UNIVERSIDADE FEDERAL DE MINAS GERAIS
INSTITUTO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA

Dissertação de Mestrado

O Problema do Isomorfismo para Álgebras de Grupos Racionais de p-Grupos Extra-Especiais

Allan Rodrigo Fonseca Teixeira

Orientadora: Ana Cristina Vieira

9 DE FEVEREIRO DE 2006

Lista de Símbolos

x^g	conjugado de x por g, ou seja, $g^{-1}xg$
$[x, y]$	comutador de x e y, i.e., $x^{-1}y^{-1}xy$
$[A, B]$	$\langle [a, b] \vert a \in A,\ b \in B \rangle$
G'	subgrupo derivado de G, ou seja, $[G, G]$
$\mathcal{Z}(G)$	centro do grupo G
$C_G(H)$	centralizador do subgrupo H em G
$\Phi(G)$	subgrupo de Frattini do grupo G
$\lhd$	subgrupo normal
$\lessdot$	subgrupo maximal
$\times$	produto direto
$\rtimes$	produto semi-direto
$\mathcal{C}_n$	grupo cíclico de ordem n
$cl(G)$	classe de nilpotência de G
$\mathcal{Z}_n(G)$	n-ésimo termo da série central superior de G
$\gamma_n(G)$	n-ésimo termo da série central inferior de G
$Aut(G)$	grupo dos automorfismos de G
C_g	classe de conjugação de $g \in G$
KG	álgebra de grupo sobre o corpo K
$\text{supp}(\alpha)$	suporte de α em KG, ou seja, $\{g \in G : \alpha_g \neq 0\}$
$M_n(A)$	anel de matrizes $n \times n$ com entradas em A
$\mathbb{H}$	álgebra dos quatérnios sobre $\mathbb{Q}$
ξ_n	n-ésima raiz primitiva da unidade
$char(K)$	característica do corpo K
$End_{KG}M$	anel dos endomorfismos do KG-módulo M
$m(M)$	índice de Schur de M
$[x]$	maior inteiro menor ou igual a x
$ker(\varphi)$	núcleo do homomorfismo φ
$G \approx H$	G é isomorfo a H.

Sumário

Resumo

Neste trabalho, baseado no artigo "Isomorphic Rational Group Algebras", de G. Leal e A. C. Vieira, estamos interessados na decomposição de Wedderburn das álgebras de grupos racionais de p-grupos extra-especiais. Explicitaremos suas componentes simples e responderemos a questão clássica sobre o problema do isomorfismo de anéis de grupos neste caso.

Abstract

In this work, based on the paper "Isomorphic Rational Group Algebras", by G. Leal and A. C. Vieira, we are interested in the Wedderburn decomposition of the rational group algebras of extra-special p-groups. We will give the explicit form of their simple components and answer the classical question about the isomorphism problem for group rings in this case.

Introdução

Neste trabalho consideramos R um anel com unidade, G, H grupos finitos, e trabalharemos com a seguinte questão clássica do problema do isomorfismo:

"Se RG é isomorfo à RH então G é isomorfo à H?"

No caso em que R é o corpo dos racionais $\mathbb{Q}$, já existem respostas positivas a esta questão, e outras negativas, para algumas classes de grupos. Nesta dissertação, pretendemos responder esta questão quando $R = \mathbb{Q}$ e G é um p-grupo extra-especial, baseando-nos no artigo [8].

Para obtermos tal resposta é necessário um bom entendimento de alguns fatos da Teoria de Grupos e particularidades dos grupos de nosso interesse, os p-grupos extra-especiais, que são p-grupos não-abelianos cujos centros e subgrupos derivados coincidem e têm a mesma ordem p.

No Capítulo 1, descrevemos alguns resultados gerais sobre p-grupos e resultados particulares sobre o subgrupo de Frattini e grupos nilpotentes que possibilitarão o entendimento da estrutura e a classificação de todos os p-grupos extra-especiais.

No Capítulo 2, daremos uma visão geral de fatos básicos sobre álgebras de grupos. Iniciamos o capítulo com algumas idéias sobre a teoria de anéis semisimples e com o Teorema de Maschke concluindo que a nossa álgebra de grupo $\mathbb{Q}G$ é um anel semisimples. Pelo Teorema de Wedderburn-Artin, temos conhecimento da estrutura desta álgebra de grupo. Em seguida, damos uma visão geral sobre elementos idempotentes em um anel,

suas propriedades e sua relação com os anéis semisimples, pois estes objetos são peças fundamentais para a decomposição de Wedderburn de uma tal álgebra. Encerramos este capítulo com uma discussão mais abrangente sobre o problema do isomorfismo, que foi inicialmente proposto por G. Higman, em 1940, a respeito de anéis de grupos sobre os inteiros.

No Capítulo 3, utilizamos todas as informações dos capítulos anteriores para atacarmos diretamente nosso problema. Na primeira seção, classificamos a componente comutativa da álgebra de grupos $\mathbb{Q}G$, no caso em que G é um p-grupo extra-especial, e conseguimos uma primeira abordagem ao problema do isomorfismo. Nas seções seguintes, classificamos a componente não-comutativa de $\mathbb{Q}G$, considerando dois casos: se p ímpar ou se $p = 2$, obtendo assim a decomposição de Wedderburn de $\mathbb{Q}G$. Finalmente, obtemos uma resposta ao problema do isomorfismo para álgebras de grupos racionais de p-grupos extra-especiais.

Completaremos o trabalho com algumas informações adicionais a respeito dos algoritmos implementados para exemplificar o teorema principal de [8] sobre o problema do isomorfismo para álgebras de grupos racionais de p-grupos nilpotentes de classe 2 com centro cíclico, cuja demonstração omitimos aqui.

Capítulo 1

Subgrupo de Frattini e Grupos Extra-Especiais

Neste capítulo, daremos algumas definições e resultados importantes para o desenvolvimento do nosso trabalho. Como veremos, o subgrupo de Frattini de um grupo G terá um papel fundamental no bom entendimento dos p-grupos extra-especiais, os quais formam um classe particular de grupos nilpotentes de classe 2. Reiteramos ainda que todos os grupos com os quais trabalharemos serão finitos.

1.1 O Subgrupo de Frattini

Definição 1.1 *O* ***subgrupo de Frattini*** *de um grupo G é a interseção de todos os subgrupos maximais de G.*

Denotamos esse subgrupo por $\Phi(G)$, ou seja, $\Phi(G) = \bigcap_{M \lneq G} M$. Observamos que $\Phi(G) \triangleleft G$ desde que é um subgrupo característico de G. Como exemplos temos $\Phi(S_3) = 1$, onde S_3 é o grupo simétrico de grau 3, enquanto que $\Phi(\mathcal{D}) = \mathcal{Z}(\mathcal{D}) = \mathcal{D}'$ e $\Phi(\mathcal{Q}) = \mathcal{Z}(\mathcal{Q}) = \mathcal{Q}'$, onde $\mathcal{D}$ é o grupo diedral de ordem 8 e $\mathcal{Q}$ é o grupo dos quatérnios.

Veremos que o subgrupo de Frattini de um grupo G é constituído por elementos não geradores de G. Consideremos a seguinte definição.

Definição 1.2 *Dizemos que um subgrupo próprio K de G é um* ***complemento parcial*** *de H em G se $G = HK$, onde $H \triangleleft G$.*

Teorema 1.1

(i) $G = \langle x_i |\, x_i \in G,\, 1 \leq i \leq n \rangle$ *se, e somente se,* $G = \langle \Phi(G), x_i |\, x_i \in G,\, 1 \leq i \leq n \rangle$. *Em particular, se* $G = \Phi(G) H$ *para algum subgrupo* H, *então* $G = H$.

(ii) Se $H \triangleleft G$ *então* H *possui um complemento parcial em* G *se, e somente se,* $H \not\subseteq \Phi(G)$.

Demonstração:

(i)

($\Rightarrow$) Imediato.

($\Leftarrow$) Assuma que $G = \langle \Phi(G), x_i |\, x_i \in G, 1 \leq i \leq n \rangle$ e suponha, por absurdo, que $\overline{G} = \langle x_i |\, x_i \in G, 1 \leq i \leq n \rangle \subsetneq G$. Logo $\overline{G} \subseteq M$, onde M é algum subgrupo maximal de G. Mas por definição temos que $\Phi(G) \subseteq M$, e assim $G = \langle \Phi(G), \overline{G} \rangle \subseteq M$, uma contradição.

(ii)

($\Leftarrow$) Suponha $H \triangleleft G$ e $H \not\subseteq \Phi(G)$. Assim, existe um subgrupo maximal M de G tal que $H \not\subseteq M$, logo $HM \supset M$. Mas pela maximalidade de M, $HM = G$ e, portanto, M é um complemento parcial de H em G.

($\Rightarrow$) Assuma que H tem um complemento parcial K em G e suponha, por absurdo, que $H \subseteq \Phi(G)$. Então $G = HK \subseteq \Phi(G) K$ e por (i) teríamos $G = K$, o que contradiz a definição de complemento parcial. ■

Corolário 1.2 *Se $G/\Phi(G)$ é cíclico então G é cíclico.*

Demonstração:

Tome $x \in G$ tal que $x\Phi(G)$ gere $G/\Phi(G)$. Logo $G = \langle \Phi(G), x \rangle$, pois todo elemento $g \in G$ é da forma $g = yx$, $y \in \Phi(G)$. Pelo teorema anterior, temos que $G = \langle \Phi(G), x \rangle = \langle x \rangle$, portanto G é cíclico. ■

Definição 1.3 *Um grupo no qual todos os seus elementos possuem ordem de uma potência de algum primo fixo p é chamado de um p-**grupo**.*

O próximo resultado é muito importante, pois classifica o grupo quociente de um p-grupo pelo seu subgrupo de Frattini.

Teorema 1.3 *Se G é um p-grupo então $G/\Phi(G)$ é um p-grupo abeliano elementar. Além disso, $\Phi(G) = 1$ se, e somente se, G é abeliano elementar.*

Demonstração:

Se M é maximal em G, então $M \lhd G$ e $[G : M] = p$. Logo $G' = [G, G] \subseteq M$, pois G/M é abeliano e $x^p \in M$, $\forall\, x \in G$. Mas isto vale para todo M maximal, ou seja, $G' \subseteq M$, $\forall\, M \lessdot G$ e, portanto, $G' \subseteq \Phi(G)$ e $x^p \in \Phi(G)$, $\forall\, x \in G$. Logo $G/\Phi(G)$ é abeliano elementar.

Em particular, se $\Phi(G) = 1$ então G é abeliano elementar. Por outro lado, se G é p-grupo abeliano elementar, então G possui uma base x_i, $1 \leq i \leq n$, ou seja, $G = \langle x_1, \ldots, x_n \rangle$, onde $x_i^p = 1$. Para cada $j = 1, \ldots, n$, considere o subgrupo $H_j = \langle x_i |\, 1 \leq i \leq n,\ i \neq j \rangle$ maximal em G. Assim, $\Phi(G) \subset \bigcap_{j=1}^{n} H_j = \{1\}$. Portanto, $\Phi(G) = \{1\}$. ■

Teorema 1.4 *Se G é um grupo arbritário e $N \lhd G$ então $\dfrac{\Phi(G)\,N}{N} \leq \Phi\left(\dfrac{G}{N}\right)$. Em particular, se $N \trianglelefteq \Phi(G)$ então $\dfrac{\Phi(G)}{N} = \Phi\left(\dfrac{G}{N}\right)$.*

Demonstração: Considere $\overline{G} = G/N$. Se $\overline{M} \lessdot \overline{G}$ então pelo Teorema da Correspondência, $\exists\ M \lessdot G$ com $(N \lhd M)$ tal que $\overline{M} = M/N$. Então $\Phi(G)\,N/N \leq M/N = \overline{M}$, $\forall\, \overline{M} \lessdot \overline{G}$. Logo

$$\frac{\Phi(G)\,N}{N} \leq \Phi\left(\frac{G}{N}\right).$$

Se $N \trianglelefteq \Phi(G)$, é claro que $\Phi\left(\dfrac{G}{N}\right) = \dfrac{\Phi(G)}{N}$. ■

1.2 Grupos Nilpotentes

Definição 1.4 *Um grupo G é dito* ***nilpotente*** *se G possui uma série de subgrupos tal que*

$$\{1\} \leq G_1 \leq \ldots \leq G_n = G,$$

onde

(i) $G_i \triangleleft G$ *(ou seja, a série é normal) e*

(ii) $G_{i+1}/G_i \leq \mathcal{Z}(G/G_i)$ *(ou seja, a série é central).*

Se G é um grupo nilpotente então sua classe de nilpotência, $cl(G)$, é o comprimento da menor série central de G. Observamos que, para $n \geq 3$, o grupo simétrico S_n não é nilpotente pois $\mathcal{Z}(S_n) = \{1\}$.

Definição 1.5 *A* ***série central inferior*** *de um grupo G é definida recursivamente por:*

(i) $\gamma_1(G) = G$ *e*

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

Observamos que o segundo termo da série central inferior de G é o seu subgrupo derivado, ou seja, $\gamma_2(G) = G' = [G, G]$. A série central inferior de um grupo G pode estabilizar antes de alcançar o subgrupo trival. Por exemplo, notamos que $\gamma_n(S_3) = A_3 \neq \{1\}$, para todo $n \geq 2$.

Definição 1.6 *A* ***série central superior*** *de um grupo G é definida recursivamente por:*

(i) $\mathcal{Z}_0(G) = \{1\}$, $\mathcal{Z}_1(G) = \mathcal{Z}(G)$ *e*

(ii) $\mathcal{Z}_{i+1}(G)/\mathcal{Z}_i(G) = \mathcal{Z}(G/\mathcal{Z}_i(G))$, *para* $i \geq 1$.

Da mesma forma que acontece para a série central inferior, a série central superior também pode estabilizar a partir de um determinado termo. Se $\mathcal{Z}_c(G) = G$ e $\mathcal{Z}_{c-1}(G) \neq G$ então G é nilpotente de classe igual a c. Do mesmo modo, se $\gamma_{d+1}(G) = \{1\}$ e

$\gamma_d(G) \neq \{1\}$ então G é nilpotente de classe igual a d. Além disso, temos o seguinte resultado, cuja demonstração pode ser encontrada em [3].

Teorema 1.5 *Se G é um grupo nilpotente então suas séries centrais inferior e superior têm o mesmo comprimento e este número é a classe de nilpotência de G.*

Exemplo:
Consideremos o grupo diedral de ordem 8 dado por $G = \langle a, b \mid a^4 = 1,\ b^2 = 1,\ a^b = a^{-1} \rangle$. Sua série central inferior é:

$$\gamma_1(G) = G,\ \gamma_2(G) = [G, G] = \langle a^2 \rangle,\ \gamma_3(G) = [G, [G, G]] = \{1\}$$

e sua série central superior é:

$$\mathcal{Z}_0(G) = \{1\},\ \mathcal{Z}_1(G) = \langle a^2 \rangle,\ \mathcal{Z}_2 = G.$$

Desta forma, G é nilpotente de classe 2.

Para nosso trabalho, estaremos muito interessados em grupos nilpotentes de classe 2. Por definição, neste caso, as séries centrais inferior e série superior têm comprimento 2. Assim, olhando para a série central superior, temos $\mathcal{Z}_2(G) = G$. Logo $\frac{G}{\mathcal{Z}(G)} = \frac{\mathcal{Z}_2(G)}{\mathcal{Z}(G)} = \mathcal{Z}\left(\frac{G}{\mathcal{Z}(G)}\right)$ e então $\frac{G}{\mathcal{Z}(G)}$ é abeliano. Portanto $G' \leq \mathcal{Z}(G)$. Reciprocamente, se G é um grupo tal que $1 \neq G' \leq \mathcal{Z}(G)$, então obviamente G é nilpotente de classe 2.

Exploremos agora mais alguns resultados sobre grupos nilpotentes.

