Códigos de peso constante

Ruth Nascimento

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

Programa: Matemática
Orientador: Prof. Dr. Raul Antonio Ferraz

Durante o desenvolvimento deste trabalho a autora recebeu auxílio financeiro da CAPES e do CNPQ

São Paulo, agosto de 2014

Códigos de peso constante

Esta versão definitiva da tese
contém as correções e alterações sugeridas pela
Comissão Julgadora durante a defesa realizada
por Ruth Nascimento em 09/06/2014.

Comissão Julgadora:

- Prof. Dr. Raul Antonio Ferraz (orientador) - IME-USP.
- Prof. Dr. Francisco César Polcino Milies - IME-USP.
- Profa. Dra. Sueli Irene Rodrigues Costa- UNICAMP.
- Profa. Dra. Marinês Guerreiro - UFV.
- Prof. Dr. Thierry Corrêa Petit Lobão - UFBA.

Resumo

Sejam $\mathcal{F}_q$ um corpo finito com q elementos, e C_n um grupo cíclico de n elementos com $mdc(q,n) = 1$, Iniciamos nosso trabalho inspirados nos resultados de Vega [19], estabelecendo condições para que um código de $\mathcal{F}_qC_n$ tenha peso constante. Com tal resultado concluímos que um código de peso constante em $\mathcal{F}_qC_n$ é da forma $\{rg^ie | r \in \mathcal{F}_q, 0 \leq i \leq n\}$. A partir disto, determinamos a quantidade de códigos de peso constante de $\mathcal{F}_qC_n$, e construímos exemplos de códigos de dois pesos em $\mathcal{F}_q(C_n \times C_n)$. Em seguida, estabelecemos sob quais condições um código em $\mathcal{F}_qA$, para A um grupo abeliano finito, tem peso constante. Analisamos também os códigos de peso constante em RG, quando R um anel de cadeia finito e C_n é um grupo cíclico de n elementos com $mdc(n,q) = 1$. Além disso, analisamos o caso em que os elementos de um ideal de RA, para R um domínio de integridade infinito e A um grupo abeliano finito têm peso constante.

Palavras-chave: Códigos de peso constante, anéis de grupo, anéis de cadeia, grupo cíclico, grupo abeliano.

Abstract

Let $\mathcal{F}_q$ be a field with q elements, C_n be a cyclic group of order n and suppose that $gcd(q, n) = 1$. In this work conditions are given to ensure that a code in $\mathcal{F}_q C_n$ is a one weight code, inspired in the work of Vega [19]. As a consequence of this result we showed that a one weight code in $\mathcal{F}_q C_n$ is of the form $\{rg^i e | r \in \mathcal{F}_q, 0 \leq i \leq n\}$. With this, we determined the number of one weight codes in $\mathcal{F}_q C_n$, and constructed examples of two weight codes in $\mathcal{F}_q(C_n \times C_n)$. After this, we gave conditions to ensure that a code had constant weight in $\mathcal{F}_q A$, for A a finite abelian group. We also analyzed the one weight codes in RG, R a chain ring and C_n a cyclic group with n elements with $gcd(n, q) = 1$. Moreover, we analyzed the case when the elements of an ideal in RA, for R an infinite integral domain and A a finite abelian group, have constant weight.

Key words: One weight codes, group rings, chain ring, cyclic group, abelian group.

Sumário

Introdução

Ao se tentar transmitir uma informação, que consiste de uma sequência finita de símbolos que são elementos de um alfabeto finito, podem ocorrer erros de tal modo que o receptor da mensagem receba uma informação distorcida, podendo assim cometer erros na interpretação da informação. A Teoria de Códigos auxilia para que estes erros tornem-se menos frequentes, ajudando a detectar e corrigir os erros ocorridos na transmissão da informação.

Segundo [13], um dos marcos iniciais desta teoria é um famoso teorema de C.E. Shannon, encontrado no artigo intitulado "A Mathematical Theory of Communication", também publicado no "The Bell System Technical Journal"[16], que garante a existência de códigos que podem transmitir informação com uma probabilidade arbitrariamente pequena de erro, sendo um campo de pesquisa muito ativo na atualidade em diversas áreas do conhecimento, como Matemática, Computação, Engenharia Elétrica e Estatística. Um dos propósitos da Teoria Algébrica de Códigos é desenvolver métodos para a construção de tais códigos.

É importante na teoria o estudo do peso de Hamming de um código. Em particular, temos os códigos de peso constante, isto é, aqueles em que todas as suas palavras não nulas têm o mesmo peso de Hamming. Muitos dos trabalhos nesta área estão baseados no estudo de códigos binários de peso constante, que possui várias aplicações, como por exemplo na comunicação móvel. Atualmente, tem crescido também o interesse em códigos não binários de peso constante, pelo crescente uso de alfabetos não binários

(veja por exemplo [3]). Mas tais códigos foram bem menos explorados comparados com os códigos binários.

Em nosso trabalho estudamos códigos, não necessariamente binários, em determinados anéis de grupo, buscando inicialmente dar condições para que tais códigos tenham peso constante.

O primeiro capítulo traz os resultados e definições encontrados na bibliografia e que serão utilizados ao longo do texto.

No segundo capítulo, analisamos os códigos de peso constante em $\mathcal{F}_qC_n$, para $\mathcal{F}_q$ um corpo com q elementos e C_n um grupo cíclico de n elementos com $mdc(q,n)=1$, buscando dar condições para garantir que um código de $\mathcal{F}_qC_n$ tenha peso constante. Tal trabalho foi baseado no seguinte resultado de Vega [19]:

Teorema 0.1 ([19], Teorema 9)**.** *Seja $\mathcal{F}_q$ um corpo com q elementos, $n=\lambda\frac{q^k-1}{q-1}$, com λ dividindo $(q-1)$, e $\mathcal{C}$ um código cíclico de $\mathcal{F}_q$ de comprimento n e dimensão k, gerado por $g(x)$, e com polinômio de checagem $h(x)$. Então, $\mathcal{C}$ tem peso constante se, e somente se, $w(ge)=\lambda(q^{k-1})$.*

Nosso trabalho deu origem ao seguinte resultado:

Teorema 0.2. *Sejam $\mathcal{F}_q$ um corpo com q elementos, n um inteiro positivo tal que $mdc(q,n)=1$, $C_n =< g >$ um grupo cíclico com n elementos, e $\mathcal{F}_qC_n$ o anel de grupo de C_n sobre $\mathcal{F}_q$. Considere e um idempotente primitivo de $\mathcal{F}_qC_n$, $\mathcal{C}=\mathcal{F}_qC_ne$ o respectivo código irredutível e $dim_{\mathcal{F}_q}\mathcal{C}=k$. São equivalentes:*

1. *$\mathcal{C}$ tem peso constante;*
2. *Todo elemento não nulo de $\mathcal{C}$ tem peso $\frac{q^{k-1}(q-1)n}{q^k-1}$;*
3. *Existe um elemento de $\mathcal{C}$ cujo peso é $\frac{q^{k-1}(q-1)n}{q^k-1}$;*
4. *$(\mathcal{F}_qC_ne)^*=\mathcal{F}_q^*eC_ne$.*

Como consequência de tal resultado concluímos que os códigos de peso constante de $\mathcal{F}_qC_n$, com $mdc(n,q)=1$, são da forma $\{rg^ie | r\in\mathcal{F}_q, 0\leq i\leq n\}$. Em seguida,

chegamos a uma fórmula que determina a quantidade de códigos de peso constante em $\mathcal{F}_q C_n$. Finalizando o capítulo, construímos exemplos de códigos de dois pesos em $\mathcal{F}_q(C_n \times C_n)$.

O terceiro capítulo foi destinado a dar condições que garantissem que um código é de peso constante em outras classes de anéis de grupo. Analisamos os códigos de peso constante nos anéis de grupo $\mathcal{F}_q A$, com A um grupo abeliano finito, RG, com R um anel de cadeia finito e G um grupo cíclico de ordem n, com $mdc(n, q) = 1$, além de analisar os ideais de peso constante de RG, para R um domínio de integridade infinito e G um grupo abeliano finito.

Capítulo 1

Preliminares

Daremos aqui as principais definições e resultados encontrados na bibliografia [8], [9], [10], [14], [15] e [17], e que serão usados ao longo do texto.

1.1 Grupos

Definição 1.1. *Um* **grupo** $(G, \cdot)$ *consiste de um conjunto* G*, fechado em relação à operação binária* $\cdot$*, tal que os seguintes axiomas são satisfeitos:*

1. *A operação binária* $\cdot$ *é associativa.*
2. *Existe um elemento* $1 \in G$ *tal que* $1 \cdot x = x \cdot 1 = x$*, para todo* $x \in G$ *(tal elemento é chamado* **elemento identidade** *de* $(G, \cdot)$*).*
3. *Para cada* $a \in G$*, existe um elemento* $a' \in G$ *com a propriedade que* $a \cdot a' = a' \cdot a = 1$ *(tal elemento* a' *é chamado* **inverso** *de* a *com respeito à operação* $\cdot$*).*

Denotaremos o grupo $(G, \cdot)$ por G.
Se a operação $\cdot$ é comutativa o grupo G é dito **abeliano**.

Definição 1.2. *Dados* G, G' *dois grupos, uma função* $f : G \to G'$ *é um* **homomorfismo de grupos** *se, dados* $a, b \in G$*,* $f(ab) = f(a)f(b)$*. Se* f *é também bijetora*

então temos um **isomorfismo de grupos**, *e dizemos que G é isomorfo a G', o que denotamos por $G \simeq G'$.*

A **ordem** de um grupo G é a quantidade de elementos de G, que pode ser finita ou infinita. Neste trabalho, todos os grupos considerados têm ordem finita. Denotamos por $|G|$ a ordem do grupo G.

Dado $g \in G$, caso exista um natural n tal que $g^n = 1$, o menor natural positivo tal que isso ocorre é chamado de **ordem** de g.

Definição 1.3. *Um elemento a de um grupo G* **gera** *G se $\langle a \rangle = \{a^n | n \in \mathbb{Z}\} = G$. Um grupo G é dito* **cíclico** *se existe algum $a \in G$ que gera G.*

Definição 1.4. *Seja H um subgrupo de um grupo G e a um elemento de G. O subconjunto $aH = \{ah | h \in H\}$ é a* **classe lateral à esquerda** *de H contendo a enquanto $Ha = \{ha | h \in H\}$ é a* **classe lateral à direita** *de H contendo a.*

Se G é um grupo abeliano $aH = Ha$ é simplesmente a classe lateral de H contendo a.

Definição 1.5. *Um subgrupo H de um grupo G é* **normal** *se, para todo $a \in G$, $aH = Ha$, ou equivalentemente, se $aHa^{-1} \subseteq H$, para todo $a \in G$.*

Note que se G é abeliano, todo subgrupo de G é normal em G.

Definição 1.6. *Seja H subgrupo normal de um grupo G. Definimos um novo grupo G/H, cujos elementos são as classes aH, $a \in G$, e a operação é dada por*

$$(aH)(bH) = (abH), \text{ para todos } a, b \in G.$$

Notação: Denotaremos por $[G : H]$ o índice de H em G, que é o número de classes laterais de H em G.

Teorema 1.7. *([8], Teorema 2.5)[Teorema de Lagrange] Seja H um subgrupo de um grupo finito G. Então, a ordem de H divide a ordem de G. Mais precisamente, temos*

$$|G| = [G : H] \, |H| \, .$$

Teorema 1.8. *Seja H um subgrupo normal de um grupo G. Então*

1. *Para cada subgrupo K de G contendo H, o conjunto $\frac{K}{H} = \{xH : x \in K\}$ é um subgrupo de $\frac{G}{H}$.*

2. *Reciprocamente, se $\mathcal{K}$ é um subgrupo do grupo quociente $\frac{G}{H}$, então a pré-imagem $K = \{x \in G : xH \in \mathcal{K}\}$ é um subgrupo de G contendo H tal que $\mathcal{K} = \frac{K}{H}$.*

Definição 1.9. *Dado um grupo G, definimos o* **expoente** *de G como o menor inteiro positivo m tal que $g^m = 1$, para todo $g \in G$, caso tal número exista.*

Teorema 1.10. *Se H_1, $H_2 < G$, G cíclico finito, então $|H_1H_2| = mmc(|H_1|, |H_2|)$, e $|H_1 \cap H_2| = mdc(|H_1|, |H_2|)$.*

Prova: Pelo Teorema de Lagrange, $|H_1|\,||H_1H_2|$ e $|H_2|\,||H_1H_2|$, donde $mmc(|H_1|, |H_2|)||H_1H_2|$. Como H_1H_2 é subgrupo de G, então H_1H_2 é cíclico já que G é cíclico. Digamos $H_1H_2 =< \alpha >$, com $\alpha = \beta_1\beta_2$, $\beta_1 \in H_1$, $\beta_2 \in H_2$. Logo

$$\alpha^{mmc(|H_1||H_2|)} = (\beta_1\beta_2)^{mmc(|H_1||H_2|)} = \beta_1^{mmc(|H_1||H_2|)}\beta_2^{mmc(|H_1||H_2|)} = 1,$$

donde $|H_1H_2| = o(\alpha)|mmc(|H_1|\,|H_2|)$, e portanto $|H_1H_2| = mmc(|H_1|\,|H_2|)$. Como $|H_1|\,|H_2| = mmc(|H_1|, |H_2|)mdc(|H_1|, |H_2|)$, bem como $|H_1|\,|H_2| = |H_1H_2|\,|H_1 \cap H_2|$ o resultado segue. □

1.2 Anéis e Anéis de grupo

Definição 1.11. *Um* **anel** $(R, +, \cdot)$ *consiste de um conjunto não vazio R munido de duas operações binárias $+$ e $\cdot$, que chamamos* **adição** *e* **multiplicação**, *tal que os seguintes axiomas são satisfeitos:*

1. *$(R, +)$ é um grupo abeliano.*

2. *a multiplicação é associativa.*

3. *Para todo $a, b, c \in R$, a* **lei distributiva à esquerda**, *$a \cdot (b + c) = a \cdot b + a \cdot c$, e a* **lei distributiva à direita**, *$(a + b) \cdot c = a \cdot c + b \cdot c$, ocorrem.*

Denotaremos $(R, +, \cdot)$ por R. Se existe um elemento $1 \in R$ tal que $1 \cdot x = x \cdot 1 = x$, para todo $x \in R$, então R é dito um **anel com unidade** e, se a operação $\cdot$ é comutativa, R é dito **anel comutativo**. Ao longo do texto, por anel estaremos entendendo anel comutativo com unidade. Um **corpo** é um anel comutativo com unidade tal que todo elemento não nulo possui um inverso multiplicativo.

