Sobre o Algoritmo de Newman-O'Brien para Geração de p-Grupos

Ángela Mabel Maldonado

Prof.Dr. Noraí Romeu Rocco
Orientador

IMECC-UNICAMP

Campinas, agosto de 1994

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida pela Srta. **Angela Mabel Maldonado** e aprovada pela Comissão Julgadora.

Campinas, 31 de agosto de 1994

Prof. Dr. Noraí Romeu Rocco

Orientador

Dissertação apresentada ao Instituto de Matemática, Estatística e Ciência da Computação, UNICAMP, como requisito parcial para obtenção do Título de MESTRE em Matemática.

À minha mãe

(*minha força e minha fé*)

Ao meu irmão Luis

(*com eterna saudade*)

"... la soledad te ayuda únicamente si la vas a colmar de ecos necesarios de nostalgias tangibles / solo asi podrá llegar a ser tu cantera de prójimos".

Mario Benedetti

Agradecimentos

Mesmo na aparente solidão que nos impõe o trabalho intelectual, há sempre uma "porção de presenças" que nos acompanham e nos ajudam para que possamos alcançar nossos objetivos. Por isso eu quero expressar aqui os meus agradecimentos a todos aqueles que estiveram comigo e possibilitaram de alguma ou outra maneira a conclusão deste trabalho.

Em especial

Ao Professor Noraí R. Rocco pela sua paciente orientação e o seu exemplo de trabalho e dedicação.

Aos meus colegas e amigos do "predinho".

Aos funcionários do IMECC.

À Sra. Roseli R. Rodrigues pela sua inestimável colaboração e seu excelente trabalho de digitação.

À Sirlene pela sua sensibilidade, à Michelle pelo "pé no chão", à Julimara pelas aulas de português e às três, pela amizade.

À minha mãe pela sua generosidade e pelo seu constante exemplo de luta, de amor e de coragem.

Aos meus "pais postiços", Nilda G. de Guiotto e Omar Guiotto ("Coco"), pelo carinho e apoio incondicionais e, mais ainda, por partilharem comigo da família maravilhosa que eles souberam edificar.

Aos meus amigos do Departamento de Matemática (Facultad de Cs. Exatas) e do Departamento de Físico-Matemática (Facultad de Ingenieria) da Universidad Nacional de La Plata.

Ao Capes pelo auxílio financeiro e, fundamentalmente:

Ao Brasil, pelo coração aberto.

Resumo

O propósito deste trabalho é estudar os aspectos teóricos e certos detalhes da implementação do *Algoritmo para geração de p-grupos* desenvolvido por M.F. Newman e E.A. O'Brien. A implementação deste algoritmo permite o cálculo de certas extensões particulares de p-grupos, possibilitando assim, a determinação dos p-grupos finitos.

Fazemos isto no capítulo 3, onde também incluimos um exemplo de algumas iterações deste procedimento, calculando manualmente os 2-grupos 2-gerados de ordem menor o igual a 2^4.

Lista de Símbolos

$\mathbb{N}, \mathbb{Z}$	:	conjunto de números naturais e inteiros
$\hookrightarrow$	:	homomorfismo injetor
$\twoheadrightarrow$	:	homomorfismo sobrejetor
$\cong$	:	isomorfismo
$H \leq G$	:	H é subgrupo de G
$H \leq G$	:	H é subgrupo próprio de G
$H \overset{<}{_{\max}} G$	:	H é subgrupo maximal de G
$H \trianglelefteq G$	:	H é subgrupo normal de G
$< X >$	:	grupo gerado pelo conjunto X
$\|G\|$	:	ordem (cardinalidade) de G
$[x, y]$	:	comutador de x e y
$[A, B]$	:	subgrupo comutador dos conjuntos A e B
G'	:	subgrupo derivado de G
$Z(G)$	:	centro de G
$\mathrm{Aut}(G)$	:	grupo dos automorfismos de G
$G \times H$	:	produto semidireto de G por H
$\phi(G)$	:	subgrupo de Frattini de G
V	:	grupo de Klein
Q_{2n}	:	grupo quatêrnio generalizado de ordem $4n$
D_n	:	grupo diedral de ordem $2n$
S_n	:	grupo simétrico de ordem n
$\mathrm{m}(Y)$	:	grupo das permutações de Y
C_n	:	grupo cíclico de ordem n

Índice

"Die Hauptschwierigkeit besteht dabei nicht in einer Konstruktion aller Gruppen eines bestimmten Typs, sondern in der Angabe eines vollständigen Systems nicht isomorpher Gruppen aus den konstruierten Gruppen".

W. Magnus, 1937

Introdução

O problema de descrever todos os grupos de ordem n, para n, um inteiro positivo, dando uma apresentação por geradores e relações para cada tipo de isomorfismo de tais grupos foi iniciado por A. Cayley [2] em 1878. Ele chamou este problema de "*problema ger[illegible] para grupos finitos*".

Já neste século, no final dos anos 30, o problema tinha sido resolvido para $n \leq 215$ com exceção de $n = 128$ e $n = 192$. Pouco depois, P. Hall fez alguns trabalhos referentes à determinação e classificação dos grupos de ordem 128. Num artigo de 1940 [5], ele comenta que algumas técnicas usadas na classificação de grupos de ordem pequena falhavam para grupos de ordem 128 e então estabelece o conceito de isoclinismo que, enfraquecendo a noção de isomorfismo e admitindo que os p-grupos abelianos finitos dispensam classificação, permite a classificação dos p-grupos finitos em *famílias* mutuamente excludentes.

Em 1980, Rodemich publicou um trabalho no qual afirmava que existem 2358 grupos de ordem 128 divididos em 113 famílias de isoclinismo. Ele calculava manualmente essas famílias e, na maioria dos casos, usava cálculos computacionais para contar o número de tipos de isomorfismo de grupos dentro de cada família.

Em 1975, M.F. Newman [10] deu a descrição de um algoritmo para o cálculo de extensões particulares de p-grupos, conhecido como "*algoritmo para geração de p-grupos*". Uma implementação parcial do mesmo foi desenvolvida por Alford, J.A. Ascione, G. Havas, C.R. Leedham-Green e M.F. Newman em 1976.

Em 1982, R. James e M.F. Newman, fazendo uso dessa implementação parcial, descobriram alguns erros no trabalho de Rodemich. Posteriormente, um programa feito por um aluno de Newman especialmente para checar os cálculos de Rodemich revelou também alguns erros nos cálculos de James e Newman.

Em 1986, uma implementação geral do algoritmo para geração de p-grupos foi desenvolvida por M.F. Newman e E.A. O'Brien [12]. Esta implementação permitiu a determinação completa dos grupos de ordem 128 pelo computador, mostrando que existem 2328 tais grupos (o tempo de CPU gasto em gerar a lista das apresentações foi aproximadamente 8 minutos num VAX 8700).

A aplicação deste algoritmo para determinar os grupos de ordem dividindo 256 é descrita em James, Newman e O'Brien [7] e em O'Brien [11].

Assim, o algoritmo para geração de p-grupos se revelou uma ferramenta importantíssima para resolver o problema formulado por Cayley no caso particular dos p-grupos finitos.

O presente trabalho tem por objetivo o estudo desse algoritmo. No capítulo 1, incluimos alguns conceitos e propriedades básicas da teoria de grupos que são utilizados no decorrer do mesmo. Esses conceitos podem ser encontrados na maioria dos textos em teoria de grupos, onde o leitor interessado poderá apreciar as demonstrações omitidas aqui. Na seção 1.7 apresentamos com razoável grau de detalhes o algoritmo de Schreier-Sims para o cálculo do estabilizador de um ponto em grupos de permutações.

No capítulo 2, estudamos o algoritmo do quociente nilpotente, que é básico para se determinar quocientes nilpotentes finitos de um dado grupo finitamente apresentado. O material aí exposto tem como base os trabalhos de Havas-Newman [6] e Vaughan-Lee [15], este último, no caso particular da consistência.

Finalmente no capítulo 3, com base no artigo de E.A. O'Brien [12] abordamos os aspectos teóricos bem como certos detalhes da implementação do algoritmo para geração de p-grupos. Concluimos esta dissertação com um exemplo elaborado de aplicação do algoritmo para um grupo 2-gerado.

Capítulo 1

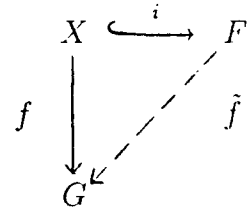
Alguns conceitos básicos da teoria de grupos

Neste capítulo destacamos alguns resultados básicos que são usados no decorrer deste trabalho. Com isto pretendemos facilitar a leitura do mesmo, evitando a necessidade de referências constantes a outros textos.
As demonstrações, na maioria omitidas, podem ser encontradas em [8], [14], [3], [13].

1.1 Grupos Livres e Apresentações de Grupos

Grupos Livres

Definição 1.1.1: Um grupo F é dito livre sobre um seu subconjunto X se, dado um grupo arbitrário G e uma função $f : X \to G$, existe um único homomorfismo $\tilde{f} : F \to G$ tal que $f|_X = f$.



□

Proposição 1.1.2: *Se F é livre sobre X, então X gera F.*

Demonstração. v. JOHNSON [8]. ■

Proposição 1.1.3: *Dois grupos livres F_1 e F_2 sobre X_1 e X_2 respectivamente são isomorfos se, e somente se, $|X_1| = |X_2|$.*

Demonstração. v. JOHNSON [8]. ■

Definição 1.1.4: *Se F é livre sobre X, X é dito uma base (livre) para F e $|X|$ é chamado de* posto *de F.* □

Construção de um Grupo Livre sobre X

Se $X = \emptyset$, então $F := \{e\}$.

Se $|X| = 1$, então é claro que $F \cong (\mathbb{Z}, +)$.

Se $|X| \geq 2$, seja $X = \{x_i | i \in I\}$. Podemos supor X bem ordenado.

Seja $\hat{X}$ equipolente a X tal que $X \cap \hat{X} = \emptyset$.

Considere $T = X \cup \hat{X}$ e $T^n = T \times T \times \cdots \times T$, $n \in N$, onde, se $n = 0$, definimos $T^0 := \{e\}$.

Seja $W := \cup_{n \geq 0} T^n$ o conjunto das *palavras no alfabeto* X, isto é,

$$\begin{aligned} w \in W &\iff \exists n \in N \text{ tal que } w \in T^n \\ &\iff w = (y_{i_1}, y_{i_2}, \ldots, y_{i_n}) \ , \ y_{i_j} \in X \cup \hat{X} \end{aligned}$$

Um segmento $(y_{i_r}, y_{i_{r+1}}, \ldots, y_{i_s})$ de w com $1 \leq r \leq s \leq n$ é uma *subpalavra* de w. A *composta* uv de duas palavras $u = (x_{i_1}, \ldots, x_{i_n})$ e $v = (y_{i_1}, \ldots, y_{i_m})$ pertencentes a W é dada por

$$uv = (x_{i_1}, \ldots, x_{i_n}, y_{i_1}, \ldots, y_{i_m}) \ .$$

Definamos em W a seguinte relação de equivalência, que denotaremos por $\sim$: se $u, v \in W$, então $u \sim v$ se, e somente se, v pode ser obtida de u através de um número finito de inserções ou remoções de subpalavras da forma $(\hat{y_i}, y_i)$ ou $(y_i, \hat{y_i})$.

Diremos que $u \in W$ é reduzida se u não contém subpalavras da forma $(\hat{x}, x)$ ou $(x, \hat{x})$.

Para $u \in W$ (arbitrária), seja $\rho(u)$ a palavra obtida de u pela remoção sucessiva (da direita para a esquerda) das subpalavras da forma $(x, \hat{x})$ ou $(\hat{x}, x)$.

Exemplo: Seja $u = (x_1, x_1, x_2, \hat{x_2}, x_3, x_1, \hat{x_2}, x_2, x_3)$. Removendo a subpalavra $(\hat{x_2}, x_2)$, temos $u' = (x_1, x_1, x_2, \hat{x_2}, x_3, x_1, x_3)$. Removendo agora a subpalavra $(x_2, \hat{x_2})$, temos a palavra $u'' = (x_1, x_1, x_3, x_1, x_3)$ que é uma palavra reduzida. Logo $\rho(u) = (x_1, x_1, x_3, x_1, x_3)$.

É claro que $\rho(u)$ é uma palavra reduzida que coincide com u se u for reduzida e, mais ainda, $u \sim \rho(u)$.

Denotaremos $u \equiv v$ no caso em que u e v sejam idênticas como palavras. Com esta notação, estabeleçamos os seguintes resultados:
Se $u, v \in W$, $uv := (u, v)$, então

(i) $\rho(uv) = \rho(u\ \rho(v))$, segue da definição de ρ.

(ii) $\rho(x_i, \hat{x}_i, u) \equiv \rho(u) \equiv \rho(\hat{x}_i, x_i, u)$ (segue de (i)).

(iii) $\rho(u, x_i, \hat{x}_i, v) \equiv \rho(uv) \equiv \rho(u, \hat{x}_i, x_i, v)$ (segue de (i) e (ii)).

(iv) $\rho(uv) \equiv \rho(\rho(u)\rho(v))$ (por indução sobre o comprimento de u, usando (i), (ii) e (iii)).

Note que, se $u \sim v$ e ambas são reduzidas, então $u \equiv v$ e, portanto, em cada classe de equivalência de W sob $\sim$ existe exatamente uma palavra reduzida.

Chamamos $F(X)$ ao conjunto de todas as palavras reduzidas correspondentes às palavras em W.

Resultado 1: *$F(X)$ é um grupo sob a operação definida como segue $u, v \in F(X)$, $u.v := f(uv)$.*

Resultado 2: *$F(X)$ é livre sobre X.*

Temos assim construído o grupo livre sobre o conjunto X.

Apresentações de Grupos

Proposição 1.1.5: *Todo grupo é imagem homomórfica de um grupo livre (isto é, um quociente de um grupo livre).*

Demonstração: De fato, dado o grupo G, seja $Y = G$. É claro que Y é um conjunto de geradores para G, consideremos Y indexado por um conjunto I, i.e. $Y = \{y_i | i \in I\}$. Se $X = \{x_i, i \in I\}$ é um conjunto equipolente a Y e construirmos $F := F(X)$ o grupo livre sobre X, temos que a aplicação $x_i \mapsto y_i$, $i \in I$ se estende a um único homomorfismo φ sobrejetor (Y gera G), $\varphi : F \twoheadrightarrow G$, assim $G \cong F/\ker\varphi$. ∎

Com a notação da proposição anterior, seja $R \subseteq F(X)$ um conjunto de palavras que geram N como subgrupo normal de F, i.e., $N =< R >^F =< r^f = f^{-1}rf | r \in R,\ f \in F >$.

Definição 1.1.6: Na situação acima, denotaremos $G =< X/R >$ e diremos que $< X/R >$ é uma *apresentação para* G. Os elementos de X são chamados *geradores* e os de R são chamados *relatores*. □

Cada um dos elementos de R tem por imagem 1_G pelo homomorfismo φ, i.e., se $r = x_{i_1}^{\alpha_1} \ldots x_{i_k}^{\alpha_k} \in R$, então temos a seguinte *relação entre os geradores de* G: $y_{i_1}^{\alpha_1} \ldots y_{i_k}^{\alpha_k} = 1_G$, por isso às vezes na apresentação $< X/R >$ para o grupo G, falamos de *relações* em lugar de relatores e escrevemos $G =< X |\ r = 1,\ r \in R >$.

Exemplos:

- O grupo cíclico de ordem n, C_n, tem apresentação $< x/x^n = 1 >$;
- O grupo diedral D_n (das simetrias de um polígono regular de n lados) tem apresentação $< x, y/x^n = 1, y^2 = 1, (x, y)^2 = 1 >$.

Observação 1.1.7: *Pode provar-se que um grupo F é livre sobre um seu subconjunto Y se e somente se:*

1) *Y gera F*

2) *Não existe relação não trivial entre os geradores.*

Neste caso, uma apresentação para F é: $F =< Y/ >$.

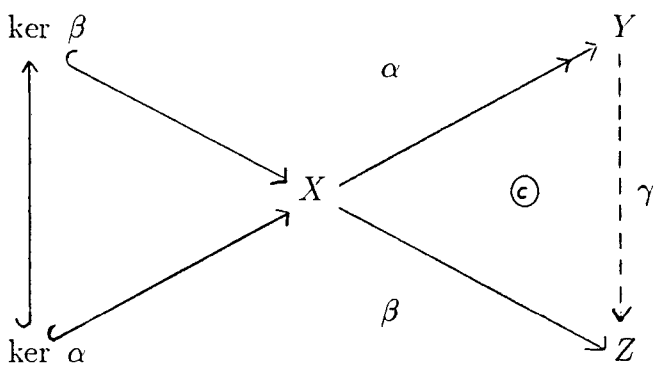
G é finitamente apresentado se existem X e R finitos tais que $G \cong < X/R >$. □

Proposição 1.1.7: *Todo grupo tem uma apresentação e todo grupo finito tem uma apresentação finita.*

Demonstração:v. JOHNSON [8]. ■

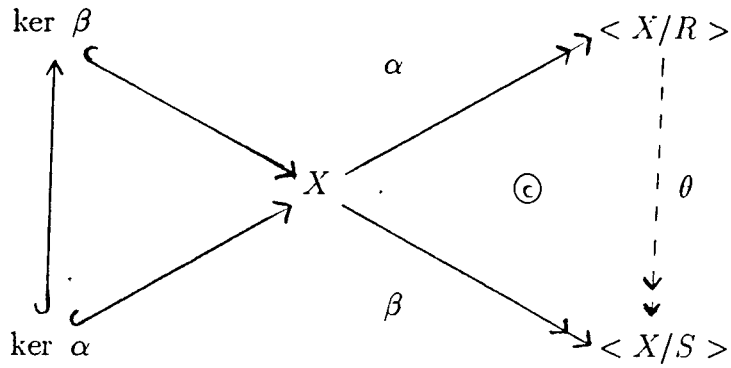
Propriedades das Apresentações.

Lema 1.1.8: *Sejam* X, Y, Z *grupos e* $\alpha : X \to Y$, $\beta : X \to Z$ *homomorfismos,* α *sobrejetor e* $\ker \alpha \subseteq \ker \beta$. *Então existe um homomorfismo* $\gamma : Y \to Z$ *tal que* $\alpha\gamma = \beta$.



Demonstração: v. JOHNSON [8]. ■

Teorema 1.1.9 (von Dyck): *Seja* X *um conjunto e* F *o grupo livre sobre* X. *Se* R *e* S *são subconjuntos de* F *tais que* $R \subseteq S$, *então existe um epimorfismo* $\theta :< X/R > \twoheadrightarrow < X/S >$ *que fixa* X *elemento a elemento. O núcleo de* θ *é justamente o fecho normal de* $S - R$ *em* $< X/R >$.



Demonstração: v. JOHNSON [8]. ■

Teorema 1.1.10 (Teste de Substituição): *Sejam $G =< X/R >$, um grupo H e $\theta : X \to H$ uma função. Então θ se estende a um homomorfismo $\theta'' : G \to H$ se, e so mente se, para todo $x \in X$ e todo $r \in R$, o resultado da substituição de x por $x\theta$ em r dá a identidade de H.*

Demonstração: v. JOHNSON [8]. ■

Teorema 1.1.11: *Sejam $F =< X/ >, G =< X/R >$ e suponhamos $w, r \in F$ com w arbitrário e $r \in \overline{R} - R$. Se y é um símbolo que não está em X, então ambas as inclusões:*

$$X \mapsto < X/R, r >$$
$$X \mapsto < X, y/R, y^{-1}w >$$

se estendem a isomorfismos com domínio G.

Demonstração: v. JOHNSON [8]. ■

Este teorema fornece quatro formas de modificar uma apresentação dada, $< X/R >$, para obter outra, $< X'/R' >$ digamos, do mesmo grupo. Essas formas são chamadas de *transformações de Tietze* e são definidas da seguinte maneira:

Seja $G =< X/R >$.

$\underline{R^+}$: Se $r \in < X >$ e $r = 1$ em G, então sejam $X' = X$ e $R' = R \cup \{r\}$

$\underline{R^-}$: Se $r \in R$ é tal que $r = 1$ em $< X/R - \{r\} >$, então sejam $X' = X$ e $R' = R - \{r\}$

$\underline{X^+}$: Se $w \in < X >$ e $x \notin X$, sejam $X' = X \cup \{x\}$ e $R' = R \cup \{wx^{-1}\}$

$\underline{X^-}$: Se $x \in X$ e $w \in < X - \{x\} >$ é tal que $wx^{-1} \in R$, então substitua x por w em todo elemento de $R - \{wx^{-1}\}$ para obter R' e seja $X = X - \{x\}$.

(As transformações R^+ e R^- correspondem a adicionar e remover relatores supérfluos enquanto X^+ e X^- correspondem a adicionar e remover geradores supérfluos respectivamente).

Observações:

1) *Dadas duas apresentações finitas do mesmo grupo, cada uma pode ser obtida a partir da outra por uma seqüência finita de transformações de Tietze.*

2) *Se a apresentação* $< X'/R' >$ *é obtida a partir de* $< X/R >$ *por uma seqüência finita de transformações de Tietze, então* $< X'/R' > \cong < X/R >$.

Teorema 1.1.12: *Se* $G =< X/R >$ *e* $H =< Y/S >$, *então o produto direto* $G \times H$ *tem apresentação* $< X, Y/R, S, T >$ *onde* T *é o seguinte conjunto*

$$\{x^{-1}y^{-1}xy \ / \ x \in X, \ y \in Y\}.$$

Demonstração: v. JOHNSON [8]. ■

1.2 p-Grupos

Definição 1.2.1: Seja p um primo. Um grupo G é dito um *p-grupo* se a ordem de todo elemento de G é uma potência de p. □

Observação 1.2.1 (1): *Se* G *for finito, dizer que* G *é um p-grupo é equivalente a dizer que* $|G| = p^n$ *para algum* $n \in N$. □

Exemplos: $p = 2$

1) $D_4, Q_8, \mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ são 2-grupos finitos de ordem 2^3

2) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \ldots \times \mathbb{Z}/2\mathbb{Z} \times \ldots$ é um 2-grupo infinito.

Definição 1.2.2: Um subgrupo S de um grupo G é um subgrupo de Sylow de G se:

1) S é um P-grupo

2) Se $S' \leq G, S'$ é um p-grupo e $S \leq S'$, então $S' = S$. □

Proposição 1.2.3:

(i) *Se G é um p-grupo finito não trivial, então $|Z(G)| > 1$.*

(ii) *Seja $H \trianglelefteq G$. Se H e G/H ambos são p-grupos, então G é um p-grupo.*

(iii) *Seja $|G| = p^n$, com p primo. Se $0 \leq k \leq n$, então G contém um subgrupo normal de ordem p^k.*

(iv) *Se G é um p-grupo finito e $M \leq G$ é maximal, então $M \trianglelefteq G$ é $[G : M] = p$.*

(v) *Se G é um p-grupo finito e $H \leq G$, então $H \leq N_G(H)$. $(N_G(H) = \{g \in G / x^g = x\})$.*

Demonstração: v. ROTMAN [14] ou HALL [3]. ■

Definição 1.2.4: Um p-grupo G é dito *p-grupo abeliano elementar* se G for abeliano e $x^p = 1 \ \forall \ x \in G$. □

1.3 Grupos Nilpotentes e Séries Centrais

Grupos Nilpotentes

Definição 1.3.1: Um grupo G é dito *nilpotente* se tem uma *série central*, i.e., uma série:

(1) $$G = G_0 > G_1 > \ldots > G_n = \{1\} \quad \text{tal que:}$$

a) $G_i \lhd G, \quad i = 0, 1, \ldots, n$

b) $G_i/G_{i+1} \leq Z(G/G_{i+1})$

O *comprimento* da série (1) é n.

A *classe de nilpotência* de um grupo nilpotente $G, cl(G)$, é o comprimento da menor série central de G. □

Observação: *Note que* b) *requer, em particular, que* $\{1\} \neq G_{n-1} \leq Z(G)$. □

Exemplos:

1) Os grupos abelianos não triviais são os grupos nilpotentes de classe 1, pois $G = G_0 > G_1 = \{1\}$ é uma série central, de comprimento 1.

2) O grupo simétrico S_3 não é nilpotente, pois $Z(S_3) = \{1\}$.

Proposição 1.3.2: *Subgrupos, quocientes e produtos diretos finitos de grupos nilpotentes são também nilpotentes.*

Demonstração: v. ROTMAN [14]. ■

Proposição 1.3.3: *Todo p-grupo finito é nilpotente.*

Demonstração: v. ROTMAN [14]. ■

Subgrupos Comutadores

Definição 1.3.4: Sejam $x_1, x_2, \ldots$ elementos de um grupo G. O *comutador de* x_1 e x_2 (nesta ordem) é o elemento $[x_1, x_2] := x_1^{-1}x_2^{-1}x_1x_2 = x_1^{-1}x_1^{x_2}$, onde $x_1^{x_2} = x_2^{-1}x_1x_2$. Para $n \geq 2$, o *comutador simples de peso* n é definido recursivamente por

$$[x_1, x_2, \ldots, x_n] := [[x_1, \ldots, x_{n-1}], x_n], \quad \text{com a convenção que} \quad [x_1] = x_1. \qquad \square$$

Proposição 1.3.5: *Sejam x, y, z elementos de um grupo G. Então:*

i) $[x,y] = [y,x]^{-1}$

ii) $[xy,z] = [x,z]^y[y,z]$; $[x,yz] = [x,z][x,y]^z$

iii) $[x,y^{-1}] = [y,x]^{y^{-1}}$; $[x^{-1},y] = [y,x]^{x^{-1}}$

iv) $[x,y^{-1},z]^y[y,z^{-1},x]^z[z,x^{-1},y]^x = 1$ (Identidade de Hall Witt)

Demonstração: Segue da definição do comutador. ■

Definição 1.3.6: Sejam $X_1, X_2, \ldots$ subconjuntos não vazios de um grupo G. *O subgrupo comutador* de X_1 e X_2, denotado $[X_1, X_2]$ é definido por:

$$[X_1, X_2] =< [x_1, x_2] \ / \ x_1 \in X_1, x_2 \in X_2 > .$$

Para $n \geq 2$, definimos recursivamente

$$[X_1, X_2, \ldots X_n] = [[X_1, \ldots, X_{n-1}], X_n]$$

convencionando que $[X_1] =< X_1 >$. □

Proposição 1.3.7: *Sejam $\phi \neq X \subseteq G$ e $K \leq G$. Então*

i) $< X >^K =< X, [X,K] >$

ii) $[X,K]^K = [X,K]$

iii) Se $K =< Y >$ então $[X,K] = [X,Y]^K$.

Demonstração: v. ROCCO [13]. ■

Proposição 1.3.8: Sejam $H, K \leq G$. Então:

i) $[H,K] \trianglelefteq < H,K >$

ii) Se $H_1 \leq H, K_1 \leq K$, então $[H_1, K_1] \leq [H,K]$.

iii) $[H,K] \leq H \Leftrightarrow K \leq N_G(H)$

iv) Se $\alpha : G \to G_1$ é um homomorfismo de grupos, então

$$[H,K]^\alpha = [H^\alpha, K^\alpha] \quad (\text{onde } X^\alpha = \text{ imagem de } X \text{ por } \alpha).$$

v) Se H e K são normais (respectivamente característicos) em G, então $[H,K]$ é um subgrupo normal (respectivamente característico) de G.

Demonstração: v. ROCCO [13]. ■

Série Central Inferior

Definição 1.3.9: A série central inferior de um grupo G

$$G = \gamma_0(G) \geq \gamma_1(G) \geq \ldots \geq \gamma_i(G) \geq \ldots \tag{2}$$

é definida recursivamente por $\begin{cases} \gamma_0(G) &= G \\ \gamma_{i+1}(G) &= [\gamma_i(G), G], \quad i \geq 1. \end{cases}$

É comum denotar-se por G' o segundo termo desta série, i.e., $G' = \gamma_1(G) = [G,G]$ o qual é dito *grupo derivado de* G. □

Observação: *Cada termo* $\gamma_i(G)$ *é um subgrupo totalmente invariante em* G, *i.e., é invariante por qualquer endomorfismo de* G, *fato este que decorre da proposição* 1.3.8 (iv). *Em particular,* $\gamma_i(G) \trianglelefteq G, \forall\ i$. *Portanto tomando-se o quociente por* $\gamma_{i+1}(G)$ *na igualdade* $\gamma_{i+1}(G) = [\gamma_i(G), G]$, *obtem-se*

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

o que significa que para cada $i \geq 1, \dfrac{\gamma_i(G)}{\gamma_{i+1}(G)} \leq Z(G/\gamma_{i+1}(G))$. *Ou seja que* (2) *é uma série central.*

Notemos também que a série (2) *pode tornar-se estacionária e partir de algum termo* $\gamma_w(G) > \{1\}$ (*é o que acontece, por exemplo com o grupo simétrico* $S_3, \gamma_2(S_3) = \gamma_3(S_3) = \ldots = A_3$). □

Proposição 1.3.10: *Se G é nilpotente, então*

$$cl(G) = k \Leftrightarrow \gamma_{k-1}(G) \neq \{1\} \quad \text{e} \quad \gamma_k(G) = \{1\}.$$

Proposição 1.3.11: *Seja G gerado por um conjunto X. Então*

i) $\gamma_i(G) =< [x_1, \ldots, x_i]^g / x_j \in X, j = 1, \ldots, i, g \in G >$.

ii) $\gamma_i(G) =< [x_1, \ldots, x_i]; \gamma_{i+1}(G) >$ *onde* $x_j \in X$ *para* $j = 1, \ldots, i$.

iii) *Se* $X = \{x, y\}$ *então* $\gamma_2(G) =< [x, y]; \gamma_3(G) >$ *e assim,* $\gamma_2(G)/\gamma_3(G)$ *é cíclico.*

iv) *Se* $X = \{x, y\}$ *então* $G'' := \gamma_2(G') \leq \gamma_5(G)$.

Demonstração: v. ROCCO [13]. ■

Proposição 1.3.12: *Seja G um grupo nilpotente finitamente gerado então G tem uma série central*

$$\{1\} = G_0 \leq G_1 \leq \ldots \leq G_n = G$$

tal que cada fator G_{i+1}/G_i é cíclico, $i = 0, \ldots, n-1$.

Demonstração: v. ROCCO [13]. ■

Corolário 1.3.13: Se G é nilpotente finitamente gerado, então todo subgrupo de G é finitamente gerado.

Demonstração: v. ROCCO [13]. ■

Teorema 1.3.14: Seja G nilpotente, gerado pelo conjunto junto $\{x_1, \ldots, x_r\}$. Se cada x_i tem ordem finita m_i, então G é finito e $|G|$ divide alguma potência de $m = m_1 \ldots m_r$.

Demonstração: v. ROCCO [13]. ■

Definição 1.3.15: Seja G um grupo e $H \leq G$. Dizemos que H *é subnormal em* G se existe uma cadeia:

$$H = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_m = G, \quad \text{ligando} \quad H \quad \text{e} \quad G. \qquad \square$$

Encerrando esta seção damos algumas caracterizações dos grupos nilpotentes finitos.