Teorema 1.6 *Se G é um p-grupo finito então G é nilpotente.*

Demonstração: O centro de um p-grupo finito é não trival, para maiores detalhes veja [3]. Como todo grupo quociente de G também é um p-grupo, segue que $\mathcal{Z}_{i-1}(G) \subsetneq \mathcal{Z}_i(G)$ para todo inteiro positivo i. Como G é finito, então existe um inteiro n tal que $\mathcal{Z}_n(G) = G$ e, portanto, G é nilpotente. ■

Teorema 1.7 *Sejam G um grupo nilpotente finito e $\{1\} \neq H \triangleleft G$. Então $H \cap \mathcal{Z}(G) \neq \{1\}$.*

Demonstração: Se G é um grupo nilpotente finito então $G = \mathcal{Z}_n(G)$ para algum n. Logo existe um menor inteiro i tal que $H \cap \mathcal{Z}_i(G) \neq \{1\}$, com $i \geq 1$. Como $H \triangleleft G$, temos $[H, G] \trianglelefteq H$ e, por definição, $[\mathcal{Z}_i(G), G] \leq \mathcal{Z}_{i-1}(G)$. Portanto

$$[H \cap \mathcal{Z}_i(G), G] \leq H \cap \mathcal{Z}_{i-1}(G) = \{1\}.$$

Assim, $\{1\} \neq H \cap \mathcal{Z}_i(G) \leq \mathcal{Z}(G)$. Desde que $H \cap \mathcal{Z}(G) \leq H \cap \mathcal{Z}_i(G)$ obtemos que $H \cap \mathcal{Z}(G) = H \cap \mathcal{Z}_i(G) \neq \{1\}$. ■

1.3 Grupos Extra-Especiais

Definiremos agora uma classe particular de grupos nilpotentes de classe 2 com a qual trabalharemos no Capítulo 3, com a intenção de explicitar as componentes simples de sua álgebra de grupo racional.

Definição 1.7 *Um p-grupo G é **extra-especial** se é não abeliano, $G' = \mathcal{Z}(G)$ e $|\mathcal{Z}(G)| = p$.*

Devido ao fato de $\mathcal{Z}(G) = G'$, temos que o grupo quociente $G/\mathcal{Z}(G)$ é abeliano. Mas temos que $x^p \in \mathcal{Z}(G)$, para todo $x \in G$, ou seja, $[x^p, y] = 1$, para todo $x,\ y \in G$. De fato, observemos que

$$[x^2, y] = [x, y]^x [x, y] = x^{-1}[x, y]x[x, y] = [x, y][x, y] = [x, y]^2,\ \forall\ x, y \in G.$$

Por indução, obtemos $[x^n, y] = [x, y]^n$, para todo $x, y \in G$.
Como $|G'| = p$, concluímos que $[x^p, y] = [x, y]^p = 1$, para todo $x, y \in G$. Com isso, $G/\mathcal{Z}(G)$ é abeliano elementar. Assim, aplicando o Teorema 1.3, temos

$$\Phi\left(\frac{G}{\mathcal{Z}(G)}\right) = \overline{1}. \tag{1.1}$$

Por outro lado, como G é não abeliano temos $G' \neq 1$ e pelo Teorema 1.3, temos que $G' \subseteq \Phi(G)$. Mas como $G' = \mathcal{Z}(G)$ concluímos que $\mathcal{Z}(G) \subseteq \Phi(G)$. Agora, pelo Teorema 1.4 e por (1.1), temos

$$\Phi\left(\frac{G}{\mathcal{Z}(G)}\right) = \frac{\Phi(G)}{\mathcal{Z}(G)} = \overline{1} \Rightarrow \Phi(G) = \mathcal{Z}(G).$$

Desta forma, em um p-grupo extra-especial G, temos que $G' = \mathcal{Z}(G) = \Phi(G)$ tem ordem p. Notemos ainda que G é um grupo nilpotente de classe 2.

Exemplos de p-grupos extra-especiais:
Para apresentar um conjunto de exemplos provaremos o seguinte resultado.

Teorema 1.8 *Todo grupo não abeliano de ordem p^3 é extra-especial.*

Demonstração: Se G é um grupo não abeliano de ordem p^3, queremos mostrar que $\mathcal{Z}(G) = G'$ e $|\mathcal{Z}(G)| = p$. Temos as seguintes possibilidades para a ordem de $\mathcal{Z}(G)$:

$$|\mathcal{Z}(G)| = 1,\ p,\ p^2 \text{ ou } p^3.$$

Mas $|\mathcal{Z}(G)| \neq 1$ pois todo p-grupo tem centro não trivial (veja [3]). Se $|\mathcal{Z}(G)| = p^3$, então G seria abeliano, contradizendo a hipótese. Se $|\mathcal{Z}(G)| = p^2$, então $G/\mathcal{Z}(G)$ é cíclico, o que é uma contradição. Logo $|\mathcal{Z}(G)| = p$. Assim $|G/\mathcal{Z}(G)| = p^2$ e como todo grupo de ordem p^2 é abeliano, temos $G/\mathcal{Z}(G)$ abeliano. Logo $G' \leq \mathcal{Z}(G)$. Agora, desde que G é não abeliano, temos $G' \neq 1$. Portanto $G' = \mathcal{Z}(G)$. ■

Os primeiros exemplos de p-grupos extra-especiais são $\mathcal{D}$ (diedral de ordem 8) e $\mathcal{Q}$ (quatérnios). Para estes grupos, deste momento em diante, utilizaremos as seguintes apresentações:

$$\mathcal{D} = \left\langle a, b \mid a^2 = 1,\ b^2 = 1,\ (ab)^4 = 1 \right\rangle \tag{1.2}$$

$$\mathcal{Q} = \left\langle a, b \mid a^4 = 1,\ b^2 = a^2,\ a^b = a^{-1} \right\rangle. \tag{1.3}$$

Temos $\mathcal{Z}(\mathcal{D}) = \mathcal{D}' = \langle (ab)^2 \rangle$ e $\mathcal{Z}(\mathcal{Q}) = \mathcal{Q}' = \langle a^2 \rangle = \langle [a, b] \rangle$.

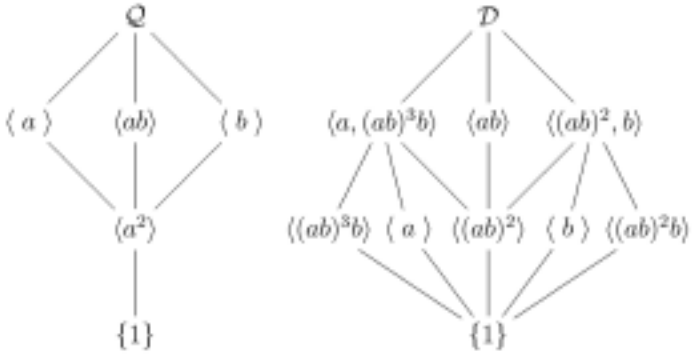

Figura 1.1: Reticulados dos grupos Quatérnios e Diedral

Agora, para p ímpar, construiremos p-grupos não abelianos de ordem p^3 e, pelo Teorema 1.8, esses grupos serão extra-especiais.

Contruiremos um grupo $\mathcal{N}$ de ordem p^3 através de um produto semi-direto de $G = \mathcal{C}_{p^2} = \langle x \rangle$ por $H = \mathcal{C}_p = \langle y \rangle$, definindo uma ação não trivial de H sobre G, ou seja,

$$\mathcal{N} = \mathcal{C}_{p^2} \rtimes \mathcal{C}_p.$$

A ação φ de H sobre G será dada por conjugação, definida como:

$$\begin{aligned} \varphi : H &\longrightarrow Aut(G) \\ y &\longmapsto \varphi_y : G \longrightarrow G \\ & \qquad\quad x \longmapsto x^{p+1} \end{aligned}$$

Podemos dar uma apresentação para $\mathcal{N}$ por:

$$\mathcal{N} = \left\langle x, y \mid x^{p^2} = 1,\ y^p = 1,\ x^y = x^{p+1} \right\rangle.$$

De maneira análoga, construiremos um grupo $\mathcal{M}$ que será dado através do produto semi-direto de $G = \mathcal{C}_p \times \mathcal{C}_p = \langle x \rangle \times \langle z \rangle$ por $H = \mathcal{C}_p = \langle y \rangle$. Assim

$$\mathcal{M} = (\mathcal{C}_p \times \mathcal{C}_p) \rtimes \mathcal{C}_p.$$

Definiremos a ação φ de H sobre G por:

$$\begin{aligned} \varphi : H &\longrightarrow Aut(G) \\ y &\longmapsto \varphi_y : G \longrightarrow G \\ & \qquad\quad x \longmapsto xz \\ & \qquad\quad z \longmapsto z \end{aligned}$$

Desta maneira temos que $x^y = xz$ e z comuta com y. Portanto, uma apresentação para $\mathcal{M}$ é

$$\mathcal{M} = \langle x, y, z \mid x^p = y^p = z^p = 1,\ [x,y] = z,\ [x,z] = [z,y] = 1 \rangle .$$

Antes de classificarmos todos os p-grupos extra-especiais de ordem p^3, precisamos do seguinte lema técnico.

Lema 1.9 *Se G é um p-grupo extra-especial com $\mathcal{Z}(G) = \langle z \rangle = [x,y]$ e $x, y \in G$, então, para todo inteiro i, temos*

(i) $x^i y = z^i y x^i$ *e*

(ii) $(yx)^i = z^{\frac{1}{2}(i-1)i} y^i x^i$.

Demonstração:
(i) Temos $[x,y] = z$, onde $z \in \mathcal{Z}(G)$. Logo $y^{-1}xy = zx$ e portanto $(y^{-1}xy)^i = z^i x^i$. Assim, $y^{-1}x^i y = z^i x^i$, ou seja, $x^i y = z^i y x^i$.
(ii) Faremos a demonstração por indução. Para $i = 1$, é claro o resultado. Suponha que o resultado seja válido para $i-1$. Logo $(yx)^i = (yx)^{i-1}(yx) = z^{\frac{1}{2}(i-1)(i-2)} y^{i-1} x^{i-1} yx$. Por (i) temos $x^{i-1}y = z^{i-1} y x^{i-1}$. Assim, $(yx)^i = z^{\frac{1}{2}(i-1)(i-2)} y^{i-1} z^{i-1} y x^{i-1} x = z^{\frac{1}{2}(i-1)i} y^i x^i$.

■

Classificação dos p-grupos extra especiais:

Agora, vamos garantir que os grupos $\mathcal{D}$, $\mathcal{Q}$, $\mathcal{M}$ e $\mathcal{N}$ são os únicos grupos extra-especiais de ordem p^3, ou seja, vamos provar o seguinte teorema:

Teorema 1.10 *Seja G um grupo não abeliano tal que $|G| = p^3$.*

(i) Se $p = 2$, então $G \approx \mathcal{D}$ ou $G \approx \mathcal{Q}$

(ii) Se p é ímpar, então $G \approx \mathcal{M}$ ou $G \approx \mathcal{N}$.

Demonstração: A demonstração será dividida em duas partes. Classificaremos os grupos que contém um subgrupo cíclico de ordem p^2 e os grupos de expoente p.

1^a parte:

Suponha que G contenha um subgrupo cíclico H de ordem p^2. Assim $H \lhd G$, $H = \langle x \rangle$, e G/H é cíclico de ordem p.

Considere p ímpar. Seja $u \in G \backslash H$. Pelo Teorema 1.8, G é extra-especial, logo $[x, u] = z \in \mathcal{Z}(G)$ e $\mathcal{Z}(G) = \langle z \rangle = \langle x^p \rangle$. Então $[x, u^i] = z^i = x^p$, para algum $i \in \mathbb{Z}$. Note que $u^i \notin H$, pois caso contrário teríamos $[x, u^i] = 1$. Tomemos $v = u^i$. Assim $[x, v] = x^p$ e daí $x^v = x^{1+p}$. Como x é gerador de um subgrupo maximal de G e $v \notin H$, temos $G = \langle x, v \rangle$. Observe que $v^p \in H$ mas não gera H, pois caso contrário G seria cíclico, o que é um absurdo. Logo $v^p = x^{ap}$, para algum $a \in \mathbb{Z}$. Tomemos $y = vx^{-a}$. Por p ser ímpar e pelo Lema 1.9, $y^p = z^{\frac{1}{2}(p-1)p} v^p x^{-ap} = 1$. Temos também que $x^y = x^{vx^{-a}} = x^{1+p}$. Portanto, $G = \langle x, y \rangle$ e $G \approx \mathcal{N}$.

Se $p = 2$ então $|H| = 4$ e, sendo G um p-grupo extra-especial, temos $\mathcal{Z}(G) = \langle x^2 \rangle$. Tomemos $y \in G \backslash H$. Logo $[x, y] = x^2$, então $x^y = x^{-1}$. Como $G/\mathcal{Z}(G)$ é 2-grupo abeliano elementar, temos $y^2 \in \mathcal{Z}(G)$. Logo $y^2 = x^{2a}$, para algum $a \in \mathbb{Z}$. Se a for par, implica que $y^2 = 1$ e portanto $G \approx \mathcal{D}$, enquanto que, para a ímpar, temos $y^2 = x^2$ e $G \approx \mathcal{Q}$.

2^a parte:

Suponha que G tenha expoente p. Neste caso, p é ímpar, pois caso contrário G seria abeliano. Se H é um subgrupo maximal de G, então $|H| = p^2$ e H é p-grupo abeliano elementar do tipo (p, p). Temos que $H \lhd G$ e assim, pelo Teorema 1.7, $H \cap \mathcal{Z}(G) \neq 1$. Logo $\mathcal{Z}(G) \subset H$, pois $|\mathcal{Z}(G)| = p$. Tomemos $y \in G \backslash H$ e $x \in H \backslash \mathcal{Z}(G)$. Assim, $[x, y] = z \in \mathcal{Z}(G)$. Portanto, $G = \langle z, x, y \rangle \approx \mathcal{M}$. ■

Nosso interesse, a partir de agora, é obter uma classificação geral para todos os p-grupos extra-especiais. Para isso precisaremos do seguinte resultado.

Teorema 1.11 *Seja P um subgrupo extra-especial de um p-grupo G tal que $[G, P] \subseteq \mathcal{Z}(P)$. Então $G = P\, C_G(P)$.*

Demonstração: É suficiente mostrar que dado $x \in G$, existe $y \in P$ tal que xy^{-1} centraliza P, assim $u = xy^{-1} \in C_G(P)$ e então $x = uy$, ou seja, $x = uy$, com $u \in C_G(P)$. Mostraremos esse fato através de automorfismos. Sejam $x \in G$ e ϕ_x o automorfismo

interno induzido pela conjugação por x. Por hipótese $[G, P] \subseteq \mathcal{Z}(P)$, logo se $a \in P$ então $[a, x] = a^{-1}a^x \in \mathcal{Z}(P)$. Desta forma, $a^x\mathcal{Z}(P) = a\mathcal{Z}(P)$, ou seja, ϕ_x age trivialmente sobre $P/\mathcal{Z}(P)$. Vamos ver qual a consequência deste fato.

Suponha que ψ seja um automorfismo de G que age trivialmente sobre $P/\mathcal{Z}(P)$, vamos ver que ψ é automorfismo interno de P, ou seja, existe $y \in P$ tal que $\psi = \phi_y$. Sabemos que $P/\mathcal{Z}(P) \approx P/\Phi(P)$ é um p-grupo abeliano elementar, pelo Teorema 1.3, ou seja, $P/\mathcal{Z}(P) = \underbrace{C_p \times \ldots \times C_p}_{n \text{ vezes}}$. Seja $\{x_i\mathcal{Z}(P)\}_{1 \leq i \leq n}$ uma base de $P/\mathcal{Z}(P)$, onde $x_i \in P$. Por hipótese $\mathcal{Z}(P) = \langle z \rangle$, $|z| = p$ e $|P| = p^{n+1}$. Como ψ age trivialmente sobre $P/\mathcal{Z}(P)$ temos $\psi(x_i) = x_i z^{a_i}$, $0 \leq a_i < p$. Portanto teremos no máximo p^n automorfismos distintos que agem trivialmente sobre $P/\mathcal{Z}(P)$.

Por outro lado, se $\mathcal{U} = \{u_j\}_{1 \leq j \leq p^n}$, é um conjunto completo de representantes das classes laterais de $\mathcal{Z}(P)$ em P, então cada u_j corresponde a um automorfismo interno ϕ_{u_j} de P, e portanto atua trivialmente sobre $P/\mathcal{Z}(P)$. De fato, como $P' = \mathcal{Z}(P)$, temos $[b, u_j] \in \mathcal{Z}(P)$, onde $b \in P$. Assim, $b^{-1}b^{u_j} \in \mathcal{Z}(P)$, ou seja, $b^{u_j}\mathcal{Z}(P) = b\mathcal{Z}(P)$. Logo, $\phi_{u_j}(b)\mathcal{Z}(P) = b\mathcal{Z}(P)$, para todo $b \in P$. Além disso, $\phi_{u_j} \neq \phi_{u_k}$, se $j \neq k$, $u_j,\ u_k \in \mathcal{U}$. Isto é claro, pois se $\phi_{u_j} = \phi_{u_k}$ teríamos $u_j\mathcal{Z}(P) = u_k\mathcal{Z}(P)$. Com isso, u_j e u_k representariam a mesma classe, o que é um absurdo. Portanto, os automorfismos de P são dados por p^n automorfismos internos de P que atuam trivialmente sobre $P/\mathcal{Z}(P)$. Assim, $\psi = \phi_{u_l}$ para algum l.

