UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA

SILVIO SANDRO ALVES DE MACEDO

Comutatividade Fraca por Bijeção entre Grupos Abelianos

Goiânia
2010

Dados Internacionais de Catalogação na Publicação (CIP)
GPT/BC/UFG

M134c

Macedo, Silvio Sandro Alves de.
Comutatividade fraca por bijeção entre grupos abelianos [manuscrito] / Silvio Sandro Alves de Macedo. - 2010.
xv, 69 f. : figs, tabs.

Orientador: Prof. Dr. Ricardo Nunes de Oliveira; Co-orientador: Paulo Henrique de Azevedo Rodrigues.
Dissertação (Mestrado) – Universidade Federal de Goiás, Instituto de Matemática e Estatística, 2010.
Bibliografia.
Inclui lista de figuras, abreviaturas, siglas e tabelas.
Apêndices.

1. Grupos livres. 2. Apresentação de grupos. 3. Comutatividade fraca. I. Título.

CDU: 512.541

SILVIO SANDRO ALVES DE MACEDO

Comutatividade Fraca por Bijeção entre Grupos Abelianos

Dissertação apresentada ao Programa de Pós–Graduação do Instituto de Matemática e Estatística da Universidade Federal de Goiás, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de concentração: Álgebra.

Orientador: Prof. Dr. Ricardo Nunes de Oliveira

Coorientador: Prof. Dr. Paulo Henrique de Azevedo Rodrigues

Goiânia
2010

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR AS TESES E DISSERTAÇÕES ELETRÔNICAS (TEDE) NA BIBLIOTECA DIGITAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio da Biblioteca Digital de Teses e Dissertações (BDTD/UFG), sem ressarcimento dos direitos autorais, de acordo com a Lei nº 9610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou download, a título de divulgação da produção científica brasileira, a partir desta data.

1. Identificação do material bibliográfico: **[X] Dissertação** **[ ] Tese**

2. Identificação da Tese ou Dissertação

Autor (a):	Silvio Sandro Alves de Macedo					
E-mail:	silviosiandro@yahoo.com.br					
Seu e-mail pode ser disponibilizado na página? [X]Sim [ ] Não						
Vínculo empregatício do autor						
Agência de fomento		Coordenação de Aperfeiçoamento de Pessoa: l de Nível Superior		Sigla:	CAPES	
País:	Brasil	UF:	DF	CNPJ:	00889834/0001-08	
Título:	Comutatividade fraca por bijeção entre grupos abelianos					
Palavras-chave:	Grupos livres, apresentação de grupos, comutatividade fraca, classe de nilpotência, classes duplas					
Título em outra língua:	Weak commutativity by bijection between abelian groups					
Palavras-chave em outra língua:	Free groups, presentations of groups, weak commutativity, nilpotency class, double cosets					
Área de concentração:	Algebra					
Data defesa: (28/06/2010)						
Programa de Pós-Graduação:	Mestrado em Matemática					
Orientador (a):	Ricardo Nunes de Oliveira					
E-mail:	ricardo@mat.ufg.br					
Co-orientador (a):	Paulo Henrique de Azevedo Rodrigues					
E-mail:	paulo@mat.ufg.br					

3. Informações de acesso ao documento:
Liberação para disponibilização?[1] [X] total [ ] parcial

Em caso de disponibilização parcial, assinale as permissões:
[ ] Capítulos. Especifique: _____
[ ] Outras restrições: _____
Havendo concordância com a disponibilização eletrônica, torna-se imprescindível o envio do(s) arquivo(s) em formato digital PDF ou DOC da tese ou dissertação.
O Sistema da Biblioteca Digital de Teses e Dissertações garante aos autores, que os arquivos contendo eletronicamente as teses e ou dissertações, antes de sua disponibilização, receberão procedimentos de segurança, criptografia (para não permitir cópia e extração de conteúdo, permitindo apenas impressão fraca) usando o padrão do Acrobat.

_____ Data: _____ / _____ / _____
Assinatura do autor

[1] Em caso de restrição, esta poderá ser mantida por até um ano a partir da data de defesa. A extensão deste prazo suscita justificativa junto à coordenação do curso. Todo resumo e metadados ficarão sempre disponibilizados.

SILVIO SANDRO ALVES DE MACEDO

Comutatividade Fraca por Bijeção entre Grupos Abelianos

Dissertação defendida no Programa de Pós–Graduação do Instituto de Matemática e Estatística da Universidade Federal de Goiás como requisito parcial para obtenção do título de Mestre em Matemática, aprovada em 28 de Junho de 2010, pela Banca Examinadora constituída pelos professores:

Prof. Dr. Ricardo Nunes de Oliveira
Instituto de Matemática e Estatística – UFG
Presidente da Banca

Prof. Dr. Paulo Henrique de Azevedo Rodrigues
Instituto de Matemática e Estatística – UFG

Prof. Dr. Adilson Antonio Berlatto
Instituto de Ciências Exatas e da Terra - UFMT

Profa. Dra. Ticianne Proença Bueno Adorno
Instituto de Matemática e Estatística-UFG

Silvio Sandro Alves de Macedo

Dedico este trabalho à Madalena, minha mãe.

Agradecimentos

À Deus por me permitir chegar até aqui. À minha família, o alicerce da minha vida. À minha namorada por estar sempre comigo, em momentos fáceis e difíceis. Ao meu orientador Ricardo pela paciência e zêlo que dedicou a minha orientação. Ao Paulo Henrique por acreditar em mim. À todos os meus companheiros do mestrado, em especial ao Valdomiro e ao Sinomar, pessoas com as quais aprendi muito. Ao meu amigo Agenor, parceiro de sempre. Aos meus amigos Profº Josué, que me ensinou os primeiros passos e Profº Jones, que me ensinou os segundos passos. À Procon pela eficiência no trato das questões estudantis. Aos amigos que fiz na CEU IV. À CAPES pelo apoio financeiro.

Porque é preceito sobre preceito, preceito e mais preceito; regra sobre regra, regra e mais regra; um pouco aqui, um pouco ali.

Isaías 28.10,

.

Resumo

de Macedo, Silvio Sandro Alves. **Comutatividade Fraca por Bijeção entre Grupos Abelianos**. Goiânia, 2010. 69p. Dissertação de Mestrado. Instituto de Matemática e Estatística, Universidade Federal de Goiás.

O grupo de comutatividade fraca por bijeção $G(H,K,\sigma) = \langle H,K | [h,h^\sigma] = 1,\ \forall h \in H \rangle$ é definido como sendo o quociente do produto livre $H * K$ pelo fecho normal de $\{[h,h^\sigma] : \forall h \in H\}$ em $H * K$. Nessa dissertação, estudamos os resultados obtidos em 2009 por Oliveira e Sidki [7] que suportam a seguinte conjectura:

$$\text{Se } H,K \cong \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p, \text{ então } G(H,K,\sigma) \text{ é um } p\text{-grupo.}$$

Palavras–chave

Grupos livres, apresentação de grupos, comutatividade fraca, classe de nilpotência, classes duplas.

Abstract

de Macedo, Silvio Sandro Alves. **Comutatividade Fraca por Bijeção entre Grupos Abelianos**. Goiânia, 2010. 69p. MSc. Dissertation. Instituto de Matemática e Estatística, Universidade Federal de Goiás.

The weak commutativity group by bijection $G(H,K,\sigma) = \langle H,K | [h,h^{\sigma}] = 1,\ \forall h \in H \rangle$ is defined as being the quotient of the free product $H * K$ by normal closure of $\{[h,h^{\sigma}] : \forall h \in H\}$ in $H * K$. In this dissertation, we studied the results obtained in 2009 by Oliveira and Sidki [7] that support the following conjecture:

$$\text{If } H,K \cong \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p, \text{ then } G(H,K,\sigma) \text{ is } p\text{-group.}$$

Keywords

Free groups, presentations of groups, weak commutativity, nilpotency class, double cosets.

Sumário

Introdução

Em 1980, Sidki [11] introduziu o grupo de comutatividade fraca

$$\chi(H) = \langle H, H^{\varphi} | [h, h^{\varphi}] = 1, \ \ \forall h \in H \rangle,$$

definindo-o como o quociente do produto livre $H * H^{\varphi}$ ($\varphi : H \longrightarrow H^{\varphi}$ um isomorfismo) pelo fecho normal de $\{[h, h^{\varphi}] : \ \forall h \in H\}$ em $H * H^{\varphi}$, (h^{φ} denota $\varphi(h)$). Nesse artigo, Sidki fez um estudo detalhado do grupo $\chi(H)$ e obteve, dentre outros resultados, o seguinte

Teorema 0.1. *Seja $\mathscr{P}$ qualquer uma das seguintes propriedades de grupos: finitude, p-grupo, nilpotente, solúvel; então*

$$H \text{ é um } \mathscr{P}\text{-grupo} \Longrightarrow \chi(H) \text{ é um } \mathscr{P}\text{-grupo}.$$

Em 1981, Rocco [9] considerou o caso onde H é um p-grupo finito de ordem p^n, p ímpar e classe de nilpotência c e provou que $\chi(H)$ é um p-grupo de ordem divisor de $p^{2n}p^{\binom{n}{2}}$ com classe de nilpotência no máximo $2c$. Posteriormente, Gupta, Rocco e Sidki [1], obtiveram um refinamento para esse resultado, mostrando que a classe de nilpotência é no máximo $2+c$.

Seguindo outra direção, em 2009, Oliveira e Sidki [7] consideraram um caso mais geral do grupo de comutatividade fraca $\chi(H)$, a saber, quando $\sigma : H \longrightarrow K$ é uma bijeção entre grupos finitos com σ fixando a identidade, o grupo

$$G(H, K, \sigma) = \langle H, K | [h, h^{\sigma}] = 1, \ \ \forall h \in H \rangle$$

foi definido como sendo o quociente do produto livre $H * K$ pelo fecho normal de $\{[h, h^{\sigma}] : \ \forall h \in H\}$ em $H * K$. Quando $H \cong K$, poderemos escrever $G(H, \sigma)$ ao invés de $G(H, K, \sigma)$; observe que se σ for um isomorfismo, os grupos $G(H, \sigma)$ e $\chi(H)$ coincidem, assim é natural perguntar quais resultados obtidos para $\chi(H)$ continuam válidos para $G(H, K, \sigma)$. Oliveira e Sidki [7] proporam então a seguinte

Conjectura 1. *Se H e K são grupos nilpotentes finitos e $\sigma : H \longrightarrow K$ é uma bijeção fixando a identidade, então $G(H, K, \sigma)$ é nilpotente.*

Mas devido a dificuldade do problema, eles se concentraram no caso muito particular em que os grupos H e K da conjectura acima são isomorfos a $\mathbb{Z}_p \times \ldots \times \mathbb{Z}_p$, p primo. Assim o problema básico tratado nesse artigo foi o seguinte:

Conjectura 2. *Se* $H, K \cong \mathbb{Z}_p \times \ldots \times \mathbb{Z}_p$, *então* $G = G(H, K, \sigma)$ *é um p-grupo.*

Neste caso, o estudo do grupo G é facilitado pelas seguintes propriedades do grupo $H = \mathbb{Z}_p \times \ldots \times \mathbb{Z}_p$:

(i) H pode ser visto como um espaço vetorial sobre $\mathbb{Z}_p$;

(ii) Todo elemento de H possui ordem p.

