Idempotentes Centrais Primitivos Em Algumas Álgebras de Grupos

Vitor Araujo Garcia

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

Programa: Matemática

Orientador: Prof. Dr. Raul Antonio Ferraz

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

São Paulo, julho de 2015

Idempotentes Centrais Primitivos Em Algumas Álgebras de Grupos

Esta versão da dissertação contém as correções e alterações sugeridas pela Comissão Julgadora durante a defesa da versão original do trabalho, realizada em 25/09/2015. Uma cópia da versão original está disponível no Instituto de Matemática e Estatística da Universidade de São Paulo.

Comissão Julgadora:

- Prof. Dr. Raul Antonio Ferraz (orientador) - IME-USP
- Prof. Dr. Francisco Cesar Polcino Milies - IME-USP
- Prof. Dr. Antonio Paques - UFRGS

Agradecimentos

Agradeço a Deus em primeiro lugar.

Também agradeço à minha família e amigos pelo apoio e companhia, sem os qual seria impossível chegar até aqui.

Não posso deixar de agradecer aos professores e colegas, pelo apoio e pelas orientações, em especial agradeço ao professor Raul Antonio Ferraz pela sua paciência e orientação, que sem dúvida não foram apenas de grande ajuda, mas foram essenciais para que este trabalho pudesse ser realizado.

Resumo

GARCIA, V. A. **Idempotentes Centrais Primitivos em Algumas Álgebras de Grupos**. 2015. Dissertação (Mestrado) - Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2015.

O objetivo do trabalho é apresentar alguns resultados acerca de anéis de grupos e aplicações, segundo o que foi estudado em livros e artigos sobre o assunto. Inicialmente, apresentaremos alguns fatos básicos sobre anéis de grupos, que podem ser encontrados em [**5**], e em seguida, apresentaremos os resultados principais, mais recentes, que foram estudados em dois artigos diferentes. No primeiro artigo [**4**], apresentou-se uma forma de calcular o número de componentes simples de certas álgebras de grupos abelianos finitos, bem como também foi apresentada uma forma de calcular geradores idempotentes de códigos abelianos minimais, suas dimensões e seus pesos. No segundo artigo [**2**], encontra-se uma descrição feita dos idempotentes centrais primitivos da álgebra de grupo racional de grupos nilpotentes finitos.

Palavras-chave: Anel de Grupo; Idempotentes; Álgebra de Grupo; Código Minimal; Código Abeliano.

Abstract

GARCIA, V. A. **Primitive Central Idempotents in Some Group Algebras**. 2015. Master's Thesis - Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2015.

Our goal in this project is to present some results about group rings and its applications, as presented in books and articles about this subject. First of all we are going to establish some basic fact about group rings, which can be found mainly in [**5**], and then we will present the main results, which are more recent, and have been studied in two different articles. In [**4**], the authors presented a way of evaluating the number of simple components of some finite group algebras, as well presented a way of evaluating idempotent generators of some minimal abelian codes, their dimension and their weights. In [**2**] there is a complete description of all the primitive central idempotents of the rational group algebra of finite nilpotent groups.

Keywords: Group Rings; Idempotents; Group Algebras; Minimal Code; Abelian Code.

Sumário

Lista de Símbolos

$H \leq K$	H subgrupo de K
$\langle g \rangle$	Grupo gerado por g
$U(\mathbb{Z}_n)$	Grupo multiplicativo das unidades de Z_n
$o(g)$	Ordem do elemento g
$\mathbb{C}$	Corpo dos números complexos
$\mathbb{Q}$	Corpo dos números racionais
F_q	Corpo finito com q eleentos
$C_G(H)$	Centralizador de H em G
C_g	Conjunto dos G conjugados de g
$Z(G)$	Centro de G
$Z_i(G)$	i-ésimo centro de G
$[h, k]$	Comutador de $h, , k$. O mesmo que escrever $hkh^{-1}k^{-1}$
h^g	o mesmo que escrever $g^{-1}hg$
$UT(n, F)$	Matrizes $n \times n$ unitriangulares com entradas no corpo F
$\mathcal{M}(G)$	Conjunto de todos os subgrupos normais minimais do grupo G
$\widehat{H}$	$\frac{1}{\lvert H \rvert} \sum_{g \in H} g$
$\varepsilon(G)$	$\prod_{M \in \mathcal{M}(G)} (1 - \widehat{M})$, se $G \neq \{1\}$, e $\varepsilon(\{1\}) = 1$
$\varepsilon(G, N)$	$\prod_{\bar{M} \in \mathcal{M}(G/N)} (\widehat{N} - \widehat{M})$, se N é subgrupo próprio de G, e $\varepsilon(G, G) = \widehat{G}$

Capítulo 1

Introdução

Nesta dissertação estudaremos em detalhes os artigos *Idempotents in group algebras and minimal abelian codes* [**4**] escrito por Ferraz, R. A., e Polcino Milies, C., e *Central idempotents in the rational group algebra of a finite nilpotent group* [**2**] escrito por Jespers, E., Leal, G., e Paques, A..

O primeiro artigo trata de idempotentes primitivos e componentes simples de certas álgebras de grupos abelianos finitos sobre corpos finitos e da dimensão de ideais minimais de alguns códigos e será abordado no Capítulo 2.

O segundo artigo traz uma identificação de todos os idempotentes centrais primitivos de álgebras racionais de grupos nilpotentes finitos, começando pelo caso abeliano. Também faremos um exemplo simples para mostrar uma aplicação do resultado principal deste segundo artigo. Será abordado no Capítulo 3.

Neste capítulo introdutório, enunciaremos alguns resultados básicos de que precisaremos como pré-requisitos para as partes principais do trabalho, e deixaremos os demais pré-requisitos para os capítulos seguintes.

Na subseção 1.1.1, enunciaremos alguns resultados e algumas definições básicas da teoria de anéis de grupos de que precisaremos nos capítulos seguintes.

Na subseção 1.1.2, nosso objetivo principal será chegar em um resultado conhecido que relaciona subgrupos e quocientes de grupos abelianos finitos, usando para isso grupos de caracteres. Este resultado será usado no Capítulo 2.

Na subseção 1.1.3, listaremos algumas definições e propriedades básicas sobre códigos cíclicos, bem como sua relação com anéis de polinômios e anéis de grupos.

Também usaremos essas informações no Capítulo 2.

Na subseção 1.1.4, falaremos sobre grupos nilpotentes e séries centrais, com alguns resultados importantes que serão usados no Capítulo 3. Também apresentaremos uma classe de grupos nilpotentes bem conhecida, como exemplo.

Neste capítulo, aqueles resultados que se encontram em referências não serão provados, mas citaremos onde encontrar as suas demonstrações.

1.1 Objetivos

O objetivo deste trabalho é estudar em detalhes os artigos [**4**] e [**2**], ambos tratando sobre idempotentes centrais primitivos em algumas álgebras de grupo. Para isso, utilizaremos os conceitos e resultados que foram apresentados no sub-tópico anterior.

Estudar esses artigos permitirá pensar em investigações futuras a respeito do assunto anéis de grupos, bem como permitirá estudar outros artigos mais avançados a respeito do tema.

1.2 Contribuições

As principais contribuições deste trabalho foram detalhar (em idioma português) dois artigos matemáticos relativamente recentes, bem como apresentar alguns pré-requisitos básicos da teoria e colocá-los numa ordem em que se possa entender os artigos, se estudados como apresentados desde a introdução até o Capítulo 3.

Obs.: Não foi desenvolvido nenhum resultado original/inédito na elaboração desta dissertação.

1.3 Organização do Trabalho

No capítulo introdutório, como já dito, o conteúdo principal foi explicar qual o objetivo da dissertação e apresentar uma série de resultados e conceitos básicos que servem como pré-requisitos para os artigos seguintes (principais). As referências que utilizamos para escrever este capítulo foram [**5**], [**1**], [**9**], [**8**] e [**7**].

No Capítulo 2, apresentaremos e provaremos em detalhes os resultados do artigo [4], que estuda certas álgebras de grupo comutativas sobre corpos finitos. Este artigo será nossa principal referência para este capítulo - também utilizaremos resultados que foram apresentados no capítulo introdutório.

No Capítulo 3, apresentaremos e provaremos os resultados do artigo [2], que apresenta uma caracterização dos idempotentes centrais primitivos da álgebra de grupo racional de grupos nilpotentes finitos.

1.4 Considerações Preliminares

Listaremos a seguir algumas noções e resultados básicos que serão usados ao longo dos capítulos principais (capítulos 2 e 3). Os resultados citados a seguir são bem conhecidos, e a maior parte deles não serão provados aqui. No entanto, há referências para textos em que se pode encontrar a prova para eles. Os resultados para os que não há referência serão provados, ou terão um pequeno esboço de prova.

1.4.1 Anéis de Grupos

Nesta subseção, introduziremos alguns dos conceitos e resultados básicos da teoria de anéis de grupos, nos baseando principalmente em [**5**] e [**1**].

Definição 1.4.1 *Seja G um grupo e R um anel com* 1. *Definimos RG como sendo o conjunto de todas as somas formais do tipo*

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

onde $a_g \in R, g \in G$, e apenas uma quantidade finita dos a_g´s é diferente de zero. Definimos as operações em RG por:

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

Se $\alpha = \sum_{g\in G} a_g g$ e $\beta = \sum_{g\in G} b_g g$:

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

Com estas operações, RG é chamado ***anel de grupo de*** G ***sobre*** R.

Com as operações acima definidas, temos que RG é um anel com $1 = \sum_{g\in G} u_g g$, *onde* $u_{1_G} = 1$ *e, se* $g \neq 1_G$, $u_g = 0$.

Definimos o suporte de α: $supp(\alpha) = \{g \in G : a_g \neq 0\}$.

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

Se R for comutativo, também podemos definir, para $\lambda \in R$ e $\alpha = \sum_{g\in G} a_g g \in RG$, o produto

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

e com esta operação, temos naturalmente que RG é um R-módulo. Neste caso, RG também é chamado **álgebra de grupo de** G **sobre** R.

Existe uma aplicação injetora natural de G em RG, dada por $h \mapsto \sum_{g\in G} a_g g$, onde $a_g = 0$, se $g \neq h$, e $a_h = 1$ e, com esta aplicação, podemos ver G como um subconjunto de RG. Desta forma, podemos dizer que RG é módulo livre, onde G é uma base. Temos, em particular, que se R for comutativo, então a dimensão de RG sobre R está bem definida, e será a cardinalidade de G (se G for finito, será |G|).

Também existe aplicação injetora natural de R em RG, dada por $r \mapsto \sum_{g\in G} a_g g$, onde $a_{1_G} = r$ e, se $g \neq 1_G$ então $a_g = 0$. Esta aplicação é um homomorfismo e, portanto, podemos, através dela, enxergar R como um sub-anel de RG.

Se R é anel comutativo e G, H são grupos, então

$$R(G \times H) \simeq (RG)H,$$

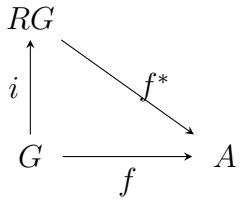
(podemos supor que $G \times H$ se trata de produto direto interno) e isso segue do fato de que a função $\varphi : R(G \times H) \to (RG)H$, dada por

$$\varphi\Big(\sum_{gh\in G\times H}\alpha_{gh}gh\Big)=\sum_{h\in H}\Big(\sum_{g\in G}\alpha_{gh}g\Big)h$$

é um isomorfismo.

Agora, enunciaremos uma propriedade universal de anéis de grupos:

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



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

Prova: veja Proposição 3.2.7 de [**5**]. □

O seguinte resultado é um caso particular da proposição acima e, vamos enunciá-lo separadamente porque precisaremos dele mais adiante.

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

Prova: veja o Corolário 3.2.8 de [**5**]. □

Precisaremos de resultados acerca de anéis de grupos semisimples para estudarmos os capítulos principais. Para chegar nesses resultados, [**5**] utiliza alguns fatos

sobre ideais de aumento:

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

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

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

Chegamos então no conhecido teorema que determina condições necessárias e suficientes para um anel de grupo ser semisimples:

Teorema 1.4.5 ***(Maschke)*** *Seja G um grupo. Então o anel de grupo RG é semisimples se, e somente se valem as seguintes condições:*

(i) R é um anel semisimples;

(ii) G é finito;

(iii) $|G|$ é inversível em R.

Prova: ver subseção 3.4 de [**5**] e, para pré-requisitos sobre ideais de aumento, veja a subseção 3.3 de [**5**]. □

Temos, em particular, que se $R = K$ é um corpo e G é um grupo finito, então $RG = KG$ é semisimples se, e somente se $car(K) \not| |G|$. Portanto, sempre que K for um corpo de característica zero e G for um grupo finito, teremos que KG é semissimples.

É bem conhecido o teorema de Wedderburn-Artin, para anéis semissimples. Enunciemos este teorema para o contexto de anéis de grupos:

Teorema 1.4.6 *Seja G um grupo finito e K um corpo tal que $char(K) \nmid |G|$. Então:*

(i) KG é a soma direta de uma quantidade finita de ideais bilaterais $\{B_i\}_{1\leq i\leq r}$, os componentes simples de KG. Cada B_i é um anel simples.

(ii) Qualquer ideal bilateral de KG é a soma direta de alguns membros da família $\{B_i\}_{1\leq i\leq r}$.

(iii) Cada B_i é isomorfo a um anel de matrizes da forma $M_{n_i}(D_i)$, onde D_i é um anel com divisão que contém uma cópia de K no seu centro.
E o isomorfismo

$$KG \overset{\varphi}{\simeq} \oplus_{i=1}^{r} M_{n_i}(D_i)$$

é um isomorfismo de K-álgebras.

(iv) Em cada anel de matrizes $M_{n_i}(D_i)$, o conjunto $I_{i,j}$ das matrizes cujas entradas fora da coluna j são todas nulas é ideal minimal à esquerda e, além disso, $M_{n_i}(D_i) = \oplus_{j=1}^{n_i} I_{i,j}$.
Além disso, dado $x \in KG$, considerando $\varphi(x) = (\alpha_1, ..., \alpha_r) \in \oplus_{i=1}^{r} M_{n_i}(D_i)$ e definindo $xm_i = \alpha_i m_i$, para todo $m_i \in I_{i,j}$, então $I_{i,j}$ pode ser visto como um KG-módulo simples.

(v) $I_{i,j} \simeq I_{k,l}$ se, e somente se $i = k$.

(vi) Qualquer KG-módulo simples é isomorfo a algum $I_{i,j}$.

Também temos uma versão do Teorema 2.6.9 de [**5**], que será muito importante nos capítulos seguintes:

Teorema 1.4.7 *Seja $KG = \oplus_{i=1}^{r} B_i$ uma decomposição de KG (semisimples) como soma direta de ideais bilaterais minimais da álgebra de grupo KG. Então existe uma família $\{e_1, ..., e_r\}$ de elementos de KG tais que:*

(i) $e_i \neq 0$ *é idempotente e central,* $1 \leq i \leq r$*;*

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

(iii) $1 = e_1 + ... + e_r$*;*

(iv) e_i *não pode ser escrito como a soma de dois elementos não-nulos idempotentes centrais de* KG *que sejam ortogonais.*

Este último motiva a seguinte definição:

Definição 1.4.8 *Os elementos* e_i *conforme o teorema acima são chamados* ***idempotentes centrais primitivos*** *de* KG*.*

Se KG for semissimples temos, pelo Teorema de Wedderburn-Artin que

$$KG \simeq M_{n_1}(D_1) \oplus ... \oplus M_{n_r}(D_r),$$

e, pela demonstração do teorema acima, temos que os idempotentes centrais primitivos de KG são relacionados às matrizes identidade, isto é, os idempotentes centrais primitivos $e_1, ..., e_r$ são levados pelo isomorfismo nas matrizes identidade de $M_{n_1}(D_1), ..., M_{n_r}(D_r)$, respectivamente. Segue que todo idempotente central não nulo é soma de idempotentes primitivos centrais (pois os únicos elementos centrais de cada anel de matrizes acima são as matrizes escalares, e só são idempotentes se forem identidades).

Quando G é um grupo abeliano finito, temos ainda o seguinte teorema:

Teorema 1.4.9 ***(Perlis-Walker)*** *Seja* G *um grupo abeliano finito, de ordem* n*, e seja* K *um corpo tal que* $char(K) \nmid n$*. Então:*

$$KG \simeq \oplus_{d|n} a_d K(\zeta_d)$$

onde ζ_d *é uma raiz primitiva da unidade de ordem* d *e* $a_d = \frac{n_d}{[K(\zeta_d):K]}$*. Nesta fórmula,* n_d *denota a quantidade de elementos de ordem* d *em* G*.*

Em particular, se $K = \mathbb{Q}$, então a_d é o número de subgrupos cíclicos de ordem d em G.

Obs.: a parte 'em particular' nós temos do fato de que $[\mathbb{Q}(\zeta_d) : \mathbb{Q}] = \phi(d)$, o número de geradores do grupo cíclico de ordem d.

Prova: ver subseção 3.5 de [**5**].

Como corpos são anéis simples, temos que o teorema acima nos dá as componentes simples destes anéis de grupos. A parte 'em particular' do teorema nos diz ainda que, se G é um grupo abeliano finito, então a quantidade de idempotentes (centrais) primitivos de $\mathbb{Q}G$ é igual à quantidade de subgrupos cíclicos de G.