Assim, considerando $\psi = \phi_x$, temos $\phi_x = \phi_y$ sobre P, para algum $y \in P$. Então $\phi_x(a) = \phi_y(a)$, para todo $a \in P$, isto é, $a^{xy^{-1}} = a$, para todo $a \in P$. Portanto, $u = xy^{-1} \in C_G(P)$ e segue o resultado. ■

Definição 1.8 *Dizemos que um grupo G é o* ***produto central*** *de seus subgrupos G_i, para $1 \leq i \leq n$, se*

(i) $G = \langle G_i \mid 1 \leq i \leq n \rangle$, *com* $[G_i, G_j] = 1$ *e*

(ii) $\mathcal{Z}(G) = \mathcal{Z}(G_i)$, *para todo* $1 \leq i \leq n$.

Agora, já possuímos todas as ferramentas para classificarmos todos os p-grupos extra-especiais.

Teorema 1.12 *Um p-grupo extra-especial G é o produto central de $r \geq 1$ subgrupos não abelianos de ordem p^3. Além disso, temos*

(i) Se p é ímpar, G é isomorfo à $\mathcal{N}^k\mathcal{M}^{r-k}$, enquanto se $p = 2$, G é isomorfo à $\mathcal{D}^k\mathcal{Q}^{r-k}$, para algum k. Em ambos os casos $|G| = p^{2r+1}$.

(ii) Se p é ímpar e $k \geq 1$, $\mathcal{N}^k\mathcal{M}^{r-k}$ é isomorfo à $\mathcal{N}\mathcal{M}^{r-1}$ e os grupos $\mathcal{M}^r$ e $\mathcal{N}\mathcal{M}^{r-1}$ não são isomorfos.

(iii) Se $p = 2$, então $\mathcal{D}^k\mathcal{Q}^{r-k}$ é isomorfo à $\mathcal{D}\mathcal{Q}^{r-1}$ se k for ímpar e à $\mathcal{Q}^r$ se k for par e os grupos $\mathcal{Q}^r$ e $\mathcal{D}\mathcal{Q}^{r-1}$ não são isomorfos.

Demonstração: Durante toda a demonstração, os produtos considerados são centrais. (i) Para $x \in G\backslash\mathcal{Z}(G)$, existe $y \in G$ tal que $[x, y] = z \neq 1$. Então $\langle z\rangle = \mathcal{Z}(G)$ pois $G' = \mathcal{Z}(G)$ possui ordem p. Além disso, x^p, $y^p \in \mathcal{Z}(G)$, pois $G/\mathcal{Z}(G)$ é abeliano elementar. Então $G_1 = \langle x, y, z\rangle$ é não abeliano de ordem p^3. Pelo Teorema 1.8, G_1 é extra-especial. Como $[G, G_1] \subset [G, G] = \mathcal{Z}(G) = \mathcal{Z}(G_1)$. Pelo Teorema 1.11, temos $G = G_1R_1$, onde $R_1 = C_G(G_1)$. Como R_1 centraliza G_1, $\mathcal{Z}(R_1) \subseteq \mathcal{Z}(G)$ e então $\mathcal{Z}(R_1) = \mathcal{Z}(G)$. Assim, temos as seguintes possibilidades: ou $R_1 = \mathcal{Z}(R_1) \subseteq G_1$ e então $G = G_1$, ou R_1 é não abeliano. No primeiro caso o teorema está demonstrado. Caso R_1 seja não abeliano, temos $R_1' = G' = \mathcal{Z}(G)$. Conseqüentemente, R_1 é extra-especial. Trabalhando indutivamente podemos repetir esse processo e concluir que R_1 é o produto central de G_i, $2 \leq i \leq r$, subgrupos não abelianos de ordem p^3. Logo G é o produto central de subgrupos G_i, $1 \leq i \leq r$, onde abaixo temos $G_i \cap R_i = \mathcal{Z}(R_i)$ de ordem p:

$$|G| = \frac{|G_1| \cdot |R_1|}{|G_1 \cap R_1|} = \frac{|G_1|}{|G_1 \cap R_1|}\frac{|G_2| \cdot |R_2|}{|G_2 \cap R_2|} = \ldots = \frac{|G_1| \ldots |G_r|}{|G_1 \cap R_1| \ldots |G_{r-1} \cap R_{r-1}|} = \frac{p^{3r}}{p^{r-1}} = p^{2r+1}.$$

Concluímos que cada G_i é isomorfo à $\mathcal{M}$ ou $\mathcal{N}$ se p é ímpar e à $\mathcal{D}$ ou $\mathcal{Q}$ se $p = 2$, usando o Teorema 1.10.

(ii) Como $\mathcal{M}$ tem expoente p e as componentes de $\mathcal{M}^r$ comutam, segue que $\mathcal{M}^r$ possui expoente p. De forma análoga, temos que $\mathcal{N}\mathcal{M}^{r-1}$ possui expoente p^2, logo $\mathcal{N}\mathcal{M}^{r-1}$ não é isomorfo à $\mathcal{M}^r$.

Para mostrar que $\mathcal{N}^k\mathcal{M}^{r-k}$ e $\mathcal{N}\mathcal{M}^{r-1}$ são isomorfos para todo k, mostraremos que

$\mathcal{N}^2 \approx \mathcal{N}\mathcal{M}$. Seja $G = \mathcal{N}^2$ com geradores x_1, y_1, x_2, y_2 onde $\langle x_1, y_1\rangle$ centraliza $\langle x_2, y_2\rangle$, $|x_i| = p^2$, $|y_i| = p$ e $x_i^{y_i} = x_i^{1+p}$, $1 \leq i \leq 2$. Além disso, $\langle x_1^p\rangle = \langle x_2^p\rangle = \mathcal{Z}(G)$. Substituindo x_2 por uma potência apropriada, podemos supor que $x_1^p = x_2^p$. Definindo $u_2 = x_2x_1^{-1}$, temos $u_2^p = (x_2x_1^{-1})^p = x_2^p(x_1^p)^{-1} = 1$. E como y_2 não centraliza u_2 então $G_1 = \langle y_2, u_2\rangle$ é isomorfo à $\mathcal{M}$. Mas pela prova de (i), $G = G_1G_2$, onde G_2 é também extra-especial de ordem p^3. Se G_2 fosse isomorfo à $\mathcal{M}$, então G seria isomorfo à $\mathcal{M}^2$ e teria expoente p, absurdo. Portanto, G_2 é isomorfo à $\mathcal{N}$ e $G = \mathcal{N}^2 \approx \mathcal{N}\mathcal{M}$, como queríamos.

(iii) Suponha que $p = 2$. Mostraremos que $\mathcal{D}^2$ e $\mathcal{Q}^2$ são isomorfos. Se $G = \mathcal{Q}^2$, então $G = \langle x_1, y_1, x_2, y_2\rangle$ com $\langle x_1, y_1\rangle$ centralizando $\langle x_2, y_2\rangle$, $x_i^{y_i} = x_i^{-1}$, $x_i^2 = y_i^2 = z$ e $z^2 = 1$, $1 \leq i \leq 2$. Seja $G_1 = \langle x_1, y_1x_2\rangle$ e $G_2 = \langle x_2, y_2x_1\rangle$. Então y_1x_2 e y_2x_1 são cada um de ordem 2. Conseqüentemente G_1 e G_2 são ambos isomorfos à $\mathcal{D}$. Como x_1 centraliza x_2 e y_2 temos que também centraliza G_2. Analogamente, y_1x_2 centraliza x_2. Finalmente, $(y_2x_1)^{y_1x_2} = y_2^{y_1x_2}x_1^{y_1x_2} = y_2^{x_2}x_1^{y_1} = y_2^{-1}x_1^{-1} = (zy_2)(zx_1) = y_2x_1$. Assim, y_2x_1 e y_1x_2 também comutam, logo G_1 centraliza G_2. Concluímos que $\mathcal{Q}^2$ e $\mathcal{D}^2$ são isomorfos. Isto implica que $\mathcal{D}^k\mathcal{Q}^{r-k} \approx \mathcal{D}\mathcal{Q}^{r-1}$, se k for ímpar, e $\mathcal{D}^k\mathcal{Q}^{r-k} \approx \mathcal{Q}^r$, se k for par.
Falta mostrar que $\mathcal{D}\mathcal{Q}^{r-1}$ não é isomorfo à $\mathcal{Q}^r$. Demonstraremos esse fato contando a quantidade de subgrupos cíclicos de ordem 4 existentes em cada grupo e veremos quantidades diferentes, logo os grupos não serão isomorfos. Considere $\mathcal{Q}^r = \mathcal{Q}_1\mathcal{Q}_2\ldots\mathcal{Q}_r$, e $\mathcal{Z}(\mathcal{Q}^r) = \langle z\rangle$. Seja $\langle x\rangle$ um subgrupo cíclico de ordem 4 de $\mathcal{Q}^r$ e $x = x_1\ldots x_r \in \mathcal{Q}^r$ com $x_i \in \mathcal{Q}_i$, para $1 \leq i \leq r$. Assim, podemos reescrever x como

$$x = z^a x_{i_1}\ldots x_{i_h}, \text{ com } x_{i_j} \in \mathcal{Q}_{i_j} - \langle z\rangle, \text{ para } 1 \leq j \leq h \tag{1.4}$$

e $a = 0$ ou 1. Se $a = 1$, então $zx_{i_1} = x_{i_1}^{-1} \in \mathcal{Q}_{i_1} - \langle z\rangle$. Por outro lado se $i_j \neq i_k$ para $j \neq k$, então x_{i_j} e x_{i_k} comutam. Assim, $x^2 = z^h$ e, conseqüentemente, x tem ordem 4 se, e somente se, h é ímpar. Além disso, sendo h ímpar, $x^{-1} = x_{i_1}^{-1}x_{i_2}^{-1}\ldots x_{i_h}^{-1} = x_{i_1}^{-1}x_{i_2}\ldots x_{i_h}$. De forma análoga, se substituirmos x_{i_k} por $x_{i_k}^{-1}$ obtemos x^{-1}, para $1 \leq k \leq h$, e sabemos também que $\langle x\rangle = \langle x^{-1}\rangle$.

Para uma dada escolha de índices $i_1,\ i_2,\ \ldots,\ i_h$, com h ímpar, pela análise acima dentre os 6 elementos em $\mathcal{Q}_{i_k} - \langle z\rangle$ podemos escolher 3 elementos para gerar o subgrupos cíclicos de ordem 4, pois seus inversos geram o mesmo subgrupo. Então temos 3^h subgrupos cíclicos de ordem 4 em $\mathcal{Q}$. Mas o conjunto de índices determina um conjunto distinto de subgrupos cíclicos de ordem 4. Concluímos que o número total m de subgrupos cíclicos de ordem 4 em $\mathcal{Q}^r$ será

$$m = \sum_h 3^h \binom{r}{h}, \tag{1.5}$$

onde h ímpar e $1 \leq h \leq r$. Utilizando a fórmula binomial para (1.5), temos

$$m = \frac{1}{2}\{(1+3)^r - (1-3)^r\} = \frac{1}{2}\{2^{2r} - (-2)^r\}. \tag{1.6}$$

Contemos agora a quantidade de subgrupos cíclicos de ordem 4 em $\mathcal{D}\mathcal{Q}^{r-1}$. Consideremos $\mathcal{D}\mathcal{Q}^{r-1} = \mathcal{D}\mathcal{Q}_2 \ldots \mathcal{Q}_r$, $\mathcal{Z}\left(\mathcal{D}\mathcal{Q}^{r-1}\right) = \langle z\rangle$ e $\mathcal{D} = \langle \overline{x}, \overline{y}\rangle$. Seja $\langle x\rangle$ um subgrupo cíclico de ordem 4 de $\mathcal{D}\mathcal{Q}^{r-1}$. Logo $x = x_1 x_2 \ldots x_r$, com $x_1 \in \mathcal{D}$, $x_i \in \mathcal{Q}_i$, para $2 \leq i \leq r$. Reescrevendo x, temos $x = z^a x_{i_1} x_{i_2} \ldots x_{i_h}$, onde $x_{i_j} \in \mathcal{Q}_{i_j} - \langle z\rangle \cup \mathcal{A}$, para $1 \leq j \leq h$ e $\mathcal{A} = \{\overline{x}, \overline{y}, \overline{x}\ \overline{y}\}$. Faremos nossa contagem em duas partes. Contaremos a quantidade de subgrupos cíclicos de ordem 4 em que $x_{i_j} \notin \mathcal{D}$, para todo $1 \leq j \leq h$, isto é, estaremos contando os subgrupos cíclicos de ordem 4 nos quais seus geradores são constituídos por apenas elementos em $\mathcal{Q}_j$, para $2 \leq j \leq r-1$. Assim, vale a análise já feita acima, pois estamos contando a quantidade de subgrupos cíclicos de ordem 4 em $\mathcal{Q}^{r-1}$ e por (1.6) temos que o número de tais subgrupos é

$$n_1 = \frac{1}{2}\{2^{2(r-1)} - (-2)^{r-1}\}. \tag{1.7}$$

Nos resta contar os sugbrupos cíclicos de ordem 4 que possuam $x_{i_1} \in \mathcal{A}$. Assim

$$x = z^a x_{i_1} x_{i_2} \ldots x_{i_h},\ x_{i_1} \in \mathcal{A},\ \text{com } x_{i_j} \in Q_j - \langle z\rangle,\ \text{para } 2 \leq j \leq h \tag{1.8}$$

com $a = 1$ ou 0. Se $a = 1$, então $z x_{i_2} = x_{i_2}^{-1} \in Q_{i_2} - \langle z\rangle$. Por outro lado se $i_j \neq i_k$ para $j \neq k$ temos que x_{i_j} e x_{i_k} comutam. Mas $x_{i_1} \in \mathcal{A}$ também comuta com $x_{i_j} \in \mathcal{Q} - \langle z\rangle$. Portanto, $x^2 = x_{i_1}^2 z^{h-1}$. Deste modo, se h for ímpar e $x_{i_1}^2 = z$ então x possuirá ordem 4, ou se h for par e $x_{i_1}^2 = 1$, então x terá ordem 4. Observemos que os grupos cíclicos em

cada caso são diferentes, logo teremos que contar os subgrupos cíclicos em cada caso.
Suponha h ímpar e $x_{i_1}^2 = z$. Se $x_{i_1} \in \mathcal{A}$ tal que $x_{i_1}^2 = z$ então $x_{i_1} = \overline{x}\ \overline{y}$ ou $x_{i_1} = (\overline{x}\ \overline{y})^{-1}$. Notemos que $x^{-1} = x_{i_1}^{-1}x_{i_2}^{-1}\dots x_{i_h}^{-1} = x_{i_1}^{-1}x_{i_2}\dots x_{i_h}$ e o mesmo acontecendo se substituirmos x_{i_k} por $x_{i_k}^{-1}$, para $1 \leq k \leq h$. Temos também que $\langle x\rangle = \langle x^{-1}\rangle$. Para escolhermos os elementos que constituem o gerador x, temos 3^{h-1} possibilidades. Como o conjunto de índices distintos determina um conjunto de subgrupos cíclicos de ordem 4 distintos, o total de tais subgrupos é

$$n_2 = \sum_h 3^{(h-1)}\binom{r-1}{h-1}, \tag{1.9}$$

com h ímpar variando de 1 até r. Mas (1.9) pode ser reescrita como

$$n_2 = \sum_h 3^h\binom{r-1}{h} = 2^{2(r-1)} - \frac{1}{2}\{2^{2(r-1)} - (-2)^{r-1}\}, \tag{1.10}$$

com h par variando de 0 até $r-1$.
Suponha agora h par e $x_{i_1}^2 = 1$. Se $x_{i_1} \in \mathcal{A}$ tal que $x_{i_1}^2 = 1$, então $x_{i_1} = \overline{x}$ ou $x_{i_1} = \overline{y}$. Temos que $\overline{x}^{-1} = \overline{x}$ e $\overline{y}^{-1} = \overline{y}$. Notemos que $x^{-1} = x_{i_1}x_{i_2}^{-1}\dots x_{i_h}^{-1} = x_{i_1}x_{i_2}^{-1}\dots x_{i_h}$ e o mesmo acontecendo se substituirmos x_{i_k} por $x_{i_k}^{-1}$. Logo, para escolhermos os elementos que constituem o gerador x temos $2\cdot 3^{h-1}$ possibilidades, desde que em $\mathcal{Q}_{i_k} - \langle z\rangle$ tenhamos 3 possibilidades. Como o conjunto de índices distintos determinam um conjunto de subgrupos cíclicos de ordem 4 distintos, temos no total da seguinte quantidade de tais subgrupos:

$$n_3 = \sum_h 2\cdot 3^{(h-1)}\binom{r-1}{h-1}, \tag{1.11}$$

onde h é par variando de 2 até r. Reescrendo (1.11) temos

$$n_3 = \sum_h 2\cdot 3^h\binom{r-1}{h} = 2^{2(r-1)} - (-2)^{r-1}, \tag{1.12}$$

onde h ímpar variando de 1 até $r-1$.
Por (1.7), (1.10) e (1.12), a quantidade de subgrupos cíclicos de ordem 4 em $\mathcal{DQ}^{r-1}$, será dada por

$$n = n_1 + n_2 + n_3 = \frac{1}{2}\{2^{2r} + (-2)^r\} \tag{1.13}$$

Claramente $m \neq n$, para todo r. Portanto, $\mathcal{Q}^r$ e $\mathcal{DQ}^{r-1}$ não são isomorfos. ■

O teorema acima nos informa que dados um primo p e $n \geq 1$, existem (a menos de isomorfismo) dois p-grupos extra-especiais de ordem p^{2n+1}:

- para $p = 2$: $\mathcal{Q}^n$ e $\mathcal{DQ}^{n-1}$
- para p ímpar: $\mathcal{M}^n$ e $\mathcal{NM}^{n-1}$.

