Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Idempotentes em Álgebras de Grupos
e
Códigos Abelianos Minimais

por

Ailton Ribeiro de Assis

sob orientação do

Prof. Dr. Antônio de Andrade e Silva

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCEN - UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Setembro/2011

João Pessoa - PB

A848i Assis, Ailton Ribeiro de.
Idempotentes em álgebras de grupos e códigos abelianos minimais / Ailton Ribeiro de Assis. – João Pessoa, 2011.
67f.
Orientador: Antônio de Andrade e Silva.
Dissertação (Mestrado) - UFPB/CCEN.
1.Matemática. 2.Álgebras de grupos. 3.Corpos finitos. 4.Código minimal. 5. Código abeliano.

UFPB/BC CDU: 51(043)

Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Idempotentes em Álgebras de Grupos e Códigos Abelianos Minimais

por

Ailton Ribeiro de Assis

Dissertação apresentada ao Departamento de Matemática da Universidade Federal da Paraíba, como requisito parcial para a obtenção do título de Mestre em Matemática.

Área de Concentração: Álgebra

Aprovada por:

Prof. Dr. Antônio de Andrade e Silva - UFPB (Orientador)

Prof. Dr. André Luiz Meireles Araújo - UFPE

Prof. Dr. Fernando Xavier de Souza - UFPB

Dedicatória

Aos meus pais.

Agradecimentos

Agradeço a Deus por me dar saúde, força e capacidade, mesmo não merecendo.

Agradeço aos meus pais pelo apoio e amor incondicional. A Arilson e Hélen, meus queridos irmãos. A Jéssica, por sempre me apoiar, e aos meus amigos Elton, Hellosman, David Patrício, Ruben Neto e tantos outros que fazem meus dias serem mais divertidos.

Agradeço ao meu orientador, Professor Antônio de Andrade e Silva. Posso dizer que tive a sorte de contar com a sua ajuda. Muito obrigado pela dedicação, amizade e acima de tudo, pela confiança depositada em mim ao aceitar me orientar.

Agradeço também o apoio de todos os professores e funcionários do DM da UFPB.

Agradeço a todos os meus colegas de graduação e pós-graduação, em especial a Joedson, Claudemir, Tarciana, Valdecir, Marcos Aurélio, Antônio Pereira e Flávio Alves.

Por fim a Capes pelo apoio financeiro.

Resumo

Neste trabalho, estudamos álgebras de grupos semisimples $\mathbb{F}_q C_n$ de grupos abelianos finitos C_n sobre um corpo finito $\mathbb{F}_q$ e as condições para que o número de componentes simples seja mínimo, ou seja igual ao número de componentes simples sobre a álgebra de grupos racionais do mesmo grupo. Sob tais condições, calculamos o conjunto de idempotentes primitivos de $\mathbb{F}_q G$ e a de partir daí, estudamos os códigos cíclicos como ideais minimais da álgebra de grupo, os quais são gerados pelos idempotentes primitivos, calculando suas dimensões e distâncias mínimas.

Palavras chave: Álgebras de grupos; Corpos finitos; Código minimal, Código abeliano

Abstract

In this work, we study the semisimple group algebras $\mathbb{F}_q C_n$ of the finite abelian groups C_n over a finite field $\mathbb{F}_q$ and give conditions so that the number of its simple components is minimal; i.e. equal to the number of simple components of the rational group algebra of the same group. Under such conditions, we compute the set of primitive idempotents of $\mathbb{F}_q C_n$ and from there, we study the abelian codes as minimal ideals of the group algebra, which are generated by the primitive idempotents, computing their dimension and minimum distances.

Key words: Group algebra; Finite field; Minimal code; Abelian code

Notação

- $\mathbb{F}_q$ - corpo finito com q elementos onde q é a potência de um número primo;
- C_n - grupo cíclico de ordem n;
- $\mathbb{F}_q C_n$ - álgebra de grupo;
- $m_\alpha(x)$ - polinômio minimal de α;
- $\mathcal{C}_i$ - classes ciclotômicas;
- RG - Anel de Grupo;
- e_i - idempotentes centrais primitivos de R;
- $d(x,y) = |\{i : x_i \neq y_i,\ \ i = 0, \ldots, n-1\}|$ - distância de Hamming;
- $\deg P$ - grau do divisor P.

Sumário

Introdução **ix**

Introdução **x**

1 Resultados Básicos **1**

1.1 Corpos Finitos 1

1.2 Aneis de Grupos 8

1.3 Álgebras de Grupos Abelianos 14

2 Teoria dos Códigos **27**

2.1 Conceitos Básicos 28

2.2 Códigos Lineares 29

2.3 Códigos Cíclicos 32

3 Códigos Abelianos Minimais **37**

3.1 O Número de Componentes Simples 37

3.2 Códigos Cíclicos Minimais 43

3.3 Códigos Abelianos Minimais 46

3.4 Dimensão e Distância Mínima 49

Referências Bibliográficas **52**

Introdução

Histórico

Em nosso cotidiano os códigos corretores de erros aparecem de várias maneiras: surgem, por exemplo, quando fazemos o uso de informações digitalizadas, tais como na comunicação móvel, nos aparelhos de armazenamento de dados (gravador, CD, DVD), na comunicação via satélite, no processamento de imagens digitais, na internet, no rádio, etc. Um código corretor de erros é, basicamente, uma forma organizada de acrescentar algum dado a cada informação que precise ser transmitida ou armazenada, de modo que permita, ao recuperar a informação, detectar e corrigir os erros no processo de transmissão da informação.

Esta teoria teve início na década de 40 e atualmente é um campo de pesquisa muito atraente, tanto do ponto de vista científico quanto tecnológico, o que a torna um campo amplamente pesquisado em diversas áreas do conhecimento tais como, Matemática, Computação, Engenharia Elétrica, Estatística, entre outras. A teoria dos códigos é capaz de misturar conceitos e técnicas importantes da Álgebra abstrata com aplicações imediatas da vida real, o que mostra como a sofisticação tecnológica torna cada vez mais imperceptível a relação entre a chamada matemática pura e a matemática aplicada.

Na Teoria de Códigos Corretores de Erros, um conjunto finito $\mathbb{A}$ com q elementos é chamado de *alfabeto*. Os elementos de $\mathbb{A}$ serão chamados de *letras* ou *dígitos*. Uma sequência de n elementos de $\mathbb{A}$ é chamada de *palavra de comprimento* n. Um *código* de comprimento n é um subconjunto não trivial de $\mathbb{A}^n$, para algum $n \in \mathbb{N} : \mathcal{C} \subset \mathbb{A}^n$.

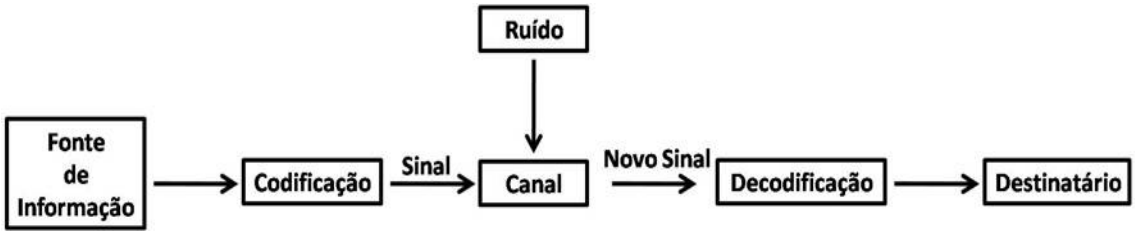
Um nome de destaque na Teoria dos Códigos é Richard W. Hamming. Ele se interessou pelos erros que ocorriam internamente nos computadores e desenvolveu um código corretor de único erro e códigos que detectam até dois erros e corrigem um único erro. Seu trabalho foi publicado em abril de 1950 no "*The Bell System Thechnical Journal*", publicação esta

que ocorreu dois anos após a conclusão do trabalho, devido ao pedido de patente feito pelo Laboratório Bell e durante os anos em que tais códigos foram elaborados, ele publicou alguns memorandos conforme sua pesquisa evoluía.

Hamming queria fazer um código mais eficiente e indagou se era possível construir um código corretor de único erro onde as palavras teriam quatro dígitos de informações e menos que oito dígitos de verificações. Esta questão foi respondida indiretamente em outubro de 1948 por C.E. Shannon, no artigo "*A Mathematical Theory of Communication*", publicado também no "*The Bell System Thechnical Journal*". Este artigo deu início a um novo campo da Engenharia Elétrica, a Teoria da Informação, cuja ênfase era o estudo do canal de comunicação que recebia interferência durante as transmissões de dados. A partir deste artigo, podemos dizer que houve um desenvolvimento contínuo e bastante significativo da Teoria de Códigos.

Em seu artigo, Shannon enfatiza que o problema fundamental da comunicação é a reprodução exata de cada caracter de modo como este foi enviado, pois cada mensagem tem um significado próprio.

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



Este esquema consiste essencialmente em cinco partes:

- **Fonte de Informação**: produz uma mensagem ou sequência de mensagens para serem transmitidas a um terminal receptor.
- **Codificador ou transmissor**: opera a mensagem produzindo um sinal para transmissão sobre um canal.
- **Canal**: meio usado para transmitir o sinal do codificador para o receptor.
- **Decodificador ou Receptor**: desempenha a operação inversa feita pelo codificador, reconstruindo a mensagem.

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

A medida que a Teoria de Códigos Corretores de Erros foi avançando, novas técnicas foram desenvolvidas incorporando estruturas algébricas mais elaboradas. Para nossos propósitos, consideramos *códigos lineares*, que são subespaços próprios do espaço vetorial $\mathbb{F}_q^n$, onde o alfabeto escolhido é um corpo finito $\mathbb{F}_q$ com q elementos. Em particular, um código linear $\mathcal{C}$ é chamado de *código cíclico* se para toda palavra $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ a palavra $(c_{n-1}, c_0, \ldots, c_{n-2})$, obtida através de c pela *troca cíclica* de coordenadas $i \mapsto i+1$, tomada módulo n, também é uma palavra código em $\mathcal{C}$. Os códigos cíclicos são muito utilizados por formarem uma classe de códigos lineares que possui bons algoritmos de codificação e de decodificação.

Observamos que o espaço vetorial $\mathbb{F}_q^n$ de dimensão n sobre $\mathbb{F}_q$ é isomorfo a álgebra de grupo $\mathbb{F}_qC_n$, onde C_n é o grupo cíclico de ordem n. Este isomorfismo estabelece uma correspondência entre os códigos cíclicos de $\mathbb{F}_q^n$ e os ideais do anel de grupo $\mathbb{F}_qC_n$. Desta maneira, códigos cíclicos de $\mathbb{F}_qC_n$ podem ser realizados como ideais de $\mathbb{F}_qC_n$. Além disso, sabemos que tal álgebra é um anel semisimples quando a característica do corpo $\mathbb{F}_q$ não divide n. Desta forma, um código cíclico minimal é um ideal minimal de $\mathbb{F}_qC_n$.

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

Descrição do trabalho

Este trabalho tem como objetivo principal o estudo dos códigos abelianos minimais. Para isto, no Capítulo 1 apresentaremos noções básicas sobre corpos finitos, aneis de grupos e alguns resultados sobre semissimplicidade de aneis e álgebras, culminando em uma adaptação do Teorema de Wedderburn-Artin 1.9. Em seguida, apresentaremos as definições e principais resultados sobre aneis de grupo bem como o Teorema de Maschke 1.10 que estabelece condições necessárias e suficientes para que uma anel de grupo seja semissimples e, assim, se decomponha em uma soma direta de ideais minimais bilaterais.

Para o caso em que G é um grupo finito e $\mathbb{F}$ é um corpo tal que a característica de $\mathbb{F}$ não divide a ordem de G, a álgebra de grupo é semissimples e, como tal, pode ser decomposta em uma soma direta de ideais minimais bilaterais, cada um deles gerado por um idempotente central primitivo. Desta maneira para descrever os códigos de grupo,

basta conhecermos os seus idempotentes geradores.

Como nosso foco são os códigos abelianos minimais, iniciaremos o Capítulo 2 com uma introdução à Teoria de Códigos Corretores de Erros, para estabelecer a linguagem utilizada nesta teoria. Em seguida, descreveremos os códigos cíclicos como ideais na álgebra de grupo $\mathbb{F}_q C_n$ do grupo cíclico finito C_n de ordem n e, para os códigos cíclicos minimais, utilizaremos a estrutura de subgrupos do grupo cíclico para calcular os idempotentes centrais primitivos geradores desses códigos.

O Capítulo 3 é o principal deste trabalho. Iniciaremos calculando o número de componentes simples de uma álgebra de grupo abeliano finito $\mathbb{F}G$ sobre corpos finitos e determinaremos sob que condições este número é mínimo, ou seja, igual número de componentes simples sobre a álgebra de grupos racionais de tais grupos. Utilizaremos estes resultados para calcular os idempotentes geradores de códigos abelianos minimais e estendemos os resultados de Arora e Pruthi. Sob estas condições, mostraremos como calcular as dimensões e as distâncias mínimas dos códigos abelianos minimais a partir de resultados gerais de aneis de grupos.

Capítulo 1

Resultados Básicos

Neste capítulo fixaremos algumas notações e apresentaremos algumas definições e resultados básicos sobre corpos finitos, aneis de grupos, necessários para o desenvolvimento do nosso trabalho. As demonstrações omitidas neste capítulos podem ser encontradas em [6, 8].

1.1 Corpos Finitos

Sejam $p \in \mathbb{N}$ um número primo e

$$\mathbb{F}_p = GF(p) = \{0, 1, \ldots, p-1\}$$

um conjunto de inteiros. Então $\varphi : \mathbb{Z}_p \to \mathbb{F}_p$ definida como $\varphi(\overline{a}) = a$ é uma bijeção. Logo, $\mathbb{F}_p$ com as operações induzidas por φ é um corpo finito, chamado de *corpo de Galois* de ordem p. Portanto, φ é um isomorfismo.

Sejam $\mathbb{F}$ um corpo finito e $\mathbb{K}$ um subcorpo de $\mathbb{F}$. Então o grau de $\mathbb{F}$ sobre $\mathbb{K}$, em símbolos $[\mathbb{F} : \mathbb{K}]$, é a dimensão de $\mathbb{F}$ visto como um espaço vetorial sobre $\mathbb{K}$. O corpo $\mathbb{F}$ é chamado uma *extensão finita* de $\mathbb{K}$ se $[\mathbb{F} : \mathbb{K}]$ é finito.

Lema 1.1 *Sejam $\mathbb{F}$ um corpo finito e $\mathbb{K}$ um subcorpo de $\mathbb{F}$, com $|\mathbb{K}| = q$. Então $|\mathbb{F}| = q^m$, em que $[\mathbb{F} : \mathbb{K}] = m$.*

Prova. Como $\mathbb{F}$ é um espaço vetorial sobre $\mathbb{K}$ e $\mathbb{F}$ é um corpo finito temos que $[\mathbb{F} : \mathbb{K}] = m$, para algum $m \in \mathbb{N}$. Assim,

$$\mathbb{F} \cong \mathbb{K}^m.$$

Portanto, $|\mathbb{F}| = q^m$. ■

Corolário 1.1 *Seja $\mathbb{F}$ um corpo finito. Então $|\mathbb{F}| = p^m$, com p a característica de $\mathbb{F}$ e $[\mathbb{F} : \mathbb{Z}_p] = m$.*

Seja R um anel comutativo com identidade. Um elemento $p \in R$ é *irredutível* sobre R se as seguintes condições são satisfeitas:

1. $p \neq 0$ e $p \notin \mathcal{U}(R)$.

2. Se $p = bc$, então $b \in \mathcal{U}(R)$ ou $c \in \mathcal{U}(R)$, isto é, p não tem divisores próprios.

Proposição 1.1 *Sejam $\mathbb{K}$ um corpo qualquer e $f(x) \in \mathbb{K}[x]$. Então $f(x)$ é irredutível sobre o corpo $\mathbb{K}$ se, e somente se,*

$$\frac{\mathbb{K}[x]}{\langle f(x) \rangle}$$

é um corpo. ■

Se $\mathbb{K} = \mathbb{F}_p$ e $\partial(f(x)) = m$, então o número de elementos do corpo

$$\frac{\mathbb{F}_p[x]}{\langle f(x) \rangle} = \{r(x) + \langle f(x) \rangle : r(x) \in \mathbb{F}_p[x] \text{ e } \partial(r(x)) < m\}$$

é igual ao número de polinômios em $\mathbb{F}_p[x]$ com grau menor do que m, a saber, p^m. Neste caso,

$$\frac{\mathbb{F}_p[x]}{\langle f(x) \rangle} = \{a_0 + a_1 x + \cdots + a_{m-1}x^{m-1} : a_i \in \mathbb{F}_p\} \cong \mathbb{F}_{p^m}$$

Teorema 1.1 (Kronecker) *Se $\mathbb{K}$ é um corpo qualquer e $f(x) \in \mathbb{K}[x]$ é irredutível sobre $\mathbb{K}$, então existe um corpo L contendo $\mathbb{K}$ e as raízes de $f(x)$.*

Lema 1.2 *Seja $\mathbb{K}$ um corpo de característica $p > 0$. Então*:

1. *$pa = 0$, para todo $a \in \mathbb{K}$.*

2. *$(a \pm b)^{p^k} = a^{p^k} \pm b^{p^k}$, para todos $a, b \in \mathbb{K}$ e $k \in \mathbb{N}$.*

3. *A função $\varphi : \mathbb{K} \to \mathbb{K}$ definida por $\varphi(a) = a^p$ é um homomorfismo de corpos injetor. Neste caso,*

$$Im(\varphi) = \mathbb{K}^p$$

é um subcorpo de $\mathbb{K}$.

