denotaremos por $E(R)$ o conjunto dos idempotentes do anel comutativo R. Assumindo as hipóteses da Proposição 2.1.1 segue que

$$|E(R)| = \left|E\left(\frac{R}{N}\right)\right|.$$

De fato, tome o homomorfismo canônico $\varphi : R \to \frac{R}{N}$. Temos que $\varphi|_{E(R)}$ é uma bijeção de $E(R)$ em $E\left(\frac{R}{N}\right)$, pois da Proposição 2.1.1, dado $\overline{f} \in E\left(\frac{R}{N}\right)$ existe $e \in E(R)$ tal que $\overline{e} = \overline{f}$. Assim $\varphi|_{E(R)}(e) = \overline{e} = \overline{f}$. Logo $\varphi|_{E(R)}$ é sobrejetora. Com R é comutativo, se $f \in E\left(\frac{R}{N}\right)$ então existe um único idempotente $e \in E(R)$ levantado de $\overline{f}$. Donde segue a injetividade.

Dado um inteiro positivo z e um conjunto não vazio A, denotaremos por zA o conjunto dos elementos da forma $za = \underbrace{a + a + \cdots + a}_{z}$, para cada $a \in A$.

No que segue, veremos maneiras de como calcular os idempotentes levantados de um anel comutativo.

Proposição 2.1.4. Seja R um anel comutativo com unidade e N um ideal nilpotente de índice $t \geq 2$ em R. Se $\overline{f}$ é um elemento idempotente do anel quociente $\frac{R}{N}$ e e é o idempotente levantado correspondente a $\overline{f}$ em R, então:

1. Para qualquer número primo $p \geq t$ e para todo $n \in N$ existe $r \in R$ tal que

$$(e + n)^p = e + pnr.$$

2. Se existir um natural $s > 1$ tal que $sN = 0$, e todos os fatores primos do número s são maiores ou iguais que o índice de nilpotência t do ideal N, então

$$e = f^s.$$

3. Em particular, quando o índice de nilpotência $t = 2$ e $sN = 0$ para algum $s \geq 2$, então $e = f^s$.

Demonstração. 1. Seja p um número primo maior ou igual que t e sabendo que $n^j = 0$ para todo $n \in N$ e $j \geq t$ temos

$$\begin{aligned}(e + n)^p &= \sum_{j=0}^{p} \binom{p}{j} e^{p-j} n^j \\ &= \binom{p}{0} e^P n^0 + \sum_{j=1}^{t-1} \binom{p}{j} e^{p-j} n^j \\ &= e + \sum_{j=1}^{t-1} \binom{p}{j} e n^j.\end{aligned}$$

Como p é primo, temos que p divide $\binom{p}{j} = \frac{p!}{(p-j)!j!}$, para todo $1 \leq j \leq p-1$, e como $t \leq p$, então

$$(e+n)^p = e + pn(k_1 e + k_2 en + \cdots + k_{t-1} en^{t-2}),$$

onde $k_j = \binom{p}{j}/p$. Escrevendo $r = k_1 e + k_2 en + \cdots + k_{t-1} en^{t-2} \in R$, temos enfim que

$$(e+n)^p = e + pnr.$$

2. Seja $s = p_1 p_2 \ldots p_m$ a decomposição em primos do natural s. Desde que $\overline{f} = \overline{e}$, então $f = e + n$, para algum $n \in N$. Como $p_1 \geq t$, do item 1 segue que existe $r_1 \in R$ tal que

$$f^{p_1} = (e+n)^{p_1} = e + p_1 nr_1.$$

Da mesma maneira, como $p_2 \geq t$ e $p_1 nr_1 \in N$, pois N é um ideal, então existe $r_2 \in R$ tal que

$$f^{p_1 p_2} = (f^{p_1})^{p_2} = (e + p_1 nr_1)^{p_2} = e + p_2(p_1 nr_1)r_2.$$

Seguindo o mesmo raciocínio para $p_3, p_4, \ldots, p_m$, existem $r_3, r_4, \ldots, r_m \in R$ tais que

$$f^{p_1 p_2 \cdots p_m} = e + (p_1 p_2 \cdots p_m) n (r_1 r_2 \cdots r_m)$$
$$\Leftrightarrow f^s = e + sh,$$

onde $h = nr_1 r_2 \ldots r_m \in N$. Por hipótese, $sN = 0$, logo $sh = 0$. Portanto $f^s = e$.

3. Todo primo da decomposição de s é maior ou igual a $t = 2$. Assim, pelo item 2, segue que $e = f^s$.

■

Relembrando que dado um ideal N de um anel R e $k > 1$, N^k denota o ideal gerado por todos os produtos da forma $x_1 x_2 \ldots x_k$, onde cada $x_i \in N, \forall i = 1, 2, \ldots, k$.

Definição 2.1.5. Dizemos que a coleção $\mathcal{N} = \{N_1, N_2, \ldots, N_k\}$ de ideais de um anel comutativo R satisfaz a uma **condição CNC** se:

1. **Condição de cadeia:** Os ideais de $\mathcal{N}$ formam uma cadeia como a seguir:

$$\{0\} = N_k \subset N_{k-1} \subset \cdots \subset N_2 \subset N_1.$$

2. **Condição de nilpotência:** Para cada $i = 1, 2, \ldots, k-1$, existe um inteiro positivo $t_i \geq 2$ tal que $N_i^{t_i} \subset N_{i+1}$.

3. **Condição característica:** Para $i = 1, 2, \ldots, k-1$ existe um inteiro $s_i \geq 1$ tal que $s_i N_i \subset N_{i+1}$. E mais, os fatores primos de s_i são maiores ou iguais que t_i.

Chamaremos o menor inteiro t_i que satisfaz a condição de nilpotência de **índice de nilpotência** do ideal N_i no ideal N_{i+1}. O menor inteiro s_i que satisfaz a condição característica será chamado de **característica** de N_i em N_{i+1}.

As condições de nilpotência e característica podem ser lidas como segue:

Proposição 2.1.6. Sejam R um anel comutativo e $\mathcal{N} = \{N_1, N_2, \ldots, N_k\}$ uma família de ideais de R que satisfaz a condição de cadeia.

1. A condição de nilpotência acontece se, e somente se, para $i = 1, 2, \ldots, k-1$ o quociente $\frac{N_i}{N_{i+1}}$ é um ideal nilpotente de índice t_i do anel $\frac{R}{N_{i+1}}$.

2. A condição característica ocorre se, e somente se, para cada $i = 1, 2, \ldots, k-1$ existir um número natural $s_i \geq 1$ tal que $s_i\left(\frac{N_i}{N_{i+1}}\right) = 0$ no anel $\frac{R}{N_{i+1}}$.

Demonstração. Vejamos:

1. Para quaisquer t_i elementos $n_1, n_2, \ldots, n_{t_i} \in N_i$ temos que $n_1 n_2 \cdots n_{t_i} \in N^{t_i} \subset N_{i+1}$ se, e somente se,

$$0 + N_{i+1} = n_1 n_2 \cdots n_{t_i} + N_{i+1} = (n_1 + N_{i+1})(n_2 + N_{i+1}) \cdots (n_{t_i} + N_{i+1})$$

   se, e somente se, $\frac{N_i}{N_{i+1}}$ é um ideal nilpotente de índice t_i do anel $\frac{R}{N_{i+1}}$.

2. Basta notar que $s_i n \in s_i N_i \subset N_{i+1}$, para todo $n \in N_i$ se, e somente se, $s_i(n + N_{i+1}) = s_i n + N_{i+1} = 0 + N_{i+1}$ se, e somente se, $s_i\left(\frac{N_i}{N_{i+1}}\right) = 0$.

■

Sempre que tivermos um ideal nilpotente de um anel comutativo com unidade teremos uma coleção de ideais que satisfaz a condição CNC.

Lema 2.1.7. Seja R um anel comutativo com unidade. Seja N um ideal nilpotente de R com índice k e seja $s > 1$ a característica do anel quociente $\frac{R}{N}$. Então a coleção de ideais $\mathcal{N} = \{N, N^2, \ldots, N^k\}$ de R, formada pelas potências do ideal N, satisfaz a condição CNC.

Demonstração. Uma vez que $N \supset N^2 \supset \cdots \supset N^k = 0$, então a condição de cadeia é satisfeita. Como $i + 1 \leq 2i$, para todo $i = 1, 2, \ldots, k-1$, segue que $(N^i)^2 = N^{2i} \subset N^{i+1}$. Portanto $\mathcal{N}$ satisfaz a condição de nilpotência e o índice de nilpotência de N^{i+1} em N^i é igual a 2, para todo $i = 1, 2, \ldots, k-1$. Agora, sendo s a característica do anel $\frac{R}{N}$, então $s(1_R + N) = 0 + N$, ou seja, $s = s1_R \in N$. Assim, $sN^i = nN^i \subset N^{i+1}$, onde $n = s1_R \in N$. E concluímos que a característica de N^{i+1} em N^i é s, para todo $i = 1, 2, \ldots\ k-1$. Por fim, como $s \geq 2$, então os primos da sua fatoração são todos maiores ou iguais a 2. Portanto $\mathcal{N}$ é uma coleção de ideais de R que satisfazem a condição CNC. ■

Veremos a seguir que, desde que tenhamos uma coleção finita de ideais de um anel comutativo R, que satisfazem a Definição 2.1.5, podemos determinar os idempotentes de R a partir de repetidos levantamentos.

Teorema 2.1.8. Sejam R um anel comutativo e $\mathcal{N} = \{N_1, N_2, \ldots, N_k\}$ uma coleção de ideais de R que satisfazem a condição CNC, onde s_i e t_i são a característica e o índice de nilpotência do ideal N_i no ideal N_{i+1}, respectivamente. Se $f + N_1$ é um idempotente do anel $\frac{R}{N_1}$, então

$$f^{s_1 s_2 \cdots s_{k-1}}$$

é um idempotente do anel R. Além disso, $|E(R)| = |E\left(\frac{R}{N_{k-1}}\right)| = \cdots = |E\left(\frac{R}{N_1}\right)|$.

Demonstração. Como $N_{i+1} \subset N_i$, faz sentido olharmos para o anel $\frac{N_i}{N_{i+1}}$. Seja $f + N_1$ é um idempotente no anel

$$\frac{R}{N_1} \simeq \frac{R/N_2}{N_1/N_2}.$$

Então $(f + N_2) + \frac{N_1}{N_2}$ é um elemento idempotente de anel $\frac{R/N_2}{N_1/N_2}$. Desde que a coleção $\mathcal{N}$ satisfaz a condição CNC, temos que $N_1^{t_1} \subset N_2$. Logo, $\frac{N_1}{N_2}$ é um ideal nilpotente de índice t_1 no anel $\frac{R}{N_2}$, e mais, como $s_1 N_1 \subset N_2$, então $s_1\left(\frac{N_1}{N_2}\right) = 0$ e $s_1 \geq t_1$, pois os fatores primos

de s_1 são todos maiores ou iguais que t_1. Logo do item 2 da Proposição 2.1.4, segue que $f^{s_1} + N_2$ é um idempotente do anel $\frac{R}{N_2}$.

De maneira análoga, uma vez que

$$\frac{R}{N_2} \simeq \frac{R/N_3}{N_2/N_3}$$

temos que $(f^{s_1} + N_3) + \frac{N_2}{N_3}$ é um idempotente do anel $\frac{R/N_3}{N_2/N_3}$. Sendo $\frac{N_2}{N_3}$ um ideal nilpotente de índice t_2 de $\frac{R}{N_3}$, $s_2\left(\frac{N_1}{N_2}\right) = 0$ e $s_2 \geq t_2$, segue que $f^{s_1 s_2} + N_3$ é um idempotente de $\frac{R}{N_3}$.

Continuando com esse processo, como

$$\frac{R}{N_i} \simeq \frac{R/N_{i+1}}{N_i/N_{i+1}} \tag{2.1}$$

teremos que $f^{s_1 s_2 \cdots s_i} + N_{i+1}$ é um idempotente do anel $\frac{R}{N_{i+1}}$. Finalmente, como $N_k = 0$, temos que $f^{s_1 s_2 \cdots s_{k-1}} + N_k = f^{s_1 s_2 \cdots s_{k-1}}$ é um idempotente de $\frac{R}{N_k} = R$.