Na subseção seguinte, estudaremos um pouco sobre a teoria de caracteres em grupos abelianos finitos e, como resultado principal, relacionaremos a quantidade de subgrupos cíclicos de um grupo abeliano finito com a quantidade de fatores cíclicos.

1.4.2 Caracteres em Grupos Abelianos Finitos

O objetivo desta subseção é apresentar um teorema sobre teoria de caracteres em grupos abelianos finitos que culmina mostrando que, dado um grupo abeliano finito G, existe uma bijeção entre seus subgrupos cíclicos e seus quocientes cíclicos que preserva ordem, pois usaremos este resultado no capítulo 2. Usaremos, para isso, o Capítulo 10 de [**9**].

Uma definição possível para o grupo de caracteres de um grupo abeliano finito é a seguinte:

Definição 1.4.10 *Seja G um grupo abeliano finito. Então o seu **grupo de caracteres** G^* é*

$$G^* = Hom(G, \mathbb{C}^\times),$$

e para quaisquer $f, h \in G^*$, definimos o produto $(fh)(g) = f(g)h(g)$, para todo $g \in G$. Desta forma, temos que G^* é um grupo.

Temos o seguinte resultado:

Teorema 1.4.11 *Se G é um grupo abeliano finito, então $G \simeq G^*$.*

Prova: ver Teorema 10.56 de [**9**]. □

Definição 1.4.12 *Seja G um grupo abeliano finito. Para cada $x \in G$ definimos o homomorfismo $E_x : G^* \to \mathbb{C}^\times$ por $E_x(\varphi) = \varphi(x)$; assim, $E_x \in G^{**}$, e definimos a função $E : G \to G^{**}$ por $x \mapsto E_x$.*

Teorema 1.4.13 *Se G é um grupo abeliano finito, então a função E definida acima é um isomorfismo.*

Prova: ver Teorema 10.59 de [**9**]. □

Seja S um subgrupo de G. Defina $S^\perp = \{f \in G^* : f(s) = 1, \text{para todo } s \in S\}$. Temos que $S^\perp$ é subgrupo de G^* e, a função $S^\perp \to (G/S)^*$ dada por $f \mapsto \widehat{f}$, onde $\widehat{f}(\bar{g}) = f(g)$ (está bem definida) é um isomorfismo, isto é, $S^\perp \simeq (G/S)^* \simeq G/S$. Temos o seguinte lema:

Lema 1.4.14 *A função $\psi(S) = S^\perp$ é uma bijeção entre subgrupos de G e de G^*.*

Prova: Como $G \simeq G^*$, então basta mostrar que esta função é injetora, isto é, que dados S, H subgrupos distintos de G, então $S^\perp \neq H^\perp$. Temos:

$$(S^\perp)^\perp = \{E_x \in G^{**} : E_x(f) = f(x) = 1, \text{ para todo } f \in S^\perp \} \simeq (G^*/S^\perp)^* \simeq G^*/S^\perp,$$

e, portanto, $S \subseteq (S^\perp)^\perp$ e, $|(S^\perp)^\perp| = |G|/|S^\perp| = |G|/(|G/S|) = |S|$ e, assim, temos que $(S^\perp)^\perp = S$ e segue o resultado desejado.

□

Como corolário, temos o seguinte resultado:

Corolário 1.4.15 *Seja G um grupo abeliano finito. Então existe uma bijeção ϕ entre os subgrupos de G e os quocientes de G, tal que $\phi(S) \simeq S$, para todo $S \leq G$. Em particular, a quantidade de subgrupos de G cíclicos de ordem n é igual à quantidade de quocientes de G cíclicos de ordem n, para todo n inteiro positivo.*

Prova: seja $S \leq G$ um subgrupo. Segue da demonstração do lema anterior e do parágrafo que o precede que $(S^{\perp})^{\perp} = S \simeq (G^*/S^{\perp})$. Pelo Teorema 1.11 temos o resultado.

□

E assim concluímos esta parte.

1.4.3 Códigos Cíclicos

Nesta subseção veremos algumas propriedades sobre códigos cíclicos, bem como sua relação com ideais em anéis de grupos e com certos quocientes de anéis de polinômios.

Definição 1.4.16 *Um* ***código linear*** *de comprimento* $\boldsymbol{n}$ *e dimensão* $\boldsymbol{k}$ *sobre o corpo* F_q *é um subespaço vetorial* C *de dimensão* $\boldsymbol{k}$ *do espaço* F_q^n*, onde* F_q *é o corpo de ordem* q*. Um código linear* C *é dito* ***cíclico*** *se, para todo* $(c_0, ..., c_{n-1}) \in C$ *temos* $(c_{n-1}, c_0, ..., c_{n-2}) \in C$*.*

Assim, definimos a aplicação $\sigma : C \to C$ definida por $\sigma(c_0, ..., c_{n-1}) = (c_{n-1}, c_0, ..., c_{n-2})$.

Existe um homomorfismo de anéis injetor $(c_0, ..., c_{n-1}) \mapsto c_0 + c_1x + ... + c_{n-1}x^{n-1} \in F_q[x]/(x^n - 1)$, e a imagem deste homomorfismo é um ideal I de $F_q[x]/(x^n - 1)$. Aplicar a função σ em C equivale a multiplicar por x em $F_q[x]/(x^n - 1)$.

Identificaremos um código cíclico C de comprimento n com o ideal I de $F_q[x]/(x^n - 1)$ correspondente.

Proposição 1.4.17 *Seja* C *um código cíclico de comprimento* n *e dimensão* $k > 0$ *sobre* F_q*. Então existe um único polinômio mônico* $g(x) \in F_q[x]$ *tal que, para todo polinômio* $c(x) \in F_q[x]$ *de grau menor que* n*, temos que* $c(x) \in C$ *se, e somente se* $g(x)|c(x)$*.*

Prova: ver Proposição 8.1 de [8]. □

Assim, temos que a imagem de $g(x)$ em $F_q[x]/(x^n - 1)$ está em C, e $g(x)$ é o polinômio não-nulo de menor grau que satisfaz isso. Mais ainda, temos que a imagem

de $g(x)$ em C gera C (olhando como ideal do quociente do anel de polinômios). Isso motiva a seguinte definição:

Definição 1.4.18 *O polinômio $g(x)$ conforme descrito na proposição anterior é chamado* ***polinômio gerador*** *do código C (e do ideal I).*

Notemos que podemos escrever

$$C = \{\overline{g(x)u(x)} : grau(u(x)) < n - grau(g(x)) - 1\},$$

portanto, temos que a cardinalidade de C é $q^{(n-grau(g(x)))} = q^k$ e, portanto, $grau(g(x)) = n - k$.

Também temos a seguinte proposição:

Proposição 1.4.19 *Se C é um código cíclico de tamanho n e $g(x)$ é seu polinômio gerador, então $g(x)|(x^n - 1)$.*

Prova: ver Proposição 8.2 de [**8**]. □

Então, podemos fazer a seguinte definição:

Definição 1.4.20 *Com o contexto dado acima, o polinômio $h(x) = (x^n - 1)/g(x)$ é chamado* ***polinômio de verificação de*** *C (este polinômio tem grau k).*

A partir de agora, vamos supor que $mdc(n, q) = 1$.

Desta forma, temos que o polinômio $x^n - 1 \in F_q[x]$ possui n raízes distintas em um corpo de decomposição e, portanto, temos que $mdc(h(x), g(x)) = 1$.

Também podemos identificar C com um ideal da álgebra de grupo comutativa F_qC_n, de forma análoga à que fizemos para o quociente no anel de polinômios, da seguinte forma: se $g \in C_n$ é gerador, então definimos $f : C \to F_qC_n$ por:

$$f(c_1, ..., c_n) = \sum_{i=1}^{n} c_i g^i.$$

Com a suposição acima, temos que F_qC_n é semisimples (pelo Teorema de Maschke). Pelos teoremas 1.4.6(ii) e 1.4.7, temos que existe um único idempotente $e \in C$

que gera C. Seja $e(x) \in F_q[x]$ um polinômio tal que $\overline{e(x)} \in F_q[x]/(x^n-1)$ corresponde a e.

Temos a seguinte proposição, que será usada para calcular o polinômio gerador no capítulo 2:

Proposição 1.4.21 *Com as notações acima, temos que* $g(x) = mdc(x^n - 1, e(x))$

Prova: seja $h(x)$ o polinômio de verificação de C. E sejam $r(x)s(x) \in F_q[x]$ tais que

$$r(x)g(x) + s(x)h(x) = 1.$$

Multiplicando os dois lados da equação acima por $r(x)g(x)$, temos:

$$(r(x)g(x))^2 + r(x)s(x)h(x)g(x) = r(x)g(x)$$

Como $h(x)g(x) = x^n - 1$, temos que

$$\overline{(r(x)g(x))^2} = \overline{r(x)g(x)},$$

ou seja, $r(x)g(x)$ é idempotente.

A primeira equação também dos diz que $mdc(r(x), h(x)) = 1$. Portanto, como $mdc(g(x), h(x)) = 1$, temos:

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

Além disso, temos que $r(x)g(x) = 1 - s(x)h(x)$ e, temos que

$$(r(x)g(x))g(x) = g(x) - s(x)h(x)g(x) = g(x) - s(x)(x^n - 1) \equiv g(x)(mod\ (x^n - 1)\ )$$

e, portanto, $\overline{r(x)g(x)} \in C$ gera $\overline{g(x)}$, que é gerador de C. Segue que $\overline{r(x)g(x)}$ é gerador de C.

Como $\overline{r(x)g(x)}$ é idempotente e gerador de C, então $r(x)g(x) \equiv e(x)(mod\ (x^n - 1)\ )$ e temos, portanto:

$$mdc(e(x), x^n - 1) = mdc(r(x)g(x), x^n - 1) = g(x),$$

como queríamos.

□

1.4.4 Grupos Nilpotentes

Definiremos e enunciaremos alguns resultados básicos acerca de grupos nilpotentes e séries centrais que serão usados no Capítulo 3, e daremos um exemplo de um tipo de grupos nilpotentes finitos. Para isso, comecemos definindo alguns conceitos básicos:

Definição 1.4.22 *Para $h, k \in G$, definimos seu comutador $[h, k] = hkh^{-1}k^{-1}$.*

Para subgrupos H, K de G, definimos $[H, K] = \langle [h, k] : h \in H, k \in K \rangle$.

Vamos definir os subgrupos $\gamma_i(G)$ de G por indução:

$$\gamma_1(G) = G;$$

$$\gamma_{i+1}(G) = [\gamma_i(G), G].$$

Por indução, temos que cada $\gamma_i(G)$ é normal em G e, além disso, $\gamma_{i+1}(G) \leq \gamma_i(G)$. Isto possibilita a seguinte definição:

Definição 1.4.23 *Chamaremos de **série central descendente** de G a série*

$$G = \gamma_1(G) \geq \gamma_2(G) \geq ...$$

Também há outra série de interesse.

Definição 1.4.24 *Os **centros de ordem superior**, que denotaremos por $Z_i(G)$, são subgrupos de G definidos indutivamente:*

$$Z_0(G) = 1;$$

$$Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G)),$$

isto é, se $\nu_i : G \to G/Z_i(G)$ é a projeção natural, então $Z_{i+1}(G)$ é a pré-imagem do centro.

Também dizemos que $Z_i(G)$ é o i-ésimo centro de G.

É claro que $Z_1(G) = Z(G)$.

E definimos a ***série central ascendente*** *de G:*

$$1 = Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq ....$$

Teorema 1.4.25 *Seja G um grupo, então existe um inteiro não-negativo c com $Z_c(G) = G$ se, e somente se, $\gamma_{c+1}(G) = 1$. Além disso, nesse caso, $\gamma_{i+1}(G) \leq Z_{c-i}(G)$, para todo i.*

Prova: ver Teorema 5.31 de [**9**]. □

Definição 1.4.26 *Um grupo G é dito* ***nilpotente*** *se existe inteiro c tal que $\gamma_{c+1}(G) = 1$ ou, equivalentemente, $Z_c = G$. O menor c que satisfaz isso é chamado* ***classe de nilpotência*** *de G.*

Temos, por exemplo, que um grupo é nilpotente de classe 1 se, e somente se ele for abeliano.

Os próximos teoremas lidam com subgrupos e quocientes de grupos nilpotentes.

Teorema 1.4.27 *Todo subgrupo H de um grupo nilpotente G é nilpotente. Mais ainda, se G é nilpotente de classe c, então H é nilpotente de classe no máximo c.*

Prova: ver Teorema 5.35 de [**9**]. □

Teorema 1.4.28 *Se G é um grupo nilpotente de classe c e $H \triangleleft G$, então G/H é nilpotente de classe no máximo c.*

Prova: ver Teorema 5.36 de [**9**]. □

O próximo teorema será muito útil no capítulo 3:

Teorema 1.4.29 *Seja G um grupo nilpotente. Se $\{1\} \neq H \triangleleft G$, então $H \cap Z(G) \neq \{1\}$.*

Prova: ver Teorema 5.41 de [**9**]. □

Teorema 1.4.30 *Todo p-grupo finito é nilpotente.*

Prova: ver Teorema 5.33 de [**9**]. □

Temos também a seguinte definição:

Definição 1.4.31 *Uma série*

$$G = G_1 \geq G_2 \geq ... \geq G_n = 1,$$

onde cada $G_i \triangleleft G$ *e* $G_i/G_{i+1} \leq Z(G/G_{i+1})$ *é chamada uma* ***série central****.*

Por 5.1.9 de [**7**], temos que, se G for nilpotente, as séries centrais ascendente e descendente são centrais e de mesmo tamanho e, além disso, se todos os subgrupos G_i de uma série central de um grupo nilpotente G são distintos, então $\gamma_{i+1}(G) \leq G_{i+1} \leq Z_{n-1-i}$, e portanto G é nilpotente de classe $n-1$.

Obs: para uma justificativa do parágrafo acima, veja 5.1.9 de [**7**].

Exemplo: Denotemos por $G = UT(n, F_q)$ (com $n \geq 2$) o grupo (multiplicativo) das matrizes $n \times n$ triangulares superiores tais que as entradas da diagonal principal são todas iguais a 1. Pelo teorema anterior, temos que $UT(n, F_q)$ é grupo nilpotente.

Defina T_n como sendo o grupo das matrizes triangulares superiores e N como sendo o ideal de $T_n(F_q)$ composto pelas matrizes que têm apenas entradas nulas na diagonal principal e abaixo dela. Temos que N^i é o ideal de $T_n(F_q)$ das matrizes cujas entradas da diagonal principal e das (i-1) diagonais logo acima desta são todas nulas.

Pela seção 5.1 de [**7**], temos que

$$1 = U_n \leq ... \leq U_1 = G$$

é uma série central, com $U_i = 1 + N^i = \{1 + x : x \in N^i\}$.

Temos, pelo que foi observado acima, que $U_{i+1} \leq Z_{n-1-i}$. É bem conhecido o fato de que esta inclusão é, na realidade uma igualdade, ou seja, que $U_{i+1} = Z_{n-1-i}$,

para todo i. Vamos verificar sucintamente este fato, para fins de completude:

Antes, observemos os dois seguintes fatos, que são imediatos:

- Se $A \in U_i$, $B \in U_j$, então $AB \in U_{i+j}$;
- Vale que $Z_1(G) = U_{n-1}$;

Além disso, seja $A \in G$. A pode ser escrito unicamente como uma soma $A = 1 + B + C$, onde $B, C \in N$ tais que $B \in N^i$ e todas as entradas da matriz C acima da $(i-1)$-ésima diagonal acima da diagonal principal são nulas. Assim, temos que $(1 + B) \in U_i$ e, portanto, $(1 + B)^{-1} = (1 + D) \in U_i$. Temos:

$$A(1 + B)^{-1} = ((1 + B) + C)(1 + B)^{-1} = 1 + C(1 + D) = 1 + C + CD,$$

e $CD \in N^{i+1}$. Portanto, temos por indução que *no quociente* G/U_i, $A = 1 + C$.

Portanto, no quociente acima, todo elemento tem um representante que tem apenas entradas nulas acima da $(i-1)$-ésima diagonal acima da diagonal principal (chamaremos matrizes desse tipo de matrizes do tipo i).

Assim, para terminar a prova do que queremos, basta notar que para uma matriz $A \notin U_i$ do tipo i sempre há uma matriz $B \notin U_i$ do tipo i tal que AB e BA são distintos em alguma entrada abaixo da i-ésima diagonal acima da diagonal principal, e usar indução (onde o passo inicial é o segundo fato acima).

Portanto, temos que $UT(n, F_q)$ é um grupo nilpotente de classe $(n-1)$. Em particular, temos que para todo inteiro positivo m, sempre há um grupo nilpotente de classe m.