Teorema 1.3.16: *Seja G um grupo finito. Então são equivalentes:*

(i) *G é nilpotente*

(ii) *todo subgrupo de G é subnormal em G.*

(iii) *G satisfaz a condição do normalizador, i.e., todo subgrupo próprio de G está propriamente contido em seu normalizador em G. ($H \leq N_G(H)$).*

(iv) *Todo subgrupo maximal é normal*

(v) *G é um produto direto de seus subgrupos de Sylow.*

Demonstração: v. ROCCO [13]. ■

1.4 Série p-Central Inferior

Definição 1.4.1: Seja p um número primo. A série $G = P_0(G) \geq P_1(G) \geq \ldots \geq P_i(G) \geq \ldots$; onde cada $P_{j+1}(G) = P_j(G)^p[P_j(G), G]$ e $G^p =< g^p / g \in G >$ é denominada *série p-central inferior de G.*

Se $P_{k-1}(G) \neq \{1\}$ e $P_k(G) = \{1\}$ então dizemos que G tem *p-classe k.* □

Observação 1.4.1 (1): *Se G tem p-classe k, então G é nilpotente e $cl G \leq k$. (De fato, $\gamma_1(G) = G' \leq P_1(G)$ e indutivamente $\gamma_i(G) = [\gamma_{i-1}(G), G] \leq [P_{i-1}(G), G] \leq P_i(G)$, assim se $P_k(G) = \{1\}$, então $\gamma_k(G) = \{1\}$).* □

A proposição que segue justifica o termo p-central utilizado na definição anterior.

Proposição 1.4.2: *Se $G = P_0(G) \geq P_1(G) \geq P_2(G) \geq \ldots \geq P_i(G) \geq \ldots$ é a série p-central inferior de G, então, para cada $i = 1, 2, \ldots$, temos*

1) $P_i(G) \trianglelefteq G$

2) $P_i(G)/P_{i+1}(G) \leq Z(G/P_{i+1}(G))$

3) $P_i(G)/P_{i+1}(G)$ *tem expoente* p.

Demonstração:

1) Segue por indução sobre i

2) Segue da definição de $P_{i+1}(G)$

3) Se $a \in P_i(G)/P_{i+1}(G)$, então $a = gP_{i+1}(G)$ para algum $g \in P_i(G)$, logo $a^p = a^p P_{i+1}(G) = P_{i+1}(G)$ pela definição de $P_{i+1}(G)$ ∎

A continuação daremos algumas propriedades importantes da série p-central inferior de um grupo G que usaremos freqüentemente no capítulo 3.

Propriedade 1.4.3: *Dado* $c \in N$, *se* $P_c(G) = P_{c+1}(G)$, *então* $P_{c+1}(G) = P_{c+2}(G)$. (Segue-se da definição). ∎

Propriedade 1.4.4: *Se* G *é finitamente gerado, então* $G/P_i(G)$ *é um p-grupo finito,* $\forall i$. (Faça indução sobre i e note que, para cada i, tem-se que $P_i(G)/P_{i+1}(G)$ é abeliano elementar finitamente gerado e portanto um p-grupo finito). ∎

Propriedade 1.4.5: *Se* θ *é um homomorfismo de* G, *então* $(P_i(G))\theta = P_i(G\theta)$. (Segue da definição da série p-central inferior para $G\theta$). ∎

Propriedade 1.4.6: *Cada termo* $P_i(G)$ *da série p-central inferior de* G *é totalmente invariante* em G. (Faça indução sobre i e use o resultado anterior). ∎

Propriedade 1.4.7: *Se* $N \trianglelefteq G$ *e o quociente* G/N *tem p-classe* c, *então* $P_c(G) \leq N$. (Segue da propriedade 1.4.5). ∎

Propriedade 1.4.8: *Se G/N tem p-classe c, então $P_c(G) \leq N$ e $P_{c-1}(G) \nleq N$.* (Segue da definição da p-classe e da propriedade 1.4.5). ■

Propriedade 1.4.9: $[P_i(G), P_j(G)] \leq P_{i+j+1}(G)$ *para* $i, j = 0, 1, \ldots$. (Segue por indução). ■

1.5 Subgrupo de Frattini

Definição 1.5.1: Seja G um grupo arbitrário. Definimos o subgrupo $\phi(G)$, chamado *subgrupo de Frattini de* G, da seguinte forma:

$$\phi(G) = G \bigcap_{\substack{M<G \\ \max}} M$$

□

Observação 1.5.1 (1): *Segue da definição que $\phi(G) = G$ se, e somente se, G não tem subgrupos maximais.* □

Observação 1.5.1 (2): *$\phi(G)$ é um subgrupo característico (i.e., invariante por qualquer automorfismo de G), já que todo automorfismo de G age como uma permutação no conjunto dos subgrupos maximais de G.* □

O subgrupo de Frattini de G, tem uma relação interessante com a geração de G. $\phi(G)$ consiste dos elementos de G que são "supérfluos" na geração de G no seguinte sentido:

Definição 1.5.2: Um elemento $x \in G$ é dito supérfluo na geração de G, se $\forall T \subseteq G$ tal que $< T, x >= G$ tem-se também que $< T >= G$. □

Note que se $G \neq \{1\}$, certamente 1 é supérfluo na geração de G.

O resultado que antecipamos é então o seguinte.

Teorema 1.5.3: *Seja $G \neq \{1\}$, logo $\phi(G)$ é o conjunto dos elementos supérfluos na geração de G.*

Demonstração: v. HALL [3]. ■

A continuação daremos outras propriedades de $\phi(G)$.

Teorema 1.5.4: *O subgrupo de Frattini de um grupo finito é nilpotente.*

Demonstração: v. HALL [3]. ■

Teorema 1.5.5: *O subgrupo de Frattini de um grupo nilpotente G contém o grupo derivado, G'.*

Demonstração: v. HALL [3]. ■

Teorema 1.5.6 (Wielandt): *Se o subgrupo de Frattini de um grupo finito G, contém o grupo derivado G', então G é nilpotente.*

Demonstração: v. HALL [3]. ■

Observação: *Conclui-se então, dos teoremas* 1.4.5 *e* 1.4.6 *que: Se G é finito, então G é nilpotente se, e somente se $G' \leq \phi(G)$.* □

Proposição 1.5.7: *Se G é um p-grupo finito, então $\phi(G) = P_1(G) = G^p G'$.*

Demonstração: É claro que $P_1(G) \leq \phi(G)$, desde que M é maximal em G e G é um p-grupo finito, então segue da proposição 1.2.3 (iv) que $[G : M] = p$ e assim, se $g \in G$ temos que $g^p M = (gM)^p = M$ e portanto $g^p \in M \ \ \forall\, g \in G$. Analogamente $[gM, g'M] = M$ (pois G/M é cíclico) e logo $[g, g'] \in M \ \forall g, g' \in M$.

Reciprocamente, vejamos agora que $\phi(G) \leq P_1(G)$. Suponhamos que existe $x \in (\phi(G) - P_1(G))$, logo $\overline{x} = xP_1(G)$ é um elemento não trivial de $V = G/P_1(G)$ que é um

espaço vetorial sobre $\mathbb{F}_p$, portanto, $\overline{x}$ é parte de uma base para V.

Agora note que se $\{\overline{a}_1, \ldots, \overline{a}_d\}$ é uma base para $V = G/P_1(G)$ (onde cada $\overline{a}_i = a_i P_1(G)$), então $G =< a_1, \ldots, a_d, P_1(G) >$ e como $P_1(G) \leq \phi(G)$, temos pelo teorema 1.5.3 que $G =< a_1, \ldots, a_d >$ e é claro que d é o número mínimo de geradores para G.

Assim, tínhamos que $\overline{x}$ é parte de uma base para V, logo, pela observação acima x é um gerador essencial para G contradizendo o fato $x \in \phi(G)$. Conseqüentemente, $\phi(G) \leq P_1(G)$. ∎

Teorema 1.5.8 (Teorema da base de Burnside para p-grupos finitos): *Seja $|G| = p^n, n \in \mathbb{N}$. Seja $\phi = \phi(G)$ o grupo de Frattini de G. O quociente $A := G/\phi$ é um grupo abeliano elementar. Se $|A| = p^r$, então todo conjunto de elementos $z_1, \ldots, z_r$ que gera G contém um subconjunto de r elementos $x_1, \ldots, x_r$ que gera G.*

A aplicação natural $G \twoheadrightarrow A$ leva os elementos $x_1, \ldots, x_r$ numa base $a_1, \ldots, a_r$ de A e reciprocamente, todo conjunto de r elementos de G que é levado pela aplicação acima num conjunto de geradores de A, gera G.

Demonstração: Pela proposição 1.5.7, sabemos que $\phi = P_1(G) = G^p G'$, logo é claro que $A = G/\phi$ é abeliano elementar. Se $|A| = p^r$ então toda base de A (como $\mathbb{Z}_p$-espaço vetorial) consiste de r elementos, digamos $a_1, \ldots, a_r$. Se $b_1, \ldots, b_s$ geram A, podemos obter uma base para A tirando os b_i's que pertencem ao subgrupo gerado por $b_1, \ldots, b_{i-1}$.

Sejam agora $z_1, \ldots, z_s$ geradores de G. Na aplicação natural $G \twoheadrightarrow A = G/\phi$, seja b_i a imagem de z_i para $i = 1, \ldots, s$. Logo, $b_1, \ldots, b_s$ geram A e portanto um subconjunto $\{a_1, \ldots, a_r\} \subset \{b_1, \ldots, b_s\}$ é uma base para A.

Seja $\{x_1, \ldots, x_r\}$ o subconjunto de $\{z_1, \ldots z_s\}$ tal que a_i é a imagem de x_i, para $i = 1, \ldots, r$. Queremos provar então que $x_1, \ldots, x_r$ geram G.

Seja $H =< x_1, \ldots, x_r >$.

Se $H \neq G$, então H está contido num subgrupo maximal de G, digamos $H \leq M \overset{<}{_{\max}} G$.

Mas considerando novamente a aplicação natural $G \twoheadrightarrow A = G/\phi$, temos que H é levado em $\frac{H\phi}{\phi} \leq M/\phi = B$, onde B é um subgrupo de A de ordem p^{r-1} (já que $M \overset{<}{_{\max}} G \Rightarrow [G : M] = p$, logo $|G| = |M| \cdot p$ e em conseqüência $|\frac{G}{\phi}| = |\frac{M}{\phi}| \cdot p$). O que

contradiz o fato

$$H =< x_1, \ldots, x_r > \rightarrow < a_1, \ldots, a_r >= A.$$

Portanto, $H = G$ e $x_1, \ldots, x_r$ geram G. ■

1.6 Grupo de automorfismos de um grupo

Definição 1.6.1: O *grupo de automorfismos de um grupo* G, denotado $\mathrm{Aut}(G)$, é o conjunto de todos os automorfismos de G sob a operação de composição. ($\mathrm{Aut}(G) \leq S_G$). □

Definição 1.6.2: Um automorfismo α de G é dito *interno* se é a conjugação por um elemento de G, i.e., $\alpha(x) = \gamma_a(x) = a^{-1}xa$ para algum $a \in G$. Em outro caso, dizemos que α é *externo*. □

Teorema 1.6.3:

1) *Se* $H \leq G$, *então* $C_G(H) \trianglelefteq N_G(H)$ *e* $N_G(H)/C_G(H)$ *é isomorfo a um subgrupo de* $\mathrm{Aut}(H)$. *(Aqui* $(C_G(H) = \{g \in G / g^{-1}hg = h, h \in H\})$.

2) *O conjunto de todos os automorfismos interiores de* G, *denotado* $I_{nn}(G)$, *é um subgrupo normal de* $\mathrm{Aut}(G)$ *e* $G/Z(G) \cong I_{nn}(G)$.

Demonstração: v. ROTMAN [14]. ■

Teorema 1.6.4:

$$\mathrm{Aut}(\mathbb{Z}_{2^m}) \cong \begin{cases} \{1\} & se \quad m = 1 \\ \mathbb{Z}_2 & se \quad m = 2 \\ \mathbb{Z}_2 \times \mathbb{Z}_{2^{m-2}} & se \quad m \geq 3 \end{cases}$$

Se p *é um primo ímpar*

$$\mathrm{Aut}(\mathbb{Z}_{p^n}) \cong \mathbb{Z}_{(p-1)p^{n-1}}$$

Demonstração: v. ROTMAN [14]. ■

Definição 1.6.4: Um grupo G é *completo* se $Z(G) = \{1\}$ e todo automorfismo de G é interno. □

Note que se G é um grupo completo, então $\mathrm{Aut}(G) \cong G$ (segue do Teorema 1.6.3).

Teorema 1.6.5: *S_n (o grupo simétrico) é completo se $n \neq 2$ e $n \neq 6$.*

Demonstração: v. ROTMAN [14]. ■

Corolário 1.6.6: $\mathrm{Aut}(S_n) \cong S_n$ *para* $n \neq 2$ *e* $n \neq 6$.

Demonstração: Segue-se da definição 1.6.4 e do teorema 1.6.5. ■

Teorema 1.6.7: $\mathrm{Aut}(S_6)/I_{nn}(S_6) \cong \mathbb{Z}_2$.

Demonstração: v. ROTMAN [14]. ■

Teorema 1.6.8: *Se $H \trianglelefteq G$ e H é um grupo completo, então H é um fator direto de G, i.e., existe um subgrupo normal K de G tal que $G = H \times K$.*

Demonstração: v. ROTMAN [14]. ■

A continuação daremos uma lista de resultados que serão úteis na hora de fazer alguns cálculos com o algoritmo de geração de p-grupos.

Lema 1.6.9:

1) *Se V é o grupo de Kleim ($V \cong C_2 \times C_2$), então* $\mathrm{Aut}(V) \cong S_3$.

2) *Se G é um grupo abeliano elementar de ordem p^n, com p primo, então* $\mathrm{Aut}(G) \cong GL(n, p)$.

3) *Se H e K são grupos finitos cuja ordens são relativamente primos, então* $\mathrm{Aut}(H \times K) \cong \mathrm{Aut}(H) \times \mathrm{Aut}(K)$.

4) $\mathrm{Aut}(Q_8) \cong S_4$, *onde* Q_8 *é o grupo dos quatérnios, de ordem* 8.

5) *Se* G *é um grupo abeliano finito com mais de dois elementos, então* $\mathrm{Aut}(G)$ *não pode ter ordem ímpar. (Se* $x \mapsto x^{-1}$ *é a identidade, então* G *é abeliano elementar de ordem* 2^m *e* $\mathrm{Aut}(G) \cong GL(n,2)$*).*

6) *Se* G *é não abeliano, então* $\mathrm{Aut}(G)$ *não é cíclico. (*$I_{nn}(G)$ *não é cíclico).*

Observação: *De* 5) *e* 6) *conclui-se que um grupo cíclico de ordem ímpar, não é* $\mathrm{Aut}(G)$ *para nenhum grupo finito* G. □

1.7 Cálculo do estabilizador de um ponto num grupo de permutações

Seja X um conjunto finito não vazio e $G \leq S_X$ um grupo de permutações sobre X.

Definição 1.7.1:

a) Definamos a seguinte relação sobre os elementos de X:
Se $x, y \in X$, $x \sim_G y$ se e somente se $\exists g \in G$ tal que $y = x^g$. É claro que $\sim_G$ é uma relação de equivalência. A classe de equivalência de um ponto $x \in X$ é dita a *G-órbita de* x.

b) Dado X_0 um subconjunto não vazio de X, definimos o *estabilizador de* X_0 e denotamos $\mathrm{Stab}_G(X_0)$ ao seguinte conjunto

$$\mathrm{Stab}_G(X_0) = \{g \in G / x^g = x,\ \forall x \in X_0\}.$$

c) Em particular, se $X_0 = \{x\}$ definimos o *estabilizador do ponto* x e denotamos $\mathrm{Stab}_G(x)$ ao conjunto

$$\mathrm{Stab}_G(x) = \{g \in G / x^g = x\}.$$

Proposição 1.7.2: $\mathrm{Stab}_G(X_0) \leq G$ *para qualquer subconjunto não vazio de* G.

Demonstração: Imediata. ■

Proposição 1.7.3: *Se $G \leq S_X$ e $x \in X$, então* $|\mathrm{Orb}(x)| = [G : \mathrm{Stab}_G(x)]$.

O objeto desta seção é dar um algoritmo para o cálculo de estabilizador de um ponto num grupo de permutações. Para isso será importante estudarmos em detalhe o seguinte teorema:

Teorema 1.7.4 (Schreier): *Sejam G um grupo finitamente gerado e $H \leq G$ um subgrupo de índice finito. Então H é finitamente gerado.*

Demonstração: Sejam $G =< S >, S = \{s_1, \ldots, s_r\}$ e $[G : H] = n$.
Seja agora $T = \{t_1, t_2, \ldots, t_n\}$ um tranversal à direita para H em G (i.e., um conjunto completo e irredundante de representantes das classes laterais à direita de H em G). Logo, $Y = \{H, Ht_2, \ldots, Ht_n\}$ é o conjunto das classes laterais à direita. Temos então que G age sobre Y da seguinte forma: $(Ht_i)g = H(t_i g) = Ht_j$ fornecendo uma permutação de Y e consequentemente de $\{1, \ldots, n\}$ tal que $j = (i)g$.

Assim, $Ht_i g = Ht_{(i)g}$ para $i \in \{1, \ldots, n\}$ e $g \in G$ e portanto, dado $g \in G$, temos

$$t_i g = h(t_i, g)t_{(i)g} \quad \text{onde} \quad h(t_i, g) \in H \tag{1}$$

Seja então $a \in H$. Como elemento de G temos que a é um produto de elementos de $S \cup S^{-1}$, i.e.:

$$a = u_1 \ldots u_k \quad \text{com} \quad u_i \in S \cup S^{-1},\ k \geq 0.$$

Portanto

$$\begin{aligned}
a &= 1_d \cdot a = 1_d \cdot u_1 \ldots u_k = (t_1 u_1)u_2 \ldots u_k \\
&= (h(t_1, u_1)t_{(1)u_1})u_2 \ldots u_k && \text{por (1)} \\
&= h(t_1, u_1)(t_{(1)u_1} \cdot u_2)u_3 \ldots u_k \\
&= h(t_1, u_1)h(t_{(1)u_1}, u_2)(t_{(1)u_1 u_2}u_3)u_4 \ldots u_k \\
&= \ldots\ldots \\
&= h(t_1, u_1)h(t_{(1)u_1}, u_2) \ldots h(t_{(1)u_1 \ldots u_{k-1}}, u_k)t_{(1)u_1, u_2 \ldots u_k} \\
&= h(t_1, u_1)h(t_{(1)u_1}, u_2) \ldots h(t_{(1)u_1 \ldots u_{k-1}}, u_k)t_{(1)a}
\end{aligned}$$

Como $a \in H$ e $h(t,u_1),\ldots,h(t_{(1)u_1\ldots u_{k-1}},u_k) \in H$, temos que $t_{(1)a} = t_1 = 1_d$ e portanto

$$a = h(t_1,u_1)h(t_{(1)u_1},u_2)\ldots h(t_{(1)u_1\ldots u_{k-1}},u_k)$$

Logo H e gerado pelos elementos de forma $h(t_i,u)$, com $1 \leq i \leq n$, $u \in S \cup S^{-1}$. Segue-se entao que H e finitamente gerado. ■

Observação 1.7.4 (1): *O conjunto* $Z = \{h(t,u)/t \in T, u \in S \cup S^{-1}\}$ *é chamado conjunto de* geradores de Schreier *para* H. □

Observação 1.7.4 (2): *Denotemos* $\overline{g}$ *o representante da classe* H_g. Assim $t_i g = h(t_i,g)t_{(i)g}$ e portanto $\overline{t_i g} = t_{(i)g}$. Logo $t_i g \cdot \overline{t_i g}^{-1} = h(t_i,g)$.

Temos então $Z = \{t\overline{tu}^{-1}/t \in T,\ u \in S \cup S^{-1}\}$. □

Seja agora $G \leq S_X$ onde $X = \{1,\ldots,n\}$ e $G =< S >=< \tau_1,\ldots,\tau_r >$. É claro então que para construir $H = \mathrm{Stab}_G(1)$ é suficiente construir um conjunto de geradores de Schreier para H. Para seguir os passos do teorema, é preciso construir primeiro um transversal para H em G. Para isso, proceda da seguinte maneira:

ALGORITMO 1.7.5:

Passo 1: Aplique cada gerador de G, τ_j, ao ponto 1, marcando os novos elementos que aparecem pela primeira vez.

Passo 2: Aplique cada gerador τ_j aos novos pontos assim obtidos até que nenhum ponto novo ocorra.

Observação 1.7.5 (1): *Desta maneira temos calculado a órbita do elemento 1 e temos então a informação sobre a cardinalidade do transversal* T *que procuramos, já que* $|T| = |\mathrm{Orb}_G(1)|$ *pela proposição* 1.7.3.

Passo 3: Agora observe que se $1g = j$, tem-se $\overline{g} = t_j$, de modo que para encontrar o representante $t_j \in T$, basta olhar para o traço do elemento j, rastreando sua imagem a

partir do ponto 1.

Exemplo: Sejam $X = \{1,2,3,4\}$; $G = S_4 =< S >$ onde $S = \{\tau_1 = (12); (1231)\}$. Seja $H = \text{Stab}_G(1)$. Procuremos um transversal para H em G.

Executando o algoritmo 1.7.5, temos:

$$\begin{array}{llll} 1\tau_1 = \underline{2}\ ; & 2\tau_1 = 1\ ; & 3\tau_1 = 3\ ; & 4\tau_1 = 4 \\ 1\tau_2 = 1\ ; & 2\tau_2 = \underline{3}\ ; & 3\tau_2 = \underline{4}\ ; & 4\tau_2 = 1 \end{array}$$

Portanto: $\text{Orb}_G(1) = \{1,2,3,4\}$ e $|T| = 4$, i.e., $T = \{t_1, t_2, t_3, t_4\}$ onde t_1 é um representante da classe trivial e portanto será sempre escolhido sendo a identidade, $t_1 = id_G$. Para calcular os representantes restantes, calculemos os traços dos elementos 2, 3 e 4 a partir do ponto 1:

$$\begin{array}{lll} 2 = 1\tau_1\ , & \text{logo} & t_2 = \tau_1 \\ 3 = 2\tau_2 = 1\tau_1\tau_2\ , & \text{logo} & t_3 = \tau_1\tau_2 \\ 4 = 3\tau_2 = 2\tau_2\tau_2 = 1\tau_1\tau_2^2\ , & \text{logo} & t_4 = \tau_1\tau_2^2 \end{array}$$

Portanto $T = \{t_1 = id_G;\ t_2 = \tau_1;\ t_3 = \tau_1\tau_2;\ t_4 = \tau_1\tau_2^2\}$. ■

Uma vez obtido o transversal para H em G, proceda da seguinte maneira para obter um conjunto de geradores de Schreier para H:

ALGORITMO 1.7.6:

Passo 1: Para cada $t_i \in T$ e cada $\tau_j \in S \cup S^{-1}$ calcule $g_{ij} = t_i\tau_j$;

Passo 2: Se $(1)g_{ij} = k$, faça $\overline{g_{ij}} = t_k$;

Passo 3: Calcule $s_{ij} = g_{ij}\overline{g_{wij}}^{-1}$ que é um gerador de Schreier. Logo construa o conjunto de geradores de Schreier para H:

$$Z = \left\{ s_{ij}/u \in \{1,\ldots,|\text{Orb}(1)|\};\ j \in \{1,\ldots r\} \right\}.$$

Voltando ao exemplo acima, tínhamos

$$T = \{t_1 = id_G,\ t_2 = \tau_1,\ t_3 = \tau_1\tau_2,\ t_4 = \tau_1\tau_2^2\} = \{id_G, (12), (134), (1432)\}.$$

Assim

$g_{11} = t_1\tau_1 = \tau_1$; $(1)g_{11} = 2$, logo $\overline{g_{11}} = \tau_1$ e portanto $s_{11} = \tau_1\tau_1 = id_G$

$g_{12} = t_1\tau_2 = \tau_2$; $(1)g_{12} = 2$, logo $\overline{g_{12}} = \tau_1$ e portanto $s_{12} = \tau_2\tau_1 = (234)$

$g_{13} = t_1\tau_2^{-1} = \tau_2^{-1}$; $(1)g_{13} = 4$, logo $\overline{g_{13}} = \tau_1\tau_2^2$ e portanto $s_{13} = \tau_2^{-3}\tau_1 = \tau_2\tau_1 = (234)$

$g_{21} = t_2\tau_1 = id_G$; $(1)g_{21} = 1$, logo $\overline{g_{21}} = id_G$ e portanto $s_{21} = id_G$

$g_{22} = t_2\tau_2 = \tau_1\tau_2$; $(1)g_{22} = 3$, logo $\overline{g_{22}} = \tau_1\tau_2$ e portanto $s_{22} = id_G$

$g_{23} = t_2\tau_2^{-1} = \tau_1\tau_2^{-1}$; $(1)g_{23} = 1$, logo $\overline{g_{23}} = id_G$ e portanto $s_{23} = \tau_1\tau_2^{-1} = s_{12}^{-1} = (432)$

$g_{31} = t_3\tau_1 = \tau_1\tau_2\tau_1$; $(1)g_{31} = 3$, logo $\overline{g_{31}} = \tau_1\tau_2$ e portanto $s_{31} = \tau_1\tau_2\tau_1\tau_2^{-1}\tau_1 = (24)$

$g_{32} = t_3\tau_2 = \tau_1\tau_2^2$; $(1)g_{32} = 4$, logo $\overline{g_{32}} = \tau_1\tau_2^2$ e portanto $s_{32} = id_G$

$g_{33} = t_3\tau_3 = \tau_1$; $(1)g_{33} = 2$, logo $\overline{g_{33}} = \tau_1$ e portanto $s_{33} = id_G$

$g_{41} = t_4\tau_1 = \tau_1\tau_2^2\tau_1$; $(1)g_{41} = 4$, logo $\overline{g_{41}} = \tau_1\tau_2^2$ e portanto $s_{41} = \tau_1\tau_2^2\tau_1(\tau_1\tau_2^2)^{-1} = (34)$

$g_{42} = t_4\tau_2 = \tau_1\tau_2^3$; $(1)g_{42} = 1$, logo $\overline{g_{42}} = id_G$ e portanto $s_{42} = \tau_1\tau_2^3 = (432)$

$g_{43} = t_4\tau_2^{-1} = \tau_1\tau_2$; $(1)g_{43} = 3$, logo $\overline{g_{43}} = \tau_1\tau_2$ e portanto $s_{43} = id_G$

Assim $Z = \{id_G, (234), (34), (432)\}$ e como $(432) = (234)^{-1}$ e $(24) = (234)(24)$, temos então

$$H = \mathrm{Stab}_G(1) = < (34); (234) > .$$

■

Capítulo 2

Algoritmo do quociente nilpotente

Nosso objetivo neste capítulo é descrever um algoritmo que, partindo de uma apresentação abstrata finita de um grupo, dê como resultado uma apresentação por potências e comutadores do maior quociente nilpotente finito deste grupo.

O algoritmo do quociente nilpotente, NQA, constitui-se essencialmente por um conjunto de rotinas para manipular apresentações por potências e comutadores.

Dado um grupo G finitamente apresentado e um primo p, o NQA constrói uma apresentação consistente por potências e comutadores para o maior p-quociente finito de G. Desta forma, o NQA determina o p-subgrupo de Sylow do maior quociente nilpotente finito de G.

Note que se o grupo dado, G, for nilpotente finito, o NQA constrói uma apresentação consistente por potências e comutadores para G a partir de uma apresentação finita qualquer.

2.1 Apresentações por potências e comutadores

Definição 2.1.1: Uma apresentação por potências e comutadores para um grupo G consiste de um conjunto finito $A = \{a_1, a_2, \ldots, a_n\}$ de geradores e um conjunto de $\frac{n(n+1)}{2}$

relações:

$$a_i^p = \prod_{l=i+1}^{n} a_l^{\alpha(i,l)} \ , 1 \leq i \leq n-1 \quad \text{e} \quad a_n^p = e$$

$$[a_j, a_i] = \prod_{l=j+1}^{n} a_l^{\beta(i,j,l)} \ , 1 \leq i < j \leq n-1 \quad \text{e} \quad [a_n, a_i] = e \ , 1 \leq i \leq n-1$$

onde p é um primo e $\alpha(i,l), \beta(i,j,l)$ variam em $\{0, 1, \ldots, p-1\}$. □

Proposição 2.1.2: *Todo p-grupo finito tem uma apresentação por potências e comutadores.*

Demonstração: Seja G um p-grupo finito de ordem p^n, logo existe uma série central

$$\{e\} = H_{n+1} \leq H_n \leq H_{n-1} \leq \ldots \leq H_1 = G$$

tal que H_i/H_{i+1} é cíclico de ordem p, $\forall\, i \in \{1, \ldots, n\}$ (proposição 1.3.12).

Assim, temos

$$H_n/H_{n+1} = H_n =< a_n \ / \ a_n^p = e > \overset{(1)}{\leq} Z(G)$$

e

$$H_{n-1}/H_n =< a_{n-1} \ / \ a_{n-1}^p = e > \overset{(2)}{\leq} Z(G/H_n)$$

conseqüentemente

$$H_{n-1} =< a_{n-1}, a_n \ / \ a_{n-1}^p = a_n^{\alpha(n-1,n)}, a_n^p = e, [a_n, a_{n-1}] \overset{(1)}{=} e > \ .$$

Analogamente

$$\begin{aligned} H_{n-2} =< a_{n-2}, a_{n-1}, a_n \quad / \quad & a_{n-2}^p = a_{n-1}^{\alpha(n-2,n-1)} a_n^{\alpha(n-2,n)}, a_{n-1}^p = a_n^{\alpha(n-1,n)} \ , \\ & a_n^p = e \ , [a_n, a_{n-1}] = [a_n, a_{n-2}] = e \ , \\ & [a_{n-1}, a_{n-2}] \overset{(2)}{=} a_n^{\alpha(n-1,n-2,n)} > \end{aligned}$$

e para $k \in \{1, 2, \ldots, n\}$ temos

$$\begin{aligned} H_k = \langle a_k, a_{k+1}, \ldots, a_{n-1}, a_n \quad / \quad & a_i^p = a_{i+1}^{\alpha(i,i+1)} a_{i+2}^{\alpha(i,i+1)} \ldots a_n^{\alpha(i,n)} \ , \\ & k \leq i \leq n-1 \ , 0 \leq \alpha(i,j) < p \ a_n^p = e \\ & [a_j, a_i] = a_{j+1}^{\alpha(i,j,i+1)} a_{j+2}^{\alpha(i,j,i+2)} \ldots a_n^{\alpha(i,j,n)} \ , \\ & k \leq i < j \leq n-1 \ , 0 \leq \alpha(i,j,l) < p \\ & [a_n, a_j] = e \ , k \leq j \leq n \ .\rangle \end{aligned}$$

Obtemos assim a seguinte apresentação por potências e comutadores para o p-grupo G:

$$G = H_1 = \langle a_1, a_2, \ldots, a_{n-1}, a_n \ / \ a_i^p = \prod_{l=i+1}^{n} a_l^{\alpha(i,l)} \ , 1 \leq i \leq n-1 \ , 0 \leq \alpha(i,j) < p \ ,$$
$$a_n^p = e \ , [a_j, a_i] = \prod_{l=j+1}^{n} a_l^{\alpha(i,j,l)} \ ,$$
$$1 \leq j < i \leq n-1 \ , 0 \leq \alpha(i,j,l) < p \ ,$$
$$[a_n, a_j] = e \ , 1 \leq j \leq n \ .\rangle$$

■

Observação 2.1.3: *Seja agora G um grupo finito com a seguinte apresentação por potências e comutadores:*

$$\begin{cases} \textit{geradores} : & a_1, a_2, \ldots, a_n \\ \textit{relações}: & a_i^p = \prod_{l=i+1}^{n} a_l^{\alpha(i,l)} \ , 1 \leq i \leq n-1 \ \ e \ \ a_n^p = e \\ & [a_j, a_i] = \prod_{l=j+1}^{n} a_l^{\alpha(j,i,l)} \ , 1 \leq i < j \leq n-1 \\ & [a_n, a_i] = e \ , 1 \leq i \leq n \end{cases} \tag{2.1.4}$$

onde $0 \leq \alpha(i,l), \alpha(j,i,l) < p$.