Considere a restrição do isomorfismo dado em (2.1) ao conjunto de idempotentes do anel $\frac{R}{N_i}$. Como para cada idempotente em $E\left(\frac{R/N_{i+1}}{N_i/N_{i+1}}\right)$ existe um único idempotente correspondente em $E\left(\frac{R}{N_i}\right)$, então a restrição é uma bijeção entre $E\left(\frac{R}{N_i}\right)$ e $E\left(\frac{R/N_{i+1}}{N_i/N_{i+1}}\right)$. Portanto

$$\left|E\left(\frac{R}{N_i}\right)\right| = \left|E\left(\frac{R/N_{i+1}}{N_i/N_{i+1}}\right)\right|, \quad \forall i = 1, 2, \ldots, k-1.$$

Agora, uma vez que $\mathcal{N}$ satisfaz a condição CNC, temos da Proposição 2.1.6 que $\frac{N_i}{N_i+1}$ é um ideal nilpotente de índice t_i em $\frac{R}{N_{i+1}}$ e como R é comutativo, da Observação 2.1.3, segue que

$$\left|E\left(\frac{R/N_{i+1}}{N_i/N_{i+1}}\right)\right| = \left|E\left(\frac{R}{N_{i+1}}\right)\right|.$$

Portanto $\left|E\left(\frac{R}{N_i}\right)\right| = \left|E\left(\frac{R}{N_{i+1}}\right)\right|$, para todo $i = 1, 2, \ldots, k-1$. ■

Desta forma podemos concluir que se tomarmos uma coleção de ideais $\mathcal{N} = \{N_1, N_2, \ldots, N_k\}$ de um anel comutativo R, que satisfaz a condição CNC, qualquer elemento idempotente $f + N_1$ do anel $\frac{R}{N_1}$ é levantado para o idempotente $f^{s_1} + N_2$ do anel $\frac{R}{N_2}$. Por sua vez, esse novo idempotente é levantado no idempotente $f^{s_1 s_2} + N_3$ do anel $\frac{R}{N_3}$, e assim por diante. No final desse processo obteremos o elemento idempotente $f^{s_1 s_2 \cdots s_{k-1}}$ de R.

Considere a cadeia de homomorfismos

$$R = \frac{R}{N_k} \overset{\phi_{k-1}}{\to} \frac{R}{N_{k-1}} \overset{\phi_{k-2}}{\to} \cdots \overset{\phi_3}{\to} \frac{R}{N_3} \overset{\phi_2}{\to} \frac{R}{N_2} \overset{\phi_1}{\to} \frac{R}{N_1}$$

onde $\phi_i(x + N_{i+1}) = x + N_i$, para todo $i = 1, 2, \ldots, k-1$. Vimos na demonstração do Teorema 2.1.8 que cada homomorfismo ϕ_i desta cadeia induz uma bijeção quando restrito ao conjunto de idempotentes $E\left(\frac{R}{N_{i+1}}\right)$ em $E\left(\frac{R}{N_i}\right)$, para todo $i = 1, 2, \ldots, k-1$.

Assim, para determinar os elementos idempotentes de R, é suficiente que tenhamos uma coleção $\mathcal{N} = \{N_1, N_2, \ldots, N_k\}$ de ideais de R que satisfazem a condição CNC e que saibamos todos os idempotentes do anel quociente $\frac{R}{N_1}$. Desta forma temos que o conjunto de idempotentes de R pode ser dado por:

$$E(R) = \left\{ f^{s_1 s_2 \cdots s_{k-1}};\ \ \overline{f} \in E\left(\frac{R}{N_1}\right) \right\}$$

2.2 Idempotentes em Anéis de Grupo Comutativos

Vejamos como determinar os idempotentes de um anel de grupo RG, onde R é um anel comutativo que possui uma coleção de ideais que satisfazem a condição CNC e G é um grupo comutativo, usando os resultados estudados anteriormente.

Proposição 2.2.1. Seja R um anel comutativo com unidade e seja G um grupo comutativo. Seja $\mathcal{N} = \{N_1, N_2, \ldots, N_k\}$ uma coleção de ideais de R satisfazendo a condição CNC. Se $f + N_1 G$ é um idempotente do anel de grupo $\left(\frac{R}{N_1}\right) G$, então

$$f^{s_1 s_2 \cdots s_{k-1}}$$

é um idempotente do anel de grupo RG. Além disso, $|E(RG)| = \left|E\left(\left(\frac{R}{N_1}\right) G\right)\right|$.

Demonstração. Primeiro, mostremos que $\mathcal{B} = \{N_1 G, N_2 G, \ldots, N_k G\}$ é uma coleção de ideais de RG que satisfaz a condição CNC. De fato, como $N_i \subset N_{i+1}$, para todo $i = 1, 2, \ldots, k-1$, claramente temos $N_i G \subset N_{i+1} G$, para todo $i = 1, 2, \ldots, k-1$. Logo a condição de cadeia é satisfeita. Seja t_i o índice de nilpotência de N_i em N_{i+1}, então $N_i^{t_i} \subset N_{i+1}$, o que implica que $N_i^{t_i} G \subset N_{i+1} G$. Agora note que

$$\alpha \in (N_i G)^{t_i} \Leftrightarrow \alpha = \sum_{g_1 \in G} n_{g_1} g_1 \sum_{g_2 \in G} n_{g_2} g_2 \cdots \sum_{g_{t_i} \in G} n_{g_{t_i}} g_{t_i} = \sum_{g \in G} n_g g \ \in N_i^{t_i} G,$$

onde $n_g = n_{g_1} n_{g_2} \cdots n_{g_{t_i}} \in N_i^{t_i}$, para todo $g = g_1 g_2 \cdots g_{t_i} \in G$. Assim, $(N_i G)^{t_i} = N_i^{t_i} G$. Então $(N_i G)^{t_i} \subset N_{i+1} G$, provando que a coleção $\mathcal{B}$ satisfaz a condição de nilpotência. Temos que como s_i é a característica de N_i em N_{i+1}, temos que $s_i N_i \subset N_{i+1}$, logo $(s_1 N_i)G \subset N_{i+1} G$. Veja que

$$\alpha \in (s_i N_i)G \Leftrightarrow \alpha = \sum_{g \in G} s_i n_g g = \sum_{g \in G} \underbrace{(n_g + n_g + \cdots + n_g)}_{s_i} g = s_i \sum_{g_1 \in G} n_g g \ \in s_i(N_i G),$$

o que prova que $\mathcal{B}$ satisfaz a condição característica, uma vez que $s_i(N_i G) = (s_i N_i)G \subset N_{i+1} G$. Uma vez que $\mathcal{N}$ satisfaz a condição CNC, temos que os primos na decomposição de s_i são todos maiores ou iguais a t_i, para todo $i = 1, 2, \ldots, k-1$. Com isso, provamos que $\mathcal{B}$ satisfaz a condição CNC.

Por último, sendo $f + N_1 G$ um idempotente de $\left(\frac{R}{N_1}\right) G \simeq \frac{RG}{N_1 G}$, segue do Teorema 2.1.8 que $f^{s_1 s_2 \cdots s_{k-1}}$ é um idempotente do anel de grupo RG e $|E(RG)| = \left|E\left(\frac{RG}{N_1 G}\right)\right| = \left|E\left(\left(\frac{R}{N_1}\right) G\right)\right|$. ■

Observação 2.2.2. Podemos concluir da demonstração da Proposição 2.2.1 que quando o anel R possui uma coleção de ideais $\mathcal{N} = \{N_1, N_2, \ldots, N_k\}$ que satisfazer a condição CNC, então o anel de grupo RG também possui uma coleção de ideais com essa propriedade. Tal coleção de ideais de RG é dada por $\mathcal{B} = \{N_1 G, N_2 G, \ldots, N_k G\}$.

Corolário 2.2.3. Sejam R um anel comutativo com unidade, N um ideal nilpotente de R de índice k, G um grupo comutativo e s a característica do anel quociente $\frac{R}{N}$. Se $f + NG$ é um idempotente do anel de grupo $\left(\frac{R}{N}\right) G$, então $f^{s^{k-1}}$ é um idempotente no anel de grupo RG. Além disso, $|E(RG)| = \left|E\left(\left(\frac{R}{N}\right) G\right)\right|$.

Demonstração. Do Lema 2.1.7 temos que $\{N, N^2, \ldots, N^k\}$ é uma coleção de ideais de R que satisfaz a condição CNC. Assim, o resultado segue da Proposição 2.2.1. Da Observação 2.2.2, sabemos que $\{NG, N^2 G, \ldots, N^k G\}$ é a coleção de ideais de RG que também satisfaz a condição CNC. ■

Corolário 2.2.4. Sejam R um anel comutativo com unidade, a um elemento nilpotente de R de índice k, G um grupo comutativo e s a característica do anel quociente $\frac{R}{\langle a \rangle}$. Se $f + \langle a \rangle G$ é um idempotente do anel de grupo $\left(\frac{R}{\langle a \rangle}\right) G$, então $f^{s^{k-1}}$ é um idempotente no anel de grupo RG. Além disso, $|E(RG)| = \left|E\left(\left(\frac{R}{\langle a \rangle}\right) G\right)\right|$.

Demonstração. Temos que $\langle a\rangle$ é um ideal nilpotente de índice k em R. Assim o resultado segue do Corolário 2.2.3 ■

Daremos destaque ao caso em que R é um anel de cadeia finito comutativo com unidade e G um grupo comutativo. Segue da Proposição 1.4.3, que R possui um único ideal maximal $M = \langle a\rangle$, para algum $a \in R$. Se k denota o índice de nilpotência de a e $\overline{R} = \frac{R}{\langle a\rangle}$ é um corpo de característica s, do Corolário 2.2.4, segue que

$$E(RG) = \left\{f^r;\ r = s^{k-1} \text{ e } \overline{f} \in E(\overline{R}G)\right\}.$$

Dentre os exemplos de anéis de cadeia finito, comutativo e com unidade temos o anel dos inteiros módulo p^k, denotado por $\mathbb{Z}_{p^k}$, onde p é um inteiro positivo e $k > 1$. Para este caso, o ideal nilpotente maximal é $\langle p\rangle$, com índice de nilpotência k em $\mathbb{Z}_{p^k}$ e, ainda, $\frac{\mathbb{Z}_{p^k}}{\langle p\rangle} \simeq \mathbb{Z}_p$. Então,

$$E(\mathbb{Z}_{p^k}G) = \left\{f^r;\ r = p^{k-1} \text{ e } \overline{f} \in E(\mathbb{Z}_pG)\right\}.$$

Exemplo 2.2.5. Sejam $\mathbb{Z}_{5^3}$ o anel dos inteiros módulo 5^3 e C_{7^3} um grupo cíclico de ordem 7^3 gerado por g.

Temos que os subgrupos de C_{7^3} formam a seguinte cadeia:

$$C_{7^3} = G_0 \supset G_1 \supset G_2 \supset G_3 = \{e\}.$$

Cada subgrupo possui ordem igual a $|G_i| = 7^{3-i}$, $0 \leq i \leq 3$.

Sabemos que o conjunto dos elementos idempotentes do anel de grupo $\mathbb{Z}_{5^3}C_{7^3}$ e da forma

$$E(\mathbb{Z}_{5^3}C_{7^3}) = \left\{f^{5^2};\ \overline{f} \in E(\mathbb{Z}_5C_{7^3})\right\}.$$

Da Proposição 1.1.11 temos que $\overline{\widehat{G}_i}$, em que $0 \leq i \leq 3$, são elementos idempotentes de $\mathbb{Z}_5C_{7^3}$, dados por

$$\overline{\widehat{G}_0} = \overline{2}\sum_{g\in G_0} g; \qquad \overline{\widehat{G}_1} = \overline{4}\sum_{g\in G_1} g;$$
$$\overline{\widehat{G}_2} = \overline{3}\sum_{g\in G_2} g; \qquad \overline{\widehat{G}_3} = \overline{1}1_G.$$

Podemos notar que $\overline{\widehat{G}_3} = 1$ é a unidade do anel de grupo $\mathbb{Z}_5C_{7^3}$. Uma vez que $\widehat{G}_i$, $0 \leq i \leq 3$, são idempotentes de $\mathbb{Z}_{5^3}C_{7^3}$, segue que $(\widehat{G}_i)^{5^2} = \widehat{G}_i$, assim temos os respectivos

idempotentes levantados:

$$\widehat{G}_0 = \overline{82} \sum_{g \in G_0} g; \qquad \widehat{G}_1 = \overline{74} \sum_{g \in G_1} g;$$
$$\widehat{G}_2 = \overline{18} \sum_{g \in G_2} g; \qquad \overline{\widehat{G}_3} = 1.$$

No Próximo capítulo, consideraremos um anel de grupo sobre um anel de cadeia finito, veremos como podemos caracterizar todos os códigos abelianos sobre esse anel a partir dos idempotentes obtidos pelo processo de levantamento.

Capítulo 3

Códigos Abelianos em um Anel de Grupo Sobre um Anel de Cadeia

Em [8], Dinh e López-Permouth usaram anéis de polinômios para caracterizar os códigos cíclicos de comprimento n sobre um anel de cadeia R, com q^k elementos, onde q é um número primo que não divide n. Na tese de doutorado [25], Silva usou o trabalho de Dinh e López-Permouth como base e caracterizou os códigos cíclicos usando uma abordagem de anéis de grupo. Tal caracterização se fundamenta em determinar os códigos a partir de potências do gerador do ideal maximal de um anel de cadeia R e idempotentes do anel de grupo RG, onde G é um grupo abeliano de ordem n. Com algumas adaptações, na primeira seção deste capítulo seguiremos os passos de Silva, mas agora considerando G um grupo abeliano. Assim, com o levantamento de idempotentes como ferramenta, podemos buscar os idempotentes de um anel de grupo RG, com R um anel de cadeia finito comutativo com unidade, e desta forma caracterizar os códigos abelianos de RG.