Por exemplo, os 2-grupos extra-especiais não isomorfos de ordem 2^5 são:

$\mathcal{Q}^2 = \langle a, b, c, d |\ a^4 = 1, a^2 = b^2 = c^2 = d^2 = 1, a^b = a^{-1}, c^d = c^{-1},$ o resto comuta $\rangle$
$\mathcal{DQ} = \langle a, b, c, d |\ a^2 = b^2 = c^4 = 1, (ab)^4 = 1, c^2 = d^2 = (ab)^2, c^d = c^{-1},$ o resto comuta $\rangle$.

Enquanto que os p-grupos extra-especiais não isomorfos de ordem p^5, p ímpar são:

$\mathcal{M}^2 = \langle a, b, c, d, e |\ a^p = b^p = c^p = d^p = e^p, [a, b] = [c, d] = e,$ o resto comuta $\rangle$
$\mathcal{NM} = \langle a, b, c, d |\ a^{p^2} = b^p = c^{p^2} = d^p = 1, a^b = a^{1+p}, c^d = c^{1+p}, a^p = c^p,$ o resto comuta $\rangle$.

Capítulo 2

Fatos Básicos Sobre Álgebras de Grupos

Este capítulo tem como objetivo relacionar álgebras de grupos com anéis semisimples, o que será feito através da combinação do Teorema de Maschke com o Teorema de Wedderburn-Artin. Além disso, vamos definir e dar algumas propriedades de idempotentes na álgebra de grupo racional $\mathbb{Q}G$ e fazer alguns comentários sobre o problema do isomorfismo.

2.1 Anéis Semisimples e o Teorema de Wedderburn-Artin

Considerando R um anel com unidade, recordemos que um R-módulo simples (ou irredutível) M é tal que $M \neq 0$ e seus únicos R-submódulos são $\{0\}$ e M.

Definição 2.1 *Um R-módulo é **semisimples** (ou completamente redutível) se é uma soma direta (não necessariamente finita) de R-submódulos simples.*

Um anel R é semisimples se é semisimples como módulo sobre si mesmo. Neste caso, seus submódulos simples são seus ideais minimais à esquerda. Uma maneira de verificar a semisimplicidade de um anel R é através da semisimplicidade dos R-módulos, como diz o próximo teorema cuja demonstração está em [1].

Teorema 2.1 *Um anel R é semisimples se, e somente se, todo R-módulo é semisimples.*

Exemplos:

1. Qualquer anel de divisão D é um D-módulo simples.

2. O anel $M_n(D)$ de matrizes $n \times n$ sobre um anel de divisão D é semisimples pois os elementos:

$$L_1 = \begin{bmatrix} D & 0 & \dots & 0 \\ D & 0 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ D & 0 & \dots & 0 \end{bmatrix}, \dots, L_n = \begin{bmatrix} 0 & 0 & \dots & D \\ 0 & 0 & \dots & D \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & D \end{bmatrix}$$

   são ideais minimais à esquerda de $M_n(D)$ e, além disso,

$$M_n(D) = \bigoplus_{i=1}^{n} L_i.$$

O próximo resultado é sobre a decomposição de um FG-módulo M em soma direta de FG-submódulos simples. Este resultado desempenha um papel fundamental na teoria de representações de grupos. Ele nos diz quando uma álgebra de grupo FG é um anel semisimples, para maiores detalhes veja Corolário 3.4.8 em [7].

Teorema 2.2 *(Maschke) Seja G um grupo finito e F um corpo. Então todo FG-módulo é semisimples se, e somente se, $char(F) \nmid |G|$.*

Desta forma, todo $\mathbb{Q}G$-módulo é semisimples, já que $char(\mathbb{Q}) = 0$ e $|G| < \infty$. Assim, obtemos o seguinte resultado particular.

Corolário 2.3 *Se $|G| < \infty$ então $\mathbb{Q}G$ é um anel semisimples.*

O próximo resultado nos dá a estrutura dos anéis semisimples (veja Teorema 2.6.18 em [7]).

Teorema 2.4 *(Wedderburn-Artin) Se R é um anel semisimples então R é isomorfo a soma direta de um número finito de anéis de matrizes sobre anéis de divisão, ou seja,*

$$R \approx \bigoplus_{i=1}^{k} M_{n_i}(D_i),$$

onde cada D_i é um anel de divisão. Além disso, $M_{n_i}(D_i) = \bigoplus_{j=1}^{n_i} M_{ij}$ onde M_{ij} são ideais minimais à esquerda de $M_{n_i}(D_i)$ simples e isomorfos entre si cuja dimensão sobre D_i é igual a n_i.

Assim, combinando o corolário anterior com o Teorema de Wedderburn temos o seguinte.

Corolário 2.5 *Se $|G| < \infty$ então*

$$\mathbb{Q}G \approx \bigoplus_{i=1}^{k} M_{n_i}(D_i),$$

onde cada D_i é um anel de divisão.

Nosso próximo passo é definir os idempotentes em um anel, que serão as ferramentas necessárias para a classificação dos n_i's e D_i's acima e, deste modo, poderemos dar a decomposição completa de $\mathbb{Q}G$ em situações particulares.

2.2 Idempotentes em $\mathbb{Q}G$

Definição 2.2 *Seja R um anel. Um elemento $e \in R$ é um* ***idempotente*** *se $e^2 = e$.*

Os elementos 0 e 1 são os idempotentes triviais de R.

Observação: Se e é idempotente então

(i) $(1 - e)$ também é idempotente.

(ii) Re e $R(1 - e)$ são ideais à esquerda de R e $Re \cap R(1 - e) = 0$.

Pela observação (ii) temos que se R contém um idempotente não trivial, então R pode ser escrito como soma direta de dois ideais à esquerda não triviais, ou seja, $R = Re \oplus R(1-e)$. Neste caso, dizemos que R é um anel decomponível.

Já vimos que anéis semisimples podem ser decompostos em uma soma direta de submódulos simples, que correspondem a ideais minimais à esquerda. O próximo resultado relaciona semisimplicidade com idempotentes e mostra que os idempotentes são os elementos que cindem o anel.

Teorema 2.6 *Um anel R é semisimples se, e somente se, todo ideal à esquerda I de R é da forma $I = Re$, para algum idempotente $e \in R$.*

Para maiores detalhes veja Teorema 2.5.10 em [7].

Definição 2.3 *Se $e \in R$ é um idempotente que não pode ser escrito como $e = e_1 + e_2$, onde e_1 e e_2 são idempotentes tais que $e_1,\ e_2 \neq 0$ e $e_1e_2 = 0$, então e é um* ***idempotente primitivo*** *de R.*

Definição 2.4 *Um idempotente $e \in R$ é* ***central*** *se $re = er$, para todo $r \in R$.*

Dados resultados gerais sobre idempotentes, vamos agora focar nosso interesse nos idempotentes em uma álgebra de grupo $\mathbb{Q}G$. Antes necessitamos da seguinte definição.

Definição 2.5 *Seja X um subconjunto finito do grupo G. Denotaremos por $\widehat{X}$ o seguinte elemento de $\mathbb{Q}G$*

$$\widehat{X} = \frac{1}{|\,X|} \sum_{x \in X} x.$$

Lema 2.7 *Seja H um subgrupo de um grupo G. Então $\widehat{H}$ é idempotente de $\mathbb{Q}G$. Além disso, se $H \triangleleft G$ então $\widehat{H}$ é central.*

Demonstração: Primeiro, queremos mostrar que $\widehat{H}\widehat{H} = \widehat{H}$. Assim,

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

Suponha $H \lhd G$. Queremos mostrar que $\widehat{H}$ é central. Tome $g \in G$, logo $\widehat{H}^g = \frac{1}{|H|}\sum_{h\in H} h^g$, $h^g = \bar{h} \in H$ e então $\sum_{h\in H} h^g = |H|\,\widehat{H}$. Portanto, $\widehat{H}^g = \widehat{H}$. Assim, acabamos de mostrar que $\widehat{H}$ comuta com qualquer elemento da base e, conseqüentemente, comuta com qualquer elemento de $\mathbb{Q}G$. ■

Observação: Antes de demonstrarmos o próximo resultado é necessário mostrarmos que $G\widehat{H}$, onde $H \lhd G$, é um grupo. Consideraremos o produto do anel de grupo $\mathbb{Q}G$, e $g_1,\ g_2,\ g_3\ \in G$. Assim,
(i) $g_1\widehat{H},\ g_2\widehat{H} \in G\widehat{H}$. Temos que $g_1\widehat{H}g_2\widehat{H} = g_1g_2\widehat{H}\widehat{H}$, pois $\widehat{H}$ é central em $\mathbb{Q}G$ e, conseqüentemente, $g_1\widehat{H}g_2\widehat{H} = g_1g_2\widehat{H}^2 = g_1g_2\widehat{H}$, pelo lema anterior, logo $g_1g_2\widehat{H} = g_3\widehat{H} \in G\widehat{H}$. Isto mostra que $G\widehat{H}$ é fechado.
(ii) $g_1\widehat{H}(g_2\widehat{H}g_3\widehat{H}) = (g_1\widehat{H}g_2\widehat{H})g_3\widehat{H}$ pois é herdado do produto do anel de grupo $\mathbb{Q}G$.
(iii) $\widehat{H}$ é o elemento neutro de $G\widehat{H}$, pois $g_1\widehat{H}\widehat{H} = \widehat{H}g_1\widehat{H} = g_1\widehat{H}$.
(iv) Para todo $g_1\widehat{H} \in G\widehat{H}$ existe um elemento $g_1^{-1}\widehat{H}$ tal que $g_1\widehat{H}g_1^{-1}\widehat{H} = g_1^{-1}\widehat{H}g_1\widehat{H} = \widehat{H}$.

Teorema 2.8 *Sejam G um grupo e $H \lhd G$. Então*

$$\mathbb{Q}G = \mathbb{Q}G\widehat{H} \oplus \mathbb{Q}(1 - \widehat{H}').$$

Além disso, $\mathbb{Q}G\widehat{H} \approx \mathbb{Q}(G/H)$.

Demonstração: A primeira parte está demonstrada, pois é a combinação do item (ii) da observação do início desta seção com o teorema anterior.
Para vermos que $\mathbb{Q}G\widehat{H} \approx \mathbb{Q}(G/H)$, mostraremos que G/H e $G\widehat{H}$ são isomorfos como grupos. De fato,

$$\begin{aligned} \varphi : G &\longrightarrow G\widehat{H} \\ g &\longmapsto g\widehat{H} \end{aligned}$$

é um epimorfismo de grupos. Se $g \in H$ temos que $\varphi(g) = \widehat{H}$, que é identidade de $G\widehat{H}$, logo $g \in Ker(\varphi)$. Logo $Ker(\varphi) = H$. Pelo Teorema do Homomorfismo $G/Ker(\varphi) \approx G\widehat{H}$. Como $G\widehat{H}$ é base para $\mathbb{Q}G\widehat{H}$ sobre $\mathbb{Q}$ temos que $\mathbb{Q}G\widehat{H} \approx \mathbb{Q}(G/H)$. ■

Precisamos, neste momento, escolher um subgrupo H de G que possibilite a decomposição de nossa álgebra em duas componentes interessantes. Este fato será obtido com o seguinte resultado (veja [7], Proposição 3.6.11).

Teorema 2.9 *A álgebra de grupo $\mathbb{Q}G$ pode ser decomposta como*

$$\mathbb{Q}G = \mathbb{Q}G\widehat{G}' \oplus \mathbb{Q}G(1-\widehat{G}'),$$

onde $\mathbb{Q}G\widehat{G}'$ é a soma de todas as componentes simples comutativas de $\mathbb{Q}G$ e $\mathbb{Q}G(1-\widehat{G}')$ é a soma de todas as outras.

Teremos $\mathbb{Q}G\widehat{G}' \approx \mathbb{Q}\,(G/G')$ a componente comutativa de $\mathbb{Q}G$ enquanto que $\mathbb{Q}G(1-\widehat{G}')$ é a componente não-comutativa de $\mathbb{Q}G$.

O traço de um idempotente em $\mathbb{Q}G$:

Seja G um grupo finito de ordem n e consideremos a álgebra de grupo $\mathbb{Q}G$.

Para cada elemento $x \in G$, definimos uma função

$$\begin{array}{rl} T_x : G & \longrightarrow G \\ g & \longmapsto gx \end{array}$$

que pode ser estendida linearmente para $\mathbb{Q}G$:

$$\begin{array}{rl} T_x : \mathbb{Q}G & \longrightarrow \mathbb{Q}G \\ \alpha & \longmapsto \alpha x \end{array},$$

onde $\alpha = \sum \alpha_g g$. Logo $T_x(\alpha) = \sum \alpha_g T_x(g) = \sum \alpha_g gx$.

Se considerarmos $G = \{g_1, \ldots, g_n\}$, com $g_1 = 1$, sabemos que G é uma base de $\mathbb{Q}G$ sobre $\mathbb{Q}$ e então T_x é uma transformação linear do espaço vetorial $\mathbb{Q}G$ que pode ser representada por uma matriz $n \times n$, observando que:

$$T_x : \begin{array}{ccccc} g_1 & \longmapsto & g_1x & = & g_{i_1} \\ g_2 & \longmapsto & g_2x & = & g_{i_2} \\ \vdots & & \vdots & & \vdots \\ g_n & \longmapsto & g_nx & = & g_{i_n}. \end{array}$$

A matrix T_x tem entradas contendo apenas 0 e 1 e cada linha tem exatamente um elemento não nulo. Notemos ainda que esta matriz é a identidade se, e somente se, $x = 1$.

Agora, se $\alpha \in \mathbb{Q}G$, então $\alpha = \sum_{i=1}^{n} \alpha_{g_i} g_i$ e assim, definimos a representação regular (à direita) de $\mathbb{Q}G$ por

$$\begin{aligned} T : \mathbb{Q}G &\longrightarrow M_n(\mathbb{Q}) \\ \alpha &\longmapsto T_\alpha : \mathbb{Q}G \longrightarrow \mathbb{Q}G \\ & \qquad\quad g \longmapsto \alpha g. \end{aligned}$$

Observamos que $T_\alpha = \sum_{i=1}^{n} \alpha_{g_i} T_{g_i}$ e, portanto, considerando a matriz T_α e seu traço (soma dos elementos da diagonal), temos:

$$tr(T_\alpha) = \sum_{i=1}^{n} \alpha_{g_i} tr(T_{g_i}).$$

Mas

$$tr(T_{g_i}) = \begin{cases} 0, & \text{se } g_i \neq 1 \\ 1, & \text{se } g_i = 1 \ (i = 1) \end{cases}$$

ou seja, $tr(T_\alpha) = \alpha_1 \,|\, G|$.

