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

Dissertação de Mestrado

Decomposição de Wedderburn para Álgebras de Grupos Racionais de Grupos Metacíclicos Finitos

Douglas Frederico Guimarães Santiago

Orientadora : Ana Cristina Vieira

BELO HORIZONTE, 09 DE FEVEREIRO DE 2006

Abstract

This work deals with the rational group algebra of a finite metacyclic group . The aim of the work is the study of primitive central idempotents, the Wedderburn decomposition of these algebras and, then, to use and produce computacional tools to create a method for testing the isomorphism problem for group algebras in these conditions.

To compute the Wedderburn decomposition, we do not use the classical method, that makes use first of the computation of the central primitive idempotents of $\mathbb{C}G$. We rather use results obtained by Olivieri et all, that allow us to describe the Wedderburn decomposition of $\mathbb{Q}G$ for many finite groups G, for example the abelian-by-supersolvable groups.

Resumo

Este trabalho trata de álgebras de grupos racionais de grupos metacíclicos finitos. O seu objetivo é estudar os idempotentes centrais primitivos, dar a decomposição de Wedderburn destas álgebras e, posteriormente, usar e desenvolver ferramentas computacionais para que, com a determinação da decomposição de Wedderburn, obtenhamos um método para testar o problema do isomorfismo para álgebras de grupos racionais nestas condições.

Ao invés do método clássico para a determinação da decomposição de Wedderburn de $\mathbb{Q}G$ que envolve primeiramente a determinação dos idempotentes centrais primitivos de $\mathbb{C}G$, este trabalho usa resultados obtidos por Olivieri et all, que permitem descrever a decomposição de Wedderburn de $\mathbb{Q}G$ para muitos grupos finitos G, como por exemplo os grupos abelianos-por-supersolúvel.

Sumário

Introdução **1**

1 Resultados sobre Grupos e Álgebras de Grupos **3**

1.1 Conceitos e Notações Elementares 3

1.2 Decomposição de Wedderburn e Idempotentes 7

1.3 O Problema do Isomorfismo 9

1.4 O Produto Cruzado 10

2 Decomposição de $\mathbb{Q}G$ para G Metacíclico **13**

2.1 Pares de Shoda 13

2.2 Idempotentes Centrais Primitivos de $\mathbb{Q}G$ 19

2.3 Componentes Simples de $\mathbb{Q}G$ 32

3 Exemplos com o Uso do GAP **34**

3.1 Exemplos de Decomposição de Wedderburn 34

3.2 Algoritmos Implementados 41

Comentários Finais **47**

Referências Bibliográficas **47**

Introdução

Esta dissertação de mestrado, feita sob orientação da Professora Doutora Ana Cristina Vieira, do Departamento de Matemática da UFMG, teve por base o artigo "The Group of Automorphism of the Rational Group Algebra of a Finite Metacyclic Group", de Aurora Olivieri, Ángel del Rio e Juan Jacobo Símon, [10]. Em tal artigo, os autores investigam o grupo de automorfismos $Aut(\mathbb{Q}G)$ de uma álgebra de grupo racional $\mathbb{Q}G$ de um grupo metacíclico finito G. Isto é feito através do cálculo da decomposição de Wedderburn de $\mathbb{Q}G$. O reconhecimento das componentes simples isomorfas de tal decomposição ainda não é totalmente conhecido em geral, apenas para particulares grupos metacíclicos.

O objetivo principal desta dissertação é apresentar um método para estudar o problema do isomorfismo para álgebras de grupo racionais de grupos metacíclicos finitos, usando ferramentas computacionais, mais precisamente o pacote "Wedderga"do software "Groups, Algorithms and Programming"(GAP). Classicamente, o problema do isomorfismo surgiu na tese de Doutorado de G. Higman (1940) a respeito de anéis de grupos sobre os inteiros, onde Higman perguntava se o isomorfismo $\mathbb{Z}G \cong \mathbb{Z}H$ implicava no isomorfismo $G \cong H$. Ele mesmo provou que a resposta é positiva quando G é abeliano finito, mas, em 2000, M. Hertweck respondeu negativamente a questão de forma geral exibindo dois grupos finitos não isomorfos com anéis de grupos isomorfos sobre os inteiros. O problema do isomorfismo se torna particularmente interessante quando tratado para álgebras de grupos KG, onde K é um corpo.

O Capítulo 1 revisa alguns conceitos e resultados em Teoria de Grupos, introduzindo definições e propriedades dos grupos principais de que se trata o trabalho. Além disso, também apresenta algumas noções sobre representações e caracteres de grupos, apenas na medida em que estas noções vão ser usadas. Este capítulo fala ainda sobre a decomposição de Wedderburn da álgebra de grupo $\mathbb{Q}G$, que será a forma pela qual poderemos avaliar se duas álgebras são ou não são isomorfas. Além disso, relaciona a decomposição de Wedderburn de uma álgebra de grupo com os idempotentes centrais primitivos desta álgebra. Esta é uma maneira direta de lidar com o problema do isomorfismo, principalmente para álgebras de grupos racionais.

No Capítulo 2, desenvolveremos os principais resultados de [10]. Estes resultados nos indicam como construir os idempotentes centrais primitivos de $\mathbb{Q}G$ quando G é um grupo metabeliano e mais especificamente, quando G é metacíclico, podemos explicitar as componentes simples de $\mathbb{Q}G$ através de parâmetros particulares obtidos a partir da apresentação do grupo.

Por fim, no Capítulo 3, construiremos exemplos de decomposições de $\mathbb{Q}G$ para particulares grupos metacíclicos G, usando algoritmos que foram implementados exclusivamente com este objetivo.

Capítulo 1

Resultados sobre Grupos e Álgebras de Grupos

Neste capítulo apresentaremos algumas definições e propriedades elementares a respeito de grupos e seus subgrupos, que serão importantes para o desenvolvimento desta dissertação. Além disso, daremos alguns conceitos e resultados interessantes sobre álgebras de grupos.

1.1 Conceitos e Notações Elementares

Durante todo o trabalho, consideraremos grupos finitos. A ordem de um grupo G será denotada por $|G|$, seu centro por $Z(G)$ e a álgebra de grupo racional sobre G por $\mathbb{Q}G$. Por $H \leq G$ entendemos que H é um subgrupo de G e por $H \lhd G$ que H é normal em G. Se X, Y e Z são subconjuntos não vazios de G então $\langle X \rangle$ é o subgrupo gerado por X e $\langle Y, Z \rangle$ é o subgrupo gerado por Y e Z. Se $H \leq G$ então $N_G(H)$ é o normalizador de H em G. Para $g \in G$ e $x \in \mathbb{Q}G$, denotamos o conjugado por $x^g = g^{-1}xg$. O centralizador de x em G será denotado por $Cen_G(x)$. Se $H \leq G$ também teremos $H^g = g^{-1}Hg$. Se g, $h \in G$ então o comutador de g e h será o elemento $[g, h] = g^{-1}h^{-1}gh$ e o subgrupo derivado de G é $G' = \langle [g, h] : g, h \in G \rangle$.

Para cada inteiro positivo n, ξ_n será a n-ésima raiz primitiva da unidade.

Recordemos ainda que se $\varphi : G \to GL_n(V)$ é uma representação do grupo G sobre um espaço vetorial V de dimensão finita sobre um corpo F, então definimos o caracter de φ como:

$$\begin{aligned} \chi : G &\to F \\ g &\mapsto \chi(g) = tr(g^{\varphi}). \end{aligned}$$

Dizemos que χ é um caracter de G se χ é o caracter de alguma representação de G.

Um caracter χ de G é irredutível se a representação φ é irredutível, ou seja, se V não contém subespaços não triviais invariantes sob a ação de G. Recordemos também que um caracter χ é linear se $dim_F V = 1$. Neste caso, $\chi : G \to F$ é um homomorfismo e faz sentido falar sobre o núcleo de χ. Se K é um subgrupo de G e ψ é um caracter de K então denotamos por ψ^G o caracter de G induzido por ψ.

Conforme veremos mais adiante, caracteres de grupos estão intimamente ligados com os idempotentes na álgebra de grupo $\mathbb{C}G$.

Algumas classes particulares de grupos são importantes pois possuem propriedades específicas que garantem novos resultados interessantes.

Definição 1.1 *Seja G um grupo finito. Dizemos que G é supersolúvel se existe uma sequência de subgrupos*

$$\{1\} \subset G_1 \subset G_2 \subset \ldots \subset G_n = G$$

de forma que cada G_i é normal em G e G_{i+1}/G_i é cíclico.

Desta definição conclui-se facilmente que todo grupo abeliano é supersolúvel. Pois se G é abeliano, temos que $G \cong C_1 \times \ldots \times C_k$ onde cada C_k é um grupo cíclico. Assim

$$\{1\} \subset C_1 \subset C_1 \times C_2 \subset \ldots \subset C_1 \times \ldots \times C_k \cong G$$

é uma sequência que satisfaz a definição. Observa-se então a relação entre os conjuntos de grupos

$$\{\text{grupos cíclicos}\} \subset \{\text{grupos abelianos}\} \subset \{\text{grupos supersolúveis}\}$$

e pode-se exibir exemplos mostrando que as inclusões são próprias.

Denotemos por P_1 e P_2 propriedades de grupos, como por exemplo, se este é abeliano, cíclico, supersolúvel, etc... Definimos que um grupo G é P_1 por P_2 se G possui um subgrupo normal H com a propriedade P_1 e cujo quociente G/H possui a propriedade P_2. No caso em que $P_1 = P_2$, usamos a prefixo meta, por exemplo, um grupo pode ser metacíclico ou metabeliano.

Do que já foi discutido nesta seção, observa-se a relação entre os conjuntos de grupos

$$\{\text{grupos metacíclicos}\} \subset \{\text{grupos metabelianos}\} \subset \{\text{grupos abelianos-por-supersolúvel}\}.$$

Mais especificamente, temos.

Definição 1.2 *Um grupo G é metacíclico do tipo $C_m : C_n$ se G tem um subgrupo cíclico normal H de ordem m com quociente $\dfrac{G}{H}$ cíclico de ordem n.*

Uma categoria importante de grupos nesta dissertação é o dos grupos abelianos-por-supersolúvel, isto é, um grupo G que possui um subgrupo normal abeliano H e cujo quociente G/H é supersolúvel.

O próximo lema busca caracterizar os grupos metacíclicos segundo uma apresentação específica. A demonstração deste resultado se encontra em [6].

Lema 1.3 *Se um grupo G é metacíclico do tipo $C_m : C_n$ então ele pode ser dado pela seguinte apresentação*

$$G = \langle a, b : a^m = 1, b^n = a^s, b^{-1}ab = a^r \rangle \tag{1.1}$$

satisfazendo as condições

$$m|r^n - 1 \quad m|s(r-1), \quad m, n, r, s \in \mathbb{N}, r, s \leq m\,. \tag{1.2}$$

Reciprocamente, se G tem apresentação como em (1.1) e satisfaz as condições em (1.2), então G é metacíclico do tipo $C_m : C_n$.

Lema 1.4 *Sejam $j \in \mathbb{N}$ e $i \in \mathbb{Z}$. Então um grupo G com a apresentação*

$$G = \langle a, b : a^m = 1, b^n = a^s, b^{-1}ab = a^r \rangle$$

satisfaz:

1. $b^{-1}a^ib = a^{ir}$
2. $b^{-j}a^ib^j = a^{ir^j}$
3. $a^ib^j = b^ja^{ir^j}$
4. $ba^ib^{-1} = a^{ir^{(n-1)}}$
5. $b^ja^ib^{-j} = a^{ir^{j(n-1)}}$
6. $b^ja^i = a^{ir^{j(n-1)}}b^j$

Demonstração.

1. $b^{-1}a^ib = \overbrace{\underbrace{b^{-1}ab}\,b^{-1}a\ldots\underbrace{b^{-1}ab}}^{i\ vezes} = \overbrace{\underbrace{a^r}\ldots\underbrace{a^r}}^{i\ vezes} = a^{ir}$.
2. $b^{-j}a^ib^j = \overbrace{\underbrace{b^{-1}}\ldots\underbrace{b^{-1}}}^{j\ vezes}a^i\overbrace{\underbrace{b}\ldots\underbrace{b}}^{j\ vezes} = \overbrace{\underbrace{b^{-1}}\ldots\underbrace{b^{-1}}}^{j-1\ vezes}a^{ir}\overbrace{\underbrace{b}\ldots\underbrace{b}}^{j-1\ vezes} = \overbrace{\underbrace{b^{-1}}\ldots\underbrace{b^{-1}}}^{j-2\ vezes}a^{ir^2}\overbrace{\underbrace{b}\ldots\underbrace{b}}^{j-2\ vezes}\ldots = a^{ir^j}$.

3. $a^i b^j = bb^{-j}a^i b^j$.

4. $ba^i b^{-1} = b^{-(n-1)}b^n a^i b^{-n} b^{n-1} = b^{-(n-1)}a^s a^i a^{-s}\ b^{n-1} = b^{-(n-1)}a^i b^{n-1}$.

5. Seguindo raciocínio análogo ao do item 2.

6. Seguindo raciocínio análogo ao do item 3.

□

Dado um grupo finito G e um corpo F, podemos construir a álgebra de grupo FG, considerando o espaço vetorial sobre F de base $\{g_i\}_{i=1}^{|G|}$, em que g_i percorre os elementos de G. Assim os elementos de FG assumem a forma:

$$\sum_{i=1}^{|G|} \alpha_i g_i\,,\ \alpha_i \in F$$

onde a soma é definida componente a componente e o produto é feito da seguinte forma:

$$(\sum_{i=1}^{|G|} \alpha_i g_i)(\sum_{j=1}^{|G|} \alpha_j g_j) = \sum_{i,j=1}^{|G|} \alpha_i \alpha_j g_i g_j.$$

Desta maneira, FG tem a estrutura de um anel e também é um FG-módulo, além de ser uma álgebra sobre F.

Considerando R um anel com unidade, temos as seguintes definições.

Definição 1.5 *Um R-módulo M é simples se $M \neq 0$ e seus únicos R-submódulos são os triviais.*

Definição 1.6 *Um R-módulo é semisimples se é a soma direta de R-submódulos simples.*

Definição 1.7 *Dizemos que R é um anel semisimples se é semisimples como módulo sobre si mesmo.*

Um resultado que relaciona a semisimplicidade do anel R com a semisimplicidade dos R-módulos é o seguinte teorema cuja demonstração está em [7].

Teorema 1.8 *Um anel R é semisimples se, e somente se, todo R-módulo é semisimples.*

1.2 Decomposição de Wedderburn e Idempotentes

Uma boa parte dos problemas em álgebra consiste em, tendo um conjunto com uma estrutura algébrica complicada, tentar, através de um isomorfismo, enxergar este conjunto segundo uma ótica mais simples, ou mais usual. É isto o que faz o Teorema de Wedderburn, estabelecendo condições suficientes para que um anel possa ser visto como a soma direta de anéis de matrizes sobre anéis de divisão, sendo que anéis de matrizes sobre anéis de divisão podem ser visualizados de uma forma simples como anéis de matrizes em bloco.

Os dois teoremas abaixo, unidos, dizem que a álgebra de grupo $\mathbb{Q}G$, que tem um papel importante neste trabalho, pode ser vista como anel de matrizes sobre anéis de divisão.

Teorema 1.9 *(Teorema de Maschke) Seja G um grupo finito e F um corpo cuja característica não divide a ordem de G. Então todo FG-módulo é semisimples.*

Teorema 1.10 *(Wedderburn-Artin) Se R é um anel semisimples então R é isomorfo à uma soma direta de um número finito de anéis de matrizes sobre anéis de divisão, ou seja,*

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

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

Dado um anel R, dizemos que um elemento $e \in R$ é um idempotente se $e^2 = e$. Tendo em mãos esta definição, vamos enunciar os dois teoremas abaixo, de fácil demonstração, presentes em [7].

Teorema 1.11 *Seja $R = \bigoplus_{i=1}^{t} L_i$ uma decomposição de um anel semisimples como uma soma direta de ideais minimais à esquerda. Então existe uma família $\{e_1, \ldots, e_t\}$ de elementos de R tal que:*

1. *$e_i \neq 0$ é um idempotente, para $1 \leq i \leq t$.*
2. *Se $i \neq j$, então $e_i e_j = 0$.*
3. *$1 = e_1 + \ldots + e_t$.*
4. *e_i não pode ser escrito como $e_i = e_i' + e_i''$, onde e_i' e e_i'' são idempotentes tais que e_i', $e_i'' \neq 0$ e $e_i' e_i'' = 0$, para $1 \leq i \leq t$.*

Reciprocamente, se existe uma família de idempotentes $\{e_1, \ldots, e_t\}$ *satisfazendo as condições acima então os ideais à esquerda* $L_i = Re_i$ *são minimais e* $R = \bigoplus_{i=1}^{t} L_i$.

Uma família de idempotentes satisfazendo as condições do teorema acima é uma família ortogonal completa de idempotentes. Se o idempotente satisfaz a condição 4, ele é dito primitivo.

Teorema 1.12 *Seja* $R = \bigoplus_{i=1}^{s} A_i$ *uma decomposição de um anel semisimples como uma soma direta de ideais minimais bilaterais. Então existe uma família* $\{e_1, \ldots, e_s\}$ *de elementos de* R *tal que:*

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

Os idempotentes do teorema acima são denominados **idempotentes centrais primitivos** de R. Como cada $M_{n_i}(D_i)$ da decomposição de Wedderburn é um ideal bilateral minimal, temos:

$$R \cong Re_1 \oplus \ldots \oplus Re_k$$

onde $Re_i \cong M_{n_i}(D_i)$ e os e_i são idempotentes centrais primitivos de R.

No próximo capítulo, vamos trabalhar com idempotentes centrais primitivos de $\mathbb{Q}G$ quando G é um grupo metacíclico. Vamos usar algumas notações. Em geral, se χ é um caracter irredutível complexo de G então o idempotente central primitivo de $\mathbb{C}G$ associado à χ será denotado por $e(\chi)$ e o idempotente central primitivo de $\mathbb{Q}G$ associado à χ será denotado por $e_{\mathbb{Q}}(\chi)$, isto é, $e_{\mathbb{Q}}(\chi)$ é o único idempotente central primitivo e de $\mathbb{Q}G$ tal que $\chi(e) \neq 0$. Pode-se calcular $e(\chi)$ da seguinte forma:

$$e(\chi) = \frac{1}{|G|} \sum_{g \in G} \chi(1)\chi(g^{-1})g.$$

O método clássico usado para calcular os idempotentes centrais primitivos de $\mathbb{Q}G$ necessita inicialmente o cálculo de $e(\chi)$, mas este processo pode ser muito trabalhoso. Vamos ver como resolver este problema no caso em que G metacíclico de uma maneira mais simples no Capítulo 2.