Definição 1.12. *Dados R, R' anéis, uma função $f : R \to R'$ é um* **homomorfismo de anéis** *se, para todos $a, b \in R$, $f(a+b) = f(a) + f(b)$ e $f(ab) = f(a)f(b)$. Se f é também bijetora, então f é um* **isomorfismo de anéis**. *A notação $R \simeq R'$ significa que existe um isomorfismo entre os anéis R e R' que são, assim, ditos isomorfos.*

Teorema 1.13. *Se K é um corpo finito, o conjunto $K^* = K - \{0\}$ é um grupo cíclico com a operação multiplicação de K.*

Definição 1.14. *Dado um anel comutativo com unidade R, um conjunto M é dito um* **R-módulo** *se M é um grupo abeliano e se existe uma função $\cdot : R \times M \to M$ satisfazendo, para todos $x, y \in R$, $m, n \in M$:*

1. $(x + y)m = xm + ym$.
2. $x(m + n) = xm + xn$.
3. $(xy)m = x(ym)$.
4. $1m = m$.

Definição 1.15. *Dados dois R-módulos M, M', uma função $f : M \to M'$ é um* **homomorfismo de R-módulos** *se é um homomorfismo de grupos aditivos que satisfaz $f(am) = af(m)$, para todos $a \in R$, $m \in M$. Se f é bijetora é chamada de* **isomorfismo** *de R-módulos.*

Definição 1.16. *Um* **ideal** *de um anel R (comutativo) é um subconjunto I de R, fechado para a soma de R e tal que, para todo $r \in R$, $x \in I$, $rx \in I$.*

Definição 1.17. *Dados I_1, I_2 ideais de um anel R, o ideal $I_1 + I_2$ é denotado por $I_1 \oplus I_2$ e dito* **soma direta** *de I_1 e I_2, se $I_1 \cap I_2 = \{0\}$.*

Definição 1.18. *Um ideal é dito* **indecomponível** *se é diferente de 0 e não pode ser escrito como soma direta de ideais não nulos.*

Definição 1.19. *Um* **domínio de integridade** *D é um anel comutativo com unidade sem divisores de zero, isto é, sem elementos não nulos a, b tais que $ab = 0$.*

Definição 1.20. *A* **característica** *de um anel R é o menor inteiro positivo tal que $nr = 0$, para todo $r \in R$. Se um tal inteiro não existe, dizemos que R tem característica 0.*

Denotaremos a característica de um anel por $char(R)$.

Teorema 1.21. *A característica de um domínio de integridade é 0 ou um número primo.*

Definição 1.22. *Um elemento e de um anel R é chamado* **idempotente** *se $e^2 = e$. Dois idempotentes e_1 e e_2 são chamados* **ortogonais** *se $e_1 \cdot e_2 = 0$. Um idempotente e é chamado* **primitivo** *se não existem e_1, e_2 idempotentes ortogonais não nulos tais que $e = e_1 + e_2$. Um conjunto de idempotentes de um anel com unidade $\{e_1, \cdots, e_n\}$ é um* **conjunto completo de idempotentes primitivos ortogonais** *se $e_1 + \cdots + e_n = 1$, cada e_i é primitivo e $e_i e_j = 0$, se $i \neq j$, para $1 \leq i, j \leq n$.*

Proposição 1.23. *Se $R = I_0 \oplus \cdots \oplus I_j$, I_k ideais de R, $1 \leq k \leq j$, então existem idempotentes ortogonais $e_0, \cdots, e_j$ tais que $1 = e_0 + \cdots + e_j$ e $e_k R = I_k$, para $1 \leq k \leq j$.*

Definição 1.24. *Um elemento a em um anel R é dito* **nilpotente** *se existe $n \in \mathbb{N}$ tal que $a^n = 0$. O menor inteiro positivo m tal que $a^m = 0$ é chamado* **índice de nilpotência** *de a em R.*

Definição 1.25. *Seja R um anel. O* **radical de Jacobson** *de R, denotado por $J(R)$, é a interseção de todos os ideais maximais de R.*

Definição 1.26. *Um anel R é dito* **local** *se possui um único ideal maximal.*

Teorema 1.27 (Lema de Nakayama)**.** *Seja R um anel e M um R-módulo finito e I um ideal de R. Suponha que $IM = M$. Então existe um elemento $a \in R$ da forma $a = 1 + x$, $x \in I$, tal que $aM = 0$. Se além disso $I \subset rad(R)$, então $M = 0$.*

Teorema 1.28. *([9], Proposição 7.14) Seja R anel comutativo e N um nil ideal em R, isto é, um ideal cujos seus elementos são todos nilpotentes, e seja $f = u + N$ um idempotente de $\bar{R} = \frac{R}{N}$. Então existe um único idempotente e em R tal que $f = \bar{e}$.*

Definição 1.29. *Um anel comutativo R é dito* **simples** *se R é não nulo e não possui ideais além de (0) e ele próprio.*

Definição 1.30. *Um anel R (comutativo) é dito* **semisimples** *se qualquer de seus ideais é um somando direto, isto é, se para qualquer ideal I de R, existe um ideal J de R tal que $R = I \oplus J$.*

Definição 1.31. *Um anel comutativo R é chamado* **anel de cadeia** *se o conjunto de todos os seus ideais forma uma cadeia com a relação de inclusão.*

Exemplo 1.32. *$R = \frac{\mathbb{Z}_p[x]}{\langle x^r \rangle}$ é um anel de cadeia, com a cadeia de ideais*

$$R = \langle 1 \rangle \supseteq \langle x \rangle \supseteq \cdots \supseteq \langle x^r \rangle = 0.$$

Teorema 1.33. *([4] Proposição 2.1) Para um anel finito R as seguintes condições são equivalentes:*

1. *R é um anel local e o ideal maximal M de R é principal, isto é, tem um conjunto gerador unitário.*
2. *R é um anel local de ideais principais.*
3. *R é um anel de cadeia.*

Dado um conjunto finito C, denotamos por $|C|$ a **cardinalidade** de C, isto é, a quantidade de elementos de C.

Temos o seguinte:

Teorema 1.34. *([4], Proposição 2.2) Seja 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 $\bar{R} = \frac{R}{M}$. Então:*

1. *Para algum primo q e inteiros positivos k e l, $(k \geq l)$, $|R| = q^k$, $\left|\bar{R}\right| = q^l$ e a característica de R e $\bar{R}$ são potências de q.*
2. *Para $i = 0, 1, \cdots, t$, $|a^i| = \left|\bar{R}\right|^{t-i}$. Em particular, $|R| = \left|\bar{R}\right|^t$, isto é, $k = lt$.*

Dado R um anel e G um grupo, podemos definir um novo conjunto, que denotamos por RG, cujos elementos são da forma $\sum_{g \in G} \alpha_g g$, com $\alpha_g \in R$.

Definição 1.35. *Dado um elemento* $\alpha = \sum_{g\in G} a_g g$ *de* RG*, o* **suporte** *de* α*, denotado por* $supp(\alpha)$ *é dado por*

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

Definição 1.36. *Dado* G *um grupo e* R *um anel, definimos um novo anel* RG *cujos elementos são combinações formais de suporte finito*

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

com soma dada por

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

e produto dado por

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

Um tal anel é chamado **anel de grupo**.

Dados dois elementos $\alpha = \sum_{g\in G} a_g g$ e $\beta = \sum_{g\in G} b_g g$ temos $\alpha = \beta$ se, e somente se, $a_g = b_g$, para todo $g \in G$.

Definição 1.37. *O homomorfismo*

$$\begin{aligned} \epsilon : RG &\to R \\ (\sum_{g\in G} a_g g) &\mapsto \sum_{g\in G} a_g \end{aligned}$$

é chamado **aplicação de aumento** *e seu núcleo, dado por* $Ker(\epsilon) = \{\sum_{g\in G} a_g(g-1) : g \in G, g \neq 1\}$*, é chamado* **ideal de aumento** *de* RG.

Um dos resultados básicos da teoria de anéis de grupo é o seguinte:

Teorema 1.38. *([14] Teorema 3.4.7)(Teorema de Maschke) Seja* G *um grupo. Então, o anel de grupo* RG *é semisimples se, e somente se, as seguintes condições ocorrem:*

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

Um caso de particular importância é o seguinte:

Corolário. *Seja G um grupo finito e K um corpo. Então KG é semisimples se, e somente se, $char(K)$ não divide $|G|$.*

Corolário. *Se G é um grupo abeliano e K é um corpo tal que $car(K)$ não divide $|G|$, então KG é isomorfo a uma soma direta de corpos.*

Vale o seguinte

Teorema 1.39. *([17], Teorema 2.1.3) Seja R um anel de cadeia finito, comutativo e com unidade, com $|R| = q^k$, $M = \langle a \rangle$ ideal maximal de R e t o índice de nilpotência de a em R. Seja $G = C_n$, em que q não divide n. Se I é um ideal de RGe_i, e_i idempotente primitivo, então I é da forma $I = \left\langle a^{k_j} e_i \right\rangle$, com $0 \leq k_j \leq t$.*

Proposição 1.40. *Se I é um ideal bilateral de um anel R e G é um grupo comutativo, então $IG = \{\sum_{g \in G} a_g g : a_g \in G\}$ é um ideal bilateral de RG e $\frac{RG}{IG} \simeq (\frac{R}{I})G$.*

Teorema 1.41. *([11], Teorema VII.8) Seja e um idempotente central não nulo de um anel RG. As seguintes condições são equivalentes:*

1. *e é primitivo.*
2. *RGe é um anel local.*
3. *RGe é indecomponível.*

Para um anel de grupo semisimples, sempre existe $\{e_1, e_2, ..., e_m\}$ um conjunto completo de idempotentes primitivos ortogonais de RG tal que

$$RG = RGe_1 \oplus RGe_2 \oplus \cdots \oplus RGe_m.$$

Para anéis locais, em particular para anéis de cadeia, vale o seguinte.

Teorema 1.42. *([17], Teorema 2.1.2) Sejam R um anel local com ideal maximal $M = \langle a \rangle$, com $|R| = q^k$ e G um grupo cíclico de ordem n, tal que q não divide n. Se $\{\bar{e_0}, \cdots, \bar{e_m}\}$ é um conjunto de idempotentes primitivos ortogonais de $\bar{R}G$, então $\{e_0, \cdots, e_m\}$ é um conjunto de idempotentes primitivos ortogonais de RG.*

Um último resultado estrutural sobre anéis de grupo é o seguinte.

Teorema 1.43. *([18] Proposição 1.3.1) Seja R um anel comutativo com unidade, G e H grupos. Então $R(G \times H) \simeq (RG)H$.*

Prova: Considere a função:

$$\varphi : R(G \times H) \to (RG)H$$
$$\sum_{g\in G, h\in H} \alpha_{(g,h)}(g,h) \mapsto \sum_{h\in H}(\sum_{g\in G} \alpha_{(g,h)}g)h$$

Temos que φ está bem definida. Vejamos que é um homomorfismo de anéis. Sejam $\alpha = \sum_{g\in G, h\in H} \alpha_{(g,h)}(g,h)$ e $\beta = \sum_{g\in G, h\in H} \beta_{(g,h)}(g,h) \in R(G \times H)$, Então $\alpha + \beta = \sum_{g\in G, h\in H} (\alpha_{(g,h)} + \beta_{(g,h)})(g,h)$ bem como $\alpha\beta = \sum_{g_1,g_2\in G, h_1,h_2\in H} \alpha_{(g_1,h_1)}\beta_{(g_2,h_2)}(g_1g_2, h_1h_2)$. Logo,

$$\varphi(\alpha+\beta) = \sum_{h\in H}(\sum_{g\in G}(\alpha_{(g,h)} + \beta_{(g,h)})g)h = \sum_{h\in H}(\sum_{g\in G}\alpha_{(g,h)}g)h + \sum_{h\in H}(\sum_{g\in G}\alpha_{(g,h)}g)h$$
$$= \varphi(\alpha) + \varphi(\beta).$$

Também

$$\varphi(\alpha\beta) = \sum_{h_1,h_2\in H}(\sum_{g\in G}\alpha_{(g_1,h_1)}\beta_{(g_2,h_2)}g_1g_2)h_1h_2.$$

Por outro lado,

$$\varphi(\alpha)\varphi(\beta) = [\sum_{h\in H}(\sum_{g\in G}\alpha_{(g,h)}g)h][\sum_{h\in H}(\sum_{g\in G}\beta_{(g,h)}g)h] = \sum_{h_1,h_2\in H}(\sum_{g\in G}\alpha_{(g_1,h_1)}\beta_{(g_2,h_2)}g_1g_2)h_1h_2.$$

Donde $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$. Além disso, φ é injetora, pois se $\alpha \sum_{g\in G, h\in H} \alpha_{(g,h)}(g,h) \in R(G\times H)$ é tal que $\varphi(\alpha) = \sum_{h\in H}(\sum_{g\in G}\alpha_{(g,h)}g)h = 0$, como H gera $(RG)H$ sobre RG então $\sum_{g\in G}\alpha_{(g,h)}g = 0$, para todo $h \in H$ e, portanto, $\alpha_{(g,h)} = 0$, para todos $g \in G$, $h \in H$ e, assim, $\alpha = 0$. Por fim, φ é sobrejetora, pois se $y \in (RG)H$, $y = \sum_{h\in H}\alpha_h h$. Como cada $\alpha_h \in RG$, então $\alpha_h = \sum_{g\in G}(\alpha_{(g,h)})g$. Tomando $\alpha = \sum_{g\in G, h\in H}\alpha_{(g,h)}(g,h) \in R(G\times H)$, obtemos $\varphi(\alpha) = y$. □

1.3 Códigos

Seja A um conjunto finito, ao qual chamaremos **alfabeto**.

Definição 1.44. *Um* **código de comprimento** n *é um subconjunto próprio de* A^n. *Os elementos de um código serão chamados as* **palavras** *do código.*

Definição 1.45. *Sendo* $|A|= s$, *e tomando um código em* A^n *com* M *palavras, a* **taxa de informação** *de um código é dada por* $R = \frac{log_s M}{n}$.

Com o objetivo de medir a distância entre dois elementos do código, definimos:

Definição 1.46. *Dado* $x = (x_1, ..., x_n)$ *e* $y = (y_1, ..., y_n)$ *dois elementos de* A^n, *a* **distância de Hamming** *d(x,y) entre* x *e* y *é o número de posições nas quais* x *e* y *diferem, isto é,*

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

Note que a distância de Hamming é de fato uma distância, isto é, satisfaz os três axiomas de distância.

A **distância mínima** de um código $\mathcal{C} \subset A^n$ é o inteiro

$$d(\mathcal{C}) = min\{d(x, y); x, y \in A^n, x \neq y\}.$$

Dado um alfabeto A, com $|A|= q$, q potência de um número primo, o número máximo de palavras de um código de comprimento n e distância mínima d é denotado por $A_q(n, d)$. Um código sobre A^n de distância mínima d contendo $A_q(n, d)$ palavras é chamado um **código ótimo**. É objeto de estudo na Teoria de Códigos limitantes superiores e inferiores para $A_q(n, d)$. Alguns desses limitantes são:

Teorema 1.47. *([15], Teorema 4.5.6) Limitante de Singleton:* $A_q(n, d) = q^{n-d+1}$.