Esta dissertação tem como fonte principal, o artigo de Oliveira e Sidki [7] e está dividida em dois capítulos. O primeiro capítulo traz os pré-requitos para o entendimento do problema tratado; nos estendemos um pouco mais na parte da teoria combinatória dos grupos por se tratar de um assunto ainda pouco divulgado. O segundo capítulo é o desenvolvimento do artigo principal e está dividido em nove seções. Na primeira seção, citamos sem demonstração, um critério de finitude provado por Sidki [11], da qual decorre a finitude de $G(H, K, \sigma)$. Nas Seções 2.2 e 2.3, provamos a conjectura 2 para $H = K = \mathbb{Z}_n$ e calculamos via GAP [12] os grupos $G(H, \sigma)$ com H um p-grupo abeliano elementar de ordem no máximo 16. Na Seção 2.4 provamos que se $H = \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$, então toda bijeção $\sigma : H \longrightarrow H$ permuta alguma base de H; este é um resultado técnico que utilizaremos nas Seções 2.6 e 2.9. Na Seção 2.5 mostramos que todo grupo $G(H, \sigma)$, com H p-grupo abeliano elementar, é imagem homomorfa de algum grupo $G(H, \hat{\sigma})$ com $\hat{\sigma}$ permutando os subgrupos de H. Na Seção 2.6, verificamos a Conjectura 2 quando $H = K = \mathbb{Z}_p \times \mathbb{Z}_p$. Na Seção 2.7 mostramos que para certas extensões $\tilde{H}$ e $\tilde{K}$ de H e K, o grupo $G(\tilde{H}, \tilde{K}, \tilde{\sigma})$ (para certas bijeções $\tilde{\sigma}$) é uma extensão de $G(H, K, \sigma)$ por um p-grupo abeliano elementar; esse resultado nos permitirá verificar a Conjectura 2 para uma certa quantidade de bijeções $\sigma : H \longrightarrow H$ bem maior do que o número de isomorfismos de H. A Seção 2.8 é um pequeno passo na direção da Conjectura 1, mostramos que para H e K abelianos (não necessariamente isomorfos) e $G = G(H, K, \sigma)$ temos G/G'' nilpotente. Na última seção, provamos a Conjectura 2 para p ímpar e σ uma transposição.

CAPÍTULO 1

Preliminares

Este primeiro capítulo forma um pequeno compêndio dividido em três partes: grupos solúveis e nilpotentes, grupos livres e produtos livres. Tais tópicos são pré-requisitos para a leitura do artigo principal Oliveira e Sidki [7]. Na primeia parte, a nossa referência é o capítulo 5 do livro de Rotman [10]. Para a segunda parte, a referência principal é o livro de Johnson [3], e para a última, as páginas 174-176 de Lyndon e Schupp [4] contém os resultados básicos de que precisamos, mas o leitor também poderá encontrar o assunto nas referências [3], [5], [8] e [10]. Quanto a notação, usaremos o mesmo símbolo 1 para indicar tanto o elemento neutro de um grupo como o seu subgrupo trivial $\{1\}$.

1.1 Grupos Solúveis e Nilpotentes

Uma *série normal* de um grupo G é uma sequência de subgrupos

$$G = G_0 \geq G_1 \geq \cdots \geq G_n = 1$$

em que $G_{i+1} \trianglelefteq G_i$ (G_{i+1} é um subgrupo normal de G_i) para todo i. Os *grupos fatores* desta série normal são os grupos G_i/G_{i+1} para $i = 0, 1, \ldots, n-1$; o *comprimento* desta série é o número de grupos fatores não triviais. Uma série normal na qual todos os grupos fatores são abelianos é chamada *série solúvel*.

Definição 1.1. *Um grupo G é solúvel quando ele possui uma série sóluvel.*

Naturalmente, todo grupo abeliano é solúvel. O exemplo de grupo solúvel não abeliano é o grupo simétrico S_3, de fato, a série $S_3 \geq A_3 \geq 1$ é normal e seus grupos fatores A_3 e $S_3/A_3 \cong \mathbb{Z}_2$ são abelianos.

Se G é solúvel, o comprimento da menor série solúvel de G é chamado *comprimento derivado* de G. Os grupos solúveis com comprimento derivado no máximo 1 são os grupos abelianos. Os grupos solúveis com comprimento derivado no máximo 2 são

chamados *meta-abelianos*. Assim

G é meta-abeliano se existir $N \trianglelefteq G$ tal que N e G/N são abelianos.

Proposição 1.2. *As seguintes afirmações são verdadeiras:*

(i) *Todo subgrupo de um grupo solúvel é solúvel.*

(ii) *Todo quociente de um grupo solúvel é solúvel.*

(iii) *Seja $H \trianglelefteq G$. Se H e G/H são solúveis, então G é solúvel.*

(iv) *Todo p-grupo finito é solúvel.*

Devido a (i),(ii) e (iii) da proposição acima, dizemos que a classe dos grupos solúveis é fechada a subgrupos, quocientes e extensões, respectivamente.

Sejam x, y elementos de um grupo G, o *conjugado* de x por y é denotado por $x^y = y^{-1}xy$. O *comutador* de x e y é definido por

$$[x,y] = x^{-1}y^{-1}xy.$$

O grupo $G' = \langle [x,y] : x,y \in G \rangle$, gerado por todos os comutadores em G, é chamado *subgrupo comutador* (ou *subgrupo derivado*) de G. Uma vez que $[x,y]^z = [x^z, y^z]$, para quaisquer $x,y,z \in G$, temos $G' \trianglelefteq G$. Se definirmos indutivamente

$$G = G^{(0)}, \qquad G^{(i+1)} = [G^{(i)}, G^{(i)}].$$

Obtemos uma série

$$G = G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \dots$$

que é chamada *série derivada* de G. Para esta série vale $G^{(i)} \trianglelefteq G$, para todo $i = 0, 1, \dots$. A proposição seguinte mostra a conexão entre a série derivada e a solubilidade.

Proposição 1.3. *Um grupo G é solúvel se, e somente se $G^{(n)} = 1$, para algum n natural.*

Quando G é um grupo solúvel, o menor inteiro n tal que $G^{(n)} = 1$, é precisamente o comprimento derivado de G. Como exemplo, o grupo S_3 possui comprimento derivado igual a 2 pois $S_3'' = A_3' = 1$.

Exemplo 1.1. *Seja G um grupo qualquer, o grupo G/G'' é meta-abeliano. Primeiramente, observe que G/G' é abeliano pois $G'xG'y = G'yG'x \iff [x,y] \in G'$. Temos assim que G'/G'' e $(G/G'')/(G'/G'')$ são abelianos, pois o último grupo é isomorfo a G/G'. Segue*

portanto que G/G'' é meta-abeliano.

$$\begin{array}{ccc} G & \hookrightarrow & G/G'' \\ \| & & \| \\ G' & \hookrightarrow & G'/G'' \\ \| & & \| \\ G'' & \hookrightarrow & 1 \end{array}$$

Sejam H,K subgrupos de G; o *subgrupo comutador* de H e K é definido por $[H,K] = \langle [h,k] : h \in H, k \in K \rangle$. Vamos definir indutivamente

$$\gamma_1(G) = G, \qquad \gamma_{i+1}(G) = [\gamma_i(G), G].$$

Como $\gamma_{i+1}(G) \leq \gamma_i(G)$, para todo i, obtemos uma série

$$G = \gamma_1(G) \geq \gamma_2(G) \geq \gamma_3(G) \geq \dots \tag{1-1}$$

que é chamada *série central inferior* de G. Esta série possui as seguintes propriedades:

(i) $\gamma_i(G) \trianglelefteq G$ para todo i;

(ii) $\gamma_i(G)/\gamma_{i+1}(G) \leq Z(G/\gamma_{i+1}(G))$.

Daí o motivo da série chamar-se central. A série 1-1 não precisa ser normal pois muito embora $\gamma_{i+1}(G) \trianglelefteq \gamma_i(G)$ para todo i, pode não existir um inteiro n tal que $\gamma_n(G) = 1$; mas quando existe, damos a seguinte definição:

Definição 1.4. *Um grupo G é nilpotente se existir um inteiro c tal que $\gamma_{c+1}(G) = 1$. O menor inteiro c é chamado classe de nilpotência do grupo G.*

Os grupos abelianos são os grupos nilpotentes de classe 1. Todo grupo nilpotente é solúvel, pois as propriedades (i) e (ii) acima implicam que a série

$$G = \gamma_1(G) \geq \gamma_2(G) \geq \dots \geq \gamma_{c+1}(G) = 1$$

é solúvel. Nem todo grupo solúvel é nilpotente, por exemplo, o grupo S_3 é solúvel mas não é nilpotente pois $Z(S_3) = 1$, e pela proposição abaixo, todo grupo nilpotente não-trivial possui centro não-trivial.

Proposição 1.5. *Se G é um grupo nilpotente de classe c, então as seguintes afirmações são verdadeiras:*

(i) G é solúvel.

(ii) Se $G \neq 1$, então $Z(G) \neq 1$.

(iii) Todo subgrupo H de G é nilpotente de classe no máximo c.

(iv) Se $H \trianglelefteq G$, então G/H é nilpotente de classe no máximo c.

Os itens (iii) e (iv) dessa proposição dizem que a classe dos grupos nilpotentes é fechada a subgrupos e quocientes. Ao contrário dos grupos solúveis, a classe dos grupos nilpotentes não é fechada a extensões: A_3 e $S_3/A_3 \cong \mathbb{Z}_2$ são nilpotentes mas S_3 não é nilpotente.