Para o exemplo acima ficar mais claro, vamos ver um caso mais concreto: tomemos $G = UT(4, F_q)$. Então temos:

$$G = \left\{ \begin{bmatrix} 1 & a_{12} & a_{13} & a_{14} \\ 0 & 1 & a_{23} & a_{24} \\ 0 & 0 & 1 & a_{34} \\ 0 & 0 & 0 & 1 \end{bmatrix} : a_{ij} \in F_q \right\} = Z_3(G)$$

$$Z_2(G) = \left\{ \begin{bmatrix} 1 & 0 & a_{13} & a_{14} \\ 0 & 1 & 0 & a_{24} \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} : a_{ij} \in F_q \right\}$$

$$Z_1(G) = \left\{ \begin{bmatrix} 1 & 0 & 0 & a_{14} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} : a_{14} \in F_q \right\}$$

E temos uma descrição completa da série central ascendente de G.

Capítulo 2

Idempotentes e códigos abelianos minimais

Neste capítulo, vamos calcular a quantidade de componentes simples de certas álgebras de grupos abelianos finitos sobre corpos finitos. Todas estas álgebras que estudamos são semisimples.

Vamos também calcular idempotentes geradores de códigos abelianos minimais de algumas álgebras, ou seja, seus idempotentes (centrais) primitivos. Também vamos calcular a dimensão e o peso desses códigos.

Todo o capítulo será baseado, principalmente, no trabalho que foi feito por Ferraz, R. e Polcino Milies, C. [**4**].

2.1 Considerações Iniciais

Conforme vimos em **1.1.3**, se $F = F_q$ é o corpo com q elementos, então os códigos cíclicos de comprimento m sobre F podem ser vistos como ideais em $F[X]/(X^m - 1)$ ou em FC_m, onde C_m é o grupo cíclico de ordem m.

Definição 2.1.1 *Um* ***código abeliano*** *sobre o corpo F é um ideal I na álgebra de grupo FA, onde A é um grupo abeliano finito. Um* ***código abeliano minimal*** *é um ideal I que é minimal.*

Como vimos na seção **1.1**, se $carF \nmid |A|$, então FA é semisimples e, portanto, todo ideal minimal é um componente simples $B_i = FAe_i$ de FA, onde e_i é um

idempotente central primitivo de FA.

2.2 Quantidade de Componentes Simples

Seja F um corpo finito, com q elementos, e seja A um grupo abeliano finito tal que $mdc(q, |A|) = 1$. Como vimos, FA é semisimples e, se $\{e_1, ..., e_r\}$ é o conjunto de idempotentes centrais primitivos de FA, temos:

$$FA = \oplus_{i=1}^{r}(FA)e_i \simeq \oplus_{i=1}^{r}F_i,$$

onde $F_i \simeq (FA)e_i, 1 \leq i \leq r$, são extensões finitas de F.

Defina:

$$\mathcal{A} = \oplus_{i=1}^{r}Fe_i.$$

Note que $Fe_i \simeq F$ como corpos, sob o isomorfismo $ae_i \mapsto a$ $(a \in F)$, e o número r, que representa a quantidade de componentes simples de FA, também representa a dimensão de $\mathcal{A}$ sobre F.

O próximo lema traz uma identificação de quais são os elementos de $FA = \oplus_{i=1}^{r}(FA)e_i$ que estão em $\mathcal{A}$:

Lema 2.2.1 *Seja $\alpha \in FA$. Então $\alpha \in \mathcal{A}$ se, e somente se $\alpha^q = \alpha$.*

Prova: Dado $\alpha \in FA$, podemos escrever $\alpha = \sum_{i=1}^{r}\alpha_i$, onde $\alpha_i = \alpha e_i \in FAe_i \simeq F_i, 1 \leq i \leq r$. Agora, α é um elemento de $\mathcal{A}$ se, e somente se cada α_i está em Fe_i, para cada índice i. Como $Fe_i \simeq F$ e FAe_i é uma extensão de Fe_i, isto acontece se, e somente se $\alpha_i^q = \alpha_i$ para todo i; isto é, se, e somente se $\alpha^q = \alpha$.

□

Definição 2.2.2 *Seja g um elemento do grupo abeliano A. A* ***classe q-ciclotômica de*** *g é o conjunto*

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

onde t_g é o menor inteiro positivo tal que

$$q^{t_g} \equiv 1(mod\ o(g)),$$

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

Se $(q, o(g)) = 1$, sempre haverá um tal t_g (pois $\overline{g} \in Z^*_{o(q)}$ e, portanto, $\overline{g}^{\phi(o(g))} = \overline{1}$, e se $a \in S_g$, então $a^{q^i} \in S_g$, para todo i.

Se $S_g \cap S_h \neq \emptyset$, então existe $a \in S_g \cap S_h$. Podemos escrever $a = g^{q^j} = h^{q^i}$. Temos $a^{q^{t_g - j}} = g \in S_h$ e, similarmente, $h \in S_g$. Logo, $S_g = S_h$.

Temos, portanto, que se $S_g \neq S_h$, então $S_g \cap S_h = \emptyset$. Seja $T = \{g_1, ..., g_s\}$ um conjunto de representantes das classes q-ciclotômicas dos elementos de A (há s q-classes ciclotômicas em A).

Teorema 2.2.3 *Seja F um corpo finito de ordem q, e seja A um grupo abeliano finito tal que $(q, |A|) = 1$. Então, a quantidade de componentes simples de FA é igual ao número de classes q-ciclotômicas de A.*

Prova: conforme observamos acima, o número de componentes simples de FA é igual à dimensão de $\mathcal{A}$ sobre F. Para provarmos o teorema, vamos exibir uma base de $\mathcal{A}$ com s elementos.

Dada uma classe q-ciclotômica S_g, definimos $\eta_g = \sum_{h \in S_g} h \in FA$. Vamos provar que $\mathcal{B} = \{\eta_{g_i} : 1 \leq i \leq s\}$ é uma base de $\mathcal{A}$ sobre F:

Como $S_g \cap S_h = \emptyset$ se $g \neq h$, então temos que $\mathcal{B}$ é conjunto linearmente independente. Para mostrar que o dado conjunto gera $\mathcal{A}$ sobre F, observemos que, como FA é um anel de característica q, então $\eta^q_{g_i} = \eta_{g_i}, 1 \leq i \leq s$, e portanto, pelo lema anterior, temos que $\mathcal{B} \subset \mathcal{A}$.

Seja $\alpha \in \mathcal{A} = \oplus_{i=1}^r Fe_i$. Usando novamente o lema anterior, temos que $\alpha = \alpha^q$. Assim, se $\alpha = \sum_{g \in A} \alpha_g g$, nós temos:

$$\alpha = \sum_{g \in A} \alpha_g g = \Big(\sum_{g \in A} \alpha_g g \Big)^q = \sum_{g \in A} \alpha^q_g g^q.$$

Como $\alpha_g \in F$, então $\alpha_g^q = \alpha_g$ e temos:

$$\sum_{g \in A} \alpha_g g = \sum_{g \in A} \alpha_g g^q.$$

Como $g^q = h^q$ implica $S_g = S_h$, e a função $g \mapsto g^q$ é bijetora em S_g, temos que esta mesma função é bijetora em A.

Assim, para cada $g \in A$, temos que $\alpha_g = \alpha_{g^q} = ... = \alpha_{g^{q^{t_g-1}}}$ e, portanto, em α cada coeficiente de um elemento de S_g é α_g, e temos:

$$\alpha = \sum_{g \in T} \alpha_g \eta_g,$$

e concluímos que $\mathcal{B}$ gera $\mathcal{A}$ como F - espaço vetorial, como queríamos.

□

Como enunciamos no Teorema 1.4.9, o número de componentes simples da álgebra de grupo racional de um grupo abeliano finito A é igual à quantidade de subgrupos cíclicos de A (e, como vimos em 1.4.2, também é igual ao número de fatores cíclicos).

Note que, se $h \in S_g$, então $h = g^{q^j}$ para algum j. Como $(q, o(g)) = 1$, então $(q^j, o(g)) = 1$, o que implica $\langle g \rangle = \langle h \rangle$. Assim, cada q-classe ciclotômica S_g é um subconjunto do conjunto $\mathcal{G}_g$ de todos os geradores do grupo cíclico gerado por g. Então, é claro que o número de subgrupos cíclicos de A é um limitante inferior para o número de componentes simples de FA, e este limitante é atingido se, e somente se $S_g = \mathcal{G}_g$, para todo $g \in A$.

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

$$\mathcal{G}_g = \{g^r : (r, o(g)) = 1\} = \{g^r : \overline{r} \in U(\mathbb{Z}_{o(g)})\}.$$

Antes de enunciar o próximo teorema, vamos ao seguinte lema, que será bem útil:

Lema 2.2.4 *Sejam $a, b, q \in \mathbb{Z}$, $a|b$, $mdc(q, b) = 1$ (e portanto $mdc(q, a) = 1$),*

e suponha que a imagem de q em $U(\mathbb{Z}_b)$ é um gerador (multiplicativo). Então a imagem de q em $U(\mathbb{Z}_a)$ também é gerador (multiplicativo).

Prova: Seja $x \in \mathbb{Z}$, denotemos por x_a a imagem de x em $\mathbb{Z}_a$, e por x_b a imagem de x em $\mathbb{Z}_b$, e suponha que $x_a \in U(\mathbb{Z}_a)$.

Seja $p_1^{r_1}...p_n^{r_n} = mdc(x,b)$ decomposição em fatores primos do m.d.c entre x e b (onde os p_i's são primos distintos), e sejam $m_1, ..., m_n$ os maiores inteiros tais que $p_i^{m_i}|b$. Vamos provar que $mdc\left(x + \frac{ab}{p_1^{m_1}...p_n^{m_n}}, b\right) = 1$.

Suponha que p é um número primo que divide este m.d.c.. Temos dois casos:

Primeiro caso: se $p|x$, temos que, como $p|b$, então $p = p_i$, para algum i, e $p|\frac{ab}{p_1^{m_1}...p_n^{m_n}}$. Daí, como $p \nmid \frac{b}{p_1^{m_1}...p_n^{m_n}}$, temos que $p|a$. Mas isto contradiz o fato de que a e x são primos entre si.

Segundo caso: se $p \nmid x$, então $p \neq p_i$, para todo i. Como $p|b$, temos que $p|\frac{b}{p_1^{m_1}...p_n^{m_n}}$, $\frac{b}{p_1^{m_1}...p_n^{m_n}}|\frac{ab}{p_1^{m_1}...p_n^{m_n}}$, e $p|\left(x + \frac{ab}{p_1^{m_1}...p_n^{m_n}}\right)$. Portanto temos que $p|x$, uma contradição.

Assim, por hipótese, temos que existe $m \in \mathbb{Z}$ tal que $q^m \equiv x + \frac{ab}{p_1^{m_1}...p_n^{m_n}} (mod\ b)$. Como $a|b$, temos $q^m \equiv x + \frac{ab}{p_1^{m_1}...p_n^{m_n}} \equiv x (mod\ a)$. Como x foi pego arbitrariamente dentre os relativamente primos com a, temos que q gera o grupo $U(\mathbb{Z}_a)$.

□

Usaremos este lema para provar o seguinte teorema:

Teorema 2.2.5 *Seja F um corpo finito com q elementos, e seja A um grupo abeliano finito, de expoente e, tal que $(q, |A|) = 1$. Então $S_g = \mathcal{G}_g$, para todo $g \in A$ se, e somente se $U(\mathbb{Z}_e)$ é um grupo cíclico gerado por $\overline{q} \in \mathbb{Z}_e$.*

Prova: Suponha primeiro que $U(\mathbb{Z}_e)$ é cíclico gerado por $\overline{q}$. Para $g \in A$, temos que $o(g)|e$ e, pelo lema anterior, $(\overline{q}) \in \mathbb{Z}_{o(g)}$ é um gerador de $U(\mathbb{Z}_{o(g)})$.

Para todo elemento $h \in \mathcal{G}_g$ temos que $h = g^r$, para algum inteiro positivo r tal que $\overline{r} \in U(\mathbb{Z}_{o(g)})$, então $\overline{r} = \overline{q}^j$, para algum inteiro positivo j e $h = g^{q^j} \in S_g$. Isso mostra que $\mathcal{G}_g \subset S_g$. Como a inclusão oposta sempre vale, conforme observado anteriormente, então temos igualdade.

Por outro lado, suponha que $\mathcal{G}_g = S_g$, para todo $g \in A$. Como A é abeliano de expoente e, então existe $g_0 \in A$ tal que $o(g_0) = e$ e, em particular, $\mathcal{G}_{g_0} = S_{g_0}$ (este último por hipótese). Então, para cada inteiro r tal que $\overline{r} \in U(\mathbb{Z}_e)$, temos que $g_0^r \in S_{g_0}$, e portanto existe um inteiro j tal que $\overline{r} = \overline{q}^j$. Isso mostra que $\overline{q}$ gera $U(\mathbb{Z}_e)$, como queríamos.

□

É bem conhecido o fato de que $U(\mathbb{Z}_e)$ é cíclico se, e somente se, $e = 2, 4, p^n$ ou $2p^n$, onde p é um número primo ímpar, e n é um inteiro positivo (ver, por exemplo, Teorema 2.41 de [**3**]).

Além disso, se q é ímpar, então q gera $U(\mathbb{Z}_2)$; se $q \equiv 3(mod 4)$ então q gera $U(\mathbb{Z}_4)$; e q gera $U(\mathbb{Z}_e)$, com $e = p^n$ ou $e = 2p^n$ se, e somente se $o(q) = \phi(p^n)$ em $U(\mathbb{Z}_e)$.

Temos, portanto, o seguinte corolário:

Corolário 2.2.6 *Seja F um corpo finito com q elementos, e seja A um grupo abeliano finito, de expoente e. Então $\mathcal{G}_g = S_g$ para todo $g \in A$ se, e somente se vale um dos seguintes:*

(i) $e = 2$ e q é ímpar;
(ii) $e = 4$ e $q \equiv 3(mod 4)$
(iii) $e = p^n$, onde p é um primo ímpar e $o(q) = \phi(p^n)$ em $U(\mathbb{Z}_e)$;
(iv) $e = 2p^n$, onde p é um primo ímpar e $o(q) = \phi(p^n)$ em $U(\mathbb{Z}_e)$;

□

2.3 Códigos Cíclicos Minimais

O objetivo desta subseção é calcular os idempotentes primitivos de álgebras de grupos cíclicos do tipo listado no corolário anterior.

Seja H um subgrupo de um grupo G. Se $(q, |H|) = 1$, definimos

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

.

Temos que $\widehat{H}$ está bem definido e é idempotente em FG (lema 3.6.6 de [**5**]).

Lema 2.3.1 *Seja F um corpo finito com q elementos, e seja p um número primo e $A = \langle a \rangle$ um grupo cíclico de ordem p^n, $n \geq 1$. Seja*

$$A = A_0 \supset A_1 \supset ... \supset A_n = 1$$

a cadeia decrescente de todos os subgrupos de A $\left(A_i = \left\langle a^{p^i} \right\rangle\right)$. Então os elementos

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

forma um conjunto de idempotentes ortogonais de FA tais que $e_0 + e_1 + ... + e_n = 1$.

A prova a seguir é encontrada no Lema VII.1.2 de [**1**] e, logo em seguida, é feita uma observação de que, no caso de F ser finito, estes idempotentes podem não ser primitivos:

Prova: Como $e_0\widehat{A_i} = \widehat{A_i}$, para todo i, então nós temos $e_0 e_i = 0$, para todo $i > 0$. Além disso, se $1 \leq i \leq j$, $\widehat{A_i}\widehat{A_j} = A_i$, então

$$e_i e_j = (\widehat{A_i} - \widehat{A_{i-1}})(\widehat{A_j} - \widehat{A_{j-1}}) =$$

$$= \widehat{A_i} - \widehat{A_i}\widehat{A_{j-1}} - \widehat{A_{i-1}} + \widehat{A_{i-1}} = \widehat{A_i} - \widehat{A_i}\widehat{A_{j-1}}$$

que é 0 se $i < j$ e e_i se $i = j$. Segue que $e_0, ..., e_m$ são $(n+1)$ idempotentes (centrais) dois a dois ortogonais. Além disso, observamos que a soma dos elementos é telescópica, e portanto a soma $\sum_{i=0}^{j} e_i = \widehat{A_j}$, o que imlplica que a soma de todos esses idempotentes é 1, como queríamos.

□

Se $F = \mathbb{Q}$, então temos que esses elementos são os idempotentes primitivos de FA (pelo Teorema 1.4.9, no Capítulo 1, aliado ao fato de que cada e_i é a soma de idempotentes primitivos de FA, pelo Teorema de Wedderburn - Artin).

Como esses são $(n+1)$ (o número de subgrupos [cíclicos] de A) idempotentes, temos que serão primitivos sempre que FA tiver exatamente $(n+1)$ componentes

simples. Como o expoente de A neste caso é p^n, então pelo visto na seção anterior, isso acontece se, e somente se q e p^n são da forma descrita no último corolário da seção anterior.

Portanto, temos o seguinte:

Corolário 2.3.2 *Seja F um corpo finito com q elementos, e seja A um grupo cíclico de ordem p^n. Então, o conjunto de idempotentes descrito no lema anterior é o conjunto de idempotentes primitivos de A se, e somente se um dos seguintes vale:*

(i) $p = 2$, e ou $n = 1$ e q é ímpar ou $n = 2$ e $q \equiv 3(mod 4)$;
(ii) p é um primo ímpar e $o(q) = \phi(p^n)$ em $U(\mathbb{Z}_{p^n})$

□

O corolário acima é uma generalização do seguinte teorema de Arora e Pruthi (Teorema 3.5 de [**6**]):

Teorema 2.3.3 *Seja F um corpo finito com q elementos e A um grupo cíclico com p^n elementos, onde p é um primo ímpar tal que $o(q) = \phi(p^n)$ em $U(\mathbb{Z}_{p^n})$. Seja*

$$A = A_0 \supset A_1 \supset ... \supset A_n = 1$$

a cadeia decrescente de todos os subgrupos de A.