Teorema 1.48. *([15], Teorema 4.5.4) Limitante de Gilbert-Varshamov:* $A_q(n, d) = \dfrac{q^n}{\sum_{l=0}^{d-1} \binom{n}{k} (q-1)^k}$.

A classe de códigos que será alvo de nosso estudo é a seguinte:

Definição 1.49. *Dado R um anel finito, um subconjunto próprio C de R^n é chamado* **código linear de comprimento** *n sobre R se C é um R-submódulo de R^n.*

Definição 1.50. *Dado $\alpha = (\alpha_1, ..., \alpha_n) \in R^n$, o* **peso** *de α é dado por*

$$w(\alpha) = |\{i; \alpha_i \neq 0, 1 \leq i \leq n\}|.$$

O **peso mínimo** de um código C é o inteiro

$$w(C) = min\{w(\alpha); \alpha \in C \setminus \{0\}\}.$$

Observe que o peso mínimo em um código linear é equivalente à distância mínima.

Definição 1.51. *Um código linear não nulo $\mathcal{C}$ de R^n é dito* **irredutível** *se não existe código não nulo $\mathcal{C}_0$ de R^n contido propriamente em $\mathcal{C}$.*

A classe de códigos lineares com a qual mais trabalharemos será:

Definição 1.52. *Um* **código de peso constante** *é um código tal que todos os seus elementos não nulos têm mesmo peso.*

Outro tipo de código linear é o seguinte:

Definição 1.53. *Um código linear C é dito* **código cíclico** *se, para toda palavra $\alpha = (\alpha_1, ..., \alpha_n) \in C$, a palavra $(\alpha_n, \alpha_1, ..., \alpha_{n-1})$ está em C.*

Quando as palavras do código são vistas como polinômios, temos que um código C é cíclico se é um ideal de

$$R_n = \frac{\mathcal{F}_q[x]}{\langle x^n - 1 \rangle}.$$

Usando essa linguagem polinomial, temos o seguinte resultado.

Teorema 1.54. *([15], Teorema 7.4.1) Seja C um ideal em R_n.*

1. *Existe um único polinômio mônico $g(x)$ de grau mínimo em C. Este polinômio gera C, isto é, $C = \langle g(x) \rangle$, e é chamado* **polinômio gerador** *de C.*

2. *O polinômio gerador divide $x^n - 1$ e, reciprocamente, se $p(x) \in R_n$ divide $x^n - 1$, então $p(x)$ gera um código cíclico.*

3. Se $gr(g(x)) = r$, então C tem dimensão $n - r$.

Como o polinômio gerador $g(x)$ divide $x^n - 1$, então existe um polinômio $h(x)$ tal que

$$x^n - 1 = g(x)h(x).$$

Tal polinômio $h(x)$ é chamado **polinômio de checagem** de C.

Definição 1.55. *Um polinômio $e(x) \in R_n$ é dito* **idempotente** *em R_n se $e^2(x) = e(x)$.*

Teorema 1.56. *([15], Teorema 7.4.9) Seja C um código cíclico em R_n com polinômio gerador $g(x)$ e polinômio de checagem $h(x)$, com $mdc(charR, n) = 1$. Então $g(x)$ e $h(x)$ são relativamente primos e, portanto, existem polinômios $a(x)$ e $b(x)$ para os quais*

$$a(x)g(x) + b(x)h(x) = 1.$$

O polinômio $e(x) = a(x)g(x)mod(x^n - 1)$ tem por propriedades:

1. *$e(x)$ é o único polinômio unidade em C, isto é, $p(x)e(x) = p(x)$, para todo $p(x) \in C$.*

2. *$e(x)$ é o único polinômio em C que é idempotente e gera C.*

Dado RG anel de grupo, com G um grupo cíclico de n elementos gerado por g, um código C de R^n é cíclico se, e somente se, $\varphi(C)$ é um ideal de RG, com

$$\varphi : R^n \to RG$$

$$\alpha = (a_0, ..., a_{n-1}) \mapsto a_0 + a_1 g + ... + a_{n-1} g^{n-1}$$

um isomorfismo de R-módulos. De fato, supondo C código de R^n, usando o fato de ser φ isomorfismo de R-módulos, basta provar que, dado $\beta = (a_0, ..., a_{n-1}) \in C$, $g\varphi(\beta)$ está em $\varphi(C)$. Agora $g\varphi(\beta) = a_{n-1} + a_0 g + ... + a_{n-2} g^{n-1}$. Como C é cíclico, $(a_{n-1}, a_0, ..., a_{n-2}) \in C$, donde $g\varphi(\beta) = \varphi(a_{n-1}, a_0, ..., a_{n-2}) \in \varphi(C)$ e, portanto, $\varphi(C)$ é ideal de RG.

Reciprocamente, suponha $\varphi(C)$ ideal de RG. Dado então $\beta = (a_0, ..., a_{n-1}) \in C$, $g\varphi(\beta) \in \varphi(C)$, isto é, $a_{n-1} + a_0 g + ... + a_{n-2} g^{n-1} = \varphi(a_{n-1}, a_0, ..., a_{n-2}) \in \varphi(C)$, donde $(a_{n-1}, a_0, ..., a_{n-2}) \in C$ e C é cíclico.

Como podemos ver um código cíclico como um ideal de R_n, podemos associar um ideal de RG, G grupo cíclico com n elementos gerado por g, com um código cíclico de R_n, associando g a x. Com isso, podemos associar o polinômio gerador $g(x)$, bem como o idempotente $e(x)$, a um gerador de um ideal de RG, bem como a um idempotente e de RG.

Um último resultado que gostaríamos de mencionar será muito importante no capítulo seguinte e por isso apresentaremos sua demonstração. É um resultado bastante conhecido da teoria de códigos e diz o seguinte:

Teorema 1.57. *Seja $G = \{g_1, \cdots, g_n\}$ grupo abeliano de n elementos, $\mathcal{F}_q$ corpo de q elementos e $\mathcal{C}$ código não nulo de $\mathcal{F}_qG$ de dimensão k. Então a soma dos pesos dos elementos de $\mathcal{C}$ é*

$$\sum_{\alpha \in \mathcal{C}} w(\alpha) = n(q-1)q^{k-1}.$$

Prova: Seja $\alpha = \sum_{i=1}^{n} a_i(\alpha) g_i$ um elemento não nulo de $\mathcal{C}$. Então existe algum j, $1 \leq j \leq n$, tal que $a_j(\alpha) = m \neq 0$. Neste caso, tomando $g_j^{-1}\alpha \in \mathcal{C}$, neste elemento $a_j(\alpha)$ será o coeficiente de 1. Também, para todo j_0, $1 \leq j_0 \leq n$, tomando o elemento $g_{j_0} g_j^{-1}\alpha \in \mathcal{C}$, nele $a_j(\alpha)$ será o coeficiente de g_{j_0}. Assim, dado um j_0, existe $\beta \in \mathcal{C}$ tal que $a_{j_o}(\beta) \neq 0$. Mais ainda, se $m \in \mathcal{F}_q$, $a_{j_0}(m(a_{j_0}(\alpha))^{-1}\alpha) = m$, isto é, para todo $m \in \mathcal{F}_q$, $m \neq 0$, existe $\beta \in \mathcal{C}$ tal que $a_{j_0}(\beta) = m$. Com isso, fixado $\alpha \in \mathcal{C}$ tal que $a_{j_0}(\alpha) = m$, existe uma bijeção

$$\begin{array}{ccc} \{\beta \in \mathcal{C} | a_{j_0}(\beta) = m \in \mathcal{F}_q^*\} & \longleftrightarrow & \{\beta \in \mathcal{C} | a_{j_0}(\beta) = 0\} \\ \beta & \mapsto & \beta - \alpha. \end{array}$$

E assim $\left|\{\beta \in \mathcal{C} | a_{j_0}(\beta) = m \in \mathcal{F}_q^*\}\right| = |\{\beta \in \mathcal{C} | a_{j_0}(\beta) = 0\}|$. Observe ainda que os conjuntos $\{\beta \in \mathcal{C} / a_{j_0}(\beta) = m \in \mathcal{F}_q\}$ são disjuntos para valores distintos de m. Portanto, $\mathcal{C} = \dot{\bigcup}_{m \in \mathcal{F}_q} \{\beta | a_j(\beta) = m\}$, conjuntos estes todos de mesma cardinalidade. E uma vez que $|\mathcal{C}| = q^k$, obtemos $\left|\{\beta \in \mathcal{C} | a_{j_0}(\beta) = m \in \mathcal{F}_q^*\}\right| = \frac{q^k}{q} = q^{k-1}$.

Observado isso, vejamos qual é a soma dos pesos dos elementos de $\mathcal{C}$. Dado $\alpha \in \mathcal{C}$,

$w(\alpha) = |\{j|a_j(\alpha) \neq 0\}|$, então

$$\begin{aligned}\sum_{\alpha\in\mathcal{C}} w(\alpha) &= \sum_{\alpha\in\mathcal{C}} |\{j|a_j(\alpha) \neq 0\}| \\ &= \sum_{m\in\mathcal{F}_q^*} \sum_{\alpha\in\mathcal{C}} |\{j|a_j(\alpha) = m\}| \\ &= \sum_{1\leq j\leq n} \sum_{m\in\mathcal{F}_q^*} |\{\alpha \in \mathcal{C}|a_j(\alpha) = m\}| \\ &= n(q-1)q^{k-1}.\end{aligned}$$

□

Para finalizar o capítulo, daremos duas definições que serão usadas ao longo do texto:

Definição 1.58. *A* **função φ de Euler**, *definida no conjunto dos números naturais, para cada $x \in \mathbb{N}$ é dada por:*

$$\varphi(x) = |\{n \in \mathbb{N}|n < x|mdc(n, x) = 1\}|, x > 1$$

$$e\ \varphi(1) = 1$$

Definição 1.59. *O* **delta de Kronecker** *é a notação δ_{ij} definida por:*

$$\delta_{ij} = \begin{cases} 1, & se\ i = j \\ 0, & se\ i \neq j \end{cases}$$

Capítulo 2

Códigos Cíclicos de Peso Constante

Neste capítulo apresentaremos condições que garantam que certos códigos cíclicos tenham peso constante baseados nos resultados de [19], mas fazendo uso aqui da Teoria de Anéis de Grupos, ao contrário do que é feito no artigo de Vega [19], no qual é utilizada a linguagem polinomial, sobretudo técnicas de sequências de recorrência linear. A vantagem é que, além da demonstração ter se tornado mais simples, o resultado se tornou mais geral. Os resultados serão obtidos em anéis de grupo da forma $\mathcal{F}_qG$, com $\mathcal{F}_q$ um corpo finito de q elementos, e C_n um grupo cíclico com n elementos tal que $mdc(q,n)=1$.

2.1 Quando o código tem peso constante

Nesta seção iremos generalizar um dos resultados de [19], em que o autor usou como ferramentas propriedades polinomiais. Trabalharemos aqui com códigos cíclicos vistos como ideais de anéis de grupos.

Sobre as hipóteses estabelecidas na introdução do capítulo o anel de grupo $\mathcal{F}_qG$ é semissimples. Dado H um subgrupo de G, denotaremos por $\hat{H}$ o elemento $\frac{1}{|H|}\sum_{h\in H} h \in G$. Observe que tal elemento é um idempotente.

De acordo com [2], temos a seguinte definição:

Definição 2.1. *([2],Definição 2.2) Um idempotente primitivo e em $\mathcal{F}_qG$ é dito* **essencial** *se $e\hat{H}=0$, para todo $H\neq 1$, H subgrupo de G.*

Seja e um idempotente primitivo em $\mathcal{F}_qG$ não essencial. Considere $\mathcal{H}_e = \{H < G; \hat{H}e = e\}$. Note que $\widehat{H_1H_2} = \hat{H}_1\hat{H}_2$, donde se H_1, $H_2 \in \mathcal{H}_e$, $\widehat{H_1H_2}e = e$.

Seja $H_e := \prod_{H\in\mathcal{H}_e} H$. Então $H_e \in \mathcal{H}_e$, e é o maior subgrupo H de G tal que $e\hat{H} = e$.

Dado um idempotente k, ou $ek = 0$ ou $ek = e$. De fato, se $ek = j \neq 0$, então j seria idempotente, e $ej = eek = j$. Daí, $e = e - j + j$, com $(e-j)(e-j) = e - 2j + j = e - j$, e $(e-j)j = j - j = 0$, contradizendo o fato de ser e primitivo. Assim, se $K \not\subseteq H_e$, $e\hat{K} = 0$, pois senão, como $\widehat{KH_e}$ é idempotente, $e = e\hat{K} = e\widehat{KH_e}$, o que seria uma contradição com a maximalidade de H_e. Disto $e\hat{K} = e$ se, e somente se, $K \subseteq H_e$.

Como visto em [2], Observação 2.1 e Proposição 3.3, temos:

Lema 2.2. *Seja e um idempotente primitivo de $\mathcal{F}_qG$ e H_e como definido acima. A função:*

$$\Psi : \mathcal{F}_qG\hat{H}_e \to \mathcal{F}_q\left(\frac{G}{H_e}\right)$$
$$g\hat{H}_e \mapsto \bar{g}$$
$$\sum_{g\in G}\alpha_g g\hat{H}_e \mapsto \sum_{g\in G}\alpha_g\bar{g}$$

é um isomorfismo de anéis, com $\Psi(e)$ idempotente essencial.

Prova: De fato, temos primeiramente $\frac{G}{H_e} \simeq Ge$, pois a aplicação $\phi : G \to Ge$, dada por $g \mapsto ge$ é homomorfismo sobrejetor de grupos com $Ker(\phi) = H_e$, pois se $h \in H_e$, $he = h\hat{H}_e e = \hat{H}_e e = e$, e se $ae = e$, $\langle a\rangle \subset H_e$. Como Ge gera RGe sobre R segue que Ψ é isomorfismo de anéis. Como $e\hat{H}_e = e$, $e \in \mathcal{F}_qG\hat{H}_e$.