Sejam x,y,z elementos de um grupo G, o comutador de peso 3 é definido por $[x,y,z] = [[x,y],z]$. Mais geralmente, um comutador de peso $n \geq 2$ é definido indutivamente:

$$[x_1,x_2,...,x_n] = [[x_1,x_2,...,x_{n-1}],x_n].$$

Vamos listar na forma de um lema, as identidades de comutadores que utilizaremos ao longo do texto.

Lema 1.6. *Sejam x,y,z elementos de um grupo. Então:*

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

(ii) $[x,y]^{-1} = [y,x] = \left[x^y,y^{-1}\right]$;

(iii) $[xy,z] = [x,z]^y[y,z]$ e $[x,yz] = [x,z][x,y]^z$;

(iv) $\left[x,y^{-1},z\right]^y\left[y,z^{-1},x\right]^z\left[z,x^{-1},y\right]^x = 1$ (Identidade de Witt);

(v) $\left[x^{-1},y\right] = ([x,y]^{x^{-1}})^{-1}$ e $\left[x,y^{-1}\right] = ([x,y]^{y^{-1}})^{-1}$;

(vi) $[x,y] = \left[x,y^{-1}\right]^{-y} = \left[x^{-1},y\right]^{-x}$.

Prova. São diretas se desenvolvermos separadamente, cada membro das identidades usando a definição de comutador.

□

Seja G um grupo e $R \subseteq G$ um subconjunto qualquer, defina $\langle R\rangle^G = \langle r^g : r \in R, g \in G\rangle$. É de fácil verificação que

$$\langle R\rangle^G \text{ é o menor subgrupo normal de } G \text{ contendo } R,$$

ou equivalentemente, $\langle R\rangle^G$ é o subgrupo normal de G gerado por R. Chamaremos este subgrupo de *fecho normal de R em G*. A proposição seguinte dá uma descrição dos termos da série central inferior através do fecho normal de comutadores.

Proposição 1.7. *Seja $G = \langle x_1,x_2,...,x_n\rangle$ e R o conjunto formado por todos os comutadores $\left[x_{j_1},x_{j_2},...,x_{j_i}\right]$ de peso i, onde $1 \leq j_r \leq n$. Então $\gamma_i(G) = \langle R\rangle^G$.*

Prova. Primeiramente mostremos que $\gamma_i(G) = \langle [g_1,\ldots,g_i] : g_1,\ldots,g_i \in G\rangle$. Isto é claro para $i = 2$. Suponha que o resultado seja verdadeiro para algum i. Por definição $\gamma_{i+1}(G) = [\gamma_i(G), G]$. Pondo

$$\begin{aligned} H &= \langle [g_1,\ldots,g_{i+1}] : g_1,\ldots,g_{i+1} \in G\rangle, \\ &= \langle [[g_1,\ldots,g_i], g_{i+1}] : g_1,\ldots,g_{i+1} \in G\rangle. \end{aligned}$$

Temos $H \leq \gamma_{i+1}(G)$ e $H \trianglelefteq G$. Como

$$[g_1,\ldots,g_{i+1}] \in H \Longleftrightarrow \gamma_i(G) \text{ e } G \text{ comutam módulo } H \Longleftrightarrow \gamma_{i+1}(G) = [\gamma_i(G), G] \leq H,$$

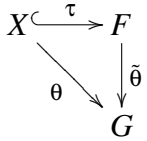
obtemos $\gamma_{i+1}(G) = H$ e a indução está completa. Agora sejam $g_1 = x_1^{s_1},\ldots,x_n^{s_n},\ldots,g_i = x_1^{t_1},\ldots,x_n^{t_n}$. Aplicando as identidades $[a,bc] = [a,c][a,b]^c$ e $[ab,c] = [a,c]^b[b,c]$ repetidas vezes no comutador $[x_1^{s_1},\ldots,x_n^{s_n};\ldots;x_1^{t_1},\ldots,x_n^{t_n}]$ vemos que $[g_1,\ldots,g_i] \in \langle R\rangle^G$ e consequentemente $\gamma_i(G) \leq \langle R\rangle^G$. Como $\gamma_i(G)$ é um subgrupo normal de G contendo R, segue que $\gamma_i(G) = \langle R\rangle^G$. □

Corolário 1.8. *Um grupo G é nilpotente de classe no máximo c se, e somente se, qualquer comutador de peso $c+1$ nos geradores de G é trivial.*

1.2 Grupos Livres

Uma palavra sobre a notação: Se $f : X \longrightarrow Y$ é uma função e $x \in X$, escreveremos x^f ao invés de $f(x)$ e X^f ao invés de $f(X)$. Poderemos também escrever $f : x \longrightarrow y$ para indicar que y é a imagem de x por f.

Definição 1.9. *Um grupo F é livre sobre um subconjunto $X \subseteq F$ se, dado qualquer grupo G e qualquer aplicação $\theta : X \longrightarrow G$, existir um único homomorfismo $\tilde{\theta} : F \longrightarrow G$ estendendo θ, isto é, $x^{\tilde{\theta}} = x^{\theta}$ para todo $x \in X$.*



Exemplo 1.2. *O grupo cíclico infinito $F = \langle a\rangle$ é livre em $X = \{a\}$.*
Seja G um grupo qualquer e $a^{\theta} = g$, com $g \in G$. Como F é infinito, a aplicação $(a^n)^{\tilde{\theta}} = g^n$ está bem definida e claramente é o único homomorfismo que estende θ.

Lema 1.10. *Se F é livre em X, então F é gerado por X.*

Prova. Seja $\theta : X \longrightarrow \langle X \rangle$ a aplicação inclusão com sua extensão $\tilde{\theta} : F \longrightarrow \langle X \rangle$. Seja $\tau : \langle X \rangle \longrightarrow F$ uma inclusão, assim $\tilde{\theta}\tau : F \longrightarrow F$ estende a inclusão $\theta\tau : X \longrightarrow F$, como esta inclusão também é estendida à aplicação identidade em F, por unicidade, $\tilde{\theta}\tau = 1_F$ e isto implica que $\tilde{\theta}$ é uma inclusão de F em $\langle X \rangle$, donde $F \subseteq \langle X \rangle$. □

Quando F é livre em X, dizemos que F tem base X. O cardinal $|X|$ é chamado *posto* de F, denotado por $r(F)$. O próximo resultado garante que o posto de um grupo livre está bem definido.

Proposição 1.11. *Sejam F_1 livre em X_1 e F_2 livre em X_2, então $F_1 \cong F_2$ se, e somente se $|X_1| = |X_2|$.*

Prova. Suponha $|X_1| = |X_2|$ e seja $\sigma : X_1 \longrightarrow X_2$ uma bijecão com inversa σ^{-1}. Seja $\phi_1 : F_1 \longrightarrow F_2$ a extensão de $X_1 \xrightarrow{\sigma} X_2 \hookrightarrow F_2$ e $\phi_2 : F_2 \longrightarrow F_1$ a extensão de $X_2 \xrightarrow{\sigma^{-1}} X_1 \hookrightarrow F_1$. Dado $x \in X_1$, temos

$$x^{\phi_1\phi_2} = (x^{\sigma})^{\phi_2} = (x^{\sigma})^{\sigma^{-1}} = x,$$

logo $\phi_1\phi_2 : F_1 \longrightarrow F_2$ estende a inclusão $X_1 \hookrightarrow F_1$. Como a aplicação identidade 1_{F_1} também estende esta inclusão, por unicidade temos $\phi_1\phi_2 = 1_{F_1}$, analogamente $\phi_2\phi_1 = 1_{F_2}$ e segue, portanto, que ϕ_1 é um isomorfismo de F_1 em F_2.
Para provar a recíproca, observe que pela definição de grupo livre, existe uma bijeção entre $Map(X_i, G)$ (o conjunto de todas as aplicações de X_i em G) e $Hom(F_i, G)$ (o conjunto de todos os homomorfismos de F_i em G), $i = 1, 2$. Tomando $G = \mathbb{Z}_2$, da hipótese $F_1 \cong F_2$ obtemos $|Hom(F_1, \mathbb{Z}_2)| = |Hom(F_2, \mathbb{Z}_2)|$, logo

$$|Map(X_1, \mathbb{Z}_2)| = |Map(X_2, \mathbb{Z}_2)| \Longrightarrow 2^{|X_1|} = 2^{|X_2|} \Longrightarrow |X_1| = |X_2|.$$

□

Observação 1.12. *Na última implicação da proposição acima, usamos a seguinte lei de cancelamento da aritmética cardinal: $\gamma^{\alpha} = \gamma^{\beta}$ implica $\alpha = \beta$ (veja [2], p. 95).*

Seja X um conjunto arbitrário. Nosso objetivo será construir um grupo livre $F(X)$, tendo X como base. Considere um novo conjunto $X^{-1} = \{x^{-1} : x \in X\}$, obtido de X por meio da bijeção $x \to x^{-1}$ e seja $X^* = X \cup X^{-1}$. Utilizando a inversa de $x \to x^{-1}$, interpretamos $(x^{-1})^{-1} = x$.

Definição 1.13. *Uma palavra em X^* é uma l-upla $a = (x_1, x_2, ..., x_l)$, onde cada $x_i \in X^*$. A palavra diz-se reduzida quando não possui os símbolos x, x^{-1} em posições adjacentes.*

Escreveremos simplesmente $a = x_1x_2...x_l$ e quando a for reduzida, diremos que possui comprimento l, denotado por $|a| = l$. A palavra de comprimento nulo, isto é, que

não contém nenhum símbolo, será denotada por 1. De agora em diante, $F(X)$ denotará o conjunto de todas as palavras reduzidas em X, claramente $1 \in F(X)$.

Teorema 1.14. *$F(X)$ forma um grupo livre em X.*

Prova. Dados $a = x_1...x_l$ e $b = y_1...y_m$ em $F(X)$, defina o produto

$$ab = x_1...x_{l-r}y_{r+1}...y_m,$$

onde r é o menor valor que torna ab reduzida. A palavra vazia 1 é a identidade e a palavra $a^{-1} = x_l^{-1}...x_1^{-1}$ é o inverso de a. Vamos verificar a associatividade. Sejam

$$c = z_1...z_n, \quad bc = y_1....y_{m-s}z_{s+1}...z_n.$$

Existem três casos a considerar:

(i) $r + s < m$: a palavra b não foi cancelada, logo $(ab)c = a(bc) = x_1...x_{l-r}y_{r+1}...y_{m-s}z_{s+1}...z_n$.

(ii) $r+s = m$: somente a palavra b foi cancelada, assim $(ab)c = a(bc) = x_1...x_{l-r}z_{s+1}...z_n$.