1.3 O Problema do Isomorfismo

Uma das grandes questões envolvendo álgebras de grupos diz respeito ao problema do isomorfismo. Este questiona quando um isomorfismo entre anéis, $RG \cong RH$ implica no isomorfismos de grupos $G \cong H$. Este problema clássico aparece primeiramente relacionado com anéis de grupos sobre os inteiros na tese de Doutorado de G. Higman. Em 1947, T. M. Thrall formulou o problema da seguinte forma

Dado um grupo G e um corpo F determine todos os grupos H tais que $FG \cong FH$.

Este problema foi tratado por S. Perlis e G. Walker [13] quando eles provaram que para o caso de grupos abelianos sobre o corpo dos racionais, o problema tem resposta positiva.

Teorema 1.13 *(Perlis e Walker) Sejam G um grupo abeliano finito e H um grupo arbitrário tal que $\mathbb{Q}G \cong \mathbb{Q}H$ então $G \cong H$.*

Um importante teorema de D. Passman permite a construção de álgebras de grupos isomorfas restringindo nossa atenção apenas para o corpo $\mathbb{Q}$ dos racionais.

Teorema 1.14 *Sejam G e H grupos finitos tais que $\mathbb{Q}G \cong \mathbb{Q}H$ então, para todo corpo K cuja característica não divide $|G| = |H|$, temos $KG \cong KH$.*

Em relação aos grupos metabelianos, o problema do isomorfismo tem resposta negativa. De fato, isto ocorre devido a um interessante exemplo construído por E. Dade, em 1971.

Para dar este exemplo, consideramos p e q primos distintos com $q \equiv 1 \pmod{p^2}$, por exemplo, podemos tomar $p = 2$ e $q = 5$.

Consideramos os seguintes grupos não abelianos de ordem q^3

$$Q_1 = \langle x_1, y_1, z_1 : x_1^q = y_1^q = z_1^q = 1, [x_1\,,\, y_1] = z_1, z_1 \text{ central}\rangle$$
$$Q_2 = \langle x_2, y_2, z_2 : x_2^q = z_2^q = 1, y_2^q = z_2, [x_2\,,\, y_2] = z_2, z_2 \text{ central}\rangle.$$

Agora, desde que $p|q-1$ e $|\mathcal{U}(\mathbb{Z}_{q^2})| = q(q-1)$ então existe um inteiro n tal que

$$n \not\equiv 1 \pmod{q^2}$$
$$n^p \equiv 1 \pmod{q^2}$$

isto implica $n \not\equiv 1 \pmod{q}$.

Desta forma, considerando $\langle u_1\rangle$ um grupo cíclico de ordem p^2 e $\langle u_2\rangle$ um grupo cíclico de ordem p, podemos definir uma ação de u_i sobre Q_j, para $1 \leq i, j \leq 2$ da seguinte maneira

$$x_j^{u_i} = x_j \;\;,\;\; y_j^{u_i} = y_j^n \;\text{ e }\; z_j^{u_i} = z_j^n$$

que é, de fato, um automorfismo de ordem p de Q_j, já que Q_j é o produto semi-direto do subgrupo normal abeliano $\langle y_j\ ,\ z_j\rangle$ por $\langle x_j\rangle$.

Desta forma, podemos definir os grupos:

$$G_1 = Q_1\langle u_1\rangle \times Q_2\langle u_2\rangle$$

e

$$G_2 = Q_2\langle u_2\rangle \times Q_2\langle u_1\rangle$$

que são grupos metabelianos de ordem p^3q^6. De fato, notamos que

$$G_i' = \langle y_1, z_1\rangle \times \langle y_2, z_2\rangle,\ i = 1, 2$$

e $G_i'' = \{1\}$. Assim, temos o seguinte resultado cuja demonstração está em [12].

Teorema 1.15 *(Dade, 1971): Os grupos G_1 e G_2 definidos acima são não isomorfos, mas para qualquer corpo K temos*

$$KG_1 \cong KG_2.$$

O caso metacíclico ainda está em aberto, ou seja, se G e H são grupos metacíclicos e $\mathbb{Q}G \cong \mathbb{Q}H$, não sabemos se $G \cong H$ ou não. Para este caso, vamos dar alguns exemplos de decomposição de Wedderburn de $\mathbb{Q}G$ no Capítulo 3.

1.4 O Produto Cruzado

Sejam F um corpo arbitrário, E uma F-álgebra de dimensão finita e G um grupo que exerce uma ação σ sobre E como um grupo de automorfismos de E que fixa F.

Desta forma:

$$\begin{aligned} \sigma : G &\to Aut_F(E) \\ g &\mapsto \quad \sigma_g : E \to E \\ &\qquad\quad \alpha \mapsto \sigma_g(\alpha). \end{aligned}$$

Consideremos A um módulo à direita sobre E com base $\beta = \{\mu_g : g \in G\}$, em que μ_g são elementos invertíveis (note que A é espaço vetorial sobre F e $dim_E A = |G|$). Assim, os elementos da base β estão em correspondência biunívoca com G:

$$\begin{aligned} G &\longleftrightarrow \beta \\ g &\longleftrightarrow \mu_g. \end{aligned}$$

Vamos agora introduzir uma multiplicação em A para que este se torne uma álgebra sobre F. Definimos, para $\alpha \in E$, $\mu_g, \mu_h \in A$:

$$\alpha\mu_g = \mu_g\sigma_g(\alpha) \quad \text{ou} \quad \mu_g^{-1}\alpha\mu_g = \sigma_g(\alpha)$$
$$\mu_g\mu_h = \mu_{gh}\tau(g,h) \quad \text{ou} \quad \mu_{gh}^{-1}\mu_g\mu_h = \tau(g,h), \quad \text{para algum } \mu_{gh} \in \beta, \tau(g,h) \in E. \quad [1]$$

Assim, todos os elementos de A podem ser escritos de maneira única como:

$$\sum_{g\in G} \sigma_g^{-1}(\alpha_g)\mu_g = \sum_{g\in G} \mu_g\alpha_g\mu_g^{-1}\mu_g = \sum_{g\in G} \mu_g\alpha_g.$$

Mais precisamente:

$$(\sum_{g\in G} \sigma_g^{-1}(\alpha_g)\mu_g)(\sum_{h\in G} \sigma_g^{-1}(\beta_h)\mu_h) = \sum_{g,h\in G} \sigma_{gh}^{-1}(\tau(g,h)\sigma_h(\alpha_g)\beta_h)\mu_{gh}.$$

Logo A é álgebra sobre F, pois é espaço vetorial sobre F, é um anel e, além disso, se $\lambda \in F$, $a, b \in A$, temos:

$$\lambda(ab) = (\lambda a)b = a(\lambda b).$$

Assim, definimos que A é o **produto cruzado** de E por G, denotado por $A = E * G$.

Particularmente, quando $E = \mathbb{Q}(\xi_p)$, $F = \mathbb{Q}$ e $G = Gal_{\mathbb{Q}}(\mathbb{Q}(\xi_p))$, temos:

$$A = \mathbb{Q}(\xi_p) * Gal_{\mathbb{Q}}(\mathbb{Q}(\xi_p)).$$

Exemplo:

Sejam N um grupo e $K \triangleleft N$. Tome $F = \mathbb{Q}$, $E = \mathbb{Q}K$ e $G = N/K$. Considere o módulo A sobre $\mathbb{Q}K$ com base $\beta = \{n_i\}_{i=1}^{l}$ onde $l = |N/K|$ e

$$N/K = \{n_1K, n_2K \ldots, n_lK\}.$$

Falando de outra forma, $n_i = \phi(n_iK)$, onde ϕ é um inverso à direita da projeção canônica $\Pi : N \to N/K$. Considere então a ação:

$$\begin{aligned} \sigma : N/K &\to Aut_{\mathbb{Q}}(\mathbb{Q}K) \\ n_iK &\mapsto \sigma_{n_i} : \mathbb{Q}K \to \mathbb{Q}K \\ k &\mapsto n_i^{-1}kn_i \ (= k^{n_i}) \end{aligned}$$

e a função cruzada:

$$\begin{aligned} \tau : N/K \times N/K &\to \mathbb{Q}K \\ (n_iK, n_jK) &\mapsto n_{ij}^{-1}n_in_j, \text{ em que } n_{ij} = \phi(n_in_jK). \end{aligned}$$

[1] $\tau : G \times G \to E$ será chamado de função cruzada, enquanto σ é a ação de G sobre E.

Fazendo desta forma, temos que os elementos de $\mathbb{Q}N$ e $\mathbb{Q}K * N/K$ podem ser identificados, pois:

$$N = n_1K \cup n_2K \cup \ldots \cup n_lK.$$

Como $n_in_j = n_{ij}(n_{ij}^{-1}n_in_j)$ e $kn_i = n_i(n_i^{-1}kn_i)$, para $k \in K$, podemos considerar a identificação:

$$\mathbb{Q}N \cong \mathbb{Q}K * N/K.$$

O produto cruzado será uma ferramenta importante no Capítulo 2, onde iremos tentar identificar as componentes simples de $\mathbb{Q}G$ no caso em que G é metacíclico.

Capítulo 2

Decomposição de $\mathbb{Q}G$ para G Metacíclico

Nosso objetivo aqui é determinar as componentes simples da decomposição de Wedderburn de uma álgebra de grupo $\mathbb{Q}G$ quando G é metacíclico finito, classificando aquelas componentes que estão na mesma classe de isomorfismo.

2.1 Pares de Shoda

Nesta seção, vamos dar algumas definições e resultados importantes que são um resumo dos resultados obtidos por A. Olivieri e Á. del Rio em [11]. Usando as notações de [5], consideramos $H \trianglelefteq K \leqslant G$ e $\widehat{K} = \frac{1}{|K|}\sum_{k\in K} k \ \in \mathbb{Q}K$ e definimos:

$$\varepsilon(K,H) = \begin{cases} \widehat{K} & \text{se } K = H \\ \prod_{M\in\mathcal{M}(K,H)}(\widehat{H} - \widehat{M}) & \text{caso contrário} \end{cases}$$

onde $\mathcal{M}(K,H)$ é o conjunto dos subgrupos normais minimais de K que contém H propriamente. Denotamos por $e(G,K,H)$ a soma dos diferentes G-conjugados de $\varepsilon(K,H)$ em $\mathbb{Q}G$. Isto é:

$$e(G,K,H) = \sum_{t\in T} \varepsilon(K,H)^t$$

onde T é um conjunto completo dos representantes de $G/Cen_G(\varepsilon(K,H))$. Notamos que $e(G,K,H)$ é um elemento central de $\mathbb{Q}G$ e se os G-conjugados de $\varepsilon(K,H)$ são ortogonais, temos que $e(G,K,H)$ é um idempotente central de $\mathbb{Q}G$.

Os idempotentes centrais primitivos de $\mathbb{Q}A$ para A abeliano são bem conhecidos (veja [1], [5] e [13].) Uma descrição destes idempotentes em termos de elementos da forma $\varepsilon(A,H)$ foi dada recentemente em [11], conforme o teorema abaixo.

Teorema 2.1 *Se A é um grupo abeliano então os idempotentes centrais primitivos de $\mathbb{Q}A$ são da forma $\varepsilon(A,H)$ em que H é um subgrupo de A tal que A/H é cíclico.*

Para atingir nossos objetivos, precisamos de duas novas definições.

Definição 2.2 *Um par (K, H) de subgrupos de G é um par de Shoda, ou um SP de G, se satisfaz:*

a) $H \lhd K$

b) K/H *é cíclico*

c) Se $g \in G$ *e* $[K, g] \cap K \subseteq H$ *então* $g \in K$.

Definição 2.3 *Um par (K, H) de subgrupos de G é um par de Shoda forte, ou um SSP de G, se satisfaz:*

a) $H \lhd K$ *e* $K \lhd N_G(H) = N$

b) K/H *é um subgrupo maximal abeliano de* N/H *e é cíclico*

c) Para cada $g \in G \setminus N$, $\varepsilon(K, H)\varepsilon(K, H)^g = 0$.

É fácil ver que se (K, H) e um SSP então (K, H) satisfaz as condições a e b da definição de par de Shoda. Na verdade como veremos enunciado no próximo teorema, SSP implica SP. Para demonstrar o item c, usa-se resultados sobre representações e caracteres de grupos, por isso não faremos esta demonstração aqui.

Considerando (K, H) um SSP de G, temos $K/H \lhd N/H$. Nestas condições, considere a projeção canônica

$$\begin{aligned} \Pi : N/H &\to N/K \\ nH &\mapsto nK. \end{aligned}$$

Esta projeção é um epimorfismo e induz um isomorfismo

$$\overline{\Pi} : \frac{N/H}{K/H} \to N/K.$$

Considere ainda uma função $\phi : N/K \to N/H$ tal que $\Pi \circ \phi = Id$. Isto é, ϕ é um inverso à direita de Π. Podemos então deduzir as seguintes observações.

a) Se x é gerador de K/H e $a \in N/K$ então $x^{\phi(a)} \in K/H$. Portanto $x^{\phi(a)} = x^i$, para algum $i \in \mathbb{Z}$.

b) Sejam $[K : H] = k$, ξ_k uma k-ésima raiz primitiva da unidade e $Gal_{\mathbb{Q}}(\mathbb{Q}(\xi_k))$ o grupo de automorfismos de $\mathbb{Q}(\xi_k)$. Temos que

$$\begin{array}{rcl} \sigma : N/H \to Gal_{\mathbb{Q}}(\mathbb{Q}(\xi_k)) & & \\ a \quad \mapsto \quad \sigma(a) : \mathbb{Q}(\xi_k) \to \mathbb{Q}(\xi_k) & & \\ \xi_k \quad \to \quad \xi_k^i \ \ (se \ \ x^a = x^i) & & \end{array}$$

é homomorfismo, pois se $\sigma(a)(\xi_k) = \xi_k^i$ e $\sigma(b)(\xi_k) = \xi_k^j$, então $\sigma(a) \circ \sigma(b)(\xi_k) = \xi_k^{ij}$ e como, $x^{ab} = b^{-1}a^{-1}xab = (x^a)^b = (x^i)^b = x^{ij}$, temos que $\sigma(ab)(\xi_k) = \xi_k^{ij}$.

Claramente, $K/H \leq Ker(\sigma)$. Suponha por absurdo que exista $b \in Ker(\sigma) \leq N/H$ e $b \notin K/H$, logo $\sigma(b)(\xi_k) = \xi_k$ e portanto $x^b = x$. Mas se assim fosse, teríamos:

$$K/H = \langle x \rangle \leq \langle x, b \rangle \leq N/H$$

e $\langle x, b \rangle$ seria abeliano, um absurdo pois K/H é maximal abeliano em N/H, portanto $Ker(\sigma) = K/H$, isto é

$$\frac{N}{K} \cong \frac{N/H}{K/H} \cong \sigma(N/H) \leq Gal_{\mathbb{Q}}(\mathbb{Q}(\xi_k)).$$

Conclui-se então que N/K é abeliano pois é um subgrupo do grupo de automorfismos de $\mathbb{Q}(\xi_k)$.

c) Temos $\Pi(\phi(a)\phi(b)) = \Pi(\phi(a))\Pi(\phi(b)) = ab$ e $\Pi(\phi(ab)) = ab$. Logo, como $\overline{\Pi}$ é isomorfismo, $\overline{\Pi}(\phi(ab)K/H) = \overline{\Pi}(\phi(a)\phi(b)K/H)$ e assim $\phi(ab)^{-1}\phi(a)\phi(b) = x^j \in K/H$.

O próximo resultado nos diz como descrever a álgebra simples $\mathbb{Q}Ge(G, K, H)$, para um (K, H) SSP de G. Sua demonstração está em [11].

Teorema 2.4 *Seja G um grupo finito e $H \leq K \leq G$.*

1. *Se H é o núcleo de um caracter linear χ de K então o caracter induzido χ^G é irredutível se, e somente se, (K, H) é um par de Shoda.*
   Reciprocamente, se (K, H) é um par de Shoda de G então existe um caracter linear χ de K com núcleo H tal que χ^G é irredutível. Neste caso, existe um único $\alpha \in \mathbb{Q}$ tal que

$$e_{\mathbb{Q}}(\chi^G) = \alpha e(G, K, H)$$

   e dizemos que o idempotente central primitivo $e_{\mathbb{Q}}(\chi^G)$ é realizável pelo par de Shoda (K, H).

2. *Se (K, H) é um SSP de G então também é um SP de G e $e(G, K, H)$ é um idempotente central primitivo de $\mathbb{Q}G$, i.e, $\alpha = 1$.*

3. *Se G é abeliano-por-supersolúvel então todo idempotente central primitivo de $\mathbb{Q}G$ é realizável por um SSP.*

4. *Sejam (K, H) um SSP de G, $N = N_G(H)$, $n = [G : N]$ e $\varepsilon = \varepsilon(K, H)$. Então a álgebra simples $\mathbb{Q}Ge(G, K, H)$ pode ser descrita como segue:*

   - $\mathbb{Q}Ge(G, K, H) \cong M_n(\mathbb{Q}N\varepsilon)$.
   - $\mathbb{Q}N\varepsilon = \mathbb{Q}K\varepsilon * N/K$, *i.e,* $\mathbb{Q}N_\varepsilon$ *é um produto cruzado de* N/K *com coeficientes no anel* $\mathbb{Q}K\varepsilon$.
   - *Se* $\phi : N/K \to N/H$ *é um inverso à direita da projeção canônica* $\Pi : N/H \to N/K$ *então* $\phi(N/K)$ *é uma base de* $\mathbb{Q}K\varepsilon * N/K$.
   - *Se* $k = [K : H]$, x *é um gerador de* K/H *e* $y \in K$ *é um representante de* x *então* $\mathbb{Q}K\varepsilon = \mathbb{Q}\langle y\rangle\varepsilon$ *e existe um isomorfismo* $\psi : \mathbb{Q}K\varepsilon \to \mathbb{Q}(\xi_k)$ *dado por* $\psi(y\varepsilon) = \xi_k$.
   - *Se* $\mathbb{Q}K\varepsilon$ *e* $\mathbb{Q}(\xi_k)$ *são identificados por* ψ, *e assim,* $QK\varepsilon * N/K$ *é considerado como o produto cruzado de* N/K *com coeficientes no anel* $\mathbb{Q}(\xi_k)$, *então a ação* σ *e a função cruzada* τ *do produto cruzado associado à base* $\phi(N/K)$ *são dadas por:*

$$\sigma(\xi_k) = \xi_k^i \ , \ se \quad x^a = x^i$$

$$\tau(a, b) = \xi_k^j \ , \ se \quad \phi(ab)^{-1}\phi(a)\phi(b) = x^j.$$

Segue uma idéia da demonstração do item 4 do Teorema anterior.
Primeiro, verificamos que, se (K, H) é um SSP, então conseguimos mostrar que:

1. $\varepsilon(K, H)$ é um idempotente central primitivo de $\mathbb{Q}K$ e, além disso, $g \in H$ se, e somente se, $g\varepsilon(K, H) = \varepsilon(K, H)$.