Então o conjunto de idempotentes primitivos de FA é dado por:

$$e_0 = \frac{1}{p^n}\Big(\sum_{a \in A} a\Big);$$

$$e_i = \widehat{A_i} - \widehat{A_{i-1}}, 1 \leq i \leq n.$$

□

Claramente, estes idempotentes determinam o conjunto dos ideais minimais em FA e, portanto, os códigos cíclicos minimais de comprimento p^n sobre F.

A partir disso, podemos calcular os idempotentes geradores de ideais minimais no caso de grupos cíclicos de ordem $2p^n$:

Teorema 2.3.4 *Seja F um corpo finito com q elementos e G um grupo cíclico de ordem $2p^n$, com p primo ímpar, tal que $o(q) = \phi(p^n)$ em $U(\mathbb{Z}_{2p^n})$. Escrevendo $G = C \times A$, onde A é o subgrupo p-Sylow de G e $C = \{1, t\}$ é o seu 2-Sylow. Se $e_i, 0 \leq i \leq n$, denotam os primitivos idempotentes de FA então, os idempotentes primitivos de FG são*

$$\frac{1+t}{2}e_i,\ 0 \leq i \leq n;$$

$$\frac{1-t}{2}e_i,\ 0 \leq i \leq n.$$

Prova: Temos que, como $o(q)$ está em $U(\mathbb{Z}_{2p^n})$, então q é ímpar. Sendo assim, aplicando o teorema anterior, temos que os idempotentes primitivos de FC são $(1+t)/2$ e $(1-t)/2$. Assim:

$$FG \simeq F(C \times A) = (FC)A = (F\frac{1+t}{2} \oplus F\frac{1-t}{2})A \simeq (F \oplus F)A.$$

Como os idempotentes primitivos de FC correspondem a $(1,0)$ e $(0,1)$ em $(F \oplus F)$ e os idempotentes primitivos de FA são os do teorema anterior, o resultado segue imediatamente.

□

Depois que nós calcularmos a dimensão dos ideais minimais $I_i = (FA)(\widehat{A_i} - \widehat{A_{i-1}})$ e, portanto, o grau do seu polinômio gerador, calcular o polinômio gerador de I_i.

2.4 Códigos Abelianos Minimais

Queremos estender os resultados da seção anterior para grupos abelianos finitos. Para isso, consideremos primeiro o caso dos p-grupos abelianos finitos.

Seja A um p-grupo abeliano finito. Para cada subgrupo H de A tal que $A/H \neq 1$ é cíclico, vamos construir um idempotente de FA.

Observemos que, como A/H é um grupo cíclico cuja ordem é uma potência de p, então existe apenas um subgrupo H^* de A contendo H, tal que $|H^*/H| = p$. Vamos definir $e_H = \widehat{H} - \widehat{H^*} \neq 0$. Temos os seguintes lemas:

Lema 2.4.1 *Seja R um anel e seja H um subgrupo normal de um grupo G. Se $|H|$ é invertível em R, então*

$$(RG)\widehat{H} \simeq R(G/H).$$

Prova: ver Proposição 3.6.7 de [5].

□

Lema 2.4.2 *Seja G um grupo finito e, sejam H, K subgrupos de G. Então*

$$\widehat{H}\widehat{K} = \widehat{HK}.$$

Em particular, se $H \leq K$, então $\widehat{H}\widehat{K} = \widehat{K}$.

Prova: Primeiro, notemos que $h_1k_1 = h_2k_2$ implica que $h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K$, e além disso, $k_2k_1^{-1} = kk_1^{-1}$ se, e somente se $k_2 = k$ e, portanto, concluímos que

$$|\{(h,k) : hk = \alpha, h \in H, k \in K\}| = |H \cap K|,$$

para todo $\alpha \in HK$.

Temos que, se $h_1, ..., h_n$, e $k_1, ..., k_m$ são as listas de todos os elementos de H e K, respectivamente, então:

$$\widehat{H}\widehat{K} = \left(\frac{1}{n}(h_1 + ... + h_n)\right)\left(\frac{1}{m}(k_1 + ... + k_m)\right) = \frac{1}{|H||K|}\sum_{h\in H, k\in K} hk =$$

$$= \frac{|H \cap K|}{|H||K|}\sum_{\alpha\in HK} \alpha = \widehat{HK},$$

como queríamos provar.

□

Lema 2.4.3 *Os elementos e_H definidos acima, junto com $e_A = \widehat{A}$, formam um conjunto de idempotentes de FA dois a dois ortogonais, cuja soma é 1.*

Prova: o fato de que estes elementos são idempotentes segue diretamente do lema anterior.

Sejam agora $H, K \leq A$ tais que $A/H, A/K$ são cíclicos e não triviais, e sejam H^*, K^* subgrupos de A contendo H e K, respectivamente, tais que $H^*/H, K^*/K$ são cíclicos de ordem p. Vamos considerar primeiro o caso em que $H \subset K$ (propriamente). Neste caso, $H^* \subseteq K$ e temos:

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

Agora, se nenhum desses dois subgrupos está contido no outro, então ambos H e K estão contidos propriamente em HK, e temos que H^* e K^* estão contidos em HK. Assim, $H^*K^* \subset HK$, e claro que $HK \subset H^*K^*$ (pois $H \subset H^*, K \subset K^*$). Então $H^*K^* = HK$. Agora, como $HK \subset HK^* \subset H^*K^*$, segue que $HK^* = HK$ e, analogamente, nós temos $H^*K = HK$. Portanto

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

Falta só provar que a soma de todos esses idempotentes é 1. Para cada subgrupo cíclico C de A, denotemos por $\mathcal{G}(C)$ o conjunto dos elementos de C que geram este subgrupo; isto é:

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

Se $\mathcal{C}$ denota a família de todos os subgrupos cíclicos de A, então $|A| = \sum_{C \in \mathcal{C}} |\mathcal{G}(C)|$ e, como A é um p-grupo (e também C), então $|\mathcal{G}(C)| = \phi(|C|) = |C| - |C|/p$.

Seja $\mathcal{S}$ o conjunto de todos os subgrupos H de A tais que o quociente A/H é cíclico e seja $e = \sum_{H \in \mathcal{S}} e_H$.

Afirmação: $e = 1$.

Para provar tal afirmação, é suficiente provar que $(FA)e = FA$, visto que e é a soma de idempotentes dois a dois ortogonais. E devido a estes idempotentes serem dois a dois ortogonais, temos que

$$(FA)e = \bigoplus_{H \in \mathcal{S}} (FA)e_H,$$

daí, temos

$$dim_F\big((FA)_e\big) = \sum_{H\in\mathcal{S}} dim_F\big((FA)_{e_H}\big).$$

Note que $\widehat{H} = \widehat{H^*} + e_H$, e que $H^*e_H = 0$ (ou seja, H^* e e_H são idempotentes e ortogonais entre si), então temos

$$(FA)\widehat{H} = (FA)\widehat{H^*} \oplus (FA)e_H.$$

E ainda

$$dim_F\big((FA)e_H\big) = dim_F(FA)\widehat{H} - dim_F(FA)\widehat{H^*}.$$

Segue da equação acima e do Lema 2.12 que

$$dim_F\big((FA)e_H\big) = dim_F F[A/H] - dim_F F[A/H^*]. \tag{2.1}$$

Temos claramente que:

$$dim_F F[A/H] = |A/H|,$$

$$dim_F F[A/H^*] = |A/H^*|.$$

Segundo vimos em 1.4.2, existe uma bijeção $\Phi : \mathcal{C} \to \mathcal{S}$ tal que, se denotarmos por $C \in \mathcal{C}$ o subgrupo tal que $\Phi(C) = H$, temos $|C| = |A/H|$. Portanto, temos

$$dim_F F[A/H] = |C|,$$

$$dim_F F[A/H^*] = |A/H^*| = |A/H|/|H^*/H| = |C|/p,$$

então, pelo teorema acima

$$dim_F\big((FA)e_H\big) = |C| - |C|/p = |\mathcal{G}(C)|,$$

e portanto

$$dim_F\big((FA)e\big) = \sum_{H\in\mathcal{S}} dim_F\big((FA)e_H\big) = \sum_{C\in\mathcal{C}} |\mathcal{G}(C)| = |A|,$$

e portanto $e = 1$, como queríamos.

□

O seguinte resultado está contido na demonstração acima:

Corolário 2.4.4 *Nas condições do lema anterior, temos que*

$$dim_F\big((FA)e_H\big) = dim_F F[A/H] - dim_F F[A/H^*].$$

O seguinte resultado é uma consequência direta do lema que acabamos de provar e do Corolário 2.2.6.

Teorema 2.4.5 *Seja p um primo e seja A um p-grupo abeliano finito de expoente p^r.*
Então, o conjunto de idempotentes acima é o conjunto de idempotentes primitivos de FA se, e somente se, um dos seguintes vale:

(i) $p^r = 2$, e q é ímpar;

(ii) $p^r = 4$ e $q \equiv 3 (mod\, 4)$;

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

Prova: se o tal conjunto de idempotentes for de idempotentes primitivos, como sua soma é 1, então estes são todos os idempotentes primitivos, e as hipóteses do Corolário 2.2.6 estarão satisfeitas. Por outro lado, se um dos três itens acima for satisfeito, então o conjunto de idempotentes acima é o conjunto de idempotentes primitivos de FA, pelo Corolário 2.2.6.

□

Também, temos o seguinte:

Teorema 2.4.6 *Seja p um primo ímpar e seja A um grupo abeliano de expoente $2p^r$, e seja F um corpo finito com q elementos, onde $o(q) = \phi(2p^r)$ em $U(\mathbb{Z}_{2p^r})$ (em particular, temos que q é ímpar). Escrevamos $A = E \times B$, onde E é um 2-grupo abeliano elementar e B é um p-grupo. Então os idempotentes primitivos de FA são todos os produtos da forma $e.f$, onde e é um idempotente primitivo de FE e f é um idempotente primitivo de FB.*

Prova: escrevendo $E = \langle a_1 \rangle \times ... \times \langle a_n \rangle$, um produto de grupos cíclicos, temos que

$$FA \simeq F(E \times B) \simeq (FE)B,$$

e

$$(FE) \simeq F(\langle a_1 \rangle \times ... \times \langle a_n \rangle) \simeq (F\langle a_1 \rangle)(\langle a_2 \rangle \times ... \times \langle a_n \rangle) \simeq (F \oplus F)(\langle a_2 \rangle \times ... \times \langle a_n \rangle).$$

Continuando indutivamente o processo acima, temos que $FE \simeq F^{2^n}$, e imediatamente temos o desejado.

□

Temos ainda que, com as hipóteses do teorema acima, os idempotentes primitivos de FB são dados no teorema anterior.

Escrevendo $E = \langle a_1 \rangle \times ... \times \langle a_n \rangle$, um produto de grupos cíclicos, então os idempotentes primitivos de FE são todos os produtos do tipo $e = e_1...e_n$, onde

$$e_i = \frac{1 + a_i}{2}, \text{ou}$$

$$e_i = \frac{1 - a_i}{2}, 1 \leq i \leq n,$$

pois temos, pela demonstração do teorema acima, que $FE \simeq F^{2^n}$ e, portanto, FE tem exatamente 2^n idempotentes primitivos, e estes elementos descritos acima são 2^n idempotentes todos ortogonais entre si e somam 1 e, portanto, são os idempotentes primitivos de FE.

Sendo assim, temos uma descrição completa dos idempotentes primitivos de FA, nas hipóteses do teorema anterior.

Vale notar que, pelo Corolário 2.2.6, já temos os únicos casos em que os idempotentes primitivos de álgebras de grupos abelianos finitos sobre corpos finitos podem ser calculados desta forma.

2.5 Dimensão e Distância Mínima

Nesta seção, calcularemos a dimensão de certos códigos abelianos minimais sobre F e a distância mínima dos mesmos. Para isso precisaremos das seguintes definições:

Definição 2.5.1 *Dado um ideal I de FG, onde G é um grupo finito, sejam $a = \sum_{g\in G} a_g g$, $b = \sum_{g\in G} b_g g$ elementos de G. Então definimos a* ***distância*** *entre a e b como sendo*

$$d(a,b) = |\{g \in G : a_g \neq b_g, g \in G\}|$$

Definimos a ***distância mínima*** *do ideal I como sendo*

$$l(I) = min\{d(a,b) : a,b \in I,\ a \neq b\}$$

Definimos o ***peso*** *de um elemento $a \in FG$ como sendo*

$$w(a) = |\{g \in G : a_g \neq 0\}|,$$

note que $w(a) = d(a,0)$.

E definimos o ***peso*** *de um ideal I de FG como sendo*

$$w(I) = min\{w(a) : a \in I, a \neq 0\}$$

Obs.: temos que $d(a,b) = w(a-b)$. Se $w(I) = c$, então existe $0 \neq a \in I$ tal que $w(a) = c = d(a,0)$. Logo $c \in \{d(a,b) : a \neq b\}$ e, portanto, $l(I) \leq w(I)$. E como $d(a,b) = w(a-b)$, para todos $a,b \in FG$, temos $w(I) \leq l(I)$. Então $w(I) = l(I)$, para todo ideal I de FG.

Suponha que $|A| = 2^m p^n$, onde p é um primo ímpar e $m \geq 0$. Como fizemos antes, escrevamos $A = E \times B$, onde E é um 2-grupo abeliano elementar (eventualmente trivial) e B um p-grupo.

Como foi notado no fim da seção anterior, os idempotentes primitivos de FE são todos os produtos da forma $e_E = e_1 ... e_m$, onde

$$e_i = \frac{1+a_i}{2},\ \text{ou}\ e_i = \frac{1-a_i}{2}, 1 \leq i \leq m,$$

e os idempotentes primitivos de FA são todos os produtos da forma $e_E e_B$, onde e_E é um idempotente primitivo de FE e e_B é um idempotente primitivo de FB.

Para um idempotente primitivo e_E de FE fixo e um elemento $y \in E$, podemos escrever $y = a_1^{\epsilon_1}...a_m^{\epsilon_m}$, onde $\epsilon_i = 0$ ou 1. Temos

$$ye_E = a_1^{\epsilon_1}\Big(\frac{1 \pm a_1}{2}\Big)...a_m^{\epsilon_m}\Big(\frac{1 \pm a_m}{2}\Big) = \pm e_E = (-1)^{\epsilon_y} e_E, \tag{2.2}$$

onde $\epsilon_y = 0$ ou 1.

Considere primeiro os idempotentes da forma $e_E\widehat{B}$. Um elemento de $(FA).e_e\widehat{B}$ é da forma $\gamma.e_E\widehat{B}$, tal que γ pode ser escrito $\gamma = \sum_{y\in E, b\in B} x_{yb}yb$, onde cada x_{yb} é um elemento do corpo F; e então nós temos que

$$\gamma.e_E\widehat{B} = \sum_{y\in E, b\in B} x_{yb}ye_E.b\widehat{B} \overset{(2.2)}{=} \Big(\sum_{y\in E, b\in B} x_{yb}(-1)^{\epsilon_y}\Big)e_E\widehat{B}.$$

Como $\Big(\sum_{y\in E, b\in B} x_{yb}(-1)^{\epsilon_y}\Big) \in F$, temos que a dimensão do ideal $I = (FA).e_E\widehat{B}$ é 1, e que seu peso é $w(I) = |A|$ (pois $supp(e_E\widehat{B}) = A$, e para cada elemento do ideal, todos os coeficientes são iguais).

Agora, consideremos os idempotentes do tipo $e = e_E e_H$, com $e_E \in FE$, como acima, e $e_H = \widehat{H} - \widehat{H^*}$, onde H é um subgrupo de B tal que B/H é cíclico de ordem, digamos, p^i, e H^* é o único subgrupo de B que contém H tal que $[H^*/H] = p$. Seja $I_e = (FA)e$.

Seja $b \in B$ um elemento tal que $B = \langle b, H\rangle$ (tome b um representante da co-classe do gerador do grupo cíclico B/H). Assim, temos também que $H^* = \Big\langle b^{p^{i-1}}, H\Big\rangle$.

Como $b^{p^{i-1}} \in H^*$, temos que $(1 - b^{p^{i-1}})\widehat{H^*} = 0$.

Então segue que

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

Como $b^{p^{i-1}} \notin H$, então $supp((1 - b^{p^{i-1}})\widehat{H})$ é a união disjunta $H \cup b^{p^{i-1}}H$, e o peso do elemento acima é $w((1-b^{p^{i-1}})e_E\widehat{H}) = 2|E||H|$, de tal forma que a distância

mínima do ideal I_e é $l(I_e) \leq 2^{m+1}|H|$.