Seja $A_i =< a_i, a_{i+1}, \ldots, a_n >$, $1 \leq i \leq n$. Observe que $A_i \trianglelefteq G$ e que, por indução inversa sobre i, qualquer elemento de A_i pode ser expresso na forma normal:

$$a_i^{\beta_i} a_{i+1}^{\beta_{i+1}} \ldots a_n^{\beta_n} \ \ onde \ \ 0 \leq \beta_j < p$$

para cada i temos um quociente $A_i/A_{i+1} =< a_i A_{i+1} >$, onde $a_i^p \in A_{i+1}$ e assim

$$|A_i/A_{i+1}| = 1 \quad ou \quad |A_i/A_{i+1}| = p$$

logo, temos que G é um p-grupo e $|G| \leq p^n$. □

Definição 2.1.5: A apresentação (2.1.4) será dita *consistente* se $|G| = p^n$. □

Observação 2.1.6: *Como o NQA tem por objetivo o cálculo de apresentações consistentes por potências e comutadores, será importante, no que segue, estabelecer um critério de consistência para tais apresentações.* □

2.2 Consistência

Seja p um primo e G um p-grupo finito, d-gerado (i.e $\dim_{F_p} \frac{G}{G^p G'} = d$), de ordem no máximo p^n. Seja P a seguinte apresentação de G por potências e comutadores:

$$P : \begin{cases} \text{geradores} : & a_1, a_2, \ldots, a_n \\ \text{relações} : & a_i^p = \prod_{l=i+1}^{n} a_l^{\alpha(i,l)} \ , 1 \leq i \leq n-1 \ \text{ e } \ a_n^p = e \\ & [a_j, a_i] = \prod_{l=j+1}^{n} a_l^{\alpha(j,i,l)} \ , 1 \leq i < j \leq n-1 \\ & [a_n, a_i] = e \ , 1 \leq i \leq n \end{cases}$$

com $0 \leq \alpha(i,l), \alpha(j,i,l) < p$.

Seja $W = \{a_1^{\alpha(1)} a_2^{\alpha(2)} \ldots a_n^{\alpha(n)} \ ; \ 0 \leq \alpha(i) < p, 1 \leq i \leq n\}$.

Definição 2.2.1: Os elementos de W são chamados *palavras normais* nos geradores de G. □

Definição 2.2.2: Processo de Coleta Toda palavra nos geradores de G pode ser transformada numa palavra normal usando o processo de coleta que descrevemos a seguir.

Seja ω uma palavra nos geradores $a_1, \ldots, a_n$. Então

1 - Se w é normal, pare.

2 - Caso contrário, w contém no mínimo uma subpalavra não normal minimal, digamos u, que é da forma a_i^p ou $a_j a_i$ com $j > i$. Substitua então u usando a relação correspondente em P, obtendo assim uma nova palavra w', nos geradores $a_1, \ldots, a_n$.

3 - Faça $w = w'$ e volte a 1. □

Observação 2.2.3: *É claro que este processo termina numa palavra normal após um número finito de passos.* □

Observação 2.2.4: *O processo descrito no ponto 2 é referido como* coleta *de* u.

Se em algum estágio do processo tivermos mais de uma subpalavra não normal minimal a coletar, pode-se começar por coletar qualquer subpalavra não normal minimal ou decidir então coletar sempre o menor índice não coletado, da direita para a esquerda. Este processo é conhecido como o processo de coleta à direita. *Analogamente pode ser definido um* processo de coleta à esquerda. □

Um critério para a consistência da apresentação P

Sendo W o conjunto das palavras normais nos geradores $a_1, \ldots, a_n$ da apresentação P, i.e. $W = \{a_1^{\alpha(1)} \ldots a_n^{\alpha(n)}, 0 \leq \alpha(i) \leq p\}$, temos que $|W| = p^n$.

Como toda palavra nos geradores $a_1, \ldots, a_n$ pode ser transformada numa palavra normal usando o processo de coleta descrito acima, definimos o produto $u.v$ dos elementos $u, v \in W$ como sendo a palavra normal obtida de uv pelo processo de coleta. Este produto torna W um *grupoide* com identidade 1 (a palavra vazia), de ordem p^n.

Se W é um grupo, então $W \cong G$, G tem ordem p^n e P é consistente. Logo, um critério de consistência é obtido a partir de um critério para estabelecer a associatividade da operação $\cdot$ definida acima. Um critério para tal associatividade está dado no seguinte teorema:

Teorema 2.2.5: *A operação $\cdot$ definida acima é associativa se se verificam as seguintes identidades*

$$\begin{aligned}
&(a_i.a_j).a_k = a_i.(a_j.a_k) \quad para \quad 1 \leq k < j < i \leq n \\
&(a_j^{p-1}.a_j).a_k = a_j^{p-1}.(a_j.a_k) \quad para \quad 1 \leq k < j \leq n \\
&(a_i.a_j).a_j^{p-1} = a_i.(a_j.a_j^{p-1}) \quad para \quad 1 \leq j < i \leq n \\
&(a_i.a_i^{p-1}).a_i = a_i.(a_i^{p-1}.a_i) \quad para \quad 1 \leq i \leq n
\end{aligned} \tag{2.2.6}$$

Mais ainda, as identidades acima com $k \leq d$ são suficientes para garantir a associatividade de W.

Observação 2.2.7: *As identidades* (2.2.6) *são chamadas condições ou testes de associatividade de Wamsley, pois foi ele o primeiro a provar que elas implicam que W é associativo* (v. WAMSLEY [14]).

A demonstração que daremos aqui é diferente, baseada na demonstração de Vaughan-Lee em VAUGHAUN-LEE [9]. □

Observação 2.2.8: *Antes de entrarmos na demonstração do teorema, discutiremos um detalhe sobre o processo de coleta. O* output *do processo de coleta é uma seqüência finita $w_1, w_2, \ldots, w_r$ de palavras nos geradores, que termina com a palavra normal w_r. Se P é consistente e W um grupo, então podemos identificar a palavra $a_i a_j \ldots a_k$ com o produto $a_i.a_j.\ldots.a_k$ no grupo, e assim, temos que $w_1, w_2, \ldots, w_r$ são expressões diferentes para o mesmo elemento de W.* □

Demonstração: Para $r = 1, 2, \ldots, n$, seja W_r o subgrupóide consistindo das palavras normais da forma

$$a_r^{\alpha(r)} a_{r+1}^{\alpha(r+1)} \ldots a_n^{\alpha(n)} \ , \ 0 \leq \alpha(i) < p \ , r \leq i \leq n$$

Assumiremos que as condições de associatividade de Wamsley são satisfeitas em W e usaremos indução para mostrar que $W = W_1, W_2, \ldots, W_n$ são todos grupos.

É claro que W_n é um grupo cíclico de ordem p.

Vamos supor agora que W_{k+1} é um grupo para algum $k \in \{1, 2, \ldots, n\}$ e provaremos que W_k é um grupo.

Definamos a aplicação $\theta_k : W_{k+1} \to W_{k+1}$ por $w\theta_k := u$, onde $a_k u$ é a palavra normal obtida de wa_k através do processo de coleta. Mostraremos que θ_k é um automorfismo de W_{k+1} como segue.

Primeiro mostraremos que se $a_i a_j \ldots a_r a_s$ é uma palavra normal em W_{k+1}, então

$$(a_i a_j \ldots a_r a_s)\theta_k = a_i\theta_k a_j\theta_k \ldots a_r\theta_k a_s\theta_k$$

como elemento de W_{k+1}.

Para calcular $(a_i a_j \ldots a_r a_s)\theta_k$, devemos aplicar o processo de coleta à palavra $a_i a_j \ldots a_r a_s a_k$. As duas primeiras palavras no output são

$$a_i a_j \ldots a_r a_s (a_s\theta_k) \ \text{ e } \ a_i a_j \ldots a_k (a_r\theta_k)(a_s\theta_k) \ .$$

Observe que na segunda podemos ter mais de uma subpalavra não normal minimal. De fato, existe uma subpalavra não normal minimal envolvendo a_k e pode existir também

alguma em $(a_r\theta_k)(a_s\theta_k)$. Porém, se identificamos $(a_r\theta_k)(a_s\theta_k)$ como um elemento de W_{k+1}, então a coleta de qualquer destas subpalavras não muda estes valores como elementos de W_{k+1} (pela observação 2.2.8). Assim podemos ignorar a coleta de subpalavras à direita de a_k. Por outro lado, sabemos que não existe uma subpalavra não normal minimal à esquerda de a_k em qualquer estágio do processo de coleta. Deste modo, quando o processo de coleta é completado, obtemos uma palavra $a_k u$, onde u é a palavra normal igual a $a_i\theta_k a_j\theta_k \ldots a_r\theta_k a_s\theta_k$ como elemento de W_{k+1}.

Então $(a_i a_j \ldots a_r a_s)\theta_k = u$ e este é o resultado desejado.

Note que para $k+1 \leq i \leq n$, $a_i\theta_k = a_i$ módulo W_{i+1} (pois, se $i \geq k+1$, temos $a_i a_k = a_k a_i w$, onde $w = a_{i+1}^{\alpha(i,k,i+1)} \ldots a_n^{\alpha(i,k,n)}$, logo $a_i\theta_k = a_i w$ com $w \in W_{i+1}$) e isto implica que todo elemento de W_{k+1} pode ser expresso de maneira única como uma palavra normal nos elementos $a_{k+1}\theta_k, a_{k+2}\theta_k, \ldots, a_n\theta_k$ e portanto, que θ_k é uma permutação de W_{k+1}.

Mostremos agora que a condição de associatividade

$$(a_i.a_j).a_k = a_i.(a_j.a_k) \text{ com } 1 \leq k < j < i \leq n$$

é equivalente à condição

$$(a_i.a_j)\theta_k = (a_j a_i a_{i+1}^{\beta(i,j,i+1)} \ldots a_n^{\beta(i,j,n)})\theta_k = (a_i\theta_k).(a_j\theta_k)$$

De fato,

$$(a_i.a_j).a_k = a_k(a_i.a_j)\theta_k = a_k(a_j a_i a_{i+1}^{\beta(i,j,i+1)} \ldots a_n^{\beta(i,j,n)})\theta_k$$

e

$$a_i.(a_j.a_k) = a_i.(a_k a_j\theta_k) = a_k(a_i\theta_k.a_j\theta_k)) \ .$$

De forma análoga, temos que a condição

$$(a_j^{p-1}.a_j).a_k = a_j^{p-1}.(a_j.a_k) \text{ com } 1 \leq k < j \leq n$$

é equivalente à condição

$$(a_j^p)\theta_k = (a_{j+1}^{\alpha(j,j+1)} \ldots a_n^{\alpha(j,n)})\theta_k = (a_j\theta_k)^p \ .$$

Assim, a permutação θ_k é induzida homomorficamente por uma aplicação dos geradores de W_{k+1} em W_{k+1} e θ_k preserva as relações satisfeitas pelos geradores. Isto prova que θ_k é um automorfismo de W_{k+1}.

Vejamos agora que a condição de associatividade

$$(a_i.a_k).a_k^{p-1} = a_i.(a_k.a_k^{p-1}) \text{ com } 1 \leq k < i \leq n \ ,$$

é equivalente à condição

$$a_i(\theta_k)^p = u^{-1}.a_i.u \text{ onde } u = a_{k+1}^{\alpha(k,k+1)} a_{k+2}^{\alpha(k,k+2)} \ldots a_n^{\alpha(k,n)} \in W_{k+1} \ ,$$

onde a palavra u é o lado direito da relação cujo lado esquerdo é a_k^p.

De fato,

$$\begin{aligned}(a_i.a_k).a_k^{p-1} &= a_k a_i \theta_k \ . \ a_k^{p-1} = a_k^2(a_i\theta_k)\theta_k \ . \ a_k^{p-2} = \\ &= \ldots = a_k^p \ . \ a_i(\theta_k)^p = u \ . \ a_i(\theta_k)^p \ ,\end{aligned}$$

e, por outro lado,

$$a_i.(a_k.a_k^{p-1}) = a_i.a_k^p = a_i.u \ .$$

Finalmente, é claro que a condição de associatividade $(a_k.a_k^{p-1}).a_k = a_k.(a_k^{p-1}.a_k)$ é equivalente à condição $u\theta_k = u$.

Agora seja $H =< \theta_k > \ltimes W_{k+1}$ o produto semidireto de $< \theta_k >$ por W_{k+1} (isto é,

$$H = (< \theta_k > \times W_{k+1}, \odot) \ , \text{ onde } \odot :< \theta_k > \times W_{k+1} \rightarrow < \theta_k > \times W_{k+1}$$

é definida por $(\theta_k^r, w) \odot (\theta_k^{r'}, w') = (\theta_k^{r+r'}, w\theta_k^{r'}.w')$ para $w, w' \in W_{k+1}$; $r, r' \in \mathbb{Z}$ e $\cdot$ a operação definida antes em W_{k+1}).

Notemos que o elemento (θ_k^{-p}, u) é central em H. De fato, dado $(\theta_k^r, w) \in H$, temos que $(\theta_k^r, w)(\theta_k^{-p}, u) = (\theta_k^{r-p}, w\theta_k^{-p}.u) = (\theta_k^{r-p}, u.w)$ desde que $w = (w\theta_k^{-p})\theta_k^p = u^{-1}.(w\theta_k^{-p}).u$ e, portanto, $u.w = w\theta_k^{-p}.u$.

E, por outro lado, $(\theta_k^{-p}, u)(\theta_k^r, w) = (\theta_k^{r-p}, u\theta_k^r.w) = (\theta_k^{r-p}, u.w)$ desde que $u\theta_k = u$.

Agora defina $\mu : H \rightarrow W_k$ o homomorfismo tal que

$$\begin{cases} (\theta_k, 1)\mu = a_k \\ (\mathrm{id}, a_i)\mu = a_i \ , \quad k+1 \leq i \leq n \end{cases}$$

μ é claramente sobrejetor e $\ker \mu =< (\theta_k^{-p}, u) >$, logo $W_k \cong H/ < (\theta_k^{-p}, u) >$ e, portanto, W_k é um grupo, como queríamos demonstrar.

Desta forma, temos provado que, se as condições de Wamsley são satisfeitas, então W é um grupo.

Mostraremos agora que as condições de associatividade de Wamsley com $k > d$ são redundantes. Como vimos acima, elas foram usadas para mostrar que θ_k é um automorfismo de W_{k+1}. Mostraremos então que se $k > d$, as definições de $a_{d+1}, a_{d+2}, \ldots, a_k$ podem ser usadas para expressar θ_k em termos de $\theta_1, \theta_2, \ldots, \theta_d$. Deste modo, como $\theta_1, \ldots, \theta_d$ agem como automorfismos de W_{k+1}, teremos que θ_k é também um automorfismo de W_{k+1}.

Para isto estabeleceremos o seguinte roteiro:

Vamos supor que as condições de Wamsley valem para $k \leq d$ e faremos a hipótese tripla de indução:

Primeiro suponha que W_{k+1} é um grupo para algum $1 \leq k < n$.

Em seguida, suponha que $\theta_1, \theta_2, \ldots, \theta_{r-1}$ agem como automorfismos sobre W_{k+1} para algum $d < r \leq k$ (de fato, segue das condições de Wamsley para $k \leq d$ que $\theta_1, \ldots, \theta_d$ são automorfismos de W_{k+1}).

Finalmente, suponha que θ_r age como automorfismo sobre W_{s+1} para algum $k+1 < s+1 \leq n$ (claramente θ_r age como o automorfismo identidade sobre W_n).

Mostraremos que isto implica que θ_r age como um automorfismo sobre W_s; logo, por indução sobre s, isto implicará que θ_r age como automorfismo sobre W_{k+1} e finalmente, por indução sobre r, isto implicará que θ_k age como automorfismo sobre W_{k+1}. Desta forma, como antes, teremos que W_k é um grupo e conseqüentemente concluiremos que W é um grupo.

Antes de entrar nos detalhes da demonstração, precisaremos de três lemas técnicos a respeito do processo de coleta.

Lema 2.2.9: *Seja W_{k+1} um grupo, e seja θ_r um automorfismo de W_{k+1} para algum $r \leq k$. Se u é uma palavra nos geradores de W_{k+1} cuja forma normal é v, então o resultado de aplicar o processo de coleta à palavra ua_r é a palavra $a_r(v\theta_r)$.*

Demonstração: Se $u = v$ ou se na coleta de ua_r, u é coletado na forma normal antes da coleta de qualquer subpalavra envolvendo a_r, então o resultado segue imediatamente da definição de θ_r (pois $v\theta_r$ é a palavra normal tal que $a_r(v\theta_r)$ é o resultado de coletar-se a palavra va_r que, por sua vez, é o resultado de coletar-se ua_r coletando-se u antes de qualquer subpalvra envolvendo a_r).

Em geral, temos dois tipos de subpalavras minimais não normais a considerar

i. palavras da forma $a_p a_r$ para algum $p > k$ e

ii. palavras que envolvem só geradores de W_{k+1}.

Suponha que, num estado intermediário do processo de coleta, temos uma palavra da forma $w_1 a_r w_2$, onde w_1, w_2 são palavras em $a_{k+1}, a_{k+2}, \ldots, a_n$.

Se uma seqüência de coletas de subpalavras minimais não normais do segundo tipo é aplicado a $w_1 a_r w_2$, obtemos uma palavra da forma $v_1 a_r v_2$, onde $v_1 = w_1$ e $v_2 = w_2$ como elementos do grupo W_{k+1}. Por outro lado, se uma subpalavra do primeiro tipo, digamos $a_p a_r$, é coletada, então ela é substituída por $a_r(a_p\theta_r)$. Assim, se as subpalavras da forma $a_p a_r$ coletadas durante o processo todo são, em seqüência

$$a_i a_r \ , \ a_j a_r \ , \ldots , \ a_m a_r \ ,$$

então $a_m \ldots a_j a_i = v$ como elemento de W_{k+1} e essas subpalavras são substituídas sucessivamente por $a_r(a_i\theta_r), \ldots, a_r(a_m\theta_r)$. Assim o resultado no fim do processo é $a_r w$ onde w é uma palavra normal em W_{k+1}, igual a $(a_m\theta_r).\ldots.(a_j\theta_r).(a_i\theta_r)$. Mas θ_r é um automorfismo de W_{k+1} e, portanto,

$$w = (a_m\theta_r).\ldots.(a_j\theta_r).(a_i\theta_r) = (a_m \ldots a_j a_i)\theta_r = v\theta_r \ .$$

Segue-se assim que o resultado de coletar $u a_r$ é $a_r(v\theta_r)$. ∎

Lema 2.2.10: *Seja W_{k+1} um grupo e seja $a_i a_j \ldots a_r$ uma palavra normal com $i \leq j \leq \ldots \leq r \leq k$. Suponha que $\theta_i, \theta_j, \ldots, \theta_r$ ajam como automorfismos sobre W_{k+1} e seja u uma palavra nos geradores de W_{k+1} cuja forma normal é v. Então, se o processo de coleta é aplicado a $u a_i a_j \ldots a_r$, obtemos $a_i a_j \ldots a_r (v\theta_i\theta_j \ldots \theta_r)$.*

Demonstração: A demonstração segue o mesmo raciocínio da do lema anterior.

Seja $a_p a_i, a_q a_i, \ldots, a_s a_i$ a seqüência de palavras não normais minimais envolvendo a_i, que são coletadas no processo todo de coletar a_i. Então $a_s \ldots a_q a_p = v$ e o resultado de coletar a_i é $a_i w$, onde w é o resultado de coletar

$$(a_s\theta_i) \ldots (a_q\theta_i)(a_p\theta_i) a_j \ldots a_r \ .$$

Mas $v\theta_i$ é a palavra normal correspondente a $(a_s\theta_i)\ldots(a_q\theta_i)(a_p\theta_i)$. Indutivamente temos que $a_j\ldots a_r(v\theta_i\theta_j\ldots\theta_r)$ é o resultado de coletar

$$(a_s\theta_i)\ldots(a_q\theta_i)(a_p\theta_i)a_j\ldots a_r\ .$$

Conseqüentemente, o resultado de coletar $ua_ia_j\ldots a_r$ é $a_ia_j\ldots a_r(v\theta_i\theta_j\ldots\theta_r)$. ■

Lema 2.2.11: *Seja W_{k+1} um grupo e seja $a_ia_j\ldots a_ta_r$ uma palavra normal com $i \leq j \leq \ldots \leq t \leq r \leq k$. Suponha que $\theta_i, \theta_j, \ldots, \theta_t$ ajam como automorfismos sobre W_{k+1} e que θ_r aja como um automorfismo de W_{s+1} para algum $s > k$. Então, se o processo de coleta é aplicado a $a_sa_ia_j\ldots a_ta_r$, obtemos $a_ia_j\ldots a_ta_ru$, onde u é a palavra normal em W_{k+1} igual a*

$$a_s\theta_r(a_s^{-1}(a_s\theta_i\theta_j\ldots\theta_t))\theta_r\ .$$

Demonstração: Como nas demonstrações dos lemas anteriores, vemos que, se $a_sa_ia_j\ldots a_ta_r$ é coletada, obtemos $a_ia_j\ldots a_tv$, onde v é o resultado de coletar uma palavra da forma $a_sa_p\ldots a_qa_r$, com $p,\ldots,q > s$ e $a_sa_p\ldots a_q = a_s\theta_i\theta_j\ldots\theta_t$ como elemento de W_{k+1}.

Porém, na coleta de $a_sa_p\ldots a_qa_r$, a última subpalavra minimal não normal envolvendo a_r a ser coletada é sempre a_sa_r. Assim, o resultado da coleta de $a_sa_p\ldots a_qa_s$ é a_su, onde

$$\begin{aligned} u &= a_s\theta_r\ .\ (a_p\ldots a_q)\theta_r = a_s\theta_r\ .\ (a_s^{-1}(a_s\theta_i\theta_j\ldots\theta_t))\theta_r \\ \text{pois}\quad a_p\ldots a_q &= a_s^{-1}\ .\ (a_s\theta_i\theta_j\ldots\theta_t) \end{aligned}$$

e portanto o resultado de coletar $a_sa_ia_j\ldots a_ta_r$ é

$$a_ia_j\ldots a_ta_ra_s\theta_r.(a_s^{-1}.(a_s\theta_i\theta_j\ldots\theta_t))\theta_r\ .$$

■

Podemos agora completar a nossa tripla indução. A nossa hipótese consiste de

1) Supor que W_{k+1} é um grupo para algum k, $1 \leq k < n$

2) Supor que $\theta_1,\ldots,\theta_{r-1}$ agem como automorfismos sobre W_{k+1} para algum r, $d < r \leq k$.

3) Supor que θ_r age como automorfismo sobre W_{s+1} para algum s, $k+1 < s \leq n$.

Mostraremos então que θ_r age como um automorfismo sobre W_s.

De fato, como $r > d$, a_r tem uma definição da forma

$$a_j a_k = a_k a_j a_{j+1}^{\alpha(j+1)} \dots a_{r-1}^{\alpha(r-1)} a_r \quad \text{com} \quad k \leq d \quad \text{e} \quad k < j$$

ou uma definição da forma

$$a_j^p = a_{j+1}^{\alpha(j+1)} \dots a_{r-1}^{\alpha(r-1)} a_r \ .$$

Suponhamos que a definição de a_r seja da primeira forma. Mostraremos que θ_r age como

$$\left(\theta_k \theta_j \theta_{j+1}^{\alpha(j+1)} \dots \theta_{r-1}^{\alpha(r-1)}\right)^{-1} \theta_j \theta_k$$

sobre W_s. Como pela hipótese de indução, $\theta_1, \dots, \theta_{r-1}$ são todos automorfismos de W_s, basta provar que θ_r também é um automorfismo de W_s.

Seja $\phi = \theta_k \theta_j \theta_{j+1} \dots \theta_{r-1}$.

É claro que θ_r age como $\phi^{-1}\theta_j\theta_k$ sobre W_n, pois em ambos os casos a ação é igual à identidade sobre W_n.

Suponhamos então que θ_r age como $\phi^{-1}\theta_j\theta_k$ sobre W_{s+1}. (1)

Agora, se $a_1^{\beta(s)} \dots a_n^{\beta(n)}$ é uma palavra normal em W_s, então

$$\left(a_s^{\beta(s)} \dots a_n^{\beta(n)}\right) \theta_r = (a_s\theta_r)^{\beta(s)} \dots (a_n\theta_r)^{\beta(n)}$$

e assim, é suficiente mostrar que

$$a_s\theta_r = a_s\phi^{-1}\theta_j\theta_k$$

(pois, pela suposição (1), temos que $a_i\theta_r = a_i\phi^{-1}\theta_j\theta_k$ para $i > s$). Mas $k \leq d$ e, portanto,

$$(a_s.a_j).a_k = a_s.(a_j.a_k)$$

Agora,

$$a_s.(a_j.a_k) = (a_j(a_s\theta_j)).a_k = a_k a_j a_{j+1}^{\alpha(j+1)} \dots a_{r-1}^{\alpha(r-1)} a_r(a_s\theta_j\theta_k) \ .$$

E também, pelo lema 2.2.11

$$\begin{aligned} a_s.(a_j.a_k) &= a_s.(a_k a_j a_{j+1}^{\alpha(j+1)} \dots a_{r-1}^{\alpha(r-1)} a_r) \\ &= a_k a_j a_{j+1}^{\alpha(j+1)} \dots a_{r-1}^{\alpha(r-1)} a_r u \end{aligned}$$

onde $u = a_s\theta_r \cdot (a_s^{-1} \cdot a_s\phi)\theta_r$ como elemento de W_s.

Assim

$$a_s\theta_j\theta_k = a_s\theta_r.(a_s^{-1}.a_s\phi)\theta_r \ .$$

Mas $(a_s^{-1}.a_s\phi) \in W_{s+1}$, já que, como vimos na prova do lema 2.2.11, $a_s\phi = a_s a_p \ldots a_q$ como elemento de W_{k+1}, com $p, \ldots, q > s$, e desta forma

$$\begin{aligned} (a_s^{-1}.a_s\phi)\theta_r &= (a_s^{-1}.a_s\phi)\phi^{-1}\theta_j\theta_k \\ &= a_s^{-1}\phi^{-1}\theta_j\theta_k \cdot a_s\theta_j\theta_k \end{aligned}$$

Segue-se então que

$$a_s\theta_j\theta_k = a_s\theta_r \cdot a_s^{-1}\phi^{-1}\theta_j\theta_k \cdot a_s\theta_j\theta_k$$

e conseqüentemente

$$a_s\theta_r = a_s\phi^{-1}\theta_j\theta_k$$

como queríamos.

A prova é análoga se a definição de a_r é da forma

$$a_j^p = a_{j+1}^{\alpha(j+1)} \ldots a_{r-1}^{\alpha(r-1)} a_r \ .$$

Isto completa a demonstração de que as condições de associatividade de Wamsley $k \leq d$ implicam que W é um grupo e conseqüentemente estabelecem um critério para testar consistência. ∎

2.3 Processo de Redução

Consideremos a seguinte apresentação por potências e comutadores:

$$\begin{aligned} &\text{geradores} : \ a_1, \ldots, a_n \\ &\text{relações} : \quad a_i^p = \prod_{l=i+1}^{n} a_l^{\alpha(i,l)} \\ &\qquad\qquad [a_j, a_i] = \prod_{l=j+1}^{n} a_l^{\alpha(i,j,l)} \ , i < j \ ; \end{aligned}$$

onde p é um primo e $\alpha(i,l), \alpha(i,j,l) \in \{0, 1, \ldots, p-1\}$.

Denotaremos esta apresentação por $(n; p, \alpha)$ e ao grupo apresentado por ela $< n; p, \alpha >$.

Como já vimos antes, todo elemento de $< n; p, \alpha >$ pode ser escrito como uma palavra normal nos geradores, i.e., na forma $\xi := \prod_{l=1}^{n} a_l^{\xi(l)}$ com $\xi(l) \in \{0, 1, \ldots, p-1\}$ (veja processo de coleta). Por outro lado, sabemos também que, embora o conjunto dessas palavras normais tenha p^n elementos, a ordem de $< n; p, \alpha >$ pode ser menor do que p^n (veja consistência).

Definamos T_n como o conjunto de todas as palavras da forma

$$\begin{aligned} a_k a_j a_i \ ; &\quad i < j < k \\ a_j^p a_i \ ; &\quad i < j \\ a_j a_i^p \ ; &\quad i < j \\ a_i^{p+1} \ . & \end{aligned}$$

Observe que cada palavra em T_n tem exatamente duas subpalavras minimais não normais que se sobrepõem. Assim, cada palavra em T_n pode ser escrita de maneira única na forma $\xi\eta\zeta$ com ξ, η e ζ palavras normais não vazias e $\xi\eta$, $\eta\zeta$ não normais minimais.

Por último, notemos que o critério de consistência estabelecido através das condições de associatividade de Wamsley pode ser reformulado assim:

A apresentação $(n; p, \alpha)$ é consistente, isto é, $< n; p, \alpha >$ tem ordem p^n se, e somente se, para cada palavra $\xi\eta\zeta \in T_n$, tem-se $((\xi\eta)\zeta) = (\xi(\eta\zeta))$ (onde (w) denota a palavra normal resultante da coleta de w). Portanto, se $(n; p, \alpha)$ não for consistente, então alguma dessas palavras será coletada em duas palavras normais diferentes.

Apresentaremos agora um procedimento básico, chamado *redução*, que a partir de uma apresentação por potências e comutadores $(n; p, \alpha)$ e um par μ, ν de palavras normais diferentes, produz um subconjunto, B, do conjunto $\{a_1, \ldots, a_n\}$ com $n-1$ elementos e uma apresentação por potências e comutadores com B como conjunto de geradores para o grupo definido por $(n; p, \alpha)$ e $\mu = \nu$.

Quando as palavras μ e ν provêm da coleta de uma palavra em T_n, o grupo definido pela apresentação resultante é claramente isomorfo a $< n; p, \alpha >$. Iterando o processo, obtemos uma apresentação consistente para $< n; p, \alpha >$.

Não descreveremos aqui o processo de redução em geral, já que o usaremos somente no caso em que μ e ν são palavras obviamente centrais e de ordem p (dizemos que a

palavra normal ξ é *obviamente central e de ordem p* se, para todo gerador a_l que aparece em ξ, i.e., $\xi(l) \neq 0$, todas as relações em $(n; p, \alpha)$ com a_l no lado esquerdo têm a palavra vazia no lado direito).

O processo de redução:

Seja G o grupo definido por $(n; p, \alpha)$ e $\mu = \nu$, onde μ e ν são duas palavras normais diferentes e são obviamente centrais e de ordem p.

Como μ e ν são diferentes, seja k o maior inteiro positivo tal que $\mu(k) \neq \nu(k)$.

Para cada l, seja a seguinte congruência linear:

$$(\mu(k) - \nu(k))\chi \equiv \nu(l) - \mu(l)(\mathrm{mod} p) \ . \tag{2.3.1}$$

Como $0 \leq \nu(l), \mu(l) < p$, temos que $|\mu(k) - \nu(k)| < p$ e assim $\mathrm{mdc}(\mu(k) - \nu(k), p) = 1$. Portanto $(\nu(l) - \mu(l))$ é múltiplo do $\mathrm{mdc}(\mu(k) - \nu(k), p)$ e dessa forma concluímos que a congruência (2.3.1) tem solução.