Seja $L < \frac{G}{H_e}$. Então $L = \frac{L'}{H_e}$, para algum L' subgrupo de G tal que $H_e \subseteq L' \subseteq G$. Suponha $L \neq 1$, o que ocorre se, e somente se $L' \neq H_e$. Analisemos $\Psi(e)\hat{L} = \Psi(e\hat{L'})$. Se $L' \supset H_e$, $\hat{L'}\hat{H}_e = \hat{L'} \mapsto \frac{1}{|L'|}\sum_{h\in L/H_e}\bar{h}$. Como temos $|H_e|$ cópias de $\bar{h}$ em $\frac{G}{H_e}$, então

$$\Psi(\hat{L'}) = \frac{|H_e|}{|L'|}\sum_{\bar{h}\in L'/H_e}\bar{h} = \frac{1}{\left|\frac{L'}{H_e}\right|}\sum_{\bar{h}\in\frac{L'}{H_e}}\bar{h}$$

donde

$$\Psi(e)\hat{L} = \Psi(e)(\widehat{\frac{L}{H_e}}) = \Psi(e)\Psi(\hat{L'}) = \Psi(e\hat{L'}) = 0$$

pois L' não está contido em H_e e portanto $\Psi(e)$ é um idempotente primitivo essencial de $\mathcal{F}_q(\frac{G}{H_e})$. □

Lema 2.3. *([2], Proposição 2.3) Seja e um idempotente primitivo em $\mathcal{F}_qG$, para G um grupo abeliano finito. Então e é essencial se, e somente se $G \simeq Ge$ via o homomorfismo de grupos*

$$\pi : G \to Ge$$

$$g \mapsto ge.$$

Prova: O homomorfismo de grupos π é claramente sobrejetor. Suponha e não essencial. Então existe $H \neq 1$ subgrupo de G tal que $e\hat{H} = e$. Seja $h \in H$, $h \neq 1$. Então $he = h\hat{H}e = \hat{H}e = e$ e, portanto, $\pi(h) = e$, donde π não é injetora, não sendo assim isomorfismo. Por outro lado se π não é isomorfismo, ou seja, se π não é injetora, então existe $h \neq 1 \in G$ tal que $\pi(h) = e$, donde, para todo i, $h^ie = e$ e, portanto, para $H = \langle h \rangle$, $e\hat{H} = e$, e e não é essencial. □

No artigo de Vega [19], é muito usada a noção de ordem e quase ordem de um polinômio, definições essas que podem ser encontradas em [10]. Comecemos discutindo o equivalente da definição de ordem na linguagem de anéis de grupo.

Definição 2.4. *Assuma $C_n =< g >$ o grupo cíclico com n elementos, $\mathcal{F}_q$ corpo finito com q elementos e e um idempotente primitivo em $\mathcal{F}_qC_n$. A* **ordem de** *ge, que denotaremos por $o(ge)$, é o menor m inteiro positivo tal que $(ge)^m = 1$, isto é, é a ordem de ge em C_ne. Observe que a ordem de ge é igual a ordem de $p(x)$, em que $p(x)$ é polinômio irredutível de $\mathcal{F}_q[x]$ tal que $\mathcal{F}_qC_ne \simeq \frac{\mathcal{F}_q[x]}{\langle p(x) \rangle}$, $p(x)$ dividindo $x^n - 1$.*

Vejamos agora o que é a quase ordem na linguagem de anéis de grupos.

Sabemos que, tomando e idempotente primitivo em $\mathcal{F}_qC_n$, $\mathcal{F}_qC_ne$ é um corpo. Considere os conjuntos $\mathcal{F}_q^*e$ e C_ne. Ambos são subgrupos de $(\mathcal{F}_qC_ne)^* = U(\mathcal{F}_qC_ne)$, donde $C_ne \cap \mathcal{F}_qe \subseteq U(\mathcal{F}_qC_ne)$. Pelo Teorema1.10, $\left|C_ne \cap \mathcal{F}_q^*e\right| = mdc(o(ge), q-1)$. Mas o único subgrupo cíclico de C_ne de ordem $mdc(o(ge), q-1)$ é $\left\langle (ge)^{o(ge)/mdc(o(ge),q-1)} \right\rangle$, donde $C_ne \cap \mathcal{F}_q^*e = \left\langle (ge)^{o(ge)/mdc(o(ge),q-1)} \right\rangle$ e, portanto, $(ge)^{o(ge)/mdc(o(ge),q-1)} \in \mathcal{F}_qe$, digamos $(ge)^{(o(ge)/mdc(o(ge),q-1)} = ke$, $k \in \mathcal{F}_q^*$. E $o(ge)/mdc(o(ge), q-1)$ é o menor inteiro λ tal que $(ge)^\lambda \in \mathcal{F}_q^*e$. Com isso, temos:

Definição 2.5. *Com a notação acima, a* **quase ordem de** *ge, que denotaremos por $qord(ge)$, é dada por $qord(ge) = \frac{o(ge)}{mdc(o(ge),q-1)}$.*

Antes do nosso principal resultado desta seção, façamos um último resultado sobre um código em $\mathcal{F}_qC_n$:

Lema 2.6. *Se $\mathcal{C}$ é um código de $\mathcal{F}_qC_n$ de peso constante, então $\mathcal{C}$ é irredutível.*

Prova: *Tome $\mathcal{C}$ um código de $\mathcal{F}_qC_n$ de peso constante e suponha que ele não seja irredutível. Seja $\mathcal{C}_0 \neq 0$ um código contido em $\mathcal{C}$ e diferente de $\mathcal{C}$. Suponha $dim_{\mathcal{F}_q}\mathcal{C} = k$, e $dim\mathcal{F}_q\mathcal{C}_0 = k_0$. Então $k_0 < k$. Se $\mathcal{C}$ tem peso constante, dado $0 \neq \alpha \in \mathcal{C}$, usando a fórmula de soma de pesos, e sabendo que existem $q^k - 1$ elementos não nulos em $\mathcal{C}$, concluímos que $\omega(\alpha) = \frac{q^{k-1}(q-1)n}{q^k-1}$. Como $\mathcal{C}_0$ também terá peso constante, então, para $\alpha \in \mathcal{C}_0$, $\omega(\alpha) = \frac{q^{k_0-1}(q-1)n}{q^{k_0}-1}$. Assim, fixando $0 \neq \alpha \in \mathcal{C}_0 \subset \mathcal{C}$, $\frac{q^{k-1}(q-1)n}{q^k-1} = \omega(\alpha) = \frac{q^{k_0-1}(q-1)n}{q^{k_0}-1}$, o que é absurdo, uma vez que manipulando a igualdade acima concluiríamos que $q^k = q^{k_0}$, o que não ocorre uma vez que $k \neq k_0$, e, portanto, o código deve ser irredutível.* □

Sendo assim, para determinar os códigos de peso constante em $\mathcal{F}_qC_n$, basta que analisemos seus códigos irredutíveis. Temos então:

Teorema 2.7. *Sejam $\mathcal{F}_q$ corpo com q elementos, n um inteiro positivo com $mdc(q,n) = 1$, $C_n =< g >$ grupo cíclico com n elementos e $\mathcal{F}_qC_n$ o anel de grupo de C_n sobre $\mathcal{F}_q$. Considere e um idempotente primitivo de $\mathcal{F}_qC_n$ e $\mathcal{C} = \mathcal{F}_qC_ne$ o respectivo código irredutível. Seja $dim_{\mathcal{F}_q}\mathcal{C} = k$. São equivalentes:*

1. *$\mathcal{C}$ tem peso constante;*
2. *Todo elemento não nulo de $\mathcal{C}$ tem peso $\frac{q^{k-1}(q-1)n}{q^k-1}$;*
3. *Existe um elemento de $\mathcal{C}$ cujo peso é $\frac{q^{k-1}(q-1)n}{q^k-1}$;*
4. *$(\mathcal{F}_qC_ne)^* = \mathcal{F}_q^*eC_ne$.*

Prova: *($1 \implies 2$): Segue do fato que para um código abeliano $\mathcal{C}$ nas condições do teorema vale, pelo Teorema 1.57, a seguinte fórmula de soma de pesos:*

$$\sum_{\alpha\in\mathcal{C}} \omega(\alpha) = q^{k-1}(q-1)n$$

e do fato que existem $q^k - 1$ elementos não nulos no código.

(2 $\Longrightarrow$ 3) Imediata.

(3 $\Longrightarrow$ 4) Assuma inicialmente e essencial. Neste caso, $|C_n e| = n$*, de acordo com o Lema 2.3. Pelo Lema 1.10,* $\left|C_n e \cap \mathcal{F}_q^* e\right| = mdc(|C_n e|, \left|\mathcal{F}_q^* e\right|)$*, bem como* $\left|C_n e \mathcal{F}_q^* e\right| = mmc(|C_n e|, \left|\mathcal{F}_q^* e\right|)$*. Seja* $\mu = mdc(|C_n e|, \left|\mathcal{F}_q^* e\right|)$*, e* $t = n/\mu$*. Só há um subgrupo de ordem* μ *em* $(\mathcal{F}_q C_n e)^*$*, que é* $\langle g^t e\rangle$*. Como* $C_n e \cap \mathcal{F}_q^* e$ *também tem tal ordem, então* $C_n e \cap \mathcal{F}_q^* e = \langle g^t e\rangle$*. Logo* $g^t e = \lambda e$*, para algum* $\lambda \in \mathcal{F}_q^*$*. Seja* α *o elemento de peso* $\frac{q^{k-1}(q-1)n}{q^k-1}$*. Como* e *é a unidade de* $\mathcal{F}_q C_n e$*,* $g^t\alpha = g^t e\alpha = \lambda e\alpha = \lambda\alpha$*. Como*

$$\alpha = \alpha_0 + \alpha_1 g + ... + \alpha_{n-1} g^{n-1},$$

temos

$$\alpha g^t = \alpha_0 g^t + \alpha_1 g^{t+1} + ... + \alpha_{n-t} + \alpha_{n-t+1} g + ... + \alpha_{n-1} g^{n+t-1} = \lambda\alpha.$$

Disto $\alpha_0 = \alpha_t\lambda$*, bem como* $\alpha_t = \alpha_{2t}\lambda$*, isto é,* $\alpha_{2t} = \alpha_t\lambda^{-1} = \alpha_0\lambda^{-2}$ *e, de um modo geral,* $\alpha_{i+kt} = \alpha_i\lambda^{-k}$*, para todos* $0 \leq i \leq t-1, 0 \leq k \leq \mu - 1$*.*

Considere $\beta = \alpha_0 + \alpha_1 g + ... + \alpha_{t-1} g^{t-1}$*. Então*

$$\begin{aligned} \alpha &= \beta + \lambda^{-1}\beta g^t + \lambda^{-2}\beta g^{2t} + ... + \lambda^{-(\mu-1)}\beta g^{(\mu-1)t} \\ &= \sum_{i=1}^{\mu-1} \lambda^{-i} g^{it}\beta. \end{aligned}$$

com $supp(\lambda^{-i}g^{it}\beta) \cap supp(\lambda^{-j}g^{jt}\beta) = \emptyset$*, se* $i \neq j$*. Disto*

$$\omega(\alpha) = \omega(\beta) + ... + \omega(\lambda^{\mu-1}\beta g^{(\mu-1)t}) = \mu\omega(\beta)$$

e, assim, $\mu = mdc(|C_n e|, \left|\mathcal{F}_q^* e\right|)$ *divide* $\frac{q^{k-1}(q-1)n}{q^k-1}$*, isto é,* $mdc(n, q-1)$ *divide* $\frac{q^{k-1}(q-1)n}{q^k-1}$*. Como* $mdc(q^{k-1}, mdc(n, q-1)) = 1$*, pois por hipótese* $mdc(n, q) = 1$*, segue que* $mdc(n, q-1)$ *divide* $\frac{(q-1)n}{q^k-1}$ *e, portanto,* $q^k - 1$ *divide* $\frac{(q-1)n}{mdc(n,q-1)} = mmc(q-1, n) = \left|\mathcal{F}_q^* e C_n e\right|$*, isto é,* $|(\mathcal{F}_q C_n e)^*|$ *divide* $\left|\mathcal{F}_q^* e C_n e\right|$*. Como* $\mathcal{F}_q^* e C_n e$ *é subgrupo de* $(\mathcal{F}_q C_n e)^*$*, então* $(\mathcal{F}_q C_n e)^* = \mathcal{F}_q^* e C_n e$*. Isto termina o caso em que* e *é essencial.*

Suponha agora e *não essencial. Tome então* H_e *o maior subgrupo de* C_n *tal que* $eH_e = e$*. Como vimos anteriormente* $\mathcal{F}_q C_n \hat{H}_e \simeq \mathcal{F}_q \frac{C_n}{H_e}$ *via o isomorfismo* ψ *tal que* $\Psi(g\hat{H}_e) = \bar{g}$*. Considere* $|H_e| = d_1$*,* $\left|\frac{C_n}{H_e}\right| = d_2$*, com* $H_e = \left\langle g^{d_2}\right\rangle$*. Seja* $\alpha \in \mathcal{F}_q C_n \hat{H}_e$ *de peso* $\frac{q^{k-1}(q-1)n}{q^k-1}$*. Então, como* $\alpha\hat{H}_e = \alpha$*, como antes, temos*

$$\begin{aligned} \alpha &= (\alpha_0 + \alpha_1 g + ... + \alpha_{d_2-1} g^{d_2-1}) + \alpha_0 g^{d_2} + \cdots \\ &= (\alpha_0 + \alpha_1 g + ... + \alpha_{d_2-1} g^{d_2-1})\hat{H}_e, \end{aligned}$$

e assim

$$\omega(\alpha) = \omega(\alpha_0 + \alpha_1 g + ... + \alpha_{d_2-1} g^{d_2-1}) \left|H_e\right|.$$

Agora

$$\Psi(\alpha) = \alpha_0 + \alpha_1 \bar{g} + ... + \alpha_{d_2-1} \bar{g}^{d_2-1},$$

logo $\omega(\Psi(\alpha)) = \frac{\omega(\alpha)}{d_1}$, *e daí* $\omega(\Psi(\alpha)) = \left(\frac{q^{k-1}(q-1)n}{q^k-1}\right)/d_1 = \frac{q^{k-1}(q-1)d_2}{q^k-1}$, *com* $d_2 = \left|\frac{C_n}{H_e}\right|$. *Em* $\mathcal{F}_q \frac{C_n}{H_e}\Psi(e)$, $\Psi(e)$ *é essencial e, neste caso,* $\mathcal{F}_q^*\Psi(e)\frac{C_n}{H_e}\Psi(e) = (\mathcal{F}_q \frac{C_n}{H_e}\Psi(e))^*$. *Deste fato, um elemento qualquer é da forma* $\lambda\bar{g}^i\Psi(e)$, *logo, voltando pela* Ψ^{-1} *(pois* Ψ *é isomorfismo), segue que os elementos de* $(\mathcal{F}_q C_n e)^*$ *são da forma* $\lambda g^i e$ *e temos o resultado também neste caso.*

($4 \Longrightarrow 1$*): Como* $(\mathcal{F}_q C_n e)^* = \mathcal{F}_q^* e C_n e$, *os elementos não nulos de* $\mathcal{F}_q C_n e$ *são da forma* $\lambda g^i e$, *com* $\lambda \in \mathcal{F}_q^*$, *donde todos têm o mesmo peso.* □

Uma consequência imediata deste resultado é o seguinte:

Corolário 2.8. *Se* $\mathcal{C}$ *é um código de* $\mathcal{F}_q C_n$ *(com* $mdc(n,q) = 1$*), então* $\mathcal{C}$ *tem peso constante se, e somente se,* $\mathcal{C} = \{0\} \cup \{kg^i e | k \in \mathcal{F}_q^*, g^i \in C_n\}$.