(iii) $r+s > m$: cancelou-se b e símbolos de a ou c. Façamos

$$\beta = y_1...y_{m-s}, \quad \gamma = y_{m-s+1}...y_r, \quad \delta = y_{r+1}...y_m.$$

Observe que $\gamma \neq 1$, pois γ possui $r+s-m > 0$ símbolos. Temos assim

$$\begin{aligned} b &= \beta\gamma\delta \\ a &= \alpha\gamma^{-1}\beta^{-1} \qquad \text{onde } \alpha = x_1...x_{l-r} \\ c &= \delta^{-1}\gamma^{-1}\varepsilon \qquad \text{onde } \varepsilon = z_{s+1}...z_n \\ (ab)c &= (\alpha\delta)(\delta^{-1}\gamma^{-1}\varepsilon) = \alpha(\gamma^{-1}\varepsilon) \\ a(bc) &= (\alpha\gamma^{-1}\beta^{-1})(\beta\varepsilon) = (\alpha\gamma^{-1})\varepsilon. \end{aligned}$$

Como α e γ^{-1} são adjacentes na palavra reduzida a, segue que $\alpha(\gamma^{-1}\varepsilon)$ é a forma reduzida de $(ab)c$, analogamente, $(\alpha\gamma^{-1})\varepsilon$ é a forma reduzida de $a(bc)$. Pelo caso (ii), obtemos $a(bc) = (ab)c$.

Vamos mostrar que $F(X)$ é livre em X. Seja G um grupo arbitrário e $\theta : X \longrightarrow G$ uma aplicação qualquer, dado $w = x_1...x_l \in F(X)$, defina $\tilde{\theta} : F(X) \longrightarrow G$ por

$$w^{\tilde{\theta}} = x_1^{\theta}...x_l^{\theta}, \quad 1^{\tilde{\theta}} = 1, \quad x^{\tilde{\theta}} = x, \quad (x^{-1})^{\tilde{\theta}} = (x^{\theta})^{-1} \text{ com } x \in X.$$

Mostremos que $\tilde{\theta}$ é um homomorfismo. Sejam a, b e ab como definidos acima,

$$\begin{aligned} a^{\tilde{\theta}}b^{\tilde{\theta}} &= x_1^{\theta}\dots x_l^{\theta}y_1^{\theta}\dots y_m^{\theta} \\ &= x_1^{\tilde{\theta}}\dots x_{l-r}^{\tilde{\theta}}(y_r^{-1})^{\tilde{\theta}}\dots(y_1^{-1})^{\tilde{\theta}}y_1^{\tilde{\theta}}\dots y_r^{\tilde{\theta}}y_{r+1}^{\tilde{\theta}}\dots y_m^{\tilde{\theta}} \\ &= x_1^{\tilde{\theta}}\dots x_{l-r}^{\tilde{\theta}}y_{r+1}^{\tilde{\theta}}\dots y_m^{\tilde{\theta}} \\ &= (ab)^{\tilde{\theta}}. \end{aligned}$$

Agora pela própria construção de $F(X)$, temos que X gera $F(X)$, disso decorre a unicidade de $\tilde{\theta}$. □

Muitos resultados na teoria de grupos livres são provados com indução sobre a ordem das palavras, por isso, a seguinte caracterização é fundamental.

Proposição 1.15. *Um grupo F é livre em um subconjunto X se, e somente se*

(i) *X gera F;*

(ii) *Toda palavra reduzida em X^* de comprimento positivo é diferente de 1.*

Prova. Seja $\tilde{\theta}: F(X) \longrightarrow F$ o homomorfismo que estende a inclusão $\theta: X \longrightarrow F$. Se (i) e (ii) são válidas, então $\tilde{\theta}$ é um isomorfismo, logo F é livre em X. Reciprocamente, seja F livre em X e $\tilde{\phi}: F \longrightarrow F(X)$ a extensão da inclusão $\phi: X \longrightarrow F(X)$. Como X gera F, (Lema 1.10), temos $\tilde{\phi}\tilde{\theta} = 1_F$, analogamente, $\tilde{\theta}\tilde{\phi} = 1_{F(X)}$ e sendo $\tilde{\theta}$ um isomorfismo, valem (i) e (ii). □

Proposição 1.16. *Todo grupo é isomorfo a um quociente de grupo livre.*

Prova. Dado um grupo G seja X um conjunto gerador para G (X sempre existe, tome $X = G$, por exemplo). Seja $\tilde{\theta}: F(X) \longrightarrow G$ a extensão da inclusão $\theta: X \longrightarrow G$. Como $G = \langle X \rangle$, temos $Im(\tilde{\theta}) = G$, logo $G = Im(\tilde{\theta}) \cong F(X)/Ker(\tilde{\theta})$. □

Definição 1.17. *Uma palavra reduzida $a = x_1x_2\dots x_l$, $x_i \in X^*$, é chamada ciclicamente reduzida quando $x_l \neq x_1^{-1}$.*

Claramente, toda palavra reduzida a é do tipo $a = u^{-1}\widehat{a}u$ onde $\widehat{a}$ é ciclicamente reduzida. Quando $a \neq 1$, temos $\widehat{a} \neq 1$ e para todo natural n, $\widehat{a}^n$ é ciclicamente reduzida, disto segue que $a^n = u^{-1}\widehat{a}^n u \neq 1$ quando $a \neq 1$. Concluimos assim que todo subgrupo não trivial de $F(X)$ é infinito, em particular, $F(X)$ é infinito. Note que se F é um grupo livre arbitrário com base X, então pela Proposição 1.11, podemos escrever $F = F(X)$. A seguir, vamos demonstrar algumas propriedades dos grupos livres.

Lema 1.18. *Se $a,b \in F(X)$ são tais que $ab = ba$, então existe $c \in F(X)$ tal que $a = c^k$ e $b = c^h$ com $k,h \in \mathbb{Z}$.*

Prova. Sejam $a = x_1...x_l$ e $b = y_1...y_m$ com $l \leq m$, usaremos indução sobre $|a|+|b|$. De $ab = ba$ temos

$$x_1...x_{l-r}y_{r+1}...y_m = y_1...y_{m-r}x_{r+1}...x_l.$$

Admitindo $0 \leq l \leq m$, temos três possibilidades:

(i) $r = 0$. Segue da expressão acima que $x_i = y_i, i = 1,...,l$. Assim $b = au$ com $|u| = m-l < m$ e $|a|+|u| < |a|+|b|$. Agora $[a,u] = [a,au] = [a,b] = 1$ e por hipótese de indução, a e u são potências de algum $c \in F(X)$, o mesmo valendo para $b = au$.

(ii) $r = l$. Temos $y_i = x_{l-i+1}^{-1}, 1 \leq i \leq l$ e $b = a^{-1}u$ com $|u| = m-l \leq m$. O resultado segue de modo análogo ao caso (i).

(iii) $0 \leq r < l$. Neste caso temos $x_1 = y_1, x_l = y_m$ e $y_m = x_1^{-1}$, consequentemente $a = (a')^{x_1}$ e $b = (b')^{x_1}$ onde $a' = x_2...x_{l-1}$ e $b' = y_2...y_{m-1}$ com $|a'| = l-2$ e $|b'| = m-2$. Assim

$$\begin{aligned} 1 = [a,b] &= \left[(a')^{x_1},(b')^{x_1}\right] \\ &= \left[a',b'\right] \qquad \text{(conjugando por } x_1^{-1}\text{)}. \end{aligned}$$

Segue da hipótese de indução que a' e b' são potências de algum c', consequentemente a,b são potências de $c = (c')^{x_1}$.

□

Observação 1.19. *Seja F um grupo livre e $a,b \in F$ satisfazendo $a^n = b^n$ com $n \geq 1$ inteiro. Pondo $a = u^{-1}\widehat{a}u$ e $b = v^{-1}\widehat{b}v$ com $\widehat{u},\widehat{v}$ ciclicamente reduzidas, das equações $a^n = b^n$ e $a^{2n} = b^{2n}$, obtemos*

$$\begin{aligned} n|\widehat{a}|+2|u| &= n|\widehat{b}|+2|v|; \\ 2n|\widehat{a}|+2|u| &= 2n|\widehat{b}|+2|v|. \end{aligned}$$

Subtraindo membro a membro, temos $|\widehat{a}| = |\widehat{b}|$ e $|u| = |v|$. Como não há cancelamentos na igualdade $u^{-1}\widehat{a}^n u = v^{-1}\widehat{b}^n v$, obtemos $u = v$ e $\widehat{a} = \widehat{b}$ o que implica $a = b$. Vamos utilizar esta observação para generalizar o Lema 1.18.

Lema 1.20. *Se $a^h b^k = b^k a^h$, com a e b pertencendo ao grupo livre F e h,k inteiros não nulos, então $ab = ba$. Assim a e b são potências de um mesmo elemento.*

Prova. Como $a^{\pm h}$ comuta com $b^{\pm k}$, podemos assumir que h,k são inteiros positivos. Como

$$a^h = b^k a^h b^{-k} = (b^k a b^{-k})^h,$$

segue da observação anterior que $a = b^k a b^{-k}$, isto é $b^k = (a^{-1}ba)^k$, novamente pela observação anterior, $b = a^{-1}ba$. □

Lema 1.21. *Para todo $a \neq 1$ pertencente a um grupo livre F, o centralizador $C_F(a) = \{u \in F : ua = au, u \in F\}$ é um grupo abeliano.*

Prova. Sejam $u, v \in C_F(a)$ com $ua = au$ e $va = av$. Pelo Lema 1.18 (ou lema anterior), existem inteiros p, q, r, s tais que

$$u = b^p,\ a = b^q,\ v = d^r,\ a = d^s.$$

Como b^q e d^s comutam (porque são iguais), segue do lema anterior que b e d são potências de um elemento em comum c. De $u = b^p$ e $v = d^r$ temos que u e v também são potências de c e portanto comutam. □

Proposição 1.22. *Para todo $a \neq 1$ em um grupo livre F, $C_F(a)$ é um grupo cíclico.*

Prova. Seja $d \neq 1$ um elemento de comprimento minimal em $C_F(a)$ e $v \in C_F(a)$ arbitrário. Afirmamos que v é potência de d. De fato, como v comuta com d (Lema 1.21), pelo Lema 1.18, existem inteiros h, k e $c \in F$ tais que

$$d = c^h, \quad v = c^k.$$

Da segunda equação c^k comuta com a, consequentemente $c \in C_F(a)$ (Lema 1.20). Da primeira equação

$$\begin{aligned} |d| = |c^h| = |(u^{-1}\widehat{c}u)^h| &= |h||\widehat{c}| + 2|u|, \\ &= |h||\widehat{c}| + (|c| - |\widehat{c}|) \quad \text{(por substituição de } 2|u| = |c| - |\widehat{c}|), \\ &= (|h| - 1)|\widehat{c}| + |c|. \end{aligned}$$

Sendo $d \neq 1$, temos $h \neq 0$. Como $c \in C_F(a)$, segue da minimalidade de $|d|$ que $|h| = 1$, logo $v = d^{\pm k}$. □

Proposição 1.23. *Um grupo livre F é nilpotente se, e somente se $r(F) = 1$.*

Prova. Um grupo livre de posto 1 é cíclico infinito, portanto nilpotente pelo Exemplo 1.2. Para a recíproca, observe que se $F \neq 1$ for nilpotente, então possui centro $Z(F)$ não trivial (Proposição 1.5). Tomando $a \in Z(F)$, como $a^w = a$ para todo $w \in F$, temos $F = C_F(a)$. Sendo $C_F(a)$ um subgrupo cíclico (lema anterior), o resultado segue.