2. $Cen_G(\varepsilon(K, H)) = N_G(H) = N$, os $g-$conjugados de $\varepsilon(K, H)$ são ortogonais e $e(G, K, H)$ é um idempotente central primitivo de $\mathbb{Q}G$.

Chamando $\varepsilon(K, H)$ de f, temos que $e(G, K, H) = \sum_{g\in T} f^g$, em que T é um conjunto de representantes de N/H. Este conjunto tem $n = [N : H]$ elementos. Além disso, é fácil ver que $\mathbb{Q}Gf \cong \mathbb{Q}Gf^g$ (como $\mathbb{Q}G$-módulos), através da aplicação $x \mapsto g^{-1}xg$. Assim temos:

$$\mathbb{Q}Ge = \bigoplus_{g\in T} \mathbb{Q}Gf^g \cong (\mathbb{Q}Gf)^n$$

Tendo em vista estas considerações, verifica-se que:

$$\mathbb{Q}Ge \cong End_{\mathbb{Q}G}(\mathbb{Q}Ge)^o \cong M_n(End_{\mathbb{Q}G}(\mathbb{Q}gf))^o \cong M_n(End_{\mathbb{Q}G}(\mathbb{Q}gf)^o) \cong M_n(f\mathbb{Q}Gf).$$

O segundo e o terceiro isomorfismo segue de resultados já bem conhecidos. Vamos então analisar o primeiro isomorfismo, mas antes façamos as seguintes considerações.

Por $End_{\mathbb{Q}G}(\mathbb{Q}Ge)^o$ entendemos o anel de endomorfismos de $\mathbb{Q}Ge$ sobre $\mathbb{Q}G$ em que a soma $(+)$ e o produto $(*)$ é definido da seguinte forma:

Se φ e $\overline{\varphi} \in End_{\mathbb{Q}G}(\mathbb{Q}Ge)$ e $\alpha \in \mathbb{Q}G$, então:

- $(\varphi + \overline{\varphi})(\alpha e) = \varphi(\alpha e) + \overline{\varphi}(\alpha e)$

- $(\varphi * \overline{\varphi})(\alpha e) = \overline{\varphi} \circ \varphi(\alpha e)$

Assim para mostrar que $\mathbb{Q}Ge \cong End_{\mathbb{Q}G}(\mathbb{Q}Ge)^o$, construímos a aplicação:

$$\begin{array}{rcl} \psi : \mathbb{Q}Ge \to End_{\mathbb{Q}G}(\mathbb{Q}Ge)^o & & \\ \beta e & \mapsto & \psi_{\beta e} : \mathbb{Q}Ge \to \mathbb{Q}Ge \\ & & \alpha e \quad \mapsto \quad \alpha e \beta e \end{array}$$

ψ é injetiva pois se $\psi(\beta e) = \psi(\gamma e)$ então para todo $\alpha e \in \mathbb{Q}Ge$, $\alpha e \beta e = \alpha e \gamma e$, em particular, se $\alpha = 1$, temos $e\beta e = e\gamma e \Rightarrow \beta e = \gamma e$ (e é central).

ψ é sobrejetiva pois se $\psi \in End_{\mathbb{Q}G}(\mathbb{Q}Ge)^o$ então $\psi(e) = \beta e$, para algum $\beta e \in \mathbb{Q}G$ e, se $\alpha \in \mathbb{Q}G$, $\psi(\alpha e) = \alpha\psi(e) = \alpha\beta e = \alpha e \beta e$.

ψ é homomorfismo, pois:

1. $\psi(\beta e + \gamma e)(\alpha e) = \psi_{\beta e + \gamma e}(\alpha e) = \alpha e(\beta e + \gamma e) = \alpha e \beta e + \alpha e \gamma e = \psi_{\beta e}(\alpha e) + \psi_{\gamma e}(\alpha e)$, Logo: $\psi(\beta e + \gamma e) = \psi(\beta e) + \psi(\gamma e)$.

2. $\psi(\beta e \gamma e)(\alpha e) = \psi_{\beta e \gamma e}(\alpha e) = \alpha e(\beta e \gamma e) = (\alpha e \beta e)\gamma e = \psi_{\gamma e} \circ \psi_{\beta e}(\alpha e) = \psi(\gamma e) \circ \psi(\beta e)(\alpha e) = \psi(\beta e) * \psi(\gamma e)(\alpha e)$ logo, $\psi(\beta e \gamma e) = \psi(\beta e) * \psi(\gamma e)$.

Para mostrar que $f\mathbb{Q}Gf \cong End_{\mathbb{Q}G}(\mathbb{Q}Gf)^o$, construimos uma aplicação semelhante a anterior, observando que, se $\varphi \in End_{\mathbb{Q}G}(\mathbb{Q}Gf)$, então, considerando $\varphi(f) = \alpha f$, $(\alpha \in \mathbb{Q}G)$, temos:

$$\alpha f = \varphi(f) = \varphi(f^2) = f\varphi(f) = f\alpha f.$$

Concluimos então de forma análoga que φ será o produto a direita por um elemento de $f\mathbb{Q}Gf$.

Analisando o anel $f\mathbb{Q}Gf$, verificamos que se $g \in G \setminus N$ então $fgf = gg^{-1}fgf = 0$, assim, na verdade, temos:

$$f\mathbb{Q}Gf = f\mathbb{Q}Nf = \mathbb{Q}Nf \quad \text{pois } f \text{ é central em } N.$$

De tudo isto, concluimos que:

$$\mathbb{Q}Ge \cong M_n(\mathbb{Q}Nf).$$

De acordo com o capítulo anterior, $\mathbb{Q}Nf \cong \mathbb{Q}K * N/Kf = \mathbb{Q}Kf * N/K$. Como $\mathbb{Q}Kf \cong \mathbb{Q}(\xi_k)$ através da aplicação:

$$H \mapsto 1$$
$$x \mapsto \xi_k$$

então concluimos o resultado:

$$\mathbb{Q}Ge(G, K, H) \cong M_n(\mathbb{Q}(\xi_k) *_\tau^\sigma N/K).$$

Tendo em vista o exposto no item 4 do resultado anterior, temos por objetivo agora apresentar um formato mais concreto para a álgebra

$$\mathbb{Q}(\xi_k) * N/K.$$

Para isto, introduziremos a seguir os parâmetros α_i, o_i, β_i e γ_{ij}.

Como N/K é abeliano, consideramos $N/K = C_1 \times C_2 \ldots \times C_m$ onde cada C_i é cíclico de ordem o_i. Desta forma, podemos considerar $N/K = \langle a_1, \ldots, a_m \rangle$ onde $a_i^{o_i} = 1$ e os elementos de N/K são da forma $a_1^{k_1} a_2^{k_2} \ldots a_m^{k_m}$, com $0 \leq k_i < o_i$. Se $\phi : N/K \to N/H$ é o inverso à direita da projeção canônica $\Pi : N/H \to N/K$ do teorema anterior, podemos então tomar:

$$\beta = \{g_1^{k_1} g_2^{k_2} \ldots g_m^{k_m}\}_{k_i=0}^{o_i}$$

para ser a base de $\mathbb{Q}(\xi_k) * N/K$, onde $g_i = \phi(a_i)$.

Desta forma, para determinar o produto de dois elementos de β, precisamos saber o que ocorre com $g_j g_i$, se $j > i$. Neste caso, temos:

$$\phi(a_j a_i)^{-1} \phi(a_j)\phi(a_i) = x^{\lambda_{ij}} \text{ , onde } x \text{ é o gerador de } K/H.$$

Como N/K é abeliano, $a_j a_i = a_i a_j$, mas pela escolha da nossa base, $\phi(a_i a_j) = \phi(a_i)\phi(a_j) = g_i g_j$ daí

$$\phi(a_j a_i)^{-1} \phi(a_j)\phi(a_i) = \phi(a_j)^{-1}\phi(a_i)^{-1}\phi(a_j)\phi(a_i) = [g_j \, , \, g_i] = x^{\lambda_{ij}}.$$

Como $\Pi(\phi(a_i)^{o_i}) = \Pi(\phi(a_i))^{o_i} = 1$ em N/K e $N/K \cong \frac{N/H}{K/H}$, então $g_i^{o_i} = \phi(a_i)^{o_i} = x^{\beta_i} \in K/H$.

Com esta notação, $x^{\phi(a_i)} = x^{g_i} = x^{\alpha_i}$ e assim:

$$\mathbb{Q}(\xi_k) * N/K \cong \mathbb{Q}(\xi_k)(g_1, \ldots, g_m : \xi_k g_i = g_i \xi_k^{\alpha_i}, g_i^{o_i} = \xi_k^{\beta_i}, g_j g_i = g_i g_j \xi_k^{\gamma_{ij}}).$$

No Capítulo 3, veremos alguns exemplos de decomposição de Wedderburn para algumas álgebras de grupos $\mathbb{Q}G$ nos quais explicitaremos a álgebra acima como uma álgebra de matrizes sobre um anel de divisão. Mas, de acordo com os autores de [8], nem sempre é simples dar uma descrição explícita para tal álgebra desta maneira, pois em alguns casos são necessários métodos mais sofisticados para esta interpretação.

2.2 Idempotentes Centrais Primitivos de $\mathbb{Q}G$

O teorema abaixo (veja [11], Teorema 4.7 e [8], Proposição 3.1) fornece meios de encontrar os idempotentes centrais primitivos de $\mathbb{Q}G$ e as álgebras simples geradas por estes idempotentes quando G é um grupo metabeliano. Através dele vamos dar uma forma mais concreta para os idempotentes no caso em que G é metacíclico.

Teorema 2.5 *Se G é um grupo metabeliano finito e A é o elemento maximal do conjunto*

$$\{B \leq G: \quad B \text{ é abeliano} \quad e \quad G' \leq B\} \tag{2.1}$$

então os idempotentes centrais primitivos de $\mathbb{Q}G$ são os elementos da forma $e(G,K,H)$ para (K,H) pares de subgrupos de G satisfazendo as condições:

1. *K é um elemento maximal no conjunto $X_H = \{B \leq G : A \leq B \quad e \quad B' \leq H \leq B\}$*
2. *$\dfrac{K}{H}$ é cíclico.*

Além disso, sejam $k = [K:H]$, $N = N_G(H)$, $n = [G:N]$, x um gerador de K/H e $N/K = C_1 \times \ldots \times C_m$, onde cada C_i é cíclico de ordem o_i. Para cada $i = 1, \ldots, m$, seja $g_i \in N/H$ um representante de um gerador de C_i(um inverso na projeção canônica $\Pi : \frac{N}{H} \to \frac{N}{K}$). Sejam ainda $[\alpha_i]_{i=1,\ldots,m}$, $[\beta_i]_{i=1,\ldots,m}$ e $[\gamma_{ij}]_{1\leq i<j\leq m}$ parâmetros satisfazendo as seguintes relações:

$$x^{g_i} = x^{\alpha_i} \ , \ g_i^{o_i} = x^{\beta_i} \ , \ g_j^{-1} g_i^{-1} g_j g_i = x^{\gamma_{ij}}.$$

Então $\mathbb{Q}Ge(G,K,H) \cong M_n(\mathbf{A})$, onde $\mathbf{A}$ é a álgebra definida pela apresentação:

$$\mathbf{A} = \mathbb{Q}(\xi_k)(g_1, \ldots, g_m : \xi_k g_i = g_i \xi_k^{\alpha_i}, g_i^{o_i} = \xi_k^{\beta_i}, g_j g_i = g_i g_j \xi_k^{\gamma_{ij}}).$$

Um resultado importante, que visa complementar o teorema anterior, decide quando dois pares de Shoda forte (K_1, H_1) e (K_2, H_2) geram o mesmo idempotente. A sua demonstração depende apenas de resultados em Teoria de Representações de Grupos (veja [2], Teorema 45.3).

Proposição 2.6 *Sejam (K_1, H_1) e (K_2, H_2) dois pares de Shoda forte de G e $e_1 = e(G, K_1, H_1)$ e $e_2 = e(G, K_2, H_2)$ os respectivos idempotentes centrais de $\mathbb{Q}G$. Então $e_1 = e_2$ se, e somente se, existe $g \in G$ tal que*

$$K_1^g \cap H_2 = K_2 \cap H_1^g.$$

A partir deste ponto, a não ser se especificado o contrário, G **é um grupo metacíclico do tipo** $C_m : C_n$ **dado pela apresentação (1.1), satisfazendo (1.2)**, e, portanto, a não ser quando especificado o contrário, os inteiros m, n, r e s estão fixados. Vamos em busca dos pares (K, H) de subgrupos de G que satisfazem as condições 1 e 2 do teorema anterior.

Como $\frac{G}{\langle a\rangle}$ é abeliano, temos que $G' \leq \langle a\rangle$, logo $\langle a\rangle$ pertence ao conjunto dado em (2.1), assim é natural tentar buscar um elemento maximal deste conjunto que contenha $\langle a\rangle$. Definindo, para cada $x \in \mathbb{Z}$, o subgrupo $G_x = \langle a, b^x\rangle$, veremos de acordo com o lema abaixo que os subgrupos que contém $\langle a\rangle$ vão assumir justamente esta forma. Para a determinação do subgrupo comutador, também vai ser útil definir o número $m_x = mdc(r^x - 1, m)$.

Lema 2.7 *Os subgrupos de G que contém $\langle a\rangle$ são da forma G_d, com $d|n$. Além disso,*

$$G'_d = \langle [a, b^d]\rangle = \langle a^{r^d-1}\rangle = \langle a^{m_d}\rangle.$$

Demonstração.

Seja A um subgrupo de G que contém $\langle a\rangle$. Pelo Lema 1.4, vemos que todo elemento de G é da forma $a^i b^k$. Se $A \neq \langle a\rangle$ então existe $a^i b^k$ tal que $a^i b^k \in A \setminus \langle a\rangle$. Isto ocorre se, e somente se, $b^k \in A \setminus \langle a\rangle$, logo $\langle a\rangle < \langle a, b^k\rangle \leq A$. Da mesma forma, se $a^{\overline{i}} b^{\overline{k}} \in A \setminus \langle a, b^k\rangle$ então $b^{\overline{k}} \in A \setminus \langle a, b^k\rangle$ e assim, $\langle a\rangle < \langle a, b^k\rangle < \langle a, b^k, b^{\overline{k}}\rangle \leq A$. Como existem k_1 e k_2 tais que $k_1 k + k_2 \overline{k} = mdc(k, \overline{k})$, temos $(b^k)^{k_1}(b^{\overline{k}})^{k_2} = b^{mdc(k,\overline{k})}$. Portanto $\langle a, b^{mdc(k,\overline{k})}\rangle \leq \langle a, b^k, b^{\overline{k}}\rangle$. Como é claro que $\langle a, b^k, b^{\overline{k}}\rangle \leq \langle a, b^{mdc(k,\overline{k})}\rangle$, então obviamente $\langle a, b^k, b^{\overline{k}}\rangle = \langle a, b^{mdc(k,\overline{k})}\rangle$ e desde que G é finito, o processo pára. Concluímos então que todo subgrupo de G que contém $\langle a\rangle$ é da forma $\langle a, b^{\overline{d}}\rangle = G_{\overline{d}}$. Se $d = mdc(\overline{d}, n)$ então $\langle a, b^{\overline{d}}\rangle \leq \langle a, b^d\rangle$. Como existem n_1 e d_1 tais que $n_1 n + d_1 \overline{d} = d$ então $(b^n)^{n_1}(b^{\overline{d}})^{d_1} = b^d$, ou seja, $a^{sn_1}(b^{\overline{d}})^{d_1} = b^d$. Logo $\langle a, b^d\rangle \leq \langle a, b^{\overline{d}}\rangle$ e portanto $\langle a, b^d\rangle = \langle a, b^{\overline{d}}\rangle$. Concluímos assim que sempre podemos tomar d tal que $d|n$.

Para mostrar que $G'_d = \langle a^{r^d-1}\rangle$, basta observar que

$$G'_d = \langle [a, b^d]\rangle = \langle a^{-1}b^{-d}ab^d\rangle = \langle a^{r^d-1}\rangle = \langle a^{m_d}\rangle.$$

□

No próximo lema, daremos efetivamente um elemento maximal para o conjunto dado em (2.1). Para isto, definimos de forma geral o número o_y como sendo a ordem multiplicativa de r módulo y, onde $y > 1$ é um inteiro.

Lema 2.8 *G_{o_m} é um elemento maximal do conjunto*

$$C = \{B \leq G : B \text{ é abeliano e } G' \leq B\}.$$

Demonstração.

1. Temos que $G_{o_m} \in C$, pois $G' = \langle a^{r-1} \rangle \leq \langle a, b^{o_m} \rangle = G_{o_m}$. Além disto, G_{o_m} é abeliano, pois $G'_{o_m} = \langle a^{r^{o_m}-1} \rangle = 1$, desde que $r^{o_m} \equiv 1 \bmod m$.

2. G_{o_m} é um elemento maximal de C, pois se $B \in C$ e $G_{o_m} \leq B$, então $B = G_d$ para algum $d|n$ e $G'_d = \langle a^{r^d-1} \rangle = 1$. Portanto, $r^d \equiv 1 \bmod m$, segue que $o_m|d$, isto é, $B = G_{o_m}$.

□

De acordo com a condição 1 do Teorema 2.5, levando em conta que qualquer grupo que contenha G_{o_m} é da forma G_d com $d|n$, dado um subgrupo E de G temos que analisar o conjunto

$$X_E = \{G_d \leq G : G_{o_m} \leq G_d \quad \text{e} \quad G'_d \leq E \leq G_d\}.$$

Para isto, primeiro vamos caracterizar os subgrupos H de G tais que $G'_d \leq H \leq G_d$ para um inteiro d tal que $d|n$. Com esta intenção, se $x, y, z \in \mathbb{Z}$, definimos:

- $H_{x,y,z} = \langle a^x, a^y b^z \rangle$

- $\beta_d = \{(v, i, c) \in \mathbb{Z}^3 : 0 < dc|n,\ \ 0 < v|m_d \text{ e } v|s + i\frac{n}{dc}\}$.