Seja $f(x) \in \mathbb{K}[x]$ irredutível sobre o corpo F. Então, pelo Teorema de Kronecker, existe um corpo L contendo $\mathbb{K}$ tal que

1. $f(x) = (x - a_1) \cdots (x - a_m)$ em L.

2. $L = \mathbb{K}[a_1, \ldots, a_m]$.

O corpo L é chamado o *corpo de decomposição* de $f(x)$ sobre $\mathbb{K}$. Note que L é minimal com respeito à condição (1), isto é, se f decompõe sobre F, com $\mathbb{K} \subseteq F \subseteq L$, então $F = L$.

Teorema 1.2 *Sejam p um número primo e $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$, para algum $n \in \mathbb{N}$. Então L é o corpo de decomposição de $f(x)$ se L possui p^n elementos.*

Prova. Suponhamos que L seja o corpo de decomposição de $f(x)$ sobre $\mathbb{F}_p$. Como o $mdc(f(x), f'(x)) = 1$ temos que as raízes de $f(x)$ são todas distintas em L. Logo, L possui pelo menos p^n elementos. Agora, consideremos o subconjunto

$$F = \{\alpha \in L : f(\alpha) = 0\} = \{\alpha \in L : \alpha^{p^n} = \alpha\}$$

de L. Então é fácil verificar que F é um subcorpo de L, com p^n elementos. Portanto, $F = L$.

Suponhamos que L contenha p^n elementos. Como $L^\bullet$ é um grupo multiplicativo de ordem $p^n - 1$ temos, pelo Teorema de Lagrange, que $\alpha^{p^n - 1} = 1$, para todo $\alpha \in L^\bullet$, ou seja, $\alpha^{p^n} = \alpha$, para todo $\alpha \in L^\bullet$. Assim, $\alpha^{p^n} = \alpha$, para todo $\alpha \in L$. Portanto, $f(x)$ fatora-se em L. Neste caso,

$$f(x) = \prod_{\alpha \in L} (x - \alpha),$$

que é o resultado desejado. ■

Corolário 1.2 *Quaisquer dois corpos finitos, com p^n elementos, são isomorfos.*

Corolário 1.3 *O corpo $GF(p^n) = \mathbb{F}_{p^n}$ é o corpo de decomposição de $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$.*

Corolário 1.4 *O corpo $\mathbb{F}_{q^n}$ existe, para qualquer número primo p e qualquer número $n \in \mathbb{N}$.*

Lema 1.3 *Sejam G um grupo abeliano e $a, b \in G$, com ordens m e n. Então*:

1. *Existe um elemento de ordem $k = mmc(m, n)$.*

2. *Se a ordem maximal dos elementos de G é igual a N, então $a^N = e$, para todo $a \in G$.*

Teorema 1.3 *Sejam $\mathbb{K}$ um corpo qualquer e G um subgrupo finito de $\mathbb{K}^\bullet$. Então G é um grupo cíclico. Em particular, se $\mathbb{K}$ é um corpo finito, então $\mathbb{K} = \mathbb{Z}_p(\alpha)$, para algum $\alpha \in \mathbb{K}$.*

Prova. Seja $|G| = n$. Então, pelo item (2) do Lema 1.3, existe um número inteiro maximal N tal que $a^N = 1$, para todo $a \in G$. Como o polinômio $f(x) = x^N - 1 \in \mathbb{K}[x]$ possui no máximo N raízes distintas em $\mathbb{K}$ temos que $n \leq N$. Por outro lado, pelo Teorema de Lagrange, $N \leq n$. Portanto, $n = N$ e G contém um elemento de ordem n, isto é, G é um grupo cíclico. Finalmente, existe $\alpha \in \mathbb{K}^\bullet$ tal que $\mathbb{K}^\bullet = \langle \alpha \rangle$. Como $\mathbb{Z}_p(\alpha)$ é a menor extensão que contém α e $\mathbb{Z}_p$ temos que $\mathbb{K} = \mathbb{Z}_p(\alpha)$. ■

Teorema 1.4 *Seja $\mathbb{K}$ um corpo qualquer. Então $x^m - 1$ divide $x^n - 1$ em $\mathbb{K}[x]$ se, e somente se, m divide n. Além disso,*

$$mdc(x^m - 1, x^n - 1) = x^{mdc(m,n)} - 1.$$

Prova. Pelo o Algoritmo da Divisão, existem $q, r \in \mathbb{Z}$ tais que

$$n = qm + r, \text{ com } 0 \leq r < m.$$

Logo,

$$\begin{aligned} x^n - 1 &= x^{qm+r} - 1 = x^r x^{qm} - x^r + x^r - 1 \\ &= x^r(x^{qm} - 1) + x^r - 1 \\ &= x^r \left(\sum_{i=0}^{q-1} x^{iq} \right) (x^m - 1) + x^r - 1. \end{aligned}$$

Portanto, $x^m - 1$ divide $x^n - 1$ em $\mathbb{K}[x]$ se, e somente se, m divide n. ■

Corolário 1.5 *Para qualquer número primo p, $p^m - 1$ divide $p^n - 1$ se, e somente se, m divide n.*

Seja $\mathbb{F}$ um corpo finito de característica p. Diremos que $\alpha \in \mathbb{F}$ é um *elemento primitivo* se $\mathbb{F} = \mathbb{Z}_p(\alpha)$. Neste caso, o número de elementos primitivos de $\mathbb{F}$ é igual a

$$\phi(p^n - 1),$$

em que ϕ é a função de Euler.

Teorema 1.5 *Sejam p um número primo p e $m, n \in \mathbb{N}$. Então*:

1. *$\mathbb{F}_{p^m}$ é um subcorpo de $\mathbb{F}_{p^n}$ se, e somente se, m divide n.*

2. *Para cada divisor m de n, existe um único subcorpo $\mathbb{F}_{p^m}$ de $\mathbb{F}_{p^n}$.*

Prova. (1) Suponhamos que $\mathbb{F}_{p^m}$ seja um subcorpo de $\mathbb{F}_{p^n}$. Então a dimensão de $\mathbb{F}_{p^n}$ sobre $\mathbb{F}_{p^m}$ é igual k, para algum $k \in \mathbb{N}$. Logo,

$$p^n = (p^m)^k = p^{km}$$

e m divide n. Reciprocamente, pelo Teorema 1.4 e seu Corolário, obtemos $x^{p^m-1} - 1$ divide $x^{p^n-1} - 1$. Logo, qualquer raíz de $x^{p^m} - x$ em $\mathbb{F}_{p^m}$ é também uma raíz de $x^{p^n} - x$. Portanto, estão em $\mathbb{F}_{p^n}$, ou seja, $\mathbb{F}_{p^m}$ é um subcorpo de $\mathbb{F}_{p^n}$.

(2) Note que para cada divisor m de n, existe um único subcorpo $\mathbb{F}_{p^m}$ de $\mathbb{F}_{p^n}$, caso contrário, existiria mais do que p^m raízes de $x^{p^m} - x$. ■

Teorema 1.6 *Seja $f(x) \in \mathbb{F}_q[x]$ um polinômio irredutível de grau k, com $q = p^m$. Então $\mathbb{F}_{q^k}$ é o corpo de decomposição de f.*

Prova. Seja α uma raiz de f e consideremos a extensão $\mathbb{F}_q(\alpha)$. Se

$$f(x) = a_0 + a_1 x + \cdots + a_k x^k,$$

então, pelo Lema 1.2,

$$f(\alpha^{q^i}) = \sum_{j=0}^{k} a_j (\alpha^{q^i})^j = \sum_{j=0}^{k} a_j \alpha^{jq^i} = \left(\sum_{j=0}^{k} a_j \alpha^j \right)^{q^i} = 0,$$

isto é,

$$\alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{k-1}}$$

são todas as outras raízes de $f(x)$, chamadas *conjugadas* de α. Sejam l o menor inteiro positivo tal que

$$\alpha^{q^l} = \alpha.$$

e

$$g(x) = \prod_{j=0}^{l-1} (x - \alpha^{q^j})$$

Então, pelo Lema 1.2,

$$(g(x))^q = \prod_{j=0}^{l-1}(x-\alpha^{q^j})^q = \prod_{j=0}^{l-1}(x^q-\alpha^{q^{j+1}}) = \prod_{j=0}^{l-1}(x^q-\alpha^{q^j}) = g(x^q).$$

Assim, se

$$g(x) = b_0 + b_1x + \cdots + b_lx^l,$$

então

$$\sum_{j=0}^{l} b_j^q x^{jq} = (g(x))^q = g(x^q) = \sum_{j=0}^{l} b_j x^j,$$

ou seja, $b_j^q = b_j$ e $g(x) \in \mathbb{F}_q[x]$. Como $g(x)$ divide $f(x)$ no corpo de decomposição para $f(x)$ temos que $g(x)$ divide $f(x)$ em $\mathbb{F}_q[x]$. Portanto, $g(x) = f(x)$ e $l = k$. Consequentemente, $\mathbb{F}_{q^k}$ é o corpo de decomposição de f, pois

$$1, \alpha, \ldots, \alpha^{k-1}$$

são linearmente independentes. ■

Teorema 1.7 *Seja $f(x) \in \mathbb{F}_q[x]$ um polinômio irredutível de grau k, com $q = p^m$. Então $f(x)$ divide $x^{q^n} - x$ em $\mathbb{F}_q[x]$ se, e somente se, k divide n.*

Prova. Suponhamos que $f(x)$ divida $x^{q^n} - x$ em $\mathbb{F}_q[x]$. Então o corpo de decomposição $\mathbb{F}_{q^k}$ de $f(x)$ está contido em $\mathbb{F}_{q^n}$, pois todas as raízes de $f(x)$ estão em $\mathbb{F}_{q^n}$. Assim, pelo Teorema 1.5, k divide n. Reciprocamente, suponhamos que k divide n. Então, pelo Teorema 1.5, $\mathbb{F}_{q^k}$ está contido em $\mathbb{F}_{q^n}$. Assim, $f(x)$ divide $x^{q^n} - x$ em $\mathbb{F}_{q^n}[x]$, pois $f(x)$ e $x^{q^n} - x$ fatoram-se sobre $\mathbb{F}_{q^n}$. Portanto, $f(x)$ divide $x^{q^n} - x$ em $\mathbb{F}_q[x]$. ■

Observação 1.1 *Já vimos que se α é uma raiz do polinômio irredutível $f(x)$ de grau k, então*

$$\alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{k-1}}$$

são as outras raízes de $f(x)$. Note que como $mdc(p, q-1) = 1$ temos que

$$\left(\alpha^{q^j}\right)^{q-1} = 1,$$

pois $\mathbb{F}_q^\bullet$ é um grupo cíclico de ordem $q-1$, ou seja, os conjugados de α com relação à qualquer subcorpo de $\mathbb{F}_q$ possuem a mesma ordem em $\mathbb{F}_q^\bullet$. Além disso, $f(x)$ só possui raízes simples, pois as raízes de $x^{q^n} - x$ são todas simples.

Corolário 1.6 *O polinômio* $f(x) = x^{q^n} - x \in \mathbb{F}_q[x]$ *pode ser fatorado em um produto de polinômio mônicos irredutíveis sobre* $\mathbb{F}_q$*, cujo grau divide* n*.*

Prova. Basta observar que se $g(x)$ e $h(x)$ são polinômio mônicos irredutíveis e distintos sobre $\mathbb{F}_q$ que dividem $f(x)$, então $g(x)h(x)$ divide $f(x)$, pois $mdc(g(x), h(x)) = 1$. Agora, aplique a Observação. ■

Seja α um elemento de $\mathbb{F}_{q^n}$. O *polinômio minimal* de α, em símbolos $m_\alpha(x)$, é o polinômio mônico irredutível sobre $\mathbb{F}_q$ que tem α como raiz. Note que α e α^p possuem o mesmo polinômio minimal, pois pela prova do Teorema 1.6, $[m_\alpha(x)]^p = m_\alpha(x^p)$. Além disso, o grau k de $m_\alpha(x)$ é o menor inteiro positivo tal que

$$\alpha^{q^k} \equiv 1 \ \ (mod q^n - 1).$$

Seja $\eta \in \mathbb{F}_{q^n}$ um elemento primitivo. Então

$$\mathbb{F}_{q^n} = \mathbb{F}_q(\eta) = \langle \eta \rangle = \{\eta^i : i = 0, 1, \ldots, q^n - 2\}.$$

Logo,

$$x^{q^n} - x = m_1(x) \cdots m_l(x),$$

com $m_i(x) = m_{\eta^i}(x) = m_{\eta^{iq^j}}(x)$, $i = 1, \ldots, l$. Assim,

$$\mathcal{R}_{m_i} = \{\eta^i, \eta^{qi}, \eta^{q^2 i}, \ldots, \eta^{(q^{k_i}-1)i}\}$$

é o conjunto das raízes de $m_i(x)$ e $\partial(m_i(x)) = k_i$ divide n. Note que estes conjuntos formam uma partição de $\mathbb{F}_{q^n}$, com $|\mathcal{R}_{m_i}| = 1$ nos elementos de $\mathbb{F}_q$. Portanto, essa partição de $\mathbb{F}_{q^n}$ induz uma partição no conjunto de inteiros

$$S_{q^n-1} = \{0, 1, \ldots, q^n - 2\},$$

a saber,

$$\mathcal{C}_i = \{i, qi, q^2 i, \ldots, (q^{k_i}-1)i\},$$

onde os inteiros são lidos módulo $q^n - 1$. Reciprocamente, a função $\sigma : S_{q^n-1} \to S_{q^n-1}$ definida como

$$\sigma(i) = iq \ \ (mod q^n - 1)$$

está bem definida. Portanto, obtemos uma partição

$$\mathcal{C}_i = \{i, qi, q^2 i, \ldots, (q^{k_i}-1)i\},$$

de S_{q^n-1} e cada conjunto $\mathcal{C}_i$ corresponde a um polinômio minimal $m_i(x)$, pois k_i é o menor inteiro positivo tal que

$$q^{k_i} i \equiv i \ \ (mod q^n - 1) \ \ (\alpha^{q^{k_i}} \equiv 1 \ \ (mod q^n - 1)).$$

Os conjuntos $\mathcal{C}_i$ são chamados de *classes ciclotômicas* módulo $q^n - 1$ ou $(q^n - 1)$-*classes ciclotômicas*. Note que i no índice do conjunto $\mathcal{C}_i$ é o representante de classe e

$$m_i(x) = \prod_{j \in \mathcal{C}_i} (x - \eta^j).$$

Exemplo 1.1 *Sejam* $p = 2$, $n = 4$ *e* $q = 2$. *Então* $\mathbb{F}_{2^4}$ *é um corpo, com* 16 *elementos, e as classes ciclotômicas módulo* 15 *são*:

$$\begin{aligned} \mathcal{C}_0 &= \{0\} \\ \mathcal{C}_1 &= \{1, 2, 4, 8\} \\ \mathcal{C}_3 &= \{3, 6, 12, 9\} \\ \mathcal{C}_5 &= \{5, 10\} \\ \mathcal{C}_7 &= \{7, 14, 13, 11\}. \end{aligned}$$

1.2 Aneis de Grupos

Nesta seção introduzimos a definição de um anel de grupo RG de um grupo G sobre um anel com unidade R. Além disso, discutiremos condições sobre o grupo G e sobre o anel R para que o anel de grupo RG seja semissimples e apresentaremos o Teorema de Maschke.

Sejam G um grupo e R um anel com unidade. Definiremos por RG o conjunto de todas as "somas formais" do tipo

$$\alpha = \sum_{g \in G} \alpha(g) g, \ \text{ onde } \ \alpha(g) \in R.$$

Note que a definição implica que dados

$$\alpha = \sum_{g \in G} \alpha(g) g \ \text{ e } \ \beta = \sum_{g \in G} \beta(g) g \in RG,$$

diremos que α é *igual* β se, e somente se,

$$\alpha(g) = \beta(g), \ \ \forall \ g \in G.$$

O suporte de α, em símbolos $supp(\alpha)$, é o conjunto

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

Pode-se definir a soma de dois elementos α e β de RG como

$$\alpha + \beta = \sum_{g \in G} (\alpha(g) + \beta(g))g \tag{1.1}$$

e seu produto por um escalar $\lambda \in R$ como

$$\lambda\alpha = \lambda \left(\sum_{g \in G} \alpha(g)g \right) = \sum_{g \in G} (\lambda\alpha(g))g \tag{1.2}$$

Finalmente, pode-se definir o produto de dois elementos α e β de RG como

$$\alpha\beta = \sum_{g \in G} \sum_{h \in G} (\alpha(g)\beta(h))gh = \sum_{f \in G} \gamma(f)f, \tag{1.3}$$

com

$$\gamma(f) = \sum_{g \in G} \alpha(g)\beta(g^{-1}f)$$

e $\alpha(g)\beta(h)$ indica o produto em R e gh o produto em G. Com as operações soma e produto definidas em (1.1) e (1.3) acima, RG é um anel com unidade

$$1 = \sum_{g \in G} \alpha(g)g,$$

com $\alpha(1) = 1$ e $\alpha(g) = 0$, para todo $g \in G - \{1\}$. O anel RG será chamado de *anel de grupo*.