Definimos o traço do elemento $\alpha \in \mathbb{Q}G$ como traço$(\alpha) = \alpha_1$, isto é, traço(α) é o coeficiente de 1 em α.

Consideremos agora um idempotente $e = \sum_{i=1}^{n} \alpha_{g_1} g_i \in \mathbb{Q}G$. Já sabemos que

$$\mathbb{Q}G = \mathbb{Q}Ge \oplus \mathbb{Q}G(1-e).$$

Escolhemos uma base β de $\mathbb{Q}G$ como união de bases β_1 de $\mathbb{Q}Ge$ e β_2 de $\mathbb{Q}G(1-e)$, ou seja, $\beta = \beta_1 \cup \beta_2$, onde $\beta_1 = \{r_1 e, \ldots, r_s e\}$ e $\beta_2 = \{t_1(1-e), \ldots, t_m(1-e)\}$, $\dim_{\mathbb{Q}} \mathbb{Q}Ge = s$ e $\dim_{\mathbb{Q}} \mathbb{Q}G(1-e) = m$. Assim, podemos escrever qualquer elemento $\gamma \in \mathbb{Q}G$ como combinação linear destes elementos:

$$\gamma = \gamma_1 r_1 e + \ldots + \gamma_s r_s e + \widetilde{\gamma_1} t_1(1-e) + \ldots + \widetilde{\gamma_m} t_m(1-e).$$

Logo $T_e(\gamma) = \gamma_1 r_1 e + \ldots + \gamma_s r_s e$, ou seja, T_e age como identidade em $\mathbb{Q}Ge$ e anula $\mathbb{Q}G(1-e)$. Portanto,

$$tr(T_e) = e_1 \,|\, G| = \text{traço}(e) \,|\, G| = \dim_{\mathbb{Q}} \mathbb{Q}Ge.$$

Assim, demonstramos o seguinte resultado.

Teorema 2.10 *Se $e \in \mathbb{Q}G$ é um idempotente então*

$$dim_{\mathbb{Q}} \mathbb{Q}Ge = |\, G| \; traço(e).$$

Notemos que $0 \leq \underbrace{\dim_{\mathbb{Q}} \mathbb{Q}Ge}_{e_1|G|} \leq \underbrace{\dim_{\mathbb{Q}} \mathbb{Q}G}_{|G|}$, consequentemente e_1 é um racional entre 0 e 1.

2.3 O Problema do Isomorfismo

O Problema do Isomorfismo pergunta se um isomorfismo de anéis $RG \approx RH$ implica no isomorfismo de grupos $G \approx H$. Referindo-se a anéis de grupos sobre os inteiros, G. Higman (1940) sugeriu este problema clássico pela primeira vez em sua tese de Doutorado e respondeu positivamente esta questão quando $R = \mathbb{Z}$ e G é um grupo abeliano finito. Em 1947, T. M. Thrall formulou o tema nos seguintes termos: *Dado um grupo G e um corpo F, determine todos os grupos H tais que $FG \approx FH$.* Isto foi primeiramente considerado por S. Perlis e G. Walker, em 1950, quando eles estabeleceram que grupos abelianos finitos são determinados por suas álgebras de grupo racionais.

Teorema 2.11 *(Perlis-Walker) Seja G um grupo abeliano finito. Se $\mathbb{Q}G \approx \mathbb{Q}H$ então $G \approx H$.*

D. Passman em [6] provou que podemos considerar exemplos de álgebras de grupos isomorfas restringindo nossa atenção apenas para o corpo $\mathbb{Q}$ dos racionais.

Teorema 2.12 *Sejam G e H grupos finitos tais que $\mathbb{Q}G \approx \mathbb{Q}H$. Então, para todos os corpos K para os quais $charK$ não divide $|G| = |H|$, temos $KG \approx KH$.*

Podemos aplicar este resultado para álgebras de grupos de p-grupos finitos de classe 2 e a razão para isto é o seguinte lema de G. Higman (1960) que garante a existência de um número grande de tais grupos.

Lema 2.13 *Seja p um primo e $n \in \mathbb{N}$. Existem pelo menos*

$$\left[p^{\frac{1}{27}(2n^3-25n^2)}\right]$$

p-grupos de ordem p^n, classe de nilpotência ≤ 2 e expoente dividindo p^2.

Grosseiramente falando, o próximo resultado, provado por D. Passman (1965), diz que existem muitos p-grupos de uma mesma ordem e poucas álgebras de grupos sobre os mesmos.

Teorema 2.14 *Existe um conjunto com pelo menos*

$$\left[p^{\frac{2}{27}(n^3-23n^2)}\right]$$

p-grupos não-isomorfos de ordem p^n que tem álgebras de grupos isomorfas sobre $\mathbb{Q}$ e, conseqüentemente, sobre todos os corpos de característica diferente de p.

Este resultado é trivial para $n \leq 23$, mas podemos ter dificuldade para encontrar exemplos quando n é grande.

No próximo capítulo, como já foi citado anteriormente, vamos tratar do problema do isomorfismo para álgebras de grupos racionais de uma classe particular de p-grupos, garantindo novos exemplos para o teorema anterior.

Capítulo 3

Decomposição de Wedderburn para $\mathbb{Q}G$: Caso Extra-Especial

Neste capítulo, baseado na referência [8], temos o objetivo de descrever todas as componentes simples na decomposição de Wedderburn para $\mathbb{Q}G$ sendo G um p-grupo extra-especial.

3.1 As Componentes Comutativa e Não-Comutativa de $\mathbb{Q}G$

Inicialmente, recordemos que se G é um p-grupo extra-especial de ordem p^{2n+1} então G/G' é um p-grupo abeliano elementar de ordem p^{2n}. Portanto,

$$G/G' \approx \underbrace{\mathcal{C}_p \times \ldots \times \mathcal{C}_p}_{2n \text{ vezes}}.$$

Além disso, é conhecido que (veja [1] e [7]):

1. $\mathbb{Q}\mathcal{C}_p \approx \mathbb{Q} \oplus \mathbb{Q}(\xi_p)$, onde ξ_p é a p-ésima raiz primitiva da unidade.
2. Se A e B são grupos finitos, então $\mathbb{Q}(A \times B) \approx \mathbb{Q}A \otimes \mathbb{Q}B$.
3. $\mathbb{Q} \otimes \mathbb{Q}(\xi_p) \approx \mathbb{Q}(\xi_p)$ e $\mathbb{Q}(\xi_p) \otimes \mathbb{Q}(\xi_p) \approx (p-1)\mathbb{Q}(\xi_p)$.

A partir destas observações, provemos o próximo resultado.

Proposição 3.1 *Se G é um p-grupo abeliano elementar de ordem p^n, $n \geq 2$, então*

$$\mathbb{Q}G \approx \mathbb{Q}(\underbrace{\mathcal{C}_p \times \ldots \times \mathcal{C}_p}_{n \text{ vezes}}) \approx \mathbb{Q} \oplus (p^{n-1} + p^{n-2} + \ldots + p + 1)\mathbb{Q}(\xi_p).$$

Demonstração: Demonstraremos essa proposição por indução sobre n. Para $n = 2$ temos que $|G| = p^2$. Logo, utilizando as propriedades (1), (2) e (3) acima, temos $\mathbb{Q}(\mathcal{C}_p \times \mathcal{C}_p) \approx \mathbb{Q}\mathcal{C}_p \otimes \mathbb{Q}\mathcal{C}_p \approx (\mathbb{Q} \oplus \mathbb{Q}(\xi_p)) \otimes (\mathbb{Q} \oplus \mathbb{Q}(\xi_p)) \approx (\mathbb{Q} \otimes \mathbb{Q}) \oplus (\mathbb{Q} \otimes \mathbb{Q}(\xi_p)) \oplus (\mathbb{Q}(\xi_p) \otimes \mathbb{Q}) \oplus (\mathbb{Q}(\xi_p) \otimes \mathbb{Q}(\xi_p)) = \mathbb{Q} \oplus \mathbb{Q}(\xi_p) \oplus \mathbb{Q}(\xi_p) \oplus (p-1)\mathbb{Q}(\xi_p) = \mathbb{Q} \oplus (p+1)\mathbb{Q}(\xi_p)$. Suponha que o resultado seja válido para $n = k$. Assim, se $|G| = p^{k+1}$ temos $\mathbb{Q}G \approx \mathbb{Q}(\mathcal{C}_p \times \underbrace{(\mathcal{C}_p \times \ldots \times \mathcal{C}_p)}_{k \text{ vezes}}) = \mathbb{Q}\mathcal{C}_p \otimes \mathbb{Q}(\mathcal{C}_p \times \ldots \times \mathcal{C}_p)$, mas pela hipótese de indução, temos $\mathbb{Q}G = (\mathbb{Q} \oplus \mathbb{Q}(\xi_p)) \otimes (\mathbb{Q} \oplus (p^{k-1} + \ldots + p + 1)\mathbb{Q}(\xi_p)) = \mathbb{Q} \oplus (p^{k-1} + \ldots + p + 1)\mathbb{Q}(\xi_p) \oplus \mathbb{Q}(\xi_p) \oplus (p^{k-1} + \ldots + p + 1)(p-1)\mathbb{Q}(\xi_p) = \mathbb{Q} \oplus (p^k + \ldots + p + 1)\mathbb{Q}(\xi_p)$. ■

Agora, pelo Teorema 2.8, temos $\mathbb{Q}G \approx \mathbb{Q}G\widehat{G'} \oplus \mathbb{Q}G(1 - \widehat{G'})$ e $\mathbb{Q}G\widehat{G'} \approx \mathbb{Q}G(G/G')$ e com a proposição acima, provamos:

Lema 3.2 *Seja G p-grupo extra-especial de ordem p^{2n+1}. A componente comutativa de $\mathbb{Q}G$ é*

$$\mathbb{Q} \oplus (p^{2n-1} + p^{2n-2} + \ldots + p + 1)\mathbb{Q}(\xi_p).$$

Desta maneira, temos o seguinte.

Lema 3.3 *Sejam G e H p-grupos extra-especiais de mesma ordem. Então*

$$\mathbb{Q}G\widehat{G'} \approx \mathbb{Q}H\widehat{H'}.$$

Ou seja, as componentes comutativas de $\mathbb{Q}G$ e $\mathbb{Q}H$ são isomorfas.

Vamos agora estabelecer alguns resultados que nos ajudarão a descrever a componente não-comutativa de $\mathbb{Q}G$. O próximo lema foi provado em [8], neste C_g denota a classe de conjugação de g em G e $\widehat{z}$ é o mesmo que $\widehat{\langle z \rangle}$.

Lema 3.4 *Seja $g \in G$. Se $g^{-1}C_g \cap \mathcal{Z}(G) \neq \{1\}$ então G contém um elemento central z de ordem prima tal que $\widehat{C}_g = \widehat{C}_g\widehat{z}$.*

Demonstração: Se $g^{-1}C_g \cap \mathcal{Z}(G) \neq \{1\}$, então existe um elemento $\{1\} \neq z \in \mathcal{Z}(G)$ tal que $z \in g^{-1}C_g$, isto é, existe $h \in G$ tal que $z = g^{-1}g^h$, logo $zg = h^{-1}gh$.
Assim,

$$z^2g = z(h^{-1}gh) = h^{-1}zgh = h^{-1}h^{-1}ghh = h^{-2}gh^2.$$

Por indução, temos que, para qualquer n, $z^ng = h^{-n}gh^n$. Com isso, $(z^ng)^x = (h^{-n}gh^n)^x$, $\forall\ x \in G$. Portanto, $\langle z\rangle C_g \subset C_g$, logo $\langle z\rangle C_g = C_g$ e então $\widehat{C}_g = \widehat{C}_g\widehat{z}$. Se necessário, substituindo z por uma potência de z, podemos assumir que z tem ordem prima. ■

O próximo resultado é uma adaptação do Lema 2.2 de [4].

Lema 3.5 *Se G é um grupo nilpotente finito de classe 2 e α pertence ao centro de $\mathbb{Q}G(1-G')$, então o suporte de α está no centro de G.*

Demonstração: Suponha α central em $\mathbb{Q}G(1-G')$. Observemos então que $\bar{\alpha}$ é central em $\mathbb{Q}\bar{G}(1-\bar{G}')$ para qualquer imagem homomórfica de $\bar{G}$ de G.

Como vimos no Capítulo 1, se G é nilpotente de classe 2 a série central inferior possui comprimento 2 e $G' \neq \{1\}$. Escolha um subgrupo N de G' tal que G'/N tenha ordem prima. Seja $\bar{c}$ o gerador deste grupo. Então $\bar{G}' = (G/N)' = G'/N = \langle\bar{c}\rangle$. Além disso, $\widehat{\bar{c}}$ e $1-\widehat{\bar{c}}$ são idempotentes de $\mathbb{Q}\bar{G}$ e, pelo Teorema 2.8, temos $\mathbb{Q}\bar{G} = \mathbb{Q}\bar{G}\widehat{\bar{c}} \oplus \mathbb{Q}\bar{G}(1-\widehat{\bar{c}})$.

Como $\bar{\alpha}$ é central em $\mathbb{Q}\bar{G}(1-\bar{G}')$ então é central em $\mathbb{Q}\bar{G}$. Assim, temos $\bar{\alpha}\bar{g} = \bar{g}\bar{\alpha}$, $\forall\ \bar{g} \in \bar{G}$. Logo os elementos de uma mesma classe de conjugação têm o mesmo coeficiente, e assim podemos reescrever $\bar{\alpha}$ como combinação linear das somas de classes de G:

$$\bar{\alpha} = \sum_{\bar{g}\in\mathcal{Z}(\bar{G})} \alpha_{\bar{g}}\bar{g} + \sum_{\bar{g}\notin\mathcal{Z}(\bar{G})} \alpha_{\bar{g}}\widehat{C}_{\bar{g}}. \tag{3.1}$$

Mas $\bar{\alpha} = \lambda(1-\widehat{\bar{c}})$, onde $\lambda \in \mathbb{Q}\bar{G}$, logo $\bar{\alpha}(1-\widehat{\bar{c}}) = \lambda(1-\widehat{\bar{c}})^2 = \lambda(1-\widehat{\bar{c}}) = \bar{\alpha}$. Assim podemos reescrever a equação (3.1) como:

$$\bar{\alpha} = \sum_{\bar{g}\in\mathcal{Z}(\bar{G})} \alpha_{\bar{g}}(1-\widehat{\bar{c}}) + \sum_{\bar{g}\notin\mathcal{Z}(\bar{G})} \alpha_{\bar{g}}\widehat{C}_{\bar{g}}(1-\widehat{\bar{c}}). \tag{3.2}$$

Agora, para cada $\bar{g} \notin \mathcal{Z}\left(\bar{G}\right)$, existe $\bar{h} \in \bar{G}$ tal que $1 \neq [\bar{g}, \bar{h}] \in \bar{g}^{-1}C_{\bar{g}} \cap \mathcal{Z}\left(\bar{G}\right)$, pois $\bar{G}' \leq \mathcal{Z}\left(\bar{G}\right)$. Pelo Lema anterior, existe $\bar{z} \in \mathcal{Z}\left(\bar{G}\right)$ de ordem prima tal que $\widehat{C}_{\bar{g}} = \widehat{C}_{\bar{g}}\langle\widehat{\bar{z}}\rangle$. Como $\bar{z}$ tem ordem prima, temos que $\langle\widehat{\bar{z}}\rangle = \langle\widehat{\bar{c}}\rangle$ e então $\widehat{C}_{\bar{g}} = \widehat{C}_{\bar{g}}\langle\widehat{\bar{c}}\rangle$. Substituindo em (3.2) obtemos:

$$\bar{\alpha} = \sum_{\bar{g}\in\mathcal{Z}\left(\bar{G}\right)} \alpha_{\bar{g}}(1-\widehat{\bar{c}}) + \sum_{\bar{g}\notin\mathcal{Z}\left(\bar{G}\right)} \alpha_{\bar{g}}\widehat{C}_{\bar{g}}\langle\widehat{\bar{c}}\rangle(1-\widehat{\bar{c}})$$

$$\bar{\alpha} = \sum_{\bar{g}\in\mathcal{Z}\left(\bar{G}\right)} \alpha_{\bar{g}}(1-\widehat{\bar{c}})$$

Logo $\mathrm{supp}(\bar{\alpha}) \subseteq \mathcal{Z}\left(\bar{G}\right)$ e como N é um subgrupo central, temos $\mathrm{supp}(\alpha) \subseteq \mathcal{Z}\left(G\right)$. ■

Este lema traz como consequência o seguinte resultado sobre o centro da componente não-comutativa da álgebra de grupo racional de um grupo nilpotente de classe 2.