Como B é igual à união disjunta $B = H \cup bH \cup ... \cup b^{p^i-1}H$, então nós temos que $A = E \times B$ é a união disjunta $A = E \times H \cup ... \cup b^{p^i-1}(E \times H)$, de tal forma que um elemento arbitrário de FA pode ser escrito na forma $\alpha = \sum_{j=0}^{p^i-1} \alpha_j b^j$, com $\alpha_j \in F[E \times H]$.

Pela fórmula (2.2), e utilizando o fato de que, se $h \in H$, vale que $h\widehat{H} = \widehat{H}$, temos que cada produto $\alpha_j e_E e_H$ é da forma $\alpha j e_E e_H = k_j e_E e_H$, onde $k_j \in F, 0 \leq j \leq p^i - 1$ (O mesmo vale pondo $\widehat{H}$ no lugar de e_H: $\alpha j e_E \widehat{H} = k_j e_E \widehat{H}$) (*).

Como $e_E e_H . e_E \widehat{H} = e_E e_H$, temos que $(FA).e_E e_H \subset (FA).e_E \widehat{H}$, e esta inclusão é estrita, pois se existisse $\beta \in FA$ tal que $\beta e_E e_H = e_E \widehat{H}$, multiplicando por e_H dos dois lados, concluiríamos que $e_E \widehat{H} = e_E e_H$, o que não pode ser verdade, pois b^{p^i-1} está no suporte do membro da direita, mas não no suporte do membro da esquerda desta última igualdade. Portanto, um elemento $0 \neq \gamma \in (FA).e_E e_H = I_e$ pode ser escrito na forma

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

Como $\gamma \neq 0$, temos que pelo menos um dos coeficientes $k_j \neq 0$. Se $\gamma = k_j b^j e_E \widehat{H}$, teríamos que $e_E \widehat{H} \in (FA).e_E e_H$. Mas isso não pode acontecer, pois a inclusão $(FA).e_E e_H \subset (FA).e_E \widehat{H}$ é estrita. Então, pelo menos dois k_j's diferentes são diferentes de 0. Como $\gamma \neq 0$ foi pego arbitrário em I_e, temos que $l(I_e) \geq 2^{m+1}|H|$. Como a inclusão oposta nós já tínhamos concluído, temos portanto que

$$l(I_e) = 2^{m+1}|H|$$

e calculamos a distância mínima de todos os ideais minimais.

Finalmente, vamos calcular a dimensão dos códigos abelianos minimais; isto é, a dimensão dos ideais da forma $FA.e$, onde e é um idempotente primitivo de FA.

Teorema 2.5.2 *Seja $e = e_E e_H$ um idempotente primitivo de FA, conforme as definições acima. Temos que:*

$$dim(FA.e) = \phi(p^i),$$

$$dim(FA.e_E\widehat{B}) = 1$$

Prova: Temos

$$FA.e_Ee_H = F[E \times B].e_Ee_H = ((FE)B).e_Ee_H = (FE.e_E)B.e_H.$$

Pela fórmula (2.2), temos que $(FE).e_E \simeq F$, para todo idempotente primitivo e_E de FE. E segue da fórmula acima que

$$FA.e_Ee_H \simeq FB.e_H$$

e do Corolário 2.4.4, temos que

$$dim[FA.e_Ee_H] = \phi(p^i).$$

Agora vamos ao caso em que $e_H = \widehat{B}$. Como já vimos ao calcular a distância mínima do ideal $(FA).e_E\widehat{B}$, todo elemento deste ideal é um múltiplo por um elemento de F do elemento $e_E\widehat{B}$. Assim, temos

$$dim[FA.e_E\widehat{B}] = dim[FB.\widehat{B}] = 1.$$

□

2.6 Polinômio Gerador de Códigos Cíclicos Minimais de Tamanho p^n

Agora, para completar, vamos encontrar qual é o polinômio gerador dos códigos cíclicos $I_i = (FA)(\widehat{A_i} - \widehat{A_{i-1}})$ (como descrito no Teorema 2.10), e $I_0 = (FA)(\widehat{A})$, onde A é cíclico de ordem p^n, e F é corpo finito com q elementos, e $(q, |A|) = 1$.

Começaremos com o caso $i > 0$:

Pela Proposição 1.4.21, temos que, se $e_i(x)$ corresponde ao idempotente primitivo e_i, então o polinômio gerador $g_i(x)$ do ideal $I = (FA)e_i$ satisfaz:

$$g_i(X) = mdc(e_i(X), X^{p^n} - 1).$$

Então, basta escolher $e_i(x)$ tal que $e_i(a) = e_i$, onde a é gerador de A. Então vamos escolher

$$e_i(x) = \frac{1}{p^{n-i}} \sum_{j=0}^{p^{n-i}-1} X^{jp^i} - \frac{1}{p^{n-i+1}} \sum_{j=0}^{p^{n-i+1}-1} X^{jp^{i-1}}.$$

Vamos simplificar a expressão acima:

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

$$= \frac{1}{p^{n-i+1}} \Big[p \sum_{j=0}^{p^{n-i}-1} X^{jp^i} - \sum_{j=0}^{p^{n-i+1}-1} X^{jp^{i-1}} \Big]$$

Note que

$$\left(\sum_{j=1}^{p-1} X^{jp^{i-1}} \right) \left(\sum_{j=0}^{p^{n-i}-1} X^{jp^i} \right) = \sum_{k=1}^{p-1} \sum_{j=0}^{p^{n-i}-1} X^{kp^{i-1}+jpp^{i-1}} =$$

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

Portanto, temos

$$= \frac{1}{p^{n-i+1}} \Big[p \sum_{j=0}^{p^{n-i}-1} X^{jp^i} - \sum_{j=0}^{p^{n-i+1}-1} X^{jp^{i-1}} \Big] =$$

$$= \frac{1}{p^{n-i+1}} \Big[(p-1) \Big(\sum_{j=0}^{p^{n-i}-1} X^{jp^i} \Big) - \Big(\sum_{j=1}^{p-1} X^{jp^{i-1}} \Big) \Big(\sum_{j=0}^{p^{n-i}-1} X^{jp^i} \Big) \Big]$$

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

Também:

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

Notando que $X^{jp^{i-1}}=(X^{p^{i-1}})^j$, concluímos imediatamente toda raiz de $(X^{p^{i-1}}-1)$ em um fecho algébrico de F é também uma raiz de

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

e, portanto, $(X^{p^{i-1}}-1)$ divide $p-\sum_{j=0}^{p-1}X^{jp^{i-1}}$.

Como já sabemos que a dimensão de $I_i=\phi(p^i)=p^i-p^{i-1}$ é igual a $p^n-deg(g_i(X))$ (pela observação logo após a Definição 1.4.18), temos que

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

E assim concluímos o caso $i>0$.

Agora vamos analisar o caso $i=0$:

Como fizemos na escolha dos e_i's acima, podemos escolher $e_0(X)=\sum_{i=0}^{p^n-1}X^i$, que tem grau p^n-1. Como $g_0(X)=mdc(e_0(X),X^{p^n}-1)$, e além disso $(X^{p^n}-1)=e_0(X)(X-1)$, temos que $g_0(X)=e_0(X)$.

Assim, concluímos este capítulo.

Capítulo 3

Idempotentes Centrais Primitivos em Álgebras de grupo Racionais de Grupos Nilpotentes Finitos

O objetivo deste capítulo é descrever quais são os idempotentes centrais primitivos de uma álgebra de grupo racional de um grupo nilpotente finito, sem fazer uso da tabela de caracteres do grupo G, e utilizando para isso o artigo *Central idempotents in the rational group algebra of a finite nilpotent group*, de E., Jespers, G., Leal e A., Paques. Descreveremos, em primeiro lugar, os idempotentes primitivos de $\mathbb{Q}G$ quando G é um grupo abeliano finito.

Precisaremos ainda de mais alguns pré-requisitos, e começaremos este capítulo por eles.

3.1 Pré-requisitos

Antes de partirmos para o problema proposto acima, vamos considerar alguns dos requisitos de que precisamos. Começaremos com um pouco de representações de grupos:

Definição 3.1.1 *Seja G um grupo e V um $\mathbb{C}$ - espaço vetorial de dimensão finita. Uma* ***representação de*** *G* ***(sobre*** *$\mathbb{C}$)****, com espaço de representação V, é um homomorfismo de grupos***

$$T : G \to L(V)$$

$$T(g) \mapsto T_g,$$

onde $L(V)$ é o grupo de operadores lineares bijetores de V (que pode ser identificado com o grupo de matrizes quadradas de tamanho $dim_{\mathbb{C}}V$ e determinante não nula).

Uma tal representação é dita ***fiel*** *se T for injetora.*

Uma representação é dita ***irredutível*** *se $V \neq \{0\}$ e os únicos subespaços de V invariantes sob todos os T_g's são os triviais: $\{0\}$ e V.*

Temos o seguinte resultado:

Lema 3.1.2 ***(Schür)*** *Seja G um grupo e $T : G \to M_n(\mathbb{C})$ uma representação irredutível de G. Então, se $M \in M_n(\mathbb{C})$ comuta com cada elemento T_g da imagem de T, então $M \in Z(M_n(\mathbb{C}))$, ou seja, M é um múltiplo da matriz identidade.*

Prova: seja $M \in M_n(\mathbb{C})$ matriz que comuta com cada elemento da imagem de T. Como $\mathbb{C}$ é algebricamente fechado, então existe um autovalor $\lambda \in \mathbb{C}$ da matriz M. Seja V_λ o auto-espaço correspondente. Vamos provar que V_λ é invariante sobre todo $T_g \in T(G)$. Seja $v \in V_\lambda$:

$$MT_g(v) = T_gM(v) = T_g(\lambda v) = \lambda T_g(v)$$

$$\Rightarrow T_g(v) \in V_\lambda.$$

Portanto, temos que, como $V_\lambda \neq \{0\}$ e a representação é irredutível, então $V_\lambda = V$ e, portanto, $M = \lambda I$.

□

Continuaremos denotando o centro de um grupo G por $Z(G)$.

Temos o seguinte corolário:

Corolário 3.1.3 *Se G é um grupo finito que tem representação irredutível e fiel, então $Z(G)$ é um grupo cíclico.*

Prova: Seja T uma tal representação. Pelo lema anterior, temos que cada elemento de $T(Z(G))$ é um escalar multiplicado pela matriz identidade. Portanto, temos que, naturalmente, $T(Z(G))$ é isomorfo a um subgrupo finito do grupo multiplicativo $\mathbb{C}^*$. Como todo subgrupo finito do grupo multiplicativo de um corpo é cíclico, temos que $T(Z(G))$ é cíclico. Como a representação é fiel, temos que $Z(G) \simeq T(Z(G))$, e temos o resultado que desejamos.

□

Tendo os resultados desta seção em mente, vamos agora às partes principais do capítulo.

3.2 Quando G é Grupo Abeliano Finito

De agora em diante, G sempre denotará um grupo finito.

Defina, para e um idempotente central primitivo de $\mathbb{K}G$, o subgrupo

$$G_e = \{g \in G : ge = e\}$$

Temos que G_e é subgrupo normal de G, pois se $he = e$ $(h \in G_e)$, então para $g \in G$ temos

$$(ghg^{-1})e = (gh)(g^{-1}e) = (gh)(eg^{-1}) = g(he)g^{-1} = geg^{-1} = gg^{-1}e = e$$

Como temos o resultado ([**5**], Lema 3.6.6) de que, para $H \leq G$, $\widehat{H}$ é sempre idempotente em $\mathbb{Q}G$, e é central se H é normal, então temos que $\widehat{G_e}$ é idempotente central de $\mathbb{Q}G$.

Além disso,

$$e\widehat{G_e} = e\frac{1}{|G_e|}\sum_{g\in G_e} g = \frac{1}{|G_e|}\sum_{g\in G_e} eg = \frac{1}{|G_e|}\sum_{g\in G_e} e = e.$$

Portanto, temos que e é um idempotente central primitivo de $(\mathbb{Q}G)\widehat{G_e} \simeq \mathbb{Q}(G/G_e)$, então $\bar{e}$ é idempotente central primitivo de $\mathbb{Q}(G/G_e)$.

Se G for não trivial, denotemos por $\mathcal{M}(G)$ o conjunto de todos os subgrupos normais minimais de G. E vamos definir

$$\varepsilon(G) = \prod_{M \in \mathcal{M}(G)} (1 - \widehat{M}).$$

E definimos $\varepsilon(\{1\}) = 1$.

Seja N um subgrupo normal de G e seja M um subgrupo de G que contém N. Então já sabemos que $\widehat{N}\widehat{M} = \widehat{M}$ (pelo Lema 2.4.2). Denotemos por $\bar{M}$ o grupo M/N. Se $N \neq G$ definimos

$$\varepsilon(G,N) = \prod_{\bar{M} \in \mathcal{M}(G/N)} (\widehat{N} - \widehat{M}) = \prod_{\bar{M} \in \mathcal{M}(G/N)} (\widehat{N} - \widehat{N}\widehat{M}) = \widehat{N} \prod_{\bar{M} \in \mathcal{M}(G/N)} (1 - \widehat{M}).$$

E definimos $\varepsilon(G,G) = \widehat{G}$. Desta forma, temos que a pré-imagem de $\varepsilon(G/N)$ em $(\mathbb{Q}G)\widehat{N}$ é $\varepsilon(G,N)$. Obs.: aqui estamos utilizando o isomorfismo $((\mathbb{Q}G)\widehat{G_e}) \simeq \mathbb{Q}(G/G_e)$, encontrado na demonstração da Proposição 3.6.7 de [5], que identifica G/G_e e $G\widehat{G_e}$ como grupos, pelo morfismo $\phi : G \to G\widehat{G_e}$, dado por $\phi(g) = g\widehat{G_e}$, que é um epimorfismo de núcleo G_e.

Temos o seguinte lema:

Lema 3.2.1 *Se e é um idempotente central primitivo de $\mathbb{Q}G$ e N é um subgrupo normal de G, então $e\widehat{N} = e$ se, e somente se, $N \subset G_e$.*

Prova: Se $N \subset G_e$, temos:

$$e\widehat{N} = e\frac{1}{|N|}\sum_{g \in N} g = \frac{1}{|N|}\sum_{g \in N} eg = \frac{1}{|N|}\sum_{g \in N} e = e.$$

Por outro lado, se $e\widehat{N} = e$, seja $n \in N$. Temos

$$en = (e\widehat{N})n = e(\widehat{N}n) = e\widehat{N} = e,$$

portanto $n \in G_e$ e, logo, $N \subset G_e$.

□

Observemos que, se f é um idempotente central, como $e = ef + e(1-f)$, e cada um dos termos é idempotente e central, e são ortogonais entre si (isto é, $(ef)(e(1-f)) = 0$), como e é idempotente central primitivo segue que $ef = e$ ou $ef = 0$. Em particular, se N é como no lema anterior, então $e\widehat{N} = e$ ou 0.

Há outros lemas de que precisaremos:

Lema 3.2.2 *Se e é um idempotente central primitivo de $\mathbb{Q}G$ e $G_e = \{1\}$, então G tem representação irredutível fiel.*

Prova: Seja e como no enunciado. Temos que e um idempotente central (não necessariamente primitivo) de $\mathbb{C}G$. Assim sendo, existem idempotentes centrais primitivos $e_1, ..., e_m$ de $\mathbb{C}G$ distintos tais que $e = e_1 + ... + e_m$. Como $\mathbb{C}Ge_i$ é um módulo semissimples, então existem ideais à esquerda minimais $I_{i,j}$ de $\mathbb{C}Ge_i$ tais que

$$\mathbb{C}Ge_i = I_{i,1} \oplus ... \oplus I_{i,n_i}.$$

Podemos escolher os $I_{i,j}$ como sendo matrizes coluna, (conforme vimos no Teorema 1.4.6 (iv)).

Temos homomorfismos $T_{i,k}$ do tipo:

$$T_{i,k} : G \to L(I_{i,k})$$

$$g \mapsto T_g, 1 \leq k \leq n_i, 1 \leq i \leq m,$$

onde $T_g(x) = gx$. Como x pode ser escrito como sendo $x = e_i y$ ($y \in \mathbb{C}G$), temos que $T_g(x) = T_g(e_i y) = ge_i y = (ge_i)(e_i y)$, então de fato T_g está definida em $I_{i,k}$. Além disso, temos que cada T_g é injetora (e, portanto, bijetora), pois $T_g x = T_g z$ se, e somente se $gx = gz$, e este último acontece se, e somente se $x = z$. Portanto as funções do tipo $T_{i,k}$ acima são representações de G.

Além disso, cada representação $T_{i,k}$ é irredutível: suponha que existe um $\mathbb{C}$-subespaço V de $I_{i,k}$ invariante sob todos os elementos da imagem de $T_{i,k}$. Isto implica que $(\mathbb{C}G)V \subset V$ e, em particular, V é um ideal à esquerda de $\mathbb{C}Ge_i$. Como $I_{i,k}$ é ideal à esquerda minimal, então $V = \{0\}$ ou $V = I_{i,k}$.

Além disso temos, pela escolha dos $I_{i,k}$'s como sendo matrizes coluna que, para cada par (i,k), $T_{i,k}$ é fiel se, e somente se $T_{i,j}$ for fiel, para todo j. E este último acontece se, e somente se $G_{e_i} = \{1\}$. Portanto, para provar o nosso resultado, temos de provar que $G_{e_i} = \{1\}$, para algum i.