Note que RG com a soma (1.1) e o produto por um escalar (1.2) é um R-módulo. Além disso, se R for um anel comutativo, RG é uma R-álgebra sobre R. Neste caso, chamamos RG de *álgebra de grupo* de G sobre R.

A função imersão $\iota : G \to RG$ definida como

$$\iota(g) = \sum_{h \in G} x(h)h \in RG,$$

com $x(g) = 1$ e $x(h) = 0$, para todo $h \in G - \{g\}$. é um monomorfismo de grupos. Assim, podemos identificar G com sua imagem $\iota(G)$ em RG. Portanto, com essa identificação, podemos considerar G como uma base de RG sobre R.

A função inclusão $\nu : R \to RG$ definida como

$$\nu(a) = \sum_{g \in G} x(g)g \in RG,$$

com $x(1) = a$ e $x(g) = 0$, para todo $g \in G - \{1\}$. é um monomorfismo de aneis. Assim, podemos identificar R com sua imagem $\nu(R)$ em RG.

A partir dessas identificações podemos concluir que: $ag = ga$ em RG, para todo $a \in R$ e $g \in G$.

Lema 1.4 *Sejam $\sigma : R \to S$ um homomorfismo de aneis, com $\sigma(1) = 1$, e M um S-módulo à esquerda. Então M munido com a ação*

$$a * m = \sigma(a)m$$

é um R-módulo à esquerda.

Teorema 1.8 *Sejam R um anel e G um grupo. Então temos a seguinte propriedade universal: para qualquer anel S contendo R e qualquer função $\sigma : G \to S$ tal que $\sigma(gh) = \sigma(g)\sigma(h)$, para todos $g, h \in G$, existe um único homomorfismo de aneis R-linear $\varphi : RG \to S$ tal que $\sigma = \varphi \circ \iota$, com $\iota : G \to RG$. Em particular, se $R \subseteq \mathcal{Z}(S)$, então φ é um homomorfismo de R-álgebras.*

Prova. A função $\varphi : RG \to S$ definida como

$$\varphi\left(\sum_{g\in G} \alpha(g)g\right) = \sum_{g\in G} \alpha(g)\sigma(g)$$

tem as propriedades desejadas. ■

Corolário 1.7 *Sejam R um anel e $\varphi : G \to H$ um homomorfismo de grupos. Então existe um único homomorfismo de aneis $\widehat{\varphi} : RG \to RH$ tal que $\widehat{\varphi}|_G = \varphi$. Em particular, se R é um anel comutativo, então $\widehat{\varphi}$ é um homomorfismo de R-álgebras. Além disso, se φ é injetor, sobrejetor ou bijetor, então $\widehat{\varphi}$ também o é.*

Lema 1.5 *Sejam S um anel com identidade, R um subanel de S, com a mesma identidade de S, e G um grupo. Então*

$$SG \simeq S \otimes_R RG.$$

Prova. Note que a multiplicação sobre $S \otimes_R RG$ é definida distributivamente como segue

$$(s \otimes \alpha)(t \otimes \beta) = st \otimes \alpha\beta, \ \ \forall \ \ s, t \in S \ \text{ e } \ \alpha, \beta \in RG.$$

Assim, a função $\sigma : G \to S \otimes_R RG$ definida como $\sigma(g) = 1 \otimes g$ satisfaz as condições do Teorema 1.8, Portanto, existe um único homomorfismo de aneis R-linear $\varphi : SG \to S \otimes_R RG$ tal que

$$\varphi(\alpha) = 1 \otimes \alpha.$$

Por outro lado, a função $\tau : S \times RG \to SG$ definda como

$$\tau(s, \alpha) = s\alpha$$

é um homomorfismo de aneis R-bilinear. Assim, existe um único homomorfismo de R-álgebras $\psi : S \otimes_R RG \to SG$ definido como

$$\psi(s \otimes \alpha) = s\alpha.$$

Note que

$$(\psi \circ \varphi)(\alpha) = \psi(1 \otimes \alpha) = \alpha$$

e

$$(\varphi \circ \psi)(s \otimes \alpha) = \varphi(s\alpha) = s(1 \otimes g) = (s \otimes \alpha),$$

ou seja, $\psi \circ \varphi = I_{SG}$ e $\varphi \circ \psi = I_{(S \otimes_R RG)}$. Portanto, $SG \simeq S \otimes_R RG$. ■

Proposição 1.2 *Sejam R um anel comutativo com identidade e G, H grupos. Então*

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

Prova. A função $\sigma : G \times H \to (RG)H$ definida como

$$\varphi(g, h) = gh$$

é tal que

$$\begin{aligned} \sigma((g_1, h_1) \cdot (g_2, h_2)) &= \sigma(g_1 g_2, h_1 h_2) = g_1 g_2 h_1 h_2 = g_1 h_1 g_2 h_2 \\ &= \sigma(g_1, h_1) \cdot \sigma(g_2, h_2), \ \ \forall \ (g_1, h_1), (g_2, h_2) \in G \times H. \end{aligned}$$

Assim, pelo Teorema 1.8, existe um único homomorfismo de R-álgebras

$$\varphi : R(G \times H) \to (RG)H$$

tal que

$$\varphi\left(\sum_{(g,h)\in G\times H}\alpha(g,h)(g,h)\right) = \sum_{(g,h)\in G\times H}\alpha(g,h)\sigma(g,h)$$
$$= \sum_{h\in H}\left(\sum_{g\in G}\alpha(g,h)g\right)h.$$

É fácil verificar que φ é bijetor.

Finalmente, pelo Lema 1.5, obtemos $(RG)H \simeq RG \otimes_R RH$, $RG \otimes_R RH$ e $R(G \times H)$ são isomorfos. ■

Proposição 1.3 *Sejam $\{R_i\}_{i\in I}$ uma família de aneis e $R = \sum_{i\in I} R_i$. Então*

$$RG \simeq \sum_{i\in I} R_i G,$$

para qualquer grupo G.

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

Teorema 1.9 (Teorema de Maschke Generalizado) *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 em que $R = \mathbb{F}$ é um corpo é de grande importância, pois $\mathbb{F}$ é sempre semissimples e $|G|$ é invertível em $\mathbb{F}$ se, e somente se, $|G| \neq 0$ em $\mathbb{F}$, isto é, se, e somente se, a característica de $\mathbb{F}$ não divide $|G|$.

Corolário 1.8 *Sejam G um grupo finito e $\mathbb{K}$ um corpo. Então $\mathbb{K}G$ é semissimples se, e somente se, a característica de $\mathbb{K}$ não divide a ordem de G.*

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

Teorema 1.10 *Sejam G um grupo finito e $\mathbb{F}$ um corpo tal que a característica de $\mathbb{F}$ não divide $|G|$. Então*:

1. *$\mathbb{F}G$ é uma soma direta de um número finito de ideais minimais $\{B_i\}_{1\leq i\leq r}$, as componentes simples de $\mathbb{F}G$. Cada B_i é um anel simples.*

2. *Qualquer ideal de $\mathbb{F}G$ é uma soma direta de alguns dos membros da família $\{B_i\}_{1\leq i\leq r}$.*

3. *Cada componente simples B_i é isomorfa a um anel de matrizes completo da forma $M_{n_i}(D_i)$, com D_i um anel de divisão contendo uma cópia de $\mathbb{F}$ em seu centro, e o isomorfismo*

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

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

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

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

é um ideal minimal á esquerda.

Dado $x \in \mathbb{F}G$, consideremos

$$\phi(x) = (\alpha_1, \ldots, \alpha_r) \in \sum_{i=1}^{r} M_{n_i}(D_i)$$

e definimos o produto de x por um elemento $m_i \in I_i$ como

$$xm_i = \alpha_i m_i.$$

Com esta definição I_i torna-se um $\mathbb{F}G$-módulo simples.

5. *Se $i \neq j$, então $I_i \ncong I_j$.*

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

Corolário 1.9 *Sejam G um grupo finito e $\mathbb{F}$ um corpo algebricamente fechado tal que a característica de $\mathbb{F}$ não divide $|G|$. Então*:

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

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

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

Teorema 1.11 *Seja $R = \oplus_{i=1}^{s} A_i$ uma decomposição de um anel semissimples como soma direta de ideais minimais. Então existe uma família $\{e_1, \ldots, e_s\}$ de elementos de R tal que*:

1. *$e_i \neq 0$ é um idempotente central de R, $i = 1, \ldots, s$.*
2. *Se $i \neq j$, então $e_i e_j = 0$.*
3. *$1 = e_1 + \cdots + e_s$.*
4. *e_i não pode ser escrito como $e_i = e_i' + e_i''$, em que e_i' e e_i'' são idempotentes centrais não nulos tais que $e_i' e_i'' = 0$, $1 \leq i \leq s$.*

Os elementos $e_1, \ldots, e_s$ do teorema são chamados de *idempotentes centrais primitivos* de R.

1.3 Álgebras de Grupos Abelianos

Nesta seção descreveremos álgebras de grupo de grupos abelianos finitos G sobre corpos $\mathbb{F}$ de característica relativamente prima com a ordem do grupo, isto é, de modo que a álgebra de grupo seja semissimples. Esta caracterização foi dada por Perlis e Walker [7].

Sejam G um grupo cíclico finito de ordem n:

$$G = \langle a \rangle = \{1, a, a^2, \ldots, a^{n-1}\}$$

e $\mathbb{F}$ um corpo tal que a característica de $\mathbb{F}$ não divide n. Consideremos a função avaliação

$$\begin{array}{rccc} \varphi: & \mathbb{F}[x] & \to & \mathbb{F}G \\ & f(x) & \mapsto & f(a) \end{array}$$

É fácil verificar que φ é um epimorfismo de aneis e, pelo Primeiro Teorema de Isomorfismo,

$$\mathbb{F}G \simeq \frac{\mathbb{F}[x]}{\ker \varphi},$$

com

$$\ker \varphi = \{f(x) \in \mathbb{F}[x] : f(a) = 0\}.$$

Como $\mathbb{F}[x]$ é um domínio de ideais principais temos $\ker\varphi$ é um ideal gerado pelo polinômio mônico irredutível $f_0(x)$ de menor grau tal que $f_0(a) = 0$. Neste caso, $f_0(x) = m_a(x)$ e a é algébrico sobre $\mathbb{F}$. É importante observar, sob este isomorfismo, que a imagem do elemento a é a classe

$$\varphi(a) = x + \langle f_0(x)\rangle \in \frac{\mathbb{F}[x]}{\langle f_0(x)\rangle}.$$

É claro que $x^n - 1 \in \ker\varphi$, pois $a^n = 1$. Note que se

$$f_0(x) = \sum_{i=0}^{r} k_i x^i$$

é um polinômio de grau $r < n$, então

$$f_0(a) = \sum_{i=0}^{r} k_i a^i \neq 0$$

em RG, pois os elementos $1, a, a^2, \ldots, a^r$ são linearmente independentes sobre $\mathbb{F}$. Portanto,

$$\ker\varphi = \langle x^n - 1\rangle$$

e

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

Seja

$$x^n - 1 = f_1(x) f_2(x) \cdots f_t(x)$$

a fatoração de $x^n - 1$ em fatores irredutíveis sobre $\mathbb{F}$. Como a característica de $\mathbb{F}$ não divide n temos que $f_i \neq f_j$, quando $i \neq j$. Logo, pelo o Teorema Chinês dos Restos, obtemos

$$\mathbb{F}G \simeq \frac{\mathbb{F}[x]}{\langle x^n - 1\rangle} \simeq \frac{\mathbb{F}[x]}{\langle f_1(x)\rangle} \oplus \frac{\mathbb{F}[x]}{\langle f_2(x)\rangle} \oplus \cdots \oplus \frac{\mathbb{F}[x]}{\langle f_t(x)\rangle},$$

pois

$$\langle f_i(x)\rangle + \langle f_j(x)\rangle = \mathbb{F}[x].$$

Assim, o gerador a de G é aplicado em

$$\varphi(a) = (x + \langle f_1(x)\rangle, \ldots, x + \langle f_t(x)\rangle).$$

Sejam ζ_i as raízes de $f_i(x)$ em um fecho algébrico de $\mathbb{F}$. Então

$$\frac{\mathbb{F}[x]}{\langle f_i(x)\rangle} \simeq \mathbb{F}(\zeta_i).$$

Consequentemente,

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

Como todos os elementos ζ_i são raízes de $x^n - 1$ temos que $\mathbb{F}G$ isomorfo a uma soma direta de extensões de $\mathbb{F}$. Neste caso, o elemento a é aplicado em

$$(\zeta_1, \zeta_2, \ldots, \zeta_t).$$

Observação 1.2 *Seja*

$$\widehat{f}_i(x) = \frac{x^n - 1}{f_i(x)} = \prod_{j \neq i} f_j, \;\; i = 1, \ldots, t.$$

Então é fácil verificar que os $\widehat{f}_1(x), \ldots, \widehat{f}_t(x)$ *são relativamente primos e que* $x^n - 1$ *divide* $\widehat{f}_i(x)\widehat{f}_j(x)$ *se* $i \neq j$. *Assim, existem* $g_1(x), \ldots, g_k(x) \in \mathbb{F}[x]$ *tais que*

$$\widehat{f}_1(x)g_1(x) + \cdots + \widehat{f}_k(x)g_k(x) = 1.$$

Pondo $e_i = \widehat{f}_i(a)g_i(a)$, *em* $\mathbb{F}G$, $i = 1, \ldots, t$, *obtemos*

$$e_1 + \cdots + e_t = 1 \;\; e \;\; e_i e_j = \delta_{ij} e_i.$$

Portanto,

$$\mathbb{F}G = \mathbb{F}Ge_1 \oplus \cdots \oplus \mathbb{F}Ge_t.$$

Fazendo $\zeta_i = ae_i$, $i = 1, \ldots, t$, *temos que* $\mathbb{F}Ge_i$ *é uma álgebra com unidade* e_i *e* $m_{\zeta_i}(x) = f_i(x)$.

Exemplo 1.2 *Sejam* G *um grupo cíclico de ordem* 7,

$$G = \langle a \rangle = \{1, a, a^2, a^3, a^4, a^5, a^6\},$$

e $\mathbb{F} = \mathbb{Q}$ *o corpo dos números racionais. Então*

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

é a fatoração de $x^7 - 1$ *em fatores irredutíveis sobre* $\mathbb{F}$. *Assim, se* ζ *é uma raíz sétima primitiva da unidade, então*

$$\mathbb{F}G \simeq \mathbb{F} \oplus \mathbb{F}(\zeta).$$

Neste caso, o gerador a *do grupo* G *é aplicado em*

$$(1, \zeta).$$

Finalmente, como

$$\widehat{f_1}(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \ \ e \ \ \widehat{f_2}(x) = x - 1$$

temos que

$$\frac{1}{7}\widehat{f_1}(x) + \left(-\frac{1}{7}\right)\widehat{f_2}(x)\left(x^5 + 2x^4 + 3x^3 + 4x^2 + 5x + 6\right) = 1.$$

Logo,

$$e_1 = \frac{1}{7}\left(a^6 + a^5 + a^4 + a^3 + a^2 + a + 1\right) \ \ e \ \ e_2 = -\frac{1}{7}\left(a^6 + a^5 + a^4 + a^3 + a^2 + a - 6\right).$$

Exemplo 1.3 *Sejam G um 2-grupo abeliano elementar de ordem 2^m e $\mathbb{F} = \mathbb{Q}$ o corpo dos números racionais. Mostre que $\mathbb{F}G$ é isomorfo a uma soma direta de 2^m cópias de $\mathbb{F}$.*

Solução. Vamos usar indução sobre m. Note que

$$G \simeq C_1 \times \cdots \times C_m,$$

com C_i, $i = 1, \ldots, m$, grupos cíclicos de ordem 2. Se $m = 1$, então, pelo Exemplo 1.2,

$$\mathbb{F}G \simeq \mathbb{F} \oplus \mathbb{F},$$

pois

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

Suponhamos que o resultado seja válido para qualquer grupo que é um produto direto de k cópias de grupos cíclicos de ordem 2, com $1 \leq k < m$. Pela Proposição 1.2, obtemos

$$\mathbb{F}G \simeq \mathbb{F}(C_1 \times \cdots \times C_{m-1}) \times C_m) \simeq (\mathbb{F}(C_1 \times \cdots \times C_{m-1}))C_m.$$

Logo, pela hipótese de indução,

$$\mathbb{F}(C_1 \times \cdots \times C_{m-1}) \simeq \mathbb{F}_1 \oplus \cdots \oplus \mathbb{F}_{m-1}, \ \text{ com } \mathbb{F}_i \simeq \mathbb{F} \oplus \mathbb{F}.$$

Como

$$\mathbb{F}G \simeq (\mathbb{F}_1 \oplus \cdots \oplus \mathbb{F}_{m-1})C_m \simeq \mathbb{F}_1 C_m \oplus \cdots \oplus \mathbb{F}_{m-1}C_m \ \text{ e } \ \mathbb{F}_i C_m \simeq \mathbb{F}C_m \oplus \mathbb{F}C_m$$

temos o resultado desejado. ■

Agora, vamos apresentar uma forma alternativa de decompor a álgebra de grupo de um grupo cíclico que nos possibilitará generalizar o resultado para grupos abelianos finitos.