Na seção seguinte, vamos considerar o caso particular dos códigos cíclicos de comprimento p^n, com p primo, sobre um anel de cadeia R, com ideal maximal M. Neste caso, Ferraz e Polcino Milies em [9], encontraram os idempotentes da álgebra de grupo semissimples $\left(\frac{R}{M}\right) C_{p^n}$, que são determinados a partir da estrutura dos subgrupos de C_{p^n}. Finalizaremos o capítulo calculando o peso dos códigos cíclicos de comprimento p^n inspirados no trabalho feito por Melo em [18].

3.1 Caracterização de Códigos Abelianos sobre Anéis de Cadeia

Nesta seção, R denotará sempre um anel de cadeia finito comutativo com unidade. Sabemos da Proposição 1.4.3 que R possui um único ideal maximal M gerado por um nilpotente $a \in R$. Denotaremos o corpo residual $\frac{R}{M}$ por $\overline{R}$. A Proposição 1.4.5 diz que existe um número primo q tal que $|R| = q^k$ e $|\overline{R}| = q^l$ e ainda, a característica de R também é potencia de q e a característica de $\overline{R}$ é q.

Seja G um grupo abeliano de ordem n, tal que $mcd(n, q) = 1$. Logo, $char(\overline{R}) \nmid |G|$, portanto, do Corolário 1.1.14, temos que $\overline{R}G$ é semissimples. Desta maneira, existem uma família de idempotentes ortogonais primitivos $\{\overline{f}_0, \overline{f}_1, \ldots, \overline{f}_m\}$ de $\overline{R}G$ tal que

$$\overline{R}G = \overline{R}G\overline{f}_0 \oplus \overline{R}G\overline{f}_1 \oplus \cdots \oplus \overline{R}G\overline{f}_m,$$

com $\overline{R}G\overline{f}_i$ um ideal minimal de $\overline{R}G$, para todo $i = 0, 1, \ldots, m$.

Uma vez que $\frac{RG}{MG} \simeq \overline{R}G$, levantando estes idempotentes para o anel RG, sabemos da Proposição 2.1.1 que existe um único $e_i \in RG$ tal que $\overline{e}_i = \overline{f}_i$, para todo $i = 0, 1, \ldots, m$. E mais, $\{e_0, e_1, \ldots, e_m\}$ é uma família de idempotentes ortogonais primitivos de RG tais que

$$RG = RGe_0 \oplus RGe_1 \oplus \cdots \oplus RGe_m.$$

Sabemos que, para cada $i = 0, 1, \ldots, m$, o anel RGe_i é comutativo finito com unidade e_i. Do Corolário 1.4.7, temos que RGe_i é um anel local, pois e_i é primitivo para todo $i = 0, 1, \ldots, m$.

Agora vamos caracterizar todos os ideais deste anel RGe_i a partir do gerador do ideal maximal M de R. Para simplificar a notação denotaremos $(RG)a^k e_i$ por $\langle a^k e_i \rangle$.

Teorema 3.1.1. Sejam R e G como assumido anteriormente. Seja $M = \langle a \rangle$ o ideal maximal de R, com t o índice de nilpotência de a em R. Se $\mathcal{J}$ é ideal de RGe_i, para algum $i = 0, 1, \ldots, m$, então $\mathcal{J} = \langle a^{k_i} e_i \rangle$, com $0 \leq k_i \leq t$.

Demonstração. Claramente temos que $RGe_i = \langle a^0 e_i \rangle$ e $0 = \langle a^t e_i \rangle$, pois $a^t = 0$. Tome $\mathcal{J}$ um ideal próprio de RGe_i e seja $x \in \mathcal{J}$ não nulo. Veja que $\frac{RGe_i}{MGe_i} \simeq \overline{R}Ge_i$ o qual é uma componente simples comutativa com unidade de $\overline{R}G$. Então, $\overline{R}Ge_i$ é corpo, portanto, MGe_i é ideal maximal de RGe_i. Sabemos que RGe_i é anel local, logo MGe_i é o único

ideal maximal. Então temos $\mathcal{J} \subset MGe_i$ e assim $x \in MGe_i$. Lembrando que $M = \langle a \rangle$, podemos escrever

$$x = \sum_{g \in G} (r_g a) g e_i = \left(\sum_{g \in G} r_g g \right) a e_i,$$

com $r_g \in R$, para todo $g \in G$. Então $x \in \langle ae_i \rangle$. Portanto $\mathcal{J} \subset \langle ae_i \rangle$.

Agora, seja k o maior inteiro positivo tal que $\mathcal{J} \subset \langle a^k e_i \rangle$, claramente $0 < k < t$. Logo, existe $y \in \mathcal{J}$ tal que $y \notin \langle a^{k+1} e_i \rangle$. Provaremos que $y = ra^k e_i$, com $r \in RGe_i$ inversível. De fato, suponha que r não seja inversível, logo $r \in MGe_i$. Então, existe $w \in RGe_i$ tal que $r = wae_i$ e assim

$$y = ra^k e_i = wa^{k+1} e_i \in \langle a^{k+1} e_i \rangle,$$

o que é uma contradição. Logo r é inversível em RGe_i, com isso, temos

$$a^k e_i = a^k (rr^{-1}) e_i = (ra^k e_i) r^{-1} \in \mathcal{J},$$

pois $y = ra^k e_i \in \mathcal{J}$. Portanto $\langle a^k e_i \rangle \subset \mathcal{J}$, concluindo que $\mathcal{J} = \langle a^k e_i \rangle$. ■

Vejamos o seguinte lema:

Lema 3.1.2. Sejam R um anel local finito com unidade, $M = \langle a \rangle$ o ideal maximal de R e t o índice de nilpotência de a. Dados $x \in R$ e $0 < k < t$, então $xa^{t-k} = 0$ se, e somente se, $x \in \langle a^k \rangle$. E mais, se G é um grupo, dado $\alpha \in RG$, $\alpha a^k = 0$ se, e somente se, $\alpha \in \langle a^{t-k} \rangle G$.

Demonstração. Suponha que $xa^{t-k} = 0$. Se x for inversível, então $a^{t-k} = 0$, o que não ocorre uma vez que $t - k < t$. Logo, x não é inversível e, portanto, $x \in \langle a \rangle$. Suponha que $x \notin \langle a^k \rangle$, então existe $r < k$ tal que r é o maior inteiro positivo com $x \in \langle a^r \rangle$. Assim $x = x_1 a^r$, com $x_1 \in R$ inversível, pois se x_1 não for inversível, então $x_1 \in \langle a \rangle$, ou seja, $x_1 = x_2 a$ o que implica que $x = x_2 a^{r+1} \in \langle a^{r+1} \rangle$, o que não ocorre pois $r < r + 1$. Veja que, $x_1 a^{t-k+r} = xa^{t-k} = 0$ e como x_1 possui inverso, segue que $a^{t-k+r} = 0$. Note que $t - k + r < t$, contradizendo o fato de t ser o menor inteiro positivo tal que $a^t = 0$. Portanto $x \in \langle a^k \rangle$. Reciprocamente, se $x \in \langle a^k \rangle$, então $x = x' a^k$, com $x' \in R$. Portanto, $xa^{t-k} = x' a^{t-k+k} = x' a^t = 0$.

Agora, tome $\alpha = \sum_{g \in G} x_g g \in RG$. Temos que

$$\begin{aligned} \alpha a^k = 0 &\Leftrightarrow \sum_{g \in G} (x_g a^k) g = 0 \\ &\Leftrightarrow x_g a^k = 0, \ \forall g \in G \\ &\Leftrightarrow x_g \in \langle a^{t-k} \rangle, \ \forall g \in G \\ &\Leftrightarrow \alpha \in \langle a^{t-k} \rangle G. \end{aligned}$$

■

Assim obetemos o seguinte Corolário do Teorema 3.1.1.

Corolário 3.1.3. Sejam R e G como assumido anteriormente. Seja $M = \langle a \rangle$ ideal maximal de R, com t o índice de nilpotência de a em R. Então, para todo $i = 0, 1, \ldots, m$, o anel RGe_i é um anel de cadeia indecomponível e o ideal $\langle a^{t-1} e_i \rangle$ é minimal.

Demonstração. Para qualquer $i = 0, 1, \ldots, m$ sabemos que RGe_i é um anel local comutativo finito com unidade cujo único ideal maximal é principal gerado por ae_i. Da Proposição 1.4.3 o anel RGe_i é um anel de cadeia. A cadeia de ideais de RGe_i é dada por

$$RGe_i = \langle a^0 e_i \rangle \supsetneq \langle a^1 e_i \rangle \supsetneq \cdots \supsetneq \langle a^{t-1} e_i \rangle \supsetneq \langle a^t e_i \rangle = 0.$$

De fato, da Proposição 3.1.1 sabemos que todo ideal de RGe_i é da forma $\langle a^k e_i \rangle$, com $0 \leq k \leq t$. É fácil ver que $\langle a^k e_i \rangle \supset \langle a^s e_i \rangle$, para $0 \leq k \leq s \leq t$. Mostremos que se $k \neq s$, então $\langle a^k e_i \rangle \neq \langle a^s e_i \rangle$. Suponha que existe k e s, com $0 \leq k < s \leq t$, tais que $\langle a^k e_i \rangle = \langle a^s e_i \rangle$. Logo existe $\alpha \in RG$ tal que $a^k e_i = \alpha a^s e_i$. Multiplicando por a^{t-s} obtemos $a^{t+k-s} e_i = 0$. Como $k < s$, temos $t + k - s = t - (s - k) < t$ e, portanto, $a^{k+t-s} \neq 0$. Pelo Lema 3.1.2 temos que como $a^{t-(s-k)} e_i = 0$ então $e_i \in \langle a^{s-k} \rangle G \subset MG$. Como MG é ideal com índice de nilpotência t, então $e_i^t = 0$, o que é um absurdo, pois e_i é um idempotentes não nulo. Portanto $\langle a^k e_i \rangle \neq \langle a^s e_i \rangle$.

Evidentemente $\langle a^{t-1} e_i \rangle$ é minimal e do Corolário 1.4.7 RGe_i é indecomponível uma vez que e_i é idempotente primitivo. ■

No próximo resultado iremos caracterizar os códigos abelianos do anel de grupo RG

a partir dos ideais de cada RGe_i, ou seja, iremos caracterizar todos os ideais do anel de grupo RG.

Teorema 3.1.4. Sejam R e G como assumido anteriormente. Seja $M = \langle a \rangle$ ideal maximal de R, com t o índice de nilpotência de a em R. Se $\mathcal{J}$ é ideal de RG, então

$$\mathcal{J} = \langle a^{k_0} e_0 \rangle \oplus \langle a^{k_1} e_1 \rangle \oplus \cdots \oplus \langle a^{k_m} e_m \rangle,$$

com $0 \leq k_i \leq t$, para todo $i = 0, 1, \ldots, m$.