Como já vimos, temos que cada $\widehat{G_{e_i}}$ é um idempotente central em $\mathbb{Q}G$ (pois G_{e_i} é normal em G) e, assim, $e\widehat{G_{e_i}} = 0$ ou $e\widehat{G_{e_i}} = e$.

Temos

$$e\widehat{G_{e_i}} = (e_1 + ... + e_m)\widehat{G_{e_i}} = \widehat{G_{e_i}}e_1 + ... + e_i + ...\widehat{G_{e_i}}e_m \neq 0.$$

Portanto, $e\widehat{G_{e_i}} = e$ e, pelo Lema 3.2.1, $G_{e_i} \subset G_e = \{1\}$ e, portanto, $G_{e_i} = \{1\}$, como queríamos.

□

O resultado do lema acima é, na verdade, uma equivalência. Apesar de que não precisaremos da afirmação recíproca, vamos prová-la para fins de completude:

Lema 3.2.3 *Se e é um idempotente central primitivo de $\mathbb{Q}G$, então $G_e = \{1\}$ se, e somente se G tem representação fiel irredutível.*

Prova: O lema anterior nos diz que se $G_e = \{1\}$, então G tem representação fiel irredutível.

Suponha agora que e é um idempotente central primitivo de $\mathbb{Q}G$ e G tem representação fiel irredutível. Vamos utilizar as mesmas notações da prova do teorema anterior:

Pelo Teorema 1.6, temos que todos os $\mathbb{Q}G$-módulos irredutíveis são isomorfos aos $I_{j,k}$ da prova do lema anterior. Como G tem representação fiel e irredutível, temos, pelas Proposições 4.2.1 e 4.2.2(ii) de [5] (que junto com o Teorema 1.4.6 dizem que

toda representação irredutível de G é equivalente a uma das representações $T_{i,j}$) e pela demonstração do lema anterior que $G_{e_i} = \{1\}$, para algum i. Portanto, temos que $G_e = \{1\}$, como queríamos.

□

E temos o seguinte lema, como consequência:

Lema 3.2.4 *Seja G um grupo finito e seja e um idempotente central primitivo de $\mathbb{Q}G$. Então $G_e = \{1\}$ se, e somente se $\varepsilon(G)e = e$. Em particular, $\varepsilon(G) \neq 0$ se, e somente se G tem uma representação fiel irredutível.*

Prova: Suponha que $G_e = \{1\}$. Se $M \in \mathcal{M}(G)$, então $\widehat{M}$ é idempotente central e, desta forma, temos que $e\widehat{M} = e$ ou 0 mas, como $G_e = \{1\}$, temos, pelo Lema 3.2.1, que $e\widehat{M} = 0$, para todo $M \in \mathcal{M}(G)$. Como G é finito, temos que $\mathcal{M}(G) = M_1, ..., M_n$ um conjunto finito. E temos

$$\varepsilon(G)e = \prod_{M \in \mathcal{M}(G)} (1 - \widehat{M})e = (1 - \widehat{M_1})...(1 - \widehat{M_n})e$$

$$= (1 - \widehat{M_1})...(1 - \widehat{M_{n-1}})(e - 0) = (1 - \widehat{M_1})...(1 - \widehat{M_{n-1}})e.$$

Repetindo o passo acima mais $n - 1$ vezes, temos que o produto acima é e.

Por outro lado, suponha que $\varepsilon(G)e = e$. Se $G_e \neq \{1\}$, então existe $M \in \mathcal{M}(G)$ subgrupo não trivial de G_e e normal em G e, portanto, $\varepsilon(G)e = 0 \neq 1$, contradizendo a hipótese.

Em particular: suponha $\varepsilon(G) \neq 0$. Como $\varepsilon(G)$ é idempotente central, então existem idempotentes centrais primitivos $e_1, ..., e_k$ tais que $\varepsilon(G) = e_1 + ... + e_k$ e, portanto, $\varepsilon(G)e_1 = e_1$. Das partes anteriores, temos que $G_{e_1} = \{1\}$. Logo, $\varepsilon(G) \neq 0$ se, e somente se, existe idempotente central primitivo e_1 tal que $G_{e_1} = \{1\}$. Assim, o resultado segue pelo Lema 3.2.3.

□

O i-ésimo centro de G ainda denotaremos por $Z_i(G)$. O centro denotaremos apenas por $Z(G)$. Lembremos aqui o conhecido fato de que, num grupo nilpotente,

todo subgrupo normal intersecta o centro de forma não trivial (Teorema 1.4.29) e, portanto, todo subgrupo normal minimal de um grupo nilpotente é central (isto é, está contido no centro); em particular, todo subgrupo normal minimal de um grupo nilpotente é um grupo cíclico de ordem prima.

Temos, portanto, o seguinte resultado:

Lema 3.2.5 *Seja G um grupo finito. Se $\varepsilon(G) \neq 0$, então $Z(G)$ é cíclico. A recíproca vale se, além diso, G for um grupo nilpotente.*

Prova: Se $\varepsilon(G) \neq 0$, pelo Lema 3.2.4 temos que G tem representação irredutível fiel e, pelo Corolário 3.1.3, temos que $Z(G)$ é cíclico.

Por outro lado, suponha G nilpotente e $Z(G)$ cíclico. Como observado anteriormente, todo subgrupo normal minimal de G é cíclico de ordem p. Pela unicidade dos subgrupos de ordem fixa de um grupo cíclico, e do fato de que, em um grupo nilpotente, todo subgrupo normal não trivial intersecta o centro não-trivialmente, temos que cada subgrupo normal minimal de G tem ordem prima, e todos têm ordens distintas e estão contidos no centro de G. Assim, pelo teorema da decomposição de grupos abelianos finitos, temos que $Z(G)$ pode ser escrito como o produto direto interno:

$$Z(G) = P_1...P_k, \tag{3.1}$$

onde cada P_i é um p_i-subgrupo (p_i primo), com $p_i \neq p_j$, se $i \neq j$. Temos que cada subgrupo normal minimal de G é o subgrupo (cíclico) $C_{p_i} = \langle a_i \rangle$ de ordem p_i contido em P_i, para algum i.

$$\varepsilon(G) = \prod_{i=1}^{k} (1 - \widehat{\langle a_i \rangle})$$

Assim sendo, como o produto (3.1) é direto, temos, pelo Lema 2.4.2, distribuindo o produto acima, que o coeficiente de $g = a_1...a_k$ em $\varepsilon(G)$ é $\frac{1}{|C|} \neq 0$, e temos, portanto, que $\varepsilon(G) \neq 0$.

□

Como aplicação dos lemas anteriores, vamos descrever quais são os idempotentes centrais primitivos da álgebra de grupo racional de um grupo abeliano finito. Mas antes, vamos precisar de um lema:

Lema 3.2.6 *Seja $A = G$ um grupo cíclico finito. Então $\varepsilon(A)$ é um idempotente primitivo de $\mathbb{Q}A$.*

Prova: seja $a \in A$ tal que $A = \langle a \rangle$. Temos $\varepsilon(A) = \prod_{M \in \mathcal{M}(A)} (1 - \widehat{M})$. Se A é um p-grupo, então o resultado segue do Lema 2.3.1 (a demonstração dele também vale quando o corpo é $\mathbb{Q}$).

Se A não é um p-grupo, então ele é produto direto de grupos de ordem potência de primos (distintos):

$$A = G_1 ... G_n,$$

onde cada G_i é um p_i-grupo, e $p_i \neq p_j$, se $i \neq j$.

Assim, temos que $\varepsilon(A) = \varepsilon(G_1)...\varepsilon(G_n)$. Para provar o que queremos, vamos provar que os idempotentes da forma $e_1...e_n$, com e_i um idempotente primitivo de $\mathbb{Q}G_i$, formam o conjunto dos idempotentes primitivos de $\mathbb{Q}G$.

Temos que a quantidade de idempotentes primitivos de $\mathbb{Q}G$ é dada pela quantidade de subgrupos cíclicos de G que é, por sua vez, igual à quantidade de divisores de $|G|$, que é igual ao produto das quantidades de divisores de todos os $|G_i|$´s, que coincide, por sua vez, com o produto da quantidade de idempotentes centrais primitivos de todos os $\mathbb{Q}G_i$´s (pelo Teorema 1.4.9). Além disso todos, os idempotentes da forma $e_1...e_n$, com e_i um idempotente primitivo de $\mathbb{Q}G_i$, satisfazem as propriedades (i) e (ii) do Teorema 1.4.7, e a quantidade de tais idempotentes é a mesma que a quantidade de idempotentes centrais primitivos de $\mathbb{Q}G$. Vamos verificar a propriedade (iii) do Teorema 1.4.7:

Sejam $e_1^i, ..., e_{r_i}^i$ todos os idempotentes de $\mathbb{Q}G_i$, então $1_{G_i} = e_1^i + ... + e_{r_i}^i$. E temos $1 = 1_{G_1}...1_{G_n} = (e_1^1 + ... + e_{r_1}^1)...(e_1^n + ... + e_{r_n}^n)$, e este último é igual à soma de todos os idempotentes da forma $e_1...e_n$, com e_i um idempotente primitivo de $\mathbb{Q}G_i$.

Portanto, temos um conjunto de idempotentes centrais 2 a 2 ortogonais que somam 1, e cuja quantidade é igual à de idempotentes centrais primitivos. Portanto,

eles são os idempotentes centrais primitivos.

□

Usaremos agora os resultados anteriores para obter uma caracterização de todos os idempotentes centrais primitivos da álgebra de grupo racional de um grupo abeliano finito.

Corolário 3.2.7 *Seja G um grupo abeliano finito. Os idempotentes centrais primitivos de $\mathbb{Q}G$ são precisamente os elementos da forma $\varepsilon(G,N)$, com N um subgrupo de G tal que G/N é cíclico. Em particular, se e é um idempotente central primitivo, então $supp(e)$ é um subgrupo de G, e e é uma combinação $\mathbb{Z}$-linear de idempotentes da forma $\widehat{H}$, onde H é subgrupo de G.*

Prova: Como já sabemos pelo lema anterior, se A é cíclico, então $\varepsilon(A)$ é um idempotente primitivo de $\mathbb{Q}A$. Em particular, se G/N é cíclico, temos que $\varepsilon(G/N)$ é idempotente primitivo de $\mathbb{Q}(G/N) \simeq (\mathbb{Q}G)\widehat{N}$ e, portanto, $\varepsilon(G,N)$ é um idempotente primitivo de $(\mathbb{Q}G)\widehat{N}$ e, portanto, de $\mathbb{Q}G$.

Seja agora e um idempotente primitivo de $\mathbb{Q}G$. Então $(G/G_e)_{\overline{e}} = \{1\}$ e, pelos lemas 3.2.4 e 3.2.5, G/G_e é cíclico e $\varepsilon(G/G_e)\overline{e} = \overline{e}$, portanto, $\varepsilon(G/G_e)$ é idempotente primitivo de $\mathbb{Q}(G/G_e) \simeq \mathbb{Q}G(\widehat{G_e})$ e, portanto, $\varepsilon(G,G_e)$ é idempotente central primitivo de $\mathbb{Q}G$, e também $\varepsilon(G,G_e)e = e$ e, portanto, $\varepsilon(G,G_e) = e$.

Provemos agora a segunda parte. Seja e um idempotente primitivo de $\mathbb{Q}G$. Então temos que $e = \varepsilon(G,G_e)$. Se $M_1,...,M_n$ são os subgrupos de G que contém G_e minimais, então temos que e é combinação $\mathbb{Z}$-linear de $\widehat{G_e}$ e elementos do tipo $\widehat{G_e}\widehat{M_{i_1}}...\widehat{M_{i_k}} = \widehat{M_{i_1}}...\widehat{M_{i_k}}$.

Temos:

$$\widehat{M_{i_1}}...\widehat{M_{i_k}} = \left(\frac{1}{|M_{i_1}|}\sum_{g\in M_1} g\right)...\left(\frac{1}{|M_{i_k}|}\sum_{g\in M_k} g\right) =$$

$$= \frac{1}{|M_{i_1}|...|M_{i_k}|}\left(\sum_{g\in M_{i_1}} g\right)...\left(\sum_{g\in M_{i_k}} g\right) =$$

$$= \frac{1}{|M_{i_1}|...|M_{i_k}|}\left(|G_e|\sum_{\overline{g}\in M_{i_1}/G_e} g\widehat{G_e}\right)...\left(|G_e|\sum_{\overline{g}\in M_{i_k}/G_e} g\widehat{G_e}\right) =$$

$$= \frac{|G_e|^k}{|M_{i_1}|...|M_{i_k}|} \left(\sum_{\overline{g} \in \frac{M_{i_1}...M_{i_k}}{G_e}} g\widehat{G_e} \right) = \frac{1}{|M|} \sum_{g \in M} g = \widehat{M},$$

onde $M = M_{i_1}...M_{i_k}$.

Isso prova que e é combinação $\mathbb{Z}$-linear de elementos do tipo previsto.

Para provar que $supp(e)$ é subgrupo de G, vamos novamente olhar para o quociente (G/G_e), e vamos primeiro provar que $supp(\overline{e})$ é subgrupo de G/G_e.
Como G/G_e é cíclico, então ele é o produto direto de grupos cíclicos cujas ordens são potências de primos distintos

$$G/G_e = P_1 \times ... \times P_r,$$

e pela demonstração do Lema 3.2.6, temos que $\overline{e} = e_1...e_r$, onde e_i é um idempotente primitivo de $\mathbb{Q}P_i$. Portanto, $supp(\overline{e}) = supp(e_1) \times ... \times supp(e_r)$ e, portanto, podemos reduzir o problema ao caso em que G/G_e é um p-grupo. Nesse caso, temos pelo Lema 2.3.1 do capítulo anterior que $\overline{e} = \widehat{G/G_e}$ ou $\overline{e} = \widehat{H} - \widehat{K}$, onde H, K são subgrupos de G/G_e e H é subgrupo próprio de K. No primeiro caso, temos $supp(\overline{e}) = G/G_e$ e, no segundo caso, temos $supp(\overline{e}) = K$, e nosso resultado para G/G_e está provado.

Portanto, novamente olhando para o isomorfismo $(\mathbb{Q}G)\widehat{G_e} \simeq \mathbb{Q}(G/G_e)$ (induzido pelo isomorfismo de grupos $g\widehat{G_e} \to \overline{g}$), temos que, se e é um idempotente primitivo de $\mathbb{Q}G$ (e, como sabemos, de $(\mathbb{Q}G)\widehat{G_e}$), então o suporte de $\overline{e}$ é um subgrupo $\overline{M}$ de G/G_e (portanto $G_e \leq M$), então o suporte de e é

$$supp(e) = \bigcup_{g \in M} supp(g\widehat{G_e}) = M \leq G,$$

como queríamos provar.

□

Terminamos assim esta seção.

3.3 Grupos Nilpotentes Finitos

O objetivo desta seção é generalizar o último corolário da seção anterior para o caso em que G é um grupo nilpotente finito.

Vamos precisar introduzir uma notação:

Para um elemento $g \in G$, denotemos por C_g o conjunto de todos os conjugados de g por elementos de G, isto é: $C_g = \{hgh^{-1} : h \in G\}$, e é chamada de classe de conjugação de g.

Seja $x \in Z(\mathbb{Q}G)$ um elemento do centro de $\mathbb{Q}G$. Para todo $g \in g$ temos $gxg^{-1} = x$, isto implica que, para cada $h \in supp(x)$, cada elemento de C_h está no suporte de x e tem o mesmo coeficiente de h.

Ou seja, acabamos de mostrar que os elementos $\widehat{C_g}$, com $g \in G$ formam uma $\mathbb{Q}$-base para o centro de $\mathbb{Q}G$.

Vamos provar um pequeno lema que será importante para provarmos o resultado principal:

Lema 3.3.1 *Seja G um grupo finito e $g \in G$. Se $g^{-1}C_g \cap Z(G) \neq \{1\}$, então G contém um elemento central z, de ordem prima, tal que $\widehat{C_g} = \widehat{C_g}\widehat{\langle z \rangle}$.*

Prova: Por hipótese, existe $h \in G$ tal que $g^{-1}(h^{-1}gh) = z \neq 1$, $z \in Z(G)$. Portanto, $g^{-1}h^{-1}g = zh^{-1}$.

Suponha que $|z| = pn$, onde p é primo e n é inteiro positivo. Então temos que

$$z^n h^{-n} = (g^{-1}h^{-1}g)^n = g^{-1}h^{-n}g$$

e portanto $1 \neq z^n = (g^{-1}(h^n)^{-1}g)\, h^n \in Z(G)$, e $|z^n| = p$. Portanto, podemos supor que z tem ordem prima.

Novamente de $g^{-1}(h^{-1}gh) = z$, temos que

$$h^{-1}gh = zg.$$

Multiplicando por $h^{-(n-1)}$ à esquerda e por h^{n-1} à direita da última equação, temos

$$h^{-n}gh^n = h^{-(n-1)}zgh^{n-1} = zh^{-(n-1)}gh^{n-1} =$$

$$= zh^{-(n-2)}zgh^{n-2} = z^2h^{-(n-2)}gh^{n-2},$$

e repetindo indutivamente o processo descrito acima mais $n-2$ vezes, temos que $h^{-n}gh^n = z^ng$.