Lembramos que, para um dado inteiro n, o *n-ésimo polinômio ciclotômico*, denotado por $\Phi_n(x)$, é definido como

$$\Phi_n(x) = \prod_{mdc(n,j)=1} (x - \zeta^j),$$

com ζ uma raiz n-ésima primitiva da unidade e o grau de $\Phi_n(x)$ é $\phi(n)$.

Sejam ζ_n uma raiz n-ésima primitiva da unidade e $\mathbb{F} = \mathbb{Q}$ o corpo dos números racionais. Então a função

$$\sigma : \frac{\mathbb{F}[x]}{\langle \Phi_n \rangle} \to \mathbb{F}(\zeta_n)$$

definida como $\sigma(f + \langle \Phi_n \rangle) = \zeta_n$ é claramente um isomorfismo. Portanto,

$$\mathbb{F}(\zeta_n) \simeq \frac{\mathbb{F}[x]}{\langle \Phi_n \rangle}$$

é uma extensão ciclotômica de $\mathbb{F}$ de grau $\phi(n)$.

Se $n = kd$, então ζ^k é um elemento de ordem d e é uma raiz d-ésima primitivas da unidade. Assim, existe exatamente um d-ésimo polinômio ciclotômico

$$\Phi_d(x) = \prod_{mdc(d,j)=1} (x - \zeta^{jk}),$$

Neste caso,

$$x^n - 1 = \prod_{\substack{1 \leq d \leq n \\ d|n}} \Phi_d(x).$$

Para cada d fixado, seja

$$\Phi_d(x) = \prod_{i=1}^{a_d} f_{d_i}(x),$$

a fatoração de $\Phi_d(x)$ como um produto de polinômios irredutíveis sobre $\mathbb{F}$. Então a decomposição de $\mathbb{F}G$ pode ser escrita sob a forma:

$$\mathbb{F}G \simeq \sum_{\substack{d=1 \\ d|n}}^{n} \left(\sum_{i=1}^{a_d} \frac{\mathbb{F}[x]}{\langle f_{d_i} \rangle} \right) \simeq \sum_{\substack{d=1 \\ d|n}}^{n} \left(\sum_{i=1}^{a_d} \mathbb{F}(\zeta_{d_i}) \right).$$

Para um d fixo, todos os elementos ζ_{d_i} são raízes n-ésimas primitivas da unidade. Portanto, todos os corpos da forma $\mathbb{F}(\zeta_{d_i})$ são iguais e podemos sempre escrever

$$\mathbb{F}G \simeq \sum_{\substack{d=1 \\ d|n}}^{n} a_d \mathbb{F}(\zeta_d),$$

$a_d\mathbb{F}(\zeta_d)$ denota a soma direta de a_d corpos diferentes, todos isomorfos a $\mathbb{F}(\zeta_d)$. Portanto,

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

Consequentemente,

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

em que n_d é o número de elementos de ordem d em G, o qual é precisamente $\phi(d)$.

Exemplo 1.4 *Sejam G um grupo cíclico de ordem n,*

$$G = \langle a \rangle = \{1, a, a^2, \ldots, a^{n-1}\},$$

e $\mathbb{F} = \mathbb{Q}$ o corpo dos números racionais. Então

$$x^n - 1 = \prod_{\substack{1 \leq d \leq n \\ d|n}} \Phi_d(x)$$

é a fatoração de $x^n - 1$ em fatores irredutíveis sobre $\mathbb{F}$. Assim, se ζ_d é uma raiz d-ésima primitiva da unidade, então

$$\mathbb{F}G \simeq \sum_{\substack{d=1 \\ d|n}}^{n} a_d\mathbb{F}(\zeta_d),$$

com

$$a_d = \frac{n_d}{[\mathbb{F}(\zeta_d) : \mathbb{F}]} = \frac{n_d}{\phi(d)} = 1.$$

Em particular, se $n = 6$, então

$$\begin{aligned} x^6 - 1 &= \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x) \\ &= (x-1)(x+1)(x^2+x+1)(x^2-x+1). \end{aligned}$$

Portanto,

$$\mathbb{F}G \simeq \mathbb{F} \oplus \mathbb{F} \oplus \mathbb{F}\left(\frac{-1+\sqrt{-3}}{2}\right) \oplus \mathbb{F}\left(\frac{1+\sqrt{-3}}{2}\right).$$

A descrição obtida acima pode ser estendida a aneis de grupo de um grupos abelianos finitos, conforme o teorema a seguir, cuja demonstração é feita por indução e utiliza o Teorema de Estrutura dos Grupos Abelianos Finitos.

Teorema 1.12 (Perlis-Walker) *Sejam G um grupo abeliano finito de ordem n e $\mathbb{K}$ um corpo qualquer tal que a característica de $\mathbb{K}$ não divide $|G|$. Então*

$$\mathbb{K}G \simeq \sum_{\substack{d=1 \\ d|n}}^{n} a_d\mathbb{F}(\zeta_d).$$

Corolário 1.10 *Sejam G um grupo abeliano finito de ordem n. Então*

$$\mathbb{Q}G \simeq \sum_{\substack{d=1 \\ d|_n}}^{n} a_d \mathbb{Q}(\zeta_d).$$

Corolário 1.11 *Sejam G um grupo abeliano finito de ordem n e $\mathbb{F}$ um corpo tal que a característica de $\mathbb{F}$ não divide n. Se $\mathbb{F}$ contém uma raiz n-ésima primitiva da unidade, então*

$$\mathbb{F}G \simeq \sum_{i=1}^{n} \mathbb{F}_i,$$

com $\mathbb{F}_i = \mathbb{F}$, $i = 1, \ldots, n$.

Finalizaremos esta seção apresentado uma descrição do centro de uma álgebra de grupo. Essas informações serão úteis na determinação da estrutura de uma álgebra de grupo semissimples.

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

Se g é um elemento do grupo G, então $o(g)$ indica o ordem do elemento g e o conjunto

$$C(g) = \{h^{-1}gh : h \in G\}$$

é a classe de conjugação de g em G. Se $C(g)$ é um conjunto finito, então definimos o elemento

$$A_g = \sum_{h \in C(g)} h$$

no anel de grupo RG, o qual é chamado uma *soma de classe* de G sobre R.

Teorema 1.13 *Sejam G um grupo e R um anel comutativo com unidade. Então o conjunto $\{A_g\}_{g \in G}$ de todas as somas de classes de G sobre R formam uma base de $\mathcal{Z}(RG)$.*

Teorema 1.14 *Sejam G um grupo finito e $\mathbb{F}$ um corpo algebricamente fechado tal que a característica de $\mathbb{F}$ não divide $|G|$. Então o número de componentes simples de $\mathbb{F}G$ é igual ao número de classes de conjugação de G.*

Observação 1.3 *Se o corpo $\mathbb{F}$ não for algebricamente fechado e a característica de $\mathbb{F}$ não divide $|G|$, então o número de componentes simples de $\mathbb{F}G$ será sempre menor do que ou igual ao número de classes de conjugação do grupo G.*

Sejam G um grupo e H um subgrupo de G. Se $H = \{1\}$, então, pelo Corolário 1.7, existe um único homomorfismo de aneis $\epsilon : RG \to R$ tal que

$$\epsilon\left(\sum_{g\in g}\alpha(g)g\right) = \sum_{g\in g}\alpha(g).$$

Note que

$$\Delta(G,H) = \ker\epsilon = \left\{\sum_{g\in G}\alpha(g)g : \sum_{g\in G}\alpha(g) = 0\right\}$$

é um ideal de RG chamado de *ideal aumentado*.

Já vimos que se e é um idempotente central de um anel R, então e induz uma decomposição de R como uma soma direta de ideais, ou seja,

$$R = Re \oplus R(1-e),$$

pois

$$a = ae + a - ae = ae + a(1-e) \text{ e } Re \cap R(1-e) = \{0\}.$$

Existe uma maneira padrão de construir idempotentes dos subgrupos de um determinado grupo, em um anel de grupo.

Dados um anel de grupo RG e um subconjunto finito H de G tal que $|H|$ é um elemento invertível em R, vamos denotar por $\widehat{H}$ o elemento

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

Lema 1.6 *Sejam R um anel comutativo com identidade e H subgrupo finito de um grupo G.*

1. *Se $|H|$ é um elemento invertível em R, então $e_H^2 = e_H$ em RG.*

2. *H é um subgrupo normal em G se, e somente se, e_H é central em RG. Em particular, $RGe_H \simeq e_HRG$ e*
$$(RG)e_H \simeq R\left(\frac{G}{H}\right).$$

3. *Se H é um subgrupo normal em G, então*
$$RG = RGe_H \oplus RG(1-e_H),$$
com
$$RGe_H \simeq R\left(\frac{G}{H}\right) \text{ e } RG(1-e_H) = \Delta(G,H).$$

Prova. (1) Basta observar que e_H está bem definida,

$$e_H = \frac{1}{|H|}\sum_{h\in H} h \neq 0.$$

Neste caso, $e_H y = e_H$, para todo $y \in H$, pois $hy \in H$. Em particular,

$$e_H^2 = e_H\left(\frac{1}{|H|}\sum_{h\in H} h\right) = \frac{1}{|H|}\sum_{h\in H} e_H h = \frac{1}{|H|}\sum_{h\in H} e_H = \frac{1}{|H|}\,|H|\,e_H = e_H.$$

(2) Se H é um subgrupo normal em G, então $gHg^{-1} = H$, para todo $g \in G$. Logo,

$$ge_Hg^{-1} = g\left(\frac{1}{|H|}\sum_{h\in H} h\right)g^{-1} = \frac{1}{|H|}\sum_{h\in H} ghg^{-1} = \frac{1}{|H|}\sum_{h\in H} h = e_H.$$

Portanto, $ge_H = e_H g$, para todo $g \in G$, ou seja, e_H é central. Além disso, $RGe_H \simeq e_H RG$.

Reciprocamente, se e_H é central em RG, então, para qualquer $g \in G$,

$$e_H = ge_Hg^{-1} \Rightarrow \frac{1}{|H|}\sum_{h\in H} h = \frac{1}{|H|}\sum_{h\in H} ghg^{-1}.$$

Logo, $gHg^{-1} = H$, para todo $g \in G$, ou seja, H é um subgrupo normal em G.

Finalmente, para qualquer $g \in G$,

$$ge_H = g\left(\frac{1}{|H|}\sum_{h\in H} h\right) = g\frac{1}{|H|}\left(|H| - \sum_{h\in H}(1-h)\right) = g + \delta,$$

com

$$\delta = -g\frac{1}{|H|}\sum_{h\in H}(1-h) \in \Delta(G,H).$$

Logo, as funções

$$\sigma : RGe_h \to \frac{RG}{\Delta(G,H)} \text{ e } \varphi : \frac{RG}{\Delta(G,H)} \to R\left(\frac{G}{H}\right)$$

definidas como

$$\sigma(ge_H) = g + \Delta(G,H) \text{ e } \varphi(g + \Delta(G,H)) = gH$$

são claramente isomorfismos. Portanto,

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

(3) É fácil verificar que

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

Agora,

$$RG(1-e_H) = RG\left(|H| - \sum_{h\in H} h\right) \subseteq \sum_{h\in H} RG(1-h) = \Delta(G,H).$$

Por outro lado, como

$$(1-h)(1-e_H) = 1-h-(1-h)e_H = 1-h-e_H+he_H = 1-h$$

temos que $\Delta(G,H) \subseteq RG(1-e_H)$. Portanto, $RG(1-e_H) = \Delta(G,H)$. ■

Quando $H = G$, e_G é chamado de *idempotente principal* de RG. Em particular, se RG é semissimples e $H = G'$ o subgrupo derivado de G, então a componente $\Delta(G,G')$ é a soma de todas as componentes simples não comutativas de RG.

Lema 1.7 *Sejam R um anel comutativo com identidade e H, K subgrupo normais em um grupo finito G tais que $H \subseteq K$. Então*

$$\dim RG(e_H - e_K) = \dim RGe_H - \dim RGe_K.$$

Prova. Como $H \subseteq K$ temos que $e_He_K = e_K$. Logo,

$$ge_H = ge_K + ge_H - ge_K = ge_K + g(e_H - e_K) \text{ e } e_K(e_H - e_K) = 0,$$

ou seja,

$$RGe_H = RGe_K \oplus RG(e_H - e_K),$$

que é o resultado desejado. ■

Seja $G = \langle a\rangle$ um grupo cíclico de ordem p^n, com p um número primo fixado. Então existe um único subgrupo $H = \left\langle a^{p^i}\right\rangle$ de G, para cada $i = 0,\ldots,n$. Portanto,

$$\{1\} = \left\langle a^{p^n}\right\rangle \leq \left\langle a^{p^{n-1}}\right\rangle \leq \cdots \leq \langle a^p\rangle \leq \langle a\rangle = G$$

é a única série de decomposição para G, ou seja, obtemos

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

a cadeia descendente de subgrupos cíclicos de G, em que $G_i = \langle a^{p^i}\rangle$.

Lema 1.8 *Sejam $\mathbb{F} = \mathbb{Q}$ o corpo dos números racionais, $G = \langle a\rangle$ um grupo cíclico de ordem p^n, com p um número primo fixado, e*

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

a cadeia descendente de subgrupos cíclicos de G. Então os elementos

$$e_0 = \widehat{G}_0 \ \ e \ \ e_i = \widehat{G}_i - \widehat{G}_{i-1}, \ \ i = 1, \ldots, n,$$

formam um conjunto de idempotentes primitivos de $\mathbb{F}G$. Além disso, $\mathbb{F}Ge_i \simeq \mathbb{F}(\zeta_{p^i})$, com ζ_{p^i} a raiz p^i-ésima primitiva da unidade, e $[\mathbb{F}Ge : \mathbb{F}] = e(1)p^n$, para qualquer idempotente primitivo e de $\mathbb{F}G$ e $e(1)$ denota o coeficiente de 1 em e.