Demonstração. Seja $\mathcal{J}$ um ideal próprio de RG. Sendo RG um anel finito, segue que $\mathcal{J}$ tem finitos elementos. Desta forma podemos listar os elementos de $\mathcal{J} = \{x_1, x_2, \ldots, x_s\}$. Uma vez que $e_0, e_1, \ldots, e_m$ são idempotentes ortogonais primitivos, pela Definição 1.1.6 podemos escrever a unidade de RG como $1 = e_0 + e_2 + \cdots + e_m$. Assim,

$$\begin{aligned}
x_1 =& x_1e_0 + x_1e_1 + \cdots + x_1e_m \\
x_2 =& x_2e_0 + x_2e_1 + \cdots + x_2e_m \\
& \vdots \\
x_s =& x_se_0 + x_se_1 + \cdots + x_se_m.
\end{aligned}$$

Repare que cada $x_je_i \in RGe_i$, para todo $i \in \{0, 1, \ldots, m\}$ e todo $j \in \{1, 2, \ldots, s\}$. Como, para cada $i \in \{0, 1, \ldots, m\}$, temos que RGe_i é um anel de cadeia, então existe $j_i \in \{1, 2, \ldots, s\}$ tal que $\langle x_je_i \rangle \subset \langle x_{j_i}e_i \rangle$, para todo $j \in \{1, 2, \ldots, s\}$. Do Teorema 3.1.1, para cada $i \in \{0, 1, \ldots, m\}$, temos $\langle x_{j_i}e_i \rangle = \langle a^{k_i}e_i \rangle$, onde $0 \leq k_i \leq t$. Assim, dado $j \in \{1, 2, \ldots, s\}$, temos que

$$\begin{aligned}
x_j = x_je_0 + x_je_1 + \cdots + x_je_m \in& \langle x_je_0 \rangle + \langle x_je_1 \rangle + \cdots + \langle x_je_m \rangle \\
\subset& \langle x_{j_0}e_0 \rangle + \langle x_{j_1}e_1 \rangle + \cdots + \langle x_{j_m}e_m \rangle \\
=& \langle a^{k_0}e_0 \rangle + \langle a^{k_1}e_1 \rangle + \cdots + \langle a^{k_m}e_m \rangle.
\end{aligned}$$

Portanto $\mathcal{J} \subset \langle a^{k_0}e_0 \rangle + \langle a^{k_1}e_1 \rangle + \cdots + \langle a^{k_m}e_m \rangle$. Note que, como $x_{j_i} \in \mathcal{J}$, para todo $j_i \in \{1, 2, \ldots, s\}$, então $x_{j_i}e_i \in \mathcal{J}$, logo $\langle a^{k_i}e_i \rangle = \langle x_{j_i}e_i \rangle \subset \mathcal{J}$, para todo $i \in \{0, 1, \ldots, m\}$. Concluindo que $\mathcal{J} = \langle a^{k_0}e_0 \rangle + \langle a^{k_1}e_1 \rangle + \cdots + \langle a^{k_m}e_m \rangle$. Como $RGe_i \cap RGe_j = 0$, quando $i \neq j$, segue que $\mathcal{J} = \langle a^{k_0}e_0 \rangle \oplus \langle a^{k_1}e_1 \rangle \oplus \cdots \oplus \langle a^{k_m}e_m \rangle$. ■

Agora podemos contar quantos códigos abelianos o anel de grupo RG possui.

Teorema 3.1.5. Sejam R e G como assumido anteriormente. Seja $M = \langle a \rangle$ ideal maximal de R, com t o índice de nilpotência de a em R. O anel de grupo RG possui $(t+1)^{m+1}$ códigos abelianos.

Demonstração. Para cada $i = 0, 1, \ldots, m$, sabemos do Corolário 3.1.3 que RGe_i é um anel de cadeia finito, desta forma temos que RGe_i tem $t+1$ ideais distintos. Seja $\mathcal{J}$ um ideal de RG, então $\mathcal{J} = \langle a^{k_0}e_0 \rangle \oplus \langle a^{k_1}e_1 \rangle \oplus \cdots \oplus \langle a^{k_m}e_m \rangle$, com $0 \leq k_i \leq t$, para todo $i = 0, 1, \ldots, m$. Uma vez que temos $m+1$ idempotentes, pelo princípio fundamental da contagem segue que RG tem $(t+1)^{m+1}$ códigos abelianos. ■

Teorema 3.1.6. Sejam R e G como assumido anteriormente. Seja $M = \langle a \rangle$ ideal maximal de R, com t o índice de nilpotência de a em R. Então RG é um anel de ideais principais.

Demonstração. Seja $\mathcal{C} = \langle a^{k_0}e_0 \rangle \oplus \langle a^{k_1}e_1 \rangle \oplus \cdots \oplus \langle a^{k_m}e_m \rangle$ um ideal de RG. Denote por $c = a^{k_0}e_0 + a^{k_1}e_1 + \cdots + a^{k_m}e_m \in RG$. Uma vez que $e_0, e_1, \ldots, e_m$ são idempotentes ortogonais, ou seja, $e_ie_j = 0$ sempre que $i \neq j$ então, para qualquer $i = 0, 1, \ldots, m$, temos que

$$e_ic = a^{k_0}e_ie_0 + a^{k_1}e_ie_1 + \cdots + a^{k_i}e_i^2 + \cdots + a^{k_m}e_ie_m = a^{k_i}e_i.$$

Então $a^{k_i}e_i \in \langle c \rangle$, o que implica que $\langle a^{k_i}e_i \rangle \subset \langle c \rangle$, para todo $i = 0, 1, \ldots, m$. Portanto $\mathcal{C} \subset \langle c \rangle$. Evidentemente $c \in \mathcal{C}$, o que garante que $\langle c \rangle \subset \mathcal{C}$. Assim, concluímos que $\mathcal{C} = \langle c \rangle$. ■

3.2 Códigos Cíclicos de Comprimento p^n sobre Anéis de Cadeia

Para esta seção continuaremos a considerar R um anel de cadeia finito comutativo com unidade, onde $M = \langle a \rangle$ denota o ideal maximal de R.

Seja G um grupo cíclico de ordem p^n, com p primo, o reticulado de subgrupos de G formam uma cadeia, denotada por:

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n = \{1_G\}.$$

Da Proposição 1.1.11 sabemos que $\widehat{G}_i = \frac{1}{|G_i|}\sum_{g\in G_i} g$, com $0 \leq i \leq 3$, são elementos idempotentes de RG.

Proposição 3.2.1. Seja $\mathbb{F}$ um corpo finito com q^k elementos, onde q é um número primo. Seja G um grupo cíclico G de ordem p^n, com p primo. Se $mdc(q,p) = 1$, então $e_0 = \widehat{G}$ e $e_i = \widehat{G}_i - \widehat{G}_{i-1}$, com $i = 1, 2, \ldots, n$ são idempotentes ortogonais de $\mathbb{F}G$ tais que $e_0 + e_1 + \cdots + e_n = 1$.

Demonstração. Suponha que $|G_i|$ não é inversível em $\mathbb{F}$, para algum $i = 0, 1, \ldots, n$. Então $|G_i| = 0$, logo $p^n = |G| = 0$ em $\mathbb{F}$, ou seja, $char(\mathbb{F}) \mid p^n$. Isto é um absurdo, pois $char(\mathbb{F})$ é uma potência de q e $mdc(q,p) = 1$. Portanto $|G_i|$ é inversível em $\mathbb{F}$ para todo $i = 0, 1, \ldots, n$. Da Proposição 1.1.11 temos que $\widehat{G}_i$ é um idempotente de $\mathbb{F}G$, para todo $i = 0, 1, \ldots, n$.

Agora, tome $i < j$, assim temos $G_j \subset G_i$. Em $\mathbb{F}G$ temos que

$$\begin{aligned}
\widehat{G}_i\widehat{G}_j &= \left(\frac{1}{|G_i|}\sum_{g\in G_i} g\right)\left(\frac{1}{|G_j|}\sum_{h\in G_j} h\right) \\
&= \frac{1}{|G_i|}\frac{1}{|G_j|}\sum_{h\in G_j}\left(h\sum_{g\in G_i} g\right) \\
&= \frac{1}{|G_i|}\frac{1}{|G_j|}|G_j|\left(\sum_{g\in G_i} g\right) \\
&= \frac{1}{|G_i|}\sum_{g\in G_i} g \\
&= \widehat{G}_i
\end{aligned}$$

Assim, para $1 \leq i \leq n$ temos que $G_i \subset G_{i-1}$, ou seja, $\widehat{G}_i\widehat{G}_{i-1} = \widehat{G}_{i-1}$. Portanto,

$$\begin{aligned}
e_i^2 &= \left(\widehat{G}_i - \widehat{G}_{i-1}\right)^2 \\
&= \widehat{G}_i^2 - 2\widehat{G}_i\widehat{G}_{i-1} - \widehat{G}_{i-1}^2 \\
&= \widehat{G}_i - 2\widehat{G}_{i-1} - \widehat{G}_{i-1} \\
&= \widehat{G}_i - \widehat{G}_{i-1} \\
&= e_i.
\end{aligned}$$

Agora, tomando e_i e e_j, com $1 \leq i < j \leq n$, temos $i-1 < i \leq j-1 < j$. Assim,

$$\begin{aligned} e_i e_j &= \left(\widehat{G}_i - \widehat{G}_{i-1}\right)\left(\widehat{G}_j - \widehat{G}_{j-1}\right) \\ &= \widehat{G}_i\widehat{G}_j - \widehat{G}_i\widehat{G}_{j-1} - \widehat{G}_{i-1}\widehat{G}_j + \widehat{G}_{i-1}\widehat{G}_{j-1} \\ &= \widehat{G}_i - \widehat{G}_i - \widehat{G}_{i-1} + \widehat{G}_{i-1} \\ &= 0, \end{aligned}$$

pois $G_j \subset G_{j-1} \subset G_i \subset G_{i-1}$. Uma vez que $G_j \subset G$, para qualquer $j > 0$, temos

$$e_0 e_j = \widehat{G}\left(\widehat{G}_j - \widehat{G}_{j-1}\right) = \widehat{G} - \widehat{G} = 0.$$

Portanto, $e_0, e_1, \ldots, e_n$ são idempotentes ortogonais de $\mathbb{F}G$.

Por fim, é fácil ver que $e_0 + e_1 + \cdots + e_n = 1$. ■

Observação 3.2.2. Da demonstração da Proposição 3.2.1 sempre que H e K são subgrupos de um grupo finito G, tais que $H \subset K$, com $|H|$ e $|K|$ invertíveis em R, então $\widehat{H}\widehat{K} = \widehat{K}$ em RG.

Com a Proposição 3.2.1 temos uma família de idempotentes ortogonais, basta sabermos sob quais condições tais idempotentes são primitivos. Em [9], Ferraz e Milies forneceram tais condições.

Proposição 3.2.3. [9, Corolário 4] Sejam $\mathbb{F}$ um corpo finito com q^k elementos e G um grupo cíclico de ordem p^n, onde q e p são primos com $mcd(q,p) = 1$. Então o conjunto de idempotentes dados na Proposição 3.2.1 é o conjunto de idempotentes ortogonais primitivos de $\mathbb{F}G$ se, e somente se, vale o seguinte:

1. $p = 2$ e $n = 1$ e q é ímpar, ou $n = 2$ e $q \equiv 3 \pmod 4$.

2. p é um primo ímpar e $\langle \overline{q} \rangle = \mathcal{U}(\mathbb{Z}_{p^n})$.

No que segue, consideraremos R um anel de cadeia finito comutativo com unidade, tal que $|R| = q^k$, $M = \langle a \rangle$ o ideal maximal de R. O corpo residual $\frac{R}{M}$ será denotado por $\overline{R}$ e $\left|\frac{R}{M}\right| = q^l$, com $k = lt$, onde t é o índice de nilpotência de a. Ainda G será um grupo cíclico de ordem p^n, com q e p primos distintos satisfazem as hipóteses da Proposição 3.2.3.

Pela Proposição 3.2.3 temos que $\overline{e_0} = \overline{\widehat{G}}$ e $\overline{e_i} = \overline{\widehat{G}_i - \widehat{G}_{i-1}}$, com $1 \leq i \leq n$, formam o conjunto de idempotentes ortogonais primitivos de $\overline{R}G$. Do levantamento de idempotentes, Corolário 2.2.4, denotando a característica de $\overline{R}$ por s, temos que $e_i^{s^{t-1}}$, com $i = 0, 1, \ldots, n$, formam uma família de idempotentes ortogonais primitivos de RG. E mais, sabemos que em RG o elemento $\widehat{G}_i$ é idempotente. Logo e_i é idempotente em RG, o que garante que $e_i^{s^{t-1}} = e_i$.

Desta forma concluímos que $\{e_0, e_1, \ldots, e_n\}$ é a coleção de idempotentes ortogonais primitivos de RG e, ainda,

$$RG = RGe_0 \oplus RGe_1 \oplus \cdots \oplus RGe_n.$$

Para esse conjunto de idempotentes ortogonais primitivos podemos calcular quantos elementos tem cada código cíclico de RG.

Para os próximos resultados, quando for conveniente, denotemos o ideal $\langle x \rangle$ em RG por RGx.