Seja $n(l)$ o menor inteiro não negativo, solução da congruência (2.3.1). Agora, como k é o maior inteiro positivo tal que $\mu(k) \neq \nu(k)$, temos que

$$\begin{aligned} \mu &= \prod_{l=1}^{k-1} a_l^{\mu(l)} \ . \ a_k^{\mu(k)} \ . \prod_{l=k+1}^{n} a_l^{\mu(l)} \\ \nu &= \prod_{l=1}^{k-1} a_l^{\nu(l)} \ . \ a_k^{\nu(k)} \ . \prod_{l=k+1}^{n} a_l^{\mu(l)} \end{aligned}$$

Logo, $\mu = \nu$ pode ser escrito na seguinte forma

$$\prod_{l=1}^{k-1} a_l^{\mu(l)} \ . \ a_k^{\mu(k)} = \prod_{l=1}^{k-1} a_l^{\nu(l)} \ . \ a_k^{\nu(k)}$$

Como μ e ν são palavras obviamente centrais e de ordem p, temos que cada a_l, com $\mu(l) \neq 0$ ou $\nu(l) \neq 0$, é central e de ordem p. Logo, a identidade acima é equivalente a

$$a_k^{\mu(k)-\nu(k)} = \prod_{l=1}^{k-1} a_l^{\nu(l)-\mu(l)}$$

e sabemos também que

$$a_l^{\nu(l)-\mu(l)} = a_l^{n(l)(\mu(k)-\nu(k))} \ , \forall l \ .$$

Portanto, temos

$$\left(\prod_{l=1}^{k-1} a_l^{n(l)}\right)^{(\mu(k)-\nu(k))} = \prod_{l=1}^{k-1} a_l^{n(l)(\mu(k)-\nu(k))}$$
$$= \prod_{l=1}^{k-1} a_l^{\nu(l)-\mu(l)} = a_k^{\mu(k)-\nu(k)} .$$

Desta forma, temos provado que $\mu = \nu$ é equivalente à condição

$$a_k = \prod_{l=1}^{k-1} a_l^{n(l)} . \tag{2.3.2}$$

Seja α' a função definida por

$$\begin{cases} \alpha'(i,l) & \equiv & \alpha(i,l) + n(l)\alpha(i,k)(\mathrm{mod}p) \\ \alpha'(i,j,l) & \equiv & \alpha(i,j,l) + n(l)\alpha(i,j,k)(\mathrm{mod}p) \\ \text{e} \quad 0 & \leq & \alpha'(i,l); \alpha'(i,j,l) < p . \end{cases}$$

Note que

1) G é definido por $(n; p, \alpha')$ e (2.3.2).

2) $\alpha'(i,k) = \alpha'(i,j,k) = 0$, $\forall i,j$, pois $n(k)$ é tal que

$$n(k)(\mu(k) - \nu(k)) \equiv \nu(k) - \mu(k)(\mathrm{mod}p) ,$$

logo, como $\mu(k) - \nu(k) \not\equiv 0(\mathrm{mod}p)$, temos que $(n(k) + 1 \equiv 0(\mathrm{mod}p)$ e assim $\alpha'(i,k) \equiv (1 + n(k))(\alpha(i,k))(\mathrm{mod}p)$ e $0 \leq \alpha'(i,k) < p$ implicam $\alpha'(i,k) = 0$. Analogamente temos $\alpha'(i,j,k) = 0$, $\forall i,j$.

Assim, o gerador a_k só aparece no lado esquerdo das relações de $(n; p, \alpha')$ e neste caso a relação é uma conseqüência de (2.3.2) e relações que não envolvem a_k.

Portanto, a apresentação obtida de $(n; p, \alpha')$, tirando-se a_k do conjunto gerador e todas as relações que o envolvem, é uma apresentação por potências e comutadores para G com $n - 1$ geradores.

2.4 Apresentações ponderadas por potências e comutadores

Definição 2.4.1: Uma apresentação por potências e comutadores como foi dada na definição 2.1.1 será dita *ponderada* se:

1 - Algumas das suas relações são chamadas definições, e
2 - Admite uma função peso ω de $\{a_1, \ldots, a_n\}$ no conjunto dos inteiros positivos tal que:

a) $\omega(a_1) = 1$ e $\omega(a_i) \leq \omega(a_{i+1})$

b) para cada a_k com $\omega(a_k) > 1$ existe exatamente uma definição cujo lado direito é a_k.

c) Se a definição de a_k é $a_i^p =: a_k$, então $\omega(a_k) = \omega(a_i) + 1$.

d) Se a definição de a_k é $[a_j, a_i] =: a_k$, então $\omega(a_k) = \omega(a_i) + \omega(a_j)$.

e) Se $\alpha(i, \ell) \neq 0$, então $\omega(a_\ell) \geq \omega(a_i) + 1$.
Se $\alpha(i, j, \ell) \neq 0$, então $\omega(a_\ell) \geq \omega(a_i) + \omega(a_j)$. □

Proposição 2.4.2: *Todo p-grupo finito tem uma apresentação ponderada por potências e comutadores.*

Demonstração: Seja G um p-grupo finito com série p-central inferior

$$G = P_0(G) > P_1(G) > P_2(G) > \ldots > P_{c-1}(G) > P_c(G) = \{1\}.$$

onde $P_{i+1}(G) = P_i(G)^P[P_i(G), G]$ para $i = 0, 1, \ldots c-1$.

Vamos construir uma apresentação ponderada por potências e comutadores para G. Primeiramente observe que $P_0(G)/P_1(G)\left(= \frac{G}{G^P G'}\right)$ é um p-grupo abeliano elementar. Suponha que este tenha ordem p^{r_1} e escolha elementos $a_1, a_2, \ldots, a_{r_1}$ tais que

$$a_1 P_1(G), a_2 P_1(G), \ldots, a_{r_1} P_1(G) \quad \text{geram} \quad P_0(G)/P_1(G)$$

Note que $P_1(G) = G^P G'$ é o subgrupo de Frattini de G, então $a_1, \ldots, a_{r_1}$ formam um conjunto gerador minimal para G. (Teorema 1.5.8).

Diremos então, que $\omega(a_1) = \omega(a_2) = \ldots = \omega(a_{r_1}) = 1$.

Agora, $P_1(G)/P_2(G) = \dfrac{P_1(G)}{P_1(G)^P[P_1(G), G]}$ é também um p-grupo abeliano elementar, de ordem p^{r_2}, e $P_1(G)/P_2(G)$ é gerado por

$$a_i^P P_2(G)\ (1 \leq i \leq r_1);\ [a_j, a_i]P_2(G)\ (1 \leq i < j \leq r_1).$$

Escolha, a partir deste conjunto gerador, uma base

$$x_1^{(2)}P_2(G),\ x_2^{(2)}P_2(G), \ldots, x_{r_2}^{(2)}P_2(G) \quad \text{para} \quad P_1(G)\ /\ P_2(G) \quad \text{onde}$$
$$x_1^{(2)}, \ldots, x_{r_2}^{(2)} \in \{a_i^P;\ [a_j, a_i]\ /\ 1 \leq i \leq r_1 \quad \text{e} \quad 1 \leq i < j \leq r_1\}$$

Portanto diremos que $\omega(x_1^{(2)}) = \omega(x_2^{(2)}) = \ldots = \omega(x_{r_2}^{(2)}) = 2$.

Agora suponha que já encontramos elementos:

$$a_1, a_2, \ldots, a_{r_1}, x_1^{(2)}, \ldots, x_{r_2}^{(2)}, \ldots, x_1^{(d-1)}, x_2^{(d-1)}, \ldots, x_{r_{d-1}}^{(d-1)} \text{ tais que:}$$

- $a_1P_1(G), a_2P_1(G), \ldots, a_{r_1}P_1(G)$ formam uma base para $P_0(G)/P_1(G)$ e $\omega(a_1) = \omega(a_2) = \ldots = \omega(a_{r_1}) = 1$;

- $x_1^{(2)}P_2(G), x_2^{(2)}P_2(G), \ldots, x_{r_2}^{(2)}P_2(G)$ formam uma base para $P_1(G)/P_2(G)$ e $\omega(x_1^{(2)}) = \omega(x_2^{(2)}) = \ldots = \omega(x_{r_2}^{(2)}) = 2$;

- .....

- $x_1^{(t-1)}P_{t-1}(G), x_2^{(t-1)}P_{t-1}(G), \ldots, x_{r_{t-1}}^{(t-1)}P_{t-1}(G)$, formam uma base para $P_{t-2}(G)/P_{t-1}(G)$ e $\omega(x_1^{(t-1)}) = \omega(x_2^{(t-1)}) = \ldots = \omega(x_{r_{t-1}}^{(t-1)}) = t-1$.

Sabemos então que $P_{t-1}(G)/P_t(G)$ é gerado por elementos do seguinte conjunto:

$$\{y_k^p P_t(G),\ \omega(y_k) = t-1\} \cup \{[y_j, y_i]P_t(G);\ \omega(y_j) = t-1, \omega(y_i) = 1,\ i < j\}$$

Escolha a partir deste conjunto gerador uma base

$$x_1^{(t)}P_t(G), x_2^{(t)}P_t(G), \ldots, x_{r_t}^{(t)}P_t(G) \quad \text{para} \quad P_{t-1}(G)/P_t(G) \quad \text{e}$$

considere então $\omega(x_1^{(t)}) = \omega(x_2^{(t)}) = \ldots = \omega(x_{r_t}^{(t)}) = t$.

Observação: *Neste processo, se* $\omega(y_k) = \lambda > 1$, *então* y_k *tem uma definição*

$$y_k = y_i^p \text{ com } \omega(y_i) = \lambda - 1 \quad \text{ou}$$
$$y_k = [y_j, y_i] \text{ com } \omega(y_j) = \lambda - 1,\ \omega(y_i) = 1 \text{ e } i < j \qquad \square$$

Assim, se assumirmos que $|G| = p^n$, o processo anterior nos fornece um conjunto gerador para G, $\{a_1, a_2, \ldots, a_n\}$, com as condições:

(1) $P_1(G) =< a_k/\omega(a_k) \geq i >$, que é equivalente a dizer que $P_1(G) = \{a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_n^{\alpha_n} / 0 \leq \alpha_j < p, \alpha_j = 0 \text{ se } \omega(a_j) < i\}$.

(2) Se $\omega(a_i) = t$ então $a_i \in P_t(G)$, logo $a_i^p \in P_{t+1}(G)$ e portanto, $a_i^p = a_{i+1}^{\alpha(i,i+1)} \ldots a_n^{\alpha(i,n)}$, onde $\alpha(i,j) = 0$ se $\omega(a_j) < t+1$.

(3) Se $1 \leq i < j \leq n$ então $[a_j, a_i] = a_{j+1}^{\beta(i,j,j+1)} \ldots a_n^{\beta(i,j,n)}$, onde $\beta(i,j,k) = 0$ se $\omega(a_k) < \omega(a_j) + \omega(a_i)$.

Resumindo, se tivermos um p-grupo G, tal que $|G| = p^n$, é possível encontrar um conjunto gerador $\{a_1, a_2, \ldots, a_n\}$ para G satisfazendo as relações:

$$a_i^p = a_{i+1}^{\alpha(i,i+1)} a_{i+2}^{\alpha(i,i+2)} \ldots a_n^{\alpha(i,n)}, 1 \leq i \leq n$$
$$[a_j, a_i] = a_{j+i}^{\beta(i,j,j+1)} \ldots a_n^{\beta(i,j,n)}, 1 \leq i < j \leq n$$

e satisfazendo ainda as condições de peso

$$1 = \omega(a_1) = \omega(a_2) = \ldots = \omega(a_r) < \omega(a_{r+1}) \leq \ldots \leq \omega(a_n) = c$$

(onde r = número mínimo de geradores para G), logo, pela observação anterior, temos que $n - r$ das relações são definições do tipo:

$$a_k = a_i^p \text{ com } \omega(a_k) = \omega(a_i) + 1$$
$$\text{ou } a_k = [a_j, a_i] \text{ com } \omega(a_k) = \omega(a_i) + \omega(a_j)$$

e finalmente, segue-se de (2) e (3) acima, que

$$\text{se } \alpha(i,\ell) \neq 0, \text{ então } \omega(a_\ell) \geq \omega(a_i) + 1 \text{ e}$$
$$\text{se } \alpha(i,j,\ell) \neq 0, \text{ então } \omega(a_\ell) \geq \omega(a_i) + \omega(a_j).$$

Temos construindo assim, uma apresentação ponderada por potências e comutadores para G.

■

Denotaremos $(n; p, \alpha; \omega)$ à apresentação ponderada por potências e comutadores $(n; p, \alpha)$ com peso ω e denotaremos $< n; p, \alpha; \omega >$ ao grupo definido por ela.

Proposição 2.4.3: *$\omega(a_n)$ é a p-classe de $< n; p, \alpha; \omega >$.*

Demonstração: Seja $G =< n; p, \alpha; \omega >$. Provaremos que $P_k(G)$ é gerado por todos os a_k de peso maior ou igual a $h+1$.

De fato, se $h = 0$ é claro, pois $P_0(G) = G =< a_k/\omega(a_k) \geq 1 >=< a_1 \ldots a_n >$.

Seja $h \geq 1$.

Suponhamos que $P_t(G) =< a_\ell/\omega(a_\ell \geq t+1 >$, $\forall\ 1 \leq t \leq h-1$. Em conseqüência $P_h(G)$ é gerado por:

$$\{a_\ell^P; [a_\ell, a_i] \ / \ \omega(a_\ell) \geq h, \quad a_i \ \text{ arbitrário}\}$$

e assim, segue da definição da função peso que $P_h(G) \leq < a_k/\omega(a_k) \geq h+1 >$. Reciprocamente, se $\omega(a_k) \geq k+1 > 1$, então a definição de a_k é $a_k := a_i^P$, com $\omega(a_k) = \omega(a_i)+1$, ou $a_k := [a_j, a_i]$ com $\omega(a_k) = \omega(a_i) + \omega(a_j)$. No primeiro caso, $\omega(a_i) = \omega(a_k) - 1$, logo $\omega(a_i) \geq h$ e assim, pela hipótese indutiva temos que $a_i \in P_{h-1}(G)$, seguindo-se então que $a_k = a_i^P \in P_h(G)$. No segundo caso, suponhamos que $\omega(a_i) = m$ com $1 \leq m \leq h$, logo $\omega(a_j) = \omega(k) - m \geq h+1-m$ como $1 \leq m, h+1-m \leq h$, temos pela hipótese indutiva, que $a_i \in P_{m-1}(G)$ e $a_j \in P_{h-m}(G)$ e desta forma, temos que $[a_j, a_i] \in [P_{h-m}(G), P_{m-1}(G)]$. Assim, pela propriedade 1.4.9, temos que $[a_j, a_i] \in P_h(G)$, concluindo-se então, que $< a_k/\omega(a_k) \geq h+1 > \subseteq P_h(G)$.

Dado $G =< n; p, \alpha; \omega >$, sabemos então que

$$P_h(G) =< a_k/\omega(a_k) \geq h+1 > \quad \forall\ h$$

Seja $c = \omega(a_n)$. Assim,

$$\begin{aligned} P_c(G) &= < a_k/\omega(a_k) \geq c+1 >=< a_k/\omega(a_k) \geq \omega(a_n)+1 >= \{1\} \\ \text{e} \quad P_{c-1}(G) &= < a_k/\omega(a_k) \geq c >=< a_k/\omega(a_k) \geq \omega(a_n) >=< a_n >\neq \{1\} \end{aligned}$$

Portanto, a p-classe de G é $c = \omega(a_n)$. ■

Observação 2.4.4: *Pode acontecer que uma dada apresentação por potências e comutadores para um grupo G, não admita uma função peso sobre os seus geradores no sentido da definição* 2.4.1.

Seja, por exemplo, o grupo G dado pela seguinte apresentação:

$$G =< a,b,c,d \ / \ a^2 = dc,\ b^2 = d,\ [b,a] = d,\ [b,a] = [c,a] = [d,a] = 1$$
$$[c,b] = [d,b] = [d,c] = 1,\ c^2 = d^2 = 1 >$$

É claro que esta é uma apresentação por potências e comutadores para G, mas o gerador c não aparece isolado como membro direito de nenhuma das suas relações, portanto não admite uma ponderação no sentido da definição 2.4.1.

Para obter a partir dela uma apresentação ponderada observemos que $c \in P_1(G)$ e $P_1(G)/P_2(G)$ é gerado por $\{cdP_2(G),\ dP_2(G)\}$ tanto como por $\{cP_2(G),\ dP_2(G)\}$ de modo que podemos trocar c por $c' = cd$ no conjunto inicial de geradores, obtendo assim a seguinte apresentação:

$$< a,b,c',d \ / \ a^2 = c',\ b^2 = d,\ [b,a] = [c',a] = [d,a] = 1,$$
$$[c',b] = [d,b] = [d,c'] = 1,\ c'^2 = 1,\ d^2 = 1 >$$

na qual a função peso $\omega : \{a,b,c',d\} \to \{1,2\}$ está dada por $\omega(a) = \omega(b) = 1$ e $\omega(c') = \omega(d) = 2$. □

2.5 O algoritmo do quociente nilpotente

Como já adiantamos no início deste capítulo, o objetivo do algoritmo do quociente nilpotente, NQA, é, dado um grupo G finitamente apresentado e um primo p, construir uma apresentação consistente por potências e comutadores para o maior p-quociente finito de G.

Para isso, dado G, o algoritmo trabalha com a série p-central inferior de G:

$$G = P_0(G) > P_1(G) > \ldots > P_i(G) > P_{i+1}(G) > \ldots$$
$$\text{onde} \qquad P_{j+1}(G) = (P_j(G))^p [P_j(G), G]$$

determinando uma apresentação consistente por potências e comutadores para cada quociente $G/P_i(G), i = 1, 2, \ldots$.

Note que pela propriedade 1.4.4, sabemos que $G/P_i(G)$ é um p-grupo finito e é claro que desta forma será achado o maior p-quociente finito de G. De fato, se G/N é um p-quociente finito de G, temos então que a série p-central inferior de G/N termina em N, portanto existe c' tal que

$$P_{c'}(G/N) > P_{c'+1}(G/N) = N \ ,$$

logo $P_{c'+1}(G) \leq N$ e assim $|G/P_{c'+1}(G)| \geq |G/N|$.

Antes de descrever o algoritmo, vejamos a seguinte definição:

Definição 2.5.1: Seja H um grupo. O grupo H^* é dito o p-recobrimento de H se

1 - H^* tem um subgrupo $Z \leq Z(H^*)$, Z abeliano elementar e tal que $H^*/Z \cong H$.

2 - Se $\tilde{H}$ é um grupo qualquer tal que $\tilde{Z} \leq Z(\tilde{H})$ é abeliano elementar e $\tilde{H}/\tilde{Z} \cong H$, então $\tilde{H}$ é uma imagem homomórfica de H^*, isto é, existe um epimorfismo $\theta : H^* \twoheadrightarrow \tilde{H}$. □

O algoritmo:

Seja G um grupo dado pela seguinte apresentação finita:

$$G = < x_1, \ldots, x_m \ / \ r_1 = 1, \ldots, r_n = n > \ \ n, m \in \mathbb{N}$$

e seja

$$\begin{aligned} G \ &= \ P_0(G) > P_1(G) > \ldots > P_i(G) > \ldots \\ \text{com} \quad &P_{i+1}(G) = (P_i(G))^p [P_i(G), G] \end{aligned}$$

a sua série p-central inferior.

Sabemos que $G/P_1(G)$ é o maior p-quociente abeliano elementar, logo tem uma apresentação consistente por potências e comutadores:

$$G/P_1(G) = < a_1, \ldots, a_d \ / \ a_i^p = 1 \ , [a_j, a_i] = 1 \ , 1 \leq i < j \leq d > \ .$$

onde $a_1, \ldots, a_d$ são escolhidos, independentes módulo o subgrupo de Frattini de G, dentre os geradores $x_1, \ldots, x_m$ de apresentação dada para G.

(Note então que os x_i's restantes são geradores supérfluos na geração de G e então podem ser escritos em termos dos a_i's.)

Suponha agora ter uma apresentação consistente por potências e comutadores para $G/P_i(G)$, digamos

$$G/P_i(G) =< a_1, \ldots, a_d, a_{d+1}, \ldots, a_n \ / \ s_1, \ldots, s_l > \ , \ n, l \in I\!N$$

onde $n - d$ das relações expressam os a_j, $d < j \leq n$ em termos de potências e ou comutadores dos a_i com $1 \leq i \leq d$. Estas relações são chamadas de *definições*.

Queremos então construir uma apresentação consistente por potências e comutadores para $G/P_{i+1}(G)$. Notemos que

$$P_i(G)/P_{i+1}(G) \leq Z(G/P_{i+1}(G)) \ ,$$

$P_i(G)/P_{i+1}(G)$ é abeliano elementar e $\frac{G/P_{i+1}(G)}{P_i(G)/P_{i+1}(G)} \cong G/P_i(G)$ logo, segue da definição, que $G/P_{i+1}(G)$ é uma imagem homomórfica do p-recobrimento de $G/P_i(G)$.

Assim, o primeiro passo na construção de $G/P_{i+1}(G)$ é calcular uma apresentação para o p-recobrimento de $G/P_i(G)$. Uma tal apresentação é obtida modificando todas as relações acima que não são definições módulo novos geradores centrais e de ordem p. Isto é, uma apresentação para $(G/P_i(G))^*$ é dada por

geradores: $a_1, \ldots, a_{d+\frac{n(n+1)}{2}}$

relações:
1- As $n - d$ definições na apresentação para $G/P_i(G)$.
2- $d + \frac{n(n-1)}{2}$ $(= \frac{n(n+1)}{2} - (n-d))$ da forma $u_k = v_k a_k$ para $k \in \{n+1, \ldots, d + \frac{n(n+1)}{2}\}$, onde $u_k = v_k$ é uma relação na apresentação para $G/P_i(G)$ que não é uma definição.
3- As que especificam $a_{n+1}, \ldots, a_{d+\frac{n(n+1)}{2}}$ como elementos centrais e de ordem p.

As relações dos dois primeiros tipos são chamadas *definições*.

Como a apresentação dada para $G/P_i(G)$ é consistente, se alguma das condições de Wamsley não for satisfeita nesta apresentação para o seu p-recobrimento, a palavra normal resultante da palavra teste em questão é obviamente central e de ordem p. Assim a redução descrita antes pode ser usada para obter uma apresentação consistente por potências e comutadores com n^* geradores $(n \leq n^* \leq d + \frac{n(n+1)}{2})$ e $n^* - d$ definições.

Agora para obter uma apresentação consistente por potências e comutadores para $G/P_{i+1}(G)$ basta introduzir na apresentação para o p-recobrimento, $(G/P_i(G))^*$, de $G/P_i(G)$ as relações de G (note que para isso será necessário reescrever tais relações em termos dos geradores essenciais $a_1, \ldots, a_d$), essas relações são então coletadas e possivelmente nos levarão a novas eliminações.

2.6 Um Exemplo

Seja G o seguinte grupo finitamente apresentado:

$$G =< a_1, a_2 \ / \ a_1^{p^3} = a_2^p = 1, a_1^{a_2} = a_1^{1+p^2} >$$

com p primo ímpar.

Note que G é um grupo não abeliano ($[a_1, a_2] = a_1^{-1}a_1^{a_2} = a_1^{-1}a_1^{1+p^2} = a_1^{p^2} \neq 1$) de ordem p^4 (de fato, $| < a_1 > | = p^3$, $| < a_2 > | = p$ e

$$\begin{aligned}
a_2a_1 &= a_1a_2[a_1,a_2]^{-1} = a_1a_2a_1^{-p^2} \\
&= a_1a_1^{-p^2}a_2[a_2,a_1^{-p^2}] = a_1^{1-p^2}a_2[a_1^{p^2},a_2]^{a_1^{-p^2}} \\
&= a_1^{1-p^2}a_2([a_1,a_2]^{p^2})^{a_1^{-p^2}} = a_1^{1-p^2}a_2([a_1,a_2]^{a_1^{-p^2}})^{p^2} \\
&= a_1^{1-p^2}a_2((a_1^{p^2})^{a_1^{-p^2}})^{p^2} = a_1^{1-p^2}a_2(a_1^{p^2}a_1^{p^2}a_1^{-p^2})^{p^2} \\
&= a_1^{1-p^2}a_2a_1^{p^4} = a_1^{1-p^2}a_2 \ ;
\end{aligned}$$

logo todo elemento de G pode ser escrito na forma normal $a_1^{\alpha_1}a_2^{\alpha_2}$ com $0 \leq \alpha_1 < p^3$ e $0 \leq \alpha_2 < p$ e portanto $|G| = p^4$.)

Usaremos então o NQA para apresentar G segundo uma apresentação consistente por potências e comutadores.

A série p-central inferior de G é

$$G = P_0(G) > P_1(G) > P_2(G) > P_3(G) = \{1\}$$

com

$$\begin{aligned}
P_1(G) &= G^pG' =< a_1^p > \\
P_2(G) &= P_1(G)^p[P_1(G), G] =< a^{p^2} >
\end{aligned}$$

Sabemos que $G/P_1(G)$ é o maior p-grupo quociente abeliano elementar de G. Uma apresentação consistente por potências e comutadores para $G/P_1(G)$ é dada por

$$G/P_1(G) =< a_1, a_2 \ / \ a_1^p = 1,\ a_2^p = 1,\ [a_2, a_1] = 1 >$$

Note que nesta apresentação não há definições ($n = d = 2$), logo, para obter uma apresentação para o p-recobrimento $(G/P_1(G))^*$ de $G/P_1(G)$ é preciso modificar cada uma das relações acima módulo novos geradores centrais de ordem p. Assim, uma apresentação para $(G/P_1(G))^*$ é a seguinte:

$$\begin{aligned}(G/P_1(G))^* =< a_1, a_2, a_3, a_4, a_5 \ / \ & a_1^p = a_3,\ a_2^p = a_4,\ [a_2, a_1] = a_5, \\ & a_3^p = a_4^p = a_5^p = 1, \\ & [a_3, a_1] = [a_3, a_2] = [a_4, a_1] = 1\ , \\ & [a_4, a_2] = [a_5, a_1] = [a_5, a_2] = 1 >\ .\end{aligned}$$

Uma simples avaliação das condições de Wamsley mostra que esta é uma apresentação consistente.

Agora introduzindo as relações de G temos

- $a_1^{p^3} = 1$ que é compatível com as relações acima, pois $a_1^p = a_3$ e $a_3^p = 1$.
- $a_2^p = 1$ que implica $a_4 = 1$, pois $a_2^p = a_4$.
- $a_1^{a_2} = a_1^{1+p^2}$ que implica $a_5 = 1$, pois $[a_1, a_2] = a_1^{p^2} = a_3^p = 1$ e, por outra parte, $[a_1, a_2] = a_5^{-1}$.

Assim, eliminando a_4 e a_5 obtemos uma apresentação consistente por potências e comutadores para $G/P_2(G)$

$$\begin{aligned}G/P_2(G) =< a_1, a_2, a_3 \ / \ & a_1^p = a_3,\ a_2^p = 1,\ a_3^p = 1,\ [a_2, a_1] = 1, \\ & [a_3, a_1] = [a_3, a_2] = 1 >\ .\end{aligned}$$

Calculemos agora uma apresentação consistente por potências e comutadores para $G/P_3(G)$. Para isto calcularemos primeiro uma apresentação para o p-recobrimento, $(G/P_2(G))^*$, de $G/P_2(G)$ modificando novamente as relações acima que não são definições

módulo novos geradores centrais e de ordem p, obtendo assim

$$(G/P_2(G))^* =< a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8 \ / \ a_1^p = a_3,\ a_2^p = a_4,\ a_3^p = a_5,$$
$$a_4^p = a_5^p = a_6^p = a_7^p = a_8^p = 1,$$
$$[a_2, a_1] = a_6,\ [a_3, a_1] = a_7,$$
$$[a_3, a_2] = a_8,\ [a_j, a_i] = 1,$$
$$4 \leq j \leq 8,\ 1 \leq i \leq j-1 >$$

Avaliando agora as condições de associatividade de Wamsley, temos

$$\left.\begin{array}{l}(a_1^p)a_1 = a_3a_1 = a_1a_3[a_3, a_1] = a_1a_3a_7 \\ a_1(a_1^p) = a_1a_3\end{array}\right\}, \quad \text{logo} \quad a_7 = 1$$

$$\left.\begin{array}{lcl}(a_2a_1)a_1^{p-1} & = & (a_1a_2[a_2, a_1])a_1^{p-1} = a_1a_2a_6a_1^{p-1} = a_1a_2a_1^{p-1}a_6 \\ & = & a_1a_1^{p-1}a_2a_6^{p-1}a_6 = a_1^pa_2a_6^p = a_3a_2 = a_2a_3a_8 \\ a_2(a_1^p) & = & a_2a_3\end{array}\right\}, \quad \text{logo} \quad a_8 = 1$$

enquanto as outras condições são compatíveis com as relações acima e, portanto, uma apresentação consistente por potências e comutadores para $(G/P_2(G))^*$ e dada por

$$G/P_2(G) =< a_1, a_2, a_3, a_4, a_5, a_6 \ / \ a_1^p = a_3, a_2^p = a_4,\ a_3^p = a_5,\ a_4^p = a_5^p = 1,$$
$$a_6^p = 1,\ [a_2, a_1] = a_6,\ [a_j, a_i] = 1,$$
$$3 \leq j \leq 6,\ 1 \leq i \leq j-1 > \ .$$

Introduzindo agora as relações de G, temos

- $a_1^{p^3} = 1$ que é compatível com as relações acima, pois $a_1^p = a_3$, $a_3^p = a_5$ e $a_5^p = 1$.
- $a_2^p = 1$ que implica $a_4 = 1$, pois $a_2^p = a_4$.
- $a_1^{a_2} = a_1^{1+p^2}$ que implica $a_6 = a_5^{p-1}$, pois $[a_1, a_2] = a_1^{p^2} = a_3^p = a_5$.

E assim, uma apresentação consistente por potências e comutadores para $G/P_3(G)$ é dada por

$$G/P_3(G) =< a_1, a_2, a_3, a_5 \ / \ a_1^p = a_3, a_2^p = a_5,\ a_3^p = a_5,\ a_5^p = 1,$$
$$[a_2, a_1] = a_5^{p-1},\ [a_3, a_1] = [a_3, a_2] = 1,$$
$$[a_5, a_1] = [a_5, a_2] = 1 > \ .$$

Como sabemos que $P_3(G) = \{1\}$, temos que $G/P_3(G) \cong G$ e, portanto, uma apresentação consistente por potências e comutadores para G é a seguinte:

$$G = < a_1, a_2, a_3, a_4 \quad / \quad a_1^p = a_3, a_2^p = 1, \ a_3^p = a_4, \ a_4^p = 1,$$
$$[a_2, a_1] = a_4^{p-1}, \ [a_3, a_1] = [a_3, a_2] = 1,$$
$$[a_4, a_1] = [a_4, a_2] = 1 > \ .$$

Capítulo 3

Algoritmo para geração de p-grupos

Num artigo de 1977, M.F. Newman deu a descrição teórica de um algoritmo que pode ser usado para gerar descrições de p-grupos finitos. A teoria e implementação desse algoritmo, agora conhecido como *algoritmo para geração de p-grupos*, são descritos por E. O'Brien em O'BRIEN [12].