Prova: *Do teorema anterior, um código de* $\mathcal{F}_q C_n$ *tem peso constante se, e somente se,* $(\mathcal{F}_q C_n e)^* = \mathcal{F}_q^* e C_n e$, *isto é, se, e somente se,* $\mathcal{C} = \{0\} \cup \{kg^i e | k \in \mathcal{F}_q^*, g^i \in C_n\}$. □

A partir do teorema obtemos o seguinte resultado encontrado no artigo de Vega em [19].

Corolário 2.9 ([19], Teorema 9)**.** *Seja* $\mathcal{F}_q$ *um corpo com* q *elementos,* $n = \lambda\frac{q^k-1}{q-1}$, *com* λ *dividindo* $(q-1)$, *e* $\mathcal{C}$ *um código cíclico sobre* $\mathcal{F}_q$ *de comprimento* n *e dimensão* k, *gerado por* $g(x)$ *e com polinômio de checagem* $h(x)$. *Então* $qord(ge) = \frac{q^k-1}{q-1}$ *se, e somente se,* $w(ge) = \lambda(q^{k-1})$.

Prova: *De fato,* $qord(h(x)) = \frac{o(ge)}{mdc(o(ge),q-1)}$ *é igual a* $\frac{q^k-1}{q-1}$ *se, e somente se* $\frac{o(ge)(q-1)}{mdc(o(ge),q-1)} = q^k - 1$, *isto é, se, e somente se,* $(\mathcal{F}_q C_n e) = \mathcal{F}_q^* e C_n e$, *o que ocorre de acordo com o Teorema 2.7 se, e somente se,* $\mathcal{C}$ *tem peso constante. Assim, isto ocorre se, e somente se,* $\omega(ge) = \frac{q^{k-1}(q-1)n}{q^k-1}$. *Como* $\lambda = \frac{n(q-1)}{q^k-1}$, *isso ocorre se, e somente se,* $\omega(ge) = \lambda(q^{k-1})$. □

2.2 Quantidade de códigos de peso constante

Agora que já sabemos quais são os códigos de peso constante, nosso objetivo aqui é determinar a quantidade de códigos de peso constante de dimensão k e comprimento n em $\mathcal{F}_qC_n$, $C_n = \langle g \rangle$ grupo cíclico de n elementos com $mdc(n,q) = 1$, usando para isso o Teorema 2.7, bem como propriedades de idempotentes essenciais encontradas em [2], generalizando assim o Teorema 12 de [19] . Para isso, começaremos com uma análise dos idempotentes primitivos de $\mathcal{F}_qC_n$.

Seja $n = p_1^{r_1}p_2^{r_2}\cdots p_t^{r_t}$. Então $C_n = P_1 \times \cdots P_t$, em que P_i é o p_i-Sylow de C_n. Como C_n é cíclico, seus subgrupos são cíclicos e, em particular, cada P_i é cíclico, donde existe K_i subgrupo minimal de P_i, para cada i, $1 \leq i \leq t$. Então

$$e_0 = (1 - \hat{K_1})(1 - \hat{K_2})\cdots(1 - \hat{K_t})$$

é um idempotente e um idempotente primitivo e de $\mathcal{F}_qC_n$ é essencial se, e somente se, $ee_0 = e$. De fato, se e é essencial, $e\hat{H} = 0$, para todo H subgrupo próprio de C_n, donde $ee_0 = e(1 - \hat{K_1})(1 - \hat{K_2})\cdots(1 - \hat{K_t}) = (e - e\hat{K_1})(1 - \hat{K_2})\cdots(1 - \hat{K_t}) = (e - 0)(1 - \hat{K_2})\cdots(1 - \hat{K_t}) = \cdots = e$. E se e não for essencial, existe $H \neq 1$ subgrupo próprio de C_n com $e\hat{H} = e$. Como H é um subgrupo não trivial de C_n, existe $i, 1 \leq i \leq t$, tal que $K_i \subset H$. Assim $ee_0 = e\hat{H}e_0 = 0$, pois $\hat{H}(1 - \hat{K_i}) = 0$. Disto, ao decompor e_0 como soma de idempotentes primitivos dois a dois ortogonais, digamos $e_0 = e_1 + e_2 + \cdots + e_m$, uma vez que teremos $e_0e_i = e_i$, para todos $1 \leq i \leq m$, o que implicará que cada e_i é essencial, bem como todo essencial é um dos e_i pois $e_0 = e_i + (e_0 - e_i)$, obtemos $e_0 = \sum_{e \text{ essencial}} e$, isto é, e_0 é soma de todos os idempotentes essenciais em $\mathcal{F}_qC_n$.

Em [2], encontramos o seguinte resultado:

Teorema 2.10. *([2], Teorema 4.2) Seja C_n um grupo cíclico com n elementos e com gerador g e seja m o menor inteiro positivo tal que $n|(q^m - 1)$. Então:*

1. *$dim(\mathcal{F}_qC_n)e_0 = \varphi(n)$, em que φ denota a função de Euler.*
2. *Existem precisamente $\frac{\varphi(n)}{m}$ idempotentes essenciais em $\mathcal{F}_qC_n$.*

Com esse resultado e o Teorema 2.7, temos o seguinte:

Teorema 2.11. *Sejam $\mathcal{F}_q$ um corpo com q elementos, n um inteiro positivo com $mdc(q,n) = 1$, $C_n =< g >$ grupo cíclico com n elementos e $\mathcal{F}_qC_n$ o anel de grupo de C_n sobre $\mathcal{F}_q$. O número de códigos de peso constante de comprimento n e dimensão k é*

$$\sum_{d|n} \delta_{(q^k-1,mmc(d,q-1))} \frac{\varphi(d)}{k},$$

em que φ é a função de Euler e δ é a função delta de Kronecker.

Prova: *Pelo Teorema 2.7, dado e idempotente primitivo de $\mathcal{F}_qC_n$, $\mathcal{F}_qC_ne$ de dimensão k tem peso constante se, e somente se, $(\mathcal{F}_qC_ne)^* = \mathcal{F}_q^*eC_ne$, isto é, se e somente se, sendo $d = o(ge)$ e $q^k - 1 = mmc(q-1,d)$.*

Seja $d|n$ com $q^k - 1 = mmc(q-1,d)$. Considere C_d grupo cíclico com d elementos, e tome os idempotentes primitivos essenciais em $\mathcal{F}_qC_d$, que são, de acordo com o Lema 2.2 os idempotentes primitivos de $\mathcal{F}_qC_n$ com $o(ge) = d$, temos, como $e_0 = \sum_{e\ essencial} e$, e usando o Teorema 2.10, sendo l o número de essenciais de $\mathcal{F}_qC_d$:

$$\begin{aligned} \mathcal{F}_qC_de_0 &= \bigoplus_{e\ essencial} \mathcal{F}_qC_de \\ \Rightarrow dim_{\mathcal{F}_q}\mathcal{F}_qC_de_0 &= \sum_{e\ essencial} dim_{\mathcal{F}_q}\mathcal{F}_qC_de \\ \Rightarrow \varphi(d) &= l \cdot k \\ \Rightarrow l &= \frac{\varphi(d)}{k}. \end{aligned}$$

Como o número de idempotentes essenciais determina a quantidade de códigos distintos de peso constante, temos para um tal d que a quantidade de códigos de peso constante é $\frac{\varphi(d)}{k}$. Somando as quantidades para cada $d|n$ que satisfaz $q^k - 1 = mmc(q-1,d)$, obtemos o resultado. □

2.3 Códigos de dois pesos

Nesta seção construiremos códigos de dois pesos, usando para isso o que sabemos sobre códigos de peso constante pela seção anterior.

Considere o anel de grupo $\mathcal{F}_q(C_{q^m-1} \times C_{q^m-1}) = (\mathcal{F}_q \langle g \rangle) \langle h \rangle$, em que g (bem como h) gera C_{q^m-1}. Seja e um idempotente essencial de $\mathcal{F}_qC_{q^m-1}$, o qual representaremos

por $e(g)$ em $\mathcal{F}_q\langle g\rangle$ e por $e(h)$ em $\mathcal{F}_q\langle h\rangle$, e suponha que $\mathcal{F}_qC_{q^m-1}e$ tenha peso constante. Seja

$$\hat{g} = \frac{1}{q^m-1}\sum_{0\leq i\leq q^m-2} g^i$$

bem como

$$\hat{h} = \frac{1}{q^m-1}\sum_{0\leq i\leq q^m-2} h^i.$$

Então $\hat{g}$ e $\hat{h}$ são idempotentes e, assim, $e(g)\hat{h}$ e $e(h)\hat{g}$ são idempotentes. Seja $e_0 = e(g)\hat{h} + e(h)\hat{g}$. Analisemos então o código

$$\mathcal{F}_q(C_{q^m-1}\times C_{q^m-1})e_0.$$

Queremos saber quais os pesos dos elementos não nulos deste código. Para isso, verifiquemos antes quais são os elementos de tal código.

Teorema 2.12. *Com a notação introduzida acima, os elementos não nulos de $\mathcal{F}_q(C_{q^m-1}\times C_{q^m-1})e_0$ são da forma $g^ie(g)\hat{h}, 1\leq i\leq q^m-1$, $h^ie(h)\hat{g}, 1\leq i\leq q^m-1$, e $g^th^se_0$, $1\leq t,s\leq q^m-1$.*

Prova: *Considere $L = \{0\}\cup\{g^ie(g)\hat{h}\}\cup\{h^je(h)\hat{g}\}\cup\{g^th^se_0\}$. Vejamos que $L = \langle e_0\rangle$.*

A inclusão $L\subseteq\langle e_0\rangle$ é verdadeira, pois uma vez que $e(h)$ e $e(g)$ são essenciais em $\langle h\rangle$ e $\langle g\rangle$, respectivamente, temos $e(h)\cdot\hat{h} = 0 = e(g)\cdot\hat{g}$, e devido a isso é imediato que os elementos da forma $g^ie(g)\hat{h}$, $1\leq i\leq q^m-1$, bem como os elementos da forma $h^ie(h)\hat{g}, 1\leq i\leq q^m-1$, além do 0, estão em $\mathcal{F}_q(C_{q^m-1}\times C_{q^m-1})e_0$. Já para elementos da forma $g^th^se_0$, com $1\leq t,s\leq q^m-1$, a inclusão é imediata.

Para verificar a inclusão $\langle e_0\rangle\subseteq L$, uma vez que $e_0\in L$, basta provar que L é ideal. Vejamos inicialmente que L é fechado para a soma.

Comecemos analisando a soma $g^th^se_0 + g^{t_1}h^{s_1}e_0$, quando esta é não nula. Temos

$$\begin{aligned} g^th^se_0 + g^{t_1}h^{s_1}e_0 &= g^th^s(e(g)\hat{h} + e(h)\hat{g}) + g^{t_1}h^{s_1}(e(g)\hat{h} + e(h)\hat{g}) \\ &= g^te(g)\hat{h} + g^{t_1}e(g)\hat{h} + h^se(h)\hat{g} + h^{s_1}e(h)\hat{g} \\ &= ((g^t + g^{t_1})e(g))\hat{h} + ((h^s + h^{s_1})e(h))\hat{g}. \end{aligned}$$

Note que o elemento $(g^t + g^{t_1})e(g)$ é um elemento do código $\mathcal{F}_qC_{q^m-1}e(g)$. Suponha inicialmente que $g^t + g^{t_1}$ é diferente de zero. Como $\mathcal{F}_qC_{q^m-1}e(g)$ tem peso constante, temos, pelo Teorema 2.7 (que pode ser aplicado aqui pois $mdc(q, q^m-1) = 1$),

$(\mathcal{F}_qC_{q^m-1}e(g))^* = \mathcal{F}_q^*e(g)C_{q^m-1}e(g)$. *Como* $e(g)$ *é essencial, pelo Lema 2.3,* $C_{q^m-1}e(g) \simeq C_{q^m-1}$, *donde* $|C_{q^m-1}e(g)| = q^m - 1$ *e, assim,* $|\mathcal{F}_qC_{q^m-1}e(g)| = q^m - 1$, *donde* $|(\mathcal{F}_qC_{q^m-1}e(g))^*| = q^m - 1$. *Como* $e(g)$ *é essencial,* $g^ie(g) \neq g^je(g)$, *se* $i \neq j$, *donde* $|\{g^ie(g)\}| = q^m - 1$ *e, daí,* $(g^t + g^{t_1})e(g) = g^ie(g)$, *para algum* i, $1 \leq i \leq q^m - 1$.

O mesmo vale para $(h^s+h^{s_1})e(h)$, *caso a soma* $h^s+h^{s_1}$ *seja diferente de zero.Portanto*

$$\begin{aligned} g^th^se_0 + g^{t_1}h^{s_1}e_0 &= ((g^t + g^{t_1})e(g))\hat{h} + ((h^s + h^{s_1})e(h))\hat{g} \\ &= g^ie(g)\hat{h} + h^je(h)\hat{g} = g^ih^je_0, \end{aligned}$$

pois $\hat{g} = g^i\hat{g}$, *e* $\hat{h} = h^i\hat{h}$.

Caso alguma dessas somas dê igual a 0, recaímos numa soma em $\langle e(g)\rangle$ *(ou* $\langle e(h)\rangle$*), que é ideal, sendo portanto fechado para a soma.*

Por fim, se tomamos elementos da forma $g^th^se_0 + g^ie(g)\hat{h}$, *temos que tal soma é igual a* $g^te(g)\hat{h} + h^se(h)\hat{g} + g^ie(g)\hat{h} = (g^t + g^i)e(g)\hat{h} + h^se(h)\hat{g}$, *donde recaímos na análise feita anteriormente. O mesmo vale para a soma* $g^th^se_0 + h^je(h)\hat{g}$. *Assim,* L *é fechado para a soma.*

Além disso, dado $0 \neq r \in \mathcal{F}_q$, *temos* $rL = L$. *De fato,* $rg^ie(g)\hat{h} = g^je(g)\hat{h}$, *pois* $\langle e(g)\rangle$ *é essencial. Pela mesma razão* $rh^je(h)\hat{g} = h^le(h)\hat{g}$ *e, por fim, do mesmo argumento segue* $rg^th^se_0 = r(g^te(g)\hat{h} + h^se(h)\hat{g}) = g^{t_1}e(g)\hat{h} + h^{s_1}e(h)\hat{g} = g^{t_1}h^{s_1}e_0$.

Finalmente, é claro que $gL = L$ *(bem como* $hL = L$*) e, portanto,* L *é ideal e o resultado segue.* □.