Teorema 3.2.4. Sejam R e G como fixado. Se $\mathcal{C}$ é um código cíclico de RG da forma $\mathcal{C} = \langle a^{k_0}e_0 \rangle \oplus \langle a^{k_1}e_1 \rangle \oplus \cdots \oplus \langle a^{k_n}e_n \rangle$, com $0 \leq k_i \leq n$, então

$$|\mathcal{C}| = |\overline{R}|^{\left(\sum_{j=1}^{n}(t-k_j)(p^j-p^{j-1})+(t-k_0)\right)}.$$

Demonstração. Como $\mathcal{C}$ é soma direta de ideais, então $|\mathcal{C}| = |\langle a^{k_0}e_0 \rangle||\langle a^{k_1}e_1 \rangle| \cdots |\langle a^{k_n}e_n \rangle|$. Vamos determinar $|\langle a^{k_i}e_i \rangle|$. Seja $0 < i \leq n$, note que $a^{k_i}e_i = a^{k_i}\widehat{G}_i - a^{k_i}\widehat{G}_{i-1}$, assim $a^{k_i}e_i + a^{k_i}\widehat{G}_{i-1} = a^{k_i}\widehat{G}_i$. Agora, como $G_i \subset G_{i-1}$, então

$$e_i\widehat{G}_{i-1} = (\widehat{G}_i - \widehat{G}_{i-1})\widehat{G}_{i-1} = \widehat{G}_{i-1} - \widehat{G}_{i-1} = 0.$$

Logo,

$$RGa^{k_i}\widehat{G}_i = RGa^{k_i}e_i \oplus RGa^{k_i}\widehat{G}_{i-1}$$

Assim,

$$\left|RGa^{k_i}e_i\right| = \frac{\left|RGa^{k_i}\widehat{G}_i\right|}{\left|RGa^{k_i}\widehat{G}_{i-1}\right|}.$$

Considere $\psi : RG \to RGa^{k_i}$, dada por $\psi(x) = xa^{k_i}$. Temos que ψ é um homomorfismo

de grupos aditivos, pois $\psi(x+y) = (x+y)a^{k_i} = xa^{k_i} + ya^{k_i}$. Dado $xa^{k_i} \in RGa^{k_i}$ basta tomar $x \in RG$ e teremos que $\psi(x) = xa^{k_i}$, o que mostra que ψ é sobrejetora. Do Lema 3.1.2 temos que $xa^{k_i} = 0$ se, e somente se, $x \in \langle a^{t-k_i}\rangle G$. Portanto,

$$RGa^{k_i} \simeq \frac{RG}{\langle a^{t-k_i}\rangle G} \simeq \left(\frac{R}{\langle a^{t-k_i}\rangle}\right) G.$$

Denotando $\frac{R}{\langle a^{t-k_i}\rangle}$ por $\overline{R}_{k_i}$, temos

$$|RGa^{k_i}\widehat{G}_i| = |\overline{R}_{k_i} G\widehat{G}_i|.$$

Pela Proposição 1.1.12, temos que $\overline{R}_{k_i} G\widehat{G}_i \simeq \overline{R}_{k_i}\left(\frac{G}{G_i}\right)$. Como $\frac{G}{G_i}$ é base do módulo $\overline{R}_{k_i}\left(\frac{G}{G_i}\right)$, então

$$|RGa^{k_i}\widehat{G}_i| = |\overline{R}_{k_i} G\widehat{G}_i| = |\overline{R}_{k_i}|^{\frac{|G|}{|G_i|}} = |\overline{R}_{k_i}|^{p^i}.$$

De forma análoga, $|RGa^{k_i}\widehat{G}_{i-1}| = |\overline{R}_{k_i}|^{p^{i-1}}$. Logo,

$$\left|RGa^{k_i}e_i\right| = \frac{|\overline{R}_{k_i}|^{p^i}}{|\overline{R}_{k_i}|^{p^{i-1}}} = |\overline{R}_{k_i}|^{p^i - p^{i-1}}.$$

Temos, da Proposição 1.4.5, que

$$|\overline{R}_{k_i}| = \frac{|R|}{|\langle a^{t-k_i}\rangle|} = \frac{|\overline{R}|^t}{|\overline{R}|^{k_i}} = |\overline{R}|^{t-k_i}.$$

Então,

$$\left|RGa^{k_i}e_i\right| = |\overline{R}|^{(t-k_i)(p^i-p^{i-1})}.$$

Agora, tome $i = 0$. Como $e_0 = \widehat{G}$, analogamente ao o que foi feito antes, temos que

$$|RGa^{k_0}e_0| = |RGa^{k_0}\widehat{G}| = |\overline{R}_{k_0} G\widehat{G}|,$$

onde $\overline{R}_{k_0} = \frac{R}{\langle a^{t-k_0}\rangle}$. Assim,

$$|RGa^{k_0}e_0| = |\overline{R}_{k_0}|^{\frac{|G|}{|G|}} = |\overline{R}|^{t-k_0}.$$

Concluindo que $|\mathcal{C}| = |\overline{R}|^{\left(\sum_{j=1}^{m}(t-k_j)(p^j-p^{j-1})+(t-k_0)\right)}$. ■

Estudaremos todos os possíveis pesos dos códigos de RG, ou seja, calcularemos $\omega(\mathcal{C}) =$

$min\{\omega(\alpha);\ \alpha \in \mathcal{C}-\{0\}\}$, para cada ideal $\mathcal{C}$ de RG (veja a Observação 1.3.4). Veremos que nas condições fixadas os pesos dos códigos de RG dependem diretamente dos subgrupos de G.

Proposição 3.2.5. Sejam R e G como fixado. Então $\omega(RG\widehat{G}_i) = |G_i|$, para todo $i = 0, 1, \ldots, n$.

Demonstração. Seja $\gamma \in RG\widehat{G}_i$. Seja τ uma transversal de G_i em G. Logo, $\gamma = \sum_{h\in\tau} x_h h\widehat{G}_i$, com $x_h \in R$, para todo $h \in \tau$. Como $\frac{1}{|G_i|}$ é inversível em R, então $x_h\frac{1}{|G_i|} \neq 0$, para todo $h \in \tau$ tal que $x_h \neq 0$. Assim, podemos concluir que $\omega(\gamma)$ é múltiplo de $|G_i|$. Daí, $\omega(RG\widehat{G}_i) \geq |G_i|$. Como $\widehat{G}_i \in RG\widehat{G}_i$ e $\omega(\widehat{G}_i) = |G_i|$, logo, $\omega(RG\widehat{G}_i) = |G_i|$. ■

Observação 3.2.6. Da demonstração anterior podemos concluir que para R e G como fixado, qualquer palavra de RG da forma $\alpha\widehat{G}_i$, com $\alpha \in RG$, tem peso múltiplo de $|G_i|$.

Teorema 3.2.7. Sejam R e G como fixado. Então, para $0 \leq k \leq t-1$, quando $i \neq 0$ temos $\omega(RGa^k e_i) = 2|G_i|$ e $\omega(RGa^k e_0) = |G|$.

Demonstração. Tome $i \neq 0$. Primeiro, note que $e_i\widehat{G}_i = (\widehat{G}_i - \widehat{G}_{i-1})\widehat{G}_i = e_i$. Desta forma, $RGe_i \subset RG\widehat{G}_i$. Seja τ uma transversal de G_i em G. Portanto, toda palavra de $RG\widehat{G}_i$ é da forma $\sum_{h\in\tau} x_h h\widehat{G}_i$, com $x_h \in R$, para todo $h \in \tau$.

Como $RGa^k e_i \subset RGa^k\widehat{G}_i$, então qualquer palavra de $RGa^k e_i$ é da forma $\sum_{h\in\tau} x_h a^k h\widehat{G}_i$, com $x_h \in R$, para todo $h \in \tau$.

Seja $\gamma = \sum_{h\in\tau} x_h a^k h\widehat{G}_i \in RGa^k e_i$, então $\omega(\gamma)$ é múltiplo de $|G_i|$. Suponha que $|supp(\gamma)| = 1$, ou seja, apenas um coeficiente de γ, digamos $x_h a^k$, é não nulo. Uma vez que, $x_h a^k h\widehat{G}_i \in RGa^k e_i \subset RGe_i$, então existe $\beta \in RG$, tal que $x_h a^k h\widehat{G}_i = \beta a^k e_i$ Logo, $x_h a^k h\widehat{G}_i\widehat{G}_{i-1} = \beta a^k e_i\widehat{G}_{i-1}$. Como $e_i\widehat{G}_{i-1} = 0$ e $\widehat{G}_i\widehat{G}_{i-1} = \widehat{G}_{i-1}$, então $x_h a^k h\widehat{G}_{i-1} = 0$, o que implica que $x_h a^k = 0$. Logo $x_h a^k h\widehat{G}_i = 0$, o que é uma contradição. Portanto, $\omega(RGa^k e_i) \geq 2|G_i|$.

Como o peso de um código é o mínimo dos pesos das suas palavras não nulas, basta encontrarmos uma palavra com peso exatamente $2|G_i|$. Para isso, tome $x \in G_{i-1}\backslash G_i$,

considere $(1-x)a^k e_i \in RGa^k e_i$. Como

$$\begin{aligned}(1-x)a^k e_i &= (1-x)a^k(\widehat{G}_i - \widehat{G}_{i-1}) \\ &= (1-x)a^k\widehat{G}_i - (1-x)a^k\widehat{G}_{i-1} \\ &= (1-x)a^k\widehat{G}_i - a^k\widehat{G}_{i-1} + xa^k\widehat{G}_{i-1} \\ &= (1-x)a^k\widehat{G}_i - a^k\widehat{G}_{i-1} + a^k\widehat{G}_{i-1} \\ &= (1-x)a^k\widehat{G}_i\end{aligned}$$

e $supp(a^k\widehat{G}_i) \cap supp(xa^k\widehat{G}_i) = \emptyset$, pois $x \notin G_i$, logo $xg \notin G_i$, para todo $g \in G_i$. Desta forma $\omega((1-x)a^k e_i) = 2|G_i|$. Concluindo que $\omega(RGa^k e_i) = 2|G_i|$.

Agora tome $i = 0$. Temos que $RGa^k e_0 = RGa^k\widehat{G}$. Se $\gamma \in RGa^k\widehat{G}$ não nulo, então $\gamma = \sum_{g\in G} r_g a^k g\widehat{G} = \sum_{g\in G} r_g a^k\widehat{G}$, com $r_g \in RG$. Temos que $\omega(\gamma) = k|G|$, para algum inteiro positivo k, ou seja, o peso de todas as palavras de RGe_0 é múltiplo de $|G|$. Assim, $\omega(RGe_0) \geq |G|$. Como $a^k\widehat{G} \in RGe_0$ é tal que $\omega(a^k\widehat{G}) = |G|$, então $\omega(RGe_0) = |G|$. ■

Teorema 3.2.8. Sejam R e G como fixado. Seja $\mathcal{C} = \mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_j$, com $0 \leq j \leq n-1$, onde $\mathcal{C}_j = RGa^{k_j}e_j$ e $0 \leq k_j \leq t-1$. Então $\omega(\mathcal{C}) = |G_j|$.

Demonstração. Seja $\gamma \in \mathcal{C}$, então existem $x_0, x_1, \ldots, x_j \in RG$, tais que

$$\gamma = x_0 a^{k_0} e_0 + x_1 a^{k_1} e_1 + \cdots + x_j a^{k_j} e_j.$$

Uma vez que $G_j \subset G_i$, para $1 \leq i \leq j-1$, então

$$\widehat{G}_j e_i = \widehat{G}_j\widehat{G}_i - \widehat{G}_j\widehat{G}_{i-1} = \widehat{G}_i - \widehat{G}_{i-1} = e_i, \quad \forall\ i = 1, 2, \ldots, j-1.$$

Assim, $\gamma\widehat{G}_j = \gamma$. Portanto, $\mathcal{C} \subset RG\widehat{G}_j$ e assim $\omega(\mathcal{C}) \geq \omega(RG\widehat{G}_j) = |G_j|$.

Seja $k = max\{k_0, k_1, \ldots, k_j\}$. Então,

$$RGa^k\widehat{G}_j \subset RGa^k e_0 \oplus RGa^k e_1 \oplus \cdots \oplus RGa^k e_j.$$

Como $k \geq k_i$, para todo $i = 0, 1, \ldots, j$, e RGe_i é anel de cadeia, temos que

$$RGa^k e_i \subset RGa^{k_i} e_i, \quad \forall i = 0, 1, \ldots, j.$$

Logo $RGa^k e_0 \oplus RGa^k e_1 \oplus \cdots \oplus RGa^k e_j \subset RGa^{k_0} e_0 \oplus RGa^{k_1} e_1 \oplus \cdots \oplus RGa^{k_j} e_j$. Então, $RGa^k \widehat{G}_j \subset \mathcal{C}$. Assim, $|G_j| = \omega(RGa^k \widehat{G}_j) \geq \omega(\mathcal{C})$. Concluimos que $\omega(\mathcal{C}) = |G_j|$. ■

Teorema 3.2.9. Sejam R e G como fixado. Sejam $\mathcal{C}_j = RGa^{k_j} e_j$, com $0 \leq k_j \leq t-1$. Seja $\{j_1, j_2, \ldots, j_r\}$ um subconjunto de índices tais que $j_i < j_{i+1}$ e $\{j_1, j_2, \ldots, j_r\} \subsetneq \{0, 1, \ldots, j_r\}$. Se $\mathcal{C} = \mathcal{C}_{j_1} \oplus \mathcal{C}_{j_2} \oplus \cdots \oplus \mathcal{C}_{j_r}$, então $\omega(\mathcal{C}) = 2|G_{j_r}|$.