Neste capítulo estudamos os aspectos teóricos bem como certos detalhes da implementação desse algoritmo. Na seção 3.3 damos um exemplo de aplicação do mesmo, calculando manualmente os 2-grupos 2-gerados de ordem $\leq 2^4$.

Dada uma apresentação finita para G e um primo p, o N.Q.A. constrói, como vimos no capítulo anterior, uma apresentação consistente por potências e comutadores para o maior p-quociente finito de G. O algoritmo para geração de p-grupos desenvolvido por O'Brien é baseado no N.Q.A. e calcula apresentações para extensões particulares de um p-grupo finito, chamadas de descendentes imediatos.

3.1 Aspectos teóricos do Algoritmo

No que segue, G sempre denotará um p-grupo finito, d-gerado, de p-classe c e $G = P_0(G) > P_1(G) > \ldots > P_c(G) = \{1\}$ a sua série p-central inferior.

Definição 3.1.1: Um grupo H é um *descendente de* G se H é d-gerado e o quociente $H/P_c(H)$ é isomorfo a G. Se H é um descendente de G e tem p-classe $c+1$ diremos que H é um *descendente imediato de* G. □

Observação 3.1.2: *É claro que* $H = G$ *é um descendente do grupo abeliano elementar* $\tilde{G} = G/P_1(G)$ *de ordem* p^d.

De fato,

i. *Desde que* G *é um* p*-grupo finito, temos* $P_1(G) = \phi(G)$ (*Proposição* 1.5.7), *logo o número mínimo de geradores de* $H = G$ *e* $\tilde{G} = G/P_1(G)$ *coincidem* (*Teorema* 1.5.8).

ii. *A classe de* $\tilde{G} = G/P_1(G)$ *é* 1 *e tem-se*

$$H/P_1(H) = G/P_1(G) = \tilde{G} .$$

Logo, $H = G$ *é descendente de* $\tilde{G} = G/P_1(G)$. □

Observação 3.1.3: $H = G/P_{i+1}(G)$ *é descendente imediato de* $\tilde{G} = G/P_i(G)$ *para* $1 \leq i \leq c-1$.

De fato,

i. *É claro que* $G/P_j(G)$ *é* d*-gerado para* $1 \leq j \leq c$, *uma vez que* $P_j(G) \leq P_1(G) = \phi(G)$. *Logo* H *e* $\tilde{G}$ *são* d*-gerados.*

ii. *A* p*-classe de* $\tilde{G} = G/P_i(G)$ *é* $c = i$ (*pois pela propriedade* 1.4.5, *temos que* $P_i(G/P_i(G)) = P_i(G)/P_i(G) = \{1\}$ *e* $P_{i-1}(G/P_i(G)) = P_{i-1}(G)/P_i(G) \neq \{1\}$). *E tem-se*

$$\frac{H}{P_c(H)} = \frac{G/P_{i+1}(G)}{P_i(G/P_{i+1}(G))} = \frac{G/P_{i+1}(G)}{P_i(G)/P_{i+1}(G)} \cong \frac{G}{P_i(G)} = \tilde{G} .$$

iii. *A* p*-classe de* $H = G/P_{i+1}(G)$ *é* $c+1 = i+1$. *Logo,* $G/P_{i+1}(G)$ *é descendente imediato de* $G/P_i(G)$, $1 \leq i \leq c-1$. □

Com os resultados das observações 3.1.1 e 3.1.2, é possível calcular G usando um método iterativo para calcular descendentes imediatos a partir do grupo abeliano elementar de posto d.

Já que todo p-grupo pode ser calculado nesta forma, é teoricamente possível obter uma lista completa de todos os p-grupos d-gerados. Na prática, é desejável que esta lista seja ao mesmo tempo completa e irredudante (i.e., um representante de cada tipo de isomorfismo está presente, mas não há dois elementos na lista tendo o mesmo tipo de isomorfismo).

O seguinte teorema é fundamental para a construção de uma tal lista.

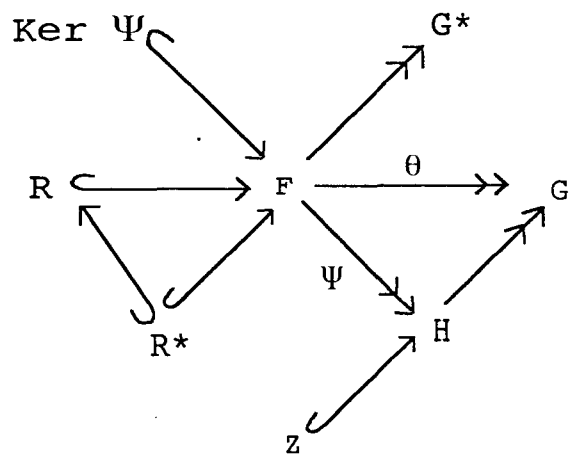
Teorema 3.1.4: *Seja G um p-grupo finito d-gerado. Então existe um grupo G^* d-gerado tal que se H é d-gerado e tem um subgrupo central abeliano elementar Z, com $H/Z \cong G$, então H é uma imagem homomórfica de G^*.*

Demonstração: Seja F o grupo livre de posto d, livremente gerado por $a_1, \ldots, a_d$, i.e. $F = < a_1, \ldots, a_d / >$.

Seja $\theta : F \twoheadrightarrow G$ o epimorfismo natural e $R = \ker\theta$. Defina $R^* = R^p[R,F]$ e $G^* = F/R^*$. Assim, G^* é d-gerado, pois $R^* = R^p[R,F] \leq F^pF'$ e, desde que $R \trianglelefteq F$, temos que $R^* \leq R$.

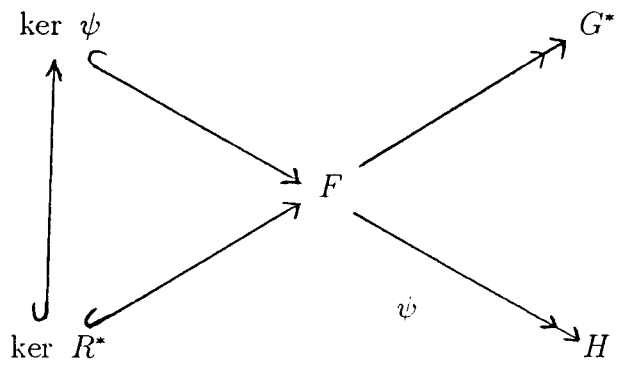
Seja H um grupo d-gerado nas condições acima. Desse modo, temos que o homomorfismo θ pode ser fatorado através de H e o homomorfismo resultante $\psi : F \twoheadrightarrow H$ leva R em Z.

De fato, observe o seguinte diagrama:



Note que $\theta = \psi\eta$, logo $(f)\theta = (f)\psi\eta$, $\forall f \in F$. Assim, se $r \in R = \ker\theta$, então $e_G = (r)\theta = ((r)\psi)\eta$ e, portanto, $(r)\psi \in Z$.

Como Z é abeliano elementar, temos que $(R^p)\psi = ((R)\psi)^p = Z^p = \{e_H\}$ e, por ser Z um subgrupo central de H, temos também que $([R,F])\psi = [(R)\psi,(F)\psi] \leq [Z,H] = \{e_H\}$. Deste modo, temos provado que $(R^*)\psi = \{e_H\}$ e, portanto, temos uma injeção de R^* em $\ker\psi$. A situação obtida é então



e conseqüentemente, pelo teorema 1.1.9, temos que existe um epimorfismo de G^* sobre H. Concluímos assim, que H é uma imagem homomórfica de G^*. ∎

Observação 3.1.5:

i. *Segue-se do teorema acima que todo descendente imediato de G é isomorfo a um quociente de G^*.*

De fato, se H é descendente imediato de G, temos que a p-classe de H é $c+1$, logo $P_c(H)$ é um subgrupo abeliano elementar e central em H, e também $H/P_c(H) \cong G$, segue-se então, pelo teorema acima, que H é isomorfo a um quociente de G^*.

ii. *Como a p-classe de F/R é c, G^* tem p-classe no máximo $c+1$.*

De fato, pela propriedade 1.4.5, *temos*

$$P_c(G^*) = P_c(F/R^*) = \frac{P_c(F)R^*}{R^*} .$$

Além disso, pela propriedade 1.4.7, *temos $P_c(F) \leq R$, pois a p-classe de F/R é c.*

Deste modo, temos que $P_c(G^*) \leq R/R^*$ *e portanto*

$$\begin{aligned} P_{c+1}(G^*) &= (P_c(G^*))^p[P_c(G^*), G^*] \leq (R/R^*)^p\,[R/R^*, F/R^*] \\ &\leq \frac{R^p[R,F]}{R^*} = \{1\} \end{aligned}$$

e conseqüentemente a p-classe de G^* *é no máximo* $c+1$.

□

Lema 3.1.6: *O tipo de isomorfismo de* G^* *depende apenas de* G *e não do subgrupo* R.

Demonstração: Sejam $R_1, R_2 \trianglelefteq F$ tais que

$$F/R_1 = G_1 \cong G_2 = F/R_2 \ .$$

Considere $R_1^*, G_1^*, R_2^*, G_2^*$ como no teorema 3.1.4. Seja $Z_1 = R_1/R_1^*$, logo $G_1^*/Z_1^* \cong G_1$ e Z_1 é abeliano elementar e central em G_1^*. Então pelo teorema 3.1.4, podemos concluir que G_1^* é uma imagem homomórfica de G_2^*. Analogamente, G_2^* é uma imagem homomórfica de G_1^* e assim $G_1^* \cong G_2^*$. ■

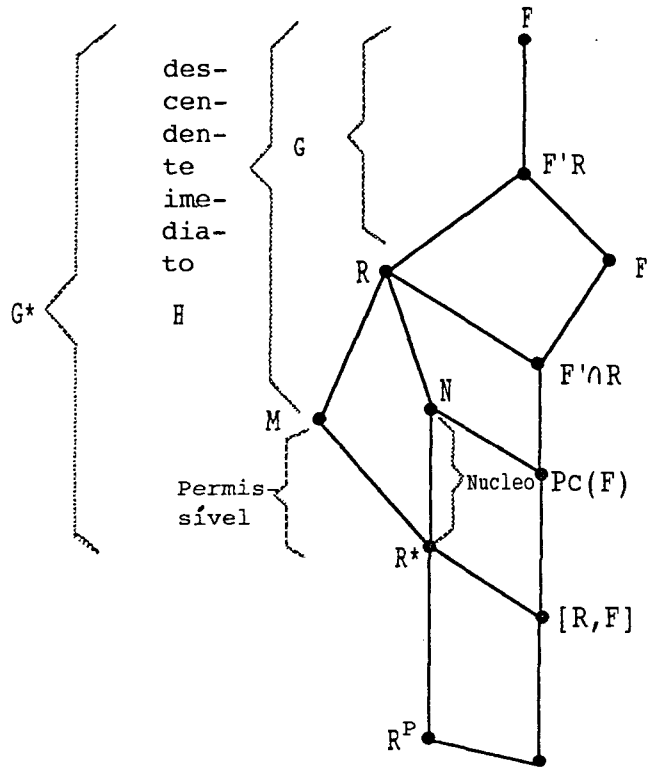
Observação 3.1.7: *Essencialmente, o lema anterior nos diz que* G^* *depende só de* G *e não da particular apresentação deste grupo com a qual trabalhemos.*

Como já dissemos antes, o nosso objetivo será calcular iterativamente descendentes imediatos a partir do grupo abeliano elementar $G/P_1(G)$ *de posto* d. *Desta forma, é claro que os grupos* H, *dos quais calcularemos respectivos* H^*, *são todos p-grupos finitos e portanto têm apresentações por potências e comutadores (proposição* 2.1.1). *Logo, assumiremos daqui em diante que a apresentação dada para* $G \cong F/R$ *é uma apresentação por potências e comutadores e, portanto, teremos sempre* $R \leq P_1(F)$. □

A notação estabelecida no teorema 3.1.4 será usada daqui em diante.

Definição 3.1.8: O grupo $G^* = F/R^*$ é chamado de *p-recobrimento de* $G = F/R$. R/R^* é chamado de *p-multiplicador de* G e $P_c(G^*) = \frac{P_c(F)R^*}{R^*}$ é chamado de *núcleo de* G.

Um *subgrupo permissível* é um subgrupo M/R^* de R/R^* que é o núcleo de um epimorfismo de G^* sobre um descendente imediato de G. □



Dado um grupo G, o primeiro passo no algoritmo de geração é calcular G^*. Uma exigência importante do algoritmo para a construção de descendentes imediatos de G é caracterizar de forma simples os quocientes de G^*. O seguinte resultado é significativo para tais propósitos:

Teorema 3.1.9: *Um subgrupo M/R^* é permissível se, e somente se, é um subgrupo próprio do p-multiplicador de G que complementa o núcleo.*

Demonstração:

$\Rightarrow$) Seja M/R^* um subgrupo permissível, i.e., $M/R^* \leq R/R^*$ é o núcleo de um homomorfismo, digamos Π, de F/R^* sobre um descendente imediato, H, de G. Como G tem p-classe c e H tem p-classe $c+1$, é claro que M é um subgrupo próprio de R (de fato, suponha $M = R$, logo $\ker \Pi = R/R^*$ e assim $H \cong \frac{G^*}{R/R^*} \cong \frac{F/R^*}{R/R^*} \cong F/R = G$, absurdo).

Pela propriedade 1.4.7, temos que $P_c(F) \leq R$ (desde que $R \trianglelefteq F$ e F/R tem p-classe c). Conseqüentemente, $MP_c(F) \leq R$.

Por outro lado, segue do teorema 3.1.4 que $(R)\psi \leq P_c(H)$ (onde $\psi : F \twoheadrightarrow H$ é o epimorfismo natural como antes) e, mais ainda, pela propriedade 1.4.7, temos que $P_c(H) = P_c(F\psi) = P_c(F)\psi \leq R\psi$. Logo,

$$(R)\psi = P_c(H) .$$

Mas $(R)\psi = R/M$, pois $(F)\psi = H \cong \frac{G^*}{M/R^*} \cong \frac{F/R^*}{M/R^*} \cong F/M$. Portanto, $P_c(H) = P_c((F)\psi) = (P_c(F))\psi = \frac{P_c(F)M}{M}$. Assim $R/M = \frac{P_c(F)M}{M}$ e então $R = P_c(F)M$. Logo $\frac{P_c(F)R^*}{R^*}\frac{M}{R^*} = R/R^*$ e como $\frac{P_c(F)R^*}{R^*} = P_c(F/R^*)$ temos $P_c(G^*)\frac{M}{R^*} = R/R^*$, i.e. M/R^* complementa o núcleo de G.

$\Leftarrow$) Reciprocamente, seja $M/R^* < R/R^*$ tal que $P_c(G^*)\frac{M}{R^*} = R/R^*$. Assim $\frac{P_c(F)M}{R^*} = R/R^*$ e, portanto, $\frac{P_c(F)M}{M} = R/M$. Pela propriedade 1.4.5, temos que $P_c(F/M) = \frac{P_c(F)M}{M} = R/M$. Seja $H = F/M$, então H é um quociente de F/R^*, é d-gerado (pois $M \leq R \leq P_1(F)$ pela observação 3.1.7) e o quociente $\frac{H}{P_c(H)} = \frac{F/M}{P_c(F/M)} = \frac{F/M}{R/M} \cong F/R = G$. Portanto H é um descendente de G.

Como $P_c(F/M) = R/M \neq \{1\}$ (pois $M < R$) e

$$P_{c+1}(F/M) = \left(\frac{R}{M}\right)^p \left[\frac{R}{M}, \frac{F}{M}\right] = \frac{R^P[R,F]M}{M} = \frac{R^*M}{M} = \{1\} ,$$

a p-classe de F/M é $c+1$.

Segue-se então que H é um descendente imediato de G e, portanto, M/R^* é um subgrupo permissível. ∎

Definição 3.1.10: Dado um grupo G, diremos que ele é *capaz* se tem descendentes imediatos. Caso contrário diremos que G é *terminal*. □

Observação 3.1.11: *É claro que G é capaz se, e somente se, G^* tem p-classe $c+1$.*

De fato, já vimos que a p-classe de G^* é menor ou igual a $c+1$, mas se G é capaz, seja H um descendente imediato de G, sabemos então que $P_c(H) \neq \{1\}$. Logo, se $\Pi : G^* \twoheadrightarrow H$ é o epimorfismo do teorema 3.1.4, temos que $P_c(G^*) \neq \{1\}$ ($\{1\} \neq P_c(H) = P_c((G^*)\Pi) = (P_c(G^*))\Pi$, pela propriedade 1.4.5) e, portanto, a p-classe de G^* é exatamente $c+1$. □

Observação 3.1.12: *Se G é capaz, tomando os quocientes do grupo G^* pelos seus subgrupos permissíveis obtemos uma lista completa dos descendentes imediatos de G. Esta lista usualmente contém redundâncias. Para eliminá-las, é definida uma relação de equivalência, digamos $\sim$, sobre os subgrupos permissíveis da seguinte forma*

$$M_1/R^* \sim M_2/R^* \quad \textit{se, e somente se,} \quad F/M_1 \cong F/M_2 \ .$$

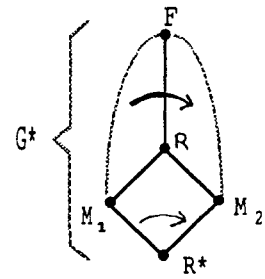
Assim, tomando quocientes de G^* por um representante de cada classe de equivalência, obtem-se uma lista completa e irredundante dos descendentes imediatos de G. □

Na prática, a relação de equivalência acima é útil porque pode ser caracterizada usando-se $\mathrm{Aut}(G)$ (o grupo de automorfismos de G). Cada automorfismo $\alpha \in \mathrm{Aut}(G)$ pode ser estendido a $\alpha^* \in \mathrm{Aut}(G^*)$. A restrição de α^* sobre R/R^* é unicamente determinada por α, e α^* induz uma permutação entre os subgrupos permissíveis. Mostraremos que as classes de equivalência de subgrupos permissíveis são exatamente as órbitas dos subgrupos permissíveis sob a ação destas permutações.

Para isso, estudemos os seguintes resultados:

Teorema 3.1.13: *Sejam M_1/R^* e M_2/R^* subgrupos permissíveis de F/R^*, ambos contidos em R/R^* e seja ϕ um isomorfismo de F/M_1 em F/M_2. Então existe $\alpha^* \in \mathrm{Aut}(G^*)$ tal que*

1. $(M_1/R^*)\alpha^* = M_2/R^*$ *e*
2. *A aplicação de F/M_1 em F/M_2 induzida por α^* coincide com ϕ.*



Demonstração: Usando a propriedade 1.4.5 e a hipótese de M_i/R^* $i = 1,2$ serem permissíveis, temos que

$$R/M_1\phi = P_c(F/M_1)\phi = P_c(F/M_1\phi) = P_c(F/M_2) = R/M_2$$

(já que, se M_i/R^* é permissível, temos pelo teorema 3.1.9 que M_i/R^* complementa o núcleo e portanto $\frac{P_c(F)M}{M} = R/M$ e assim $P_c(F/M) = R/M$ pela propriedade 1.4.5).

Agora, sendo ϕ um isomorfismo de F/M_1 em F/M_2 que leva R/M_1 em R/M_2, temos que ϕ induz um automorfismo, α, sobre F/R.

Escolha um representante $u_i \in F$ da classe lateral $(a_iR)\alpha$; logo $(a_iR)\alpha = u_iR$. Então defina α^* pondo

$$(w(a_1,\ldots,a_d)R^*)\alpha^* := w(u_1,\ldots,u_d)R^* .$$

α^* está bem definida, pois $(R)\alpha = R$ e $R^* = R^p[R,F]$ (já que $(w(a_1,\ldots,a_d)R)\alpha = w(u_1,\ldots,u_d)R$ portanto $w(a_1,\ldots,a_d) \in R$ implica que $w(u_1,\ldots,u_d) \in R^*$; logo se $w(a_1,\ldots,a_d) \in R^*$ tem-se que $w(u_1,\ldots,u_d) \in R^*$).

É claro que α^* é um homomorfismo.

Vejamos agora que α^* é sobrejetor. Temos que α é um automorfismo de F/R e $(a_iR)\alpha = u_iR$, logo $F/R =< u_1R,\ldots,u_dR >$ e conseqüentemente

$$F/R^* =< u_1R^*,\ldots,u_dR^*, R/R^* > .$$

Como estamos supondo $R \leq P_1(F)$ (observação 3.1.7), temos $R/R^* \leq P_1(F/R^*)$ e assim

$$F/R^* =< u_1R^*,\ldots,u_dR^* >=< a_1R^*\alpha^*,\ldots,a_dR^*\alpha^* > .$$

Portanto α^* é um automorfismo de F/R^*.

Embora α^* não seja univocamente determinada por α, a sua restrição a R/R^* o é. De fato, suponha que $a_iR\alpha = u_iR = u_ir_iR = v_iR$ com $r_i \neq 1$, $r_i \in R$. Então temos dois automorfismos de F/R^*, α_1^* e α_2^*,

$$\begin{aligned} \alpha_1^* &: w(a_1,\ldots,a_d)R^* \longmapsto w(u_1,\ldots,u_d)R^* \\ \alpha_2^* &: w(a_1,\ldots,a_d)R^* \longmapsto w(v_1,\ldots,v_d)R^* \end{aligned}$$

Em ambos os casos tem-se $(R/R^*)\alpha_i^* = R/R^*$. Logo, se $w(a_1,\ldots,a_d) \in R$, então $w(u_1,\ldots,u_d) \in R$ e $w(v_1,\ldots,v_d) \in R$. Mas as palavras em R são produtos de potências p-ésimas e comutadores e, já que $[v_j,v_i]R^* = [u_j,u_i]R^*$ e $v_i^pR^* = u_i^pR^*$, segue-se que $w(u_1,\ldots,u_d)R^* = w(v_1,\ldots,v_d)R^*$. Portanto a restrição $\alpha^*|_{R/R^*}$ é univocamente determinada por α.

Seja $\hat{\alpha^*}$ essa restrição.

Se $w(a_1,\ldots,a_d) \in M_1$ e se $(a_iM_1)\phi = b_iM_2$, então

$$w(a_1,\ldots,a_d)R^*\hat{\alpha^*} = w(b_1,\ldots,b_d)R^* .$$

Vejamos agora que $w(b_1,\ldots,b_d) \in M_2$:

$$\begin{aligned} w(b_1,\ldots,b_d)M_2 &= w(b_1M_2,\ldots,b_dM_2) = w(a_1M_1o,\ldots,a_dM_1o) = \\ &= w(a_1,\ldots,a_d)M_1\phi = M_1o = M_2 . \end{aligned}$$

Segue-se então que $(M_1R^*)\hat{\alpha^*}$ é um subgrupo de M_2/R^* e como ambos têm o mesmo índice em F/R^*, pois $F/M_1 \cong F/M_2$, eles são isomorfos, isto é, $(M_1/R^*)\hat{\alpha^*} = M_2/R^*$.

Desta forma, α^* induz um isomorfismo de F/M_1 em F/M_2 e é claro que $(a_iM_1)\theta = (a_iM_1)\phi$ para $i = 1, \ldots, d$. ∎

Lema 3.1.14: *Todo automorfismo α de F/R pode ser estendido a um automorfismo α^* de F/R^*. A restrição de α^* ao p-multiplicador é univocamente determinada por α.*

Demonstração: Segue do teorema 3.1.13, onde ambos M_1/R^* e M_2/R^* são escolhidos sendo R/R^*. ∎

Definição 3.1.15: O automorfismo α^* é chamado de *automorfismo estendido.* □

Lema 3.1.16: *Cada automorfismo estendido α^*, induz uma permutação dos subgrupos permissíveis.*

Demonstração: Como o núcleo, $P_c(F/R^*)$, é característico em G^* (segue da propriedade 1.4.6) e o p-multiplicador, R/R^*, é fixado por α^*, se M/R^* é um subgrupo permissível, temos

$$(M/R^*)\alpha^* P_c(F/R^*) = ((M/R^*)P_c(F/R^*))\alpha^* = (R/R^*)\alpha^* = R/R^*$$

e $M/R^* \lneq R/R^*$, logo $(M/R^*)\alpha^* \lneq R/R^*$.

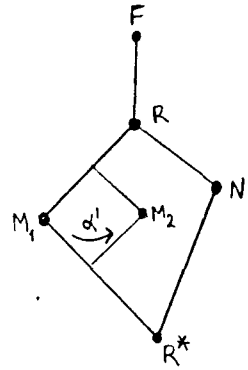
Logo, segue do teorema 3.1.9 que a imagem de um subgrupo permissível é um subgrupo permissível.

É claro que esta aplicação é $1-1$ e sobrejetora, pois α^* é um automorfismo de F/R^*, sendo portanto uma permutação dos subgrupos permissíveis. ∎

Denotemos por α' a permutação de subgrupos permissíveis induzida por α^*. Como no caso da restrição de α^* ao p-multiplicador, α' depende somente do automorfismo α de G.

Seja $\mathcal{P}$ o grupo de permutações gerado pelas α^* correspondentes aos automorfismos α de G. A aplicação $\alpha \mapsto \alpha'$ é um homomorfismo sobrejetor de $\mathrm{Aut}(G)$ em $\mathcal{P}$.

Temos



onde

$$\begin{aligned} \mathcal{P} &= < \alpha' \in \mathrm{Sym}(\Omega)/\alpha \in \mathrm{Aut}(G) > \\ \text{e} \quad \Omega &= \{M/R^* \ / \ R/R^* = P_c(F/R^*)M/R^* \ , M \lneq R\} \end{aligned}$$

O teorema seguinte é fundamental na determinação das classes de equivalência de subgrupos permissíveis.

Teorema 3.1.17: *As órbitas dos subgrupos permissíveis sob a ação de $\mathcal{P}$ são exatamente as classes de equivalência de subgrupos permissíveis. Isto é, $M_1/R^* \sim M_2/R^*$ se, e somente se, $M_2/R^* = (M_1/R^*)\alpha'$, com $\alpha' \in \mathcal{P}$.*

Demonstração: Sejam M_1/R^* e M_2/R^* subgrupos permissíveis na mesma classe de equivalência, logo $F/M_1 \cong F/M_2$ via o automorfismo α. Pelo teorema 3.1.4, existe um automorfismo α^* de F/R^* que leva M_1/R^* em M_2/R^* e α^* induz uma permutação α' em Ω.

Assim, $(M_1/R^*)\alpha' = M_2/R^*$, o que mostra que M_1/R^* e M_2/R^* estão na mesma órbita.

Reciprocamente, sejam M_1/R^* e M_2/R^* subgrupos permissíveis que pertencem à mesma órbita sob $\mathcal{P}$. Então existe uma permutação, digamos α', em Ω tal que $(M_1/R^*)\alpha' = M_2/R^*$.

Esta permutação é induzida por um automorfismo, digamos α^*, de F/R^*, onde $(M_1/R^*)\alpha^* = M_2/R^*$. Assim, temos

$$F/M_2 \cong \frac{F/R^*}{M_2/R^*} \cong \frac{F/R^*}{(M_1/R^*)\alpha^*} \cong \frac{F/R^*}{M_1/R^*} \cong F/M_1$$

Logo M_1/R^* e M_2/R^* pertencem à mesma classe de equivalência. ■

Assim, uma lista completa e irredundante dos descendentes imediatos de G é obtida escolhendo um representante de cada órbita de $\mathcal{P}$ e construindo o correspondente grupo quociente. Cada tal quociente é um representante de um tipo diferente de isomorfismo.

Como já dissemos, dado um p-grupo G, o algoritmo de geração produz uma lista completa e irredundante dos seus descendentes imediatos.

Para calcular iterativamente os descendentes imediatos de G, o algoritmo requer um conjunto gerador para o grupo de automorfismos de cada descendente imediato. A informação dos automorfismos é calculada como parte do algoritmo.

Definição 3.1.18: Se $M/R^* \in \Omega$, definimos o *estabilizador de* M/R^* como o grupo de automorfismos S_{M/R^*} tal que

$$S_{M/R^*} =< \alpha \in \mathrm{Aut}(G) \mid (M/R^*)\alpha' = M/R^* > \ .$$

□

Se $\xi \in S_{M/R^*}$, seja ξ^* uma extensão de ξ a um automorfismo de F/R^*. Então $(M/R^*)\xi^* = (M/R^*)\xi' = M/R^*$, pois $M/R^* \leq R/R^*$ e sabemos que a restrição de ξ^* a R/R^* é univocamente determinada por ξ.

Assim a restrição de ξ^* ao descendente imediato, F/M, de G pode ser calculada.

O grupo de automorfismo de F/M é descrito no seguinte teorema:

Teorema 3.1.19: *Se S consiste das restrições a F/M de uma extensão ξ^* para cada automorfismo ξ em S_{M/R^*} e se V é o grupo de todos os automorfismos de F/M cuja restrição a G é a identidade, então*

$$\mathrm{Aut}(F/M) = SV \ .$$

Demonstração: Seja $\gamma \in \mathrm{Aut}(F/M)$. Pelo teorema 3.1.13, sabemos que γ induz um automorfismo $\alpha \in \mathrm{Aut}(F/R)$ que se estende a um $\alpha^* \in \mathrm{Aut}(F/R^*)$ tal que $(M/R^*)\alpha^* = M/R^*$ e o homomorfismo $\overline{\alpha^*} : F/M \to F/M$, induzido por α^*, coincide com γ.

Sabemos que o efeito de α' em M/R^* é o mesmo de α^*. Logo $\alpha \in S_{M/R^*}$.

Escolha uma extensão $\alpha^* \in \mathrm{Aut}(G^*)$ e tome o automorfismo induzido, $\hat{\alpha}$, sobre F/M. Logo $\hat{\alpha} \in S$.

Agora, por construção, $\overline{\alpha^*}$ e $\hat{\alpha}$ têm a mesma ação induzida sobre $F/R = G$.

Logo, $\hat{\alpha}^{-1}\gamma$ induz a identidade em G, pois $\overline{\alpha^*} = \gamma$, isto é, $\hat{\alpha}^{-1}\phi \in V$.

Portanto, $\gamma = (\hat{\alpha})(\hat{\alpha}^{-1}\gamma) \in SV$ e assim $\mathrm{Aut}(F/M) = SV$. ∎

3.2 Alguns Aspectos da Implementação

Em toda implementação do algoritmo para geração de p-grupos existe uma divisão natural no cálculo de descendentes imediatos de acordo com as suas ordens.

A implementação que descrevemos calcula descendentes imediatos tendo ordem p^{n+s} de um grupo de ordem p^n, aqui s é um inteiro positivo chamado *tamanho de passo*. Os descendentes imediatos de ordem p^{n+s} são chamados *descendentes imediatos de passo s*.

O algoritmo toma como "input" a descrição de um grupo e um conjunto de geradores a o seu grupo de automorfismos e produz um conjunto de descrições para os descendentes imediatos de determinada ordem. As descrições aqui mencionadas são apresentações sistentes por potências e comutadores.

Seja G um grupo tal que:

$$|G| = p^n,\ G \quad \text{é} \quad d-\text{gerado} \quad \text{e a} \quad p-\text{classe de } G \quad \text{é} \quad c.$$

Para calcular descendentes imediatos de ordem p^{n+s}, o algoritmo procede da seguinte forma:

1 – Constrói uma apresentação consistente por potências e comutadores para G^* e determina o núcleo;

2 – Se a ordem do núcleo é menor que p^s, para;

3 – Para cada gerador $\alpha \in \mathrm{Aut}(G)$:

- Calcula α^* o automorfismo estendido;
- Calcula $\alpha' \in \mathcal{P} \subset \mathrm{Sym}(\Omega)$ a permutação de subgrupos permissíveis induzida por α^*;

4 - Calcula as órbitas de subgrupos permissíveis sob a ação de $\mathcal{P}$;

5 - Para cada órbita

- Escolhe um representante, M/R^*;
- Calcula o estabilizador S_{M/R^*};
- Calcula o quociente de G^* pelo representante escolhido para obter um descendente imediato.
- Calcula o grupo de automorfismos do descendente imediato.