Se $k \in G$, multiplicando a última equação por k^{-1} à esquerda e por k à direita, temos que

$$k^{-1}h^{-n}gh^nk = (h^nk)^{-1}g(h^nk) = k^{-1}z^ngk = z^n(k^{-1}gk).$$

Daí, temos que $\langle z\rangle\, C_g \subseteq C_g$. A inclusão contrária é óbvia, pois $1 \in < z >$. Então temos $\langle z\rangle\, C_g = C_g$. Em particular, temos que as funções $f_i : C_g \to C_g$ definidas por $f_i(x) = z^ix$ são bijetoras. Daí, segue que $\widehat{C_g} = \widehat{C_g}\widehat{\langle z\rangle}$, pois $\widehat{C_g}\widehat{\langle z\rangle} = \frac{1}{o(z)}\widehat{C_g}(z + ... + z^{o(z)}) = \frac{1}{o(z)}o(z)\widehat{C_g} = \widehat{C_g}$.

□

O centralizador de um subconjunto S do grupo G será denotado por $C_G(S)$, e é o cunjunto de todos os elementos de G que comutam com todos os elementos de S. Prosseguiremos com o seguinte lema:

Lema 3.3.2 *Seja G um grupo finito e N um subgrupo normal de G. Suponha que $e_1, ..., e_n$ é a lista de idempotentes centrais primitivos de $\mathbb{Q}N$, e seja $g \in G$. Então $g^{-1}e_1g, ..., g^{-1}e_ng$ também é a lista de idempotentes centrais primitivos de $\mathbb{Q}N$.*

Prova: como N é subgrupo normal de G, temos que a função $n \in N \mapsto g^{-1}ng \in N$ é um automorfismo, que induz um automorfismo em $\mathbb{Q}N$, também dado pela conjugação pelo elemento $g \in G$. Assim, temos o resultado desejado.

□

A próxima proposição descreve os idempotentes centrais e da álgebra de grupo racional de um grupo nilpotente finito com $G_e = \{1\}$.

Proposição 3.3.3 *Seja G um grupo finito, e seja $e \in \mathbb{Q}G$. Se e é um idempotente central primitivo de $\mathbb{Q}G$, com $G_e = \{1\}$, então e é a soma de todos os G-conjugados de um idempotente central primitivo $e_1 \in \mathbb{Q}G_1$, onde $G_1 = C_G(Z_2(G))$, e $\cap_{g\in G}((G_1)_{e_1})^g = 1$. A recíproca vale se G for nilpotente.*

Em particular, qualquer idempotente central primitivo e com G_e trivial tem suporte contido em $C_G(Z_2(G))$.

Prova: Suponha que $e \in \mathbb{Q}G$ é um idempotente central primitivo, com $G_e = \{1\}$. Seja $\mathcal{C}$ um conjunto de representantes de todas as classes de conjugação de G. Como já foi notado, e pode ser escrito como $e = \sum_{g\in\mathcal{C}} \alpha_g \widehat{C_g}$, onde cada $\alpha_g \in \mathbb{Q}$.
Seja $g \notin C_G(Z_2(G))$ um elemento de G. Seja $h^{-1}gh \in C_g$, com $h \in Z_2(G)$ tal que $hg \neq gh$. Temos que $g^{-1}(h^{-1}gh) \neq 1$.

Afirmação: $g^{-1}(h^{-1}gh) \in Z(G)$.

Para provar tal afirmação, olhemos para o quociente $G/Z(G)$: neste quociente, temos que $\overline{h}$ e $\overline{h^{-1}}$ são centrais (pois $h \in Z_2(G)$). Então

$$\overline{g^{-1}(h^{-1}gh)} = \overline{1} = Z(G) \Rightarrow g^{-1}(h^{-1}gh) \in Z(G).$$

Assim, se $g \notin C_G(Z_2(G))$, temos pelo Lema 3.3.1 que existe $w_g \in Z(G)$ de ordem prima tal que $\widehat{C_g} = \widehat{C_g}\widehat{\langle w_g\rangle}$. Além disso, como $Z_2(G)$ é normal em G, temos que $G_1 = C_G(Z_2(G))$ é normal e, portanto, os conjugados de elementos em G_1 estão em G_1. Então podemos escrever

$$e = \sum_{g\in C_G(Z_2(G))\cap\mathcal{C}} \alpha_g \widehat{C_g} + \sum_{g\notin C_G(Z_2(G)),g\in\mathcal{C}} \alpha_g \widehat{C_g}\widehat{\langle w_g\rangle}$$

Como G_e é trivial, pelo Lema 3.2.4, temos que $e\varepsilon(G) = e$. Mas como cada $\langle w_g\rangle$ é normal minimal, temos

$$\varepsilon(G)\widehat{\langle w_g\rangle} = \left(\prod_{M\in\mathcal{M}\setminus\{\langle w_g\rangle\}} (1-\widehat{M})\right)(1-\widehat{\langle w_g\rangle})\widehat{\langle w_g\rangle} = 0.$$

Portanto, podemos escrever

$$e = \sum_{g\in C_G(Z_2(G))\cap\mathcal{C}} \alpha_g \widehat{C_g}.\varepsilon(G). \tag{3.2}$$

Analogamente, podemos escrever

$$\varepsilon(G) = \sum_{g\in C_G(Z_2(G))\cap\mathcal{C}} \beta_g \widehat{C_g} + \sum_{g\notin C_G(Z_2(G)),g\in\mathcal{C}} \beta_g \widehat{C_g}\widehat{\langle w_g\rangle},$$

e como $\varepsilon(G)\widehat{\langle w_g\rangle} = 0$, temos:

$$0 = \sum_{g\in C_G(Z_2(G))\cap\mathcal{C}} \beta_g \widehat{C_g}\widehat{\langle w_g\rangle} + \sum_{g\notin C_G(Z_2(G)),g\in\mathcal{C}} \beta_g \widehat{C_g}\widehat{\langle w_g\rangle}, \tag{3.3}$$

e como $C_G(Z_2(G))$ é normal em G e $\langle w_g\rangle \subset C_G(Z_2(G)) = G_1$, temos

$$supp\left(\sum_{g\in C_G(Z_2(G))\cap\mathcal{C}} \eta_g \widehat{C_g}\widehat{\langle w_g\rangle}\right) \subset C_G(Z_2(G)),$$

$$supp\left(\sum_{g\notin C_G(Z_2(G)),g\in\mathcal{C}} \eta_g \widehat{C_g}\widehat{\langle w_g\rangle}\right) \cap C_G(Z_2(G)) = \emptyset,$$

para quaisquer $\eta_g \in \mathbb{Q}$.

Em particular, temos, pela equação (3.3) que $\sum_{g\notin C_G(Z_2(G)),g\in\mathcal{C}} \beta_g \widehat{C_g}\widehat{\langle w_g\rangle} = 0$ e, portanto, $supp(\varepsilon(G)) \subset C_G(Z_2(G))$.

Aplicando o parágrafo anterior na equação (3.2), temos que $supp(e) \subset C_G(Z_2(G)) = G_1$. Ou seja, $e \in \mathbb{Q}G_1$.

Não temos certeza se e é idempotente central primitivo em $\mathbb{Q}G_1$, mas com certeza é idempotente central. Portanto, podemos escrever

$$e = e_1 + ... + e_n,$$

onde cada e_i é um idempotente central primitivo de $\mathbb{Q}G_1$.

Seja $g \in G$. Temos que

$$e = e^g = e_1^g + ... + e_n^g. \tag{3.4}$$

Seja $\widetilde{e} = e_1^{g_1} + ... + e_1^{g_k}$ a soma de todas as G-classes de conjugação de e_1. Temos que $\widetilde{e}$ é central em $\mathbb{Q}G$. E pelo Lema 3.3.2, podemos concluir que $\widetilde{e}$ é idempotente e não nulo.

Assim sendo, $\widetilde{e}e = e$ ou 0. Usando a equação (3.4) temos:

$$\widetilde{e}e = e_1^{g_1}e + ... + e_1^{g_k}e = e_1^{g_1}(e_1^{g_1} + ... + e_n^{g_1}) + ... + e_1^{g_k}(e_1^{g_k} + ... + e_n^{g_k}) = e_1^{g_1} + ... + e_1^{g_k} = \widetilde{e} \neq 0,$$

desta equação, temos que $e = \widetilde{e}$ (isso prova uma parte da proposição, e também prova que $n = k$).

Como $((G_1)_{e_1})^{g_i} = (G_1)_{e_1^{g_i}}$, então segue que $\cap_{i=1}^{n}((G_1)_{e_1})^{g_i} = \cap_{i=1}^{n}(G_1)_{e_1^{g_i}} \subseteq G_e = \{1\}$ e segue que $\cap_{i=1}^{n}((G_1)_{e_1})^{g_i} = \{1\}$. Assim, provamos um dos lados da proposição.

Por outro lado, suponha que e_1 é um idempotente central primitivo de $\mathbb{Q}G_1$, com $G_1 = C_G(Z_2(G))$ e suponha que $\cap_{i=1}^{n}((G_1)_{e_1})^{g_i} = \{1\}$.

Seja $e = e_1^{g_1} + ... + e_1^{g_n}$ a soma de todas as G-classes de conjugação de e_1.

Temos que e é central em $\mathbb{Q}G$ e, além disso, concluímos pelo Lema 3.3.2 que e é idempotente. Portanto, existem $f_1, ..., f_k$ idempotentes centrais primitivos em $\mathbb{Q}G$ tais que $e = f_1 + ... + f_k$.

Seja N um subgrupo central não trivial de G. Temos que $\widehat{N}$ é um idempotente central em $\mathbb{Q}G_1$ e, portanto, $\widehat{N}e_1 = 0$ ou e_1, sendo que se for igual a e_1, implica $N \subseteq (G_1)_{e_1}$ (pelo Lema 3.2.1) e então

$$N \subseteq \bigcap_{g \in G} ((G_1)_{e_1})^g = \{1\},$$

o que não é possível.

Sendo assim, $\widehat{N}e_1 = 0$. Como $(G_1)_{e_1}$ é normal em G e G é grupo nilpotente, temos que existe subgrupo $N \neq \{1\}$ de G, contido em $Z(G) \cap (G_1)_{e_1}$, se $(G_1)_{e_1} \neq \{1\}$.

Mas como $\widehat{N}e_1 = 0$, então $(G_1)_{e_1} = \{1\}$ e, pelo Lema 3.2.4, temos que $\varepsilon(G_1)e_1 = \varepsilon(G)e_1 = e_1$ (obs.: $\varepsilon(G) = \varepsilon(G_1)$, pois G é nilpotente e também $Z(G) \subseteq G_1$).

Consequentemente, temos $\varepsilon(G)e = e$ e, portanto, $\varepsilon(G)f_i = f_i$, para todo i. Pelo Lema 3.2.4, temos que G_{f_i} é trivial e, portanto, pela primeira parte da prova, temos $f_i \in \mathbb{Q}G_1$.

Como e_1 aparece na representação de e como soma de idempotentes centrais primitivos de $\mathbb{Q}G_1$, então e_1 também aparece na mesma representação de algum f_i. Pela primeira parte da prova, temos que $f_i = e_1^{g_1} + ... + e_1^{g_n} = e$, portanto, $e = f_i$ é idempotente central primitivo de $\mathbb{Q}G$, como queríamos.

□

Agora vamos ao resultado principal deste capítulo, onde descreveremos os idempotentes primitivos centrais de quaisquer álgebras racionais de grupos nilpotentes

finitos, dando uma descrição que depende apenas da estrutura do reticulado de subgrupos do grupo nilpotente em questão.

Teorema 3.3.4 *Seja G um grupo nilpotente finito. Então os idempotentes centrais primitivos são precisamente todos os elementos da forma*

$$(\varepsilon(G_m, H_m))^{g_1} + ... + (\varepsilon(G_m, H_m))^{g_n}$$

isto é, a soma de todos os G-conjugados de $\varepsilon(G_m, H_m)$, onde H_m, G_m são subgrupos de G que satisfazem às seguintes propriedades:

(1) $H_0 \subseteq H_1 \subseteq ... \subseteq H_m \subseteq G_m \subseteq ... \subseteq G_1 \subseteq G_0 = G$;
(2) para $0 \leq i \leq m$, H_i *é um subgrupo normal de* G_i *e* $Z(G_i/H_i)$ *é cíclico;*
(3) para $0 \leq i < m$, G_i/H_i *não é abeliano, e* G_m/H_m *é abeliano;*
(4) para $0 \leq i < m$, $G_{i+1}/H_i = C_{G_i/H_i}(Z_2(G_i/H_i))$;
(5) para $1 \leq i \leq m$, $\cap_{x \in G_{i-1}/H_{i-1}} H_i^x = H_{i-1}$.

Prova: Em primeiro lugar, vamos ver que um elemento do tipo acima é mesmo um idempotente central primitivo.

Seja $e = (\varepsilon(G_m, H_m))^{g_1} + ... + (\varepsilon(G_m, H_m))^{g_n}$ satisfazendo às propriedades acima. Por causa do Corolário 3.2.7, temos que as propriedades (2) e (3) implicam que $\overline{f_m} = \varepsilon(G_m/H_m)$ é um idempotente (central) primitivo de $\mathbb{Q}(G_m/H_m) \simeq (\mathbb{Q}G_m)\widehat{H_m}$. Daí, temos que $\varepsilon(G_m, H_m) = f_m$ é um idempotente central primitivo de $\mathbb{Q}G_m$.

Como $\varepsilon(G_m/H_m)\overline{f_m} = \overline{f_m}$, então $(G_m/H_m)_{\overline{f_m}} = \{\overline{1}\}$, pelo Lema 3.2.4. Lembrando que $\mathbb{Q}(G_m/H_m) \simeq (\mathbb{Q}G_m)\widehat{H_m}$ pelo isomorfismo induzido pelo isomorfismo de grupos $g \in G\widehat{H_m} \to \overline{g} \in G/H_m$, temos:

$$g \in (G_m)_{f_m} \Leftrightarrow gf_m = (g\widehat{H_m})(f_m\widehat{H_m}) = f_m\widehat{H_m} = f_m \Leftrightarrow$$

$$\Leftrightarrow \overline{g} \in (G_m/H_m)_{\overline{f_m}} = \{\overline{1}\} \Leftrightarrow g \in H_m.$$

Assim, temos que $(G_m)_{f_m} = H_m$.

A propriedade (4) implica que, em particular, G_{i+1}/H_i é subgrupo normal de G_i/H_i e, usando o teorema da correspondência, temos que G_m é normal em G_{m-1}.

Portanto temos, pelo Lema 3.3.2, que f_{m-1} a soma de todos os G_{m-1}-conjugados de f_m é idempotente, além disso, f_{m-1} é claramente central em $\mathbb{Q}G_{m-1}$. A propriedade (5) nos dá

$$\bigcap_{g\in G_{m-1}} ((G_m)_{f_m})^g = \bigcap_{g\in G_{m-1}} H_m^g = H_{m-1}$$

$$\Rightarrow \bigcap_{g\in G_{m-1}/H_{m-1}} ((G_m/H_{m-1})_{\overline{f_m}})^g = \bigcap_{g\in G_{m-1}/H_{m-1}} (H_m/H_{m-1})^g = \{1\}.$$

Assim, as propriedades (2), (4) e a fórmula acima, junto com a proposição anterior implicam que f_{m-1} é um idempotente central primitivo de $(\mathbb{Q}G_{m-1})\widehat{H_{m-1}} \simeq \mathbb{Q}(G_{m-1}/H_{m-1})$ (olhando primeiro para o quociente). Portanto, f_{m-1} é idempotente primitivo central de $\mathbb{Q}G_{m-1}$.

Repetindo o argumento acima para f_{m-2} a soma de todos os G_{m-2}-conjugados de f_{m-1}, temos que f_{m-2} é idempotente central primitivo de $\mathbb{Q}G_{m-2}$. A única parte da prova que não é análogo ao que fizemos, é para provar que $(G_{m-1})_{f_{m-1}} = H_{m-1}$. Para isso, vamos escrever $f_{m-1} = f_m^{g_1} + ... + f_m^{g_k}$. Assim,

$$h \in (G_{m-1})_{f_{m-1}} \Leftrightarrow f_{m-1}h = f_{m-1}, \tag{3.5}$$

como o suporte de f_{m-1} está contido em G_m, então temos $h \in G_m$. Portanto, pelo Lema 3.3.2 e o Teorema de Wedderburn-Artin, temos que vale (3.5) se, e somente se $f_m^{g_i}h = f_m^{g_i}$, para todo i, que equivale a dizer que $f_m h^{g_i^{-1}} = f_m$ e, portanto, $h^{g_i^{-1}} \in H_m$ e, portanto $h \in H_m^{g_i}$. Como a escolha de f_m perite que g_i seja qualquer elemento de G_{m-1} temos, pela propriedade (5) que $h \in H_{m-1}$. Portanto, provamos assim que $(G_{m-1})_{f_{m-1}} = H_{m-1}$.

Repetindo esse processo indutivamente (para $f_{m-3}, f_{m-4}, ...f_0$), chegaremos que f_0 será idempotente central primitivo de $\mathbb{Q}G_0 = \mathbb{Q}G$.