Demonstração. Considere inicialmente

$$\mathcal{C} = \mathcal{C}_{j_1} \oplus \mathcal{C}_{j_2} \oplus \cdots \oplus \mathcal{C}_{j_r},$$

com $j_1 \neq 0$ e $j_i < j_{i-1}$, para $1 \leq r \leq r$. Seja $\gamma \in \mathcal{C}$. Logo, existem $x_{j_1}, x_{j_2}, \ldots, x_{j_r}$, elementos de RG tais que

$$\gamma = x_{j_1} a^{k_{j_1}} e_{j_1} + x_{j_2} a^{k_{j_2}} e_{j_2} + \cdots + x_{j_r} j a^{k_{j_r}} e_{j_r}.$$

Como $G_{j_r} \subset G_{j_i}$, para $1 \leq i \leq r-1$, temos $\widehat{G} + j_r e_{j_i} = e_{j_i}$, para $1 \leq i \leq r-1$. Assim, $\gamma = \gamma \widehat{G}_{j_r} \in RG\widehat{G}_{j_r}$. Portanto, $\mathcal{C} \subset RG\widehat{G}_{j_r}$. Seja τ uma transversal de G_{j_r} em G. Assim podemos escrever $\gamma = \sum_{h \in \tau} x_h h \widehat{G}_{j_r}$, com $x_h \in R$. Suponha que $|supp(\gamma)| = 1$, ou seja, existe apenas um $h_0 \in \tau$, tal que $x_{h_0} \neq 0$. Assim,

$$x_{h_0} h_0 \widehat{G}_{j_r} = x_{j_1} a^{k_{j_1}} e_{j_1} + x_{j_2} a^{k_{j_2}} e_{j_2} + \cdots + x_{j_r} a^{k_{j_r}} e_{j_r}.$$

Uma vez que $G_{j_i} \subset G_{j_1 - 1}$, para $1 \leq i \leq r$, então $\widehat{G}_{j_i} \widehat{G}_{j_1 - 1} = \widehat{G}_{j_1 - 1}$, para $1 \leq i \leq r$. Logo, $\widehat{G}_{j_1 - 1} e_{j_i} = 0$, para $1 \leq i \leq r$. Disso segue que

$$\begin{aligned} & x_{h_0} h_0 \widehat{G}_{j_r} \widehat{G}_{j_1 - 1} = \left(x_{j_1} a^{k_{j_1}} e_{j_1} + x_{j_2} a^{k_{j_2}} e_{j_2} + \cdots + x_{j_r} a^{k_{j_r}} e_{j_r} \right) \widehat{G}_{j_1 - 1} \\ & \Leftrightarrow x_{h_0} h_0 \widehat{G}_{j_1 - 1} = 0. \end{aligned}$$

Concluindo que $x_{h_0} = 0$, o que contradiz a nossa escolha inicial de $x_{h_0} \neq 0$. Portanto, $\omega(\mathcal{C}) \geq 2|G_{j_r}|$. Por outro lado, como $\mathcal{C}_{j_r} \subset \mathcal{C}$, então $2|G_{j_r}| = \omega(\mathcal{C}_{j_r}) \geq \omega(\mathcal{C})$. Concluindo que, $\omega(\mathcal{C}) = 2|G_{j_r}|$.

Agora considere o caso em que

$$\mathcal{C} = \mathcal{C}_0 \oplus \mathcal{C}_{j_1} \oplus \cdots \oplus \mathcal{C}_{j_r},$$

com $j_i < j_{i+1}$, para $1 \leq i \leq r$ e $\{j_1, j_2, \ldots, j_r\} \subsetneq \{1, 2, \ldots, j_r\}$.

como assumido anteriormente, uma vez que $\mathcal{C}_{j_r} \subset \mathcal{C}$, então $2|G_{j_r}| = \omega(\mathcal{C}_{j_r}) \geq \omega(\mathcal{C})$.

Seja $\gamma \in \mathcal{C}$. Então existem $x_0, x_{j_1}, \ldots, x_{j_r} \in RG$, tais que

$$\gamma = x_0 a^{k_0} e_0 + x_{j_1} a^{k_{j_1}} e_{j_1} + \cdots + x_{j_r} a^{k_{j_r}} e_{j_r}.$$

Assim, $\gamma \widehat{G}_{j_r} = \gamma$. Portanto, $\mathcal{C} \subset RG\widehat{G}_{j_r}$. Tome τ a transversal de G_{j_r} em G, assim podemos escrever $\gamma = \sum_{h \in \tau} x_h h \widehat{G}_{j_r}$, com $x_h \in R$. Suponha que existe apenas um $t_0 \in \tau$ tal que $x_{t_0} \neq 0$. Assim,

$$x_{t_0} t_0 \widehat{G}_{j_r} = x_0 a^{k_0} e_0 + x_{j_1} a^{k_{j_1}} e_{j_1} + \cdots + x_{j_r} a^{k_{j_r}} e_{j_r}.$$

Como $\{j_1, j_2, \ldots, j_r\} \subsetneq \{1, 2, \ldots, j_r\}$, existe $s \in \{1, 2, \ldots, j_r\} \backslash \{j_1, j_2, \ldots, j_r\}$. Tome s sendo o menor índice pertencente à $\{1, 2, \ldots, j_r\}$ e que não pertence a $\{j_1, j_2, \ldots, j_r\}$. Logo, $1, 2, \ldots, s-1 \in \{j_1, j_2, \ldots, j_r\}$. Sabemos que, para todo $j_i > s$ temos $G_{j_i} \subset G_s$. Assim, se $j_i > s$, então $e_{j_i} \widehat{G}_s = 0$. Desta forma,

$$\begin{aligned} x_{t_0} t_0 \widehat{G}_{j_r} \widehat{G}_s &= (x_0 a^{k_0} e_0 + x_{j_1} a^{k_{j_1}} e_{j_1} + \cdots + x_{j_r} a^{k_{j_r}} e_{j_r}) \widehat{G}_s \\ \Leftrightarrow x_{t_0} t_0 \widehat{G}_s &= x_0 a^{k_0} e_0 + x_1 a^{k_1} e_1 + \cdots + x_{s-1} a^{k_{s-1}} e_{s-1}. \end{aligned}$$

Logo $x_{t_0} t_0 \widehat{G}_s \in \mathcal{C}' = RGa^{k_0} e_0 \oplus RGa^{k_1} e_1 \oplus \cdots \oplus RGa^{k_{s-1}} e_{s-1}$. Do Teorema 3.2.8 temos que $\omega(\mathcal{C}') = |G_{s-1}|$, e como $x_{t_0} t_0 \widehat{G}_s \in \mathcal{C}'$, segue que $\omega(x_{t_0} t_0 \widehat{G}_s) \geq \omega(\mathcal{C}')$. O que é um absurdo, pois $\omega(x_{t_0} t_0 \widehat{G}_s) = |G_s| < |G_{s-1}|$, uma vez que $G_s \subsetneq G_{s-1}$. Logo $\omega(\mathcal{C}) \geq 2|G_{j_r}|$. Portanto, $\omega(\mathcal{C}) = 2|G_{j_r}|$. ■

Exemplo 3.2.10. Retomemos o exemplo 2.2.5. Temos que o anel $\mathbb{Z}_5 C_{7^3}$ satisfaz as hipóteses da Proposição 3.2.3, assim temos os seguintes idempotentes primitivos ortogonais de $\mathbb{Z}_5 C_{7^3}$:

$$\begin{aligned} \overline{e_0} &= \overline{2} \sum_{g \in G_0} g; & \overline{e_1} &= \overline{4} \sum_{g \in G_1} g - \overline{2} \sum_{g \in G_0} g; \\ \overline{e_2} &= \overline{3} \sum_{g \in G_2} g - \overline{4} \sum_{g \in G_1} g; & \overline{e_3} &= \overline{1} 1_G - \overline{3} \sum_{g \in G_2} g. \end{aligned}$$

Os elementos obtidos pelo levantamento de idempotentes, dados por

$$e_0 = e_0^{5^2} = \overline{82}\sum_{g\in G_0} g; \qquad e_1 = e_1^{5^2} = \overline{74}\sum_{g\in G_1} g - \overline{82}\sum_{g\in G_0} g;$$
$$e_2 = e_2^{5^2} = \overline{18}\sum_{g\in G_2} g - \overline{74}\sum_{g\in G_1} g; \qquad e_3 = e_3^{5^2} = \overline{1}1_G - \overline{18}\sum_{g\in G_2} g.$$

formam uma coleção de idempotentes ortogonais primitivos de $\mathbb{Z}_{5^3}C_{7^3}$ (lembrando que agora os coeficientes de cada e_i, com $0 \leq i \leq 3$, são elementos do anel $\mathbb{Z}_{5^3}$). Assim, temos que

$$\mathbb{Z}_{5^3}C_{7^3} = \langle e_0\rangle \oplus \langle e_1\rangle \oplus \langle e_2\rangle \oplus \langle e_3\rangle.$$

Sabemos que $\langle\overline{5}\rangle$ é o ideal maximal do anel $\mathbb{Z}_{5^3}$ e o índice de nilpotência de $\overline{5}$ neste mesmo anel é 3. O Teorema 3.1.5 nos garante que $\mathbb{Z}_{5^3}C_{7^3}$ possui $(3+1)^{3+1} = 4^4 = 256$ códigos cíclicos.

Usando a caracterização dada pelo Teorema 3.1.4, considere o código $\mathcal{C} = \langle e_0\rangle \oplus \langle\overline{25}e_1\rangle \oplus \langle\overline{5}e_3\rangle$ de $\mathbb{Z}_{5^3}C_{7^3}$, do Teorema 3.2.9 temos que $\omega(\mathcal{C}) = 2|G_3| = 2$, uma vez que $G_3 = \{1_G\}$. Tome outro código $\mathcal{C}' = \langle\overline{5}e_0\rangle \oplus \langle e_1\rangle \oplus \langle\overline{5}e_2\rangle$ de $\mathbb{Z}_{5^3}C_{7^3}$, o Teorema 3.2.8 garante que o peso de $\mathcal{C}'$ é igual a $|G_2| = 7$.

Com o Teorema 3.2.4 podemos calcular quantos elementos há em cada um desses códigos:

$$|\mathcal{C}| = |\mathbb{Z}_5|^{\left[(3-2)(7-1)+(3-3)(7^2-7)+(3-1)(7^3-7^2)+(3-0)\right]} = 5^{597}.$$
$$|\mathcal{C}'| = |\mathbb{Z}_5|^{\left[(3-0)(7-1)+(3-1)(7^2-7)+(3-3)(7^3-7^2)+(3-1)\right]} = 5^{104}.$$

Capítulo 4

Códigos de Grupo com Complemento Dual

Neste capítulo estudaremos os códigos lineares com complemento dual, os quais chamamos de Códigos LCD (linear code complementary dual). Esses códigos foram definidos por Massey em [16] como códigos lineares tais que a interseção com seu dual é trivial. Veremos que as álgebras de grupo possuem uma forma bilinear simétrica que nos permite definir o dual de um código de grupo e mostraremos algumas propriedades de tal forma bilinear. Por fim, mostraremos o resultado que nos permite determinar se um código é LCD caso ele seja gerado por um idempotente autoadjunto.

4.1 Códigos LCD Gerados por Idempotentes

Os resultados nesta seção não se restringem apenas a códigos abelianos, dessa forma, a fim de obtermos resultados mais gerais tomaremos o anel de grupo RG, com R sendo um anel comutativo com unidade e G um grupo finito qualquer. Consideraremos sempre os ideais à direita, pois o caso para ideais à esquerda será análogo. Quando não nos referirmos à direita nem à esquerda é por que estamos olhando para um ideal bilateral.

Nesta seção tomaremos sempre R um anel comutativo com unidade e G um grupo finito.

Lema 4.1.1. Seja A uma R-álgebra com unidade de dimensão finita. Então:

1. Se $A = A_1 \oplus A_2$, com A_1 e A_2 ideais à direita de A, então existe um idempotente $e \in A$ tal que $A_1 = eA$ e $A_2 = (1 - e)A$.

2. Se $e \in A$ é um idempotente, então $A = eA \oplus (1-e)A$.

Demonstração. Vejamos

1. Suponha que $A = A_1 \oplus A_2$. Logo existem $a_1 \in A_1$ e $a_2 \in A_2$ tais que $1 = a_1 + a_2$. Assim $a_1 = a_1^2 + a_2a_1$ e $a_2 = a_1a_2 + a_2^2$. Dai, $a_1 - a_1^2 = a_2a_1$ e $a_2 - a_2^2 = a_1a_2$. Como A_1 e A_2 são ideais à direita e $A_1 \cap A_2 = 0$ segue que $a_1 = a_1^2$, $a_2 = a_2^2$ e $a_1a_2 = a_2a_1 = 0$. Portanto, a_1 e a_2 são idempotentes de A.

   Como $a_1 \in A_1$ e $a_2 \in A_2$, então $a_1A \subset A_1$ e $a_2A \subset A_2$. Agora, se $x \in A_1$, então $x = a_1x + a_2x$, assim $x - a_1x = a_2x \in A_1 \cap A_2 = 0$, logo $x = a_1x \in a_1A$. Então $A_1 = a_1A$. Da mesma forma, se $y \in A_2$, temos $y = a_1y + a_2y$, logo $y = a_2y \in a_2A$. Então $A_2 = a_2A$.