Com isso temos o seguinte:

Corolário 2.13. *O código* $\mathcal{F}_q(C_{q^m-1} \times C_{q^m-1})e_0$ *é um código de dois pesos.*

Baseados no Teorema 2.12, podemos calcular os pesos dos elementos de $\mathcal{F}_q(C_{q^m-1} \times C_{q^m-1})e_0$.

Observe inicialmente que

$$w(e(g)\hat{h}) = w(e(g))(q^m - 1).$$

Vamos então determinar o peso de $e(g)$. *Como* $e(g)$ *é idempotente essencial,* $dim_{\mathcal{F}_q}\mathcal{F}_qC_{q^m-1}e(g) = m$ *e, como* $\mathcal{F}_qC_{q^m-1}e(g)$ *tem peso constante, pelo Teorema 2.7, o peso de* $e(g)$ *é* $\frac{q^{m-1}(q-1)(q^m-1)}{q^m-1} = q^{m-1}(q-1)$. *O mesmo vale para* $e(h)$, *isto é,* $w(e(h)) = q^{m-1}(q-1)$.

Chamemos de $\mathcal{C} = \mathcal{F}_q(C_{q^m-1} \times C_{q^m-1})e_0$. *Tal código tem dimensão* $2m$, *donde a soma dos seus pesos é*

$$\sum_{\alpha \in \mathcal{C}} w(\alpha) = q^{2m-1}(q-1)(q^m-1)^2.$$

Como $\mathcal{F}_q C_{q^m-1} e(g)$ *e* $\mathcal{F}_q C_{q^m-1} e(h)$ *têm peso constante, a soma dos pesos em cada um desses conjuntos é* $q^{m-1}(q-1)(q^m-1)$. *Daí*

$$\begin{aligned} w(g^i h^j e_0) &= \frac{q^{2m-1}(q^m-1)^2(q-1) - 2q^{m-1}(q-1)(q^m-1)^2}{(q^m-1)^2} \\ &= q^{2m-1}(q-1) - 2q^{m-1}(q-1) \\ &= (q^{2m-1} - 2q^{m-1})(q-1). \end{aligned}$$

Assim, temos determinados os dois pesos do código $\mathcal{F}_q(C_{q^m-1} \times C_{q^m-1})e_0$.

Exemplo 2.14. *Para ilustrar o que discutimos acima, vamos trabalhar com o anel de grupo* $\mathcal{F}_3 C_8$, C_8 *subgrupo cíclico com* 8 *elementos gerado por* g. *Comecemos encontrando um idempotente essencial, usando para isso o isomorfismo* $\mathcal{F}_3 C_8 = \frac{\mathcal{F}_3(x)}{\langle x^8-1 \rangle}$. *Para tal, usaremos a tabela de polinômios irredutíveis encontrada em [10], a partir da página* 553. *Um dos polinômios fornecido pela tabela é*

$$(1\ 1\ 2) = x^2 + x + 2 = x^2 + x - 1 = p(x).$$

A notação (1 1 2), *usada em [10], indica justamente as coordenadas do polinômio em* $\mathcal{F}_3(x)$.

Considere o código isomorfo a $\frac{(\mathcal{F}_3(x)}{\langle p(x) \rangle}$.

Queremos encontrar um polinômio $e(x)$ *tal que* ge *seja raiz de* $p(x)$ *em* $\mathcal{F}_3 C_8 e$ *(em que* e *é a unidade), isto é, tal que* $g^2e + ge - e = 0$. *Seja*

$$e(x) = a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0.$$

Podemos montar então um sistema de equações com coeficientes em $\mathcal{F}_3$ *para encontrar cada um dos* $a_i's$, *usando para isso também o fato de que* $e^3 = e$. *Para isso utilizamos a equação* $g^2e + ge - e = 0$ *(encontrando para isso* g^2e *e* ge*) e fazendo a igualdade de polinômios, além de tomar* $a_3 = a_1$ *uma vez que* $e^3 = e$ *(pois* $e^2 = e$*), obtemos o*

seguinte sistema de equações:

$$\begin{aligned} a_2 &= -a_1 + a_0 \\ a_3 &= -a_2 + a_1 \\ a_4 &= -a_3 + a_2 \\ a_5 &= -a_4 + a_3 \\ a_6 &= -a_5 + a_4 \\ a_7 &= -a_6 + a_5 \\ a_3 &= a_1 \end{aligned}$$

Resolvendo o sistema, encontramos que $a_2 = 0$, *donde* $a_1 = a_0$, $a_4 = -a_3$, $a_5 = a_4$, $a_6 = 0$ *e* $a_7 = a_5$. *Tomando* $a_7 = -1$, *encontramos como solução para o sistema* $(1\ 1\ 0\ 1\ -1\ -1\ 0\ -1) = 1 + x + x^3 - x^4 - x^5 - x^7 = ke, k \in \mathcal{F}_3$. *Obtemos essas duas possibilidades de solução uma vez que utilizamos* $e^3 = e$. *Como* $e^2 = e$, *e temos que* $(1 + x + x^3 - x^4 - x^5 - x^7)^2 = 1 + x + x^3 - x^4 - x^5 - x^7$, *concluímos que* $k = 1$ *e, assim,* $e = 1 + x + x^3 - x^4 - x^5 - x^7$, *em que* g *é tal que* $C_8 = \langle g \rangle$. *Assim, e é essencial. De fato, os subgrupos próprios não triviais de* C_8 *são* $\{1, g^2, g^4, g^6\}$ *e* $\{1, g^4\}$, *e* $e \times (1 + g^4) = 0 = e \times (1 + g^2 + g^4 + g^6)$, *bem como* $e \times \hat{g} = 0$. *Além disso,* $\mathcal{F}_3 C_8 e$ *tem peso constante, pois* $\mathcal{F}_3 C_8 e$ *é um código de comprimento 8, e, sendo* $h(x)$ *polinômio tal que* $\mathcal{F}_3 C_8 e \simeq \langle h(x) \rangle$, *como grau de* $p(x)$ *é dois, temos* $gr(h(x)) = 6$, *e portanto pelo Teorema 1.54, a dimensão de* $\mathcal{F}_3 C_8 e$ *é* $8 - gr(p(x)) = 8 - 6 = 2$, *e portanto* $w(e) = 6 = \frac{3^{2-1} \times 2 \times 8}{3^2 - 1}$, *donde temos satisfeita a condição 3 do Teorema 2.7. Conseguimos assim construir um código de dois pesos em* $\mathcal{F}_3(C_8 \times C_8)$, *usando o idempotente essencial e construído acima, tomando o código* $\mathcal{F}_3(C_8 \times C_8)(e(g)\hat{h} + e(h)\hat{g})$.

Vejamos quais são os pesos de tal código. Efetuando a multiplicação, temos $w(e(g)\hat{h}) = w((1 + g + g^3 - g^4 - g^5 - g^7)(1 + h + h^2 + h^3 + h^4 + h^5 + h^6 + h^7)) = 48$, *uma vez que todos os termos da multiplicação terão suporte distintos. Além disso,*

$$(1 + g + g^3 - g^4 - g^5 - g^7)(1 + h + h^2 + h^3 + h^4 + h^5 + h^6 + h^7) +$$

$$+(1 + g + g^2 + g^3 + g^4 + g^5 + g^6 + g^7)(1 + h + h^3 - h^4 - h^5 - h^7) =$$

$$2 + 2g + h^6 + 2g^3 + 2h - 2g^4h^7 + 2g^3h + g^3h^2 + 2g^3h^3 + g^3h^6$$

$$+g^2h + g^2h^3 - g^2h^4 - g^2h^5 - g^2h^7 + 2gh + gh^2 + 2gh^3 + gh^6 + g^2$$

$$+2h^3 - g^7h^2 - 2g^7h^4 - 2g^7h^5 - g^7h^6 - 2g^7h^7 + g^6h + g^6h^3 - g^6h^4 - g^6h^5$$
$$-g^6h^7 - g^5h^2 - 2g^5h^4 - 2g^5h^5 - g^5h^6 - 2g^5h^7 - g^4h^2 - 2g^4h^4 - 2g^4h^5$$
$$-g^4h^6 + h^2 + g^6$$

donde $w(e(g)\hat{h} + e(h)\hat{g}) = 42$, *que são justamente os pesos obtidos nos cálculos anteriores ao exemplo para o caso geral.*

Capítulo 3

Códigos de peso constante em outras classes de anéis de grupos

Analisaremos aqui condições que garantam que um código tenha peso constante trabalhando agora com outras classes de anéis de grupos, usando novamente como ferramenta propriedades de anéis de grupo.

3.1 Grupo Abeliano

Começaremos trabalhando com o caso do anel de grupo $\mathcal{F}_qA$, em que A é um grupo abeliano com n elementos. Primeiramente, vamos assumir que $mdc(n,q) = 1$, isto é, que $\mathcal{F}_qA$ é um anel semissimples.

Teorema 3.1. *Sejam $\mathcal{F}_q$ um corpo com q elementos, n um inteiro positivo com $mdc(q,n) = 1$, A um grupo abeliano com n elementos e $\mathcal{F}_qA$ o anel de grupo de A sobre $\mathcal{F}_q$. Considere e um idempotente primitivo de $\mathcal{F}_qA$ e $\mathcal{C} = \mathcal{F}_qAe$ o respectivo código irredutível. Seja $dim_{\mathcal{F}_q}\mathcal{C} = k$. São equivalentes:*

1. *$\mathcal{C}$ tem peso constante;*
2. *Todo elemento não nulo de $\mathcal{C}$ tem peso $\frac{q^{k-1}(q-1)n}{q^k-1}$;*
3. *Existe um elemento de $\mathcal{C}$ cujo peso é $\frac{q^{k-1}(q-1)n}{q^k-1}$;*

4. $(\mathcal{F}_qAe)^* = \mathcal{F}_q^*Ae$.

Prova: *As implicações* $(1 \Longrightarrow 2)$, *(*$2 \Longrightarrow 3$*) e (*$4 \Longrightarrow 1$*) são demonstradas de modo análogo ao Teorema 2.7. Vejamos então o caso* $(3 \Longrightarrow 4)$. *Caso o idempotente e seja essencial, a demonstração é similar a feita no Teorema 2.7, pois a argumentação só usa o fato de* $\mathcal{F}_qAe$ *ser corpo finito, que resulta em* $(\mathcal{F}_qAe)^*$ *ser um grupo cíclico, o que ainda vale no caso em que A é abeliano. Analisemos por fim o caso em que e é não essencial. Observe que na demonstração do Teorema 2.7, para este caso, a argumentação foi baseada somente no fato de* $\frac{C_n}{H_e}$ *ser um grupo cíclico. Assim, se mostrarmos que* $\frac{A}{H_e}$ *é cíclico, com* $H_e = \prod_{H \in \mathcal{H}e} H$, *em que* $\mathcal{H}e = \{H < A; He = e\}$, *o resultado se demonstra de maneira análoga.*

Considere então a função

$$\varphi : A \to (\mathcal{F}_qAe)^*$$

$$a \mapsto ae$$

que é um homomorfismo de grupos. Calculemos $Ker(\varphi)$. *Seja* $a \in Ker(\varphi)$. *Então* $ae = e$, *donde* $a^ie = e$ *e, assim,* $\frac{1}{|\langle a \rangle|}\Sigma a^ie = e$, *consequentemente,* $\langle a \rangle \in \mathcal{H}e$, *ou seja,* $\langle a \rangle \subset H_e$, *logo* $Ker(\varphi) \subset H_e$. *Se* $h \in H_e$, $he = h\hat{H}_ee = e$ *e* $\ker(\varphi) = H_e$. *Disto,* $\frac{A}{H_e}$ *é isomorfo a um subgrupo de* $(\mathcal{F}_qAe)^*$, *que é cíclico, donde tal subgrupo é cíclico e temos assim (*$3 \Longrightarrow 4$*).* □

Trabalhemos agora com o caso em que A é um grupo abeliano com n elementos, mas sem a hipótese de que $mdc(n, q) = 1$, *isto é, sem a hipótese que* $\mathcal{F}_qA$ *é semissimples. Seja* $A = A_{p'} \times A_p$, *com* $A_{p'}$ *o somando de A cujos elementos têm ordem relativamente prima com p e* A_p *o p-subgrupo de Sylow de A. Então* $\mathcal{F}_qA_{p'}$ *é um anel de grupo semissimples, digamos* $\mathcal{F}_qA_{p'} = \mathcal{F}_qA_{p'}e_1 \oplus ... \oplus \mathcal{F}_qA_{p'}e_t$, *com* e_i *idempotentes primitivos e* $\mathcal{F}_qA_{p'}e_i = K_i$, *com* K_i *um corpo finito. Sob tais condições, concluímos que* $\mathcal{F}_qA = \mathcal{F}_q(A_{p'} \times A_p) = (\mathcal{F}_qA_{p'})A_p = (K_1 \oplus ... \oplus K_t)A_p = K_1A_p \oplus ... \oplus K_tA_p$.

Vale o seguinte:

Lema 3.2. *Com a notação acima,* K_iA_p *é um anel local, para todo* $1 \leq i \leq t$, *cujo radical é o ideal de aumento* $Ker(\epsilon)$.