Lema 2.9 *Se $d|n$ então os subgrupos H de G_d tais que $G'_d \leq H \leq G_d$ são os grupos da forma $H_{v,i,dc}$ com $(v, i, c) \in \beta_d$.*

Demonstração.

Suponha $(v, i, c) \in \beta_d$, isto é, $\overbrace{0 < v|m_d}^{I}$, $\overbrace{0 < dc|n}^{II}$ e $\overbrace{v|s + i\frac{n}{dc}}^{III}$. Daí temos que

$$G'_d = \langle a^{m_d} \rangle \leq \langle a^v \rangle \leq H_{v,i,cd} = \langle a^v, a^i b^{cd} \rangle \leq G_d = \langle a, b^d \rangle.$$

Isto é, $H_{v,i,cd}$ é um subgrupo de G_d contendo G'_d. Reciprocamente, seja H um subgrupo de G_d contendo G'_d e considere $H \cap \langle a \rangle = \langle a^v \rangle$. Como $\langle a^v \rangle = H \cap \langle a \rangle$ contém $G'_d \cap \langle a \rangle = G'_d = \langle a^{m_d} \rangle$, temos então a relação I. Agora, pelo segundo Teorema do Isomorfismo:

$$\frac{H}{\langle a^v \rangle} = \frac{H}{H \cap \langle a \rangle} \cong \frac{H\langle a \rangle}{\langle a \rangle} \leq \frac{G_d}{\langle a \rangle} = \frac{\langle a, b^d \rangle}{\langle a \rangle}.$$

Como todo elemento de G_d é da forma $(b^d)^l a^k$, então $\dfrac{G_d}{< a >}$ é cíclico de ordem $\frac{n}{d}$ gerado por $b^d\langle a\rangle$. Assim, $\dfrac{H\langle a\rangle}{\langle a\rangle}$ é cíclico gerado por $(b^d)^c\langle a\rangle = b^{dc}\langle a\rangle$ para algum divisor c de d, o que garante a relação II.

Por outro lado, existe $i \in \mathbb{Z}$ tal que $\dfrac{H}{\langle a^v\rangle}$ é gerado por $a^i b^{cd}\langle a^v\rangle$. Então, $H = \langle a^v, a^i b^{cd}\rangle = H_{v,i,cd}$. Além disto, como $\dfrac{G_d}{G'_d}$ é abeliano, temos $(a^i b^{cd})^{\frac{n}{cd}} G'_d = (a^{s+i\frac{n}{cd}})G'_d$. Desde que $G'_d \leq \langle H\rangle$ e $H \cap \langle a\rangle = \langle a^v\rangle$, isto implica III.

□

De acordo com o Lema 2.9, vemos que os pares (K, H) do Teorema 2.5 sempre vão ter $H = H_{v,i,cd}$, com $(v, i, c) \in \beta_d$. O próximo lema busca caracterizar $N_G(H)$, que é um grupo importante para o cálculo dos idempotentes e para a decomposição de Wedderburn de $\mathbb{Q}G$. Além disso, este resultado busca condições para que dois grupos satisfazendo as relações impostas para H sejam iguais. Para isto, definimos $o_{v,i} = o_{\frac{v}{mdc(v,i)}}$.

Lema 2.10 *Se $cd|n$, $v|m_d$ e $i \in \mathbb{Z}$ então $H_{v,i,cd} = \{a^j b^k : k \in cd\mathbb{Z}$ e $j \equiv i\frac{k}{cd}$ mod $v\}$. Além disso, se $v|s + i\frac{n}{cd}$ então $H_{v,i,cd} \cap \langle a\rangle = \langle a^v\rangle$ e $N_G(H_{v,i,cd}) = G_{o_{v,i}}$.*

Se $(v_1, i_1, c_1) \in \beta_{d_1}$ e $(v_2, i_2, d_2) \in \beta_{d_2}$ então H_{v_1,i_1,c_1d_1} e H_{v_2,i_2,c_2d_2} são iguais se, e somente se, $v_1 = v_2$, $c_1d_1 = c_2d_2$ e $i_1 \equiv i_2$ mod v_1.

Demonstração.

Primeiramente, considere $L = \{a^j b^k : k \in cd\mathbb{Z}$ e $j \equiv i\frac{k}{cd} \bmod v\}$. Vemos que L é grupo, pois, $1 = a^0 b^0 \in L$ e se $(a^j b^k)$, $(a^{\overline{j}} b^{\overline{k}}) \in L$, usando o Lema 1.4, temos

$$(a^j b^k)(a^{\overline{j}} b^{\overline{k}})^{-1} = a^j b^k b^{-\overline{k}} a^{-\overline{j}} = a^j b^{k-\overline{k}} a^{-\overline{j}} = a^{j-\overline{j}r^{(k-\overline{k})(n-1)}} b^{k-\overline{k}}.$$

Claramente, $k - \overline{k} \in cd\mathbb{Z}$. Como $v|m_d$, temos $v|r^d - 1$, ou seja, $r^d \equiv 1 \bmod v$. Assim

$$r^{(k-\overline{k})(n-1)} = (r^d)^{[\frac{(k-\overline{k})}{d}(n-1)]} \equiv 1 \bmod v.$$

Como $-\overline{j} \equiv -i\frac{\overline{k}}{cd}$ então $-\overline{j}r^{(k-\overline{k})(n-1)} \equiv -i\frac{\overline{k}}{cd}$. Segue que

$$j - \overline{j}r^{(k-\overline{k})(n-1)} \equiv i\frac{k-\overline{k}}{cd}$$

portanto $(a^j b^k)(a^{\overline{j}} b^{\overline{k}})^{-1} \in L$. Agora, considerando $H = H_{v,i,cd}$, ainda das relações $v|m_d$ e $m_d|r^d - 1$ e observando que a^v e $a^i b^{cd} \in L$, temos

$$G'_d \leq \langle a^v\rangle \leq H \leq L \leq G_d = \langle a, b^d\rangle.$$

Assim, $\frac{K}{G'_d}$ é abeliano e portanto

$$a^j b^k G'_d = a^{j-i\frac{k}{cd}}(a^i b^{cd})^{\frac{k}{cd}} G'_d = (a^v)^t (a^i b^{cd})^{\frac{k}{d}} G'_d$$

quando $j \equiv i\frac{k}{d} \bmod v$, ou seja, $a^j b^k \in H$. Logo $H = L$. Por outro lado, se $x \in H \cap \langle a \rangle$ então $x = a^j b^k$, sendo que $n|k$ e $j \equiv i\frac{k}{cd} \bmod v$. Logo $x = a^{j+s\frac{k}{n}}$. Se $v|s + i\frac{n}{cd}$ então $(j + s\frac{k}{n}) \equiv (i\frac{k}{cd} + s\frac{k}{n}) \equiv (i\frac{n}{cd} + s)\frac{k}{n} \equiv 0 \bmod v$. Portanto $x \in \langle a^v \rangle$ e assim, $H \cap \langle a \rangle = \langle a^v \rangle$. Da relação $G'_d \leq H \leq G_d$, tiramos que $N_G(H) \geq G_d$ e portanto, pelo Lema 2.7, $N_G(H) = G_t$ para algum divisor t de d. Do fato que $H \lhd G_t$ temos que

$$b^{-t}(a^i b^{cd})b^t = a^{ir^t} b^{cd} \in H \Leftrightarrow a^{ir^t} b^{cd} (a^i b^{cd})^{-1} = a^{i(r^t-1)} \in H$$
$$a^{ir^t} b^{cd} (a^i b^{cd})^{-1} = a^{i(r^t-1)} \in H \Leftrightarrow v|i(r^t-1) \Leftrightarrow \tfrac{v}{mdc(v,i)}|r^t - 1$$
$$\tfrac{v}{mdc(v,i)}|r^t - 1 \Leftrightarrow r^t \equiv 1 \bmod \tfrac{v}{mdc(v,i)} \Leftrightarrow t \in o_{v,i}\mathbb{Z}.$$

Logo $t = o_{v,i}$.

Tome $H_1 = \langle a^{v_1}, a^{i_1} b^{c_1 d_1} \rangle = \langle a^{v_2}, a^{i_2} b^{c_2 d_2} \rangle = H_2$ satisfazendo $0 < c_j d_j | n$, $0 < v_j | s + i_j \frac{n}{c_j d_j}$ e $0 < v_j | m_{d_j}$ $(j = 1, 2)$. Desta forma,

$$H_1 \cap \langle a \rangle = \langle a^{v_1} \rangle = \langle a^{v_2} \rangle = H_2 \cap \langle a \rangle.$$

Da relação $v_j | m_{d_j} | m$, segue que $v_1 = v_2$. Como $G'_{d_j} \leq \langle a^{v_j} \rangle \leq H_j \leq G_{d_j}$, $\frac{H_j}{\langle a^{v_j} \rangle}$ é abeliano e temos assim que os elementos de $\frac{H_j}{\langle a^{v_j} \rangle}$ são da forma :

$$a^{i_j} b^{c_j d_j} \langle a^{v_j} \rangle, (a^{i_j} b^{c_j d_j})^2 \langle a^{v_j} \rangle \ldots (a^{i_j} b^{c_j d_j})^{\frac{n}{c_j d_j}} \langle a^{v_j} \rangle = a^{i_j \frac{n}{c_j d_j}} b^n \langle a^{v_j} \rangle = a^{i_j \frac{n}{c_j d_j} + s} \langle a^{v_j} \rangle.$$

O último termo é a identidade pois $v_j | s + i_j \frac{n}{c_j d_j}$ e assim, $\frac{H_j}{\langle a^{v_j} \rangle}$ é cíclico de ordem $\frac{n}{c_j d_j}$, logo $c_j d_j = \frac{n|<a^{v_j}>|}{|H_j|}$. Como $v_1 = v_2 = v$ e $H_1 = H_2$, temos que $c_1 d_1 = c_2 d_2$. Como $H_1 = H_2$ e $a^{i_2} b^{c_2 d_2} \in H_1$, $i_2 \equiv i_1 \frac{c_2 d_2}{c_1 d_1} \bmod v$ e como $c_1 d_1 = c_2 d_2$, segue que $i_1 \equiv i_2 \bmod v$. A recíproca é imediata.

□

Pelos lemas anteriores, vimos que fixado um subgrupo E de G, se o conjunto

$$X_E = \{B \leq G : G_{o_m} \leq B \quad \text{e} \quad B' \leq E \leq B\}$$

é não vazio então um elemento maximal deste tem que assumir a forma G_d, com $d|n$ e $E = H = H_{v,i,cd}$, com $(v, i, c) \in \beta_d$. O próximo objetivo é estabelecer condições para que $\dfrac{G_d}{H}$ seja cíclico e, neste caso, dar uma forma para seu gerador. Isto vai ser feito através de dois lemas, o primeiro de caráter mais geral e técnico, envolve resultados de Teoria de Números.

Lema 2.11 *Sejam m, $r \in \mathbb{Z}$ tais que $mdc(r,m) = 1$. Então para todo $k > 0 \in \mathbb{Z}$, existe j tal que $mdc(j, mk) = 1$ e $j \equiv r \ mod\ m$.*

Demonstração.

Como $mdc(r,m) = 1$, então dado um inteiro k, $mdc(k,m)$ e $mdc(k,r)$ não possuem fatores primos comuns. Assim, o número $R = \frac{k}{mdc(k,m)mdc(k,r)}$ é inteiro.

Faça $j = r + Rm$. Temos, $j \equiv r \bmod m$. Suponha que $mdc(j, mk) \neq 1$. Logo, existe um primo q tal que $q|mk$ e $q|j$. Se $q|m$ temos $q|r$ e chega-se a uma contradição. Se q não divide m, então $q|\frac{k}{mdc(k,m)}$. Neste caso, temos: 1) Se $q|r$, pela expressão de j, vemos que $q|R$, o que é um absurdo pois R não tem fatores primos de r. 2) Se q não divide r, pela expressão de R, vemos que $q|R$, mas se assim fosse, pela expressão de j teríamos que $q|r$, um absurdo. Logo $mdc(j, mk) = 1$.

□

Lema 2.12 *Sejam $(v,i,c) \in \beta_d$ e $H = H_{v,i,dc}$. Se G_d/H é cíclico então $mdc(v,i,c) = 1$. Reciprocamente, se $mdc(v,i,c) = 1$ então existem inteiros v_1, c_1, i_1, i' e c' satisfazendo:*

$$v_1 v + c_1 c = 1 + i_1 i \quad e \quad i' i_1 + c' c = 1$$

e $x = a^{c_1} b^{di_1} H$ é um gerador de G_d/H, ou seja, este grupo é cíclico.

Demonstração.

Seja $(v,i,c) \in \beta_d$ e tome $H = H_{v,i,cd}$. Do lema anterior, temos que $G'_d \leq H$, logo $\dfrac{G_d}{H}$ é abeliano, então:

$$\frac{G_d}{H} = \langle a, b^d : a^v = 1, b^{cd} = a^{-i}, b^d a = a b^d \rangle.$$

Pela apresentação acima vemos que $|\dfrac{G_d}{H}| = vc$. Se $z = a^l b^{dj} H \in \dfrac{G_d}{H}$, então:

$$z^{(\frac{vc}{mdc(v,i,c)})} = (a^l b^{dj})^{(\frac{vc}{mdc(v,i,c)})} H = (a^v)^{(\frac{lc}{mdc(v,i,c)})} (b^{cd})^{(\frac{vj}{mdc(v,i,c)})} H = (a^v)^{(\frac{-ij}{mdc(v,i,c)})} H = H.$$

Assim, como $|\frac{G_d}{H}| = vc$, se $\frac{G_d}{H}$ é cíclico então $mdc(v,i,c) = 1$.

Reciprocamente, suponha agora $mdc(v,i,c) = mdc(i, mdc(v,c)) = 1$. Logo existem α e β inteiros, tais que $\alpha i + \beta mdc(v,c) = 1$. É fácil verificar que para qualquer $\gamma \in \mathbb{Z}$, vale:

$$(\alpha + \gamma\, mdc(v,c))i + (\beta - \gamma i) mdc(v,c) = 1. \tag{2.2}$$

Temos que $mdc(\alpha, mdc(v,c)) = 1$ e como c é múltiplo de $mdc(v,c)$, pelo Lema 2.11, temos que existe j tal que $j \equiv \alpha \bmod (mdc(v,c))$ e $mdc(j,c) = 1$, isto é, $j = \alpha + Rmdc(v,c)$. Fazendo $\gamma = R$ em (3.2), temos que:

$$ji + (\beta - Ri) mdc(v,c) = 1.$$

Mas $mdc(v,c) = \overline{\alpha}v + \overline{\beta}c$, logo:

$$ji + (\beta - Ri)\overline{\alpha}v + (\beta - Ri)\overline{\beta}c = 1.$$

Considerando $v_1 = (\beta - Ri)\overline{\alpha}$, $c_1 = (\beta - Ri)\overline{\beta}$ e $j = -i_1$, temos que:

$$-i_1 i + v_1 v + c_1 c = 1 \qquad \text{e} \qquad mdc(i_1, c) = 1.$$

Concluímos então que existem i_1, v_1, c_1, i' e c' tais que:

$$-i_1 i + v_1 v + c_1 c = 1 \qquad \text{e} \qquad c'c + i'i_1 = 1.$$

Tome então $x = a^{c_1} b^{di_1} H \in \dfrac{G_d}{H}$. Assim:

$$x^c H = (a^{c_1} b^{di_1})^c H = a^{c_1 c} a^{-ii_1} H = a^{c_1 c - ii_1} H = a^{1 - v_1 v} H = aH.$$

além disso,

$$\begin{aligned}
&x^{i'v_1 v - i} H = x^{i'(1 - c_1 c + i_1 i) - i} H = x^{i'(1 - c_1 c) - i(1 - i'i_1)} H = x^{i'(1 - c_1 c) - i(c'c)} H \\
&= a^{c_1 i'} b^{di_1 i'} a^{-c_1 c(c'i + c_1 i')} b^{-di_1(c'i + c_1 i')} H = a^{c_1 i'} b^{di_1 i'} a^{-c_1 c(c'i + c_1 i')} a^{ii_1(c'i + c_1 i')} H \\
&= a^{c_1 i'} b^{di_1 i'} a^{(-1 - i_1 i + v_1 v)(c'i + c_1 i')} a^{ii_1(c'i + c_1 i')} H = a^{c_1 i'} b^{di_1 i'} a^{-(c'i + c_1 i')} H = b^{di_1 i'} a^{-ic'} H \\
&= b^{di_1 i'} b^{dcc'} H = b^{d(i_1 i' + cc')} H = b^d H.
\end{aligned}$$

Como x gera os geradores de $\dfrac{G_d}{H}$, este é cíclico gerado por x.

□

Fixado $H = H_{v,i,cd}$ com $(v,i,c) \in \beta_d$, o próximo lema determina efetivamente um elemento maximal K do conjunto

$$\{B \leq G : G_{o_m} \leq B \quad \text{e} \quad B' \leq H \leq B\}$$

e, usando o Teorema 2.5 e os lemas anteriores, chegamos a uma conclusão sobre a álgebra simples gerada pelo idempotente relacionado ao par (K,H), quando $\dfrac{K}{H}$ é cíclico.

Lema 2.13 *Seja $d|n$ e assuma que $(v,i,c) \in \beta_d$ e $mdc(v,i,c) = 1$. Então G_{o_v} é o único elemento maximal de $\{B \leq G : G_{o_m} \leq B, B' \leq H_{v,i,dc} \leq B\}$.*

Demonstração.

Tome $H = H_{v,i,cd}$ e considere o conjunto:

$$X = \{B \leq G : G_{o_m} \leq B, B' \leq H \leq B\}.$$

Temos que X é não vazio, pois como $(v,i,c) \in \beta_d$, temos

$$v|m_d \,\text{e}\, m_d|m \Rightarrow r^{o_m} \equiv 1 \bmod v \Rightarrow o_v|o_m \Rightarrow G_{o_m} \leq G_{o_v}.$$

Além disso, $v|m_d$, portanto $v|r^d - 1$, isto é, $r^d \equiv 1 \bmod v$ e portanto $o_v|d$. Assim, $G_d = \langle a, b^d \rangle \leq \langle a, b^{o_v} \rangle = G_{o_v}$. Segue que:

$$G'_{o_v} = \langle a^{r^{o_v}-1} \rangle \leq \langle a^v \rangle \leq H \leq G_d \leq G_{o_v},$$

isto é, $G_{o_v} \in X$.