Prova. Como

$$\mathbb{F}G \simeq \sum_{j=0}^{n} \mathbb{F}(\zeta_{p^j})$$

temos que $\mathbb{F}G$ contém exatamente $n+1$ idempotentes primitivos. Note que

$$e_0 e_i = \widehat{G}_0 \left(\widehat{G}_i - \widehat{G}_{i-1} \right) = \widehat{G}_0 \widehat{G}_i - \widehat{G}_0 \widehat{G}_{i-1} = 0, \ \ i = 1, \ldots, n,$$

pois

$$\widehat{G}_0 \widehat{G}_i = \widehat{G}_0, \ \ i = 0, 1, \ldots, n.$$

Além disso, se $1 \leq i \leq j$, então

$$\widehat{G}_i \widehat{G}_j = \widehat{G}_i.$$

Logo,

$$e_i e_j = (\widehat{G}_i - \widehat{G}_{i-1})(\widehat{G}_j - \widehat{G}_{j-1}) = \widehat{G}_i - \widehat{G}_i \widehat{G}_{j-1} - \widehat{G}_{i-1} + \widehat{G}_{i-1} = \delta_{ij}(\widehat{G}_i - \widehat{G}_i \widehat{G}_{j-1}).$$

Assim,

$$e_0, e_1, e_i, \ldots, e_m$$

são $m+1$ idempotentes centrais ortogonais aos pares. Portanto, eles são primitivos e

$$\sum_{i=0}^{n} e_i = \widehat{G}_0 + \widehat{G}_1 - \widehat{G}_0 + \widehat{G}_2 - \widehat{G}_1 + \cdots + \widehat{G}_{n-1} - \widehat{G}_{n-2} + \widehat{G}_n - \widehat{G}_{n-1} = 1.$$

Finalmente, pelo Lema 1.6, obtemos

$$\mathbb{F}G \simeq \mathbb{F} \ \text{ e } \ \mathbb{F}Ge_i \simeq \mathbb{F}\left(\frac{G}{G_i}\right) e_i \simeq \mathbb{F}L, \ \ i = 1, \ldots, n,$$

com L um grupo cíclico de ordem p^i. Assim, pelo Lema 1.7,

$$\begin{aligned} [\mathbb{F}Ge_i : \mathbb{F}] &= \left[(\mathbb{F}G)\widehat{G}_i : \mathbb{F} \right] - \left[(\mathbb{F}G)\widehat{G}_{i-1} : \mathbb{F} \right] \\ &= p^i - p^{i-1} \\ &= \phi(p^i) = \left[\mathbb{F}(\zeta_{p^i}) : \mathbb{F} \right]. \end{aligned}$$

Portanto, $\mathbb{F}Ge_i \simeq \mathbb{F}(\zeta_{p^i})$, $i = 1, \ldots, n$. Note que

$$e_i(1)p^n = \left(\frac{1}{p^{n-i}} - \frac{1}{p^{n-(i-1)}}\right) p^n = p^i - p^{i-1} = [\mathbb{F}Ge_i : \mathbb{F}]\,.$$

Enquanto,

$$e_0(1)p^n = 1 = [\mathbb{F}Ge_0 : \mathbb{F}]\,.$$

Assim, $[\mathbb{F}Ge : \mathbb{F}] = e(1)p^n$, para qualquer idempotente primitivo e de $\mathbb{F}G$. ■

Observação 1.4 *Na prova do Lema* 1.8 *usamos o fato de que os polinômios ciclotômicos são irredutíveis sobre* $\mathbb{Q}$*. Assim, podemos estendê-lo somente para álgebras de grupos sobre corpos com a mesma propriedade, ou seja, o Lema não é verdade em geral, por exemplo, sejam* G *um grupo cíclico de ordem* 3 *e* $\mathbb{F} = \mathbb{F}_7$ *um corpo finito. Então*

$$\begin{aligned} x^3 - 1 &= \prod_{\substack{1 \le d \le n \\ d \mid n}} \Phi_d(x) = \Phi_1(x)\Phi_3(x) = (x-1)(x^2+x+1) \\ &= (x-1)(x-2)(x-4). \end{aligned}$$

Logo,

$$\mathbb{F}G \simeq \frac{\mathbb{F}[x]}{\langle x^3-1\rangle} \simeq \frac{\mathbb{F}[x]}{\langle x-1\rangle} \oplus \frac{\mathbb{F}[x]}{\langle x-2\rangle} \oplus \frac{\mathbb{F}[x]}{\langle x-4\rangle}.$$

Por outro lado,

$$\mathbb{Q}G \simeq \frac{\mathbb{Q}[x]}{\langle x^3-1\rangle} \simeq \frac{\mathbb{Q}[x]}{\langle x-1\rangle} \oplus \frac{\mathbb{Q}[x]}{\langle x^2+x+1\rangle} \simeq \mathbb{Q} \oplus \mathbb{Q}(\zeta_3),$$

com ζ_3 *a raiz terceira primitiva da unidade. Assim, a álgebra de grupo* $\mathbb{F}G$ *contém três elementos idempotentes primitivos, enquanto a álgebra grupo* $\mathbb{Q}G$ *contém dois elementos idempotentes primitivos. Portanto, eles não podem ser obtidos do Lema.*

Exemplo 1.5 *Sejam* G *um grupo cíclico de ordem* 3^3 *e* $\mathbb{F} = \mathbb{Q}$ *o corpo dos números racionais. Então*

$$\begin{aligned} G_0 &= \langle a\rangle = \{1, a, a^2, \ldots, a^{26}\} \\ G_1 &= \langle a^3\rangle = \{1, a^3, a^6, a^9, a^{12}, a^{15}, a^{18}, a^{21}, a^{24}\} \\ G_2 &= \langle a^9\rangle = \{1, a^9, a^{18}\} \\ G_3 &= \langle a^{27}\rangle = \{1\}. \end{aligned}$$

Logo,

$$\begin{aligned} e_0 &= \widehat{G}_0 = \frac{1}{27}(1 + a + a^2 + \cdots + a^{25} + a^{26}) \\ \widehat{G}_1 &= \frac{1}{9}(1 + a^3 + a^6 + a^9 + a^{12} + a^{15} + a^{18} + a^{21} + a^{24}) \\ \widehat{G}_2 &= \frac{1}{3}(1 + a^9 + a^{18}) \\ \widehat{G}_3 &= 1. \end{aligned}$$

Assim,

$$\begin{aligned} e_1 &= \widehat{G}_1 - \widehat{G}_0 = \frac{1}{27}(2 - a - a^2 + 2a^3 - a^4 - \cdots - a^{23} + 2a^{24} - a^{25} - a^{26}) \\ e_2 &= \widehat{G}_2 - \widehat{G}_1 = \frac{1}{9}(2 - a^3 - a^6 + 2a^9 - a^{12} - a^{15} + 2a^{18} - a^{21} - a^{24}) \\ e_3 &= \widehat{G}_3 - \widehat{G}_2 = \frac{1}{3}(2 - a^9 - a^{18}). \end{aligned}$$

Portanto, $e_i e_j = \delta_{ij} e_i$, $e_0 + e_1 + e_2 + e_3 = 1$ *e*

$$e_i(1)3^3 = 3^i - 3^{i-1}.$$

Capítulo 2

Teoria dos Códigos

Iniciaremos este capítulo com uma introdução dos conceitos básicos da Teoria dos Códigos, para estabelecer a linguagem utilizada nesta teoria e, em seguida, apresentaremos os códigos lineares e alguns resultados sobre um tipo de código bastante relevante para o objetivo deste trabalho: os códigos cíclicos minimais que normalmente, na literatura introdutória, são apresentados utilizando-se a estrutura de anéis de polinômios, onde os códigos cíclicos são descritos como ideais no anel quociente

$$\frac{\mathbb{F}_q[x]}{\langle x^n - 1\rangle},$$

onde $\mathbb{F}_q$ é um corpo finito, que possui q elementos, e n é um número natural que indica o comprimento do código. Através de um isomorfismo entre o anel

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

e a álgebra de grupo $\mathbb{F}_qC_n$ do grupo cíclico finito C_n de ordem n, fica estabelecida uma correspondência biunívoca entre os ideais no anel quociente de polinômios e os ideais da álgebra $\mathbb{F}_qC_n$. Desta maneira, descrevemos os códigos cíclicos como ideais na álgebra de grupo $\mathbb{F}_qC_n$.

De modo geral, pela Teoria dos Anéis de Grupos, um ideal ou código (minimal) de uma álgebra de grupo semissimples é gerado por um idempotente (primitivo). Para alguns códigos cíclicos, utilizamos a estrutura de subgrupos do grupo cíclico para calcular os idempotentes centrais primitivos da álgebra de grupo geradores desses códigos.

2.1 Conceitos Básicos

Seja $\mathbb{A}$ qualquer conjunto finito, com q elementos, o qual será chamado de *alfabeto*. Os elementos de $\mathbb{A}$ serão chamados de *letras* ou *dígitos*. Uma sequência de n elementos de $\mathbb{A}$ será chamada uma *palavra de comprimento* n.

Consideremos $\mathbb{A}^n$ o conjunto de todas as palavras de comprimento n sobre $\mathbb{A}$, isto é,

$$\mathbb{A}^n = \{(c_0, c_1, \ldots, c_{n-1}) : c_i \in \mathbb{A},\ \ i = 0, \ldots, n-1\}.$$

Um *código* de comprimento n é qualquer subconjunto não trivial de $\mathbb{A}^n$, para algum $n \in \mathbb{N}$:

$$\mathcal{C} \subseteq \mathbb{A}^n.$$

Um dos principais objetivos da Teoria dos Códigos Corretores de Erros é determinar quando uma palavra transmitida através de um canal é recebida com algum erro e, o mais importante, saber corrigir este erro. Estas observações podem ser expressas em linguagem rigorosa e nos levarão aos primeiros resultados da Teoria dos Códigos.

Dados dois elementos

$$x = (x_0, \ldots, x_n), y = (y_0, \ldots, y_n) \in \mathbb{A}^n,$$

chama-se *distância de Hamming* entre eles ao número de coordenadas em que x e y diferem, ou seja:

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

Dado um código $\mathcal{C} \subseteq \mathbb{A}^n$, chama-se *distância mínima* de $\mathcal{C}$ ao número:

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

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

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

2.2 Códigos Lineares

Como estamos interessados em trabalhar com conjuntos munido de uma estrutura algébrica, o alfabeto escolhido será um corpo finito $\mathbb{F}_q$, com q elementos. Além disso, o nosso conjunto de palavras $\mathcal{C}$ sobre $\mathbb{F}_q$ será tomado de maneira a formar um subespaço vetorial não trivial de $\mathbb{F}_q^n$ e, neste caso, tal código é conhecido como *código linear*.

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

$$w(x) = |\{i : x_i \neq 0, \;\; i = 0, \ldots, n-1\}|.$$

Em outras palavras, temos

$$w(x) = d(x, 0),$$

em que d representa a distância de Hamming. O peso de um código linear $\mathcal{C}$ é o inteiro

$$w(\mathcal{C}) = \min\{w(x) \;\; : \;\; x \in \mathcal{C} - \{0\}\}.$$

Existem várias maneiras de descrevermos um código linear $\mathcal{C}$. Apresentaremos duas delas neste trabalho:

Consideremos a base canônica

$$\{f_1, \ldots, f_n\}$$

de $\mathbb{F}_q^n$, de modo que qualquer vetor v pode ser escrito de mod único sob a forma

$$v = v_1 f_1 + v_2 f_2 + \cdots + v_n f_n, \;\; \text{onde } v_i \in \mathbb{F}_q \;\; \text{e} \;\; i = 1, \ldots, n.$$

Seja $\mathcal{C}$ um código linear de dimensão k sobre $\mathbb{F}_q$. Se

$$\{e_1, \ldots, e_k\}$$

é a base canônica de $\mathbb{F}_q^k$ e

$$\{c_1, \ldots, c_k\}$$

é uma base de $\mathcal{C}$, então a função

$$\nu : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n \;\; \text{definida como} \;\; \nu(e_i) = c_i, \;\; i = 1, \ldots, n,$$

é linear e injetora, com $Im\nu = \mathcal{C}$. Esta aplicação pode ser visualizada no seguinte diagrama:

$$\begin{array}{ccc} \mathbb{F}_q^k & \stackrel{\nu}{\longrightarrow} & \mathbb{F}_q^n \\ | & & | \\ \mathbb{F}_q^k & \stackrel{\nu|_{\mathbb{F}_q^k}}{\longrightarrow} & \mathcal{C} \end{array}$$

Vamos determinar a matriz G que representa a transformação linear ν nas bases canônicas de $\mathbb{F}_q^k$ e $\mathbb{F}_q^n$, respectivamente. Para isso, escreveremos os elementos da base de $\mathcal{C}$ na base canônica de $\mathbb{F}_q^n$.

$$\left\{ \begin{array}{ccccccccccc} c_1 & = & b_{11}f_1 & + & b_{21}f_2 & + & \cdots & + & b_{n1}f_n \\ c_2 & = & b_{12}f_1 & + & b_{22}f_2 & + & \cdots & + & b_{n2}f_n \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ c_k & = & b_{1k}f_1 & + & b_{2k}f_2 & + & \cdots & + & b_{nk}f_n \end{array} \right.$$

onde os coeficientes $b_{ij} \in \mathbb{F}_q$. Como

$$\nu(e_i) = c_i = b_{1i}f_1 + b_{2i}f_2 + \cdots + b_{ni}f_n, \;\; i = 1, \ldots, k,$$

temos que a matriz de ν em relação às bases canônicas é

$$G = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1k} \\ b_{21} & b_{22} & \cdots & b_{2k} \\ \vdots & \vdots & \cdots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nk} \end{bmatrix}.$$

Note que cada coluna da matriz G corresponde a um vetor que pertence ao código $\mathcal{C}$, ou seja, podemos dizer que $\mathcal{C}$ é o subespaço de $\mathbb{F}_q^n$ gerado pelas colunas da matriz G (que formam, na realidade, uma base de $\mathcal{C}$). Os elementos de $\mathcal{C}$ são todas as palavras $w \in \mathbb{F}_q^n$ da forma $w = \nu(v)$, onde $v \in \mathbb{F}_q^k$. Uma matriz $G \in M_{n\times k}(\mathbb{F}_q)$ cujas colunas formam uma base para o código $\mathcal{C}$ é chamada de *matriz de codificação* ou *matriz geradora* do código $\mathcal{C}$.

Outra maneira de descrevermos o código linear $\mathcal{C}$ é através de uma transformação linear sobrejetora $\pi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^{n-k}$ tal que $\ker \pi = \mathcal{C}$, descrito do seguinte modo: dado uma base

$$\{c_1, \ldots, c_k\}$$

do código $\mathcal{C}$, ela pode ser estendida (de várias maneiras) para uma base

$$\{c_1, \ldots, c_k, v_1, \ldots, v_{n-k}\}$$

do espaço $\mathbb{F}_q^n$. Assim, qualquer $v \in \mathbb{F}_q^n$ pode ser escrito de modo único sob a forma

$$v = \lambda_1 c_1 + \cdots + \lambda_k c_k + \lambda_{k+1} v_1 + \cdots + \lambda_n v_{n-k}$$

onde $\lambda_i \in \mathbb{F}_q$, $i = 1, \ldots, n$. A função $\pi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^{n-k}$ definida como

$$\pi(v) = \lambda_{k+1} v_1 + \cdots + \lambda_n v_{n-k}.$$

é tal que $\ker \pi = \mathcal{C}$. Podemos representar esta função no seguinte diagrama:

$$\begin{array}{ccc} \mathbb{F}_q^n & \stackrel{\pi}{\longrightarrow} & \mathbb{F}_q^{n-k} \\ | & & | \\ \mathcal{C} & \longrightarrow & 0 \end{array}$$

Denotaremos por $H \in M_{(n-k)\times n}(\mathbb{F}_q)$ a matriz de posto $(n-k)$ que representa a transformação linear π nas bases canônicas de $\mathbb{F}_q^n$ e $\mathbb{F}_q^{n-k}$, respectivamente. Como $\ker \pi = \mathcal{C}$ temos que o código linear $\mathcal{C}$ é o conjunto de todas as palavras $w \in \mathbb{F}_q^n$ que satisfazem

$$Hw^t = 0,$$

de modo que multiplicar pela matriz H é uma forma de decidir se um dado vetor pertence, ou não, ao código $\mathcal{C}$. A matriz H é chamada de *matriz de teste de paridade* ou *matriz de verificação de paridade* do código linear $\mathcal{C}$. Portanto, um código linear $\mathcal{C}$ pode, também, ser definido através de uma matriz de teste.

Agora, vamos analisar como π e ν se relacionam: cconsideremos o diagrama

$$\begin{array}{ccccc} \mathbb{F}_q^k & \stackrel{\nu}{\longrightarrow} & \mathbb{F}_q^n & \stackrel{\pi}{\longrightarrow} & \mathbb{F}_q^{n-k} \\ | & & | & & | \\ \mathbb{F}_q^k & \longrightarrow & \mathcal{C} & \longrightarrow & 0 \end{array}$$

com $\mathcal{C} = Im\nu = \ker \pi$. Se $x \in \mathbb{F}_q^k$, então

$$(\pi \circ \nu)(x) = \pi(\nu(x)) = 0,$$

pois

$$\nu(x) \in Im\nu = \mathcal{C} = \ker \pi.$$

Em notação matricial, obtemos

$$HG = 0.$$

2.3 Códigos Cíclicos

Enriquecendo a estrutura do espaço vetorial $\mathbb{F}_q^n$, definiremos a seguir uma das principais classes de códigos lineares: os códigos cíclicos. Estes códigos são amplamente utilizados em sistemas digitais, onde os circuitos eletrônicos estão cada vez mais sucetíveis a interferências do meio devido ao avanço das tecnologias de fabricação, que permite a diminuição de suas dimensões, além disso, possuem bons algoritmos de codificação e de decodificação baseados em operações com polinômios. Assim, quando pensamos em tecnologia digital, estamos empregando, implicitamente, os códigos cíclicos.