   Tomando $e = a_1$, temos $1 - e = a_2$, e assim segue que

$$A = eA \oplus (1-e)A.$$

2. Seja $e \in A$ um elemento idempotente. Considere os ideais à direita eA e $(1-e)A$ de A. Note que $1 = e + (1-e)$, logo $A = eA + (1-e)A$. Basta mostrar que $eA \cap (1-e)A = 0$. De fato, seja $x \in eA \cap (1-e)A$, então existem $a, b \in A$ tais que $ea = x = (1-e)b$. Como $e^2 = e$, segue que

$$x = ea = e(ea) = e(1-e)b = (e - e^2)b = 0.$$

   Portanto, $A = eA \oplus (1-e)A$.

■

Definição 4.1.2. Sejam R um anel comutativo e G um grupo finito. A álgebra de grupo RG carrega naturalmente uma forma bilinear simétrica definida por $\langle\ ,\ \rangle : RG \times RG \to R$ onde

$$\langle g, h\rangle = \begin{cases} 1, \text{ se } g = h \\ 0, \text{ se } g \neq h \end{cases} \qquad \text{para } g, h \in G.$$

Assim, dados $\sum_{g\in G} a_g g$ e $\sum_{h\in G} b_h h$ elementos de RG, temos

$$\left\langle \sum_{g\in G} a_g g, \sum_{h\in G} b_h h \right\rangle = \sum_{g\in G} a_g b_g.$$

A forma bilinear $\langle\ ,\ \rangle$ é não-degenerada em RG, ou seja, se $x \in RG$ é tal que $\langle x, y\rangle = 0$, para todo $y \in RG$, então $x = 0$. De fato, seja $x = \sum_{g\in G} x_g g \in RG$ tal que $\langle x, y\rangle = 0$, para todo $y \in RG$. Em particular, como podemos ver os elementos de G da forma $g = 1_R g \in RG$, então $\langle x, g\rangle = 0$, para todo $g \in G$, assim

$$x_g = \langle x, g\rangle = 0, \quad \forall\ g \in G.$$

Logo $x = 0$. Portanto, $\langle\ ,\ \rangle$ é uma forma bilinear simétrica não-degenerada.

Note que, dado $k \in G$, temos

$$\begin{aligned}\left\langle \sum_{g\in G} a_g g\cdot k, \sum_{h\in G} b_h h\cdot k \right\rangle &= \sum_{g\in G} a_g b_h \langle kg, kh\rangle \\ &= \sum_{g\in G} a_g b_h \langle g, h\rangle \\ &= \sum_{g\in G} a_g b_g \\ &= \left\langle \sum_{g\in G} a_g g, \sum_{h\in G} b_h h \right\rangle,\end{aligned}$$

pois $kg = kh$ se, e somente se, $g = h$, para todo $g, h \in G$. Assim, dizemos que $\langle\ ,\ \rangle$ é G-invariante.

Agora, considere a aplicação

$$\begin{array}{rccc} * : & RG & \longrightarrow & RG \\ & \sum_{g\in G} a_g g & \longmapsto & \left(\sum_{g\in G} a_g g\right)^* = \sum_{g\in G} a_g g^{-1} \end{array}$$

chamada de **involução clássica** de RG.

Note que

$$\begin{aligned}\left(\sum_{g\in G} a_g g + \sum_{g\in G} b_g g\right)^* &= \left(\sum_{g\in G}(a_g + b_g)g\right)^* \\ &= \sum_{g\in G}(a_g + b_g)g^{-1} \\ &= \sum_{g\in G} a_g g^{-1} + \sum_{g\in G} b_g g^{-1} \\ &= \left(\sum_{g\in G} a_g g\right)^* + \left(\sum_{g\in G} b_g g\right)^*\end{aligned}$$

e ainda

$$\begin{aligned}\left(\sum_{g\in G} a_g g \sum_{g\in G} b_g g\right)^* &= \left(\sum_{g,h\in G}(a_g b_h)gh\right)^* \\ &= \sum_{g,h\in G}(a_g b_h)(gh)^{-1} \\ &= \sum_{g,h\in G}(b_h a_g)h^{-1}g^{-1} \\ &= \sum_{g\in G} b_g g^{-1} \sum_{g\in G} a_g g^{-1} \\ &= \left(\sum_{g\in G} b_g g\right)^* \left(\sum_{g\in G} a_g g\right)^*\end{aligned}$$

Logo $*$ é um anti-homomorfismo de anéis.

Mais ainda, dado $r \in R$, segue que

$$\left(r\sum_{g\in G} a_g g\right)^* = \left(\sum_{g\in G} r a_g g\right)^* = \sum_{g\in G} r a_g g^{-1} = r\sum_{g\in G} a_g g^{-1} = r\left(\sum_{g\in G} a_g g\right)^*$$

concluindo que $*$ é um homomorfismo de R-álgebras.

Definição 4.1.3. Dado $a \in RG$, dizemos que a^* é o **adjunto** de a em RG. Dizemos que a é **autoadjunto** quando $a = a^*$.

Proposição 4.1.4. Dados $a, b, c \in RG$, então $\langle ab, c\rangle = \langle a, cb^*\rangle = \langle b, a^*c\rangle$.

Demonstração. Sejam $a = \sum_{g\in G} a_g g$ e $b = \sum_{h\in G} b_h h$ elementos de RG. Facilmente vemos que, dado $c \in RG$, então

$$\langle g, c\rangle = \left\langle gg^{-1}, cg^{-1}\right\rangle = \left\langle 1, cg^{-1}\right\rangle,$$

para todo $g \in G$, pois $\langle\ ,\ \rangle$ é G-invariante. Assim, para $h \in G$, segue

$$\begin{aligned}
\langle ah, c\rangle &= \left\langle \sum_{g\in G} a_g gh, c \right\rangle \\
&= \sum_{g\in G} a_g \langle gh, c\rangle \\
&= \sum_{g\in G} a_g \left\langle g, ch^{-1}\right\rangle \\
&= \left\langle \sum_{g\in G} a_g g, ch^{-1} \right\rangle \\
&= \left\langle a, ch^{-1}\right\rangle
\end{aligned}$$

Por fim, temos

$$\begin{aligned}
\langle ab, c\rangle &= \left\langle \sum_{g\in G} a_g g \sum_{h\in G} b_h h, c \right\rangle \\
&= \left\langle \sum_{g,h\in G} a_g b_h gh, c \right\rangle \\
&= \sum_{g,h\in G} a_g b_h \langle gh, c\rangle \\
&= \left\langle \sum_{g\in G} a_g g, c \sum_{h\in G} b_h h^{-1} \right\rangle \\
&= \langle a, cb^*\rangle .
\end{aligned}$$

Analogamente obtemos que $\langle ab, c\rangle = \langle b, a^*c\rangle$. ■

Definição 4.1.5. Sejam R um anel comutativo com unidade e G um grupo finito. Dado um código de grupo à direita $\mathcal{C}$ de RG, definimos o **dual** de $\mathcal{C}$ como sendo o conjunto

$$\mathcal{C}^\perp = \{x \in RG;\ \langle x, c\rangle = 0,\ \forall c \in \mathcal{C}\}.$$

Um código de grupo à direita $\mathcal{C}$ de RG é chamado de **código com complemento dual** ou **LCD** se

$$RG = \mathcal{C} \oplus \mathcal{C}^\perp,$$

ou seja, $\mathcal{C} \cap \mathcal{C}^{\perp} = \{0\}$.

Proposição 4.1.6. Seja $\mathcal{C}$ um código de grupo à direita de RG, então $\mathcal{C}^{\perp}$ também é um código de grupo à direita de RG. E mais, se $\mathcal{C}$ for um código de grupo de RG, então $\mathcal{C}^{\perp}$ também é.

Demonstração. Suponha que $\mathcal{C}$ é um código de grupo à direita de RG. Uma vez que $\langle c, 0\rangle = 0$, para todo $c \in \mathcal{C}$, segue que $0 \in \mathcal{C}^{\perp}$. Sejam $a, b \in \mathcal{C}^{\perp}$. Dado $c \in \mathcal{C}$, temos que $\langle a - b, c\rangle = \langle a, c\rangle - \langle b, c\rangle = 0$. Agora, dado $r \in RG$ então $\langle ar, c\rangle = \langle a, cr^*\rangle = 0$, uma vez que $cr^* \in \mathcal{C}$. Portanto, $a - b \in \mathcal{C}^{\perp}$ e $ar \in \mathcal{C}^{\perp}$, provando que $\mathcal{C}^{\perp}$ é um código de grupo à direita de RG.

Se $\mathcal{C}$ é um código de grupo, basta notar que $\langle ra, c\rangle = \langle a, r^*c\rangle = 0$, e assim teremos que $\mathcal{C}^{\perp}$ é um código de grupo de RG. ■

Em [7] de la Cruz e Willems demonstraram o resultado a seguir para o caso em que $R = \mathbb{K}$ é um corpo finito. Com algumas adaptações pudemos demonstrar este resultado para o caso mais geral, em que R é um anel comutativo com unidade, como segue:

Teorema 4.1.7. Sejam R um anel comutativo com unidade e G um grupo finito. Seja $\mathcal{C}$ um código de grupo à direita de RG. O código $\mathcal{C}$ é um código LCD de RG se, e somente se, existe $e \in RG$ um idempotente autoadjunto tal que $\mathcal{C} = eRG$.

Demonstração. Suponha que $\mathcal{C}$ é um código LCD de RG, ou seja, $RG = \mathcal{C} \oplus \mathcal{C}^{\perp}$. Como $\mathcal{C}$ e $\mathcal{C}^{\perp}$ são ideais à direita de RG, do Lema 4.1.1, existe um idempotente $e \in RG$ tal que $\mathcal{C} = eRG$ e $\mathcal{C}^{\perp} = (1 - e)RG$. Agora falta apenas mostrarmos que e é autoadjunto. Para tal, tome $a \in RG$ qualquer, temos que $ea \in \mathcal{C}$, assim

$$0 = \langle ea, 1 - e\rangle = \langle a, e^*(1 - e)\rangle .$$

Uma vez que tomamos $a \in RG$ é arbitrário, segue que $\langle x, e^*(1 - e)\rangle = 0$, para todo $x \in RG$. Como a forma bilinear $\langle\ ,\ \rangle$ é não-degenerada, então $e^*(1 - e) = 0$, ou seja, $e^* = e^*e$. Com isso e usando propriedades da involução segue que

$$e = (e^*)^* = (e^*e)^* = e^*(e^*)^* = e^*e = e^*.$$

Portanto, e é um idempotente autoadjunto.

Reciprocamente suponha que $\mathcal{C} = eRG$, onde $e \in RG$ é tal que $e^2 = e = e^*$. Pelo Lema 4.1.1, como e é um idempotente, então $RG = eRG \oplus (1-e)RG$. Vamos mostrar que $\mathcal{C}^\perp = (1-e)RG$. De fato, dados $a, b \in RG$, temos $ea \in eRG = \mathcal{C}$ e $(1-e)b \in (1-e)RG$. Vejamos que

$$\langle ea, (1-e)b\rangle = \langle a, e^*(1-e)b\rangle = \langle a, e(1-e)b\rangle = 0.$$

Disso segue que, $(1-e)RG \subset \mathcal{C}^\perp$. Por outro lado, dado $x \in \mathcal{C}^\perp$, temos que $\langle ea, x\rangle = 0$, para todo $a \in RG$. Assim

$$0 = \langle ea, x\rangle = \langle a, e^*x\rangle = \langle a, ex\rangle\,, \quad \forall\ a \in RG.$$

Sendo $\langle\ ,\ \rangle$ não-degenerada, segue que $ex = 0$. Como $x \in RG = eRG \oplus (1-e)RG$, então existem $x_1, x_2 \in RG$ tais que $x = ex_1 + (1-e)x_2$. Desta forma, multiplicando por e em ambos os lados, temos

$$\begin{aligned} & ex = e^2x_1 + e(1-e)x_2 \\ \Leftrightarrow\quad & 0 = ex_1 + (e-e)x_2 \\ \Leftrightarrow\quad & 0 = ex_1. \end{aligned}$$

Logo, $x = (1-e)x_2 \in (1-e)RG$. Concluindo que $\mathcal{C}^\perp \subset (1-e)RG$. Então, $\mathcal{C}^\perp = (1-e)RG$, logo $RG = \mathcal{C} \oplus \mathcal{C}^\perp$. Portanto, $\mathcal{C}$ é um código LCD. ■

Novamente consideraremos R um anel de cadeia finito comutativo com unidade, tal que $|R| = q^k$, com q primo e k um inteiro positivo. Seja $M = \langle a\rangle$ o ideal maximal de R, com índice de nilpotência t, e denote o corpo residual $\frac{R}{M}$ por $\overline{R}$, onde $\left|\overline{R}\right| = q^l$, com $k = lt$. Tome G um grupo cíclico de ordem p^n, com q e p primos distintos satisfazem as hipóteses da Proposição 3.2.3.