No que segue faremos um refinamento dos passos deste algoritmo.

Construção do p-Recobrimento de G e do Núcleo

Dada uma apresentação consistente por potências e comutadores para G, utiliza-se o procedimento descrito no N.Q.A. para obter uma apresentação consistente por potências e comutadores para G^*.

O p-multiplicador, R/R^*, é um grupo abeliano elementar e logo, pode ser visto como um espaço vetorial sobre $\mathbb{F}_p$. Assim, seja $q = \dim_{\mathbb{F}_p} R/R^*$, q será chamado *posto* de R/R^* e é o número mínimo de geradores para R/R^*. Estes geradores, na apresentação consistente de G^*, são denotados por $a_{n+1}, \ldots, a_{n+q}$.

Uma característica da implementação é que os geradores do p-multiplicador são introduzidos em ordem descrescente dos pesos e na adição de geradores de mesmo peso, são adicionados primeiro aqueles que são definidos por comutadores.

O núcleo de G pode ser determinado usando o seguinte resultado.

Lema 3.2.1: *O núcleo de G é gerado por $[a_j, a_i]$ e a_j^P onde a_j é um gerador de peso c, $i \in \{i, \ldots, d\}$ e $i < j$.*

Suponhamos que o núcleo tem posto r, onde $1 \leq r \leq q$. Como os geradores do núcleo tem peso $c+1$, e os geradores são introduzidos em ordem decrescente dos pesos, estes geradores são $a_{n+1}, \ldots, a_{n+r}$.

Cálculo de Automorfismos Estendidos

Dado um conjunto de geradores $\{\alpha_1, \ldots, \alpha_m\}$ para $\mathrm{Aut}(G)$, cada automorfismo α_i é descrito pela sua ação sobre cada um dos geradores $a_1, \ldots, a_d$, de G e *são armazenados os expoentes das imagens de cada um desses geradores sob a ação de cada automorfismo.*

Seja $\alpha \in \{\alpha_1, \ldots, \alpha_m\} \subset \mathrm{Aut}(G)$. Na seção 3.1, vimos que a ação de α sobre os geradores está descrita por $a_i R\alpha = u_i R$ para cada $i \in \{1, \ldots, d\}$, onde u_i é uma palavra nos geradores $a_1, \ldots, a_d$. Mais ainda, a ação de um automorfismo estendido, α^*, sobre os geradores de G^* é dada por $a_i R^* \alpha^* = u_i R^*$ para $i \in \{1, \ldots, d\}$.

Se $\omega(a_1, \ldots, a_{i-1}) =: a_i$ é a definição de a_i para $i \in \{d+1, \ldots, n+q\}$, então definamos o u_i correspondente como $u_i := w(u_i, \ldots, u_{i-1})$. Seja $v(a_1, \ldots, a_d) \in R$, logo $v(u_1, \ldots, u_d) \in R$ e por definição $v(a_1, \ldots, a_d)R^*\alpha^* := v(u_1, \ldots, u_d)R^*$.

Como α^* é um automorfismo e $(R/R^*)\alpha^* = R/R^*$, então

$$u_{n+i}R^* = (a_{n+i}R^*)\alpha^* = (a_{n+1}^{\delta_{i1}} \ldots a_{n+q}^{\delta_{iq}})R^* \quad \text{com} \quad 0 \leq \delta_{ij} < p$$

e portanto $u_{n+i} = a_{n+1}^{\delta_{i1}} \ldots a_{n+q}^{\delta_{iq}} (\mathrm{mod} R^*)$ para $i \in \{1, \ldots, q\}$.

A ação de cada automorfismo estendido sobre o p-multiplicador de G é armazenada como uma matriz para facilitar o cálculo das imagens dos subgrupos permissíveis.

A ação de α^* sobre cada gerador a_{n+i} é escrita como um vetor $1 \times q$ cujas entradas são os expoentes δ_{ij} da imagem de a_{n+i} por α^*. Os q vetores são armazenados como uma matriz $q \times q$.

Definição 3.2.2: A matriz definida acima é dita *matriz do automorfismo* α^* e denotada A_{α^*}. □

Um Método para Representar Subgrupos Permissíveis

Os subgrupos permissíveis para um tamanho de passo fixado s, onde $1 \leq s \leq r$, são conhecidos como *subgrupos permissíveis de passo* s e o grupo gerado pelas permutações induzidas sobre eles será denotado por $\mathcal{P}$.

Pelo teorema 3.1.9, os subgrupos permissíveis são aqueles subgrupos do p-multiplicador tendo ordem p^{q-s} e completando o núcleo. De fato:

q = posto de R/R^*, i.e.: $|R/R^*| = p^q$.

$$\left|\frac{F}{M}\right| = p^{n+1} \quad \text{e} \quad \frac{F}{R} \simeq \frac{F/M}{R/M} \quad \text{logo} \quad |R/M| = p^s$$

Portanto $\left|\frac{M}{R^*}\right| = \frac{|R/R^*|}{|R/M|} = p^{q-s}$. Mais ainda:

$$r = \quad \text{posto de} \quad \frac{N}{R^*}, \quad \text{i.e.:} \quad \left|\frac{N}{R^*}\right| = p^r.$$

Logo, $|\frac{N \cap M}{R^*}| = p^{r-s}$ e assim, $\left|\frac{M}{N \cap M}\right| = \left|\frac{M/R^*}{N \cap M/R^*}\right| = p^{q-s-(r-s)} = p^{q-r}$.

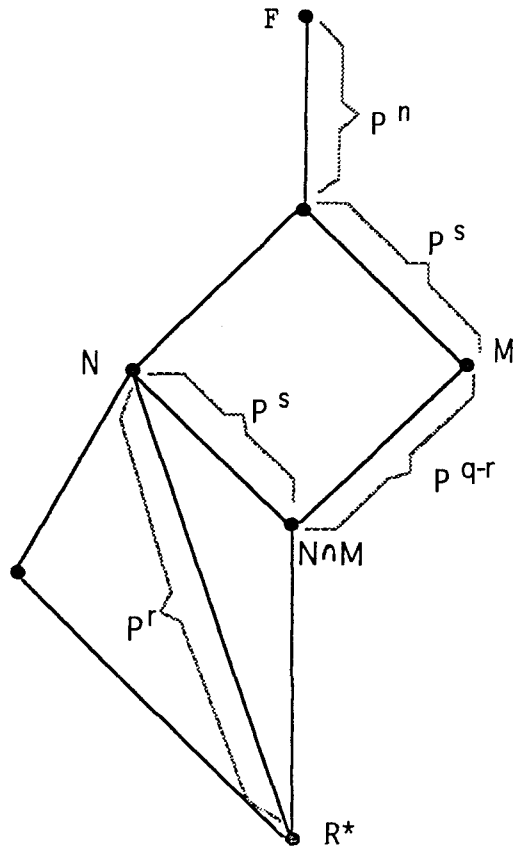


Fig. I

Seguindo a notação da álgebra linear, diremos que o posto de um subgrupo de ordem p^{q-s} é $q - s$.

Assim, os subgrupos permissíveis de passo s são os subespaços de posto $q - s$ que complementam o subespaço fixo de posto r num espaço de dimensão q.

Observação 3.2.3: *Existe uma correspondência* $1-1$ *entre os subgrupos permissíveis de passo* s *e algumas matrizes* $s \times q$ *escalonadas à esquerda.*

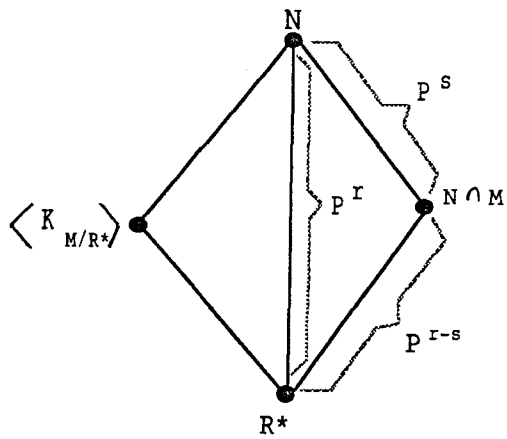
De fato:

Seja M/R^* *um subgrupo permissível de passo* s. *Lembre que o núcleo,* N/R^*, *tem base* $\{a_{n+1}, \ldots, a_{n+r}\}$. *Sabemos que* $\left|\frac{N}{R^*} \cap \frac{M}{R^*}\right| = p^{r-s}$, *logo o posto de* $\frac{N}{R^*} \cap \frac{M}{R^*}$ *é* $r-s$.

Defina $U = M/R^*$ *e* $K_{M/R^*} = \phi$.

Se $< U, a_{n+1} > \neq U$, *defina* $K_{M/R^*} = K_{M/R^*} U\{a_{n+1}\}$, $U =< U, a_{n+1} >$ *e repita o processo com cada* $a_{n+2}, \ldots, a_{n+r}$ *até obter os* s *elementos de* $\{a_{n+1}, \ldots, a_{n+r}\}$ *que junto com a interseção,* $\frac{N}{R^*} \cap \frac{M}{R^*}$, *geram* $\frac{N}{R^*}$.

Note que, no j*-ésimo passo, o subgrupo é* $< U, a_{n+j} >$ *e* $K_{M/R^*} = \{a_{n+k}, \ldots, a_{n+ki}\}$ *onde cada* $k_\ell < j$. *Se* $< U, a_{n+j} > \neq U$ *então adicione* a_{n+j} *a* K_{M/R^*}; *se não, temos que* $a_{n+j} = \omega a_{n+k_1}^{\xi_1} \ldots a_{n+k_i}^{\xi_i}$ *onde* $\omega \in M/R^*$ *e* $0 \leq \xi_\ell < p$.



Definição 3.2.4: O conjunto $K_{M/R^*} = \{a_{n+k_1}, \ldots, a_{n+k_s}\}$, com cada $k_i \leq r$ descrito acima é chamado *conjunto definidor de* M/R^*. □

Seja $\theta : \frac{R}{R^*} \longrightarrow < K_{M/R^*} >$ *a transformação linear entre estes espaços vetoriais de dimensões* q *e* s *respectivamente tal que:*

$$(a_{n+j})\theta = \begin{cases} a_{n+j} & \text{se } a_{n+j} \in K_{M/R^*} \\ a_{n+k_1}^{\xi_1} \ldots a_{n+k_s}^{\xi_s} & \text{onde } \xi_\ell = 0 \text{ se } k_\ell > j; \text{ se } a_{n+j} \notin K_{M/R^*} \end{cases}$$

(*Note que se* $1 \leq j \leq r$ *e* $a_{n+j} \notin K_{M/R^*}$, *pela observação anterior, temos que* $a_{n+j} = \omega a_{n+k}^{\xi_s}$ *com* $\omega \in \frac{M}{R^*}$ *e* $k_1, \ldots k_i < j$ $0 \leq \xi_i < p$. *Agora se* $r < j \leq q$ (*portanto*

$a_{n+j} \notin K_{M/R^*}$), *temos também que* $a_{n+j} \in \frac{M}{R^*} < K_{M/R^*} >$, *logo* $a_{n+j} = \omega a_{n+k_1}^{\xi_1} \ldots a_{n+k_s}^{\xi_s}$, *com* $\omega \in M/R^*$, $0 \leq \xi_i < p$).

Assim, temos que $\ker\theta = \dfrac{M}{R^*}$.

A matriz de θ *relativa à base* $\{a_{n+1}, \ldots, a_{n+q}\}$ *é uma matriz* $s \times q$ *escalonada à esquerda e a submatriz* $s \times r$ *correspondente às* r *primeiras colunas tem posto* s (*segue da definição*).

Assim, cada subgrupo permissível pode ser identificado com uma matriz $s \times q$, *escalonada à esquerda cuja submatriz* $s \times r$ *correspondente às* r *primeiras colunas, tem posto* s.

Definição 3.2.5: A matriz acima definida é chamada *matriz padrão* do subgrupo permissível M/R^*. □

Reciprocamente, dada uma matriz $s \times q$, *escalonada à esquerda e cuja submatriz* $s \times r$ *correspondente às* r *primeiras colunas tem posto* s, *esta define uma transformação linear de* R/R^* (*com a sua base usual*) *num espaço de dimensão* s *e o núcleo dessa transformação é um subgrupo permissível de passo* s. □

Os subgrupos permissíveis são construídos como núcleos ao invés de imagens pois dessa maneira, são representados por matrizes $s \times q$ em vez de matrizes $(q - s) \times q$, já que na prática o valor de s é pequeno e geralmente menor do que $q - s$.

Um conjunto definidor é um subconjunto ordenado de s elementos do conjunto $\{a_{n+1}, \ldots, a_{n+r}\}$ também ordenado. O número de tais subconjuntos é $\binom{r}{s}$. Definamos entre os conjuntos definidores, a seguinte relação de ordem, conhecida como *ordem lexicográfica.*

Definição 3.2.6: Sejam K e K^* dois conjuntos definidores, então $K > K^*$ se existe um $\ell \in \{1, \ldots, s\}$ tal que $k_\ell > k_\ell^*$ e $k_i = k_i^*$ para $1 \leq i < \ell$. □

Assim, os conjuntos definidores são escolhidos na ordem lexicográfica e todos os subgrupos permissíveis determinados por um conjunto definidor particular serão também ordenados.

Para descrever explicitamente as permutações dos subgrupos permissíveis, associaremos a cada matriz padrão, e portanto a cada subgrupo permissível, uma *etiqueta (ou rótulo)* que estabelecerá essa ordem que mencionamos acima.

A base de cada subgrupo permissível, consistindo de $q-s$ geradores, é obtida escolhendo um conjunto definidor, digamos $K = \{a_{n+k_1}, \ldots, a_{n+k_s}\}$, do conjunto dos r geradores do núcleo.

Seja $a_{n+j} \in (\{a_{n+1}, \ldots, a_{n+q}\} - K)$. Defina o seguinte elemento h_j assim:

$$h_j = a_{n+k_1}^{\xi_{1j}} \ldots a_{n+k_s}^{-\xi_{sj}} a_{n+j}$$

onde para cada $a_{n+\ell} \in K$:

$$\xi_{\ell j} \in \begin{cases} \{0, 1, \ldots, p-s\} & \text{se } k_\ell < j\ . \\ \{0\} & \text{em outro caso.} \end{cases}$$

Esses $q-s$ elementos, h_j para $a_{n_j} \notin K$, geram um subgrupo permissível de passo s.

Considere as matrizes padrões dos subgrupos permissíveis determinadas pelo conjunto definidor escolhido. Os elementos de K determinam as posições daquelas entradas da matriz padrão cujos valores são fixos 0 ou 1 e aquelas cujos valores pertencem ao conjunto $\{0, \ldots, p-1\}$.

Estas últimas posições são as posições que chamaremos *disponíveis.*

O número de posições disponíveis na linha ℓ de qualquer dessas matrizes é $q - k_\ell - (s - \ell)$. De fato:
Seja $K = \{a_{n+k_1}, \ldots, a_{n+k_\ell}\}$ um subconjunto ordenado de $\{a_{n+1}, \ldots, a_{n+q}\}$ (base de R/R^*) e sejam $\theta : R/R^* \rightarrowtail\!\!\!\!\rightarrow < K >$ a transformação linear tal que

$$(\mathrm{a_{n+j}})\theta = \begin{cases} a_{n+j} & \text{se } a_{n+j} \in K \\ a_{n+k_1}^{\xi_{1j}} \ldots a_{n+k_s}^{\xi_{1j}} & \text{onde } \xi_{ij} \in \left\{ \begin{array}{ll} \{0, 1, \ldots, p-1\} & \text{se } k_x < j \\ \{0\} & \text{em outro caso} \end{array} \right\}, \text{ se } a_{n+j} \notin K, \end{cases}$$

e S a matriz de θ relativa à base $\{a_{n+1}, \ldots, a_{n+q}\}$.

Para cada $\ell \in \{1, \ldots, s\}$ sabemos que $k_\ell \geq \ell$. Notemos que s dos elementos que aparecem na linha ℓ correspondem a 0 o 1 pois correspondem às colunas imagens dos elementos de K. Agora, seja $\ell < j < k_\ell$, tal que $a_{n+j} \notin K$, logo o expoente de a_{n+k_ℓ} em

$(a_{n+j})\theta$ é 0 e é claro que há $k_\ell - \ell$ elementos $a_{n+j} \notin K$ tal que $\ell < j < k_\ell$ portanto temos que as posições disponíveis na linha ℓ são $q - s - (k_\ell - \ell) = q - k_\ell - (s - \ell)$.

Uma forma de contar o número de subgrupos permissíveis tendo K como conjunto definidor é contar o número de posições disponíveis. Assim, o número de subgrupos permissíveis determinados por K é $p^{\mathcal{X}(K)}$ onde

$$\begin{aligned} \mathcal{X}(K) &= \sum_{\ell=1}^{s} q - k_\ell - (s - \ell) \quad \text{i.e.,} \\ \mathcal{X}(K) &= qs - \left(\sum_{\ell=1}^{s} k_\ell\right) - \frac{s(s-1)}{2}. \end{aligned}$$

O número total de subgrupos permissíveis, ou equivalentemente, o grau, D, do grupo de permutações $\mathcal{P}$ é:

$$D = \sum_{K} p^{\mathcal{X}(K)}$$

Portanto, a etiqueta que associaremos com cada subgrupo permissível é um inteiro positivo em $\{1, \ldots, D\}$.

Seja M/R^* um subgrupo permissível. Seja $S = (\xi_{ij})$ a sua matriz padrão e $K = \{k_1, \ldots, k_s\}$ o seu conjunto definidor. A etiqueta para S tem duas componentes. A primeira é: $0_K = \sum_{K^* < K} p^{\mathcal{X}(K^*)}$, o número de matrizes padrões determinados pelos conjuntos definidores que precedem K na ordem linear.

A segunda componente é a posição de S relativa a K. A *função posição* é definida sobre as posições disponíveis no conjunto $\{0, \ldots, \mathcal{X}(K) - 1\}$. O valor 0 é assignado à posição disponível mais à esquerda da primeira linha da matriz, o valor assignado vai crescendo através das posições disponíveis em cada linha, o valor $\mathcal{X}(K) - 1$ é assignado à posição disponível mais à direita na última linha tendo posições disponíveis.

Seja $y(i,j)$ o valor da função posição para a posição disponível (i,j) em S. Mais formalmente, $y(i,j)$ é dada pela seguinte equação:

$$y(i,j) = \sum_{\ell=1}^{i} (q - k_\ell - (1 - \ell)) - |\{t \ / \ j \leq t \leq q,\ n + t \notin K\}|.$$

A etiqueta L para S é definida então da seguinte forma:

$$L = 0_K + \sum_{i=1}^{s} \sum_{j} \xi_{ij} p^{y(i,j)} + 1$$

onde ξ_{ij} é a entrada (i,j) de S e, para cada i, a segunda soma é sobre os j tais que $k_i < j \leq q$ e $j \notin K$.

Para ilustrar esta ordenação das matrizes padrões suponhamos $q = 4$, $s = 2$ e vejamos como são ordenadas as matrizes correspondentes ao primeiro conjunto definidor (i.e., o conjunto dos dois primeiros geradores de R/R^*). É claro que tais matrizes tem 4 posições disponíveis e que as duas primeiras colunas de cada uma são os vetores $\binom{1}{0}$ e $\binom{0}{1}$ respectivamente.

Elas são, na ordem definida acima

$$S_1 = \left(I \middle| \frac{0 \mid 0}{0 \mid 0}\right); \quad S_2 = \left(I \middle| \frac{1 \mid 0}{0 \mid 0}\right); \quad S_3 = \left(I \middle| \frac{2 \mid 0}{0 \mid 0}\right); \quad \ldots, \quad S_p = \left(I \middle| \frac{p-1 \mid 0}{0 \mid 0}\right)$$

$$S_{p+1} = \left(I \middle| \frac{0 \mid 1}{0 \mid 0}\right); \quad S_{p+2} = \left(I \middle| \frac{1 \mid 1}{0 \mid 0}\right); \quad S_{p+3} = \left(I \middle| \frac{2 \mid 1}{0 \mid 0}\right); \quad \ldots, \quad S_{2p} = \left(I \middle| \frac{p-1 \mid 0}{0 \mid 0}\right)$$

$$\ldots, \quad S_{p^2} = \left(I \middle| \frac{p-1 \mid p-1}{0 \mid 0}\right); \quad S_{p^2+1} = \left(I \middle| \frac{0 \mid 0}{1 \mid 0}\right); \quad \ldots,$$

$$\ldots, \quad S_{p^4} = \left(I \middle| \frac{p-1 \mid p-1}{p-1 \mid p-1}\right).$$

Cálculo de Permutações

As etiquetas foram colocadas para facilitar o cálculo das permutações de subgrupos permissíveis.

Seja $\alpha \in \mathrm{Aut}(G)$, lembre que a ação de α^* sobre R/R^* é representada pela matriz automorfismo, $q \times q$, $A_{\alpha^*} = (\delta_{ij})$, $\delta_{ij} \in \{0, \ldots, p-1\}$ i.e., usando notação aditiva:

$$a_{n+i}\alpha^* = \sum_{j=1}^{q} \delta_{ij} a_{n+j}$$

A relação de equivalência definida entre os subgrupos permissíveis fornece uma relação de equivalência sobre as matrizes padrão.

Lembre que um subgrupo permissível M/R^* é o núcleo de uma aplicação θ do p-multiplicador no espaço que tem como base o conjunto definidor de M/R^* e a matriz dessa transformação é a matriz padrão, S.

Isto é: $\alpha^* \in \mathrm{Aut}(F/R^*)$, $\theta : R/R^* \twoheadrightarrow < K_{M/R^*} >$ e $\ker\theta = M/R^*$.

Seja $\alpha^*\theta : R/R^* \longrightarrow < K_{M/R^*} >$ a composição de α^* com θ nesta ordem. Vejamos que $\ker(\alpha^*\theta) = \left(\frac{M}{R^*}\right)(\alpha^*)^{-1}$:

$$\begin{aligned}
\ker(\alpha^*\theta) &= \{x \in R/R^* \ / \ x\alpha^*\theta = o\} \\
&= \{x \in R/R^* \ / \ x\alpha^* \in \ker\theta\} \\
&= \{x \in R/R^* \ / \ x\alpha^* \in M/R^*\}
\end{aligned}$$

Portanto, $\ker(\alpha^*\theta) = (M/R^*)(\alpha^*)^{-1}$.

Vejamos agora que a matriz do produto $\alpha^*\theta$ é $SA^t_{\alpha^*}$, de fato:
Seja a_{n+i} um elemento da base de R/R^*, logo:

$$\begin{aligned}
(a_{n+i}\alpha^*)\theta &= (\sum_{j=1}^{q}\delta_{ij}a_{n+j})\theta \\
&= \sum_{j=1}^{q}\delta_{ij}(a_{n+j}\theta) \\
&= \sum_{j=1}^{q}\delta_{ij}\sum_{\ell=1}^{s}\xi_{\ell j}a_{n+k_\ell} \\
&= \sum_{\ell=1}^{s}\Big(\sum_{j=1}^{q}\xi_{\ell j}\delta_{ij}\Big)a_{n+k_\ell}
\end{aligned}$$

e note agora que $\sum_{j=1}^{q}\xi_{\ell j}\delta_{ij}$ é a entrada (ℓ, i) da matriz $(SA^t_{\alpha^*})$.

Considere agora a matriz $SA^t_{\alpha^*}$ $(s \times q)$. A submatriz $s \times r$ de S correspondente às r primeiras colunas tem posto s. Como α^* é um automorfismo, as r primeiras colunas correspondem aos vetores do núcleo, N/R^*, e o núcleo é característico, temos então que a submatriz $s \times r$ de $SA^t_{\alpha^*}$ correspondente às r primeiras colunas tem posto s.

Uma matriz inversível, $s \times s$, corresponde a um automorfismo de $< K_{M/R^*} >$ e consequentemente não muda o núcleo de θ. Portanto o escalonamento de $SA^t_{\alpha^*}$ produz a única matriz padrão de $(M/R^*)(\alpha^*)^{-1}$.

É claro que as permutações de subgrupos permissíveis induzidas pelas inversos dos automorfismos $\alpha_1^*, \ldots, \alpha_m^*$ geram o mesmo grupo que $\alpha_1^*, \ldots, \alpha_m^*$.

Portanto, tome o menor conjunto de matrizes $s \times q$ contendo S e fechado para a multiplicação à direita por $A^t_{\alpha_1^*}, \ldots, A^t_{\alpha_m^*}$. O escalonamento das matrizes deste conjunto

dá exatamente as matrizes padrões correspondentes aos subgrupos permissíveis na órbita de M/R^*.

Na prática, calcula-se o produto $A_\alpha \cdot S^t$ e a sua transposta é escalonada à esquerda. A etiqueta da matriz padrão assim obtida é calculada e armazenada. Deste modo, a implementação constrói a inversa da permutação induzida pelo automorfismo estendido α^*.

As etiquetas das matrizes que representam subgrupos permissíveis foram arranjadas de modo tal que o produto das matrizes pode ser obtido adicionando as colunas da matriz automorfismo.

Se A é uma matriz $q \times q$ e v um vetor $1 \times q$, o produto $A(v_1, \ldots, v_q)^t$ é igual a $A_1 v_1 + \ldots + A_q v_q$ onde A_i é a i-ésima coluna de A.

Vejamos melhor num exemplo. Suponhamos $s = 2$; $p \neq 2$.

As matrizes padrões são processadas por ordem crescente das suas etiquetas, assim, o primeiro conjunto definidor escolhido é $\{a_{n+1}, a_{n+2}\}$. A matriz padrão, S_1, correspondente ao subgrupo permissível com etiqueta 1 é:

$$S_1 = \begin{pmatrix} 100\ldots0 \\ 010\ldots0 \end{pmatrix}$$

O produto $AS_1^t = (A_1 \mid A_2)$.
Agora, a matriz padrão, S_2, correspondente ao subgrupo permissível com etiqueta 2 é:

$$S_2 = \begin{pmatrix} 1010\ldots0 \\ 0100\ldots0 \end{pmatrix}$$

Neste caso, $AS_2^t = (A_1 + A_3 \mid A_2)$, i.e., pode ser obtida somando a coluna A_3 à coluna A_1.

E assim, por exemplo para obter AS_3^t basta com somar a coluna A_3 à soma $A_1 + A_3$. (De fato $S_3 = \binom{1020\ldots0}{0100\ldots0}$ e portanto $AS_3^t = (A_1 + 2A_3 \mid A_2)$).

Cálculo de Descendentes Imediatos e o Respectivo Grupo de Automorfismos

Uma vez escolhido um representante de cada órbita de subgrupos permissíveis, estes são listados na ordem crescente das suas etiquetas. Esta lista determina a seqüência na qual serão produzidos os descendentes imediatos.

Discutiremos agora a descrição do grupo de automorfismos requerido para a iteração do algoritmo.

Se um descendente imediato for terminal, não precisaremos descrever seu grupo de automorfismos, portanto para um melhor aproveitamento da memória, só as descrições dos grupos de automorfismos de grupos capazes serão armazenados num arquivo. Assim, o p-recobrimento de cada descendente imediato, H, é construído e é determinado o posto do seu núcleo. Se H é capaz, o grupo de automorfismos de H é calculado segundo o teorema 3.1.19.

A performance da implementação depende fortemente do número de geradores do grupo de automorfismos já que cada um deles determina uma permutação que deve ser construída e também afeta o tempo gasto no cálculo das órbitas. Notemos então que se a ação de um automorfismo estendido, α^*, é trivial sobre o p-multiplicador, este induz uma permutação trivial sobre os subgrupos permissíveis (já que $A_{\alpha^*} = I_d$ e logo $A_{\alpha^*}S^t = S^t$) e portanto não tem papel nenhum no cálculo das órbitas de subgrupos permissíveis.

É importante então levar em consideração o seguinte resultado:

Lema 3.2.7: *As extensões de automorfismos internos de G agem trivialmente sobre o p-multiplicador.*

Demonstração: Pela definição do automorfismo induzido, temos que se $a_iR\alpha = u_iR$, então $a_iR^*\alpha^* = u_iR^*$ para $i \in \{1, \ldots, d\}$ e, dada $\omega(a_1, \ldots, a_d)$, uma palavra nos geradores essenciais $a_1, \ldots, a_d$, temos:

$$\omega(a_1, \ldots, a_d)R^*\alpha^* = \omega(u_1, \ldots, u_d)R^*.$$

Agora, se $\alpha \in I_{nn}(G)$, digamos conjugação por um $g \in G$, então

$$a_i\alpha = a_i^g = a_i[a_i, g] = u_i.$$

Como $[a_i, g] \in [R, F]R^p$, tem-se que $u_i = a_i \pmod{R^*}$. Logo a ação de α^* é trivial em R/R^*. ∎

Assim, quando o grupo de automorfismos de um descendente imediato H é calculado, a implementação descarta os automorfismos internos induzidos pelos geradores de

peso c em H.

Teorema 3.2.8: *O grupo V, do teorema 3.1.19, tem como conjunto de geradores o conjunto $\{\theta_{ij}/i \in \{1,\ldots,d\},\ j \in \{1,\ldots s\}\}$ onde cada θ_{ij} é definido como segue*

$$\begin{aligned} \theta_{ij} : a_i &\mapsto a_i a_{n+j} \\ a_k &\mapsto a_k \quad para \quad k \in \{1,\ldots,d\} - \{i\}. \end{aligned}$$

Demonstração: V é o grupo de todos os automorfismos de F/M cuja restrição a G é a identidade, i.e., $\theta \in V$ se, e somente se, $\theta \in \mathrm{Aut}(F/M)$ e $\theta|_G = id_G$.

Sabemos que $F/M =< a_1,\ldots,a_d >$ e $R/M =< a_{n+1},\ldots,a_{n+s} >$, portanto, um automorfismo, θ, nas condições acima é tal que:

$$a_i\theta = a_i u_i \quad \text{para} \quad i \in \{1,\ldots,d\} \quad \text{onde} \quad u_i = a_{n+j_1}\ldots a_{n+j_{k_i}} \in < a_{n+1},\ldots,a_{n+s} > .$$

Logo, segue-se facilmente que

$$\theta = \prod_{i=1}^{d} (\theta_{ij_1}\ldots\theta_{ij_{k_i}})$$

com $1 \leq j_1,\ldots,j_{k_i} \leq s\ \forall i \in \{1,\ldots,d\}$. ∎

3.3 Um exemplo

Obtemos aqui todos os 2-grupos 2-gerados de ordem $\leq 2^4$. Para isso, construimos os descendentes imediatos do 2-grupo abeliano elementar 2-gerado conforme foi estudado na seção 3.1 e ilustramos os aspectos da implementação descritos na seção 3.2.

Seguindo a notação usada até agora, sejam:

$$p = d = 2 \quad \text{e} \quad F =< a_1, a_2/ > \quad \text{o grupo livre} \quad 2 - gerado.$$

Logo o 2-grupo abeliano elementar, G, pode ser descrito como F/R onde R é o fecho normal em F do conjunto $\{a_1^2, a_2^2, [a_2, a_1]\}$ (i.e., $R =< \{a_1^2, a_2^2, \{a_1^2, a_2^2, [a_2, a_1]\} >^F$), temos assim a seguinte apresentação por potências e comutadores para G:

$$G =< a_1, a_2/a_1^2 = 1,\ a_2^2 = 1,\ [a_2, a_1] = 1 >$$

Construção de G^* e $P_1(G^*)$

O primeiro passo é a construção de uma apresentação consistente por potências e comutadores para o p-recobrimento de G, G^*, onde $G^* \cong F/R^*$ com $R^* = R^p[R,F]$. Para isso, segundo foi estudado no capítulo 2, é preciso modificar cada uma das relações de G módulo novos geradores centrais e de ordem 2.