Agora tome $B \in X$. Como $G_{o_m} \leq B$, então $B = G_t$ para algum divisor t de o_m e

$$B' = \langle a^{r^t-1} \rangle \leq H \cap \langle a^v \rangle \Rightarrow v|r^t - 1 \Rightarrow r^t \equiv 1 \bmod v \Rightarrow o_v|t \Rightarrow G_t \leq G_{o_v}.$$

Logo G_{o_v} é o único elemento maximal de X.

□

Agora, como G_{o_v} é o único elemento maximal do conjunto definido acima, pelo Lema 2.9, o par (G_{o_v}, H), onde $H = H_{v,i,co_v}$ e $(v,i,c) \in \beta_{o_v}$ satisfaz a condição 1 do Teorema 2.5. Mas como $mdc(v,i,c) = 1$, pelo Lema 2.12 $\dfrac{G_{o_v}}{H}$ é cíclico. Deste modo, o par também satisfaz a condição 2 do Teorema 2.5, ou seja, quando G é metacíclico, os idempotentes centrais primitivos de $\mathbb{Q}G$ são da forma:

$$e(G, G_{o_v}, H_{v,i,co_v}) \qquad \text{com} \qquad (v,i,c) \in \beta_{o_v} \qquad \text{e} \qquad mdc(v,i,c) = 1.$$

Agora que já sabemos, de certa forma, determinar os idempotentes centrais primitivos de $\mathbb{Q}G$ para um grupo metacíclico G, resta então estabelecer condições para que dois idempotentes sejam iguais e dar uma forma mais concreta para os idempotentes, principalmente com relação à questão de quando $G_{o_v}/H_{v,i,o_v c_v}$ é cíclico. Para isto, antes vamos precisar de um lema auxiliar em Teoria de Números. Com o intuito de reduzir o texto nas demonstrações dos teoremas seguintes, vamos definir:

- $v_p(x)$ [1] como a quantidade de vezes em que o primo p aparece na fatoração do inteiro x. Por convenção, $v_p(0) = \infty$.

[1] v_p pode ser interpretada como uma valorização p-ádica em $\mathbb{Z}$

Lema 2.14 *Sejam x, h, t, f, i, $z \in \mathbb{Z}$ então:*

1. *Se f é o menor divisor positivo h de x tal que $mdc(x/h, y)$ divide z então todo divisor primo de f é também um divisor primo de $\frac{y}{mdc(x/f,y)}$.*
2. *Se $c = ft|x$, $y|z + i\frac{x}{c}$, $mdc(y, i, c) = 1$ então t divide $\frac{x/f}{mdc(x/f,y)}$.*

Demonstração.

1. Se p é um primo divisor de f então $mdc(\frac{px}{f}, y) = mdc(\frac{x}{f/p}, y)$ não divide z. Como $mdc(x/f, y)$ divide z temos que $mdc(x/f, y) \neq mdc(\frac{px}{f}, y)$. Logo $mdc(\frac{px}{f}, y) = p\, mdc(x/f, y)$ e segue que $p|y$. Suponha então que p não divida $\frac{y}{mdc(x/f,y)}$. Assim, $v_p(x/f) \geq v_p(y)$, mas desta forma, $mdc(p\frac{x}{f}, y) = mdc(\frac{x}{f/p}, y) = mdc(x/f, y)$ divide z o que é um absurdo. Logo, p divide $\frac{y}{mdc(x/f,y)}$.
2. Para mostrar que t divide $\frac{x/f}{mdc(x/f,y)}$, vamos mostrar que se p é um fator primo de t então $v_p(t) \leq v_p(\frac{x/f}{mdc(x/f,y)})$. Se p não divide $mdc(x/f, y)$ então, como $t|(x/f)$, é óbvio que $v_p(t) \leq v_p(\frac{x/f}{mdc(x/f,y)})$. Agora, se $p|mdc(x/f, y)$ então $p|c$ e $p|y$. Como $mdc(y, i, c) = 1$, p não divide i. Por outro lado, como $mdc(x/f, y)|z$, $v_p(mdc(x/f, y)) \leq v_p(z)$. Como $y|z + i\frac{x}{ft}$, $v_p(y) \leq v_p(z + i\frac{x}{ft})$ e assim, $v_p(y) \leq v_p(i\frac{x}{ft})$. Como p não divide i, $v_p(y) \leq v_p(\frac{x}{ft}) = v_p(x/f) - v_p(t)$. Portanto, $v_p(t) \leq v_p(x/f) - v_p(mdc(x/f, y))$ o que implica que $v_p(t) \leq v_p(\frac{x/f}{mdc(x/f,y)})$.

□

Agora vamos precisar de algumas notações, dadas abaixo.

- c_v = menor inteiro positivo h, divisor de $\frac{n}{o_v}$, tal que $mdc(v, \frac{n/o_v}{h})$ divide s.
- $n_v = \frac{n}{o_v c_v}$.
- $D_v = mdc(v, n_v)$.
- $n'_v = \frac{n_v}{D_v}$.
- $v'_v = \frac{v}{D_v}$.
- i_v = um inteiro arbitrário satisfazendo $v|s + i_v n_v$.

Lema 2.15 *Sejam $v|m$, $t|n'_v$ e i um inteiro qualquer então:*

1. *$mdc(v, \frac{n_v}{t}) = D_v$ e além disso, $v|s + i\frac{n_v}{t}$ se, e somente se, $i = i_v t + v'_v j$ para algum $j \in \mathbb{Z}$.*

2. *Se* $v|s+in_v$ *então* $mdc(i,c_v)=1$*, ou equivalentemente,* $mdc(i_v+v'_vj,c_v)=1$*, para cada* $j\in\mathbb{Z}$*.*

3. *Todo divisor primo de* c_v *também divide* v'_v*.*

4. *Se* $j\in\mathbb{Z}$ *e* $i=i_vt+v'_vj$ *então:*

$$mdc(v,i,c_vt)=1 \qquad \Leftrightarrow \qquad mdc(v,i,t)=1 \qquad \Leftrightarrow \qquad mdc(v,j,t)=1.$$

Demonstração.

1. Se $t|\dfrac{n_v}{mdc(v,n_v)}$ e q é um fator primo de t então $q^{v_q(t)}|\dfrac{n_v}{mdc(v,n_v)}$. Assim, $v_q(n_v)-v_q(v)\geq v_q(t)$. Logo, $mdc(v,n_v)=mdc(v,\frac{n_v}{q^{v_q(t)}})$. Como isto ocorre para todo q fator primo de t então $D_v=mdc(v,n_v)=mdc(v,\frac{n_v}{t})$.

   Suponha agora que $i=i_vt+v'_vj$ para algum $j\in\mathbb{Z}$. Então:

$$s+i\tfrac{n_v}{t}=s+(i_vt+v'_vj)\tfrac{n_v}{t}=s+i_vn_v+v'_vj\tfrac{n_v}{t}=s+i_vn_v+\tfrac{v}{D_v}j\tfrac{n_v}{t}=s+i_vn_v+\tfrac{n_v}{tD_v}jv\ .$$

   A última igualdade se deve ao fato que $D_v|\dfrac{n_v}{t}$. Por definição de i_v, temos $v|s+i_vn_v$. Assim, $v|s+i\frac{n_v}{t}$.

   Reciprocamente, suponha $v|s+i\frac{n_v}{t}$, então existe $\alpha\in\mathbb{Z}$ tal que $v\alpha=s+i\frac{n_v}{t}$. Logo $i=\frac{(v\alpha-s)t}{n_v}$. Como $v|s+i\frac{n_v}{t}$ então $mdc(v,n_v/t)=mdc(v,n_v)|s$. Portanto, existem i_v e β tais que $v\beta=s+i_vn_v$. Assim:

$$i=\tfrac{(v(\beta-\alpha)+v\beta-s)t}{n_v}=\tfrac{(v(\beta-\alpha)+i_vn_v)t}{n_v}=\tfrac{v(\beta-\alpha)t}{n_v}+i_vt=\tfrac{v(\beta-\alpha)tD_v}{d_vn_v}+i_vt=i_vt+v'_v[\tfrac{(\beta-\alpha)tD_v}{n_v}].$$

   Basta então fazer $j=\frac{(\beta-\alpha)tD_v}{n_v}$.

2. Tome $h=mdc(i,c_v)$. Então $v|s+\frac{i}{h}\frac{n/o_v}{c_v/h}$, logo existe $\alpha\in\mathbb{Z}$ tal que $s=\alpha v+\frac{i}{h}\frac{n/o_v}{c_v/h}$. Portanto, $mdc(v,\frac{n/o_v}{c_v/h})|s$. Pela definição de c_v, temos $\frac{c_v}{h}\geq c_v$, logo $h=1$.

3. Decorre do Lema 2.14.

4. Como $mdc(v,j,t)|mdc(v,i,t)|mdc(v,i,c_vt)$, temos que mostrar apenas que $mdc(v,j,t)=1$ implica em $mdc(v,i,c_vt)=1$. Suponha, por absurdo que $mdc(v,j,t)=1$ e que p seja um primo tal que $p|mdc(v,i,c_vt)$. Se $p|c_v$, pelo lema anterior, $p|v'_v$ e então $p|i_vt$. Portanto, $p|mdc(i_vt,c_v)$, o que implica $p|mdc(i,c_v)$, contradizendo 2. Logo p não divide c_v e portanto

$p|t$. Segue que $p|mdc(v,i,t)$. Desta forma, $p|v'_v j$. Como $p|t$ e $t|n'_v$, temos $p|n'_v$ e $p|v'_v$, o que é um absurdo pois $mdc(n'_v, v'_v) = 1$. Isto mostra que:

$$mdc(v,j,t) = 1 \qquad \Rightarrow \qquad mdc(v,i,t) = 1 \qquad \Rightarrow \qquad mdc(v,i,c_v t) = 1$$

o que conclui o resultado.

□

Nosso objetivo é chegar a uma conclusão final sobre a forma dos idempotentes centrais primitivos de $\mathbb{Q}G$, quando G é metacíclico dado pela apresentação (1.1). Para isto, defina:

$$\mathcal{A} = \mathcal{A}_{m,r,n,s} = \{(v,j,t) \in \mathbb{Z}^3 : \ 0 < v|m \ , \ 0 < t|n'_v \ , \ 0 \leq j \leq D_v \ \text{ e } \ mdc(v,j,t) = 1\}.$$

Se $a = (v,j,t) \in \mathcal{A}$ então defina:

$$i(a) = i_v t + v'_v j \quad \text{ e } \ e_a = e_{v,j,t} = e(G, G_{o_v}, H_{v,i(a),o_v c_v t}).$$

É fácil verificar que se $a \in \mathcal{A}$ então e_a é um idempotente central primitivo de $\mathbb{Q}G$. De fato, como $v|r^{o_v} - 1$ e $v|m$, temos que $v|m_{o_v}$. Agora, considere $i = i(a)$ e $H = H_{v,i,o_v c_v t}$. Como $t|n'_v$ e $n'_v|n_v$ e $mdc(v, n_v/t)|s$ então $v|s + i\frac{n_v}{t}$. Assim, $v|m_{o_v}$, $o_v c_v t|n$ e $v|s + \frac{n}{o_v c_v t}$, isto é, $(v,i,c_v t) \in \beta_{o_v}$. Pelo Lema 2.15, temos $mdc(v,i,c_v t) = 1$ e assim, G_{o_v}/H é cíclico pelo Lema 2.12. Do Lema 2.13, temos que G_{o_v} é o único elemento maximal do conjunto X lá definido, então concluímos que e_a é um idempotente central primitivo de $\mathbb{Q}G$.

O próximo teorema estabelece condições para que dois idempotentes da forma e_a sejam iguais. Além disso, ele determina a quantidade de elementos nestas condições. Antes, precisamos desenvolver alguns resultados.

Primeiro, note que $G_d^g = G_d$, para todo $g \in G$, pois como $G' \leq G_d$, temos $G_d \triangleleft G$.

Agora, se $g \in G$ e $H = H_{v,i,cd} = \langle a^v, a^i b^{cd} \rangle$, onde $(v,i,c) \in \beta_d$, temos:

$$g^{-1} a^v g = b^{-k} a^{-j} a^v a^j b^k = b^{-k} a^v b^k = a^{v r^k}$$

e

$$g^{-1} a^i b^{cd} g = b^{-k} a^{-j} a^i b^{cd} a^j b^k = b^{-k} a^{-j} a^i b^k b^{cd} a^{j r^k} = b^{-k} a^{-j} b^k a^{i r^k} b^{cd} a^{j r^k} = a^{-j r^k} a^{i r^k} b^{cd} a^{j r^k}$$
$$= a^{i r^k} b^{cd} a^{-j r^k (r^{cd} - 1)} = a^{i r^k} b^{cd} (a^v)^t, \quad \text{para algum} \quad t \in \mathbb{Z}, \quad \text{pois} \quad r^{cd} \equiv 1 \bmod v.$$

Assim,

$$H^g = \langle a^{v r^k}, a^{i r^k} b^{cd} (a^v)^t \rangle = \langle a^v, a^{i r^k} b^{cd} (a^v)^t \rangle.$$

Esta igualdade se deve ao fato de que $|\langle a^v\rangle^g| = |\langle a^v\rangle|$ e como $\langle a^v\rangle^g = \langle a^{vr^k}\rangle \leq \langle a^v\rangle$, então $\langle a^{vr^k}\rangle = \langle a^v\rangle$. Finalmente, obtemos de forma óbvia que:

$$H^g = \langle a^v, a^{ir^k}b^{cd}(a^v)^t\rangle = \langle a^v, a^{ir^k}b^{cd}\rangle.$$

Ainda, para demonstrar o teorema seguinte, para $k \in \mathbb{Z}$, definimos:

$$\alpha_{k,v} = \frac{i_v(r^k - 1)}{v'_v}.$$

Teorema 2.16 *Se $a_1 = (v_1, j_1, t_1)$ e $a_2 = (v_2, j_2, t_2)$ estão em $\mathcal{A} = \mathcal{A}_{m,r,n,s}$ então:*

$$e_{a_1} = e_{a_2} \quad \Leftrightarrow \quad v_1 = v_2 \ , \ t_1 = t_2 \ \text{ e } \ j_2 \equiv j_1 r^k + \alpha_{k,v}t_1 \ \text{ mod } D_{v_1} \ \text{ para algum } \ k \in \mathbb{Z}.$$

Além disso, se $a = (v, j, t)$ e $i = i(a)$ então existem exatamente $o_{v,i}$ elementos $a' \in \mathcal{A}$ tais que $e_a = e_{a'}$ que são os elementos da forma $a' = (v, j_k, t)$ com $0 \leq k \leq o_{v,i}$, onde j_k é o resto módulo D_v de $jr^k + \alpha_{k,v}t$.

Demonstração.

Se $a_1 = (v_1, j_1, t_1)$, $a_2 = (v_2, j_2, t_2)$, com $v_l | m_{o_{v_l}}$ e $t_l | n'_{v_l}$ $(l = 1, 2)$ então faça $i_l = i(a_l)$, $d_l = o_{v_l}$ e $c_l = c_{v_l}t_l$. Pela Proposição 2.6 temos que $e_{a_1} = e_{a_2}$ se, e somente se, existe $g \in G$ tal que:

$$G_{d_2} \cap H^g_{v_1,i_1,d_1c_1} = G^g_{d_1} \cap H_{v_2,i_2,c_2d_2} = G_{d_1} \cap H_{v_2,i_2,c_2d_2}.$$

Temos que $\langle a^{m_{d_1}}\rangle \leq \langle a^{v_1}, a^{i_1r^k}b^{c_1d_1}\rangle = H^g_{v_1,i_1,c_1d_1} \leq \langle a, b^{d_1}\rangle$ logo:

$$\langle a^{v_1}\rangle = G_{d_2} \cap H^g_{v_1,i_1,d_1c_1} \cap \langle a\rangle = G_{d_1} \cap H_{v_2,i_2,d_2c_2} \cap \langle a\rangle = \langle a^{v_2}\rangle.$$

Como $v_1, v_2 | m$, segue que $v_1 = v_2$ e daí, $d_1 = d_2$. Mas, sendo assim, $H^g_{v_1,i_1,d_1c_1} = H^g_{v_2,i_1,d_2c_1} \leq \langle G_{d_2}\rangle$ e $H_{v_2,i_2,d_2c_2} = H_{v_1,i_2,d_1c_2} \leq \langle G_{d_1}\rangle$ e portanto $H_{v_1,i_2,d_1c_2} = H_{v_1,i_1r^k,d_1c_1}$. Pelo Lema 2.9, temos que $c_1 = c_2$, $t_1 = t_2$ e $i_1r^k \equiv i_2 \bmod v_1$. Faça $v = v_1$ e $t = t_1$. Então:

$$v | i_1r^k - i_2 = i_vt(r^k - 1) + v'_v(j_1r^k - j_2) = v'_v(\alpha_{k,v}t + j_1r^k - j_2).$$

Segue que $j_2 \equiv j_1r^k + \alpha_{k,v}t \bmod D_v$. A recíproca segue de forma fácil.

Vimos então que os elementos de $\mathcal{A}$ que geram o mesmo idempotente que (v, j, t) são os elementos da forma $(v, j_1, t) \in A$ com $j_1 \equiv jr^k + \alpha_{k,v}t \bmod D_v$ para algum $k \in \mathbb{Z}$. Se $i = i_vt + v'_vj$ e $i_1 = i_vt + v'_vj_1$ então $j_1 \equiv jr^k + \alpha_{k,v}t \bmod D_v$ se, e somente se $i_1 \equiv ir^k \bmod v$. Assim, existem tantos inteiros $0 \leq j_1 < D_v$ satisfazendo $j_1 \equiv jr^k + \alpha_{k,v}t \bmod D_v$ quanto classes módulo v de elementos da forma ir^k.

Mas se k é solução de $i_1 \equiv ir^x \bmod v$ então k' é outra solução se, e somente se, $r^k \equiv r^{k'} \bmod \frac{v}{mdc(v,i)}$. Assim estas soluções distintas são realizadas com os expoentes $0 \leq k \leq o_{v,i}$ e assim, os $o_{v,i}$ elementos de $\mathcal{A}$ distintos que geram $e_{v,j,t}$ são os elementos da forma (v, j_1, t) com j_1 percorrendo os restos módulo D_v dos elementos da forma $jr^k + \alpha_{k,v}t$, com $0 \leq k \leq o_{v,i}$.