Corolário 3.6 *Se G é um grupo nilpotente de classe 2 então*

$$\mathcal{Z}\left(\mathbb{Q}G(1-\widehat{G}')\right) = \mathbb{Q}\mathcal{Z}\left(G\right)(1-\widehat{G}').$$

Vamos agora classificar a componente não-comutativa da álgebra de grupo racional de um p-grupo extra-especial.

Proposição 3.7 *Seja G um p-grupo extra-especial. Então $\mathbb{Q}G(1-\widehat{G}')$ é simples.*

Demonstração: Seja α um idempotente central em $\mathbb{Q}G(1-\widehat{G}')$. Pelo corolário anterior, $\alpha \in \mathbb{Q}\mathcal{Z}\left(G\right)(1-\widehat{G}')$. Mas G sendo extra-especial temos

$$\mathbb{Q}\mathcal{Z}\left(G\right) = \mathbb{Q}G' \approx \mathbb{Q}\mathcal{C}_p \approx \mathbb{Q} \oplus \mathbb{Q}(\xi_p).$$

Por outro lado, temos

$$\mathbb{Q}\mathcal{Z}\left(G\right) \approx \mathbb{Q}\mathcal{Z}\left(G\right)\widehat{\mathcal{Z}\left(G\right)} \oplus \mathbb{Q}\mathcal{Z}\left(G\right)(1-\widehat{\mathcal{Z}\left(G\right)}) \approx \mathbb{Q} \oplus \mathbb{Q}\mathcal{Z}\left(G\right)(1-\widehat{G}').$$

Portanto, $\mathbb{Q}\mathcal{Z}\left(G\right)(1-\widehat{G}') \approx \mathbb{Q}(\xi_p)$. Como $\mathbb{Q}(\xi_p)$ é simples então α é o único idempotente central de $\mathbb{Q}G(1-\widehat{G}')$ e, conseqüentemente, $\mathbb{Q}G(1-\widehat{G}')$ é simples. ■

O próximo resultado será uma primeira abordagem ao problema do isomorfismo. Consideraremos duas álgebras de grupos racionais isomorfas: a primeira é uma álgebra de um p-grupo extra-especial G e a outra será a álgebra de um grupo arbitrário H. Queremos obter informações sobre o grupo H.

Proposição 3.8 *Sejam G um p-grupo extra-especial e H um grupo tal que $\mathbb{Q}G \approx \mathbb{Q}H$. Então H é um grupo extra-especial de mesma ordem de G.*

Demonstração: Vamos mostrar primeiro que H é nilpotente de classe 2 e depois concluiremos que H será extra-especial.

É claro que se $\mathbb{Q}G \approx \mathbb{Q}H$, então $|G| = |H|$. Por hipótese, temos

$$\mathbb{Q}(G/G') \oplus \mathbb{Q}G(1-\widehat{G}') \approx \mathbb{Q}(H/H') \oplus \mathbb{Q}H(1-\widehat{H}').$$

Olhando para as partes comutativas, temos $\mathbb{Q}(G/G') \approx \mathbb{Q}(H/H')$ e, pelo Teorema 2.11, chegamos a $G/G' \approx H/H'$ e, portanto, $|H'| = p$. Como $H' \lhd H$ e H é um p-grupo, pelo Teorema 1.7, temos que $\mathcal{Z}(H) \cap H' \neq \{1\}$. Assim, $H' \leq \mathcal{Z}(H)$ e H é nilpotente de classe 2.

Estudando as componentes não-comutativas, temos

$$\begin{gathered}\mathbb{Q}G(1-\widehat{G}') \approx \mathbb{Q}H(1-\widehat{H}') \\ \mathcal{Z}\left(\mathbb{Q}G(1-\widehat{G}')\right) \approx \mathcal{Z}\left(\mathbb{Q}H(1-\widehat{H}')\right),\end{gathered}$$

e aplicando o Corolário 3.6, temos

$$\mathbb{Q}\mathcal{Z}(G)(1-\widehat{G}') \approx \mathbb{Q}\mathcal{Z}(H)(1-\widehat{H}').$$

Logo

$$\dim_{\mathbb{Q}}\mathbb{Q}\mathcal{Z}(G)(1-\widehat{G}') = \dim_{\mathbb{Q}}\mathbb{Q}\mathcal{Z}(H)(1-\widehat{H}').$$

Considerando que os idempotentes $1-\widehat{G}'$ e $1-\widehat{H}'$ têm o mesmo traço e usando o Teorema 2.10, temos $|\mathcal{Z}(G)| = |\mathcal{Z}(H)| = p$.

Assim, $\mathcal{Z}(H) = H'$ e, por definição, H é um p-grupo extra-especial. ■

Ao classificarmos os p-grupos extra-especiais no final do Capítulo 1, vimos que existem, a menos de isomorfimo, apenas dois grupos extra-especiais de mesma ordem e

suas álgebras de grupos racionais podem ser, ou não, isomorfas. Para respondermos esta questão, caracterizaremos a componente não-comutativa de uma álgebra de grupo racional de um p-grupo extra-especial.

3.2 Componente Não-Comutativa no Caso p Ímpar

Consideremos G um p-grupo extra-especial, com p ímpar.

Antes de classificarmos a componente simples não-comutativa de $\mathbb{Q}G$, vamos ver alguns exemplos que irão nos direcionar para a classificação dessa componente.

Exemplos:
Todos os exemplos de decomposições mostrados abaixo foram calculados através de uma rotina no GAP, utilizando a biblioteca wedderga (veja [5]). Nestes exemplos, ξ_3 denota a terceira raiz primitiva da unidade.

1. Decomposições das álgebras de grupos extra-especiais de ordem 3^3:

   (a) $\mathbb{Q}\mathcal{N} \approx \mathbb{Q} \oplus 4\mathbb{Q}[\xi_3] \oplus \mathrm{M}_3(\mathbb{Q}[\xi_3])$

   (b) $\mathbb{Q}\mathcal{M} \approx \mathbb{Q} \oplus 4\mathbb{Q}[\xi_3] \oplus \mathrm{M}_3(\mathbb{Q}[\xi_3])$.

   Vemos claramente pela decomposição acima que $\mathbb{Q}\mathcal{N}$ isomorfo à $\mathbb{Q}\mathcal{M}$ mas $\mathcal{N}$ não é isomorfo à $\mathcal{M}$. Temos uma resposta negativa ao problema do isomorfismo.

2. Decomposições das álgebras de grupos extra-especiais de ordem 3^5:

   (a) $\mathbb{Q}\mathcal{N}\mathcal{M} \approx \mathbb{Q} \oplus 40\mathbb{Q}[\xi_3] \oplus \mathrm{M}_9(\mathbb{Q}[\xi_3])$

   (b) $\mathbb{Q}\mathcal{M}^2 \approx \mathbb{Q} \oplus 40\mathbb{Q}[\xi_3] \oplus \mathrm{M}_9(\mathbb{Q}[\xi_3])$.

   Novamente temos as álgebras isomorfas mas os grupos não são isomorfos, dando uma resposta negativa ao problema do isomorfismo.

Com estes exemplos, vemos que no caso extra-especial, com p ímpar, teremos uma resposta negativa ao problema do isomorfismo. Confirmaremos esse fato com o resultado que será provado mais adiante.

Antes disso, definiremos um novo objeto. Consideremos K um corpo arbitrário e G um grupo qualquer. Se M é $KG-$módulo simples e $D = \mathrm{End}_{KG}M$, sabemos que D é um anel de divisão (pelo Lema de Schur). Definimos então o índice de Schur de M por:

$$m(M) = \sqrt{\dim_{\mathcal{Z}(D)} D}.$$

Pelo Lema 12.4.2 de [6], temos que $m(M)$ é um inteiro ou é ∞. Enunciaremos, sem demonstração, um lema (maiores detalhes veja Lema 12.4.7 de [6]) sobre o índice de Schur em uma situação particular.

Lema 3.9 *Sejam G um grupo nilpotente finito, M um $KG-$módulo simples e $D = End_{KG}M$. Então $m(M) \leq 2$. Se $m(M) = 2$ então o 2-subgrupo de Sylow de G é não abeliano.*

Notemos que se G é nilpotente de ordem ímpar, temos que $m(M) = 1$, caso contrário o 2-subgrupo de Sylow de G, que é $\{1\}$, seria não abeliano, um absurdo. Portanto, neste caso, $\dim_{\mathcal{Z}(D)} D = 1$, ou seja, D é um corpo.

Proposição 3.10 *Seja G um p-grupo extra-especial de ordem p^{2n+1} e p ímpar. Então $\mathbb{Q}G(1 - \widehat{G'}) \approx M_{p^n}(\mathbb{Q}[\xi_p])$, onde ξ_p é a p-ésima raiz primitiva da unidade.*

Demonstração: Por hipótese temos que $\mathcal{Z}(G) = G' \approx \mathcal{C}_p$, logo $\mathbb{Q}G(1 - \widehat{G'}) \approx \mathbb{Q}G(1 - \widehat{\mathcal{C}_p})$. Então pelo Corolário 3.6 temos

$$\mathcal{Z}\left(\mathbb{Q}G(1 - \widehat{\mathcal{C}_p})\right) = \mathbb{Q}\mathcal{Z}(G)(1 - \widehat{\mathcal{C}_p}) \approx \mathbb{Q}\mathcal{C}_p(1 - \widehat{\mathcal{C}_p}). \tag{3.3}$$

Sabemos que $\mathbb{Q}\mathcal{C}_p \approx \mathbb{Q}\mathcal{C}_p\widehat{\mathcal{C}_p} \oplus \mathbb{Q}\mathcal{C}_p(1 - \widehat{\mathcal{C}_p}) \approx \mathbb{Q} \oplus \mathbb{Q}[\xi_p]$. Assim $\mathbb{Q}\mathcal{C}_p(1 - \widehat{\mathcal{C}_p}) \approx \mathbb{Q}[\xi_p]$. Mas $\mathbb{Q}G(1 - \widehat{\mathcal{C}_p}) \approx M_r(D)$, onde D é um corpo, como observado acima. Por outro lado, pela Proposição 3.7, $\mathbb{Q}G(1 - \widehat{\mathcal{C}_p})$ é simples com centro $\mathbb{Q}[\xi_p]$. Logo

$$\mathbb{Q}[\xi_p] \approx \mathcal{Z}\left(\mathbb{Q}G(1 - \widehat{\mathcal{C}_p})\right) \approx \mathcal{Z}(M_r(D)) \approx \mathcal{Z}(D) \approx D$$

e, conseqüentemente, $\mathbb{Q}G(1 - \widehat{\mathcal{C}_p}) \approx M_r(\mathbb{Q}[\xi_p])$.

Utilizaremos a $\dim_{\mathbb{Q}}\mathbb{Q}G$ para concluirmos que $r = p^n$. Temos

$$\begin{array}{ccccc} \dim_{\mathbb{Q}}\mathbb{Q}G & = & \dim_{\mathbb{Q}}\mathbb{Q}(G/G') & + & \dim_{\mathbb{Q}}\mathbb{Q}G(1-\widehat{G'}) \\ p^{2n+1} & = & p^{2n} & + & \dim_{\mathbb{Q}}\mathbb{Q}G(1-\widehat{G'}). \end{array}$$

Logo, $\dim_{\mathbb{Q}}\mathbb{Q}G(1 - \widehat{G'}) = p^{2n}(p-1)$, mas $\dim_{\mathbb{Q}}\mathbb{Q}G(1 - \widehat{G'}) = r^2(p-1)$ e portanto $r = p^n$. ■

Utilizando a proposição anterior e o Lema 3.3, obtemos o seguinte resultado.

Corolário 3.11 *Sejam G e H p-grupos extra-especiais de mesma ordem com p ímpar. Então $\mathbb{Q}G \approx \mathbb{Q}H$.*

De fato, o resultado anterior poderia ser substituído pelo seguinte.

Teorema 3.12 *Seja G um p-grupo extra-especial de ordem p^{2n+1}, com p ímpar. A decomposição de Wedderburn de $\mathbb{Q}G$ é dada por:*

$$\mathbb{Q} \oplus (p^{2n-1} + p^{2n-2} + \ldots + p + 1)\mathbb{Q}(\xi_p) \oplus M_{p^n}(\mathbb{Q}(\xi_p)).$$

Podemos neste momento, dar uma abordagem ao problema do isomorfismo no caso p ímpar, obtendo também neste caso resposta negativa. De fato, utilizando as Proposições 3.8 e 3.11, obtemos o seguinte corolário.

Corolário 3.13 *Sejam p um primo ímpar e G um p-grupo extra-especial. Então $\mathbb{Q}G \approx \mathbb{Q}H$ se, e somente se, H é um p-grupo extra-especial com a mesma ordem de G.*

3.3 Componente Não-Comutativa no Caso $p = 2$

Antes de descrevermos a componente simples não-comutativa de $\mathbb{Q}G$ quando G é um 2-grupo extra-especial, vamos dar alguns exemplos que irão nos ajudar na classificação dessa componente.

Exemplos:

Todos os exemplos de decomposições mostrados abaixo foram calculados através de uma rotina no GAP, utilizando a biblioteca wedderga (veja [5]). Neles, usaremos $\mathbb{H}$ para denotar a álgebra dos quatérnios sobre $\mathbb{Q}$.

1. Decomposições das álgebras de grupos extra-especiais de ordem 2^3:
   (a) $\mathbb{Q}\mathcal{Q} \approx 4\mathbb{Q} \oplus \mathbb{H}$
   (b) $\mathbb{Q}\mathcal{D} \approx 4\mathbb{Q} \oplus \mathrm{M}_2(\mathbb{Q})$.
2. Decomposições das álgebras de grupos extra-especiais de ordem 2^5:
   (a) $\mathbb{Q}\mathcal{Q}^2 \approx 16\mathbb{Q} \oplus \mathrm{M}_4(\mathbb{Q})$
   (b) $\mathbb{Q}\mathcal{D}\mathcal{Q} \approx 16\mathbb{Q} \oplus \mathrm{M}_2(\mathbb{H})$.
3. Decomposições das álgebras de grupos extra-especiais de ordem 2^7:
   (a) $\mathbb{Q}\mathcal{Q}^3 \approx 64\mathbb{Q} \oplus \mathrm{M}_4(\mathbb{H})$
   (b) $\mathbb{Q}\mathcal{D}\mathcal{Q}^2 \approx 64\mathbb{Q} \oplus \mathrm{M}_8(\mathbb{Q})$.

Os exemplos mostrados acima nos dão respostas positivas para o problema do isomorfismo. Mostraremos esse fato de modo geral com o seguinte resultado, levando em consideração os 2-grupos extra-especiais segundo o Teorema 1.12, onde $D_1 \approx D$ (com a apresentação (1.2)) e $\mathcal{Q}_i \approx \mathcal{Q}$, $1 \leq i \leq n$ (com apresentação (1.3)). Além disso os produtos considerados são centrais.

Proposição 3.14 *Seja G um 2-grupo extra-especial de ordem 2^{2n+1} com $n \geq 2$.*

1. *$G \approx \mathcal{D}_1\mathcal{Q}_2 \ldots \mathcal{Q}_n$ e*
   (a) *n par, então $\mathbb{Q}G(1 - \widehat{G'}) \approx M_{2^{n-1}}(\mathbb{H})$*
   (b) *n ímpar, então $\mathbb{Q}G(1 - \widehat{G'}) \approx M_{2^n}(\mathbb{Q})$.*
2. *$G \approx \mathcal{Q}_1\mathcal{Q}_2 \ldots \mathcal{Q}_n$ e*
   (a) *n par, então $\mathbb{Q}G(1 - \widehat{G'}) \approx M_{2^n}(\mathbb{Q})$*
   (b) *n ímpar, então $\mathbb{Q}G(1 - \widehat{G'}) \approx M_{2^{n-1}}(\mathbb{H})$.*

Demonstração: Pelo Teorema 1.12, temos que G é um produto central do tipo $\mathcal{D}_1\mathcal{Q}_2\ldots\mathcal{Q}_n$ ou $\mathcal{Q}_1\mathcal{Q}_2\ldots\mathcal{Q}_n$. Em qualquer caso, $\mathcal{Z}(G) = \mathcal{Z}(\mathcal{D}_1) = \mathcal{Z}(\mathcal{Q}_i) = \langle z\rangle = \{1, z\}$, $1 \leq i \leq n$. Quando $G \approx \mathcal{D}_1\mathcal{Q}_2\ldots\mathcal{Q}_n$ consideraremos a_1 e b_1 geradores de $\mathcal{D}_1$, e a_i e b_i geradores de cada $\mathcal{Q}_i$, se $i \geq 2$, e quando $G \approx \mathcal{Q}_1\mathcal{Q}_2\ldots\mathcal{Q}_n$ consideraremos a_i e b_i geradores de cada $\mathcal{Q}_i$, de acordo com as apresentações dadas em (1.2) e (1.3). Temos que

$$\widehat{G}' = \frac{1+z}{2} \quad \text{e} \quad 1 - \widehat{G}' = \frac{1-z}{2}$$

são idempotentes centrais com $\dim_{\mathbb{Q}}\mathbb{Q}G\left(\frac{1-z}{2}\right) = 2^{2n}$, pelo Teorema 2.10.