□

Vejamos agora um exemplo concreto de grupo livre

Exemplo 1.3. *Sejam* α *e* β *funções sobre o conjunto* $\mathbb{C}\cup\{\infty\}$ *definidas por*

$$x^{\alpha}=\begin{cases} x+2, & se \quad x\in\mathbb{C}\backslash\{\infty\} \\ \infty, & se \quad x=\infty \end{cases} \quad x^{\beta}=\begin{cases} \frac{x}{2x+1}, & se \quad x\in\mathbb{C}\backslash\{\frac{-1}{2},\infty\} \\ \infty. & se \quad x=\frac{-1}{2} \\ \frac{1}{2}, & se \quad x=\infty \end{cases}$$

Observe que α *e* β *possuem inversas dadas por:*

$$x^{\alpha^{-1}}=\begin{cases} x-2, & se \quad x\in\mathbb{C}\backslash\{\infty\} \\ \infty, & se \quad x=\infty \end{cases} \quad x^{\beta^{-1}}=\begin{cases} \frac{x}{1-2x}, & se \quad x\in\mathbb{C}\backslash\{\frac{1}{2},\infty\} \\ \infty. & se \quad x=\frac{1}{2} \\ \frac{-1}{2}, & se \quad x=\infty \end{cases}$$

Assim α *e* β *geram um grupo de permutações de* $\mathbb{C}\cup\{\infty\}$. *Vamos mostrar que* $\langle\alpha,\beta\rangle$ *é um grupo livre sobre* $\{\alpha,\beta\}$. *Primeiramente, observe que* $x\in\mathbb{C}$, $|x|>1 \Longrightarrow |x^{\beta}|<1$, *isto é,* β *leva os pontos exteriores ao círculo unitário* S^1 *ao interior de* $S^1\backslash\{0\}$*; a mesma afirmação vale para* β^{-1} *pois se não fosse assim, existiriam* $x,y\in\mathbb{C}\backslash S^1$ *tal que* $\beta^{-1}: x\longrightarrow y$, *donde* $\beta: y\longrightarrow x$, *contradição. Concluímos assim que* β^n *aplica* $\mathbb{C}\backslash S^1$ *em* $S^1\backslash\{0\}$, *para todo inteiro* $n\neq 0$. *Claramente* α^m *aplica o interior de* S^1 *no exterior de* S^1 *e o exterior de* S^1 *no exterior de* S^1, *para todo inteiro* $m\neq 0$. *Com excessão de* β^n, *nenhuma outra palavra reduzida em* α,β *pode fixar a origem, logo toda palavra reduzida em* α,β *é diferente de* 1, *segue então pela Proposição 1.15 que* $\langle\alpha,\beta\rangle$ *é um grupo livre.*

1.2.1 O teorema de Schreier

Provaremos nesta seção, o famoso teorema de Schreier que afirma que todo subgrupo H de um grupo livre F é livre, mais ainda, se $|F:H|$ for finito, então $r(H)=(r(F)-1)|F:H|+1$. O primeiro passo na direção da prova é ordenar o grupo F.

Uma relação binária $<$ sobre um conjunto S é chamada de relação de boa ordem se satisfaz as quatro propriedades seguintes:

(i) $\forall s\in S, s\not< s$ (não reflexiva),

(ii) $s<t$ e $t<u \Longrightarrow s<u$ (transitiva),

(iii) $\forall s,t\in S, s<t$ ou $s=t$ ou $t<s$ (tricotomia),

(iv) Todo subconjunto não vazio de S contém um menor elemento.

Sabe-se da teoria dos conjuntos que qualquer conjunto pode ser bem ordenado (veja [2], p. 59). Seja $F=F(X)$, existe então uma boa ordem $<$ para X^*. Vamos definir uma relação de ordem para F a partir da boa ordem de X^*. Dados $a=x_1\ldots x_l, b=$

$y_1 \dots y_m \in F$, defina $a < b$ se $|a| < |b|$ ou se $|a| = |b|$ e $x_r < y_r$, onde $r = min\{i : x_i \leq y_i\}$. Não é difícil mostrar que $<$ é uma boa ordem para F.

Exemplo 1.4. *Seja $F = F(x,y)$ um grupo livre de posto 2, onde $X^* = X \cup X^{-1}$ é ordenado por $x < y < x^{-1} < y^{-1}$. Os primeiros 24 elementos de F são:*

$$1 < x < y < x^{-1} < y^{-1} < x^2 < xy < xy^{-1} < yx < y^2 < yx^{-1} < x^{-1}y < x^{-2} < x^{-1}y^{-1} < y^{-1}x < y^{-1}x^{-1} < y^{-2} < x^3 < x^2y < x^2y^{-1} < xyx < xy^2 < xyx^{-1} < xy^{-1}x < \dots.$$

A partir de agora, consideraremos F com a ordem $<$.

Lema 1.24. *Seja $w = x_1 \dots x_n$ uma palavra reduzida em X^* com $n > 1$ e $v \in F$ arbitrário. Então*

$$v < x_1 \dots x_{n-1} \ \ implica \ \ vx_n < w.$$

Prova. Se $|v| < n-1$, então $|vx_n| < n = |w|$ e o resultado segue. Podemos então assumir que $v = x_1 \dots x_{r-1} y_r \dots y_{n-1}$ é reduzida com $1 \leq r \leq n-1$ e $y_r < x_r$. Se $y_{n-1} = x_n^{-1}$, então $|vx_n| = n-2 < |w|$, se não, $vx_n = x_1 \dots x_{r-1} y_r \dots y_{n-1} x_n$ é reduzida. Em quanquer dos dois casos, $vx_n < w$.

□

Seja G um grupo e $H \leq G$. O conjunto U formado pela escolha de um representante de cada classe lateral Hg é chamado *transversal* de H em G. Para grupos livres, temos um tipo especial de transversal.

Definição 1.25. *Um transversal U de H em F é chamado transversal de Schreier (TS), se qualquer palavra $w \in U$ contém todos os seus segmentos iniciais, isto é*

$$w = x_1 \dots x_n \in U \ \ implica \ \ x_1 \dots x_{n-1} \in U. \tag{1-2}$$

Observe que todo transversal de Schreier deve conter a palavra vazia $1 \in F$.

Lema 1.26. *Todo subgrupo H de F possui um transversal de Schreier.*

Prova. Seja U o transversal consistindo do menor elemento de cada classe lateral de H em F. Vamos mostrar que U satisfaz a contrapositiva de (1-2). Seja $w = x_1 \dots x_{n-1} x_n$ e suponha que $x_1 \dots x_{n-1} \notin U$. Seja $v \in U$ o menor elemento de $Hx_1 \dots x_{n-1}$. Agora

$$\begin{aligned} v < x_1 \dots x_{n-1} &\implies vx_n < w \qquad \text{(pelo Lema 1.24)} \\ Hv = Hx_1 \dots x_{n-1} &\implies Hvx_n = Hw. \end{aligned}$$

Assim $vx_n \in Hw$ e $vx_n < w$, logo w não pode ser o menor elemento de Hw, consequentemente $w \notin U$. □

Seja $H \leq F$ e U um transversal de H em F, dado $w \in F$ definimos $\overline{w}$ por $Hw \cap U = \{\overline{w}\}$. Valem as seguintes propriedades:

$$\overline{w} = w \Leftrightarrow w \in U, \ Hw = H\overline{w}, \ \overline{\overline{w}} = w, \forall w \in F.$$

Assim, dado $x \in X^*$ e $u \in U$, temos que $Hux = H\overline{ux}$ implica $Hu = H\overline{ux}x^{-1}$, como $\overline{\overline{ux}x^{-1}} \in Hu \cap U = \{u\}$ segue que

$$\overline{\overline{ux}x^{-1}} = u, \forall u \in U, x \in X^*. \tag{1-3}$$

Lema 1.27. *Se $H \leq F$ e U é um transversal de H em F qualquer contendo a identidade, então o conjunto $A = \{ux\overline{ux}^{-1} : u \in U, x \in X^*\}$ gera H.*

Prova. Como $Hux = H\overline{ux}$, é claro que $A \subseteq H$. Agora dado $h \in H$ seja

$$h = x_1 x_2 ... x_n, \ x_i \in X^*,$$

e defina indutivamente: $u_1 = 1$, $u_{i+1} = \overline{u_i x_i}$, $1 \leq i \leq n$. Pondo $a_i = u_i x_i u_{i+1}^{-1} = u_i x_i \overline{u_i x_i}^{-1} \in A$, $1 \leq i \leq n$, temos

$$a_1 a_2 ... a_n = x_1 x_2 ... x_n u_{n+1}^{-1} = h u_{n+1}^{-1}.$$

Como o lado direito da igualdade acima pertence a H, obtemos $u_{n+1} \in H$. Mas $u_{n+1} \in U$ e $H \cap U = 1$, logo $u_{n+1} = 1$ e h fica expresso como uma palavra nos elementos de A.

□

Observe que no lema acima não usamos o fato de F ser livre em X, mas apenas gerado por X. Decorre então o seguinte: Se G é um grupo finitamente gerado e $H \leq G$ com $|G : H| < \infty$, então H é finitamente gerado.

O lema seguinte mostra que o conjunto A possui geradores redundantes, isto é, podemos obter um conjunto gerador B para H de tamanho menor do que A.