Aplicando o Teorema 4.1.7 para R e G nestas condições podemos determinar todos os códigos LCD em $\overline{R}G$ e RG.

Como vimos no Capítulo 3, temos que $\overline{e_0} = \overline{\widehat{G}}$ e $\overline{e_i} = \overline{\widehat{G}_i - \widehat{G}_{i-1}}$, com $1 \leq i \leq n$, formam o conjunto de idempotentes ortogonais primitivos do anel semissimples $\overline{R}G$.

Corolário 4.1.8. Sejam R e G como fixado. Então todos os códigos de $\overline{R}G$ são LCD.

Demonstração. Note que, como G é finito, para $i = 0, 1 \ldots, n$ temos

$$\overline{\widehat{G}_i}^* = \overline{|G_i|}^{-1} \sum_{g \in G_i} g^{-1} = \overline{|G_i|}^{-1} \sum_{g \in G_i} g = \overline{\widehat{G}_i},$$

logo $\overline{\widehat{G}_i}$ é autoadjunto em $\overline{R}G$, para todo $i = 0, 1 \ldots, n$. Assim, para $i = 1, 2 \ldots, n$, temos que $\overline{e_i}$ também é autoadjunto em $\overline{R}G$, pois

$$\overline{e_i}^* = \overline{\widehat{G}_i - \widehat{G}_{i-1}}^* = \overline{\widehat{G}_i}^* - \overline{\widehat{G}_{i-1}}^* = \overline{\widehat{G}_i - \widehat{G}_{i-1}} = \overline{e}.$$

Portanto, do Teorema 4.1.7, segue que $\overline{R}G\overline{e_i}$ é um código LCD de $\overline{R}G$. Sabemos que, nessas condições, se $\mathcal{J}$ é um código de $\overline{R}G$, então existe um subconjunto de índices $J \subset \{0, 1, \ldots, n\}$ tal que $\mathcal{J} = \underset{j \in J}{\oplus} \overline{R}G\overline{e_j}$. Como $\overline{e_i e_j} = 0$, quando $i \neq j$, então para $i \in J$ temos $\overline{e_i} \sum\limits_{j \in J} \overline{e_j} = \overline{e_i}$. Assim, tomando o idempotente $\overline{E} = \sum\limits_{j \in J} \overline{e_j}$ podemos concluir que $\overline{R}G\overline{e_i} \subset \overline{R}G\overline{E}$, para todo $i = 0, 1, \ldots, n$. Logo, $\mathcal{J} = \overline{R}G\overline{E}$, uma vez que $\overline{E} \in \mathcal{J}$. E mais, como $*$ define um anti-homomorfismo de anéis, segue que

$$E^* = \left(\sum_{j \in J} \overline{e_j} \right)^* = \sum_{j \in J} \overline{e_j}^* = \sum_{j \in J} \overline{e_j} = E.$$

Assim, do Teorema 4.1.7, $\mathcal{J}$ é um código LCD de $\overline{R}G$. Como a escolha do código $\mathcal{J}$ é arbitraria, segue que todos os códigos cíclicos de $\overline{R}G$ são LCD. ■

Com o levantamento dos idempotentes, temos que

$$RG = RGe_0 \oplus RGe_1 \oplus \cdots \oplus RGe_n.$$

onde $\{e_0, e_1 \ldots, e_n\}$ formam a família de idempotentes primitivos ortogonais de RG. Se $\mathcal{C}$ é um código abeliano de RG, então do Teorema 3.1.4

$$\mathcal{C} = \langle a^{k_0} e_0 \rangle \oplus \langle a^{k_1} e_1 \rangle \oplus \cdots \oplus \langle a^{k_n} e_n \rangle,$$

com $0 \leq k_i \leq t$.

Corolário 4.1.9. Sejam R e G como fixado. Tomando um subconjunto de índices $J \subset \{0, 1, \ldots, n\}$, então $\mathcal{C} = \underset{i \in J}{\oplus} RGe_i$ é um código LCD de RG.

Demonstração. Pelo Teorema 3.1.6 temos

$$\mathcal{C} = RGE,$$

onde $E = \sum_{i \in J} e_i$ é um idempotente de RG. Analogamente ao que fizemos no Corolário 4.1.8, temos que $E^* = E$, ou seja, E é um idempotente autoadjunto em RG. Logo $\mathcal{C}$ é um código LCD de RG. ■

Proposição 4.1.10. Sejam R e G como fixado. Seja $\mathcal{C} = \langle a^{k_0} e_0 \rangle \oplus \langle a^{k_1} e_1 \rangle \oplus \cdots \oplus \langle a^{k_n} e_n \rangle$, com $0 \leq k_i \leq t$, um ideal de RG. Se para algum $l \in \{0, 1, \ldots, n\}$ tivermos $0 < k_l < t$, então $\mathcal{C}$ não é um código LCD.

Demonstração. Considere o ideal $\langle a^{t-k_l} e_l \rangle$ de RG. Seja $x \in \mathcal{C}$, logo

$$x = x_0 a^{k_0} e_0 + x_1 a^{k_1} e_1 + \cdots + x_n a^{k_n} e_n,$$

onde $x_0, x_1, \ldots, x_n \in RG$. Observe que como $e_0, e_1, \ldots e_n$ são idempotentes ortogonais e autoadjuntos então

$$\begin{aligned}
\left\langle a^{t-k_l} e_l, x \right\rangle &= \left\langle a^{t-k_l} e_l, x_0 a^{k_0} e_0 + x_1 a^{k_1} e_1 + \cdots + x_n a^{k_n} e_n \right\rangle \\
&= \left\langle a^{t-k_l} e_l, x_0 a^{k_0} e_0 \right\rangle + \cdots + \left\langle a^{t-k_l} e_l, x_l a^{k_l} e_l \right\rangle + \cdots + \left\langle a^{t-k_l} e_l, x_n a^{k_n} e_n \right\rangle \\
&= \left\langle a^{t-k_l}, x_0 a^{k_0} e_0 e_l^* \right\rangle + \cdots + \left\langle a^{t-k_l}, x_l a^{k_l} e_l e_l^* \right\rangle + \cdots + \left\langle a^{t-k_l}, x_n a^{k_n} e_n e_l^* \right\rangle \\
&= \left\langle a^{t-k_l}, x_0 a^{k_0} e_0 e_l \right\rangle + \cdots + \left\langle a^{t-k_l}, x_l a^{k_l} e_l e_l \right\rangle + \cdots + \left\langle a^{t-k_l}, x_n a^{k_n} e_n e_l \right\rangle \\
&= \left\langle a^{t-k_l}, x_l a^{k_l} e_l \right\rangle \\
&= a^{t-k_l} a^{k_l} \langle 1, x_l e_l \rangle \\
&= a^{t-k_l+k_l} \langle 1, x_l e_l \rangle \\
&= a^t \langle 1, x_l e_l \rangle \\
&= 0.
\end{aligned}$$

Como $x \in \mathcal{C}$ é arbitrário, segue que $a^{t-k_l} e_l \in \mathcal{C}^\perp$. Portanto $\langle a^{t-k_l} e_l \rangle \subset \mathcal{C}^\perp$.

Como $0 < k_l < t$, então $0 \neq a^{k_l} e_l \in \mathcal{C}$. E mais, $0 < t - k_l < t$ e, como já vimos, $0 \neq a^{t-k_l} e_l \in \mathcal{C}^\perp$. Considere os seguintes casos:

1. Se $k_l < t - k_l$, então $\langle a^{k_l} e_l \rangle \supset \langle a^{t-k_l} e_l \rangle$, ou seja, $a^{t-k_l} e_l \in \langle a^{k_l} e_l \rangle \subset \mathcal{C}$. Portanto $\mathcal{C} \cap \mathcal{C}^\perp \neq \{0\}$.

2. Se $k_l \geq t - k_l$, então $\langle a^{k_l} e_l \rangle \subset \langle a^{t-k_l} e_l \rangle$, ou seja, $a^{k_l} e_l \in \langle a^{t-k_l} e_l \rangle \subset \mathcal{C}^{\perp}$. Portanto $\mathcal{C} \cap \mathcal{C}^{\perp} \neq \{0\}$.

Em ambos os casos o código $\mathcal{C}$ tem interseção não trivial com seu dual. Portanto $\mathcal{C}$ não é LCD. ■

Desta forma determinamos que os únicos códigos LCD de RG são do tipo $\bigoplus_{i \in J} RGe_i$, onde J é um subconjunto de índices de $\{0, 1, \ldots, n\}$ e o nulo, uma vez que o ideal nulo é sempre gerado por 0 em RG, que por sua vez é um idempotente autoadjunto.

Bibliografia

[1] G. K. Bakshi, S. Gupta, and I. B. S. Passi. Semisimple metacyclic group algebras. *Proceedings-Mathematical Sciences*, 121(4):379–396, 2011.

[2] S. Berman. Semisimple cyclic and abelian codes. ii. *Cybernetics*, 3(3):17–23, 1967.

[3] A. R. Calderbank and N. J. Sloane. Modular and p-adic cyclic codes. *Designs, codes and Cryptography*, 6:21–35, 1995.

[4] C. Carlet and S. Guilley. Complementary dual codes for counter-measures to side-channel attacks. In *ICMCTA*, pages 97–105. Springer, 2014.

[5] C. Carlet and S. Guilley. Complementary dual codes for counter-measures to side-channel attacks. *Adv. Math. Commun.*, 10(1):131–150, 2016.

[6] J. H. Conway and N. J. Sloane. Self-dual codes over the integers modulo 4. *Journal of Combinatorial Theory, Series A*, 62(1):30–45, 1993.

[7] J. de la Cruz and W. Willems. On group codes with complementary duals. *Designs, Codes and Cryptography*, 86:2065–2073, 2018.

[8] H. Q. Dinh and S. R. López-Permouth. Cyclic and negacyclic codes over finite chain rings. *IEEE Transactions on Information Theory*, 50(8):1728–1744, 2004.

[9] R. A. Ferraz and C. P. Milies. Idempotents in group algebras and minimal abelian codes. *Finite Fields and Their Applications*, 13(2):382–393, 2007.

[10] R. W. Hamming. Error detecting and error correcting codes. *The Bell system technical journal*, 29(2):147–160, 1950.

[11] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. Sloane, and P. Solé. The z/sub 4/-linearity of kerdock, preparata, goethals, and related codes. *IEEE Transactions on Information Theory*, 40(2):301–319, 1994.

[12] A. Hefez and M. L. T. Villela. *Códigos corretores de erros*. Instituto de Matemática Pura e Aplicada, 2002.

[13] N. Jacobson. *Basic Algebra. II, VV. H.* Freeman and Co, New York, 1989.

[14] P. Kanwar and S. R. Lopez-Permouth. Cyclic codes over the integers modulo p^m. *Finite fields and their applications*, 3(4):334–352, 1997.

[15] A. Kelarev and P. Solé. Error-correcting codes as ideals in group rings. *Contemporary Mathematics*, 273:11–18, 2001.

[16] J. L. Massey. Linear codes with complementary duals. *Discrete Mathematics*, 106:337–342, 1992.

[17] B. R. McDonald. *Finite rings with identity*, volume 28. Marcel Dekker Incorporated, 1974.

[18] F. D. Melo. *Sobre códigos cíclicos e abelianos*. Tese de doutorado, Universidade de São Paulo, 2012.

[19] F. D. Melo Hernández, C. A. Hernández Melo, and H. Tapia-Recillas. On idempotents of a class of commutative rings. *Communications in Algebra*, 48(9):4013–4026, 2020.

[20] C. P. Milies and F. D. de Melo. On cyclic and abelian codes. *IEEE transactions on information theory*, 59(11):7314–7319, 2013.

[21] C. P. Milies, S. K. Sehgal, and S. Sehgal. *An introduction to group rings*, volume 1. Springer Science & Business Media, 2002.

[22] G. H. Norton and A. Sălăgean. On the structure of linear and cyclic codes over a finite chain ring. *Applicable algebra in engineering, communication and computing*, 10:489–506, 2000.

[23] V. S. Pless and Z. Qian. Cyclic codes and quadratic residue codes over z_4. *IEEE Transactions on Information Theory*, 42(5):1594–1600, 1996.

[24] C. E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27(3):379–423, 1948.

[25] A. T. Silva. *Códigos cíclicos sobre anéis de cadeia*. Tese de doutorado, Universidade de São Paulo, 2012.

[26] Z.-X. Wan. Cyclic codes over galois ring. In *Algebr. Colloq.*, volume 6, pages 291–304, 1999.