□

Teorema 2.17 *Os idempotentes centrais primitivos de $\mathbb{Q}G$ são os elementos da forma e_a com $a \in \mathcal{A} = \mathcal{A}_{m,r,n,s}$.*

Demonstração.

Já foi visto que e_a é um idempotente central primitivo de $\mathbb{Q}G$. Reciprocamente, seja e um idempotente central primitivo de $\mathbb{Q}G$. Dos lemas anteriores, temos que $e = e(G, G_{o_v}, H)$, com $H = H_{v,i,o_v c}$, onde $(v, i, c) \in \beta_{o_v}$ e $mdc(v, i, c) = 1$. Assim, $v|s + i\frac{n}{o_v c}$, logo $mdc(v, \frac{n}{o_v c})|s$ e portanto $c = c_v t$ para algum $t|n_v$. Pelo Lema 2.14, $t|n'_v$ e pelo Lema 2.15, $i = i_v t + v'_v j$ para algum $j \in \mathbb{Z}$ e $mdc(v, j, t) = 1$. Assim, $e = e(G, G_{o_v}, H) = e_{v,j,t}$ e, do Lema 2.16, fazendo $k = 0$, se $j \equiv j_1 \bmod D_v$, então $e_{v,j,t} = e_{v,j_1,t}$

Temos que mostrar agora que $mdc(v, j_1, t) = 1$. Vamos fazer isto por partes. Obviamente, se $mdc(v, j, t) = 1$ então $mdc(D_v, j, t) = 1$. Agora suponha por absurdo que exista um primo p tal que $p|mdc(D_v, j_1, t)$, então, como $p|D_v$, $p|j_1$ e $j = fD_v + j_1$ para algum $f \in \mathbb{Z}$, temos que $p|j$ o que é um absurdo pois $mdc(D_v, j, t) = 1$, logo $mdc(D_v, j_1, t) = 1$.

Suponha de novo por absurdo que exista um primo p tal que $p|mdc(v, j_1, t)$. Da conclusão do parágrafo anterior, concluimos que p não divide D_v, logo $p|\frac{v}{D_v} = v'_v$. Mas $i = i_v t + v'_v j$ logo $p|i$. Como $c = c_v t$ e $p|t$, temos também que $p|c$, logo $p|mdc(v, i, c)$ o que é um absurdo, portanto $mdc(v, j_1, t) = 1$

Concluímos então que podemos trocar j pelo seu resto módulo D_v e assim, podemos assumir que $(v, j, t) \in \mathcal{A}$.

□

2.3 Componentes Simples de $\mathbb{Q}G$

Nesta seção vamos explicitar a componente simples $\mathbb{Q}Ge_a$, para $a \in \mathcal{A}$.

Lema 2.18 *Sejam $(v,i,c) \in \beta_{o_v}$, $mdc(v,i,c) = 1$ e v_1, c_1, i_1 e i' inteiros satisfazendo*

$$v_1 v + c_1 c = 1 + i_1 i \quad e \quad i' i_1 + c' c = 1.$$

Então:

$$\mathbb{Q}Ge(G, G_{o_v}, H_{v,i,o_v c}) \cong M_{o_{v,i}}(\mathbf{A})$$

onde $\mathbf{A}$ *é a álgebra dada pela apresentação:*

$$\mathbb{Q}(\xi_{vc})(g : g^{\frac{o_v}{o_{v,i}}} = \xi_{vc}^{i' v_1 v - i}, g^{-1}\xi_{vc} g = \xi_{vc}^{1 + c_1 c (r^{o_{v,i}} - 1)}).$$

Demonstração.

Como já vimos no Lema 2.12 e no Lema 2.10, considerando $H = H_{v,i,o_v c}$, o gerador de $\frac{G_{o_v}}{H}$ será $a^{c_1} b^{o_v i_1} H$ e $N = N_G(H) = G_{o_{v,i}}$. Assim, $[G_{o_v} : H] = vc$. Como todos os elementos de $G_{o_{v,i}}$ são da forma $(b^{o_{v,i}})^r a^j$, temos que $\frac{G_{o_{v,i}}}{G_{o_v}} = \frac{\langle a, b^{o_{v,i}} \rangle}{\langle a, b^{o_v} \rangle}$ é cíclico gerado por $\langle b^{o_{v,i}} G_{o_v} \rangle$. Logo, $[N : G_{o_v}] = \frac{o_v}{o_{v,i}}$.

Segindo argumento similar, temos que $[G : G_{o_{v,i}}] = o_{v,i}$. Um inverso de $b^{o_{v,i}} G_{o_v}$ segundo a projeção canônica $\Pi : \frac{G_{o_{v,i}}}{H} \to \frac{G_{o_{v,i}}}{G_{o_v}}$ é $b^{o_{v,i}} H$. Além disso, temos:

$$(b^{o_{v,i}})^{\frac{o_v}{o_{v,i}}} H = b^{o_v} H$$

e

$$(bH)^{-o_{v,i}} x (bH)^{o_{v,i}} = (b)^{-o_{v,i}} (a^{c_1} b^{o_v i_1})(b)^{o_{v,i}} H = a^{c_1 r^{o_{v,i}}} b^{o_v i_1} H = x^{cc_1 r^{o_{v,i}} + i_1 (i' v_1 v - i)}.$$

A última igualdade se deve ao fato de que $x^c = aH$ e $x^{i' v_1 v - i} = b^d H$, como mostra o Lema 2.12 onde o_v aqui faz o papel de d. Ainda usando as relações do Lema 2.12 temos:

$$\begin{aligned} & x^{cc_1 r^{o_{v,i}} + i_1 (i' v_1 v - i)} = x^{cc_1 r^{o_{v,i}} + i_1 i' v_1 v - i_1 i} = x^{cc_1 r^{o_{v,i}} + i_1 i' v_1 v + 1 - v_1 v - c_1 c} \\ & = x^{1 + cc_1 (r^{o_{v,i}} - 1) + v_1 v (i_1 i' - 1)} = x^{1 + cc_1 (r^{o_{v,i}} - 1) - v_1 v c c'} = x^{1 + cc_1 (r^{o_{v,i}} - 1)}. \end{aligned}$$

A última igualdade decorre do fato de que a ordem de x é vc. Assim, de acordo com o Teorema 2.5, temos:

$$\mathbb{Q}Ge(G, G_{o_v}, H_{v,i,o_v c}) \cong M_{o_{v,i}}(\mathbf{A})$$

onde $\mathbf{A}$ é a álgebra dada pela apresentação:

$$\mathbb{Q}(\xi_{vc})(g : g^{\frac{o_v}{o_{v,i}}} = \xi_{vc}^{i' v_1 v - i}, g^{-1}\xi_{vc} g = \xi_{vc}^{1 + c_1 c (r^{o_{v,i}} - 1)}).$$

□

Finalmente, o próximo teorema chega a um resultado conclusivo sobre as álgebras simples $\mathbb{Q}Ge_a$.

Teorema 2.19 *Se $a = (v, j, t) \in \mathcal{A}$ e $i = i(a)$, então existem inteiros v_1, c_1, i_1 e i' satisfazendo as condições:*

$$v_1 v + c_1 c_v t = 1 + i_1 i \quad e \quad i' i_1 \equiv 1 \ mod\ c_v t.$$

Além disso,

$$\mathbb{Q}Ge(G, G_{o_v}, H_{v,i,o_v c_v t}) \cong M_{o_{v,i}}(\mathbf{A})$$

onde $\mathbf{A}$ é a álgebra dada pela apresentação:

$$\mathbb{Q}(\xi_{vc_vt})(g : g^{\frac{o_v}{o_{v,i}}} = \xi_{vc_vt}^{i'v_1 v - i}, g^{-1}\xi_{vc_vt}g = \xi_{vc_vt}^{1+c_1 c_v t(r^{o_{v,i}}-1)}).$$

Demonstração.

Se $a = (v, j, t) \in \mathcal{A}$ e $i = i(a)$, então $(v, i, c_v t) \in \beta_{o_v}$ e $mdc(v, i, t) = 1$, pelo Lema 2.15. Basta então aplicar os Lemas 2.12 e 2.18.

□

Capítulo 3

Exemplos com o Uso do GAP

Este capítulo tem dois objetivos principais. O primeiro deles é mostrar como se pode utilizar o pacote "Wedderga"do GAP, mais precisamente o algoritmo implementado por Olivieri et all em [8], que determina a decomposição de Wedderburn de álgebras de grupos racionais de grupos abelianos-por-supersolúvel, como ferramenta para estudar o problema do isomorfismo para grupos metacíclicos finitos. O segundo objetivo é usar os resultados obtidos na seção anterior para implementar um algoritmo para o cálculo da decomposição de $\mathbb{Q}G$ especificamente quando G é metacíclico tendo por entrada apenas os parâmetros contidos na apresentação do grupo.

3.1 Exemplos de Decomposição de Wedderburn

Tanto no pacote como no algoritmo criado neste trabalho, a saída terá a forma:

$$[n, k, [\ [o_i, \alpha_i, \beta_i] : i = 1, \ldots, m], [\gamma_{ij} : 1 \leq i < l \leq m]\ ]$$

onde os parâmetros citados são os parâmetros do Teorema 2.5. Como no caso metacíclico vimos que o grupo N/K tem apenas um gerador, a saída assumirá a forma simplificada:

$$[n, k,\ [o, \alpha, \beta], [\,]\ ]$$

que representa a álgebra dada pela apresentação:

$$M_n(\mathbf{A})\,,\ \ \mathbf{A} \cong \mathbb{Q}(\xi_k)(g : g^o = \xi_k^{\beta}, \xi_k g = g\xi_k^{\alpha}).$$

Antes de começar com exemplos concretos, é importante ter algumas noções em mente para facilitar a interpretação das saídas.

1. Sempre que as saídas forem da forma $[n, k, [\,], [\,]]$ a álgebra correspondente será $M_n(\mathbb{Q}(\xi_k))$. Quando $\xi_k \in \mathbb{Q}$ teremos apenas $M_n(\mathbb{Q})$.

   Exemplo: $[1, 1, [\,], [\,]]$ e $[1, 2, [\,], [\,]]$ representam ambas o corpo dos racionais $\mathbb{Q}$.

2. Se as saídas forem da forma $[n, k, [2, k-1, k/2], [\,]]$ nossa álgebra poderá ser interpretada como $M_n(\mathbf{A})$ onde

$$\mathbf{A} = \mathbb{Q}(\xi_k)(g : g^2 = -1, \xi_k g = g\xi_k^{-1}).$$

   Se $\xi_k = \alpha + \beta i$ então claramente $\mathbb{Q}(\alpha + \beta i) \subset \mathbb{Q}(\alpha\,,\,\beta i)$. Como $\frac{\xi_k + \xi_k^{-1}}{2} = \alpha$ e $\frac{\xi_k - \xi_k^{-1}}{2} = \beta i$, temos $\mathbb{Q}(\alpha + \beta i) = \mathbb{Q}(\alpha\,,\,\beta i)$ assim

$$\mathbf{A} = \mathbb{Q}(\alpha\,,\,\beta i)(g : g^2 = -1,\ (\alpha + \beta i)g = g(\alpha - \beta i))$$

   e o centro da álgebra $\mathbf{A}$ é $\mathbb{Q}(\alpha)$. Portanto, escrevendo de outra forma:

$$\mathbf{A} = \mathbb{Q}(\alpha)(g,\ \beta i : g^2 = -1,\ (\beta i)^2 = -\beta^2 = \alpha^2 - 1,\ (\beta i)g = -g(\beta i)).$$

   Como $-\beta^2 \in \mathbb{Q}(\alpha)$ podemos fazer a seguinte identificação com base $\{1,\, i,\, j,\, k\}$ de uma álgebra dos quatérnios

$$1 \mapsto 1\ ,\ \beta i \mapsto i\ ,\ g \mapsto j \text{ e } (\beta i)g \mapsto k.$$

   assim temos $\mathbf{A} = \mathbb{H}(-1, -\beta^2)(\mathbb{Q}(\alpha))$. Como $\alpha = (\xi_k + \xi_k^{-1})/2$ temos

$$\mathbf{A} = \mathbb{H}(-1, -\beta^2)(\mathbb{Q}(\xi_k + \xi_k^{-1})).$$

   Se $\beta \in \mathbb{Q}(\xi_k + \xi_k^{-1})$, então podemos verificar que

$$\mathbb{H}(-1, -\beta^2)(\mathbb{Q}(\xi_k + \xi_k^{-1})) \cong \mathbb{H}(-1, -1)(\mathbb{Q}(\xi_k + \xi_k^{-1})) = \mathbb{H}(\mathbb{Q}(\xi_k + \xi_k^{-1}))).$$

3. Se as saídas forem da forma $[n, k, [2, k-1, 0], [\,]]$ nossa álgebra poderá ser interpretada como $M_n(\mathbf{A})$ onde

$$\mathbf{A} = \mathbb{H}(1, -\beta^2)(\mathbb{Q}(\xi_k + \xi_k^{-1})).$$

   Todos os elementos de $\mathbf{A}$ são da forma: $a_1 1 + a_2 i + a_3 j + a_4 k$, $a_i \in \mathbb{Q}(\xi_k + \xi_k^{-1})$. Assim, conferindo as relações, é fácil ver que podemos fazer a seguinte identificação:

$$1 \mapsto \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ i \mapsto \begin{bmatrix} 0 & -\beta^2 \\ 1 & 0 \end{bmatrix},\ j \mapsto \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},\ k \mapsto \begin{bmatrix} 0 & \beta^2 \\ 1 & 0 \end{bmatrix}.$$

Assim obtemos

$$a_1 1 + a_2 i + a_3 j + a_4 k \mapsto \begin{bmatrix} a_1 + a_3 & -a_2\beta^2 + a_4\beta^2 \\ a_2 + a_4 & a_1 - a_3 \end{bmatrix}.$$

Segue que:

$$\mathbf{A} = M_2(\mathbb{Q}(\xi_k + \xi_k^{-1})).$$

Portanto a álgebra assume a forma:

$$M_{2n}(\mathbb{Q}(\xi_k + \xi_k^{-1})).$$

Com a intenção de apresentar exemplos concretos relacionado ao que foi explicado, vejamos a interpretação das saídas:

$$[1, 6, [[2, 5, 3]], [\,]] \text{ e } [1, 6, [[2, 5, 0]], [\,]].$$

No primeiro caso, temos $\xi_6 = \frac{1}{2} + \frac{\sqrt{3}}{2}i$. Assim é fácil ver que:

$$\mathbf{A} = \mathbb{Q}(g,\ \sqrt{-3} : g^2 = -1,\ (\sqrt{-3})^2 = -3,\ \sqrt{-3}g = -g\sqrt{-3}),$$

isto é,

$$\mathbf{A} = \mathbb{H}(-1, -3)(\mathbb{Q}).$$

No segundo caso temos

$$\mathbf{A} = \mathbb{H}(1, -3)(\mathbb{Q}) = M_2(\mathbb{Q}),$$

como já foi discutido.

O método utilizado neste trabalho para atacar o problema do isomorfismo consistiu em implementar um algoritmo usando rotinas contidas no GAP para, dado um valor para $|G|$, gerar uma lista com todos os grupos metacíclicos desta ordem que não fossem isomorfos e não fossem abelianos, usar o pacote "Wedderga"para calcular as decomposições de Wedderburn para as álgebras de grupos racionais sobre cada um deles e comparar os dados. Isto foi feito tendo em vista o Lema 1.3 que diz que os grupos metacíclicos da forma $C_m : C_n$ são os grupos com a apresentação:

$$G = \langle a, b : a^m = 1, b^n = a^s, b^{-1}ab = a^r \rangle$$

satisfazendo as condições:

$$m | r^n - 1, \quad m | s(r-1), \text{ para } \ m, n, r, s \in \mathbb{N}, r, s \leq m.$$

A rotina usada para esta tarefa, denominada $DecomposicaoOrdem(u)$, está na próxima seção e a explicação de como ela funciona será apresentada resumidamente abaixo, passo a passo.

1. Fazer uma lista com grupo trivial $\{1\}$ e denominar esta lista de lista B.

2. Dado $u = |G|$, criar uma lista D com todos os divisores de u.

3. Fazer o parâmetro m ser igual a cada um dos elementos de D.

4. Para cada valor de m assim fixado, fazer $n = u/m$, de forma que $nm = u = |G|$.

5. Para cada valor de m e n assim escolhidos, fazer os parâmetros r e s percorrerem os valores de 1 até m.

6. Para cada quádrupla m, n, s e r, testar se satisfaz as condições $m|r^n - 1$ e $m|s(r-1)$.

7. Se satisfaz as condições, testar se o grupo correspondente é abeliano.

8. Se o grupo não for abeliano e satisfaz 6, testar se existe algum grupo isomorfo na lista B.

9. Se isto não ocorrer, denominar o novo grupo gerado por T, adicionar este à lista B, construir a álgebra de grupo $\mathbb{Q}T$, calcular a decomposição de Wedderburn de $\mathbb{Q}T$e guardar esta na lista C.

10. Repetir todo o processo desde 3, até que m percorra todos os valores da lista D, de divisores de $|G|$.

11. A saída final será a lista C.

Como exemplo concreto do uso desta rotina, a usamos nos casos em que $|G| = 18$, $|G| = 20$, $|G| = 24$, $|G| = 36$, $|G| = 42$, $|G| = 44$, $|G| = 50$ e $|G| = 52$, obtendo os resultados abaixo, sendo que para cada k, denotaremos $\xi_k = \alpha_k + \beta_k i$.