Lema 1.28. *Considere os conjuntos:*

$$\begin{aligned} B &= \{ux\overline{ux}^{-1} : u \in U, x \in X, ux \notin U\}, \\ \widehat{B} &= \{ux\overline{ux}^{-1} : u \in U, x \in X^{-1}, ux \notin U\}, \\ B^{-1} &= \{b^{-1} : b \in B\}. \end{aligned}$$

Temos $B^{-1} = \widehat{B}$ e portanto $A \setminus \{1\} = B \cup B^{-1}$, onde a união é disjunta.

Prova. Sejam $u \in U$ e $x \in X^*(= X \cup X^{-1})$, decorre de (1-3) que

$$(ux\overline{ux}^{-1})^{-1} = \overline{ux}x^{-1}u^{-1} = \overline{ux}x^{-1}(\overline{\overline{ux}x^{-1}})^{-1} \text{ e}$$

$$ux \notin U \Leftrightarrow ux \neq \overline{ux} \Leftrightarrow u \neq \overline{ux}x^{-1} \Leftrightarrow \overline{\overline{ux}x^{-1}} \neq \overline{ux}x^{-1} \Leftrightarrow \overline{ux}x^{-1} \notin U.$$

Se tomarmos $x \in X$ e $x \in X^{-1}$ acima, obtemos respectivamente $B^{-1} \subseteq \widehat{B}$ e $\widehat{B}^{-1} \subseteq B$. A segunda inclusão é equivalente a $\widehat{B} \subseteq B^{-1}$, deste modo $B^{-1} = \widehat{B}$. Agora observe que $ux\overline{ux}^{-1} = 1$ se, e somente se $ux \in U$, assim $A\backslash\{1\} = B \cup B^{-1}$. □

No lema abaixo, o transversal U da definição de B e B^{-1}, é de Schreier.

Lema 1.29. *Sejam $b = ux\overline{ux}^{-1}, b' = vy\overline{vy}^{-1} \in B \cup B^{-1} = A\backslash\{1\}$. Com exceção do caso*

$$v = \overline{ux},\ y = x^{-1},\ u = \overline{vy}, \tag{1-4}$$

a forma reduzida do produto bb' em X^* é igual a

$$uxwy\overline{vy}^{-1},$$

para algum $w \in F$. Em outras palavras, no produto bb' não há cancelamento dos fatores médios x e y.

Prova. Podemos olhar apenas para $x\overline{ux}^{-1}vy$, e mostrar que sua forma reduzida é xwy. Sejam $\overline{ux} = x_1x_2...x_l$ e $v = y_1y_2...y_m$ palavras reduzidas em X^*. Observe que

(1) $y_m \neq y^{-1}$, caso contrário, $vy = y_1 \cdots y_{m-1} \in U$ (porque U é TS) e teríamos $vy = \overline{vy}$, donde $b' = 1$, o que contraria a hipótese.

(2) $x_l \neq x$, caso contrário

$$\begin{aligned} ux &= \overline{\overline{ux}x^{-1}}x \qquad \text{(por (1-3))}, \\ &= \overline{x_1 \cdots x_l x^{-1}}x, \\ &= \overline{x_1 \cdots x_{l-1}}x, \\ &= x_1 \cdots x_{l-1}x \qquad \text{(porque } \overline{ux} \in U, \text{ que é TS)}, \\ &= \overline{ux} \in U, \end{aligned}$$

e seria $ux \in U$, contradição. Desse modo, $\overline{ux}^{-1}$ não cancela x e v não cancela y, resta analisar o cancelamento entre $\overline{ux}^{-1}$ e v. A forma reduzida do produto $\overline{ux}^{-1}vy$ conserva o final y, caso contrário $vy = y_1 \cdots y_m y$ seria o segmento inicial de $\overline{ux}$ e assim $vy \in U$ (porque U é TS), mas isto nos daria $vy = \overline{vy} \Longrightarrow b' = 1$, uma contradição. Analogamente, a forma reduzida de $x\overline{ux}^{-1}v$ conserva x, caso contrário $(x\overline{ux}^{-1})^{-1} = \overline{ux}x^{-1}$ seria segmento inicial

de v e então $\overline{ux}x^{-1} \in U$ pois U é TS. Por conseguinte

$$\begin{aligned} ux &= \overline{\overline{ux}x^{-1}}x \quad \text{(por (1-3))}, \\ &= \overline{ux}x^{-1}x \quad \text{(porque } \overline{ux}x^{-1} \in U\text{)}, \\ &= \overline{ux}, \end{aligned}$$

e isto nos daria $ux \in U$, contradição. Assim, o único modo de x e y serem cancelados é que $v = \overline{ux}$, $y = x^{-1}$ e $\overline{vy} = \overline{\overline{ux}x^{-1}} = u$.

□

Teorema 1.30. *(Schreier) Se H é um subgrupo de um grupo livre F, então H é livre. Mais ainda, se $|F : H| = s$ e $r(F) = r$, então $|r(H)| = (r-1)s+1$.*

Prova. Mantendo a notação prévia, seja

$$w = b_1 b_2 ... b_n,\ b_i = u_i x_i \overline{u_i x_i}^{-1},\ 1 \leq i \leq n$$

uma palavra reduzida em B. Pelo lema anterior, w contém todos os símbolos x_i de b_i com $i = 1, ..., n$. Temos assim que $|w| \geq n$, donde H é livre em B pela Proposição 1.15. Sendo $B = \{ux\overline{ux}^{-1} : u \in U, x \in X, ux \notin U\}$ (U um transversal de Schreier), obtemos

$$|r(H)| = |B| = sr - b,$$

onde $b = |\{(u,x,v) \in U \times X \times U : ux = v\}|$. Considere agora o grafo orientado Γ, cujos vértices são os s elementos de U e cada aresta (u,v) é indexada por $x \in X$ se, e somente se $ux = v$ (veja o Exemplo .7 no Apêndice). Afirmamos que Γ é uma árvore. De fato, cada vértice de Γ conecta-se por algum caminho a 1, pois U é um transversal de Schreier; não há circuitos no grafo pois F não possui relações (porque F é livre em X); por último, não existem vértices repetidos, pois se $ux = v$ e $uy = v$, então $x = y$. Observe que b é o número de arestas de Γ, portanto $b = s - 1$ (Lema .41 do Apêndice), substituindo este valor de b na expressão de $r(H)$, obtemos finalmente $|r(H)| = (r-1)s+1$.

□

Observe que o teorema de Schreier implica imediatamente que todo subgrupo de um grupo cíclico é cíclico. Menos trivial, é seguinte consequência do teorema Schreier: Se H for um subgrupo do grupo livre F tal que $|F : H| = \infty$ e H possui um subgrupo normal não trivial de F, então $r(H) = \infty$ (veja Johson [3], pág 23).

1.2.2 Apresentação de Grupos

Nesta seção, denotaremos $\langle R\rangle^G$ por $\overline{R}$, a menos que haja perigo de confusão.

Definição 1.31. *Seja $F = F(X)$ um grupo livre com base X e R um subconjunto de F. Se um grupo G é isomorfo a $F/\overline{R}$, escrevemos $G = \langle X|R\rangle$ e dizemos que o par $\langle X|R\rangle$ é uma apresentação para G.*

Quando $G = \langle X|R\rangle$, os elementos $x \in X$ e $r \in R$ são chamados, respectivamente, de *geradores* e *relações* da apresentação. Dizemos que o grupo G é *finitamente apresentado* quando X e R são finitos.

Exemplo 1.5. *(i) $\langle X|\emptyset\rangle$ é uma apresentação para o grupo livre $F = F(X)$.*
Basta observar que $\overline{\emptyset} = 1$ e $F \cong F/1$.

(ii) $\mathbb{Z}_n = \langle x|x^n\rangle$.
Considere o epimorfismo $\phi : F(x) \longrightarrow \mathbb{Z}_n$, definido por $x^n \to \overline{n}$. Como $Ker(\phi) = \{x^n : \overline{n} = 0\} = \langle x^n\rangle$ e $Ker(\phi) \trianglelefteq F(x)$ temos $\overline{\{x^n\}} = Ker(\phi)$ com $\mathbb{Z}_n \cong F/Ker(\phi)$.

(iii) $\mathbb{Z}_6 = \langle x, y\,|x^3, y^2, [x,y]\rangle$.
Seja $\mathbb{Z}_6 = \langle a\rangle$ e considere a aplicação $\theta : \{x,y\} \longrightarrow \mathbb{Z}_6$ definida por $x \to a^2$ e $y \to a^3$. Seja F livre em $\{x,y\}$ e $\tilde{\theta}$ a extensão de θ. Então

$$(x^3)^{\tilde{\theta}} = (a^2)^3 = 1; \quad (y^2)^{\tilde{\theta}} = (a^3)^2 = 1; \quad [x,y]^{\tilde{\theta}} = a^2a^{-3}a^2a^3 = 1.$$

Pondo $R = \{x^3, x^2, [x,y]\}$, as equações acima implicam que $R \subseteq Ker(\tilde{\theta})$, logo $H = \overline{R} \subseteq Ker(\tilde{\theta})$. Decorre desta última inclusão que a aplicação $\phi : F/H \longrightarrow F/Ker(\tilde{\theta})$, $Hw \to Ker(\tilde{\theta})w$ está bem definida e portanto ϕ é um epimorfismo, assim $|F/H| \geq |F/Ker(\tilde{\theta})|$. O homomorfismo $\tilde{\theta}$ é sobrejetor pois vale $(yx^{-1})^{\tilde{\theta}} = a^3a^{-2} = a$. Assim $F/Ker(\tilde{\theta}) \cong \mathbb{Z}_6$ e portanto $|F/H| \geq |F/Ker(\tilde{\theta})| = 6$. Por outro lado, como Hx e Hy geram F/H e valem $HxHy = HyHx$, $Hx^3 = H$, $Hy^2 = H$ obtemos que F/H possui no máximo seis elementos

$$H,\ Hx,\ Hx^2,\ Hy,\ Hxy,\ Hx^2y.$$

Assim $|F/H| = 6$ e portanto $F/H \cong \mathbb{Z}_6$.