Temos, pelo Teorema 2.5, que $\mathbb{Q}G\left(\frac{1-z}{2}\right) \approx M_k(D)$, faltando identificarmos k e D.

Em qualquer caso defina $\mathcal{A} = \{a_1b_1a_ib_i \mid 2 \leq i \leq n\}$. Temos que $\mathcal{A}$ possui $n-1$ elementos de ordem 2 de G que comutam entre si. Tome $N = \langle\mathcal{A}\rangle$. Assim N é um 2-subgrupo abeliano elementar e portanto $|N| = 2^{n-1}$.

Considere o idempotente $\widehat{N} = \frac{1}{2^{n-1}}\sum_{h\in N} h = \prod_{i=2}^{n}\left(\frac{1+a_1b_1a_ib_i}{2}\right)$.

Como $1 - \widehat{G}'$ é central, temos que $(1-\widehat{G}')\widehat{N}$ será um idempotente e $\mathbb{Q}G\left(\frac{1-z}{2}\right)\widehat{N} \subseteq \mathbb{Q}G\left(\frac{1-z}{2}\right)$, com $\dim_{\mathbb{Q}}\mathbb{Q}G\left(\frac{1-z}{2}\right)\widehat{N} = \frac{1}{2}\frac{1}{2^{n-1}}|G| = 2^{n+1}$, de acordo com o Teorema 2.10.

1. (a) Suponha $G = \mathcal{D}_1\mathcal{Q}_2\ldots\mathcal{Q}_n$ e n ímpar.

Defina $\gamma = b_1a_2a_3\ldots a_n \in G$, temos que $\gamma^2 = b_1^2a_2^2a_3^2\ldots a_n^2 = 1\underbrace{z\ldots z}_{par\ vezes} = 1$. Tome f o idempotente da forma $f = \frac{1-\gamma}{2}$. Observemos que γ comuta com os geradores de N, pois $\gamma(a_1b_1a_ib_i) = (b_1a_2a_3\ldots a_n)(a_1b_1a_ib_i)$, e como a_i e b_j comutam com a_j, com $j \neq i$, temos $\gamma(a_1b_1a_ib_i) = b_1a_1a_2a_3\ldots a_nb_1a_ib_i$ e, usando o Lema 1.9, temos $\gamma(a_1b_1a_ib_i) = za_1b_1a_2a_3\ldots a_nb_1a_ib_i$, logo $\gamma(a_1b_1a_ib_i) = za_1b_1a_ia_2a_3\ldots a_ib_i\ldots a_nb_1 = za_1b_1a_ia_2a_3\ldots zb_ia_i\ldots a_nb_1$ e, finalmente, $\gamma(a_1b_1a_ib_i) = z^2(a_1b_1a_ib_i)(b_1a_2a_3\ldots a_n) = (a_1b_1a_ib_i)\gamma$. Assim acabamos de mostrar que os idempotentes f e $\widehat{N}$ comutam entre si. Portanto, podemos encontrar um novo idempotente $e = \left(\frac{1-z}{2}\right)\widehat{N}f$. Calculando o traço desse idempotente, temos

$$\dim_{\mathbb{Q}}\mathbb{Q}Ge = \underbrace{\frac{1}{2^{n+1}}}_{\text{traço}(e)}\underbrace{2^{2n+1}}_{|G|} = 2^n.$$

Mas assim, $\mathbb{Q}G\left(\frac{1-z}{2}\right)$ é simples de dimensão 2^{2n} e contém um ideal à esquerda de dimensão 2^n. Logo $\dim_{\mathbb{Q}}\mathbb{Q}G\left(\frac{1-z}{2}\right) = \dim_{\mathbb{Q}}M_k(D) = k^2[D:Q]$. Assim, $2^{2n} = (2^n)^2[D:\mathbb{Q}]$

e então $[D : \mathbb{Q}] = 1$, ou seja, $D = \mathbb{Q}$. Concluímos que $\mathbb{Q}G(1 - \widehat{G}') \approx M_{2^n}(\mathbb{Q})$.

1. (b) Suponha $G = \mathcal{D}_1\mathcal{Q}_2 \dots \mathcal{Q}_n$ e n par.

Para mostrarmos que $\mathbb{Q}G\left(\frac{1-z}{2}\right) \approx M_{2^{n-1}}(\mathbb{H})$ devemos mostrar que existem elementos A, $B \in \mathbb{Q}G\left(\frac{1-z}{2}\right)$ tais que $A^2 = B^2 = -1$ e $AB = -1BA$. Assim teremos $\mathbb{H} \hookrightarrow \mathbb{Q}G\left(\frac{1-z}{2}\right)$. Considere os seguintes elementos $\alpha = b_1a_2a_3 \dots$ e $\beta = a_1a_2 \dots a_n$ de G. Usando os mesmos argumentos que no item anterior é fácil ver que $\alpha^2 = \beta^2 = z$ e $\alpha\beta = z\beta\alpha$.

Observemos que $\alpha(a_1b_1a_ib_i) = (a_1b_1a_ib_i)\alpha$ e $\beta(a_1b_1a_ib_i) = (a_1b_1a_ib_i)\beta$, deste modo α e β comutam com os geradores de N. Podemos agora definir dois elementos $A = \alpha\widehat{N}\left(\frac{1-z}{2}\right)$ e $B = \beta\widehat{N}\left(\frac{1-z}{2}\right)$ em $\mathbb{Q}G\left(\frac{1-z}{2}\right)$. Temos que $A^2 = B^2 = z\widehat{N}\left(\frac{1-z}{2}\right)$ e $AB = zBA$. Notemos que $z = z\widehat{N}\left(\frac{1-z}{2}\right)$ faz o papel de -1 na componente não comutativa $\mathbb{Q}G\left(\frac{1-z}{2}\right)$. Assim $\mathbb{Q}G\left(\frac{1-z}{2}\right) \approx M_k(\mathbb{H})$, logo $2^{2n} = k^2[\mathbb{H} : \mathbb{Q}]$ e, conseqüentemente, $k = 2^{n-1}$. Portanto, $\mathbb{Q}G\left(\frac{1-z}{2}\right) \approx M_{2^{n-1}}(\mathbb{H})$.

2. (a) Suponha $G = \mathcal{Q}_1 \dots \mathcal{Q}_n$ e n ímpar.

Usaremos o mesmo procedimento que no item anterior. Mostraremos que $\mathbb{H}$ está isomorficamente imerso em $\mathbb{Q}G(1 - \widehat{G}')$. Consideremos $\sigma = a_1a_2 \dots a_n$ e $\tau = b_1b_2 \dots b_n$ em G. Temos $\sigma^2 = \tau^2 = z$, $\sigma\tau = z\tau\sigma$, $\tau(a_1b_1a_ib_i) = (a_1b_1a_ib_i)\tau$ e $\sigma(a_1b_1a_ib_i) = (a_1b_1a_ib_i)\sigma$. Tome $A = \tau\widehat{N}\left(\frac{1-z}{2}\right)$ e $B = \sigma\widehat{N}\left(\frac{1-z}{2}\right)$. Temos que $A^2 = B^2 = z\widehat{N}\left(\frac{1-z}{2}\right)$ e $AB = zBA$. Novamente temos $z\widehat{N}\left(\frac{1-z}{2}\right)$ fazendo o papel de -1 na componente não comutativa. Desta maneira mostramos que $\mathbb{H} \hookrightarrow \mathbb{Q}G(1 - \widehat{G}')$. Assim, como antes, $\mathbb{Q}G\left(\frac{1-z}{2}\right) \approx M_{2^{n-1}}(\mathbb{H})$.

2. (b) Suponha $G = \mathcal{Q}_1 \dots \mathcal{Q}_n$ e n par.

Utilizaremos o mesmo procedimento que no item 1.(a), ou seja, queremos encontrar um idempotente e cuja dimensão de $\mathbb{Q}Ge$ seja 2^n. Para isso, tome $\lambda = a_1a_2 \dots a_n \in G$. É fácil ver que $\lambda^2 = 1$ e que $\lambda(a_1b_1a_ib_i) = (a_1b_1a_ib_i)\lambda$. Como λ comuta com os geradores de N podemos definir um idempotente $e = \left(\frac{1+\lambda}{2}\right)\widehat{N}\left(\frac{1-z}{2}\right)$. Calculando o traço desse idempotente sobre $\mathbb{Q}$, temos

$$\dim_{\mathbb{Q}}\mathbb{Q}Ge = \underbrace{\frac{1}{2^{n+1}}}_{\text{traço}(e)}\underbrace{2^{2n+1}}_{|G|} = 2^n.$$

Mas como $\dim_{\mathbb{Q}} \mathbb{Q}G\left(\frac{1-z}{2}\right) = 2^{2n}$ e encontramos um ideal à esquerda de $\mathbb{Q}G\left(\frac{1-z}{2}\right)$ cuja dimensão sobre $\mathbb{Q}$ é 2^n, concluímos, como antes, que $\mathbb{Q}G(1-\widehat{G}') \approx M_{2^n}(\mathbb{Q})$. ■

Usando o Lema 3.2 e a proposição anterior, temos os seguintes resultados.

Teorema 3.15 *Seja G um 2-grupo extra-especial de ordem 2^{2n+1}, com $G \approx \mathcal{D}_1\mathcal{Q}_2 \ldots \mathcal{Q}_n$. Então a decomposição de Wedderburn de $\mathbb{Q}G$ é dada por*

(i) $2^{2n}\mathbb{Q} \oplus M_{2^{n-1}}(\mathbb{H})$, *se n é par e*

(ii) $2^{2n}\mathbb{Q} \oplus M_{2^n}(\mathbb{Q})$, *se n é ímpar.*

Teorema 3.16 *Seja G um 2-grupo extra-especial de ordem 2^{2n+1}, com $G \approx \mathcal{Q}_1\mathcal{Q}_2 \ldots \mathcal{Q}_n$ então a decomposição de Wedderburn de $\mathbb{Q}G$ é dada por*

(i) $2^{2n}\mathbb{Q} \oplus M_{2^{n-1}}(\mathbb{H})$, *se n é ímpar e*

(ii) $2^{2n}\mathbb{Q} \oplus M_{2^n}(\mathbb{Q})$, *se n é par.*

Portanto, a respeito do problema do isomorfismo, temos uma resposta positiva e podemos dizer o seguinte.

Corolário 3.17 *Seja G um 2-grupo extra-especial de ordem 2^{2n+1} e H um grupo arbitrário. Então $\mathbb{Q}G \approx \mathbb{Q}H$ se, e somente se, $G \approx H$.*

Considerações Finais

Com o objetivo de tratar o Problema do Isomorfismo no sentido proposto por Thrall, em [8] os autores classificam os grupos H com álgebra de grupo racional isomorfa a $\mathbb{Q}G$ onde G é um p-grupo finito nilpotente de classe 2 com centro cíclico. O principal teorema leva em consideração a ocorrência, ou não, de um p-grupo extra-especial como imagem homomórfica de G.

Teorema 3.18 *Seja G um p-grupo finito nilpotente de classe 2 com centro cíclico. Se $\mathbb{Q}G \approx \mathbb{Q}H$ então H é nilpotente de classe 2, $G' \approx H'$ e o centro de G/N é isomorfo ao centro de H/N para qualquer subgrupo N de G'. Reciprocamente, suponha que G e H são p-grupos nilpotentes de classe 2 de mesma ordem com centros cíclicos, $G' \approx H'$ e o centro de G/N_G é isomorfo ao centro de H/N_H para qualquer subgrupo N_G de G' e N_H é o correspondente em H', então*

(i) Se G não é imagem homomórfica de um p-grupo extra-especial temos $\mathbb{Q}G \approx \mathbb{Q}H$.

(ii) Se G é imagem homomórfica de um p-grupo extra-especial e

(a) p ímpar, temos $\mathbb{Q}G \approx \mathbb{Q}H$.

(b) $p = 2$, temos $\mathbb{Q}G \approx \mathbb{Q}H$ se, e somente se, $G \approx H$.

No nosso trabalho mostramos um caso particular deste teorema, pois os grupos extra-especiais possuem $|\mathcal{Z}(G)| = p$ e $G' = \mathcal{Z}(G)$.

Apesar de não termos feito a demonstração do teorema acima, nesta dissertação, foi feita uma implementação no GAP de uma rotina, utilizando a biblioteca de grupos do GAP, que computa os p-grupos G e H com mesma ordem e de classe 2 tais que seus centros sejam cíclicos, $G' \approx H'$ e o centro de G/N_G é isomorfo ao centro de H/N_H

para qualquer subgrupo N_G de G' e N_H é o correspondente em H', ou seja, grupos que satisfazem a recíproca do Teorema 3.18. No entanto, a "ida"do teorema não foi possível de ser implementada, pois não existem ferramentas disponíveis para o cálculo da decomposição de Wedderburn para uma álgebra $\mathbb{Q}G$, onde G é um grupo arbitrário.

Vamos agora considerar estas implementações feitas no GAP onde os exemplos foram calculados como confirmação dos resultados propostos. Para isto, utilizamos o pacote Wedderga [5], desenvolvido por A. Olivieri e Á. del Rio para explicitar as componentes simples na decomposição de Wedderburn de $\mathbb{Q}G$, quando G é um grupo metabeliano. Podemos separar nossas rotinas em 4 partes:

(1) **Função que dada a apresentação do grupo G, calcula a decomposição de Wedderburn da álgebra de grupo $\mathbb{Q}G$.**

```
#Rotina: Calcula a decomposição de Wedderburn para QG
#Autor: Allan Rodrigo Fonseca Teixeira
#Pacotes necessários: Wedderga
#Parâmetros de entrada: Apresentação do grupo G
#Parâmetros de saída: Decomposição de Wedderburn da álgebra de QG
DecWedPGEE:=function(G)
local QG, SAIDA;
if LoadPackage("wedderga")=fail then
   LoadPackage("wedderga");
fi;
QG:=GroupRing(Rationals,G);
SAIDA:=WedderburnDecompositionInfo(QG);
return SAIDA;
end;
```

Exemplo:

```
gap> g:=FreeGroup("a","b","c","d");
gap> qq:=NormalClosure(g,Subgroup(g,[g.1^4,g.2^2*g.3^-2,g.3^2*g.4^-2,g.4^2*g.1^-2,
(g.1^g.2)*g.1,(g.3^g.4)*g.3,Comm(g.1,g.3),Comm(g.1,g.4),Comm(g.2,g.3),Comm(g.2,g.4)]));;
gap>QQ:=g/qq;;
gap> dq:=NormalClosure(g,Subgroup(g,[g.1^2,g.2^4,g.3^2,g.4^2*g.2^-2,(g.2^-2)*(g.1^g.3)*g.1,
(g.2^g.3)*g.2,(g.2^-2)*(g.1^g.4)*g.1^-1,Comm(g.1,g.2),Comm(g.2,g.4),Comm(g.3,g.4)]));
gap> DQ:=g/dq;;
gap> DecWedPGEE(QQ);
[ [ 1, 1, [  ], [  ] ], [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ],
  [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ],
  [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ],
  [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ],
  [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ],
```

```
  [ 1, 2, [  ], [  ] ], [ 4, 2, [  ], [  ] ] ]
gap> DecWedPGEE(DQ);
[ [ 1, 1, [  ], [  ] ], [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ],
  [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ],
  [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ],
  [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ],
  [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ],
  [ 1, 2, [  ], [  ] ], [ 2, 4, [ [ 2, 3, 2 ] ], [  ] ] ]
```

Assim, interpretando as saídas do pacote Wedderga, temos:

$$\mathbb{Q}\mathcal{Q}^2 \approx 16\mathbb{Q} \oplus M_4(\mathbb{Q})$$
$$\mathbb{Q}\mathcal{D}\mathcal{Q} \approx 16\mathbb{Q} \oplus M_2(\mathbb{H}).$$

Para executar essa rotina, necessitamos o conhecimento da apresentação do grupo. Visto que em alguns casos a apresentação do grupo pode ser complicada, surgiu a necessidade de buscar os p-grupos extra-especiais na biblioteca de grupos do GAP e calcular suas respectivas decomposições.