$|G| = 18$

m, n, s, r	Decomposição
3, 6, 3, 2	[[1, 1, [ ], [ ]], [1, 2, [ ], [ ]], [1, 3, [ ], [ ]], [2, 3, [ ], [ ]], [1, 3, [[2, 2, 0]], [ ]], [1, 6, [ ], [ ]]]
	$2\mathbb{Q} \oplus \mathbb{Q}(\xi_3) \oplus M_2(\mathbb{Q}(\xi_3)) \oplus M_2(\mathbb{Q}) \oplus \mathbb{Q}(\xi_6)$
9, 2, 9, 8	[[1, 1, [ ], [ ]], [1, 2, [ ], [ ]], [1, 3, [[2, 2, 0]], [ ]], [1, 9, [[2, 8, 0]], [ ]]]
	$2\mathbb{Q} \oplus M_2(\mathbb{Q}) \oplus M_2(\mathbb{Q}(\xi_9 + \xi_9^{-1}))$

$|G| = 20$

m, n, s, r	Decomposição
5, 4, 5, 2	[[1, 1, [ ], [ ]], [1, 2, [ ], [ ]], [1, 4, [ ], [ ]], [1, 5, [[4, 2, 0]], [ ]]]
	$2\mathbb{Q} \oplus \mathbb{Q}(\xi_4) \oplus \mathbf{A}, \quad \mathbf{A} \cong \mathbb{Q}(\xi_5)(g : g^4 = 1\,,\, \xi_5 g = g\xi_5^2)$
5, 4, 5, 4	[[1, 1, [ ], [ ]], [1, 2, [ ], [ ]], [1, 4, [ ], [ ]], [1, 5, [[2, 4, 0]], [ ]], [1, 10, [[2, 9, 5]], [ ]]]
	$2\mathbb{Q} \oplus \mathbb{Q}(i) \oplus M_2(\mathbb{Q}(\xi_5 + \xi_5^{-1})) \oplus \mathbb{H}(-1, -\beta_{10}^2)(\mathbb{Q}(\xi_{10} + \xi_{10}^{-1}))$
10, 2, 10, 9	[[1, 1, [ ], [ ]], [1, 2, [ ], [ ]], [1, 2, [ ], [ ]], [1, 2, [ ], [ ]], [1, 5, [[2, 4, 0]], [ ]], [1, 10, [[2, 9, 0]], [ ]]]
	$4\mathbb{Q} \oplus M_2(\mathbb{Q}(\xi_5 + \xi_5^{-1})) \oplus M_2(\mathbb{Q}(\xi_{10} + \xi_{10}^{-1}))$

$|G| = 24$

m, n, s, r	Decomposição
3, 8, 3, 2	[[1, 1, [ ], [ ]], [1, 2, [ ], [ ]], [1, 4, [ ], [ ]], [1, 3, [[2, 2, 0]], [ ]], [1, 8, [ ], [ ]], [1, 6, [[2, 5, 3]], [ ]], [1, 12, [[2, 5, 3]], [ ]]]
	$2\mathbb{Q} \oplus \mathbb{Q}(i) \oplus M_2(\mathbb{Q}) \oplus \mathbb{Q}(\sqrt{2}, i) \oplus \mathbb{H}(-1,-3)(\mathbb{Q}) \oplus \mathbb{H}(3,i)(\mathbb{Q}(i))$
4, 6, 2, 3	[[1, 1, [ ], [ ]], [1, 2, [ ], [ ]], [1, 2, [ ], [ ]], [1, 2, [ ], [ ]], [1, 3, [ ], [ ]], [1, 6, [ ], [ ]], [1, 6, [ ], [ ]], [1, 6, [ ], [ ]], [1, 4, [[2, 3, 2]], [ ]], [1, 12, [[2, 7, 10]], [ ]]]
	$4\mathbb{Q} \oplus \mathbb{Q}(\xi_3) \oplus 3\mathbb{Q}(\xi_6) \oplus \mathbb{H}(\mathbb{Q}) \oplus \mathbf{A}, \quad \mathbf{A} \cong \mathbb{Q}(\xi_{12})(g : g^2 = \xi_{12}^{10}, \xi_{12} g = g\xi_{12}^7)$
4, 6, 4, 3	[[1, 1, [ ], [ ]], [1, 2, [ ], [ ]], [1, 2, [ ], [ ]], [1, 2, [ ], [ ]], [1, 3, [ ], [ ]], [2, 2, [ ], [ ]], [1, 6, [ ], [ ]], [1, 6, [ ], [ ]], [1, 6, [ ], [ ]], [2, 6, [ ], [ ]]]
	$4\mathbb{Q} \oplus \mathbb{Q}(\xi_3) \oplus M_2(\mathbb{Q}) \oplus 3\mathbb{Q}(\xi_6) \oplus M_2(\mathbb{Q}(\xi_6))$
6, 4, 6, 5	[[1, 1, [ ], [ ]], [1, 2, [ ], [ ]], [1, 2, [ ], [ ]], [1, 2, [ ], [ ]], [1, 4, [ ], [ ]], [1, 4, [ ], [ ]], [1, 3, [[2, 2, 0]], [ ]], [1, 6, [[2, 5, 3]], [ ]], [1, 6, [[2, 5, 3]], [ ]], [1, 6, [[2, 5, 0]], [ ]]]
	$4\mathbb{Q} \oplus 2\mathbb{Q}(i) \oplus 2M_2(\mathbb{Q}) \oplus 2\mathbb{H}(-1,-3)(\mathbb{Q})$
12, 2, 6, 5	[[1, 1, [ ], [ ]], [1, 2, [ ], [ ]], [1, 2, [ ], [ ]], [1, 2, [ ], [ ]], [1, 4, [ ], [ ]], [1, 4, [ ], [ ]], [1, 3, [[2, 2, 0]], [ ]], [1, 6, [[2, 5, 0]], [ ]], [1, 12, [[2, 5, 6]], [ ]]]
	$4\mathbb{Q} \oplus 2\mathbb{Q}(i) \oplus 2M_2(\mathbb{Q}) \oplus \mathbf{B}, \quad \mathbf{B} \cong \mathbb{Q}(\xi_{12})(g : g^2 = -1, \xi_{12} g = g\xi_{12}^5)$
12, 2, 6, 11	[[1, 1, [ ], [ ]], [1, 2, [ ], [ ]], [1, 2, [ ], [ ]], [1, 2, [ ], [ ]], [1, 3, [[2, 2, 0]], [ ]], [1, 4, [[2, 3, 2]], [ ]], [1, 6, [[2, 5, 0]], [ ]], [1, 12, [[2, 11, 6]], [ ]]]
	$4\mathbb{Q} \oplus 2M_2(\mathbb{Q}) \oplus \mathbb{H}(\mathbb{Q}) \oplus \mathbb{H}(\mathbb{Q}(\sqrt{3}))$
12, 2, 12, 11	[[1, 1, [ ], [ ]], [1, 2, [ ], [ ]], [1, 2, [ ], [ ]], [1, 2, [ ], [ ]], [1, 2, [ ], [ ]], [2, 2, [ ], [ ]], [1, 3, [[2, 2, 0]], [ ]], [1, 6, [[2, 5, 0]], [ ]], [1, 12, [[2, 11, 0]], [ ]]]
	$4\mathbb{Q} \oplus 3M_2(\mathbb{Q}) \oplus M_2(\mathbb{Q}(\sqrt{3}))$

$|G| = 36$

m, n, s, r	Decomposição
3, 12, 3, 2	[[1, 1, [ ], [ ]], [1, 2, [ ], [ ]], [1, 3, [ ], [ ]], [1, 4, [ ], [ ]], [1, 6, [ ], [ ]], [2, 3, [ ], [ ]], [1, 3, [[2, 2, 0]], [ ]], [1, 6, [[2, 5, 3]], [ ]], [2, 6, [ ], [ ]], [1, 12, [ ], [ ]]]
	$2\mathbb{Q} \oplus \mathbb{Q}(\xi_3) \oplus \mathbb{Q}(i) \oplus \mathbb{Q}(\xi_6) \oplus M_2(\mathbb{Q}(\xi_3)) \oplus M_2(\mathbb{Q}) \oplus \mathbb{H}(-1,-3)(\mathbb{Q}) \oplus M_2(\mathbb{Q}(\xi_6)) \oplus \mathbb{Q}(\xi_{12})$
6, 6, 6, 5	[[1, 1, [ ], [ ]], [1, 2, [ ], [ ]], [1, 2, [ ], [ ]], [1, 2, [ ], [ ]], [1, 2, [ ], [ ]], [1, 3, [ ], [ ]], [1, 3, [[2, 2, 0]], [ ]], [1, 6, [ ], [ ]], [1, 6, [ ], [ ]], [2, 3, [ ], [ ]], [1, 6, [ ], [ ]], [2, 6, [ ], [ ]], [1, 6, [[2, 5, 0]], [ ]]]
	$4\mathbb{Q} \oplus \mathbb{Q}(\xi_3) \oplus 2M_2(\mathbb{Q}) \oplus 3\mathbb{Q}(\xi_6) \oplus M_2(\mathbb{Q}(\xi_6)) \oplus M_2(\mathbb{Q}(\xi_3))$
9, 4, 9, 8	[[1, 1, [ ], [ ]], [1, 2, [ ], [ ]], [1, 4, [ ], [ ]], [1, 3, [[2, 2, 0]], [ ]], [1, 6, [[2, 5, 3]], [ ]], [1, 9, [[2, 8, 0]], [ ]], [1, 18, [[2, 17, 9]], [ ]]]
	$2\mathbb{Q} \oplus \mathbb{Q}(i) \oplus M_2(\mathbb{Q}) \oplus \mathbb{H}(-1,-3)(\mathbb{Q}) \oplus M_2(\mathbb{Q}(\xi_9 + \xi_9^{-1})) \oplus \mathbb{H}(-1,-\beta_{18}^2)(\mathbb{Q}(\xi_{18} + \xi_{18}^{-1}))$
18, 2, 18, 17	[[1, 1, [ ], [ ]], [1, 2, [ ], [ ]], [1, 2, [ ], [ ]], [1, 2, [ ], [ ]], [1, 2, [ ], [ ]], [1, 3, [[2, 2, 0]], [ ]], [1, 6, [[2, 5, 0]], [ ]], [1, 9, [[2, 8, 0]], [ ]], [1, 18, [[2, 17, 0]], [ ]]]
	$4\mathbb{Q} \oplus 2M_2(\mathbb{Q}) \oplus M_2(\mathbb{Q}(\xi_9 + \xi_9^{-1})) \oplus M_2(\mathbb{Q}(\xi_{18} + \xi_{18}^{-1}))$

$|G| = 42$

m, n, s, r	Decomposição
3, 14, 3, 2	[[1, 1, [ ], [ ]], [1, 2, [ ], [ ]], [1, 3, [[2, 2, 0]], [ ]], [1, 7, [ ], [ ]], [1, 14, [ ], [ ]], [1, 21, [[2, 8, 6]], [ ]]]
	$2\mathbb{Q} \oplus M_2(\mathbb{Q}) \oplus \mathbb{Q}(\xi_7) \oplus \mathbb{Q}(\xi_{14}) \oplus \mathbf{A}, \quad \mathbf{A} \cong \mathbb{Q}(\xi_{21})(g : g^2 = \xi_{21}^6, \xi_{21} g = g\xi_{21}^8)$
7, 6, 7, 2	[[1, 1, [ ], [ ]], [1, 2, [ ], [ ]], [1, 3, [ ], [ ]], [1, 6, [ ], [ ]], [1, 7, [[3, 4, 0]], [ ]], [1, 14, [[3, 11, 0]], [ ]]]
	$2\mathbb{Q} \oplus \mathbb{Q}(\xi_3) \oplus \mathbb{Q}(\xi_6) \oplus \mathbf{B} \oplus \mathbf{C}, \quad \mathbf{B} \cong \mathbb{Q}(\xi_7)(g : g^3 = 1, \xi_7 g = g\xi_7^4), \quad \mathbf{C} \cong \mathbb{Q}(\xi_{14})(g : g^3 = 1, \xi_{14} g = g\xi_{14}^{11})$
7, 6, 7, 3	[[1, 1, [ ], [ ]], [1, 2, [ ], [ ]], [1, 3, [ ], [ ]], [1, 6, [ ], [ ]], [1, 7, [[6, 5, 0]], [ ]]]
	$2\mathbb{Q} \oplus \mathbb{Q}(\xi_3) \oplus \mathbb{Q}(\xi_6) \oplus \mathbf{D}, \quad \mathbf{D} \cong \mathbb{Q}(\xi_7)(g : g^6 = 1, \xi_7 g = g\xi_7^5)$
7, 6, 7, 6	[[1, 1, [ ], [ ]], [1, 2, [ ], [ ]], [1, 3, [ ], [ ]], [1, 6, [ ], [ ]], [1, 7, [[2, 6, 0]], [ ]], [1, 21, [[2, 13, 14]], [ ]]]
	$2\mathbb{Q} \oplus \mathbb{Q}(\xi_3) \oplus \mathbb{Q}(\xi_6) \oplus M_2(\mathbb{Q}(\xi_7 + \xi_7^{-1})) \oplus \mathbf{E}, \quad \mathbf{E} \cong \mathbb{Q}(\xi_{21})(g : g^2 = \xi_{21}^{14}, \xi_{21} g = g\xi_{21}^{13})$
21, 2, 21, 20	[[1, 1, [ ], [ ]], [1, 2, [ ], [ ]], [1, 3, [[2, 2, 0]], [ ]], [1, 7, [[2, 6, 0]], [ ]], [1, 21, [[2, 20, 0]], [ ]]]
	$2\mathbb{Q} \oplus M_2(\mathbb{Q}) \oplus M_2(\mathbb{Q}(\xi_7 + \xi_7^{-1})) \oplus M_2(\mathbb{Q}(\xi_{21} + \xi_{21}^{-1}))$

$|G| = 44$

m, n, s, r	Decomposição
11, 4, 11, 10	[[1, 1, [ ], [ ]], [1, 2, [ ], [ ]], [1, 4, [ ], [ ]], [1, 11, [[2, 10, 0]], [ ]], [1, 22, [[2, 21, 11]], [ ]]]]
	$2\mathbb{Q} \oplus \mathbb{Q}(\xi_4) \oplus M_2(\mathbb{Q}(\xi_{11} + \xi_{11}^{-1})) \oplus \mathbb{H}(-1, -\beta_{22}^2)(\mathbb{Q}(\xi_{22} + \xi_{22}^{-1}))$
22, 2, 22, 21	[1, 1, [ ], [ ]], [1, 2, [ ], [ ]], [1, 2, [ ], [ ]], [1, 2, [ ], [ ]], [1, 2, [ ], [ ]], [1, 11, [[2, 10, 0]], [ ]], [1, 22, [[2, 21, 0]], [ ]]]
	$4\mathbb{Q} \oplus M_2(\mathbb{Q}(\xi_{11} + \xi_{11}^{-1})) \oplus M_2(\mathbb{Q}(\xi_{22} + \xi_{22}^{-1}))$

$|G| = 50$

m, n, s, r	Decomposição
5, 10, 5, 4	[[1, 1, [ ], [ ]], [1, 2, [ ], [ ]], [1, 5, [ ], [ ]], [2, 5, [ ], [ ]], [2, 5, [ ], [ ]], [1, 5, [[2, 4, 0]], [ ]], [1, 10, [ ], [ ]]]
	$2\mathbb{Q} \oplus \mathbb{Q}(\xi_5) \oplus 2M_2(\mathbb{Q}(\xi_5)) \oplus M_2(\mathbb{Q}(\xi_5 + \xi_5^{-1})) \oplus \mathbb{Q}(\xi_{10})$
25, 2, 25, 24	[[1, 1, [ ], [ ]], [1, 2, [ ], [ ]], [1, 5, [[2, 4, 0]], [ ]], [1, 25, [[2, 24, 0]], [ ]]]
	$2\mathbb{Q} \oplus M_2(\mathbb{Q}(\xi_5 + \xi_5^{-1})) \oplus M_2(\mathbb{Q}(\xi_{25} + \xi_{25}^{-1}))$

$|G| = 52$

m, n, s, r	Decomposição
13, 4, 13, 5	[[1, 1, [ ], [ ]], [1, 2, [ ], [ ]], [1, 4, [ ], [ ]], [1, 13, [[4, 5, 0]], [ ]]]
	$2\mathbb{Q} \oplus \mathbb{Q}(\xi_4) \oplus \mathbf{A} \quad \mathbf{A} \cong \mathbb{Q}(\xi_{13})(g : g^4 = 1\,,\, \xi_{12}g = g\xi_{12}^5)$
13, 4, 13, 12	[[1, 1, [ ], [ ]], [1, 2, [ ], [ ]], [1, 4, [ ], [ ]], [1, 13, [[2, 12, 0]], [ ]], [1, 26, [[2, 25, 13]], [ ]]]
	$2\mathbb{Q} \oplus \mathbb{Q}(\xi_4) \oplus M_2(\mathbb{Q}(\xi_{13} + \xi_{13}^{-1})) \oplus \mathbb{H}(-1, -\beta_{26}^2)(\mathbb{Q}(\xi_{26} + \xi_{26}^{-1}))$
26, 2, 26, 25	[[1, 1, [ ], [ ]], [1, 2, [ ], [ ]], [1, 2, [ ], [ ]], [1, 2, [ ], [ ]], [1, 13, [[2, 12, 0]], [ ]], [1, 26, [[2, 25, 0]], [ ]]]
	$4\mathbb{Q} \oplus M_2(\mathbb{Q}(\xi_{13} + \xi_{13}^{-1})) \oplus M_2(\mathbb{Q}(\xi_{26} + \xi_{26}^{-1}))$

Mesmo não dando uma forma mais clara para as álgebras **A**, **B**, **C**, **D** e **E**, analisando os dados pode-se verificar que não existem grupos metacíclicos com as ordens 18, 20, 24 , 36, 44, 50 e 52 que não sejam isomorfos e cujas álgebras de grupos sobre $\mathbb{Q}$ sejam isomorfas. Já para a ordem 42, apesar das várias indeterminações, podemos verificar que isto também não ocorre, com o auxílio das dimensões das componentes

A segunda parte desta seção destina-se a exibir exemplos de uma rotina implementada que tem objetivo de colocar em prática os resultados da Seção 2.3 que apresentam um método para a determinação da decomposição de Wedderburn de $\mathbb{Q}G$ especificamente para grupos metacíclicos. Esta rotina, denominada $DWmetaciclico(m, n, s, r)$, se encontra na Seção 3.2 e é baseada na definição:

$$\mathcal{A} = \mathcal{A}_{m,r,n,s} = \{(v, j, t) \in \mathbb{Z}^3 : \ 0 < v|m \ , \ 0 < t|n'_v \ , \ 0 \leq j \leq D_v \ \text{ e } \ mdc(v, j, t) = 1\}.$$

Se $a = (v, j, t) \in \mathcal{A}$ então defina:

$$i(a) = i_v t + v'_v j \quad , \ e_a = e_{v,j,t} = e(G, G_{o_v}, H_{v,i(a),o_v c_v t}) \ \text{ e } \ S_a = S_{v,j,t} = \mathbb{Q}Ge_a.$$

Além disso, a rotina é baseada no Teorema 2.19 e no cálculo de todos os parâmetros associados. Para que ela funcione basta entrar com os parâmetros m, n, s e r da apresentação do grupo metacíclico G. Resumidamente o que a rotina faz é:

1. Acionar a rotina $Acharvjt(m, n, s, r)$. Esta rotina faz:

   (a) Achar os valores de v tais que $v|m$ e armazenar estes na lista A.