Observação: *Introduzimos primeiro o gerador definido pelo comutador* $[a_2, a_1]$ *e logo os correspondentes às potências* a_1^2, a_2^2, *já que todos eles tem peso* 2. □

Desta forma obtemos a seguinte apresentação:

$$G^* =< a_1, a_2, a_3, a_4, a_5 \ / \ [a_2,a_1] = a_3,\ a_1^2 = a_4,\ a_2^2 = a_5,\ a_3^2 = a_4^2 = a_5^2 = 1,$$
$$[a_3,a_1] = [a_3,a_2] = [a_4,a_2] = [a_5,a_1] = [a_5,a_2] = 1 >$$

a qual é uma apresentação consistente por potências e comutadores para G^* (todas as condições de Wamsley são satisfeitas).

Notemos então que o p-multiplicador, R/R^*, está gerado por $a_3 := [a_2, a_1]$; $a_4 := a_1^2$ e $a_5 := a_2^2$.

Agora, pelo Lema 3.2.1, temos que o núcleo de G, $P_1(G^*)$, é gerado por $a_3 := [a_2, a_1]$; $a_4 := a_1^2$ e $a_5 := a_2^2$.

Assim, $|P_1(G^*)| = p^3$ e portanto G tem descendentes imediatos de passos $s = 1$, $s = 2$ e $s = 3$.

Cálculo dos automorfismos estendidos

O passo seguinte é então calcular geradores para $\mathrm{Aut}(G)$ e para cada um desses geradores, digamos α, o correspondente $\alpha^* \in \mathrm{Aut}(G^*)$. Notemos que $G \cong V$ (onde V é o grupo de Klein) e logo, pela propriedade 1.6.10 (a), sabemos que

$$\mathrm{Aut}(G) \cong \mathrm{Aut}(V) \cong S_3 \cong < x_1, x_2 / x_1^2 = 1,\ x_2^2 = 1,\ (x_1, x_2)^3 = 1 > .$$

Sejam $\beta_{11}, \beta_{12} \in \mathrm{Aut}(G)$ como segue:

$$\beta_{11}: \begin{array}{l} a_1 \mapsto a_1 \\ a_2 \mapsto a_1 a_2 \end{array} \quad ; \quad \beta_{12}: \begin{array}{l} a_1 \mapsto a_1 a_2 \\ a_2 \mapsto a_2 \end{array}$$

Verifica-se facilmente que $\beta_{11}^2 = \beta_{12}^2 = (\beta_{11}\beta_{12})^3 = I_d$, logo existe, pelo teorema 1.1.9, um epimorfismo $\theta : \mathrm{Aut}(G) \to H$, onde

$$H =< \beta_{11}, \beta_{12} \;/\; \beta_{11}^2 = I_d, \beta_{12}^2 = I_d, (\beta_{11}\beta_{12})^3 = I_d > \leq \mathrm{Aut}(G)$$

e conseqüentemente $\mathrm{Aut}(G) \cong H$, pois $|\mathrm{Aut}(G)| = |H| = 6$.

Passemos então ao cálculo dos automorfismos estendidos. Para calcular as matrizes dos automorfismos estendidos, basta calcular as imagens de a_3, a_4, a_5 por cada β_{1i}, $i = 1, 2$ e armazenar num vetor 1×3 os expoentes de cada uma delas como segue:

$$\begin{aligned}
a_3^{\beta_{11}^*} &= [a_2, a_1]^{\beta_{11}} = [a_2^{\beta_{11}}, a_1^{\beta_{11}} = [a_1, a_2, a_1] = [a_2, a_1] = a_3 \\
a_4^{\beta_{11}^*} &= (a_1^2)^{\beta_{11}} = (a_1^{\beta_{11}})^2 = a_1^2 = a_4 \\
a_5^{\beta_{11}^*} &= (a_2^2)^{\beta_{11}} = (a_2^{\beta_{11}})^2 = (a_1a_2)^2 = a_1^2a_2^2[a_2, a_1] = a_4, a_5, a_3 = a_3, a_4a_5
\end{aligned}$$

Portanto, $A_{\beta_{11}^*} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$.

$$\begin{aligned}
a_3^{\beta_{12}^*} &= [a_2, a_1]^{\beta_{12}} = [a_2, a_1a_2] = [a_2, a_1]^{a_2} = a_3^{a_2} = a_3 \\
a_4^{\beta_{12}^*} &= (a_1^2)^{\beta_{12}} = (a_1^{\beta_{12}})^2 = (a_1a_2)^2 = a_1^2a_2^2[a_2, a_1] = a_3a_4a_5 \\
a_5^{\beta_{12}^*} &= (a_2^2)^{\beta_{12}} = (a_2^{\beta_{12}})^2 = a_2^2 = a_5
\end{aligned}$$

Portanto, $A_{\beta_{12}^*} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$.

Cálculo dos subgrupos permissíveis

Calculemos agora os *subgrupos permissíveis* de passos $s = 1$, $s = 2$ e $s = 3$ na ordem estabelecida na pág. 71 começando pelos de passo $s = 1$.

Seja $s = 1$.

Os conjuntos definidores neste caso, ordenados lexicograficamente, são $K_1 = \{a_3\}$, $K_2 = \{a_4\}$ e $K_3 = \{a_s\}$.

Para $K_1 = \{a_3\}$, as posições disponíveis são $3 - 1 - (1 - 1) = 2$ e as matrizes padrões correspondentes (ordenadas) são*:

* As posições disponíveis aparecem sublinhadas nas respectivas matrizes.

$$S_1 = (1\ \underline{0}\ \underline{0});\ S_2 = (1\ \underline{1}\ \underline{0});\ S_3 = (1\ \underline{0}\ \underline{1});\ S_4 = (1\ \underline{1}\ \underline{1}).$$

assim os subgrupos permissíveis (i.e., os núcleos das transformações lineares dadas por cada uma dessas matrizes) são respectivamente:

$$U_1 =< a_4, a_5 >;\ U_2 =< a_3a_4, a_5 >;\ U_3 =< a_3a_5, a_4 >;\ U_4 =< a_3a_5, a_4a_5 > .$$

Para $K_2 = \{a_4\}$, as posições disponíveis são $3-1-(2-1) = 1$ e as matrizes correspondentes são:

$$S_5 = (0\ 1\ \underline{0})\ ;\ S_6 = (0\ 1\ \underline{1}).$$

portanto os respectivos subgrupos permissíveis são

$$U_5 =< a_3, a_5 > \quad \text{e} \quad U_6 =< a_3, a_4a_5 >$$

Para $K_3 = \{a_5\}$, não há posições disponíveis, já que $3 - 1 - (3 - 1) = 0$ portanto a única matriz padrão é:

$S_7 = (0\ 0\ 1)$ e o subgrupo permissível correspondente é $U_7 =< a_3, a_4 >$.

Seja $s = 2$.

Os conjuntos definidores neste caso, ordenados lexicograficamente a partir dos anteriores, são:

$$K_4 = \{a_3, a_4\}\ ;\ K_5 = \{a_3, a_5\}\ ;\ K_6 = \{a_4, a_5\}.$$

Para $K_4 = \{a_3, a_4\}$, as posições disponíveis são $3.2-(1+2)-\frac{2(2-1)}{2} = 2$ e as matrizes padrões (ordenadas) correspondentes são:

$$S_8 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix};\ S_9 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix};\ S_{10} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix};\ S_{11} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Assim os subgrupos permissíveis respectivos:

$$U_8 =< a_5 >;\ U_9 =< a_3a_5 >;\ U_{10} =< a_4a_5 >;\ U_{11} =< a_3a_4a_5 > .$$

Para $K_5 = \{a_3, a_5\}$, as posições disponíveis são $3.2 - (1+3) - \frac{2(2-1)}{2} = 1$ e as matrizes padrões (ordenadas) correspondentes são:

$$S_{12} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix};\ S_{13} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

assim, os subgrupos permissíveis respectivos:

$$U_{12} =< a_4 > ;\ S_{13} =< a_3, a_4 >$$

Para $K_6 = \{a_4, a_5\}$, não há posições disponíveis, já que $3.2 - (2+3) - \frac{2(2-1)}{2} = 0$, portanto a única matriz é:

$$S_{14} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

e o subgrupo permissível correspondente:

$$U_{14} =< a_3 > .$$

Seja $s = 3$.

O único conjunto definidor neste caso é o próprio $K_7 = \{a_3, a_4, a_5\}$ para ele não há posições disponíveis já que $3.3 - (1+2+3) - \frac{3(3-1)}{2} = 0$ e portanto a única matriz padrão é: $S_{15} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ e o correspondente subgrupo permissível: $U_{15} =< >$.

Cálculo das permutações induzidas

$$A_{\beta^*_{11}} \cdot S_1^t = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \quad \text{e portanto} \quad (U_1)(\beta^*_{11})^{-1} = U_3$$

$$A_{\beta^*_{11}} \cdot S_2^t = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \quad \text{e portanto} \quad (U_2)(\beta^*_{11})^{-1} = U_2$$

$$A_{\beta^*_{11}} \cdot S_3^t = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \quad \text{e portanto} \quad (U_3)(\beta^*_{11})^{-1} = U_1$$

$$A_{\beta_{11}^*} \cdot S_4^t = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \quad \text{e portanto} \quad (U_4)(\beta_{11}^*)^{-1} = U_4$$

$$A_{\beta_{11}^*} \cdot S_5^t = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \quad \text{e portanto} \quad (U_5)(\beta_{11}^*)^{-1} = U_6$$

$$A_{\beta_{11}^*} \cdot S_6^t = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \quad \text{e portanto} \quad (U_6)(\beta_{11}^*)^{-1} = U_5$$

$$A_{\beta_{11}^*} \cdot S_7^t = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \quad \text{e portanto} \quad (U_7)(\beta_{11}^*)^{-1} = U_7$$

$$A_{\beta_{11}^*} \cdot S_8^t = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{e portanto} \quad (U_8)(\beta_{11}^*)^{-1} = U_{11}$$

$$A_{\beta_{11}^*} \cdot S_9^t = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{e portanto} \quad (U_9)(\beta_{11}^*)^{-1} = U_{10}$$

$$A_{\beta_{11}^*} \cdot S_{10}^t = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{e portanto} \quad (U_{10})(\beta_{11}^*)^{-1} = U_9$$

$$A_{\beta_{11}^*} \cdot S_{11}^t = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}; \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{e portanto} \quad (U_{11})(\beta_{11}^*)^{-1} = U_8$$

$$A_{\beta_{11}^*} \cdot S_{12}^t = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 1 & 1 \end{pmatrix} \quad \text{e portanto} \quad (U_{12})(\beta_{11}^*)^{-1} = U_{12}$$

$$A_{\beta_{11}^*} \cdot S_{13}^t = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{e portanto} \quad (U_{13})(\beta_{11}^*)^{-1} = U_{13}$$

$$A_{\beta_{11}^*} \cdot S_{14}^t = \begin{pmatrix} 0 & 0 \\ 1 & 1 \\ 0 & 1 \end{pmatrix}; \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{e portanto} \quad (U_{14})(\beta_{11}^*)^{-1} = U_{14}$$

$$A_{\beta_{11}^*} \cdot S_{15}^t = A_{\beta_{11}^*} \quad \text{e portanto} \quad (U_{15})(\beta_{11}^*)^{-1} = U_{15}.$$

Logo, a permutação induzida por $(\beta_{11}^*)^{-1} = \beta_{11}^*$ (neste caso) é:

$$(U_1U_3)(U_5U_6)(U_8U_{11})(U_9U_{11}).$$

Agora:

$$A_{\beta^*_{12}} \cdot S_1^t = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \quad \text{e portanto} \quad (U_1)(\beta^*_{12})^{-1} = U_2$$

$$A_{\beta^*_{12}} \cdot S_2^t = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \quad \text{e portanto} \quad (U_2)(\beta^*_{12})^{-1} = U_1$$

$$A_{\beta^*_{12}} \cdot S_3^t = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \quad \text{e portanto} \quad (U_3)(\beta^*_{12})^{-1} = U_3$$

$$A_{\beta^*_{12}} \cdot S_4^t = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \quad \text{e portanto} \quad (U_4)(\beta^*_{12})^{-1} = U_4$$

$$A_{\beta^*_{12}} \cdot S_5^t = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \quad \text{e portanto} \quad (U_5)(\beta^*_{12})^{-1} = U_5$$

$$A_{\beta^*_{12}} \cdot S_6^t = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \quad \text{e portanto} \quad (U_6)(\beta^*_{12})^{-1} = U_7$$

$$A_{\beta^*_{12}} \cdot S_7^t = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \quad \text{e portanto} \quad (U_7)(\beta^*_{12})^{-1} = U_6$$

$$A_{\beta^*_{12}} \cdot S_8^t = \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 0 \end{pmatrix}; \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad \text{e portanto} \quad (U_8)(\beta^*_{12})^{-1} = U_8$$

$$A_{\beta^*_{12}} \cdot S_9^t = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{e portanto} \quad (U_9)(\beta^*_{12})^{-1} = U_9$$

$$A_{\beta^*_{12}} \cdot S_{10}^t = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{e portanto} \quad (U_{10})(\beta^*_{12})^{-1} = U_{13}$$

$$A_{\beta^*_{12}} \cdot S_{11}^t = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 1 & 1 \end{pmatrix}; \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{e portanto} \quad (U_{11})(\beta^*_{12})^{-1} = U_{12}$$

$$A_{\beta_{12}^*} \cdot S_{12}^t = \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{pmatrix}; \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \quad \text{e portanto} \quad (U_{12})(\beta_{12}^*)^{-1} = U_{11}$$

$$A_{\beta_{12}^*} \cdot S_{13}^t = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{e portanto} \quad (U_{13})(\beta_{12}^*)^{-1} = U_{10}$$

$$A_{\beta_{12}^*} \cdot S_{14}^t = \begin{pmatrix} 0 & 0 \\ 1 & 1 \\ 0 & 1 \end{pmatrix}; \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{e portanto} \quad (U_{14})(\beta_{12}^*)^{-1} = U_{14}$$

$A_{\beta_{12}^*} \cdot S_{15}^t = A_{\beta_{12}}^*$ e portanto $(U_{15})(\beta_{12}^*)^{-1} = U_{15}$.

Logo, a permutação induzida por $(\beta_{12}^*)^{-1} = \beta_{12}^*$ é:

$$(U_1U_2)(U_6U_7)(U_{10}U_{13})(U_{11}U_{12}).$$

Cálculo de Órbitas

Para calcular as órbitas de subgrupos permissíveis determinadas pelas permutações

$$\sigma_1 = (U_1U_3)(U_5U_6)(U_8U_{11})(U_9U_{10}) \quad \text{e}$$
$$\sigma_2 = (U_1U_2)(U_6U_7)(U_{10}U_{13})(U_{11}U_{12})$$

Seguiremos os passos 1 e 2 do algoritmo 1.7.5 dado no capítulo 1.

- Orb(U_1):
  $U_1\sigma_1 = \underline{U_3}$; $U_3\sigma_1 = U_1$; $U_2\sigma_1 = U_2$
  $U_1\sigma_2 = \underline{U_2}$; $U_3\sigma_2 = U_3$; $U_2\sigma_2 = U_1$

  Portanto, Orb(U_1) = $\{U_1, U_2, U_3\}$.

- Orb(U_4):
  $U_4\sigma_1 = U_4$
  $U_4\sigma_2 = U_4$; portanto, Orb(U_4) = $\{U_4\}$.

- Orb(U_5):
  $U_5\sigma_1 = \underline{U_6}$; $U_6\sigma_1 = U_5$; $U_7\sigma_1 = U_7$
  $U_5\sigma_2 = \underline{U_5}$; $U_6\sigma_2 = U_7$; $U_7\sigma_2 = U_6$

  Portanto, Orb(U_5) = $\{U_5, U_6, U_7\}$.

- Orb(U_8): $U_8\sigma_1 = \underline{U_{11}}$; $U_{11}\sigma_1 = U_8$; $U_{12}\sigma_1 = U_{12}$
  $U_8\sigma_2 = \underline{U_8}$; $U_{11}\sigma_2 = \underline{U_{12}}$; $U_{12}\sigma_2 = U_{11}$

  Portanto, Orb$(U_8) = \{U_8, U_{11}, U_{12}\}$.

- Orb(U_9): $U_5\sigma_1 = \underline{U_{10}}$; $U_{10}\sigma_1 = U_9$; $U_{13}\sigma_1 = U_{13}$
  $U_9\sigma_2 = \underline{U_9}$; $U_{10}\sigma_2 = \underline{U_{13}}$; $U_{13}\sigma_2 = U_{10}$

  Portanto, Orb$(U_9) = \{U_9, U_{10}, U_{13}\}$.

- Orb(U_{14}): $U_{14}\sigma_1 = \underline{U_{14}}$
  $U_{14}\sigma_2 = \underline{U_{14}}$; portanto Orb$U_{14} = \{U_{14}\}$.

- Orb(U_{15}): $U_{15}\sigma_1 = U_{15}$
  $U_{15}\sigma_2 = U_{15}$; portanto Orb$U_{15} = \{U_{15}\}$.

Escolhemos então os seguintes representantes:

$$U_1; U_4; U_5; U_8; U_9; U_{14}; U_{15}.$$

Cálculo dos estabilizadores.

- $H_1 = \text{Stab}(U_1)$:

Temos que Orb$(U_1) = \{1 = U_1,\ 2 = U_2,\ 3 = U_3\}$, procuremos então um transversal $T_{H_1} = \{t_1, t_2, t_3\}$ para H_1 em $\mathcal{P} =< \sigma_1, \sigma_2 >$. Para isso, sigamos o passo 3 do algoritmo 1.7.5., i.e., olhemos para o "traço" dos elementos 1, 2 e 3 a partir do ponto 1:

$$\left.\begin{array}{lll} 1 = 1id\ , & \text{logo} & t_1 = id \\ 2 = 1\sigma_2\ , & \text{logo} & t_2 = \sigma_2 \\ 3 = 1\sigma_1\ , & \text{logo} & t_3 = \sigma_1 \end{array}\right\} \quad \text{portanto} \quad T_{H_1} = \{t_1 = id,\ t_2 = \sigma_2, t_3 = \sigma_1\}.$$

Assim, o conjunto de geradores de Schreier para H_1 é calculado usando o algoritmo 1.7.6.

$$\begin{array}{llllll}
g_{11} = t_1\sigma_1 = \sigma_1\ ; & (1)g_{11} = 3\ , & \text{logo} & \overline{g_{11}} = \sigma_1 & \text{e portanto} & s_{11} = id \\
g_{12} = t_2\sigma_2 = \sigma_2\ ; & (1)g_{12} = 2\ , & \text{logo} & \overline{g_{12}} = \sigma_2 & \text{e portanto} & s_{12} = id \\
g_{21} = t_2\sigma_1 = \sigma_2\sigma_1\ ; & (1)g_{21} = 2\ , & \text{logo} & \overline{g_{21}} = \sigma_2 & \text{e portanto} & \underline{s_{21} = \sigma_2\sigma_1\sigma_2} \\
g_{22} = t_2\sigma_2 = id\ ; & (1)g_{22} = 1\ , & \text{logo} & \overline{g_{21}} = id & \text{e portanto} & s_{22} = id \\
g_{31} = t_3\sigma_1 = id\ ; & (1)g_{31} = 1\ , & \text{logo} & \overline{g_{31}} = id & \text{e portanto} & s_{31} = id \\
g_{32} = t_3\sigma_2 = \sigma_1\sigma_2\ ; & (1)g_{32} = 3\ , & \text{logo} & \overline{g_{32}} = \beta_{11} & \text{e portanto} & \underline{s_{33} = \sigma_1\sigma_2\sigma_1}
\end{array}$$

Agora note que $(\beta_{11}\beta_{12})^3 = (\beta_{11}\beta_{12}\beta_{11})(\beta_{12}\beta_{11}\beta_{12}) = id$, logo as permutações induzidas satisfazem $(\sigma_1\sigma_2\sigma_1)(\sigma_2\sigma_1\sigma_2) = id$ e portanto $\mathrm{Stab}(U_1) =< \sigma_1\sigma_2\sigma_1 >$.

Assim o estabilizador do subgrupo U_1, segundo a definição 3.1.18 é:

$$\mathrm{Stab}_{U_1} =< \beta_{11}\beta_{12}\beta_{11} >$$

- $H_4 = \mathrm{Stab}(U_4)$:

É claro que $\mathrm{Stab}(U_4) =< \sigma_1, \sigma_2 >$ e assim

$$\mathrm{Stab}_{U_4} =< \beta_{11}, \beta_{12} >$$

- $H_5 = \mathrm{Stab}(U_5)$:

$\mathrm{Orb}(U_5) = \{1 = U_5,\ 2 = U_6,\ 3 = U_7\}$.

Seguindo o traço dos elementos a partir do ponto 1, temos:

$$\left.\begin{array}{ll} 1 = 1id\ , & \text{logo } t_1 = id \\ 2 = 1\sigma_1\ , & \text{logo } t_2 = \sigma_1 \\ 3 = 2\sigma_2 = 1\sigma_1\sigma_2\ , & \text{logo } t_3 = \sigma_1\sigma_2 \end{array}\right\} \quad \text{portanto} \quad T_{H_3} = \{t_1 = id,\ t_2 = \sigma_1, t_3 = \sigma_1\sigma_2\}.$$

é um transversal para H_5 em $\mathcal{P}$.

Assim, utilizando o algoritmo 1.7.6, temos:

$$\begin{array}{llllll} g_{11} = t_1\sigma_1 = \sigma_1\ ; & (1)g_{11} = 2\ , & \text{logo } \overline{g_{11}} = \sigma_1 & \text{e portanto} & s_{11} = id \\ g_{12} = t_1\sigma_2 = \sigma_2\ ; & (1)g_{12} = 1\ , & \text{logo } \overline{g_{12}} = id & \text{e portanto} & \underline{s_{12} = \sigma_2} \\ g_{21} = t_2\sigma_1 = id\ ; & (1)g_{21} = 1\ , & \text{logo } \overline{g_{21}} = id & \text{e portanto} & s_{21} = id \\ g_{22} = t_2\sigma_2 = \sigma_1\sigma_2\ ; & (1)g_{22} = 3\ , & \text{logo } \overline{g_{22}} = \sigma_1\sigma_2 & \text{e portanto} & s_{22} = id \\ g_{31} = t_3\sigma_1 = \sigma_1\sigma_2\sigma_1\ ; & (1)g_{31} = 3\ , & \text{logo } \overline{g_{31}} = \sigma_1\sigma_2 & \text{e portanto} & \underline{s_{31} = \sigma_2} \\ g_{32} = t_3\sigma_2 = \sigma_1\ ; & (1)g_{32} = 2\ , & \text{logo } \overline{g_{32}} = \sigma_1 & \text{e portanto} & s_{32} = id \end{array}$$

Logo, $\mathrm{Stab}(U_5) =< \sigma_2 >$ e assim:

$$\mathrm{Stab}_{U_5} =< \beta_{12} >$$

- $H_8 = \mathrm{Stab}(U_8)$:

$\mathrm{Orb}(U_8) = \{1 = U_8;\ 2 = U_{11};\ 3 = U_{12}\}$.

O traço dos elementos a partir do ponto 1 é:

$$1 = 1id$$
$$2 = 1\sigma_1$$
$$3 = 2\sigma_2 = 1\sigma_1\sigma_2$$

Observe que é o mesmo traço calculado para H_5 e portanto $T_{H_8} = T_{H_5} = \{t_1 = id,\ t_2 = \sigma_1;\ t_3 = \sigma_1\sigma_2\}$, assim $\mathrm{Stab}(U_8) =< \sigma_2 >$ e conseqüentemente

$$\mathrm{Stab}_{U_6} =< \beta_{12} >$$

- $H_9 = \mathrm{Stab}(U_9)$:

  $\mathrm{Orb}(U_9) = \{1 = U_9;\ 2 = U_{10};\ U_{13}\}$.

  O traço dos elementos a partir do ponto 1 é:

$$1 = 1id$$
$$2 = 1\sigma_1$$
$$3 = 2\sigma_2 = 1\sigma_1\sigma_2$$

  Logo, como acima, $\mathrm{Stab}(U_9) =< \sigma_2 >$ e conseqüentemente

$$\mathrm{Stab}_{U_9} =< \beta_{12} >$$

Construção dos descendentes imediatos de G

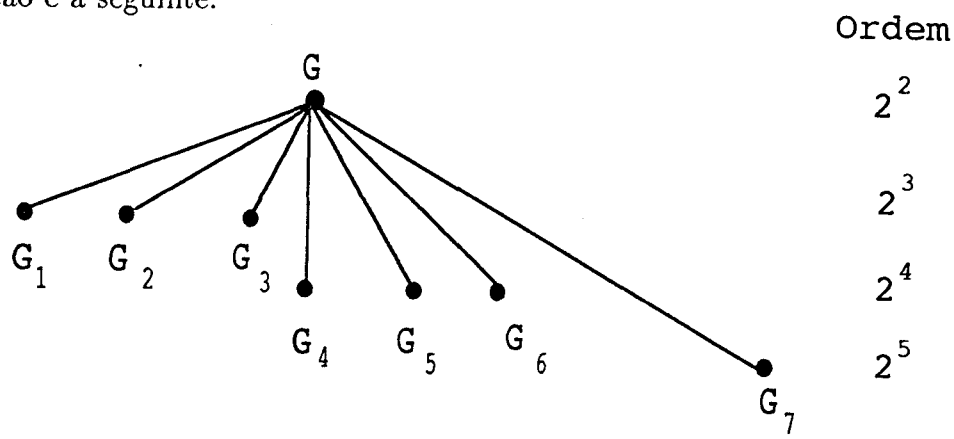
Lembrando que os descendentes imediatos são classificados através do passso (v. pág. 64), obtemos os seguintes descendentes imediatos do nosso grupo inicial G:

- $G_1 = G^*/U_1$, $G_2 = G^*/U_4$ e $G_3 = G^*/U_5$ de passo $s = 1$.
- $G_4 = G^*/U_8$, $G_5 = G^*/U_9$ e $G_6 = G^*/U_{14}$ de passo $s = 2$.
- $G_7 = G^*/U_{15}$ de passo $s = 3$.

(Onde G^* está dado pela apresentação consistente por potências e comutadores da pág. 77, i.e.:

$$G^* =< a_1, a_2, a_3, a_4, a_5 \ / \ [a_2, a_1] = a_3; a_1^2 = a_4, a_2^2 = a_5, a_3^2 = a_4^2 = a_5^2 = 1, [a_3, a_1] = \\ = [a_3, a_2] = [a_4, a_2] = [a_5, a_1] = [a_5, a_2] = 1 >)$$

A situação é a seguinte:



Construção de $G_1 = G^*/U_1$

$U_1 =< a_4, a_5 >$, logo G_1 está dado pela seguinte apresentação:

$$G_1 = G^*/U_1 =< a_1, a_2, a_3 \ / \ a_1^2 = 1, a_2^2 = 1, \ [a_2, a_1] = a_3, \ a_3^2 = 1, \ [a_3, a_1] = 1 \\ [a_3, a_2] = 1 > .$$

a qual é uma apresentação consistente por potências e comutadores.

Observação 1: *Verifica-se que* $G_1 \cong D_4 =< a_1 a_2 \ / \ a_1^2 = 1, a_2^2 = 1, \ (a_1 \ a_2)^4 = 1 >$ *(eliminando, via transformação de Tietze, o gerador supérfluo* a_3 *na apresentação acima e comprovando que as relações em* D_4 *são satisfeitas em* G_1 *temos, pelo teorema* 1.1.9, *que existe um epimorfismo* $\theta : D_4 \twoheadrightarrow G_1$. *Logo* $G_1 \cong D_4$). □

Vejamos se G_1 *é capaz.*

Uma apresentação para o p-recobrimento de G_1, G_1^*, é a seguinte:

$$G_1^* =< a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8 \ / \ [a_3, a_1] = a_4, \ [a_3, a_2] = a_5, \ a_1^2 = a_6, a_2^2 = a_7, a_3^2 = a_8, \\ [a_2, a_1] = a_3; \ a_j^2 = 1, \ [a_j, a_i] = 1, \ i \in \{1,2,3\}, \ j \in \{4,5,6,7,8\} > .$$

Avaliando as condições de associatividade de Wamsley temos:

$$\left.\begin{array}{lcl} a_2^2a_1 & = & a_7a_1 = \underline{a_1a_7} \\ a_2(a_2a_1) & = & a_2a_1a_2a_3 = a_1a_2a_3a_2a_3 = \\ & = & a_1a_2^2a_3^2a_5 = a_1a_7a_8a_5 \end{array}\right\} \quad \text{portanto} \quad \underline{a_8 = a_5}$$

$$\left.\begin{array}{lcl} (a_2a_1)a_1 & = & a_1a_2a_3a_1 = a_1a_2a_1a_3a_4 \\ & = & a_2^2a_2a_3^2a_4 = \underline{a_2a_6a_5a_4} \\ a_2a_1^2 & = & \underline{a_2a_6} \end{array}\right\} \quad \text{portanto} \quad \underline{a_5 = a_4}$$

enquanto as outras condições são compatíveis com as relações acima.

Assim re-enumerando os geradores, temos que uma apresentação consistente por potências e comutadores para G_1^* é:

$$G_1^* =< a_1, a_2, a_3, a_4, a_5, a_6 \ / \ [a_3, a_1] = [a_3, a_2] = a_3^2 = a_4;\ a_1^2 = a_5,\ a_2^2 = a_6,\ [a_2, a_1] = a_3$$
$$a_4^2 = a_5^2 = a_6^2 = 1;\ [a_j, a_i] = 1,\ j \in \{4,5,6\},\ i \in \{1,2,3\} > .$$

Temos então que o p-multiplicador de G_1 é gerado por $\{a_4, a_5, a_6\}$ e o núcleo de G_1, $P_2(G_1^*)$, é gerado por $a_4 = [a_3, a_1]$ (Lema 3.2.1).

Conseqüentemente G_1 *é capaz* (desde que $|P_2(G_1^*)| = p$ e portanto G_1 tem descendentes imediatos de passo $s = 1$).

Construção de $G_2 = G^*/U_4$:

$U_4 =< a_3a_4, a_4a_5 >$, logo G_2 está dado pela seguinte apresentação:

$$G_2 = G^*/U_4 =< a_1, a_2, a_3 \ / \ a_1^2 = a_3;\ a_2^2 = a_3; [a_2, a_1] = a_3; a_3^2 = 1, [a_3, a_1] = [a_3, a_2] = 1 >$$

Observação 2: $G_2 \cong Q_4 =< a_1, a_2 \ / \ a_1^2 = a_2^2 = (a_1a_2)^2 >$ (*segue-se como na observação 1 da pág. anterior*).

Vejamos se G_2 é capaz.