Em toda esta seção $\mathbb{F}$ significa, salvo menção explícita em contrário, um corpo finito com q elementos, ou seja, $\mathbb{F} = GL(q)$ e

$$G = \langle a \rangle = \{1, a, \ldots, a^{n-1}\},$$

um grupo cíclico de ordem n. Se deslocarmos ciclicamente a coordenada $i \mapsto i + 1$ da palavra

$$c = (c_0, c_1, \ldots, c_{n-1})$$

obtemos a palavra

$$c^1 = (c_{n-1}, c_0, \ldots, c_{n-2}),$$

chamada de *troca cíclica* de x. Se as componentes de x são deslocadas ciclicamente l posições para à direita, então obtemos a palavra

$$c^{(l)} = \left(c_{(n-l)+1}, \ldots, c_{(n-l)+2}, \ldots, c_n, c_0, \ldots, c_{n-l}\right).$$

Um código linear $\mathcal{C}$ é chamado de *código cíclico* se qualquer deslocamemto cíclico de uma palavra código

$$c = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C},$$

é também uma palavra código em $\mathcal{C}$. É conveniente identificar uma palavra código $c \in \mathcal{C}$ com um polinômio código

$$c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in \mathbb{F}[x].$$

Assim, um deslocamemto cíclico de uma palavra código

$$c = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C},$$

corresponde a multiplicação

$$x \cdot c(x),$$

onde o expoente é reduzido módulo n. Portanto, a redução módulo n corresponde a redução módulo $x^n - 1$, ou seja,

$$\mathcal{R}_n = \frac{\mathbb{F}[x]}{\langle x^n - 1 \rangle} = \{r(x) + \langle x^n - 1 \rangle : r(x) \in \mathbb{F}\,[x] \ \text{ e } \partial(r(x)) < n\} \simeq \mathbb{F}^n$$

Note que $\mathcal{R}_n$ é uma $\mathbb{F}$-álgebra que é um domínio de ideais principais. Já vimos que

$$\mathbb{F}G \simeq \mathcal{R}_n.$$

Teorema 2.1 *Um código linear $\mathcal{C}$ de comprimento n sobre $\mathbb{F}$ é cíclico se, e somente se, $\mathcal{C}$ é um ideal em $\mathcal{R}_n$.*

Prova. Suponhamos que $\mathcal{C}$ seja um código cíclico sobre $\mathbb{F}$. Então $xc(x) \in \mathcal{C}$, para todo polinômio código $c(x) \in \mathbb{F}[x]$. Portanto,

$$x^i c(x) \in \mathcal{C}, \ \ \forall \ i.$$

Como $\mathcal{C}$ é linear temos que

$$a(x)c(x) \in \mathcal{C}, \ \ \forall \ a(x) \in \mathcal{R}_n.$$

Portanto, $\mathcal{C}$ é um ideal em $\mathcal{R}_n$.

Reciprocamente, seja

$$c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$$

uma palavra código. Então

$$xc(x) \in \mathcal{C},$$

pois $\mathcal{C}$ é um ideal em $\mathcal{R}_n$. Portanto, $\mathcal{C}$ é um código cíclico sobre $\mathbb{F}$. ■

Obserque que se $mdc(q, n) = 1$, então pelo Corolário 1.8 a álgebra de grupo $\mathbb{F}G$ é semisimples, ou seja, se escreve como uma soma direta de ideais bilaterais minimais e todos os outros ideais desta álgebra são determinados como uma soma destes. Assim, diremos que um *código cíclico minimal* é um ideal minimal da álgebra de grupo semissimples $\mathbb{F}G$. Como no caso dos ideais, todos os códigos cíclicos estarão determinados a partir dos códigos cíclicos minimais. Devido a essa identificação entre códigos e ideais, todas as

definições feitas para códigos lineares de peso e distância mínima podem ser atribuídas a ideais.

Seja $\mathcal{I}$ um ideal em $\mathcal{R}_n$. Então existe um único polinômio mônico $g(x) \in \mathbb{F}[x]$ tal que $\langle g(x) \rangle = \mathcal{I}$ e $g(x)$ é um divisor de $x^n - 1$. Neste caso, diremos g é o *polinômio gerador* do ideal $\mathcal{I}$ e a dimensão de $\mathcal{I}$ é igual a $n - \partial(g(x))$. Reciprocamente, cada divisor de $x^n - 1$ gera um ideal em $\mathcal{R}_n$. Suponhamos que

$$g(x) = \sum_{i=0}^{n-k} c_i x^i = c_0 + c_1 x + \cdots + c_{n-k-1} x^{n-k-1} + x^{n-k}.$$

Então os elementos

$$g(x), xg(x), \ldots, x^{k-1} g(x)$$

são linearmente independentes em $\mathcal{I}$. Como qualquer elemento de $\mathcal{I}$ é da forma

$$h(x) \cdot g(x),$$

com $\partial(h(x)) < k$, temos que estes elementos geram $\mathcal{I}$ e a dimensão $\mathcal{I}$ é igual a k. Neste caso, a matriz geradora de $\mathcal{I}$ é da forma

$$G = \begin{bmatrix} c_0 & c_1 & c_2 & \cdots & c_{n-k-1} & 1 & 0 & \cdots & 0 & 0 \\ 0 & c_0 & c_1 & \cdots & c_{n-k-2} & c_{n-k-1} & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \ddots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & c_0 & c_1 & \cdots & c_{n-k-1} & 1 \end{bmatrix}.$$

Sejam $\mathcal{C}$ um (n, k)-código cíclico com gerador

$$g(x) = \sum_{i=0}^{n-k} c_i x^i \text{ e } h(x) = \sum_{i=0}^{k} b_i x^i.$$

Então, em $\mathcal{R}_n$,

$$h(x) \cdot g(x) \equiv 0 = \sum_{i=0}^{n-1} \left(\sum_{j=0}^{n-1} c_j b_{i-j} \right) x^i$$

implica que

$$\sum_{j=0}^{n-1} c_j b_{i-j} = 0, \;\; i = 0, 1, \ldots, n-1.$$

em que $b_i = 0$ se $i < 0$ ou $i > k$. Logo, o vetor

$$(c_0, c_1, \ldots, c_{n-k}, 0, \ldots, 0)$$

é ortogonal ao vetor

$$(b_k, b_{k-1}, \ldots, b_0, 0, \ldots, 0)$$

e todos os seus deslocamento cíclicos. Portanto, uma matriz de verificação de paridade para $\mathcal{C}$ pode ser escrita como

$$H = \begin{bmatrix} b_k & b_{k-1} & b_{k-2} & \cdots & b_1 & b_0 & 0 & \cdots & 0 & 0 \\ 0 & b_k & b_{k-1} & \cdots & b_2 & b_1 & b_0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \ddots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & b_k & b_{k-1} & \cdots & b_1 & b_0 \end{bmatrix},$$

a qual possui posto é $(n-k)$ e

$$GH^t = 0.$$

Assim, H é a matriz geradora do código dual

$$\mathcal{C}^{\perp} = \{x \in \mathbb{F}^n : xc^t = 0, \ \forall \ c \in \mathcal{C}\}$$

a $\mathcal{C}$. Note que $\mathcal{C}^{\perp}$ é um $(n, n-k)$-código cíclico com gerador $\alpha h^*(x)$, com

$$h^*(x) = x^k h\left(\frac{1}{x}\right)$$

o polinômio recíproco de $h(x)$ e α é escolhido de modo que $\alpha h^*(x)$ seja mônico.

Vamos lembrar qua a condição $mdc(q, n) = 1$ garante que as raízes de $x^n - 1$ seja todas simples e a semissimplicidade de $\mathcal{R}_n$. Neste caso,

$$\mathbb{F}G \simeq \mathcal{R}_n \simeq \frac{\mathbb{F}[x]}{\langle g_1(x)\rangle} \oplus \frac{\mathbb{F}[x]}{\langle g_2(x)\rangle} \oplus \cdots \oplus \frac{\mathbb{F}[x]}{\langle g_t(x)\rangle},$$

com

$$x^n - 1 = g_1(x)g_2(x)\cdots g_t(x)$$

a fatoração de $x^n - 1$ em fatores irredutíveis sobre $\mathbb{F}$. Note que os $M_i = \langle g_i(x)\rangle$, $i = 1, \ldots, t$, são ideais maximais em $\mathcal{R}_n$, mas os

$$B_i = \langle h_i(x)\rangle = \left\langle \frac{x^n - 1}{g_i(x)} \right\rangle, \ \ i = 1, \ldots, t.$$

são ideais minimais em $\mathcal{R}_n$. Portanto,

$$\mathcal{R}_n \simeq \mathbb{F}G \simeq B_1 \oplus B_2 \oplus \cdots \oplus B_t.$$

Assim, pelo Teorema 1.11, existem elementos idenpotentes $e_i(x)$ tais que

$$e_1(x) + e_2(x) + \cdots + e_n(x) = 1 \ \text{ e } \ e_i(x)e_j(x) = \delta_{ij}e_i(x).$$

Logo,

$$B_i = \mathbb{F}Ge_i(x) = \langle e_i(x) \rangle,$$

$e_i(x)$ é a identidade sobre B_i e se

$$f(x) = \sum_{i=1}^{t} f_i(x),$$

onde $f_i(x) \in B_i$, então

$$e_i(x)f(x) = f_i(x), \;\; i = 1, \ldots, t.$$

Portanto, B_i possui gerador $h_i(x)$ e idempotente $e_i(x)$, enquanto M_i possui gerador $g_i(x)$ e idempotente $1 - e_i(x)$, pois

$$B_i \oplus B_j = \langle mdc(h_i(x), h_j(x)) \rangle = \left\langle \frac{x^n - 1}{g_i(x)g_j(x)} \right\rangle$$

e

$$\begin{aligned} M_i &= \langle g_i(x) \rangle = \left\langle \frac{x^n - 1}{g_1(x) \cdots g_{i-1}(x) g_{i+1}(x) \cdots g_t(x)} \right\rangle \\ &= B_1 \oplus \cdots \oplus B_{i-1} \oplus B_{i+1} \oplus \cdots \oplus B_t. \end{aligned}$$

Mais geralmente, seja $\mathcal{I}$ um ideal qualquer gerado por $g(x)$. Então

$$mdc\,(g(x), h(x)) = mdc\left(g(x), \frac{x^n - 1}{g(x)}\right) = 1.$$

Logo, existem $a(x), b(x) \in \mathbb{F}[x]$ tais que

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

Pondo $e(x) = a(x)g(x) \in \mathcal{I}$, obtemos

$$e(x) = e(x)^2 + a(x)b(x)(x^n - 1) = e(x)^2$$

é um idempotente e $\mathcal{I} = \langle e(x) \rangle$.

Capítulo 3

Códigos Abelianos Minimais

Este é o principal capítulo deste trabalho. Faremos construções para códigos abelianos minimais e estendemos os resultados de Berman na medida do possível.

Para isso, na primeira seção, calcularemos o número de componentes simples de uma álgebra de grupo abeliano finito $\mathbb{F}G$ e determinaremos as condições para que este número seja mínimo, ou seja, igual ao número de componentes simples sobre a álgebra de grupos racionais do mesmo grupo. Tal cálculo pode ser obtido a partir do teorema de Berman e Witt e de um resultado de Khülshammer, utilizando a Teoria dos Caracteres. Em [10], Ferraz e Milies simplificaram os métodos de Ferraz para grupos abelianos finitos, apresentando um método geral para calcular o número de componentes simples de uma álgebra de grupo semissimples sem utilizar a Teoria de Caracteres, utilizando apenas a estrutura da $\mathbb{F}G$. Na terceira seção, utilizaremos este resultado para calcular os idempotentes geradores de códigos abelianos minimais e estendemos os resultados de Arora e Pruthi. Finalmente, na última seção, mostraremos como calcular a dimensão e peso destes códigos de forma simples.

3.1 O Número de Componentes Simples

Em todo este capítulo $\mathbb{F}$ significa, salvo menção explícita em contrário, um corpo finito com q elementos, ou seja, $\mathbb{F} = \mathbb{F}_q = GL(q)$ e G um grupo abeliano finito de ordem n tal que $mdc(q, n) = 1$. Então, pelo Corolário 1.8, a álgebra de grupo $\mathbb{F}G$ é semissimples. Além disso,

$$\mathbb{F}G \simeq \sum_{i=1}^{r} (\mathbb{F}G)e_i \simeq \sum_{i=1}^{r} \mathbb{F}_i,$$

com $\mathbb{F}_i \simeq (\mathbb{F}G)e_i$, $i = 1, \ldots, r$, extensões finitas de $\mathbb{F}$ e os e_i são idempotentes primitivos de $\mathbb{F}G$. Ferraz apresentou um método geral para calcularmos o número r de componentes simples de uma álgebra de grupo semissimples. Na álgebra de grupos finitos para grupos abelianos podemos determinar este número de uma maneira mais simples. Definindo

$$\mathbb{A} = \sum_{i=1}^{r} \mathbb{F}e_i.$$

Observe que $\mathbb{F}e_i \simeq \mathbb{F}$ são vistos como corpos de uma forma natural e que o número r de componentes simples é também a dimensão de $\mathbb{A}$ visto como um espaço vetorial sobre $\mathbb{F}$.

Lema 3.1 *Seja α um elemento de $\mathbb{F}G$. Então $\alpha \in \mathbb{A}$ se, e somente se, $\alpha^q = \alpha$. Em particular, se*

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

então

$$\alpha(g) = \alpha(g^q) = \cdots = \alpha(g^{q^{t_g - 1}}),$$

para cada $g \in G$.

Prova. Dado

$$\alpha = \sum_{i=1}^{r} \alpha_i \in \mathbb{A},$$

onde $\alpha_i = \alpha e_i \in \mathbb{F}_i$, $i = 1, \ldots, r$. Então α é um elemento de $\mathbb{A}$ se, e somente se, cada elemento $\alpha_i \in \mathbb{F}e_i$, $i = 1, \ldots, r$. Como $\mathbb{F}e_i \simeq \mathbb{F}$ temos que $\alpha_i^q = \alpha_i$, $i = 1, \ldots, r$. Então, pelo Lema 1.2, obtemos

$$\alpha^q = \left(\sum_{i=1}^{r} \alpha_i \right)^q = \sum_{i=1}^{r} \alpha_i^q = \sum_{i=1}^{r} \alpha_i = \alpha.$$

Finalmente, como

$$\sum_{g \in G} \alpha(g)g = \alpha = \alpha^q = \left(\sum_{g \in G} \alpha(g)g \right)^q = \sum_{g \in G} \alpha(g)g^q$$

temos que $\alpha(g) = \alpha(g^q)$. ■

Seja $\mathcal{C}_1 = \{1\}$ e escolhemos $g_2 \notin \mathcal{C}_1$. Então

$$\mathcal{C}_2 = \{g_2^{q^j} : j = 0, \ldots, t_{g_2} - 1\} = \{g_2, g_2^q, \ldots, g_2^{q^{t_{g_2}-1}}\},$$

em que t_{g_2} é o menor inteiro positivo tal que

$$g_2^{q^{t_{g_2}}} = g_2 \text{ ou } q^{t_{g_2}} \equiv 1 \ (mod\,|g_2|),$$

pois G é um grupo finito. Agora, escolhendo $g_3 \notin \mathcal{C}_1 \cup \mathcal{C}_2$, obtemos

$$\mathcal{C}_3 = \{g_3^{q^j} : j = 0, \ldots, t_{g_3} - 1\},$$

em que t_{g_3} é o menor inteiro positivo tal que

$$g_3^{q^{t_{g_3}}} = g_3 \text{ ou } q^{t_{g_3}} \equiv 1 \ (mod\,|g_3|).$$

Continuando deste modo, obtemos a decomposição de G em classes q-ciclotômicas

$$G = \mathcal{C}_1 \cup \mathcal{C}_2 \cup \cdots \cup \mathcal{C}_s.$$

Em particular, se $G = \langle a \rangle$ é um grupo cíclico. Então cada $g \in G$ pode ser escrito sob a forma $g = a^i$ e

$$\mathcal{C}_i = \{i, qi, q^2 i, \ldots, q^{t_i - 1} i\}.$$

Note que os inteiros t_{g_i} sempre existe. De fato. como $mdc(q, |g_i|) = 1$ temos que existem $a, b \in \mathbb{Z}$ tais que

$$aq + b\,|g_i| = 1 \Leftrightarrow aq \equiv 1 \ (mod\,|g_i|) \Leftrightarrow \overline{q} \in \left|\mathcal{U}(\mathbb{Z}_{|g|})\right|,$$

com

$$\mathcal{U}(\mathbb{Z}_{|g_i|}) = \{\overline{r} \in \mathbb{Z}_{|g|} : mdc(r, |g_i|) = 1\} \text{ e } \left|\mathcal{U}(\mathbb{Z}_{|g_i|})\right| = \phi(|g_i|).$$

Logo,

$$g_i = g_i^1 = g_i^{aq + b|g_i|} = g_i^{aq}.$$

Neste caso,

$$T = \{g_1, g_2, \ldots, g_s\}$$

é um conjunto minimal de representante das classes q-ciclotômicas.

Teorema 3.1 *Sejam $\mathbb{F}$ um corpo e G um grupo abeliano. Então o número de componentes simples de $\mathbb{F}G$ é igual ao número de classes q-ciclotômicos de G.*

Prova. Sabemos que o número de componentes simples de $\mathbb{F}G$ é igual à dimensão $\mathbb{A}$ sobre $\mathbb{F}$. Vamos apresentar uma base desta sub-álgebra com s elementos. Dada uma classe q-ciclotômicos $\mathcal{C}_i$, definimos

$$\eta_i = \sum_{g \in \mathcal{C}_i} g \in \mathbb{F}G, \;\; i = 1, \ldots, s.$$

Então

$$\eta_i^q = \left(\sum_{g \in \mathcal{C}_i} g \right)^q = \sum_{g \in \mathcal{C}_i} g^q = \sum_{g \in \mathcal{C}_i} g = \eta_i$$

e $\eta_i \in \mathbb{A}$, $i = 1, \ldots, s$.