   (b) Para cada v, calcular os parâmetros o_v, c_v, n'_v e armazenar todos os divisores positivos t de n'_v na lista B.

   (c) Criar uma lista C com os valores de j variando de 0 até $D_v = mdc(v, n_v)$.

   (d) Para cada v na lista A, cada t na lista B e cada j na lista C, testar se $mdc(v, j, t) = 1$ e caso o teste seja verdadeiro, adicionar o valor de j na lista D.

   (e) Para cada $v \in A$, $t \in B$, restringir os elementos j na lista D de forma a ficarem apenas aqueles que geram idempotentes distintos. Isto é feito de acordo com o Teorema 2.16, com a rotina denominada $Jotas(n, r, s, v, t, D)$.

   (f) As triplas (v, j, t) assim determinadas são armazenadas na lista L.

2. Para cada $(v, j, t) \in L$, achar os parâmetros $o_v(Acharov(v, r))$, c_v $(Acharcv(n, r, s, Ov, v))$, n_v, D_v, v'_v, i_v $(Achariv(v, nv))$, i, c e $o_{v,i}$.

3. Calcular os valores i_1, v_1, c_1, i' e c' $(i1v1c1ilcl(v, i, c))$. De acordo com a apresentação do Teorema 2.19, construir a saída:

$$[o_{v,i}, vc_vt\,,\, [o_v/o_{v,i}, 1 + c_1c_vt(r^o_{v,i} - 1), i'v_1v - i]\,,\, [\,]\,].$$

   Para simplificar podemos optar pela saída:

$$[n, k, [o, \alpha, \beta], [\,]\,]$$

   onde $n = o_{v,i}$, $k = vc_vt$, $o = o_v/o_{v,i}$ e $0 \leq \alpha, \beta \leq k$ tal que $1 + c_1c_vt(r^o_{v,i} - 1) \equiv \alpha \bmod k$ e $i'v_1v - i \equiv \beta \bmod k$

Antes de mostrar os exemplos, vejamos como interpretar algumas saídas.
Se a saída assumir a forma:

$$[\,n, k,\, [1, 1, x]\,,\, [\,]\,] \cong M_n(\mathbf{A})\,,\, \mathbf{A} \cong \mathbb{Q}(\xi_k)(g = \xi_k^x, \xi_k g = g\xi_k)$$

para algum $x \in \mathbb{Z}$ então claramente $\mathbf{A} \subset \mathbb{Q}(\xi_k)$ e portanto $\mathbf{A} \cong \mathbb{Q}(\xi_k)$ e a álgebra pode ser interpretada como $M_n(\mathbb{Q}(\xi_k))$.

No caso da saída ser $[\,n, 1,\, [1, 0, x]\,,\, [\,]\,]$ teremos a álgebra $M_n(\mathbb{Q})$, pois $g = 1^x = 1$, para qualquer x e $1^0 = 1$.

Como exemplo, vamos apresentar aqui as saídas obtidas por dois grupos metacíclicos e comparar esta com as saídas obtidas pela rotina contida no pacote "Wedderga".

$\langle a, b \mid a^{24} = 1,\, b^2 = a^{12},\, b^{-1}ab = a^{11} \rangle$

m, n, s, r	Pacote Wedderga
24, 2, 12, 11	[[1, 1, [ ], [ ]], [1, 2, [ ], [ ]],[1, 2, [ ], [ ]], [1, 2, [ ], [ ]], [2, 2, [ ], [ ]],[1, 3, [[2, 2, 0]], [ ]], [1, 6, [[2, 5, 0]], [ ]],[1, 8, [[2, 3, 4]], [ ]], [1, 12, [[2, 11, 0]], [ ]],[1, 24, [[2, 11, 12]], [ ]]]
	$4\mathbb{Q} \oplus 3M_2(\mathbb{Q}) \oplus M_2(\mathbb{Q}(\xi_{12} + \xi_{12}^{-1})) \oplus \mathbf{A} \oplus \mathbf{B}$, $\mathbf{A} \cong \mathbb{Q}(\xi_8)(g : g^2 = -1\,,\, \xi_8 g = g\xi_8^3)$, $\mathbf{B} \cong \mathbb{Q}(\xi_{24})(g : g^2 = -1\,,\, \xi_{24} g = g\xi_{24}^{11})$
24,2,12,11	Rotina implementada
	[[1, 1, [1, 0, 0], [ ]], [1, 2, [1, 1, 1], [ ]],[1, 2, [1, 1, 0], [ ]], [1, 2, [1, 1, 1], [ ]],[1, 3, [2, 2, 0], [ ]], [1, 4, [2, 3, 0], [ ]],[1, 6, [2, 5, 0], [ ]], [1, 8, [2, 3, 4], [ ]], [1, 12, [2, 11, 0], [ ]], [1, 24, [2, 11, 12], [ ]]]
	$4\mathbb{Q} \oplus 3M_2(\mathbb{Q}) \oplus M_2(\mathbb{Q}(\xi_{12} + \xi_{12}^{-1})) \oplus \mathbf{A} \oplus \mathbf{B}$, $\mathbf{A} \cong \mathbb{Q}(\xi_8)(g : g^2 = -1\,,\, \xi_8 g = g\xi_8^3)$, $\mathbf{B} \cong \mathbb{Q}(\xi_{24})(g : g^2 = -1\,,\, \xi_{24} g = g\xi_{24}^{11})$

Observe que ambas as saídas, $[2, 2, [\,], [\,]\,]$ e $[1, 4, [2, 3, 0], [\,]\,]$ representam $M_2(\mathbb{Q})$.

$\langle a, b \mid a^{27} = 1,\, b^2 = a^{27},\, b^{-1}ab = a^{26} \rangle$

m, n, s, r	Pacote Wedderga
27,2,27,26	[[1, 1, [ ], [ ]], [1, 2, [ ], [ ]], [1, 3, [[2, 2, 0]], [ ]],[1, 9, [[2, 8, 0]], [ ]], [1, 27, [[2, 26, 0]], [ ]]]
	$2\mathbb{Q} \oplus M_2(\mathbb{Q}) \oplus M_2(\mathbb{Q}(\xi_9 + \xi_9^{-1})) \oplus M_2(\mathbb{Q}(\xi_{27} + \xi_{27}^{-1}))$
24,2,27,26	Rotina implementada
	[[1, 1, [1, 0, 0], [ ]], [1, 2, [1, 1, 1], [ ]],[1, 3, [2, 2, 0], [ ]], [1, 9, [2, 8, 0], [ ]],[1, 27, [2, 26, 0], [ ]]]
	$2\mathbb{Q} \oplus M_2(\mathbb{Q}) \oplus M_2(\mathbb{Q}(\xi_9 + \xi_9^{-1})) \oplus M_2(\mathbb{Q}(\xi_{27} + \xi_{27}^{-1}))$

3.2 Algoritmos Implementados

Esta seção tem por finalidade apresentar os algoritmos implementados que foram usados para se atingir os objetivos do trabalho. Há duas rotinas principais, $DWmetaciclico(m, n, s, r)$ e $DecomposicaoOrdem(u)$. Como já dito, a primeira rotina implementada neste trabalho, baseada em resultados do Capítulo 2, determina a decomposição de Wedderburn no caso específico quando G é um grupo metacíclico e tem por entrada os parâmetros da apresentação do grupo. Esta rotina possui várias subrotinas que são apresentadas antes, com pequenas explicações do que fazem no corpo do texto. Por fim é apresentada a rotina $DecomposicaoOrdem(u)$ que lista os grupos metacíclicos não abelianos e não isomorfos de uma dada ordem e determina as decomposições para cada um deles. Esta última rotina faz uso do pacote Wedderga, elaborado por Olivieri et all que, no caso de uma álgebra $\mathbb{Q}G$, onde G é abeliano-por-supersolúvel, determina completamente a decomposição de Wedderburn.

```
Divisores:=function(n) #Lista os divisores de n#
 local i, E;

 E:=[];
  for i in [1..n] do
   if n/i in Integers then
   Add(E,i);
  fi;
  od;
 return E;
end;

Acharov:=function(v,r) #Determina o parâmetro Ov#
 local  i, ov;

 ov:=1;
 i:=1;
 while (r^i mod v)<>(1 mod v) do
  i:=i+1;
 od;
 ov:=i;
 return ov;
end;

Acharcv:=function(n,r,s,Ov,v)  #Determina o parâmetro cv#
 local  A, i, cv;

 A:=SortedList(Divisores(n/Ov));
 i:=1;
 while IsInt(s/Gcd(v,n/(Ov*A[i])))<>true do
  i:=i+1;
 od;
 cv:=A[i];
 return cv;
end;

Combli:=function(a,b) #Determina s1, s2 tais que s1*a+s2*b=mdc(a,b)#
 local  A, s1, s2, i, d;

 A:=[];
 d:=Gcd(a,b);
 i:=1;
 if a<>0 then
  while ((d-i*b) mod a<>0 mod a) do
   i:=i+1;
  od;
  s2:=i;
  s1:=(d-b*s2)/a;
  Add(A,[s1,a]);
  Add(A,[s2,b]);
  Add(A,d);
 fi;
```

```
 if a=0 then
  s2:=1;
  s1:=1;
  Add(A,[s1,a]);
  Add(A,[s2,b]);
  Add(A,d);
 fi;
 return A;
end;

Achariv:=function(v,nv,s) #Determina o parâmetro iv#
 local iv, Dv;

 Dv:=Gcd(v,nv);
 iv:=-1*Combli(v,nv)[2][1]*(s/Dv);
 return iv;
end;

Jotas:=function(n,r,s,v,t,D) #Lista os parâmetros j que dão origem a idempotentes distintos#
 local  j, l, k, ov, cv, nv, Dv, vlv, iv, i, ovi, alphakv, B, A, E, c, x;

 A:=D;
 B:=[];
 E:=[];
 ov:=Acharov(v,r);
 cv:=Acharcv(n,r,s,ov,v);
 nv:=n/(ov*cv);
 Dv:=Gcd(v,nv);
 vlv:=v/Dv;
 iv:=Achariv(v,nv,s);
 x:=0;
  while Size(A)>0 do
   c:=A[1];
   i:=iv*t+vlv*c;
   ovi:=Acharov(v/(Gcd(v,i)),r);
   for l in [1..Size(A)] do
    x:=0;
    k:=1;
    while (k<=ovi) do
     alphakv:=(iv*((r^k)-1))/(vlv);
     if A[l] mod Dv=(c*(r^k)+alphakv*t) mod Dv then
      x:=1;
      k:=ovi;
     fi;
     k:=k+1;
    od;
    if x=1  then
     Add(B,A[l]);
    fi;
   od;
   for l in [1..Size(B)] do
    SubtractSet(A,[B[l]]);
   od;
```

```
   Add(E,c);
   B:=[];
  od;
 return E;
end;

i1v1c1ilcl:=function(v,i,c) #Determina os parâmetros i1, v1, c1, i' e c'#
 local  aux, B, j, alpha, beta, R, alphab, betab, i1, v1, c1, il, cl;

 B:=[];
 aux:=Gcd(v,c);
 alpha:=Combli(i, aux)[1][1];
 beta:=Combli(i, aux)[2][1];
 R:=(c/aux)/(Gcd(c/aux,aux)*Gcd(c/aux,alpha));
 j:=alpha+R*aux;
 alphab:=Combli(v,c)[1][1];
 betab:=Combli(v,c)[2][1];
 i1:=-1*j;
 v1:=(beta-R*i)*alphab;
 c1:=(beta-R*i)*betab;
 il:=Combli(i1,c)[1][1];
 cl:=Combli(i1,c)[2][1];
 Add(B,i1);
 Add(B,v1);
 Add(B,c1);
 Add(B,il);
 Add(B,cl);
 return B;
end;

Acharvjt:=function(m,n,s,r) #Determina os parâmetros (v,j,t) que dão origem a idempotentes distintos#
 local  i, j, k, A, B, C, D, E, ov, cv, nv, nvl;

 A:=Divisores(m);
 B:=[];
 C:=[];
 D:=[];
 E:=[];
 for i in [1..Size(A)] do
  ov:=Acharov(A[i],r);
  cv:=Acharcv(n,r,s,ov,A[i]);
  nv:=n/(ov*cv);
  nvl:=nv/(Gcd(A[i],nv));
  B:=Divisores(nvl);
  C:=[0..Gcd(A[i],nv)];
  for j in [1..Size(B)] do
   for k in [1..Size(C)] do
    if Gcd(A[i],B[j],C[k])=1 then
     Add(D,C[k]);
    fi;
   od;
   D:=Jotas(n,r,s,A[i],B[j],D);
   for k in [1..Size(D)] do
```

```
    Add(E,[A[i],D[k],B[j]]);
   od;
   D:=[];
  od;
 od;
 return E;
end;

DWmetaciclico:=function(m,n,s,r) #Determina a decomposição de wedderburn para G metacíclico#
 local  u, v, j, t, ov, cv, nv, Dv, vlv, iv, i, ovi, v1, c1, il, L, A, B, C;

 A:=[];
 B:=[];
 C:=[];
 L:=Acharvjt(m,n,s,r);
 for u in [1..Size(L)] do
  v:=L[u][1];
  j:=L[u][2];
  t:=L[u][3];
  ov:=Acharov(v,r);
  cv:=Acharcv(n,r,s,ov,v);
  nv:=n/(ov*cv);
  Dv:=Gcd(v,nv);
  vlv:=v/Dv;
  iv:=Achariv(v,nv,s);
  i:=iv*t+vlv*j;
  ovi:=Acharov(v/Gcd(v,i),r);
  A:=i1v1c1ilcl(v,i,cv*t);
  v1:=A[2];
  c1:=A[3];
  il:=A[4];
  B:=[ovi,v*cv*t,[ov/ovi,(1+c1*cv*t*((r^ovi)-1)) mod (v*cv*t),(il*v1*v-i) mod (v*cv*t)],[]];
  Add(C,B);
 od;
 return C;
end;

DecomposicaoOrdem:=function(u) #Determina a decomposição de wedderburn para grupos#
 local  m, n, i, Au, C, s, r, k, t, g, ng, T, B, A, QT, D; #metacíclicos não abelianos#
                                                           #e não isomorfos de ordem u#
 D:=Divisores(u);
 g:=FreeGroup("a","b");
 B:=[];
 C:=[];
 Add(B,Group([()]));
 for i in [1..Size(D)] do
  m:=D[i];
  n:=u/m;
  for s in [1..m] do
  for r in [1..m] do
  t:=0;
   if ((r^n)-1)/m in Integers and (s*(r-1))/m in Integers then
     ng:=NormalClosure(g,Subgroup(g,[g.1^m,(g.2^n)*(g.1^-s),(g.1)^(g.2)*(g.1^-r)]));
```

```
      T:=g/ng;
      if Size(T)=m*n and IsAbelian(T)=false then
      Add(B,T);
      k:=1;
      while k<Size(B) do
       if IsomorphismGroups(B[k],T)<>fail  then
        t:=1;
        k:=(Size(B)-1);
        B:=B{[1..k]};
       fi;
       k:=k+1;
      od;
       if t=0 then
       QT:=GroupRing(Rationals,T);
       A:=WedderburnDecompositionInfo(QT);
       Au:=[m,n,s,r];
       Add(C,Au);
       Add(C,A);
       Add(C,"#");
       fi;
     fi;
    fi;
     od;
     od;
    od;
  return C;
end;
```

Comentários Finais

Esta parte da dissertação será usada para apresentar tópicos de estudo como sugestão para trabalhos futuros. Em primeiro lugar, seria interessante fazer um estudo mais aprofundado da questão de quando dois grupos metacíclicos vão ou não vão ser isomorfos, liberando assim, o GAP do problema desta decisão. No algoritmo utilizado, este problema exigiu a construção efetiva dos grupos metacíclicos como um quociente de um grupo livre F por N, onde

$$F = \langle a, b \rangle$$

e

$$N = \langle a, b \,:\, a^m = 1, b^n = a^s, a^b = a^r \rangle.$$

Para valores grandes dos parâmetros m e n, esta construção parece dispender muita memória.

Um outro tópico de estudo a sugerir é sobre a questão de quando duas álgebras da forma:

$$M_n(\mathbf{A}), \text{ onde } \mathbf{A} \cong \mathbb{Q}(\xi_k)(g \,:\, g^o = \xi_k^\beta, \xi_k g = g\xi_k^\alpha)$$

são ou não são isomorfas.

Com a resolução satisfatória destes dois problemas, poderíamos pensar em implementar um algoritmo mais completo, onde as ordens dos grupos iriam aumentando e todo o trabalho de análise ficaria por conta do computador, que só pararia se, por acaso encontrasse dois grupos metacíclicos não isomorfos com álgebras de grupos racionais isomorfas.

Referências Bibliográficas

[1] R. Ayoub G. and Ch. Ayoub, *On the group ring of a finite abelian group*, J. Aus. Math. Soc. 1 (1969) 245-261.

[2] C. W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Wiley-Interscience, New York, 1962.

[3] The GAP Group, 2005. GAP-Groups, Algorithms and Programming, versão 4.4. Disponível em: http://www.gap-system.org.

[4] E. G. Goodaire, E. Jespers, C. Polcino Milies, *Alternative Loop Rings*, Math. Studies 184, North Holland, 1996.

[5] E. Jespers, G. Leal and A. Paques, *Central idempotents in rational group algebras of finite nilpotent groups*, J. Alg. and its Applications. 2, 1 (2003) 57-62.

[6] D. L. Johnson, *Presentations of Groups*, Second Editon, London Mathematical Society, Students Texts 15, 1997.

[7] C. P. Milies and S. K. Sehgal, *An Introduction to Group Rings*. Kluwer Academic Publishers, 2002.

[8] A. Olivieri and Á. del Rio, *An algorithm to compute the primitive central idempotents and the Wedderburn decomposition of a rational group algebra*, J. Symbolic Computations, 35 (2003) 673-687.

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

[10] A. Olivieri, Á. del Rio and J. J. Simón, *The group of automorphisms of the rational group algebra of a finite metacyclic group*, (Preprint).

[11] A. Olivieri, Á. del Rio and J. J Simón, *On monomial characters and central idempotents of rational group algebras*, Comm. Algebra. 32, 4 (2004) 1531-1550.

[12] D. S. Passman, *The Algebraic Structure of Group Ring*, University of Winsconsin-Madison. Reprint Edition, 1985.

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