(2) **Função que, para uma dada potência de um primo p, pesquisa todos os p-grupos extra-especiais G com esta ordem e calcula a decomposição de Wedderburn da álgebra de grupo $\mathbb{Q}G$.**

```
#Rotina: Busca os p-grupos extra-especiais e calcula
#        a decomposição de Wedderburn de QG
#Autor: Allan Rodrigo Fonseca Teixeira
#Pacotes necessários: Wedderga
#Parâmetros de entrada: primo p e a ordem de G
#Parâmetros de saída: Decomposição de Wedderburn dos grupos extra-especiais
PGroupsF:=function(p,ord)
local A,G,j,i;
   j:=1;
   G:=[];
   for i in [1..NumberSmallGroups(ord)] do
   A:=SmallGroup(ord,i);
      if not(IsAbelian(A)) then
           if Size(Center(A))=p then
              if Size(DerivedSubgroup(A))=p then
                 G[j]:=A;
                 j:=j+1;
              fi;
           fi;
      fi;
   od;
   return G;
```

```
end;
WDIPGroups:=function(p,ord)
local G,i,QG,AG;
   G:=PGroupsF(p,ord);
   AG:=[];
   if LoadPackage("wedderga")=fail then
      LoadPackage("wedderga");
   fi;
   for i in [1..Size(G)] do
      QG:=GroupRing(Rationals,G[i]);
      AG[i]:=WedderburnDecompositionInfo(QG);;
   od;
   return AG;;
end;
```

Exemplo:

```
gap> WDIPGroups(3,3^5);
[ [ [ 1, 1, [  ], [  ] ], [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ],
      [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ],
      [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ],
      [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ],
      [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ],
      [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ],
      [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ],
      [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ],
      [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ],
      [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ],
      [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ],
      [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ],
      [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ],
      [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ], [ 9, 3, [  ], [  ] ] ],
  [ [ 1, 1, [  ], [  ] ], [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ],
      [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ],
      [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ],
      [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ],
      [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ],
      [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ],
      [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ],
      [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ],
      [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ],
      [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ],
      [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ],
      [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ],
      [ 1, 3, [  ], [  ] ], [ 1, 3, [  ], [  ] ], [ 9, 3, [  ], [  ] ] ] ]
```

Portanto, de acordo com as saídas obtidas, temos

$$\mathbb{Q}\mathcal{N}\mathcal{M} \approx \mathbb{Q} \oplus 40\mathbb{Q}[\xi_3] \oplus \mathrm{M}_9(\mathbb{Q}[\xi_3])$$
$$\mathbb{Q}\mathcal{M}^2 \approx \mathbb{Q} \oplus 40\mathbb{Q}[\xi_3] \oplus \mathrm{M}_9(\mathbb{Q}[\xi_3]).$$

(3) **Função que calcula as decomposições de todas as álgebras de grupos de p-grupos nilpotentes de classe 2 com centro cíclico de uma mesma ordem retornando quais álgebras são isomorfas.**

```
#Rotina: Procura p-grupos nilpotentes de classe 2 com centro cíclico cujas
#        suas álgebras são isomorfas
#Autor: Allan Rodrigo Fonseca Teixeira
#Pacotes necessários: Wedderga
PAIpGN2:=function(p,ord)
local G, #Vetor utilizado para guardar a decomposição de Wedderburn
      A, #Vetor utilizado para guardar os p-grupos nilpotentes de classe 2
      j,i,k, #Variáveis de controle de laço de repetição
      AI,VAUX, #Variáveis auxiliares na procura de álgebras isomorfas
      VAI, #Vetor utilizado para armazenar o índice das álgebras isomorfas
           #do vetor A
      SAIDA; #Vetor de resposta da busca, onde as n-1 posições iniciais contém os
             #grupos de A e a última posição guarda os índices das álgebras isomorfas
   if LoadPackage("wedderga")=fail then
      LoadPackage("wedderga");
   fi;
   j:=1;
   G:=[];
   #Todos os p-grupos de ordem ord e nilpotentes de classe 2
   A:=AllGroups(Size,ord,NilpotencyClassOfGroup,2,IsAbelian,false);
   #Coleta dos p-grupos de A tal que seus centros sejam cíclicos
   for i in [1..Size(A)] do
      if IsCyclic(Center(A[i])) then
              G[j]:=A[i];
              j:=j+1;
      fi;
   od;
   A:=G;
   G:=[];
   #Cria todas as álgebras de grupos dos p-grupos nilpotentes de classe 2
   for i in [1..Size(A)] do
      G[i]:=WedderburnDecompositionInfo(GroupRing(Rationals,A[i]));
   od;
   VAI:=[];
   VAUX:=G;
   #Procura de todas as álgebras isomorfas
   for i in [1..Size(G)-1] do
      if G[i]<>0 then #if VAUX[i]<>0 then
         AI:=[];
         AI[1]:=i;
         k:=2;
         for j in [i+1..Size(G)] do
            if AlgebrasIsomorfas(G[i],G[j]) then
               AI[k]:=j;
               k:=k+1;
               G[j]:=0;
            fi;
         od;
```

```
         G[i]:=0;
         Add(VAI,AI);
      fi;
   od;
   if G[Size(G)]<>0 then
      Add(VAI,[Size(G)]);
   fi;
   SAIDA:=A;
   Add(SAIDA,VAI);
   return SAIDA;
end;
AlgebrasIsomorfas:=function(A,B)
local i, j, VA, VB, SAIDA;
   if Size(A)=Size(B) then
   VA:=[];
   for i in [1..Size(A)] do
      VA[i]:=1;
   od;
   for i in [1..Size(A)] do
      for j in [1..Size(A)] do
         if A[i]=B[j] then
            VA[i]:=0;
            #B[j]:=0;
            break;
         fi;
      od;
   od;
   for i in [1..Size(A)] do
      j:=0;
      if VA[i]<>0 then
         j:=1;
         SAIDA:=false;
         break;
      fi;
   od;
   if j=0 then
      SAIDA:=true;
   fi;
   else
      SAIDA:=false;
   fi;
   return SAIDA;
end;
```

Exemplo:

```
 PAIpGN2(2,2^6);
[ <pc group of size 64 with 6 generators>,
  <pc group of size 64 with 6 generators>,
  <pc group of size 64 with 6 generators>,
  <pc group of size 64 with 6 generators>,
  <pc group of size 64 with 6 generators>,
  <pc group of size 64 with 6 generators>,
```

```
  <pc group of size 64 with 6 generators>,
  [ [ 1, 2 ], [ 3 ], [ 4 ], [ 5 ], [ 6 ], [ 7 ] ] ]
```

(4) Função que determina todos os p-grupos nilpotentes de classe 2 com centro cíclico satisfazendo a volta do Teorema 3.18.

```
# Pacotes necessários: Autpgrp, Sonata
LoadPackage("autpgrp");
LoadPackage("sonata");
PpGN2CCDp:=function(p,ord)
local G,A,j,i,k,l,GL,AUX,VGI,VAUX,GI,SAIDA,SBGI,SBGJ;
   j:=1;
   G:=[];
   #Todos os grupos de ordem ord e nilpotentes de classe 2
   A:=AllGroups(Size,ord,NilpotencyClassOfGroup,2,IsAbelian,false);
   #Coleta dos Grupos de A tais que seus centros sejam cíclicos
   for i in [1..Size(A)] do
      if IsCyclic(Center(A[i])) then
           G[j]:=A[i];
           j:=j+1;
      fi;
   od;
   VGI:=[];
   VAUX:=ShallowCopy(G);
   #Calcula  todos os subgrupos dos subgrupos derivados
   # e verifica se os centros dos quocientes correspondentes são isomorfos
   for i in [1..(Size(G)-1)] do
      if G[i]<>0 then
         GI:=[];
         GI[1]:=i;
         k:=2;
         for j in [i+1..Size(G)] do
            if Size(DerivedSubgroup(G[i]))=Size(DerivedSubgroup(G[j])) then
               l:=0;
               SBGI:=Subgroups(DerivedSubgroup(G[i]));
               SBGJ:=Subgroups(DerivedSubgroup(G[j]));
               for m in [2..Size(SBGI)] do
                  if IsIsomorphicGroup(Center(G[i]/SBGI[m]),Center(G[j]/SBGJ[m])) then
                     l:=l+1;
                  fi;
               od;
               if l=(Size(SBGI)-1) then
                  GI[k]:=j;
                  k:=k+1;
                  G[j]:=0;
               fi;
            fi;
         od;
         G[i]:=0;
         Add(VGI,GI);
      fi;
```

```
   od;
   if G[Size(G)]<>0 then
      Add(VGI,[Size(G)]);
      G[Size(G)]:=0;
   fi;
   SAIDA:=VAUX;
   Add(SAIDA,VGI);
   return SAIDA;
end;
```

Exemplo:

```
 PpGN2CCD(2,2^6);
[ <pc group of size 64 with 6 generators>,
  <pc group of size 64 with 6 generators>,
  <pc group of size 64 with 6 generators>,
  <pc group of size 64 with 6 generators>,
  <pc group of size 64 with 6 generators>,
  <pc group of size 64 with 6 generators>,
  <pc group of size 64 with 6 generators>,
  [ [ 1, 2 ], [ 3 ], [ 4 ], [ 5 ], [ 6 ], [ 7 ] ] ]
```

Pela saída da rotina temos 7 2-grupos finitos de ordem 2^6 e de classe 2 com centro cíclico que são não isomorfos, dos quais apenas os grupos 1 e 2 satisfazem as condições do Teorema 3.18. Concluímos que estes grupos 1 e 2, digamos G e H, não são imagens homomórficas de 2-grupos extra-especiais e por isto $\mathbb{Q}G \approx \mathbb{Q}H$ de acordo com o item (i) do Teorema 3.18. Fazendo a decomposição de Wedderburn para álgebra de grupos racionais dos grupos do exemplo anterior, temos:

```
gap> [ [ [ 1, 1, [ ], [ ] ], [ 1, 2, [ ], [ ] ], [ 1, 2, [ ], [ ] ],
      [ 1, 2, [ ], [ ] ], [ 2, 2, [ ], [ ] ], [ 2, 2, [ ], [ ] ],
      [ 1, 4, [ ], [ ] ], [ 1, 4, [ ], [ ] ], [ 1, 4, [ ], [ ] ],
      [ 1, 4, [ ], [ ] ], [ 1, 4, [ ], [ ] ], [ 2, 2, [ ], [ ] ],
      [ 1, 4, [ ], [ ] ], [ 1, 4, [ [ 2, 3, 2 ] ], [ ] ],
      [ 4, 4, [ ], [ ] ] ],
  [ [ 1, 1, [ ], [ ] ], [ 1, 2, [ ], [ ] ], [ 1, 2, [ ], [ ] ],
      [ 1, 2, [ ], [ ] ], [ 2, 2, [ ], [ ] ], [ 2, 2, [ ], [ ] ],
      [ 1, 4, [ ], [ ] ], [ 1, 4, [ ], [ ] ], [ 1, 4, [ ], [ ] ],
      [ 1, 4, [ ], [ ] ], [ 2, 2, [ ], [ ] ], [ 1, 4, [ ], [ ] ],
      [ 1, 4, [ ], [ ] ], [ 1, 4, [ [ 2, 3, 2 ] ], [ ] ],
      [ 4, 4, [ ], [ ] ] ],
  [ [ 1, 1, [ ], [ ] ], [ 1, 2, [ ], [ ] ], [ 1, 2, [ ], [ ] ],
      [ 1, 2, [ ], [ ] ], [ 1, 4, [ ], [ ] ], [ 1, 4, [ ], [ ] ],
      [ 1, 4, [ ], [ ] ], [ 1, 4, [ ], [ ] ], [ 1, 4, [ ], [ ] ],
      [ 1, 4, [ ], [ ] ], [ 2, 4, [ ], [ ] ], [ 2, 4, [ ], [ ] ],
```

```
    [ 4, 4, [  ], [  ] ] ],
[ [ 1, 1, [  ], [  ] ], [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ],
    [ 1, 2, [  ], [  ] ], [ 1, 4, [  ], [  ] ], [ 1, 4, [  ], [  ] ],
    [ 1, 8, [  ], [  ] ], [ 1, 8, [  ], [  ] ], [ 1, 16, [  ], [  ] ],
    [ 1, 16, [  ], [  ] ], [ 2, 16, [  ], [  ] ] ],
[ [ 1, 1, [  ], [  ] ], [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ],
    [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ],
    [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ], [ 1, 4, [  ], [  ] ],
    [ 1, 4, [  ], [  ] ], [ 1, 4, [  ], [  ] ], [ 1, 4, [  ], [  ] ],
    [ 1, 8, [  ], [  ] ], [ 1, 8, [  ], [  ] ], [ 1, 8, [  ], [  ] ],
    [ 1, 8, [  ], [  ] ], [ 2, 16, [  ], [  ] ] ],
[ [ 1, 1, [  ], [  ] ], [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ],
    [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ],
    [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ],
    [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ],
    [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ],
    [ 1, 2, [  ], [  ] ], [ 1, 4, [  ], [  ] ], [ 1, 4, [  ], [  ] ],
    [ 1, 4, [  ], [  ] ], [ 1, 4, [  ], [  ] ], [ 1, 4, [  ], [  ] ],
    [ 1, 4, [  ], [  ] ], [ 1, 4, [  ], [  ] ], [ 1, 4, [  ], [  ] ],
    [ 4, 4, [  ], [  ] ] ],
[ [ 1, 1, [  ], [  ] ], [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ],
    [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ],
    [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ],
    [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ],
    [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ],
    [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ],
    [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ],
    [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ],
    [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ],
    [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ],
    [ 1, 2, [  ], [  ] ], [ 1, 2, [  ], [  ] ], [ 4, 4, [  ], [  ] ] ] ]
```

E interpretando-as, obtemos:

(i) $4\mathbb{Q} \oplus 6\mathbb{Q}(i) \oplus \mathbb{H} \oplus 3M_2(\mathbb{Q}) \oplus M_4(\mathbb{Q}(i))$

(ii) $4\mathbb{Q} \oplus 6\mathbb{Q}(i) \oplus \mathbb{H} \oplus 3M_2(\mathbb{Q}) \oplus M_4(\mathbb{Q}(i))$

(iii) $4\mathbb{Q} \oplus 6\mathbb{Q}(i) \oplus 2M_2(\mathbb{Q}(i)) \oplus M_4(\mathbb{Q}(i))$

(iv) $4\mathbb{Q} \oplus 2\mathbb{Q}(i) \oplus 2\mathbb{Q}(\sqrt{2} + i\sqrt{2}) \oplus 2\mathbb{Q}(\xi_{16}) \oplus M_2(\mathbb{Q}(\xi_{16}))$

(v) $8\mathbb{Q} \oplus 4\mathbb{Q}(i) \oplus 4\mathbb{Q}(\sqrt{2} + i\sqrt{2}) \oplus M_2(\mathbb{Q}(\xi_{16}))$

(vi) $16\mathbb{Q} \oplus 8\mathbb{Q}(i) \oplus M_4(\mathbb{Q}(i))$

(vii) $32\mathbb{Q} \oplus M_4(\mathbb{Q}(i))$.

Referências Bibliográficas

[1] P. Farb & R. Keith Dennis, *Noncommutative algebra*, Springer-Verlag, New York, 1993.

[2] The GAP Group, *GAP-Groups, Algorithms, and Programming*, version 4.4, Available form: http://www.gap-system.org.

[3] D. Gorenstein, *Finite Groups*, Harper and Row Publishers, New York, 1968.

[4] G. Leal & C. Polcino, *Isomorphic Group (and Loop) Algebras*. Journal of Algebra, **155**(1993),200-201.

[5] A. Olivieri & Á. del Rio, *A GAP 4 package for computing central idempotents and simple components of rational group algebras* (submitted).

[6] D. S. Passman, *The Algebraic Structure of Group Rings*, Wiley-Interscience, New York, 1977.

[7] C. Polcino & S. K. Sehgal, *An Introduction to Group Rings*, Kluwer Academic Publishers, Netherlands, 2002.

[8] A. C. Vieira, & G. Leal, *Isomorphic Rational Group Algebras*, In: Groups, Rings and Group Rings, 2004 - Ubatuba - S.P. Lecture Notes in Pure and Applied Mathematics (2005).