Afirmação. $\mathcal{B} = \{\eta_1, \ldots, \eta_s\}$ é uma base $\mathbb{A}$ sobre $\mathbb{F}$ e $s = r$.

De fato, se

$$\sum_{i=1}^{s} \alpha_i \eta_i = 0 \Rightarrow \sum_{i=1}^{s} \sum_{g \in \mathcal{C}_i} \alpha_i g = 0,$$

então $\alpha_i = 0$, $i = 1, \ldots, s$, pois os elementos de G são linearmente independentes. Logo, $\mathcal{B}$ é um conjunto linearmente independente. Assim, resta provar que $\mathcal{B}$ gera $\mathbb{A}$. Dado $\alpha \in \mathbb{A}$, digamos

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

Então

$$\alpha = \sum_{g \in G} \alpha(g) g = \left(\sum_{g \in G} \alpha(g) g \right)^q = \sum_{g \in G} \alpha(g)^q g^q.$$

Se $\alpha(g) \in \mathbb{F}$, então $\alpha(g)^q = \alpha(g)$ e, pelo Lema 3.1, obtemos $\alpha(g) = \alpha(g^q)$, para todo $g \in G$. Portanto,

$$\alpha = \sum_{g \in G} \alpha(g) \eta_i,$$

ou seja, $\mathcal{B}$ gera $\mathbb{A}$. ■

Um teorema bem conhecido, devido a Perlis e Walker [7], mostra que o número de componentes simples da álgebra de grupo racional de um grupo abeliano finito G é igual à ambos o número de subgrupos cíclicos de G e o número dos seus fatores cíclicos. Note que se $h \in \mathcal{C}_i$, então $h = g_i^{q^j}$, para algum j. Como $mdc(q, |g_i|) = 1$ temos que

$$\langle g_i \rangle = \langle h \rangle.$$

Portanto, cada classe q-ciclotômica $\mathcal{C}_g$ é um subconjunto do conjunto de geradores do grupo cíclico $\langle g \rangle$, ou seja,

$$\mathcal{C}_g \subseteq \mathcal{G}_g = \{g^r : mdc(r, |g|) = 1\} = \{g^r : \overline{r} \in \mathcal{U}(\mathbb{Z}_{|g|})\}, \;\; \forall \;\; g \in G.$$

Assim, o número de subgrupos cíclicos de G é uma cota inferior para o número de componentes simples e esta cota é alcançada se, e somente se,

$$\mathcal{C}_g = \mathcal{G}_g, \ \forall \ g \in G.$$

Lembramos que o *expoente* de um grupo G é o menor inteiro positivo n tal que $g^n = 1$, para todo $g \in G$.

Teorema 3.2 *Sejam $\mathbb{F}$ um corpo e G um grupo de expoente e tal que $mdc(q, |G|) = 1$. Então $\mathcal{C}_g = \mathcal{G}_g$, para todo $g \in G$ se, e somente se, $\mathcal{U}(\mathbb{Z}_e)$ é um grupo cíclico gerado por $\overline{q} \in \mathbb{Z}_e$. Neste caso, q é uma raiz primitiva da unidade, ou seja,*

$$q^{\phi(e)} \equiv 1 \ (mode).$$

Prova. Suponhamos que $\mathcal{G}_g = \mathcal{C}_g$, para todo $g \in G$. Como G é um grupo de expoente e temos que existe um $g_0 \in G$ de ordem e tal que $\mathcal{G}_{g_0} = \mathcal{C}_{g_0}$. Logo, para cada $r \in \mathbb{Z}$ tal que $\overline{r} \in \mathcal{U}(\mathbb{Z}_e)$, temos que $g_0^r \in \mathcal{C}_{g_0}$ e existe $j \in \mathbb{Z}$ tal que $\overline{r} = \overline{q}^j$. Portanto, $\overline{q}$ gera $\mathcal{U}(\mathbb{Z}_e)$.

Reciprocramente, suponhamos que $\mathcal{U}(\mathbb{Z}_e)$ seja cíclico gerado por $\overline{q}$. Então, para um $g \in G$, temos que $|g|$ divide e e $\overline{q} \in \mathbb{Z}_{|g|}$ é um gerador de $\mathcal{U}(\mathbb{Z}_{|g|})$. Para cada $h \in \mathcal{G}_g$, temos que existe $r \in \mathbb{Z}_+$ tal que $h = g^r$. Logo, $\overline{r} \in \mathcal{U}(\mathbb{Z}_{|g|})$. Assim, existe $j \in \mathbb{Z}_+$ tal que $\overline{r} = \overline{q}^j$ e $h = g^{q^j} \in \mathcal{C}_g$. Portanto, $\mathcal{G}_g = \mathcal{C}_g$. ■

Lema 3.2 *$\mathcal{U}(\mathbb{Z}_e)$ é um grupo cíclico se, e somente se, $e = 2$, 4, p^n ou $2p^n$, em que p é um número primo ímpar e n é um inteiro positivo.*

Corolário 3.1 *Sejam $\mathbb{F}$ um corpo e G um grupo abeliano de expoente e tal que $mdc(q, |G|) = 1$. Então $\mathcal{C}_g = \mathcal{G}_g$, para todo $g \in G$ se, e somente se, uma das seguintes condições ocorre:*

1. *$e = 2$ e q é número ímpar.*
2. *$e = 4$ e $q \equiv 3 \ (mode)$.*
3. *$e = p^n$, em que p é um número primo ímpar e $|q| = \phi(e)$ em $\mathcal{U}(\mathbb{Z}_e)$.*
4. *$e = 2p^n$, em que p é um número primo ímpar e $|q| = \phi(e)$ em $\mathcal{U}(\mathbb{Z}_e)$.*

Prova. Primeiro note que se

$$G = \{g_1, \ldots, g_k\},$$

então

$$e = mmc(|g_1|, \ldots, |g_k|).$$

Logo, pelo Teorema 3.2, $\mathcal{C}_g = \mathcal{G}_g$, para todo $g \in G$ se, e somente se, $\mathcal{U}(\mathbb{Z}_e)$ é um grupo cíclico gerado por $\overline{q} \in \mathbb{Z}_e$.

(1) Se $e = 2$, então G é um 2-grupo e $\mathcal{U}(\mathbb{Z}_e)$ é um grupo cíclico. Se q é um número ímpar, então

$$q^{\phi(e)} = q \equiv 1 \ \ (mode).$$

Portanto, $\overline{q}$ é um gerador de $\mathcal{U}(\mathbb{Z}_e)$.

(2) Se $e = 4$ e $q \equiv 3 \ \ (mode)$, então $\mathcal{U}(\mathbb{Z}_e)$ é um grupo cíclico e

$$q^{\phi(e)} = q^2 \equiv 1 \ \ (mode).$$

Portanto, $\overline{q}$ é um gerador de $\mathcal{U}(\mathbb{Z}_e)$.

Reciprocamente, se $\overline{q}$ é um gerador de $\mathcal{U}(\mathbb{Z}_e)$, então

$$q^{\phi(e)} = q^2 \equiv 1 \ \ (mode).$$

Logo, e divide $q^2 - 1 = (q-1)(q+1)$. Como $mdc(e, q) = 1$ temos que e divide $q + 1$. Portanto, $q \equiv 3 \ \ (mode)$.

(3) Se $e = p^n$ e $|q| = \phi(e)$ em $\mathcal{U}(\mathbb{Z}_e)$, então $\mathcal{U}(\mathbb{Z}_e)$ é um grupo cíclico e

$$q^{\phi(e)} = q^{|q|} \equiv 1 \ \ (mode).$$

Portanto, $\overline{q}$ é um gerador de $\mathcal{U}(\mathbb{Z}_e)$.

Reciprocamente, se $\overline{q}$ é um gerador de $\mathcal{U}(\mathbb{Z}_e)$, então

$$q^{\phi(e)} \equiv 1 \ \ (mode).$$

Portanto, $|q| = \phi(e)$ em $\mathcal{U}(\mathbb{Z}_e)$.

(4) De modo inteiramente análogo ao item (3), pois

$$\mathcal{U}(\mathbb{Z}_{2p^n}) \simeq \mathcal{U}(\mathbb{Z}_2) \times \mathcal{U}(\mathbb{Z}_{p^n}) \simeq \mathcal{U}(\mathbb{Z}_{p^n})$$

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

Note, pelo Corolário 3.1, que se $G = C_m$ é um grupo cíclico, então $\mathbb{F}C_m$ e $\mathbb{Q}C_m$ possuem o mesmo número de componentes simples se, e somente se, $m = 2$, 4, p^n ou $2p^n$ e a ordem q de $\mathbb{F}$ satisfaz à correspondente condição deste Corolário. Neste caso, como já dissemos, os idempotentes centrais primitivos de $\mathbb{F}C_m$ serão os mesmos já conhecidos de $\mathbb{Q}C_n$, Portanto, podemos descrever os códigos cíclicos minimais.

3.2 Códigos Cíclicos Minimais

Nesta seção daremos a descrição dos idempotentes centrais primitivos de $\mathbb{Q}G$ e em seguida veremos quais são as álgebras de grupo de grupos cíclicos sobre corpos finitos que utilizam a mesma fórmula para o cálculo de seus idempotentes.

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

Lema 3.3 *Sejam $\mathbb{F}$ um corpo finito, com $|\mathbb{F}| = q$, $G = \langle a \rangle$ um grupo cíclico de ordem p^n, com p um número primo, e*

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

a cadeia descendente de subgrupos cíclicos de G. Então os elementos

$$e_0 = \widehat{G}_0 \ \ e \ \ e_i = \widehat{G}_i - \widehat{G}_{i-1}, \ \ i = 1, \ldots, n,$$

formam um conjunto de idempotentes ortogonais de $\mathbb{F}G$ tais que

$$e_0 + e_1 + \cdots + e_n = 1.$$

Prova. Segue do Lema 1.8. ■

Já vimos, pela Observação 1.4, que o método do Lema 3.3, produz o conjunto de idempotentes primitivos de $\mathbb{Q}G$, no entanto, não vale sobre um corpo qualquer. Mas temos o seguinte resultado:

Corolário 3.2 *Sejam $\mathbb{F}$ um corpo finito com $|\mathbb{F}| = q$ e $G = \langle a \rangle$ um grupo cíclico de ordem p^n, com p um número primo. Então o conjunto de idempotentes do Lema 3.3 é um conjunto de idempotentes primitivos se, e somente se, uma das seguintes condição vale*:

1. *$p = 2$, $n = 1$ e q um número ímpar ou $n = 2$ e $q \equiv 3 \ (mod 4)$.*

2. *p é um número primo ímpar e $o(q) = \phi(p^n)$ em $\mathcal{U}(\mathbb{Z}_{p^n})$.*

Prova. Pelo Lema 3.3, existem exatamente $n+1$ elementos idempotentes em $\mathbb{F}G$. Como o expoente de G é igual a p^n temos que eles são primitivos se, e somente se, p^n e q são como no Corolário 3.1. ■

Teorema 3.3 (Pruthi and Arora) *Sejam $\mathbb{F}$ um corpo finito, com $|\mathbb{F}| = q$, $G = \langle a \rangle$ um grupo cíclico de ordem p^n, com p um número primo e $o(q) = \phi(p^n)$ em $\mathcal{U}(\mathbb{Z}_{p^n})$, e*

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

a cadeia descendente de subgrupos cíclicos de G. Então o conjunto dos elementos idempotentes primitivos em $\mathbb{F}G$ é dado por

$$e_0 = \widehat{G}_0 = \frac{1}{p^n} \sum_{g \in G} g \ \ e \ \ e_i = \widehat{G}_i - \widehat{G}_{i-1}, \ \ i = 1, \ldots, n.$$

Prova. Consequência direta do Corolário 3.2. ■

Note que os idempotentes do Teorema 3.3 determinam o conjunto de ideais minimais em $\mathbb{F}G$ e, portanto, o código cíclico minimal de comprimento p^n sobre $\mathbb{F}$. Um cálculo simples mostra que esses são os mesmos idempotentes dados em Pruthi and Arora [11], onde eles são expressos em termos de classes ciclotômicos.

Os idempotentes geradores de ideais minimais no caso de grupos cíclicos de ordem $2p^n$ seguem facilmente dos resultados anteriores.

Seja G um grupo cíclico de ordem $2p^n$, com p um número primo ímpar. Então

$$G = C \times A$$

com A o p-subgrupo de Sylow de G e $C = \{1, t\}$ o 2-subgrupo de Sylow. Assim,

$$\mathbb{F}G \simeq \mathbb{F}(C \times A) \simeq (\mathbb{F}C)A \simeq (\mathbb{F} \otimes \mathbb{F})A.$$

Pelo Exemplo 1.3, os idempotentes primitivos de $\mathbb{F}C$ são

$$e_1 = \frac{(1+t)}{2} \ \text{ e } \ e_2 = \frac{(1-t)}{2},$$

e os idempotentes de $\mathbb{F}A$ são calculados no Teorema 3.3. Assim, obtemos imediatamente o seguinte resultado:

Teorema 3.4 (Arora and Pruthi) *Sejam $\mathbb{F}$ um corpo com q elementos e G um grupo cíclico de ordem $2p^n$, com p número primo ímpar, de modo que $o(q) = \phi(p^n)$ em $\mathcal{U}(\mathbb{Z}_{2p^n})$. Pondo $G = C \times A$, com A o p-subgrupo de Sylow de G e $C = \{1, t\}$ o 2-subgrupo de Sylow. Se e_i, $i = 0, 1, \ldots, n$, são os idempotentes primitivos de $\mathbb{F}A$, então os idempotentes primitivos de $\mathbb{F}G_p$ são*:

$$\frac{1+t}{2} e_i \ \ e \ \ \frac{1-t}{2} e_i, \ \ i = 0, 1, \ldots, n.$$

Prova. Como os idempotentes de $\mathbb{F}C$ são iguais a

$$e_1 = \frac{(1+t)}{2} \text{ e } e_2 = \frac{(1-t)}{2}$$

e os idempotentes de $\mathbb{F}A$ são calculados, pelo Teorema 3.3, temos o resultado. ■

Note que a dimensão e a distância mínima dos ideais mínimais

$$I_i = (\mathbb{F}G)(\widehat{G_i} - \widehat{G_{i-1}})$$

pode ser calculado diretamente de uma forma simples, que será dada na última seção em um contexto mais geral para códigos abelianos. Os polinômios geradores não são realmente necessários nesta abordagem, mas será dada por uma questão de completude. Eles podem ser facilmente calculado como se segue: Se $e_i(X) \in \mathbb{F}_q[X]$ é um polinômio qualquer tal que $e_i(a) = e_i$, então o polinômio gerador para I_i é dada por

$$g_i(X) = mdc(e_i(X), X^{p^n} - 1), \;\; i = 0, 1, \ldots, n.$$

Calculamos

$$\begin{aligned}
e_i(X) &= \frac{1}{p^{n-i}} \sum_{j=0}^{p^{n-i}-1} X^{jp^i} - \frac{1}{p^{n-i+1}} \sum_{j=0}^{p^{n-i+1}-1} X^{jp^{i-1}} \\
&= \frac{1}{p^{n-i+1}} \left[p \sum_{j=0}^{p^{n-i}-1} X^{jp^i} - \sum_{j=0}^{p^{n-i+1}-1} X^{jp^{i-1}} \right] \\
&= \frac{1}{p^{n-i+1}} \left[(p-1) \left(\sum_{j=0}^{p^{n-i}-1} X^{jp^i} \right) - \left(\sum_{j=1}^{p-1} X^{jp^{i-1}} \right) \left(\sum_{j=0}^{p^{n-i}-1} X^{jp^i} \right) \right] \\
&= \frac{1}{p^{n-i+1}} \left(p - \sum_{j=0}^{p-1} X^{jp^{i-1}} \right) \left(\sum_{j=0}^{p^{n-i}-1} X^{jp^i} \right)
\end{aligned}$$

e

$$\begin{aligned}
X^{p^n} - 1 &= (X^{p^i} - 1) \sum_{j=0}^{p^{n-i}-1} X^{jp^i} \\
&= (X^{p^{i-1}} - 1) \left(\sum_{j=0}^{(p-1)p^{i-1}} X^{jp^{i-1}} \right) \left(\sum_{j=0}^{p^{n-i}-1} X^{jp^i} \right).
\end{aligned}$$

Como qualquer raiz de $(X^{p^{i-1}} - 1)$ em um fecho algebrico $\mathbb{F}$ é uma raiz de

$$p - \sum_{j=0}^{(p-1)p^{i-1}} X^{jp^{i-1}}$$

temos que

$$\begin{aligned} g_i(X) &= mdc(e_i(X), X^{p^n}-1) \\ &= (X^{p^{i-1}}-1)\left(\sum_{j=0}^{p^{n-i}-1} X^{jp^i}\right). \end{aligned}$$