Basta provar agora que $f_0 = e$: para isso, vamos provar que f_{m-2} é a soma de todos os G_{m-2}-conjugados de $f_m = \varepsilon(G_m, H_m)$, e o restante sai trivialmente por indução (seguindo os mesmos passos).

Vamos escrever $f_{m-1} = f_m^{h_1} + ... + f_m^{h_k}$ (soma de todos os G_{m-1}-conjugados de

f_m), $f_{m-2} = f_{m-1}^{s_1} + ... + f_{m-1}^{s_l}$ (soma de todos os G_{m-2}-conjugados de f_{m-1}). Então, temos que

$$f_{m-2} = \sum_{1 \leq i \leq k; 1 \leq j \leq l} f_m^{h_i s_j}. \tag{3.6}$$

Seja $x \in G_{m-2}$. Existe j tal que $f_{m-1}^{s_j} = f_{m-1}^{h_1^{-1}x}$ e, portanto, f_m^x é um termo da equação (3.6).

Agora basta provar que cada G_{m-2}-conjugado de f_m aparece uma única vez na soma (3.6). Para isso, vamos provar que são todos ortogonais:

Usando o mesmo argumento da prova do Lema 3.3.2, concluímos que $f_m^{h_a s_b} f_m^{h_c s_b} = 0$ (podemos fazer isso, pois a propriedade (4) implica que G_{i+1} é subgrupo normal de G_i), se $a \neq c$ e, além disso, pelo Lema 3.3.2, temos que $\left(\sum_{1 \leq i \leq k} f_m^{h_i s_b}\right)\left(\sum_{1 \leq i \leq k} f_m^{h_i s_d}\right) = 0$, se $b \neq d$. Daí, temos:

$$f_m^{h_\alpha s_b} f_m^{h_\beta s_d} = \left(f_m^{h_\alpha s_b}\left(\sum_{1 \leq i \leq k} f_m^{h_i s_b}\right)\right)\left(\left(\sum_{1 \leq i \leq k} f_m^{h_i s_d}\right) f_m^{h_\beta s_d}\right) = 0.$$

Continuando indutivamente com este argumento, concluímos que f_{m-i} é a soma de todos os G_{m-i}-conjugados de f_m e, portanto, concluímos que $f_0 = e$. (Obs.: além disso, também temos que os G-conjugados de f_m são ortogonais entre si).

Agora vamos provar que todo idempotente central primitivo é dessa forma.

Seja $e \in \mathbb{Q}G$ um idempotente central primitivo de $\mathbb{Q}G$. Tomemos $H_0 = G_e$ subgrupo normal de $G = G_0$ e temos que e é idempotente central primitivo de $(\mathbb{Q}G)\widehat{H_0} \simeq \mathbb{Q}(G_0/H_0)$.

Temos que $(G_0/H_0)_{\overline{e}} = \{1\}$. Como já sabemos, isto implica $\varepsilon(G_0/H_0) \neq 0$, que por sua vez, implica $Z(G_0/H_0)$ cíclico. Portanto, se G_0/H_0 for abeliano, então será cíclico. Pelo Corolário 3.2.7 teremos $\varepsilon(G_0, H_0)$ é idempotente central primitivo de $\mathbb{Q}G_0$ e, como $e = e\varepsilon(G_0, H_0)$, então $e = \varepsilon(G_0, H_0)$, que é do tipo desejado (isto é, é do tipo que satisfaz às propriedades do enunciado do teorema).

Se G_0/H_0 não for abeliano, ainda teremos que o seu centro é cíclico. Segue da proposição anterior que $\overline{e} \in \mathbb{Q}(G_0/H_0)$ é a soma de todos os (G_0/H_0)-conjugados de um

idempotente central primitivo e_1 de $\mathbb{Q}(G_1/H_0) \simeq (\mathbb{Q}G_1)\widehat{H_0}$ (através desse isomorfismo, podemos dizer que e é a soma dos G-conjugados de e_1), onde G_1 é um subgrupo de G tal que $G_1/H_0 = C_{G_0/H_0}(Z_2(G_0/H_0)) \neq G_0/H_0$, e $\cap_{x \in G_0/H_0}(H_1/H_0)^x = 1$, com H_1 um subgrupo de G contendo H_0 tal que $H_1/H_0 = (G_1/H_0)_{e_1} \triangleleft G_1/H_0$ (isso tudo nós temos pela proposição anterior!). Isto implica $H_1 \triangleleft G_1$ e, como $(G_1/H_1)_{e_1} = \{1\}$, temos que $Z(G_1/H_1)$ é cíclico. Portanto, se (G_1/H_1) é abeliano, então é cíclico (pois será igual ao seu centro, que é cíclico). Pelo Corolário 3.2.7, temos que $e_1 = \varepsilon(G_1, H_1)$ e segue o resultado, pois verificamos as propriedades de (1) a (5). Antes de continuarmos indutivamente, observemos o seguinte:

Obs.: temos que a classe de nilpotência de (G_1/H_0) é sempre estritamente menor que a de (G_0/H_0), pois (G_1/H_0) centraliza o segundo centro de (G_0/H_0). Além disso, como (G_1/H_1) é isomorfo a um quociente de (G_1/H_0), então se (G_1/H_0) for abeliano, (G_1/H_1) também será.

Agora continuemos com o próximo passo:

Se (G_1/H_1) não for abeliano, continuemos indutivamente da seguinte maneira: Já começaremos com $e_i \in \mathbb{Q}(G_i/H_i) \simeq (\mathbb{Q}G_i)\widehat{H_i}$ um idempotente central primitivo, e repetindo o argumento acima, obteremos que e_i é a soma de conjugados por G_i de um idempotente central primitivo e_{i+1} de (G_{i+1}/H_i), onde G_{i+1} é obtido de forma análoga à que obtivemos G_1 acima, e também obteremos analogamente H_{i+1} e, novamente, se G_{i+1}/H_{i+1} for abeliano, acaba (com as propriedades (1) a (5) verificadas neste passo e nos anteriores) e, se não for, repete o processo para $e_{i+1} \in (\mathbb{Q}G_{i+1})\widehat{H_{i+1}}$.

Este processo acabará pois, temos que a classe de nilpotência de G_{i+1}/H_i é estritamente menor que a de G_i/H_{i-1}, pois

$$G_{i+1}/H_i = C_{G_i/H_i}(Z_2(G_i/H_i)),$$

onde G_i/H_i é isomorfo a um quociente de G_i/H_{i-i}. E como já observamos de forma análoga acima, G_{i+1}/H_i abeliano implica G_{i+1}/H_{i+1} abeliano.

Quando o processo acabar, escreveremos e como uma soma do mesmo tipo que f_0 (da primeira parte da prova), ou seja, e é a soma de todos os G-conjugados de

$\varepsilon(G_m, H_m)$.

E o teorema está provado.

□

Segue da demonstração deste teorema que todos os G-conjugados de $\varepsilon(G_m, H_m)$ são dois a dois ortogonais.

E temos pela demonstração do Corolário 3.2.7 que os idempotentes $\varepsilon(G_m, H_m)$ são uma combinação $\mathbb{Z}$-linear de elementos do tipo $\widehat{H}$, com H subgrupo de G (pois G_m/H_m é cíclico).

Então, temos de forma imediata o seguinte corolário, que encerra esta seção:

Corolário 3.3.5 *Seja G um grupo nilpotente finito. Se e é um idempotente central primitivo de $\mathbb{Q}G$, então e é combinação $\mathbb{Z}$-linear de idempotentes do tipo $\widehat{H}$, onde H é um subgrupo de G.*

□

3.4 Calculando um Exemplo concreto

Como vimos no capítulo introdutório, os grupos multiplicativos $G = UT(n, F_q)$ (das matrizes unitriangulares $n \times n$ com entradas no corpo F_q) são todas nilpotentes de classe $(n-1)$, e que $Z_i(G)$ é o subgrupo composto das matrizes que têm entradas nulas nas $(n-i-1)$ diagonais logo acima da diagonal principal.

Nosso objetivo ao longo desta seção será utilizar o teorema principal da seção anterior para calcular os idempotentes centrais primitivos de $\mathbb{Q}G^p := \mathbb{Q}(UT(3, F_p))$, para todo p primo, utilizando para isso as relações que nós temos entre os subgrupos de $UT(3, F_p)$.

Sejam $(G_i), (H_i)$ sequências de subgrupos de G^p que satisfazem às condições do Teorema 3.3.4. Como $|G^p| = p^3$, temos que $|G_m| = 1, p, p^2$ ou p^3.

Primeiro caso: se $|G_m| < p^3$, então como $\frac{G_{m-1}}{H_{m-1}}$ não é abeliano (condição (3)), então $G_{m-1} = G^p$ e $H_{m-1} = \{1\}$ (pois todo grupo de ordem p ou p^2 é abeliano).

Além disso, como o grau de nilpotência de G^p é 2, então o de G_{m-1}/H_{m-1} é menor ou igual a 2. Daí, temos:

$$C_{\frac{G_{m-1}}{H_{m-1}}}(Z_2(G_{m-1}/H_{m-1})) = C_{\frac{G^p}{\{1\}}}(\frac{G^p}{\{1\}}) = Z(G)/\{1\},$$

de onde, pela propriedade (4), tiramos que $G_m = Z(G)$ um grupo de ordem p. Assim temos, a princípio, duas possibilidades para H_m: $H_m = \{1\}$ ou $H_m = G_m = Z(G)$. O segundo caso nos dá:

$$\bigcap_{x \in \frac{G_{m-1}}{H_{m-1}} = \frac{G^p}{G^p}} H_m^x = H_m = Z(G) \neq H_{m-1} = \{1\},$$

contradizendo a propriedade (5). Mas no caso $H_m = \{1\}$ temos:

$$\bigcap_{x \in \frac{G_{m-1}}{H_{m-1}} = \frac{G^p}{\{1\}}} H_m^x = \{1\} = H_{m-1}$$

.

Além disso, $Z(G_{m-1}/H_{m-1}) = Z(G^p/\{1\}) \simeq Z(G^p)$ é cíclico (satisfaz (2)). Portanto temos que a sequência $H_0 = \{1\} \subset H_1 = \{1\} \subset G_1 = Z(G^p) \subset G_0 = G^p$ satisfaz as hipóteses do Teorema 3.3.4.

Portanto, $\varepsilon(Z(G^p), \{1\}) = 1 - \widehat{Z(G^p)}$ é idempotente central primitivo de $\mathbb{Q}G^p$.

Segundo caso: se $|G_m| = p^3$. Vamos primeiro fazer um cálculo:

Seja $A = \begin{pmatrix} 1 & a_{12} & a_{13} \\ 0 & 1 & a_{23} \\ 0 & 0 & 1 \end{pmatrix} \in G^p$. Temos facilmente, por indução, que

$$A^n = \begin{pmatrix} 1 & na_{12} & na_{13} + \frac{p(p-1)}{2} a_{12}a_{23} \\ 0 & 1 & na_{23} \\ 0 & 0 & 1 \end{pmatrix}.$$

Portanto temos 2 subcasos a considerar:

$p \neq 2$**:** nesse caso, temos que $A^p = I$. Sendo assim, se $a_{12} \neq 0$ ou $a_{23} \neq 0$, então $\langle A \rangle$ é grupo cíclico de ordem p que não intersecta o centro, portanto, não pode ser normal. O outro subgrupo de ordem p é o próprio $Z(G)$, que é gerado por

$$g = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in G_p.$$

Também temos subgrupos de ordem p^2 (são todos normais, pois o quociente tem ordem prima): os gerados por A e g, onde g está definido logo acima e A é tal que a_{12} ou a_{23} é não nulo (podemos supor que $a_{13} = 0$). Temos $p+1$ subgrupos de ordem p^2 no total (os casos em que $a_{12} = 1$ e a_{23} percorre F_p juntos com o caso em que $a_{12} = 0$ e $a_{23} = 1$ são todos os casos possíveis).

Assim, temos uma descrição completa de todos os subgrupos de G^p (quando p é ímpar).

Lembramos que estamos no caso $G_m = G^p$. Pela propriedade (2), temos que H_m é normal em G_m. Assim, temos, a princípio, três possibilidades para H_m: $H_m = Z(G^p), \{1\}$ ou tem ordem p^2. Os dois primeiros casos não satisfazem às propriedades (2) e (3) pois G_m/H_m não será cíclico. Portanto, o único caso que ainda pode acontecer é H_m ter ordem p^2. Nesse caso, a sequência $H_0 \subset G_0$ (com m = 0) satisfaz às propriedades do Teorema 3.3.4.

Portanto, temos que $\varepsilon(G_m, H_m) = \varepsilon(G^p, H_m) = \widehat{H_m} - \widehat{G^p}$ são idempotentes centrais primitivos de $\mathbb{Q}G^p$.

Assim, terminamos de calcular todos os $(p+2)$ idempotentes centrais primitivos de $\mathbb{Q}G^p$ no caso de p ser primo ímpar:

$$e_1 = (1 - \widehat{Z(G^p)});$$

$$e_i = \widehat{H_i} - \widehat{G^p},$$

onde H_i é subgrupo de ordem p^2 de G^p (há $(p+1)$ tais subgrupos).

$p = 2$**:** pelos cálculos feitos acima, temos um subgrupo cíclico de ordem 4 gerado

por

$$h = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Também temos 5 subgrupos de ordem 2, sendo um deles $Z(G^2)$ e os outros quatro são os gerados por:

$$\begin{pmatrix} 1 & 1 & a_{13} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, a_{13} \in F_2;$$

$$\begin{pmatrix} 1 & 0 & a_{13} \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, a_{13} \in F_2.$$

Também temos mais 2 subgrupos (não-cíclicos) de ordem 4, gerados por um dos elementos acima e por $g = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ (nesse caso, pode supor $a_{13} = 0$, por isso que são apenas 2 subgrupos desse tipo).

Lembremos que estamos no caso $G_m = G^2$. Pelas propriedades (2) e (3) do Teorema 3.3.4, temos que (G_m/H_m) é cíclico e, portanto, os únicos candidatos a H_m possíveis são quando $|H_m| = 4$ (3 casos), ou $H_m = G_m$ (1 caso).

Em todos os casos listados acima, a sequência $H_0 \subset G_0$ (aqui $m = 0$) satisfaz as hipóteses do Teorema 3.3.4.

Portanto, encontramos assim os 5 idempotentes centrais primitivos de $\mathbb{Q}G^2$:

$$\widehat{G};$$

$$\widehat{H_i} - \widehat{G},$$

$$1 - \widehat{Z(G^2)}$$

onde $|H_i| = 4$ (há 3 subgrupos com 4 elementos, conforme vimos acima).

Assim, pudemos obter a partir das relações entre os subgrupos de $G^p = UT(3, F_p)$, usando o Teorema 3.3.4, todos os idempotentes centrais primitivos de $\mathbb{Q}(UT(3, F_p))$, para todo p primo, concluindo assim este capítulo.

Capítulo 4

Conclusões

Chegamos, assim, ao fim do objetivo principal do nosso trabalho.

4.1 Considerações Finais

No capítulo introdutório, pudemos ver alguns dos resultados e conceitos básicos da teoria de anéis de grupos e algumas aplicações da teoria no estudo de códigos cíclicos. Também vimos alguns conceitos básicos necessários acerca de caracteres em grupos abelianos finitos e acerca de grupos nilpotentes.

No capítulo seguinte, foi estudado um artigo em que, dentre outras coisas, estendeu resultados antes obtidos por Arora e Pruthi [**6**], por calcular idempotentes geradores de códigos abelianos minimais de certas álgebras de grupo.

No capítulo seguinte, estudamos uma descrição dos idempotentes centrais primitivos de álgebras racionais de grupos nilpotentes finitos, sem necessitar de usar a tabela de caracteres do grupo. Além disso, neste mesmo capítulo, também estudamos uma descrição dos idempotentes primitivos de álgebras racionais de grupos abelianos, diferente da que é feita por [**1**, Teorema vii.1.4], e concluindo logo em seguida que o suporte desses idempotentes são subgrupos do grupo abeliano em questão, além de esses idempotentes poderem ser escritos como uma soma de termos de um tipo particular.

Neste capítulo também listamos alguns resultados básicos de teoria de representações, e aplicamos estes resultados para obter os resultados principais do capítulo.

Também vale notar que calculamos um exemplo concreto (e já conhecido) utili-

zando o resultado principal do capítulo. ——-

Capítulo 5

Referências

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

[2] Jespers, E., Leal, G., Paques, A., *Central idempotents in the rational group algebra of a finite nilpotent group*, Journal of Algebra and Its Applications Vol. 2, No. 1 (2003) 57-62.

[3] Niven, I., Zuckerman, H.S., Montgomery, H.L., *An Introduction to the Theory of Numbers*, fifth ed., Wiley, 1991.

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

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

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

[7] Robinson, D.J.S., *A Course in the Theory of Groups*, Grad. Texts in Math., Springer-Verlag, New York, 1993.

[8] Roth, R., *Introduction to Coding Theory*, Cambridge University Press, New York, 2006.

[9] Rotman, J.J., *An Introduction to the Theory of Groups*, fourth ed., Grad. Texts in Math., vol. 148, Springer-Verlag, New York, 1995.

Índice Remissivo