Prova: *Seja* $Ker(\epsilon) = \{\alpha = \sum_{g \in A_p} \alpha_g g \in K_iA_p; \Sigma\alpha_g = 0\}$ *o ideal de aumento. Seja* p^r *o*

expoente de A_p. Então, se $\alpha = \sum_{g \in A_p} \alpha_g g$ pertence a $Ker(\epsilon)$, $\alpha^{p^r} = (\Sigma \alpha_g g)^{p^r} = (\Sigma \alpha_g) = 0$. Seja β um elemento de $K_i A_p$ não pertencente a seu ideal de aumento. Então $\epsilon(\beta) = k_1 \neq 0$ e daí $\beta - k_1 \in Ker(\epsilon)$. Logo $\beta = k_1 + (\beta - k_1) = k_1(1 + k_1^{-1}(\beta - k_1))$. Vejamos que $1 + k_1^{-1}(\beta - k_1) = 1 + \gamma$ é inversível, o que fará com que β seja inversível. Como $\gamma \in Ker(\epsilon)$, $\gamma^{p^r} = 0$. Daí, $(1+\gamma)(1 - \gamma + \gamma^2 - ... + (-1)^{p^r - 1}\gamma^{p^r - 1}) = 1$, e $1 + \gamma$ é inversível. Como isso vale para qualquer elemento fora de $Ker(\epsilon)$, segue que ele é maximal. Além disso é o conjunto dos não inversíveis de $K_i A$, e assim $K_i A$ é local com radical $Ker(\epsilon)$. □

Seja $\tilde{A}_p = \sum_{a \in A_p} a$ e $\left\langle \tilde{A}_p \right\rangle = K_i A_p \tilde{A}_p$ o ideal de $K_i A_p$ gerado por $\tilde{A}_p$. Vale então:

Lema 3.3. *Com a notação introduzida acima, $\left\langle \tilde{A}_p \right\rangle$ é o único ideal irredutível de $K_i A_p$.*

Prova: *De fato, $\left\langle \tilde{A}_p \right\rangle$ é minimal, pois se $0 \neq J \subseteq \left\langle \tilde{A}_p \right\rangle$, então, dado $x \in J$, $x = k_i \tilde{A}_p$, com $k_i \in K_i$. Daí, como J é ideal, $\tilde{A}_p = k_i^{-1} k_i \tilde{A}_p \in J$, e $J = \left\langle \tilde{A}_p \right\rangle$. Disto $\left\langle \tilde{A}_p \right\rangle$ é irredutível. Vejamos que ele é o único.*

Suponha I um ideal irredutível de $K_i A_p$. Então $Ker(\epsilon) I \subseteq I = 0$ ou I. Se $MI = I$, pelo Lema de Nakayama, $I = 0$. Disto $MI = 0$. Dado qualquer $a \in A_p$, $1 - a \in Ker(\epsilon)$. Logo, para $\alpha \in I$, $\alpha(1 - a) = 0$. Como $\alpha = \sum_{g \in A_p} \alpha_g g$ e $(1 - a)\alpha = 0$, temos $\Sigma \alpha_g (1 - a) = 0$, donde todas as coordenadas de $\Sigma \alpha_g (1 - a)$ são nulas, em particular a coordenada que acompanha $a \in G$, isto é, $\alpha_1 - \alpha a = 0$ e, assim, $\alpha_a = \alpha_1$. E isto vale para todo $a \in A_p$, donde $\alpha = k_i \tilde{A}_p$ e, portanto, $I = \left\langle \tilde{A}_p \right\rangle$. □

Como os ideais irredutíveis de $\mathcal{F}_q A$ são os ideais irredutíveis de $K_i A_p$, uma vez que $\mathcal{F}_q A = K_1 A_p \oplus \cdots \oplus K_t A_p$, temos como consequência

Corolário 3.4. *Os ideais irredutíveis de $\mathcal{F}_q A$ são da forma $\mathcal{F}_q A_{p'} e_i \tilde{A}_p$, para todo $1 \leq i \leq t$.*

Temos ainda o seguinte resultado:

Lema 3.5. *Seja $\mathcal{F}_q$ um corpo finito com q elementos e A um grupo abeliano com n elementos. Se um código de $\mathcal{F}_q A$ tem peso constante, então ele é irredutível.*

Prova: *É a mesma do caso em que o grupo é um grupo cíclico, veja Lema 2.6.* □

Assim, para que um código de $\mathcal{F}_qA$ seja de peso constante, ele deve ser irredutível, e pelo Lema 3.3, o código deve ser da forma $\mathcal{F}_qA_{p'}e_i\tilde{A}_p$. Como um elemento de tal conjunto é da forma $\alpha = \alpha_1\tilde{A}_p$ (e para cada $g \neq h \in A_p$, $supp\alpha_1 g$ e $supp\alpha_1 h$ são conjuntos disjuntos), com $\alpha_1 \in \mathcal{F}_qA_{p'}e_i$, seu peso é $\omega(\alpha_1)\,|A_p|$, ou seja, a análise do peso dos elementos do código se restringe a análise do peso dos elementos de $\mathcal{F}_qA_{p'}e_i$. Disto, pelo já visto no caso anterior, vale:

Teorema 3.6. *Sejam $\mathcal{F}_q$ um corpo finito com q elementos, n um inteiro positivo com $mdc(q,n) \neq 1$, A um grupo abeliano com n elementos e $\mathcal{F}_qA$ o anel de grupo de A sobre $\mathcal{F}_q$. Considere e um idempotente primitivo de $\mathcal{F}_qA$ e $\mathcal{C} = \mathcal{F}_qAe = \mathcal{F}_qA_{p'}e\tilde{A}_p$ o respectivo código irredutível. Seja $dim_{\mathcal{F}_q}\mathcal{C} = k$. Então $\mathcal{C}$ tem peso constante se, e somente se, dados todos os elementos $\alpha = \alpha_1\tilde{A}_p$, com $\alpha_1 \in \mathcal{F}_qA_{p'}e$, têm o mesmo peso, isto é, se, e somente se, $\mathcal{F}_qA_{p'}e_i$ tem peso constante.*

Observe que, com tal teorema, temos em particular uma caracterização para os códigos de $\mathcal{F}_qC_n$, com C_n um grupo cíclico, para o caso em que $\mathcal{F}_qC_n$ não é semissimples.

3.2 Domínio de Integridade

Seja R um domínio de integridade infinito e A um grupo abeliano finito. Nessas condições, tomando o anel de grupos RA, embora não possamos falar nos ideais de RA como códigos, ainda assim podemos olhar o peso de Hamming dos elementos destes ideais. Para este caso, temos o seguinte:

Teorema 3.7. *Sejam R um domínio de integridade infinito e A um grupo abeliano finito. Considere o anel de grupo RA e seja I um ideal de RA. Então $w(I) = |A|$ se, e somente se, I tem peso constante.*

Prova: *Seja I um ideal de RA e suponha $w(I) \neq |A|$. Então existe $\alpha \in I$ com $w(\alpha) \neq |A|$. Assim, se $\alpha = \sum_{h\in A} \alpha_h h$, existe $g \in A$ tal que $\alpha_g = 0$. Suponha que $\alpha_1 \neq 0$ (se $\alpha_1 = 0$, basta multiplicar α por $(g')^{-1}$, com $\alpha_{g'} \neq 0$ e teremos o desejado). Como A*

é finito, existem finitos $h \in A$ tais que o coeficiente $\alpha_h \neq 0$. Como R é um domínio de integridade, existe $k \in R$ tal que $\alpha_h \neq k\alpha_{hg^{-1}}$, para todo h com $\alpha_h \neq 0$. Em particular como $\alpha_1 \neq 0$, temos $k\alpha_1 \neq 0$. Com esse k, tome o elemento $\alpha - kg\alpha$. Tal elemento está em I, uma vez que I é ideal. Para todo $h \in A$, o coeficiente de h em $\alpha - kg\alpha$ será $\alpha_h - k\alpha_{hg^{-1}}$. Pela escolha de k, os coeficientes α_h de α que são não nulos continuam sendo coeficientes diferentes de 0 em $\alpha - kg\alpha$ (pois o coeficiente de $h \in A$ em $\alpha - kg\alpha$ é $\alpha_h - k\alpha_{hg^{-1}}$). Além disso, o coeficiente de g em $\alpha - kg\alpha$ será $\alpha_g - k\alpha_g g^{-1} = k\alpha_1 \neq 0$. Assim, $w(\alpha) < w(\alpha - kg\alpha)$, donde I não tem peso constante. Portanto, para I ter peso constante é necessário que $w(I) = |A|$.

Por outro lado, se $w(I) = |A|$, então, como o maior peso possível é $|A|$, segue imediatamente que I tem peso constante. □

Exemplo 3.8. *Seja K um corpo infinito e A um grupo abeliano finito. Analisemos os ideais de peso constante de KA:*

Pelo teorema acima, um ideal I de KA tem peso constante se, e somente se, $w(I) = |A|$. Seja I um ideal de KA.

Se $dim_k(I) = 1$, então existe $\alpha \in I$ tal que $I = \{k\alpha | k \in K\}$. Neste caso, todos os elementos de I têm o mesmo peso de α, ou seja, I tem peso constante, donde $w(\alpha) = |A|$.

Agora, seja I um ideal não nulo de KA e suponha que todos os elementos não nulos de I tenham o mesmo peso. Vejamos que neste caso I deve ter dimensão 1 sobre K. Seja $\alpha = \sum_{g \in A} \alpha_g g$ um elemento não nulo de I, e suponha que exista $\beta = \sum_{g \in A} \beta_g g \in I$ tal que $\beta \neq r\alpha$, para todo $r \in K$. Como $w(I) = |A|$, $\alpha_g \neq 0 \neq \beta_g$, para todo $g \in A$. Em particular, $\alpha_1 \neq 0 \neq \beta_1$. Tome $k = \alpha_1(\beta_1)^{-1} \neq 0$. Então $k\beta = \alpha_1 + \sum_{g \in A, g \neq 1} k\beta_g g$. Como $\beta \neq r\alpha$, para todo $r \in K$, $\beta \neq k^{-1}\alpha$, isto é, $k\beta \neq \alpha$. Considere $\gamma = k\beta - \alpha \neq 0$. Temos $\gamma \in I$. Mas $\gamma_1 = k\beta_1 - \alpha_1 = \alpha_1(\beta_1)^{-1}\beta_1 - \alpha_1 = \alpha_1 - \alpha_1 = 0$, donde $w(\gamma) < |A|$, contradizendo o fato de que todos os elementos de I têm peso $|A|$. Disto $I = \{r\alpha | r \in K\}$, isto é, $dim_k(I) = 1$.

3.3 Anel de Cadeia

Seja R um anel de cadeia finito, com ideal maximal $\langle p\rangle$ e com cadeia de ideais $0 \subseteq \langle p^{r-1}\rangle \subseteq \ldots \subseteq \langle p^2\rangle \subseteq \langle p\rangle$, em que r é o índice de nilpotência de p. Seja $\frac{R}{\langle p\rangle} = \bar{R} = \mathbb{F}_{q^s}$, com q potência de um número primo.

Considere $G = \langle g\rangle$ um grupo cíclico com n elementos e o anel de grupo RG. Suponha que $mdc(q, n) = 1$. Então $\bar{R}G$ é semissimples, donde existem $e_1, e_2, \ldots, e_k$ idempotentes primitivos ortogonais em $\bar{R}G$ tais que

$$\bar{R}G = \bar{R}Ge_1 \oplus \ldots \oplus \bar{R}Ge_k$$

e, pelo Teorema 1.42, existem $e'_1, \ldots, e'_k$ idempotentes primitivos ortogonais em RG, com $\bar{e'_i} = e_i$ e tais que

$$RG = RGe'_1 \oplus \ldots \oplus RGe'_k.$$

Vamos agora analisar os códigos de peso constante em RGe'_i. Para isso, vejamos inicialmente o seguinte resultado:

Lema 3.9. *A função:*

$$\begin{aligned} \Psi' : (\bar{R}, +) &\rightarrow (\langle p^{r-1}\rangle, +) \\ \bar{x} &\mapsto p^{r-1}x \end{aligned}$$

com $\langle p^{r-1}\rangle$ visto como ideal de R, é um isomorfismo de grupos que dá origem, para cada e_i idempotente em $\bar{R}G$, à bijeção

$$\begin{aligned} \Psi : \bar{R}Ge_i &\rightarrow \langle p^{r-1}e'_i\rangle \\ \sum_{g\in G} \bar{\alpha_g} g e_i &\mapsto p^{r-1}\sum_{g\in G} \alpha_g g e'_i \end{aligned}$$

com $\langle p^{r-1}e'_i\rangle$ visto como ideal de RG. Tal bijeção preserva soma e peso.

Prova: *Note que Ψ' está bem definida, pois dados $x, y \in R$ com $\bar{x} = \bar{y}$, então $x - y = pa$, $a \in R$. Assim, $p^{r-1}(x - y) = p^{r-1}pa = 0$, donde $p^{r-1}x = p^{r-1}y$, isto é, $\Psi'(\bar{x}) = \Psi'(\bar{y})$. Além disso, dados $\bar{x}, \bar{y} \in \bar{R}$, $\Psi'(\bar{x} + \bar{y}) = \Psi'(\overline{x + y}) = p^{r-1}(x + y) = \Psi'(\bar{x}) + \Psi'(\bar{y})$. Também, se $\Psi'(\bar{x}) = 0$, então $p^{r-1}x = 0$, donde $x = pa, a \in R$, logo $\bar{x} = 0$. Por fim, dado $p^{r-1}x \in \langle p^{r-1}\rangle$, basta tomar $\bar{x} \in \bar{R}$ e temos $\Psi'(\bar{x}) = p^{r-1}x$. Portanto Ψ' é isomorfismo de grupos.*

Como Ψ' é isomorfismo e dele se origina Ψ, é imediato que Ψ é bijeção e preserva soma. Além disso,

$$\begin{aligned} w(p^{r-1}x) &= \{x_g \in supp(x) |\ x_g \text{ é unidade}\} \\ &= \{\bar{x_g} \in supp(\bar{x}) |\ \bar{x_g} \neq 0\} \\ &= w(\bar{x}) \end{aligned}$$

e, portanto, Ψ preserva peso. □

Observe que com tal resultado podemos concluir que se $\langle p^{r-1}e_i' \rangle$ tem peso constante em RG, e_i deve gerar um ideal de peso constante em $\bar{R}G$, isto é, se e_i gera um ideal que não tem peso constante, então o ideal gerado por e_i' não pode ter peso constante, uma vez que $\langle p^{r-1}e_i' \rangle$ não terá peso constante e $\langle p^{r-1}e_i' \rangle \subseteq \langle e_i' \rangle$. Mais ainda, concluímos que um ideal de RGe_i' tem peso constante se, e somente se, $\bar{R}Ge_i$ tem peso constante.

Lema 3.10. *Se I' é um ideal de RG de peso constante, então I' é indecomponível.*

Prova: *Tome I' ideal de RG decomponível, digamos $I' = I_1 \oplus I_2$. Então I_1 contém um minimal $\langle p^{r-1}e_1' \rangle$, bem como I_2 contém um minimal $\langle p^{r-1}e_2' \rangle$, com $e_1' \neq e_2'$. Então $\langle p^{r-1}(e_1' + e_2') \rangle \subseteq \langle p^{r-1}e_1' \rangle \oplus \langle p^{r-1}e_2' \rangle \subseteq I$. Como um subideal de um ideal de peso constante tem peso constante, o ideal $\langle p^{r-1}(e_1' + e_2') \rangle$ tem peso constante, donde, pelo Lema anterior, sendo $\bar{e_1'} = e_1$, $\bar{e_2'} = e_2$, $\langle (e_1 + e_2) \rangle$ deve ter peso constante em $\bar{R}G$. Mas isto não ocorre, uma vez que se um código em $\bar{R}G$ tem peso constante então ele deve ser irredutível de acordo com o Lema 2.6. Portanto, para um ideal ter peso constante em RG ele precisa ser indecomponível.* □

De acordo com o Teorema 1.39, sabemos que os ideais de RGe_i' são da forma $\langle p^j e_i' \rangle$ para $0 \leq j \leq r-1$ e $1 \leq i \leq n$. Assim, dado I' um ideal de RGe_i', ele deve ser igual a algum dos $\langle p^j e_i' \rangle$.