Algumas vezes, é mais conveniente trabalhar com apresentações na forma $G = \langle X|R = 1\rangle$, onde $R = 1$ é o conjunto $\{r = 1 : r \in R\}$. Os elementos $r = 1$ são chamados de *relações definidoras* da apresentação. Uma forma equivalente de escrever a relação definidora $rs^{-1} = 1$ é $r = s$, por exemplo

$$\begin{aligned} G &= \langle x,y|x^2, y^3, x^{-1}y^{-1}xy\rangle \\ &= \langle x,y|x^2 = 1 = y^3, xy = yx\rangle. \end{aligned}$$

Proposição 1.32. *Todo grupo possui uma apresentação e todo grupo finito possui uma apresentação finita.*

Prova. Seja G um grupo qualquer e $\tilde{\theta} : F(X) \longrightarrow G$ o homomorfismo da Proposição 1.16, temos $G \cong F(X)/Ker(\tilde{\theta})$. Pondo $R = Ker(\tilde{\theta})$, segue que $\overline{R} = R$ e $G = \langle X|R\rangle$. No caso de G ser finito, pondo $|X| = r$ e $|G : Ker(\tilde{\theta})| = s$, segue pelo teorema de Schreier que $Ker(\theta')$ é gerado por um conjunto B de cardinalidade $(r-1)s+1$. Como $\langle B\rangle = Ker(\tilde{\theta}) \trianglelefteq F(X)$, temos $\langle B\rangle = \overline{B}$ e assim $G = \langle X|B\rangle$, que é uma apresentação finita.

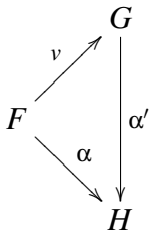
□

Lema 1.33. *Sejam F, G, H grupos e $v : F \longrightarrow G$, $\alpha : F \longrightarrow H$ homomorfismos tais que*

$$(i)\ Im(v) = G \quad (ii)\ Ker(v) \subseteq Ker(\alpha).$$

Então existe um homomorfismo $\alpha' : G \longrightarrow H$ tal que $v\alpha' = \alpha$, mais ainda $Ker(\alpha') = Ker(\alpha)^v$.

Prova. Dado $g \in G$, como v é sobrejetiva, existe $f \in F$ tal que $f^v = g$. Defina $g^{\alpha'} = f^{\alpha}$.



Dados $f_1, f_2 \in F$, temos

$$\begin{aligned} f_1^v = f_2^v &\iff f_1 f_2^{-1} \in Ker(v) \\ &\implies f_1 {f_2}^{-1} \in Ker(\alpha) \quad \text{(por (ii))} \\ &\implies f_1^{\alpha} = f_2^{\alpha}. \end{aligned}$$

Isso mostra que α' está bem definida. Para ver que α' é um homomorfismo, tomemos $g_1, g_2 \in G$ e $f_1, f_2 \in F$ tais que $f_1^v = g_1$ e $f_2^v = g_2$, temos $(f_1 f_2)^v = g_1 g_2$ e

$$(g_1 g_2)^{\alpha'} = (f_1 f_2)^{\alpha} = f_1^{\alpha} f_2^{\alpha} = g_1^{\alpha'} g_2^{\alpha'}.$$

Agora $v\alpha' = \alpha$, segue da própria definição de α' e a verificação de que $Ker(\alpha') \subseteq Ker(\alpha)^v$ e $Ker(\alpha)^v \subseteq Ker(\alpha')$ é rotineira. □

Dada uma apresentação $G = \langle X|R\rangle$, ao invés de operar com elementos na forma $\overline{R}x$, é conveniente identificar G com um tranversal de $\overline{R}$ em $F(X)$ contendo a identidade 1.

Nesse sentido podemos considerar $G = \langle X \rangle$ ao invés de $G = \langle \overline{R}x : x \in X \rangle$ e olhar para a aplicação natural $\theta : x \longrightarrow \overline{R}x$ como a inclusão $X \hookrightarrow \langle X|R \rangle$.

Proposição 1.34. *(Teorema de von Dick). Se $G = \langle X|R \rangle$ e $H = \langle X|S \rangle$, onde $R \subseteq S \subseteq F(X)$, então existe um epimorfismo $\phi : G \longrightarrow H$, que fixa todo $x \in X$ e tal que $Ker(\phi) = \langle S \backslash R \rangle^G$. Reciprocamente, todo quociente de $G = \langle X|R \rangle$ possui uma apresentação $\langle X|S \rangle$ com $S \supseteq R$.*

Prova. Considere as aplicações naturais $v : F \longrightarrow F/\overline{R}$ e $\alpha : F \longrightarrow F/\overline{S}$. Como v é sobrejetiva e $Ker(v) = \overline{R} \subseteq \overline{S} = Ker(\alpha)$, existe, pelo lema anterior, um homomorfismo $\phi = \alpha'$ de G em H tal que:

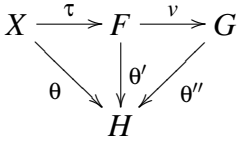
$$\begin{aligned} (i) \qquad & \alpha = v\phi; \\ (ii) \qquad & Ker(\phi) = Ker(\alpha)^v. \end{aligned}$$

Agora ϕ fixa todo $x \in X$ porque v e α o fazem e por (i), ϕ é sobrejetiva porque v e α o são. Por (ii), $Ker(\phi) = \frac{\overline{S}}{\overline{R}} = \frac{\overline{\langle S \backslash R \rangle}}{\overline{R}}$. Como $Ker(\phi) \trianglelefteq G$, com o pequeno abuso de notação mensionado acima podemos escrever $Ker(\phi) = \langle S \backslash R \rangle^G$. Reciprocamente, seja H um grupo quociente de G e seja ϕ a composta de aplicações naturais $F(X) \longrightarrow G \longrightarrow H$, temos $R \subseteq Ker(\phi)$ e sendo $Ker(\phi) = \overline{Ker(\phi)}$ obtemos $H = \langle X|Ker(\phi) \rangle$. □

A proposição seguinte é de grande utilidade na construção de homomorfismos entre apresentações de grupos.

Proposição 1.35. *(Teste da Substituição) Seja $G = \langle X|R \rangle$ uma apresentação e H um grupo. A aplicação $\theta : X \longrightarrow H$ estende-se a um homomorfismo $\theta'' : G \longrightarrow H$ se, e somente se vale a condição de substituição: Para todo $r = x_1 \dots x_l$ em R, temos $x_1^\theta \dots x_l^\theta = 1$.*

Prova. Seja $\tau : X \longrightarrow F$ uma inclusão e $v : F \longrightarrow F/\overline{R}$ $(= G)$, a aplicação natural. Como F é livre em X, θ estende-se a um homomorfismo $\theta' : F \longrightarrow H$. Agora a condição de substituição é equivalente a $R \subseteq Ker(\theta')$. Como $Ker(\theta') \trianglelefteq F$ e $\overline{R} = Ker(v)$, temos $Ker(\theta') \subseteq Ker(v)$. Uma vez que v é sobrejetiva, podemos aplicar o lema anterior para garantir a existência de um homomorfismo $\theta'' : G \longrightarrow H$.



Reciprocamente, a existência de um homomorfismo $\theta'' : G \longrightarrow H$ estendendo θ implica, pela unicidade de θ', que $v\theta'' = \theta'$. Como $Ker(v) \subseteq Ker(v\theta'')$, temos $R \subseteq \overline{R} = Ker(v) \subseteq Ker(v\theta'') = Ker(\theta')$. □

Observação 1.36. *O homomorfismo θ'' da proposição acima é único, pois X gera G. Também é de fácil verificação que θ'' é um epimorfismo se, e somente se $\langle X^{\theta}\rangle = H$.*

Proposição 1.37. *Se $G = \langle X|R\rangle$ e $H = \langle Y|S\rangle$, então o produto direto $G \times H$ possui uma apresentação*

$$\langle X,Y|R,S,[X,Y]\rangle,$$

onde $[X,Y] = \{[x,y] : x \in X, y \in Y\}$.

Prova. Seja $D = \langle X,Y|R,S,[X,Y]\rangle$, pelo teste da substituição, as inclusões $X \hookrightarrow D$ e $Y \hookrightarrow D$, estendem-se a homomorfismos $\theta : G \longrightarrow D$ e $\phi : H \longrightarrow D$, respectivamente. Observe que para todo $x \in X$ e $y \in Y$, $xy = yx$ é uma relação em D, consequentemente

$$xy = yx \Longrightarrow x^{\theta}y^{\phi} = y^{\phi}x^{\theta} \Longrightarrow g^{\theta}h^{\phi} = h^{\phi}g^{\theta},$$

para todo $g \in G$ e $h \in H$, pois X gera G e Y gera H. Decorre daí que a aplicação $\alpha : G \times H \longrightarrow D$ definida por $(g,h) \longrightarrow g^{\theta}h^{\phi}$ é um homomorfismo, mais ainda, α leva os geradores de $G \times H$ nos geradores de D, pois $\alpha : (x,1) \longrightarrow x$ e $\alpha : (1,y) \longrightarrow y$. Considere agora, a aplicação $b : X \cup Y \longrightarrow G \times H$ definida por $x \to (x,1)$ e $y \to (1,y)$. Afirmamos que b satisfaz a condição de substituição. De fato, seja r uma relação em D, se $r \in R$, temos $r^b = (r,1) = (1,1)$ pois $r = 1$ em G, do mesmo modo $r^b = 1$ quando $r \in S$; se $r \in [X,Y]$, temos $r^b = [x,y]^b = (x^{-1},1)(1,y^{-1})(x,1)(1,y) = (1,1)$. Assim, b estende-se a um homomorfismo $\beta : D \longrightarrow G \times H$ que leva os geradores de D nos geradores $G \times H$. Uma vez que $\alpha\beta$ fixa o conjunto gerador de $G \times H$ e $\beta\alpha$ fixa o conjunto gerador de D, temos que β é o inverso de α e portanto α é um isomorfismo. □

Exemplo 1.6. *(i) Sejam $\mathbb{Z}_2 = \langle x|x^2 = 1\rangle$ e $\mathbb{Z}_3 = \langle y|y^3 = 1\rangle$, temos $\mathbb{Z}_2 \times \mathbb{Z}_3 = \langle x,y|x^2 = y^3 = 1, xy = yx\rangle$, que também é uma apresentação para o grupo $\mathbb{Z}_6$ (Exemplo 1.5, (iii)), segue assim que os grupos $\mathbb{Z}_2 \times \mathbb{Z}_3$ e $\mathbb{Z}_6$ são isomorfos.*

(ii) Se $G = \langle X|R\rangle$, então $G/G' = \langle X|R,C\rangle$, onde $C = \{[x,y] : x,y \in X, x \neq y\}$. De fato, pelo teorema de von Dick, é suficiente mostrar que o fecho normal de C em G coincide com G'. Por um lado, as relações C implicam que o grupo $G/\overline{C} = \langle X|R,C\rangle$ é abeliano, logo $G' \subseteq \overline{C}$. Por outro lado, G' é um subgrupo normal de G contendo C, consequentemente $\overline{C} \subseteq G'$.