Uma apresentação para G_2^* é a seguinte:

$$G_2^* =< a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8 \ / \ [a_3, a_1] = a_4;\ [a_3, a_2] = a_5;\ a_1^2 = a_3a_6;\ a_2^2 = a_3a_7;$$
$$a_3^2 = a_8;\ [a_2, a_1] = a_3;\ a_j^2 = 1,\ [a_j, a_i] = 1,$$
$$j \in \{4, \ldots, 8\},\ i \in \{1, 2, 3\} > .$$

Avaliando as condições de associatividade de Wamsley temos:

$$\left.\begin{array}{rcl} a_2^2a_1 & = & a_3a_7a_1 = a_3a_1a_7 = \underline{a_1a_3a_7} \\ a_2(a_2a_1) & = & a_2a_1a_2a_3 = a_1a_2a_3a_2a_3 = \\ & = & a_1a_2^2a_3^2a_5 = \underline{a_1a_3a_7a_8a_5} \end{array}\right\} \text{ portanto } \underline{a_8 = a_5}$$

$$\left.\begin{array}{rcl} (a_2a_1)a_1 & = & a_1a_2a_3a_1 = a_1a_2a_1a_3a_4 \\ & = & a_1^2a_2a_3^2a_4 = a_3a_6a_2a_8a_4 \\ & = & a_2a_3a_5a_6a_8a_4 \\ & = & \underline{a_2a_3a_4a_5a_6} \\ & = & \underline{a_2a_3a_6} \end{array}\right\} \text{ portanto } \underline{a_5 = a_4}$$

$$\left.\begin{array}{rcl} a_1^2a_1 & = & a_3a_6a_1 = \underline{a_1a_3a_4a_6} \\ a_1a_1^2 & = & \underline{a_1a_3a_6} \end{array}\right\} \text{ portanto } \underline{a_4 = 1}$$

enquanto as outras condições são compatíveis com as relações acima.

Assim, uma apresentação consistente por potências e comutadores para G_2^* é a seguinte:

$$G_2^* =< a_1, a_2, a_3, a_4, a_5 \ / \ [a_3, a_1] = 1;\ [a_3, a_2] = 1;\ a_1^2 = a_3a_4;\ a_2^2 = a_5;\ [a_2, a_1] = a_3;$$
$$a_3^2 = 1;\ a_4^2 = a_5^2 = 1;\ [a_j, a_i] = 1,\ j \in \{4, 5\}, i \in \{1, 2, 3\} > .$$

Temos então que o p-multiplicador de G_2 é gerado por $\{a_4, a_5\}$ e o núcleo de G_2 é trivial, i.e., $P_2(G_2^*) =< >$, pelo Lema 3.2.1.

Portanto, G_2 *é terminal.*

Construção de $G_3 = G^*/U_5$.

$U_5 =< a_3, a_5 >$, logo G_3 está dado pela seguinte apresentação:

$$G_3 = G^*/U_5 =< a_1, a_2, a_3 \ / \ a_1^2 = a_3,\ a_2^2 = 1,\ [a_2, a_1] = 1,\ a_3^2 = 1,\ [a_3, a_2] = 1 >$$

Observação 3: $G_3 \cong C_4 \times C_2$ (*segue-se como as observações* 1 *e* 2). □

Vejamos se G_3 *é capaz.*

Uma apresentação para G_3^* é a seguinte:

$$G_3^* =< a_1, a_2, a_3, a_4, a_5, a_6, a_7 \ / \ [a_3, a_2] = a_4;\ a_3^2 = a_5;\ a_2^2 = a_6;\ [a_2, a_1] = a_7;\ a_1^2 = a_3;$$
$$a_j^2 = 1,\ [a_j, a_i] = 1,\ j \in \{4, \ldots, 7\},\ i \in \{1, 2, 3\} > .$$

Avaliando as condições de associatividade de Wamsley temos:

$$\left.\begin{array}{lcl} (a_2a_1)a_1 & = & a_1a_2a_7a_1 = a_1^2a_2a_7^2 = a_3a_2 = a_2a_3a_4 \\ a_2a_1^2 & = & a_2a_3 \end{array}\right\} \quad \text{portanto} \quad \underline{a_4 = 1}$$

enquanto as outras condições são compatíveis com as relações acima.

Em conseqüência, uma apresentação consistente para G_3^* é dada por:

$$G_3^* =< a_1, a_2, a_3, a_4, a_5, a_6 \ / \ a_3^2 = a_4;\ a_2^2 = a_5;\ [a_2, a_1] = a_6;\ [a_3, a_2] = 1;\ a_1^2 = a_3$$
$$a_j^2 = 1,\ [a_j, a_i] = 1,\ j \in \{4, 5, 6\},\ i \in \{1, 2, 3\} > .$$

Assim, o p-multiplicador de G_4 é gerado por $\{a_4, a_5, a_6\}$ e o núcleo de $G_3, P_2(G_3^*)$, é gerado por a_4. Conseqüentemente G_3 *é capaz* e tem descendentes imediatos de passo $s = 1$.

Construção de $G_4 = G^*/U_8$.

$U_8 =< a_5 >$, logo G_4 tem a seguinte apresentação:

$$G_4 = G^*/U_8 =< a_1, a_2, a_3, a_4 \ / \ a_1^2 = a_4;\ a_2^2 = 1;\ [a_2, a_1] = a_3;\ a_3^2 = a_4^2 = 1,$$
$$[a_3, a_1] = 1\ [a_3, a_2] = [a_4, a_2] = 1 > .$$

Observação 4: *Fazendo* $a = a_1$, $b = a_2$ *e* $c = a_3$, *obtemos para* G_4 *a seguinte apresentação,* $G_4 =< a, b, c \ / \ a^4 = 1,\ b^2 = 1,\ c^2 = 1,\ [b, a] = c,\ [c, a] = [c, b] = 1 >$.

É claro agora que G_4 é um produto semidireto do seu subgrupo $< a, c >$ pelo grupo cíclico de ordem 2 gerado por b, cuja ação é tal que b transforma a em ac e fixa c. □

Construção de $G_5 = G^*/U_9$.

$U_9 =< a_3 a_5 >$

$$G^*/U_9 =< a_1, a_2, a_3, a_4 \ / \ a_1^2 = a_4;\ a_2^2 = a_3;\ [a_2, a_1] = a_3;\ a_3^2 = a_4^2 = 1,$$
$$[a_3, a_1] = [a_4, a_2] = 1 > .$$

Observação 5: *Fazendo $a = a_1$ e $b = a_2$ obtemos para G_5 a seguinte apresentação, $G_5 =< a, b \ / \ a^4 = 1,\ b^4 = 1,\ b^a = b^3 >$. É claro agora que G_4 é um produto semidireto do grupo cíclico de ordem 4 gerado por a pelo grupo cíclico de ordem 4, cuja ação de a transforma b em b^{-1}.* □

Construção de $G_6 = G^*/U_{14}$.

$U_{14} =< a_3 >$

$$G_6 = G^*/U_{14} =< a_1, a_2, a_3, a_4 \ / \ a_1^2 = a_3,\ a_2^2 = a_4;\ [a_2, a_1] = 1,\ a_4^2 = a_5^2 = 1 > .$$

Observação 6: *Fazendo $a = a_1$ e $b = a_2$, obtemos para G_6 a seguinte apresentação, $G_6 =< a, b \ / \ a^4 = b^4 = 1,\ [b, a] = 1 >$, logo, segue do teorema 1.1.12 que $G_6 \cong C_4 \times C_4$.* □

Construção dos descendentes imediatos de G_1.

Temos, pelo teorema 3.1.19, que $\mathrm{Aut}(G_1) = \mathrm{Aut}(G^*/U_1) = S_{G_1} V_{G_1}$ onde:

- $S_{G_1} =< \hat{\xi} \ / \ \xi \in S_{U_1} >$, onde $\hat{\xi}$ é a restrição a G_1 de uma extensão ξ^* de ξ a G^* e
- V_{G_1} é o subgrupo de $\mathrm{Aut}(G_1)$ dos automorfismos de G_1 que induzem a identidade em G.

Assim, $\mathrm{Aut}(G_1)$ é gerado por:

$$\left\{\begin{array}{l}\left.\begin{array}{rcl}\beta_{21}: a_1 & \longmapsto & a_1a_3 \\ a_2 & \longmapsto & a_2\end{array}\right\} \\ \\ \left.\begin{array}{rcl}\beta_{22}: a_1 & \longmapsto & a_1 \\ a_2 & \longmapsto & a_2a_3\end{array}\right\}\end{array}\right. \text{ geradores de } V_{G_1} \quad \text{(teorema 3.2.8)}$$

$$\left\{\begin{array}{l}\left.\begin{array}{rcl}\beta_{23} = \beta_{11}\beta_{12}\beta_{11}: a_1 & \longmapsto & a_2 \\ a_2 & \longmapsto & a_1\end{array}\right\}\end{array}\right. \text{ gerador de } V_{G_1}$$

As respectivas matrizes dos automorfismos estendidos são:

$$A_{\beta^*_{21}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix};\ A_{\beta^*_{22}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{e} \quad A_{\beta^*_{23}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Passemos agora ao *cálculo dos subgrupos permissíveis*

$s = 1$

O único conjunto definidor neste caso é $K = \{a_4\}$. As posições disponíveis são $3 - 1 - (1 - 1) = 2$ e as matrizes "padrão" ordenadas:

$$S_1^1 = (1\ \underline{0\ 0});\ S_2^1 = (1\ \underline{1\ 0});\ S_3^1 = (1\ \underline{0\ 1});\ S_4^1 = (1\ \underline{1\ 1}).$$

Logo os subgrupos permissíveis correspondentes são:

$$U_1^1 =< a_5, a_6 >;\ U_2^1 =< a_4a_5, a_6 >;\ U_3^1 =< a_4a_6, a_5 >;\ U_4^1 =< a_4a_6, a_5a_6 > .$$

Cálculo das permutações induzidas

Note que como β^*_{21} e β^*_{22} agem trivialmente sobre o p-multiplicador de G_1, induzem a permutação trivial sobre os subgrupos permissíveis. Logo, será necessário calcular só a permutação induzida por β^*_{23}. Temos

$$A_{\beta^*_{23}} \cdot S_1^{1^t} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \quad \text{e portanto} \quad (U_1^1)(\beta^*_{23})^{-1} = U_1^1$$

$$A_{\beta^*_{23}} \cdot S_2^{1^t} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \quad \text{e portanto} \quad (U_2^1)(\beta^*_{23})^{-1} = U_3^1$$

$$A_{\beta^*_{23}} \cdot S_3^{1^t} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \quad \text{e portanto} \quad (U_3^1)(\beta^*_{23})^{-1} = U_2^1$$

$$A_{\beta^*_{23}} \cdot S_4^{1^t} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \quad \text{e portanto} \quad (U_4^1)(\beta^*_{23})^{-1} = U_4^1$$

Assim, a permutação induzida por β^*_{23} é: (U_2U_3).

Cálculo de órbitas

É claro que as órbitas são:

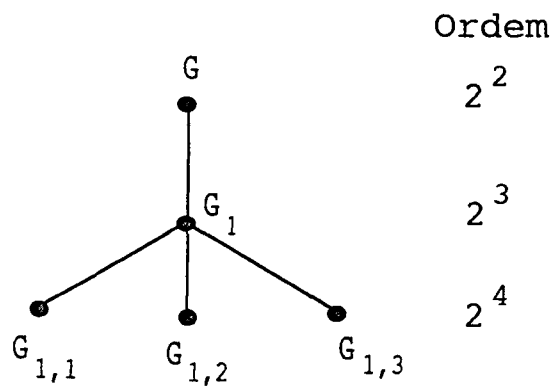
$$\text{Orb}(U_1^1) = \{U_1^1\};\ \text{Orb}(U_2^1) = \{U_2^1, U_3^1\} \quad \text{e} \quad \text{Orb}(U_4^1) = \{U_4^1\}.$$

Logo os três descendentes imediatos de $G_1 = G^*/U_1$ são:

$$G_{1,1} = G_1^*/U_1^1;\ G_{1,2} = G_1^*/U_2^1;\ G_{1,3} = G_1^*/U_4^1 \quad \text{de passo} \quad s = 1$$

onde $G_1^* =< a_1, a_2, a_3, a_4, a_5, a_6/[a_3, a_1] = [a_3, a_2] = a_3^2 = a_4;\ a_1^2 = a_5,\ a_2^2 = a_6,\ [a_2, a_1] = a_3\ a_4^2 = a_5^2 = a_6^2 = 1;\ [a_j, a_i] = 1,\ j \in \{1,2,3\} >$ (apresentação consistente por potências e comutadores obtida na pág. 88).

A situação é:



Construção de $G_{1,1} = G_1^*/U_1^1$:

$U_1^1 =< a_5, a_6 >$, logo $G_{1,1}$ está dado pela seguinte apresentação

$$G_{1,1} = G_1^*/U_1^1 = < a_1, a_2, a_3, a_4 \ / \ [a_3, a_1] = [a_3, a_2] = a_4, a_1^2 = a_2^2 = 1, \ a_3^2 = a_4, \\ [a_2, a_1] = a_3, a_4^2 = 1, \ [a_4, a_i] = 1, \ i \in \{1, 2, 3\} > .$$

Observação: $G_{1,1} \cong D_8 =< a_1, a_2 \ / \ a_1^2 = 1, \ a_2^2 = 1, \ (a_1 a_2)^8 = 1 >$ *(eliminando os geradores supérfluos* a_3 *e* a_4*, via transformações de Tietze, verificam-se em* $G_{1,1}$ *as relações de* D_8*. Assim, pelo teorema* 1.1.9*, existem epimorfismos* $\theta : D_8 \to G_{1,1}$*. Logo* $G_{1,1} \cong D_8$*).* □

Cálculo de $G_{1,2} = G_1^*/U_2^1$:

$U_2^1 =< a_4 a_5, a_6 >$, logo $G_{1,2}$ está dado por:

$$G_{1,2} = G_1^*/U_2^1 = < a_1, a_2, a_3, a_4 \ / \ [a_3, a_1] = [a_3, a_2] = a_4, a_1^2 = a^4, \ a_2^2 = 1 \\ a_3^2 = a_4; \ [a_2, a_1] = a_3, \ a_4^2 = 1; \ [a_4, a_i] = 1, \ i \in \{1, 2, 3\} > .$$

Observação: *Fazendo* $a = a_1 a_2$*,* $b = a_2$*, obtemos para* $G_{1,2}$ *a seguinte apresentação,* $G_{1,2} =< a, b \ / \ a^8 = 1, \ b^2 = 1, \ a^b = a^3 >$ *que é o grupo semidiedral* SD_4*. (Os grupos semidiedrais são 2-grupos de ordem* 2^m*, definidos para* $m \geq 4$ *por:* $SD_m =< a, b \ / \ a^{2(m-1)} = 1, \ b^2 = 1, \ a^b = a^{(-1)2^{(m-2)}}) >$. □

Cálculo de $G_{1,3} = G_1^*/U_4^1$:

$U_4^1 =< a_4 a_6, a_5 a_6 >$

$$G_{1,3} = G_1^*/U_4^1 = < a_1, a_2, a_3, a_4 \ / \ [a_3, a_1] = [a_3, a_2] = a_4, \ a_1^2 = a_2^2 = a_3^2 = a_4 \\ [a_2, a_1] = a_3; \ a_4^2 = 1; \ [a_4, a_i] = 1, \ i \in \{1, 2, 3\} > .$$

Observação: *Fazendo* $a = a_1 a_2$ *e* $b = a_2$*, obtemos para* $G_{1,3}$ *a seguinte apresentação,* $G_{1,3} =< a, b \ / \ a^8 = 1, \ b^2 = a^4, \ a^b = a^{-1} >$*, que é a apresentação do grupo quaternio*

generalizado Q_8. □

Construção dos descendentes imediatos de G_3

Pelo teorema 3.11, $\mathrm{Aut}(G_3) = \mathrm{Aut}(G^*/U_5) = S_{G_3} V_{G_3}$ onde:

- $S_{G_3} =< \tilde{\xi} \ / \ \xi \in S_{U_5} >$, onde $\tilde{\xi}$ é a restrição a G_3 de uma extensão ξ^* de ξ a G^* e
- V_{G_3} é o subgrupo de $\mathrm{Aut}(G_3)$ que induzem a identidade em G.

Assim, $\mathrm{Aut}(G_3)$ é gerado por:

$$\left\{ \begin{array}{l} \left.\begin{array}{rcl} \beta_{31} : a_1 & \longmapsto & a_1 a_3 \\ a_2 & \longmapsto & a_2 \end{array}\right\} \text{ geradores de } V_{G_1} \text{ (teorema 3.2.8)} \\ \left.\begin{array}{rcl} \beta_{32} : a_1 & \longmapsto & a_1 \\ a_2 & \longmapsto & a_2 a_3 \end{array}\right\} \\ \\ \left.\begin{array}{rcl} \beta_{33} = \beta_{12} : a_1 & \longmapsto & a_1 a_2 \\ a_2 & \longmapsto & a_2 \end{array}\right\} \text{ gerador de } V_{G_1} \end{array} \right.$$

As respectivas matrizes dos automorfismos estendidos são:

$$A_{\beta^*_{31}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}; \ A_{\beta^*_{32}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{e} \quad A_{\beta^*_{33}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Passemos agora ao *cálculo dos subgrupos permissíveis*

$s = 1$

O único conjunto definidor neste caso é $K = \{a_4\}$. As posições disponíveis são $3 - 1 - (1 - 1) = 2$ e as matrizes padrões ordenadas são:

$$S_1^3 = (1 \ \underline{0} \ 0); \ S_2^3 = (1 \ \underline{1} \ 0); \ S_3^3 = (1 \ \underline{0} \ 1) \quad \text{e} \quad S_4^3 = (1 \ \underline{1} \ 1).$$

Logo os subgrupos permissíveis correspondentes são:

$$U_1^3 =< a_5, a_6 >; \ U_2^3 =< a_4 a_5, a_6 >; \ U_3^3 =< a_4 a_5, a_5 > \quad \text{e} \quad U_4^3 =< a_4 a_7, a_5 a_7 > .$$

Cálculo das permutações induzidas

Temos:

$$A_{\beta_{32}^*} \cdot S_1^t = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \quad \text{e portanto} \quad (U_1^3)(\beta_{32}^*)^{-1} = U_2^3$$

$$A_{\beta_{32}^*} \cdot S_2^t = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \quad \text{e portanto} \quad (U_2^3)(\beta_{32}^*)^{-1} = U_1^3$$

$$A_{\beta_{32}^*} \cdot S_3^t = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \quad \text{e portanto} \quad (U_3^3)(\beta_{32}^*)^{-1} = U_4^3$$

$$A_{\beta_{32}^*} \cdot S_4^t = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \quad \text{e portanto} \quad (U_4^3)(\beta_{32}^*)^{-1} = U_3^3$$

Assim, a permutação induzida por β_{32}^* é: $(U_1^3 U_2^3)(U_3^3 U_4^3)$.

Cálculo das órbitas

É claro que as órbitas são:

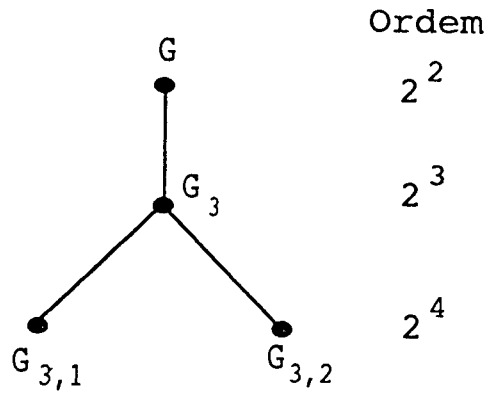
$$\mathrm{Orb}(U_1^3) = \{U_1^3, U_2^3\}$$
$$\mathrm{Orb}(U_3^3) = \{U_3^3, U_4^3\}$$

Logo os descendentes imediatos de $G_3 = G^*/G_5$ são:

$$G_3^*/U_1^3 \quad \text{e} \quad G_3^*/U_3^3 \quad \text{de passo} \quad s = 1$$

onde $G_3^* =< a_1, a_2, a_3, a_4, a_5, a_6 / a_3^2 = a_4;\ a_2^2 = a_5;\ [a_2, a_1] = a_6;\ [a_3, a_2] = 1;\ a_1^2 = a_3\ a_j^2 = 1,\ [a_j, a_i] = 1,\ j \in \{4,5,6\},\ i \in \{1,2,3\} >$ (apresentação consistente por potências e comutadores obtida na pág. 90).

A situação é:



Cálculo de $G_{3,2} = G_1^*/U_1^3$:

$U_1^3 =< a_5, a_6 >$, logo:

$$G_{3,1} = G_3^*/U_1^3 =< a_1, a_2, a_3, a_4 \ / \ a_3^2 = a_4;\ a_2^2 = 1;\ [a_2, a_1] = 1,\ a_1^2 = a_3,$$
$$a_4^2 = 1 > .$$

Observação: *Fazendo $a = a_1$ e $b = a_2$, obtemos para $G_{3,1}$ a seguinte apresentação $G_{3,1} =< a, b \ / \ a^8 = 1,\ b^2 = 1,\ [a,b] = 1 >$ logo, segue do teorema 1.1.12 que $G_{3,1} \cong C_8 \times C_2$.* □

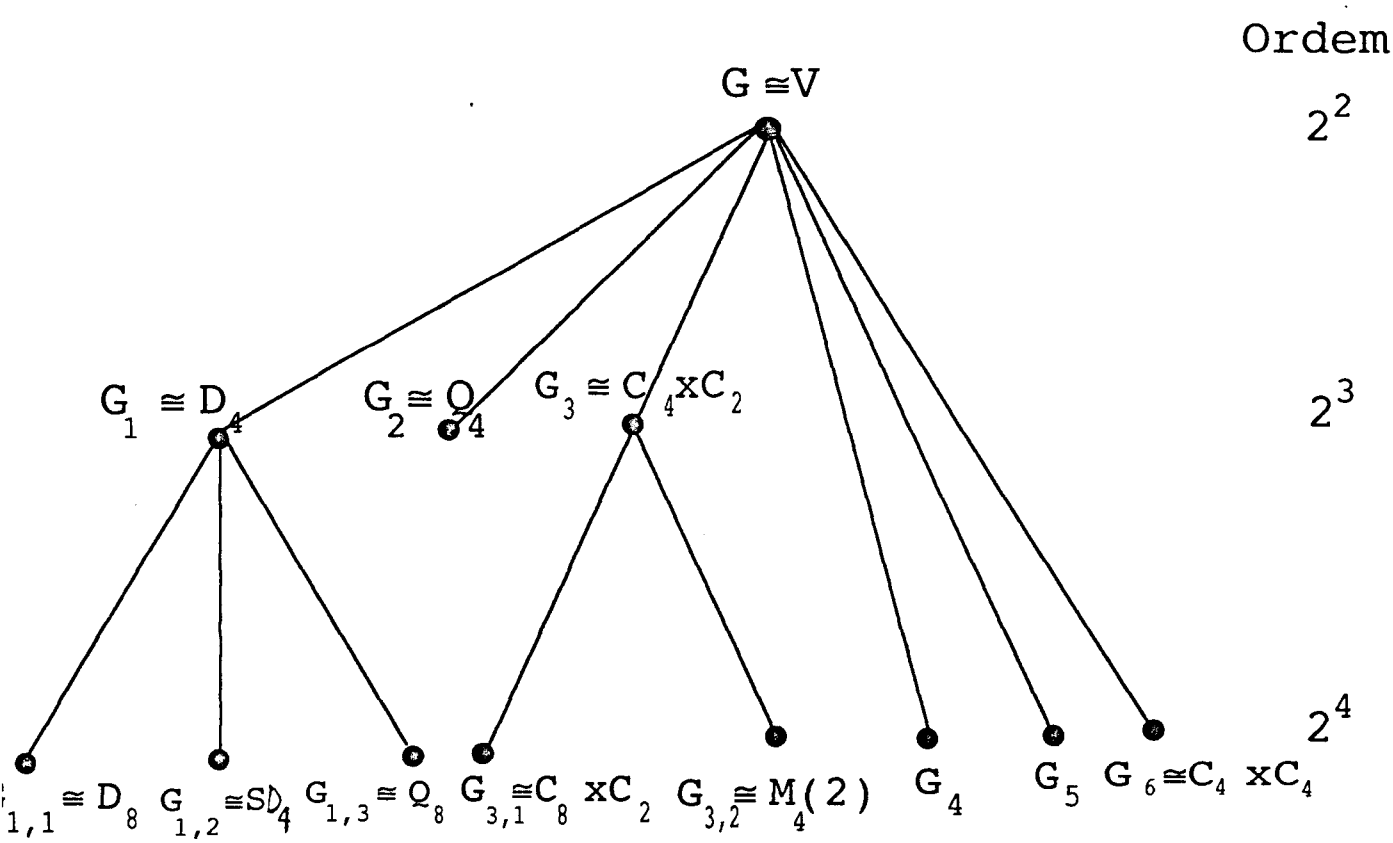
Cálculo de $G_{3,2} = G_3^*/U_3^3$:

$U_3^3 =< a_4a_6, a_5 >$.

$$G_{3,2} = G_3^*/U_3^3 =< a_1, a_2, a_3, a_4 \ / \ [a_3^2a_4];\ a_2^2 = 1; [a_2, a_1] = a_4,\ [a_3, a_2] = 1$$
$$a_1^2 = a_3;\ a_4^2 = 1 > .$$

Observação: *Fazendo $a = a_1$ e $b = a_2$, obtemos para $G_{3,2}$ a seguinte apresentação $G_{3,1} =< a, b \ / \ a^8 = 1,\ b^2 = 1,\ a^b = a^5 >$ que é o grupo "quase-diedral" $M_4(2)$. (Este grupo pertence a uma série de p-grupos $M_n(p)$, definida para $n > 2$ se p é par e para $n > 3$ se $p = 2$, da seguinte forma: $M_n(p) =< x, y \ / \ x^{p^{(n-1)}} = 1,\ y^p = 1,\ x^y = x^{(1+p^{n-2})} >$).* □

O diagrama abaixo resume os resultados do nosso exemplo, exibindo todos os 2-grupos 2-gerados de ordem ≤ 4:



No dia em que eu veja realizados absolutamente todos os meus sonhos, serei completamente infeliz ... terei perdido a capacidade de sonhar.

Comentários finais

1) **Limitações da implementação:** A performance da implementação do algoritmo de Newman-O'Brien depende fortemente do número de subgrupos permissíveis de um tamanho de passo particular, i.e., do grau, D, do grupo $\mathcal{P}$ de permutações induzidas pelos automorfismos estendidos. Cada uma destas permutações é armazenada num vetor de dimensão D. A memória requerida para armazenar este vetor é um fator limitante da implementação. Por exemplo, no cálculo dos descendentes imediatos de passo 2 do grupo abeliano elementar de ordem 16, o grau de $\mathcal{P}$ é 174.251.

   O tempo gasto no cálculo das permutações geradoras para $\mathcal{P}$ e na determinação das órbitas é uma limitação adicional. Em média, 70 % do tempo gasto em calcular descendentes imediatos é usado no cálculo de permutações geradoras de $\mathcal{P}$ e das órbitas de subgrupos admissíveis. (v. O'BRIEN [12]).

2) **Melhoras:** A performance do algoritmo pode ser melhorada usando características estruturais do p-multiplicador, tais como a presença de subgrupos característicos no p-recobrimento. Em geral, a estrutura do p-multiplicador permite dividir o conjunto de subgrupos permissíveis em subconjuntos menores que são uniões de órbitas. Essa divisão permite a construção de grupos de permutações de grau menor. (v. O'BRIEN [12]).

3) **Two-Groups:** Two-Groups é uma base de dados realizada em *Nu-Prolog*, que fornece acesso à informação sobre os 58.761 grupos de ordem dividindo 256. A linguagem de consulta, baseado na notação da Teoria de Conjuntos, permite a recuperação da informação armazenada bem como a dedução de uma informação nova (o expoente e o número de classes de conjugação de um grupo, a ordem

de seus grupos de automorfismos internos). Nesta base de dados pode incluir-se, sem maior dificuldade ou alteração, informação sobre outras listas de p-grupos. (v. BUTLER ET AL [1]).

4) **Apresentações ponderadas:** Uma vantagem do uso de apresentações ponderadas por potências e comutadores é a obtenção de um critério razoavelmente prático para estabelecer o expoente do grupo apresentado (v. HAVAS-NEWMAN [6]) o que é de muita utilidade para o estudo do problema de Burnside.

5) **Consistência:** No teorema 2.2.5 foi dada, através dos testes de consistência de Wamsley, uma solução para o problema de consistência de uma dada apresentação por potências e comutadores para um grupo G finitamente gerado. Ao mesmo tempo, prova-se que alguns desses testes são redundantes, obtendo-se assim uma considerável redução no número de testes suficientes para se analisar a consistência. Esta redução no número de testes proposta por Vaughan-Lee [15], está ligada ao número de geradores essenciais de G.

No artigo de Havas-Newman [6], fazendo-se uso de apresentações ponderadas por potências e comutadores, propõe-se uma outra redução para o número de testes, ligado ao peso do último gerador da apresentação que, como foi provado na proposição 2.4.3, representa a p-classe de G.

Achamos que seria interessante comparar, em termos computacionais, ambas as reduções propostas para o número de testes de consistência. (v. VAUGHAN-LEE [15] e HAVAS-NEWMAN [6]).

Bibliografia

[1] BUTLER, G.; IYER, S.S; O'BRIEN, E.A.; *Two Groups: A Database for Group-Theory*, Computers ad Mathematics, v. 40, n. 7, 1993, 839-841.

[2] CAYLEY, A.; *Desiderata and suggestions, N. 1, The Theory of Groups Amer.*, J. Math. 1, 1878, 50-52.

[3] HALL, M.; *The Theory of Groups*, Macmillan, New York, 1959.

[4] HALL, M. and SENIOR, J.K.; *The Groups of order* $2^n (n \leq 6)$, Macmillan, New York, 1964.

[5] HALL, P.; *The Classification of prime-power groups*, J. Reine Angew. Math., 182, 1940, 130-141.

[6] HAVAS, G. and NEWMAN, M.F.; *Application of Computers to Questions like those of Burnside*, in: Burnside Groups (Bielefeld, 1977), LNM, v. 806, Springer Verlag, 1980, 211-230.

[7] JAMES, R.; NEWMAN, M.F and O'BRIEN, E.A.; *The Groups of Order 128*, Journal of Algebra 129, 1990, 136-158.

[8] JOHNSON, D.L.; *Topics in the Theory of Group Presentations*, Cambridge University Press, 1980.

[9] MACDONALD, I.D.; *A Computer Application to Finite p-Groups*, J. Austral. Math. Soc., v. 17, 1974, 102-112.

[10] NEWMAN, M.F.; *Determination of Groups of prime-power order*, in: Groups Theory (Canberra 1975), LNM, v. 573, Springer Verlag, 1977, 73-84.

[11] O'BRIEN, E.A.; *The Groups of order 256*, Journal of Algebra 143 (1), 1991, 219-235.

[12] O'BRIEN, E.A.; *The p-Group Generation Algorithm*, J. Symbolic Computation, 1990, 677-698..

[13] ROCCO, N.R.; *Métodos de Lie em Teoria dos Grupos*, in: Atas da 9a. Escola de Álgebra, Brasília, 1987, 129-213.

[14] ROTMAN, J.J.; *An Introduction to the Theory of Groups*, Allyn and Bacon Inc., 1984.

[15] VAUGHAN-LEE, M.R.; *An Aspect of the Nilpotent Quotient Algorithm*, in: Computational Group Theory (Atkinson M.D., ed.), London: Academic Press, 76-83.

[16] WAMSLEY, J.W.; *Computation in Nilpotent Groups (theory)*, Proc. Second Internat. Conf. Theory of Groups (Canberra, 1973), LNM, v. 372, Springer Verlag, 1973, 691-700.