Podemos então dizer o seguinte:

Teorema 3.11. *Sejam R um anel de cadeia finito com ideal maximal $\langle p \rangle$, p com índice de nilpotência r, $\frac{R}{\langle p \rangle} = \bar{R} \simeq \mathcal{F}_q$, $\mathcal{F}_q$ corpo finito com q elementos, e G um grupo cíclico com n elementos tal que $mdc(q, n) = 1$. Considere e_i idempotente primitivo de $\bar{R}G$ que gera um código de peso constante, e_i' idempotente primitivo de RG, com $\bar{e_i'} = e_i$,*

e seja I' um ideal de RGe_i'. Se $w(e_i) \neq |G|$, I' tem peso constante se, e somente se, $I' = \langle p^{r-1}e_i' \rangle$

Prova: *Seja $I = \bar{R}Ge_i$ código não nulo de peso constante e assuma $w(I) \neq |G|$. Então, pelo Lema 3.9, temos que $\langle p^{r-1}e_i' \rangle$ tem peso constante. Vejamos que neste caso, para um código I' em RGe_i' ter peso constante, ele precisa ser da forma $\langle p^{r-1}e_i' \rangle$.*

Suponha, por absurdo, que exista $I' = \langle p^j e_i' \rangle$, com $j < r-1$ de peso constante. Como $w(I) \neq |G|$, existe $g_i \in G$, para $e_i = \sum_{g \in G} a_g g$, com $a_{g_i} = 0$. Assim e_i' tem coordenadas que são unidades e coordenadas que ou são nulas ou são múltiplas de p. Se todas as coordenadas de $p^j e_i'$ são não nulas, então é porque as coordenadas de e_i' também são não nulas, e pelo fato de e_i ter coordenadas nulas segue que e_i' tem coordenadas em $\langle p \rangle$. Disto $\langle p^j e_i' \rangle$ não poderá ter peso constante, pois nesse caso tal coordenada estará em $\langle p^{j+1} \rangle$, mas há coordenadas de $p^j e_i'$ que estão em $\langle p^j \rangle \setminus \langle p^{j+1} \rangle$ (pois há coordenadas de e_i' que são unidades) e, assim, multiplicando $p^j e_i'$ por p^{r-1-j}, obteremos $w(p^j e_i') > w(p^{r-1-j} p^j e_i')$. Assim, podemos assumir que $p^j e_i'$ tem alguma coordenada nula.

Tomemos então $\alpha \in \langle p^j e_i' \rangle$, $\alpha = \sum_{g \in G} \alpha_g g$, tal que algumas das coordenadas α_g'' de α é nulo. Como $I' = \langle p^j e_i' \rangle$, podemos tomar este α tal que exista $g' \in G$ com $\alpha_g' \in \langle p^j \rangle \setminus \langle p^{j+1} \rangle$. Temos dois casos a considerar:

Caso 1: todas as coordenadas não nulas de α estão em $\langle p^j \rangle \setminus \langle p^{j+1} \rangle$:

Neste caso, multiplicamos α por $p(g')^{-1}g''$. Neste caso, tomando $\alpha + p(g')^{-1}g''\alpha$, como as coordenadas de α estão em $\langle p^j \rangle \setminus \langle p^{j+1} \rangle$ e as coordenadas de $p(g')^{-1}g''\alpha$ estão em $\langle p^{j+1} \rangle$, as coordenadas não nulas de α continuam não nulas em $\alpha + p(g')^{-1}g''\alpha$. Além disso, a coordenada de g'', que em α é nula, em $\alpha + p(g')^{-1}g''\alpha$ é diferente de 0 (pois é igual a $a_{g'}p$, e $a_g \in \langle p^j \rangle \setminus \langle p^{j+1} \rangle$, com $j < r-1$). Disto $w(\alpha + p(g')^{-1}g''\alpha) > w(\alpha)$, uma contradição.

Caso 2: alguma das coordenadas não nulas de α estando em $\langle p^{j+1} \rangle$:

Assim, multiplicando α por p^{r-1-j}, teremos pela mesma argumentação do caso anterior $w(\alpha) > w(p^{r-1-j}\alpha)$, uma contradição. Portanto, para ter peso constante, $I' = \langle p^{r-1}e_i' \rangle$.

Reciprocamente, seja I' ideal em RGe_i' e suponha que $\langle e_i\rangle$ não tem peso constante. Então existem $x, y \in \langle e_i\rangle$ com $|supp(x)| \neq |supp(y)|$, digamos $|supp(x)| > |supp(y)|$ (o outro caso é análogo). Então, dados levantamentos $x' = \sum_{g\in G} \alpha_g g$ e $y' = \sum_{g\in G} \beta_g g$ de x e y, respectivamente, como existe ao menos um $g' \in G$ a mais em y, comparado a x, tal que a coordenada que acompanha g' é nula, para tal g' temos $\beta_{g'} \in \langle p\rangle$, isto é, $\beta_{g'} = p\gamma_{g'}$. Daí, ou $\gamma_{g'} = 0$, para todo g' com esta característica e, neste caso, $w(x') > w(y')$, ou algum $\gamma_{g'} \neq 0$, e daí, como $p^{r-1}y' \in I'$, teremos $w(x') > w(p^{r-1}y')$. Em qualquer dos casos concluímos que I' não tem peso constante, donde para I' ter peso constante I deve ter peso constante. □

Para o caso em que $w(e_i) = |G|$, vale o seguinte.

Teorema 3.12. *Sejam R um anel de cadeia finito com ideal maximal $\langle p\rangle$, p com índice de nilpotência r, $\frac{R}{\langle p\rangle} = \bar{R} \simeq \mathcal{F}_q$, $\mathcal{F}_q$ um corpo finito com q elementos, e G um grupo cíclico com n elementos tal que $mdc(q, n) = 1$. Considere e_i idempotente primitivo de $\bar{R}G$ que gera um ideal de peso constante e e_i' idempotente primitivo de RG, com $\bar{e_i'} = e_i$. Suponha $w(e_i) = |G|$. Então RGe_i', bem como todos os seus subideais, tem peso constante.*

Prova: *Suponha $w(e_i) = |G|$. Então, para $e_i = \sum_{g\in G} a_g g$, $a_g \neq 0$, para todo g, e portanto, para qualquer levantamento de e_i e, em particular, para e_i', suas coordenadas são todas unidades. Como $w(e_i) = |G|$, temos que $\langle e_i\rangle$ tem dimensão 1. De fato, como $\langle e_i\rangle$ tem peso constante, $w(e_i) = \frac{q^{k-1}n(q-1)}{q^k-1} = n$, então $\frac{q^{k-1}(q-1)}{q^k-1} = 1$, isto é, $q^k - q^{k-1} = q^k - 1$ donde $q^{k-1} = 1$ e consequentemente $k = 1$. Neste caso, $|\langle e_i\rangle| = q$, donde $|\langle p^{r-1}e_i'\rangle| = q$ e $|\langle e_i'\rangle| = q^r$. Assim, os elementos de $\langle e_i'\rangle$ são da forma ke_i', $k \in R$, pois dados $k_1, k_2 \in R$, $k_1e_i' \neq k_2e_i'$, uma vez que as coordenadas de e_i' são unidades. Disto todo elemento de $\langle e_i'\rangle$ tem peso $|G|$ e, portanto, $\langle e_i'\rangle$ tem peso constante, donde $\langle p^j e_i'\rangle$ tem peso constante, para $0 \leq j \leq r-1$.* □

Para o nosso último exemplo, precisaremos da seguinte definição:

Definição 3.13. *Dado A um grupo abeliano finito, g um elemento de A e q um número primo, a* **classe q-ciclotômica** *de g é o conjunto*

$$S_g = \{g^{q^j} | 0 \leq j \leq t_g - 1\},$$

em que t_g é o menor inteiro positivo tal que $q^{t_g} \equiv 1 (modo(g))$.

Em [6] encontramos o seguinte resultado, que pode ser visto como uma generalização de um resultado de Berman [1] e Witt [20]:

Teorema 3.14. *Seja F um corpo finito, com $|F| = q$, e seja A um grupo abeliano finito com $mdc(q, |A|) = 1$. Então o número de componentes simples de FA é igual ao número de classes q-ciclotômicas de A.*

Exemplo 3.15. *Vamos analisar quais são os ideais de peso constante em $\mathbb{Z}_8C_7$.*

Observe que $\mathbb{Z}_8$ é um anel de cadeia com cadeia de ideais

$$\mathbb{Z}_8 \supseteq \langle 2 \rangle \supseteq \langle 4 \rangle \supseteq (0)$$

Então, pelos resultados anteriores, para determinar os ideais de peso constante de $\mathbb{Z}_8C_7$, basta definirmos os de peso constante em $\bar{\mathbb{Z}}_8C_7 = \mathcal{F}_2C_7$. Para isso, estabelecemos inicialmente os idempotentes primitivos ortogonais de $\mathcal{F}_2C_7$. Com um cálculo similar ao feito no Exemplo 2.14, encontramos os idempotentes $e_1 = \hat{g}$, $e_2 = 1 + g + g^2 + g^4$, e $e_3 = 1 + g^3 + g^5 + g^6$. Um cálculo direto mostra que tais idempotentes são dois a dois ortogonais, com soma 1. Além disso, as classes 2-ciclotômicas de C_7 são $\{1\}$, $\{g^2, g^4, g^6\}$ e $\{g^3, g^5, g^6\}$, isto é, são 3 classes 2-ciclotômicas, donde são 3 as componentes simples de $\mathcal{F}_2C_7$ e, portanto, tais idempotentes são primitivos. Logo $\{e_1, e_2, e_3\}$ é um conjunto completo de idempotentes ortogonais primitivos. Ainda, $dim(\langle \hat{g} \rangle) = 1$, e $w(\hat{g}) = 7 = \frac{2^{1-1}(2-1)7}{2^1-1}$, bem como $dim(\langle e_1 \rangle) = dim(\langle e_1 \rangle) = 3 = \frac{2^{3-1}(2-1)7}{2^3-1}$ (tais dimensões obtidas usando o grau do polinômio que gera cada um desses idempotentes e com o Teorema 1.54, tal como foi feito no Exemplo 2.14), donde pelo Teorema 2.7 tais idempotentes geram códigos de peso constante.

Na demonstração do Teorema 1.28, é feita a construção do idempotente em R dado um idempotente em $\bar{R}$. Usando tal construção, concluímos que os idempotentes associados a e_1, e_2 e e_3 são, respectivamente, $e'_1 = 7\hat{g}$, $e'_2 = 5 + 3g + 3g^2 + 6g^3 + 3g^4 + 6g^5 + 6g^6$, $e'_3 = 5 + 6g + 6g^2 + 3g^3 + 6g^4 + 3g^5 + 3g^6$. Assim, os códigos de peso constante de $\mathbb{Z}_8C_7$ devem ser ideais de $\langle e'_1 \rangle$, $\langle e'_2 \rangle$ e $\langle e'_3 \rangle$. É fácil ver que $\langle e'_1 \rangle$ tem peso constante, donde seus ideais também têm peso constante. Já para $\langle e'_2 \rangle$, note que $w(4e'_2) < w(e'_2)$, donde $\langle e'_2 \rangle$ bem como $\langle 2e'_2 \rangle$ não têm peso constante. Já $\langle 4e'_2 \rangle$ tem peso constante pelo Lema 3.7, uma vez que $\langle e_2 \rangle$ tem peso constante. O mesmo vale para a análise de $\langle e'_3 \rangle$

e seus ideais. Logo, como nos teoremas acima, os ideais de peso constante de $\mathbb{Z}_8C_7$ *são* $\langle e_1' \rangle$ *(e seus ideais),* $\langle 4e_2' \rangle$ *e* $\langle 4e_3' \rangle$.

Capítulo 4

Conclusão

Nesta tese trabalhamos com códigos sobre os seguintes anéis de grupo :

- $\mathcal{F}_q A$, *com* $\mathcal{F}_q$ *um corpo finito com* q *elementos e* A *um grupo abeliano finito;*
- RC_n, *com* R *um anel de cadeia finito e* C_n *um grupo cíclico com* n *elementos tal que* $mdc(n, q) = 1$.

As contribuições deste trabalho foram dar condições que garantissem que um código tenha peso constante nessas classes de anéis de grupo, além da construção de códigos de dois pesos usando os códigos de peso constante em $\mathcal{F}_q C_q^{n-1}$.

Como perspectivas futuras, pretendemos analisar códigos de peso constante sobre RA, *em que* R *é um anel local finito e* A *é um grupo abeliano finito. Também queremos trabalhar com códigos de exatamente dois pesos.*

Referências Bibliográficas

[1] *S.D.Berman, The number of irreducible representations of a finite group over an arbitrary field.(Russian) Dokl. Akad. Nauk. 106: 767 - 769, (1956).*

[2] *G. Chalom, R. A. Ferraz and C. Polcino Milies, Essential Idempotents in Abelain Group Algebras (submetido).*

[3] *Y. M. Chee and S. Ling Constructions for q-ary constant-weight codes, IEEE Transactions on Information Theory, vol 53, no 1: 135 - 146, (2007).*

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

[5] *T. Etzion, A. Vardy, A new construction for constant weight codes, Arxive - 3 mar 2014.*

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

[7] *R.A.Ferraz, C.Polcino Milies and M. Guerreiro, G-equivalence in group algebras and minimal abelian codes, IEEE Transactions on Information Theory, vol 60, no1: 252 - 260, (2014).*

[8] *J.B, Fraleigh A First Course in Abstract Algebra, Fifth Edition, Addison-Wesley, (1997).*

[9] *N. Jacobson, Basic Algebra II, W.H. Freeman and Company, San Francisco, (1980).*

[10] R. Lidl and H. Niederreiter Finite Fields, Cambridge University Press, Second Edition, (1997).

[11] B.R. MacDonald, Finite Rings with Identity, A series of monographs and Textbooks, New York, (1974).

[12] H. Matsumura, Commutative Algebra, Second Edition, The Benjamin Cummings Publishing Company, Massachusettis, (1980).

[13] C. Polcino Milies, Breve Introdução à Teoria dos Códigos Corretores de Erros, Departamento de Matemática, UFMS, (2009).

[14] C.Polcino Milies and S.K. Sehgal, An Introduction to Group Rings, Kluwer Academic Publishers, (2002).

[15] S. Roman, Coding and Information Theory, Springer, New York (1992).

[16] C.E. Shannon, A Mathematical Theory of Communication, The Bell System Technical Journal **2**, *(1950).*

[17] A.T. da Silva, Códigos cíclicos sobre anéis de cadeia, Tese de doutorado apresentada ao Instituto de Matemática e Estatística da USP, São Paulo, (2012).

[18] R.R.M. Silva Unidades em $\mathbb{Z}C_{2p}$ e Aplicações, Tese de doutorado apresentada ao Instituto de Matemática e Estatística da USP, são Paulo, (2012)

[19] G. Vega, Determining the Number of One-Weight Cyclic Codes when Length and Dimension are Given, Lecture Notes in Computer Science **4547**, *284-293, (2007).*

[20] E. Witt. Die algebraische Struktur des Gruppenringes eine endlichen Gruppe über eine Zahlenkörper, J. Für Math. 190: 231 - 245, (1952).