Logo o grau de $(g_i(X))$ é igual a $p^n - p^i + p^{i-1}$. Portanto,

$$\dim(I_i) = p^n - \partial(g_i(X)) = p^i - p^{i-1} = \varphi(p^i).$$

3.3 Códigos Abelianos Minimais

Nesta seção vamos estender os resultados da Seção anterior para grupos abelianos finitos. Vamos primeiro considerar o caso de p-grupos. Seja G um p-grupo abeliano. Então, para cada subgrupo H de G tal que

$$\overline{G} = \frac{G}{H} \neq \{1\}$$

seja cíclico, construiremos um idempotente de $\mathbb{F}G$. Observe que como $\overline{G}$ é um grupo cíclico de ordem p^n temos, pelo Teorema da Correspondência, que existe um único subgrupo H^* de G contendo H tal que

$$\left|\frac{H^*}{H}\right| = p.$$

Definimos $e_H = \widehat{H} - \widehat{H^*}$, obtemos $e_H \neq 0$ e o seguinte resultado:

Lema 3.4 *Os elementos e_H, definido acima, com $e_G = \widehat{G}$ formam o conjunto de idempotentes ortogonais aos pares de $\mathbb{F}G$, cuja soma é igual a 1.*

Prova. Note que

$$e_H^2 = \left(\widehat{H} - \widehat{H^*}\right)\left(\widehat{H} - \widehat{H^*}\right) = \widehat{H} - \widehat{H}\widehat{H^*} - \widehat{H}\widehat{H^*} + \widehat{H^*} = \widehat{H} - \widehat{H^*} = e_H.$$

Sejam H e K diferentes subgrupos de G tais que

$$\frac{G}{H} \neq \{1\} \text{ e } \frac{G}{K} \neq \{1\}$$

sejam cíclicos e H^* e K^* subgrupos de G contendo de H e K, respectivamente, tais que

$$\left|\frac{H^*}{H}\right| = p \text{ e } \left|\frac{K^*}{K}\right| = p.$$

Se H e K são comparáveis, digamos $H \subset K$, então $H^* \subseteq K$ e

$$e_H e_K = (\widehat{H} - \widehat{H^*})(\widehat{K} - \widehat{K^*}) = \widehat{H}\widehat{K} - \widehat{H}\widehat{K^*} - \widehat{H^*}\widehat{K} + \widehat{H^*}\widehat{K^*} = 0.$$

Se H e K não são comparáveis, então $H, K \subset HK$. Assim, $H^*, K^* \subset HK$. Logo, $H^*K^* \subset HK$. Portanto $HK = H^*K^*$. Como

$$HK \subset HK^* \subset H^*K^*$$

temos que $HK^* = HK$. De modo análoga, obtemos $H^*K = HK$. Portanto,

$$e_H e_K = 0.$$

Em particular,

$$e_H e_G = 0 \text{ e } e_G e_K = 0.$$

Finalmente, para cada subgrupo cíclico C de G, denotamos por $\mathcal{G}(C)$ o conjunto de todos os elementos de C que geram esse subgrupo, isto é,

$$\mathcal{G}(C) = \{c \in C : mdc(o(c), |C|) = 1\}.$$

Se $\mathcal{C}$ é a família de todos os subgrupos cíclicos de G, então

$$|G| = \sum_{C \in \mathcal{C}} |\mathcal{G}(C)|$$

e como G é um p-grupo temos que

$$|\mathcal{G}(C)| = |C| - \frac{|C|}{p}.$$

Agora, seja $\mathcal{S}$ o conjunto de todos os subgrupos H de G tal que

$$\overline{G} = \frac{G}{H} \neq \{1\}$$

seja cíclico e denotamos

$$e = \sum_{H \in \mathcal{S}} e_H.$$

Afirmação. $e = 1$.

De fato, basta provar que $(\mathbb{F}G)e = \mathbb{F}G$. Já vimos que esses idempotentes são ortogonais aos pares. Logo,

$$(\mathbb{F}G)e = \sum_{H \in \mathcal{S}} (\mathbb{F}G)e_H \text{ e } \dim(\mathbb{F}G)e = \sum_{H \in \mathcal{S}} \dim(\mathbb{F}G)e_H.$$

Note que

$$\dim(\mathbb{F}G)e_H = \dim(\mathbb{F}G)\widehat{H} - \dim(\mathbb{F}G)\widehat{H^*},$$

pois $\widehat{H} = \widehat{H^*} + e_H$ e $\widehat{H^*}e_H = 0$ implicam que

$$(\mathbb{F}G)\widehat{H} = (\mathbb{F}G)e_H \oplus (\mathbb{F}G)\widehat{H^*}.$$

Pelo item (2) do Lema 1.6, obtemos

$$\dim(\mathbb{F}G)e_H = \dim \mathbb{F}\left(\frac{G}{H}\right) - \dim(\mathbb{F}\left(\frac{G}{H^*}\right) \tag{3.1}$$

e

$$\dim \mathbb{F}\left(\frac{G}{H}\right) = \left|\frac{G}{H}\right| \text{ e } \dim \mathbb{F}\left(\frac{G}{H^*}\right) = \left|\frac{G}{H^*}\right|.$$

Pode ser provado que existe uma função bijetora $\sigma : \mathcal{C} \to \mathcal{S}$ tal que

$$|X| = \left|\frac{G}{\sigma(X)}\right|, \ \forall \ X \in \mathcal{C}.$$

Se denotarmos por $C \in \mathcal{C}$ o subgrupo de G tal que $\phi(C) = H$, então, pelo Terceiro Teorema de Isomorfismos,

$$\dim \mathbb{F}\left(\frac{G}{H}\right) = |C| \text{ e } \dim \mathbb{F}\left(\frac{G}{H^*}\right) = \left|\frac{G}{H^*}\right| = \left|\frac{\frac{G}{H}}{\frac{H^*}{H}}\right| = \frac{|C|}{p}.$$

Assim,

$$|\mathcal{G}(C)| = |C| - \frac{|C|}{p} = \dim(\mathbb{F}G)e_H.$$

Portanto,

$$\dim(\mathbb{F}G)e = \sum_{H \in \mathcal{S}} \dim(\mathbb{F}G)e_H = \sum_{C \in \mathcal{C}} |\mathcal{G}(C)| = |G|$$

e $e = 1$. ■

Teorema 3.5 *Sejam p um número primo ímpar e G um p-grupo abeliano de expoente p^r. Então o conjunto de idempotentes do Lema* 3.4 *é o conjunto de idempotentes primitivos de $\mathbb{F}G$ se, e somente se, uma das seguintes condições vale*:

1. *$p^r = 2$ e q for um número ímpar.*

2. *$p^r = 4$ e $q \equiv 3 \ (mod 4)$.*

3. *p é um número primo ímpar e $o(q) = \phi(p^r)$ em $\mathcal{U}(\mathbb{Z}_{p^r})$.*

Prova. Consequência direta do Lema 3.4 e do Corolário 3.1. ■

Teorema 3.6 *Sejam p um primo ímpar e G um p-grupo abeliano de expoente $2p^n$. Pondo $G = E \times B$, com E um 2-grupo abeliano elementar e B um p-grupo. Em seguida, o idempotentes primitivos da $\mathbb{F}G$ são produtos da forma ef, em que e é um idempotente primitivo da $\mathbb{F}E$ e f um idempotente primitivo de $\mathbb{F}B$.*

Observe que o idempotentes primitivos de $\mathbb{F}B$ são dadas pelo Teorema 3.5 e, pelo Exemplo 1.3, os idempotentes primitivo de $\mathbb{F}E$ são todos os produtos da forma $e = e_1e_2\cdots e_m$, com

$$e_i = \frac{1+t_i}{2} \text{ e } e_i = \frac{1-t_i}{2}, \ \ i = 0, 1, \ldots, m.$$

Note, pelo Corolário 3.1, que esses são os únicos casos onde os idempotentes primitivos da álgebras de grupo abeliano finito pode ser calculado desta maneira.

3.4 Dimensão e Distância Mínima

Suponhamos que G é um grupo de ordem $2^m p^n$, com p um número primo ímpar e $m \geq 0$. Pondo

$$G = E \times B \text{ e } E = \langle t_1 \rangle \times \cdots \times \langle t_m \rangle,$$

com E um 2-grupo abeliano elementar de ordem 2^m (eventualmente trivial) e B um p-grupo de Sylow. Já vimos, no Teorema 3.6, que os idempotentes primitivos de $\mathbb{F}E$ são todos os produtos da forma $e = e_1e_2\cdots e_m$, com

$$e_i = \frac{1+t_i}{2} \text{ e } e_i = \frac{1-t_i}{2}, \ \ i = 0, 1, \ldots, m.$$

e os idempotentes primitivos da $\mathbb{F}G$ são produtos da forma e_Ee_B, em que e_E é um idempotente primitivo de $\mathbb{F}E$ e e_B um idempotente primitivo de $\mathbb{F}B$.

Fixado um idempotente e_E de $\mathbb{F}E$ e um elemento $y \in E$, digamos

$$y = t_1^{\varepsilon_1}\cdots t_m^{\varepsilon_m}, \text{ onde } \varepsilon_i \in \{0,1\}, \ \ i = 0, 1, \ldots, m.$$

Assim

$$ye_E = t_1^{\varepsilon_1}\left(\frac{1 \pm t_1}{2}\right)\cdots t_m^{\varepsilon_m}\left(\frac{1 \pm t_m}{2}\right) = \pm e_E = (-1)^{\varepsilon_y}e_E, \tag{3.2}$$

onde $\varepsilon_y \in \{0,1\}$.

Consideremos primeiro o idempotente primitivo da forma $e_E\widehat{B}$. Um elemento de $(\mathbb{F}G)e_E\widehat{B}$ pode ser escrito sob a forma $\gamma e_E\widehat{B}$, com

$$\gamma = \sum_{y\in E, b\in B} x_{yb}yb,$$

Logo,

$$\gamma e_E\widehat{B} = \sum_{y\in E,b\in B} x_{yb}ye_Eb\widehat{B} = \left(\sum_{y\in E,b\in B} x_{yb}(-1)^{\varepsilon_y}\right)e_E\widehat{B}.$$

Portanto, a dimensão do ideal $I = (\mathbb{F}G)e_E\widehat{B}$ é igual a 1 e a distância mínima é $l(I) = |G|$.

Agora, consideramos os idempotentes da forma $e = e_Ee_H$, onde $e_E \in \mathbb{F}E$ e $e_H = \widehat{H} - \widehat{H^*}$, com H é um subgrupo de B tal que

$$\frac{B}{H}$$

é um grupo cíclico de ordem p^i, e H^* é o único subgrupo de B contendo H tal que

$$[H^* : H] = p.$$

Sejam $I_e = (\mathbb{F}G)e$ e $b \in B$ tal que $B = \langle b, H\rangle$. Então

$$H^* = \langle b^{p^{i-1}}, H\rangle.$$

Note que

$$(1 - b^{p^{i-1}})e_E\widehat{H} = (1 - b^{p^{i-1}})e_E(\widehat{H^*} + e_H) = (1 - b^{p^{i-1}})e_Ee_H \in I_e.$$

Como $b^{p^{i-1}} \notin H$ temos que

$$supp((1 - b^{p^{i-1}})\widehat{H}) = H \cup b^{p^{i-1}}H$$

é uma união disjunta e o peso deste elemento é

$$w((1 - b^{p^{i-1}})e_E\widehat{H}) = 2\,|E|\,|H|\,,$$

de modo que, se denotarmos por $l(I_e)$ a distância mínima de I_e, temos que $l(I_e) \leq 2^{m+1}\,|H|$.

Sendo

$$B = H \cup bH \cup \cdots \cup b^{p^i-1}H,$$

uma união disjunta, obtemos

$$G = E \times H \cup b(E \times H) \cup \cdots \cup b^{p^i-1}(E \times H)$$

união disjunta. Assim, qualquer elemento α de $\mathbb{F}G$ pode ser escrito sob a forma

$$\alpha = \sum_{j=0}^{p^i-1} \alpha_j b^j, \text{ onde } \alpha_j \in \mathbb{F}[E \times H].$$

Note que pela equação (3.2) e pelo fato de que $h\widehat{H} = \widehat{H}$, para todo $h \in H$, obtemos

$$\alpha_j e_E e_H = \alpha_j e_E e_H = k_j e_E e_H, \text{ onde } k_j \in \mathbb{F}, \ j = 0, 1, \ldots, p^i - 1.$$

Como

$$(\mathbb{F}G)e_E e_H \subset (\mathbb{F}G)e_E\widehat{H},$$

temos que

$$0 \neq \gamma \in (FA).e_E e_H = I_e$$

pode ser escrito sob a forma

$$\gamma = \alpha e_E\widehat{H} = (k_0 + k_1 b + \cdots + k_{p^i-1}b^{p^i-1})e_E\widehat{H},$$

com pelo menos um dos coeficientes $k_j \neq 0$. Se $\gamma = k_j b^j e_E\widehat{H}$, então $e_E\widehat{H} \in (\mathbb{F}G)e_E e_H$, o que uma é contradição. Assim, pelo menos dois coeficientes diferentes k_j e $k_{j'}$ são diferentes de zero em γ. Portanto,

$$l(I_e) \geq 2^{m+1}\,|H| \text{ e } l(I_e) = 2^{m+1}\,|H|\,.$$

Finalmente, vamos calcular a dimensão do código abeliano minimal, ou seja, a dimensão dos ideais da forma $\mathbb{F}Ge$, com e um idempotente primitivo de $\mathbb{F}G$. Seja $e = e_E e_H$ um idempotente primitivo. Então

$$\mathbb{F}Ge_E e_H = \mathbb{F}[E \times B]e_E e_H = ((\mathbb{F}E)B)e_E e_H = (\mathbb{F}Ee_E)Be_H.$$

Como $(\mathbb{F}E)e_E$ é isomorfo a $\mathbb{F}$, para todos os idempotentes primitivos de $\mathbb{F}E$, temos que

$$\mathbb{F}Ge_E e_H \simeq \mathbb{F}Be_H.$$

Assim, pela equação (3.1), temos que

$$\dim(\mathbb{F}Ge_E e_H) = \phi(p^i).$$

De modo análogo, obtemos

$$\dim(\mathbb{F}Ge_E\widehat{B}) = \dim(\mathbb{F}B\widehat{B}) = 1.$$

Exemplo 3.1 *Sejam G um grupo cíclico de ordem 2^3 e $\mathbb{F} = \mathbb{F}_3$ um corpo com três elementos. Então*

$$\begin{aligned} G_0 &= \langle a \rangle = \{1, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8\} \\ G_1 &= \langle a^2 \rangle = \{1, a^2, a^4, a^8\} \\ G_2 &= \langle a^4 \rangle = \{1, a^4, a^8\} \\ G_3 &= \langle a^8 \rangle = \{1\}. \end{aligned}$$

Portanto, os idempotentes primitivos de $\mathbb{F}G$ são:

$$\begin{aligned} e_0 &= \widehat{G}_0 = 2 + 2a + 2a^2 + 2a^3 + 2a^4 + 2a^5 + 2a^6 + 2a^7 \\ e_1 &= \widehat{G}_1 - \widehat{G}_0 = 2 + a + 2a^2 + a^3 + 2a^4 + a^5 + 2a^6 + a^7 \\ e_2 &= \widehat{G}_2 - \widehat{G}_1 = 1 + 2a^2 + a^4 + 2a^6 \\ e_3 &= \widehat{G}_3 - \widehat{G}_2 = 2 + a^4. \end{aligned}$$

Referências Bibliográficas

[1] Bhattacharya, P. B., Jain, S. K. e Nagpaul, S. R., *Basic Abstract Algebra*. Cambridge, New York, 1995.

[2] I.F. Blake, R.C. Mullin, *The Mathematical Theory of Coding*, Academic Press, New York, 1975.

[3] C.W. Curtis, I. Reiner, *Methods of Representation Theory*, vol. I, Wiley-Interscience, New York, 1981.

[4] L. Dornhoff, *Group Representation Theory*, Part B, Dekker, New York, 1971.

[5] R. Ferraz, "Simple components and central units in group algebras," *J. Algebra* 279 (2004) 191-203.

[6] Lidl, R. and Niederreiter, H., *Finite Fields*. in Encyclopedia of Mathematics and Its Applications, vol. 20, 1983.

[7] S. Perlis, G. Walker, "Abelian group algebras of finite order," *Trans. Amer. Math. Soc.* 68 (1950) 420-426.

[8] C. Polcino Milies, S.K. Sehgal, *An Introduction to Group Rings*, Kluwer Academic, Dordrecht, 2002.

[9] E.G. Goodaire, E. Jespers, C. Polcino Milies, *Alternative Loop Rings*, North-Holland Math. Stud., vol. 184, Elsevier, Amsterdam, 1996.

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

[11] M. Pruthi, S.K. Arora, "Minimal codes of prime power length," *Finite Fields Appl.* 3 (1997) 99-113.

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

[13] J.J. Rotman, *An Introduction to the Theory of Groups*, fourth ed., Springer-Verlag, New York, 1995.