(iii) Seja $F = \langle X|\emptyset\rangle$ o grupo livre em X, temos pelo item anterior que $F/F' = \langle X|[X,X]\rangle$. Decorre daí que se F tem posto r, então F/F' é isomorfo ao produto direto de r cópias de $\mathbb{Z}$. Para mostrar isso usamos indução sobre r. O caso $r = 1$ é imediato; supondo o resultado válido para r cópias $\mathbb{Z} \times \cdots \times \mathbb{Z} = \langle x_1, \cdots, x_r|C_r\rangle$,

onde $C_r = \{[x_i, x_j] : 1 \leq i < j \leq r\}$. *Temos:*

$$\begin{aligned}(\mathbb{Z} \times \cdots \times \mathbb{Z}) \times \mathbb{Z} &= \langle x_1, \cdots, x_r | C_r \rangle \times \langle x_{r+1} | \emptyset \rangle \\ &= \langle x_1, \cdots, x_{r+1} | C_r, [x_1, x_{r+1}], \cdots [x_r, x_{r+1}] \rangle \text{ (pela Proposição 1.37)} \\ &= \langle x_1, \cdots, x_{r+1} | C_{r+1} \rangle.\end{aligned}$$

Em uma apresentação $\langle X|R\rangle$, quando $w \in \overline{R}$ (isto é, $w = 1$), dizemos que a relação w é consequência das relações de R. Por exemplo, para $\mathbb{Z}_6 = \langle x, y | x^2 = 1 = y^3, xy = yx \rangle$, temos que $w = (xy)^6$ é consequência das relações de $\mathbb{Z}_6$. De fato

$$\begin{aligned}w &= (xy)^6 = x^6 y^6 && \text{(pela relação definidora } xy = yx) \\ &= (x^2)^3 (y^3)^2 \\ &= 1 && \text{(pelas relações definidoras } x^2 = 1 = y^3)\end{aligned}$$

Dada a apresentação $G = \langle X|R\rangle$. Se $w \in \overline{R} \backslash R$, é claro que $\overline{R \cup w} = \overline{R}$ e segue que $\langle X|R, w\rangle$ também é uma apresentação para G. Do mesmo modo, se $R' = \overline{R} \backslash w$, com $w \in R \cap \overline{R \backslash w}$ então $\overline{R'} = \overline{R}$, logo $\langle X|R'\rangle$ também é uma nova apresentação para G. Obtemos assim que as seguintes operações sobre $\langle X|R\rangle$ não alteram o grupo G:

(T1) Adicionar consequências: $X' = X, \quad R' = R \cup r$, onde $r \in \overline{R} \backslash R$;

(T2) Remover redundâncias: $X' = X, \quad R' = R \backslash r$, onde $r \in R \cup \overline{R \backslash r}$.

Veremos agora, outras duas operações sobre $\langle X|R\rangle$ que não alteram o grupo G. Seja $w \in F$ arbitrário e y um símbolo que não pertence a X. Pondo $H = \langle X, y | R, y^{-1} w \rangle$, vemos pelo teste da substituição que a inclusão $X \hookrightarrow H$ estende-se a um homomorfismo $\alpha : G \longrightarrow H$ que fixa o conjunto gerador de G. Seja a aplicação $b : X \cup y \longrightarrow \langle X|R\rangle$, definida por $x \to x$ e $y \to w$. Novamente pelo teste da substituição, obtemos um homomorfismo $\beta : H \longrightarrow G$ que fixa o conjunto gerador de H. Assim, α e β são homomorfismos inversos um do outro e consequentemente $\langle X|R\rangle$ e $\langle X, y | R, y^{-1} w \rangle$ são duas apresentações para G. Essas duas operações são resumidas no seguinte:

(T3) Introduzir abreviações: $X' = X \cup y, \quad R' = R \cup y^{-1} w; \quad y \notin X, w \in F$.

(T4) Remover abreviações: $X' = X \backslash y, \quad R' = R \backslash y^{-1} w; \quad y \in X$, $w \in \langle X \backslash y \rangle$ e $y^{-1} w$ é a única relação em R envolvendo o símbolo y.

As operações $(T1), (T2), (T3)$ e $(T4)$ acima são chamadas de *transformações de Tietze* e têm como objetivo simplificar a apresentação de um grupo. Na prática, trabalhamos com relações definidoras ao invés de relações.

Exemplo 1.7. *Usando as transformações de Tietze, vamos mostrar que* $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$.

Seja $\mathbb{Z}_2 \times \mathbb{Z}_3 = \langle x,y|x^2 = 1, y^3 = 1, xy = yx\rangle$. *Introduzindo a abreviação* $a = xy$ *e notando que* $x^2 = 1, y^3 = 1, xy = yx \Longrightarrow a^6 = 1$, *podemos escrever*

$$\langle x,y,a|x^2 = 1, y^3 = 1, xy = yx, a = xy, a^6 = 1\rangle.$$

Substituindo $y = x^{-1}a$ *em* $y^3 = 1$ *e* $xy = yx$ *segue que* $(x^{-1}a)^3 = 1$ *e* $ax = xa$, *podemos então remover a abreviação* $y = x^{-1}a$:

$$\langle x,a|x^2 = 1, (x^{-1}a)^3 = 1, ax = xa, a^6 = 1\rangle.$$

Como $x = a^3$ *é consequência de* $x^2 = 1, (x^{-1}a)^3 = 1, ax = xa$, *acrescentamos* $x = a^3$ *a apresentação de* $\mathbb{Z}_2 \times \mathbb{Z}_3$. *Agora sendo* $x^2 = 1, (x^{-1}a)^3 = 1, ax = xa$ *consequências de* $a^6 = 1, x = a^3$, *obtemos* $\mathbb{Z}_2 \times \mathbb{Z}_3 = \langle x,a|a^6 = 1, x = a^3\rangle$. *Finalmente, removendo a abreviação* $x = a^3$ *segue que* $\mathbb{Z}_2 \times \mathbb{Z}_3 = \langle a|a^6 = 1\rangle$.

Exemplo 1.8. *O grupo* $G = \langle a,b|abab^2 = 1 = baba^2\rangle$ *é isomorfo a* $\mathbb{Z}_5$. *Observe que* $baba^2 = 1$ *implica* $ba = a^{-2}b^{-1}$, *substituindo em* $abab^2 = 1$, *temos* $a(a^{-2}b^{-1})b^2 = 1 \Longrightarrow a = b$, *logo* $G = \langle a|a^5\rangle$.

Exemplo 1.9. *O grupo* $H = \langle a,b,c,d|ab = c, bc = d, cd = a, da = b\rangle$ *é isomorfo a* $\mathbb{Z}_5$. *Substituindo* $c = ab$ *e* $d = bc = bab$ *nas outras duas relações obtemos* $cd = a \Longrightarrow (ab)(bab) = a \Longrightarrow b^2ab = 1$ *e* $da = b \Longrightarrow (bab)(a) = b \Longrightarrow aba = b$, *assim* $H = \langle a,b|b^2ab = 1 = aba = b\rangle$. *Agora de* $aba = b$ *obtemos* $b = a^{-2}$ *e substituindo em* $b^2ab = 1$, *temos* $(a^{-2})^2a(a^{-2}) \Longrightarrow a^5 = 1$ *e finalmente* $H = \langle a|a^5\rangle$.

1.3 Produtos Livres

Definição 1.38. *Sejam* $H = \langle X|R\rangle$ *e* $K = \langle Y|S\rangle$ *grupos com* X *e* Y *disjuntos. O produto livre* $H * K$ *é definido pela apresentação*

$$H * K = \langle X,Y|R,S\rangle.$$

Os grupos H e K são chamados de grupos fatores do produto livre $H * K$. A seguir, veremos que o produto livre não depende das apresentações escolhidas para H e K.

Proposição 1.39. *O produto livre* $H * K$ *está bem definido.*

Prova. Sejam $H' \cong H$ e $K' \cong K$ com apresentações $H' = \langle X'|R'\rangle$ e $K' = \langle Y'|S'\rangle$, onde $X' \cap Y' = \emptyset$. Considere os isomorfismos $\alpha : H \longrightarrow H'$ e $\beta : K \longrightarrow K'$. Uma vez que α e β levam relações definidoras em relações definidoras, obtemos pelo teste da substituição, o homomorfismo natural $\alpha * \beta : H * K \longrightarrow H' * K', x \to x^{\alpha},\ y \to y^{\beta}$. De modo análogo, obtemos o homomorfismo natural $\alpha^{-1} * \beta^{-1} : H' * K' \longrightarrow H * K, \quad x' \to (x')^{\alpha^{-1}}, y' \to (y')^{\beta^{-1}}$.

Como $\alpha^{-1} * \beta^{-1}$ é o inverso de $\alpha * \beta$, temos $H * K \cong H' * K'$. □

Sejam $\overline{H}$ e $\overline{K}$ subgrupos de $H * K$, gerados por X e Y, respectivamente. Pelo teste da substituição, a inclusão $X \hookrightarrow H * K$ e a aplicação $\pi : X \cup Y \longrightarrow H$, $x \to x, y \to 1$ estende-se ao homomorfismo $\alpha : H \longrightarrow H * K$ e a projeção $\pi_1 : H * K \to H$, respectivamente. Observe que $H^{\alpha} = \overline{H}$, $\overline{H}^{\pi_1} = H$, $\alpha\pi_1 : x \longrightarrow x$ e $\pi_1\alpha : x \longrightarrow x$ para todo $x \in X$, logo $\alpha\pi_1 = 1_H$ e $\pi_1\alpha = 1_{\overline{H}}$ e portanto $H \cong \overline{H}$. Analogamente $K \cong \overline{K}$. Sendo $H * K$ gerado por $\overline{H}$ e $\overline{K}$, se identificarmos H com $\overline{H}$ e K com $\overline{K}$, podemos considerar que o produto livre $H * K$ é gerado pelos seus grupos fatores H e K.

Exemplo 1.10. *Para $A = \langle a | a^m = 1 \rangle$ e $B = \langle b | b^n = 1 \rangle$ temos $A * B = \langle a, b | a^m = 1 = b^n \rangle$. Seja $A \times B = \langle a, b | a^m = 1 = b^n, a^{-1}b^{-1}ab = 1 \rangle$. Pelo teorema de von Dick (Proposição 1.34),*

$$A \times B \cong \frac{A * B}{\langle a^{-1}b^{-1}ab \rangle^{A*B}}.$$

Seguindo a notação dada para a definição de apresentação de grupos, escrevemos

$$A \times B = \langle A, B | [a, b] = 1 \rangle.$$

De maneira geral, temos a seguinte

Definição 1.40. *(Sidki, [11]) Sejam H e K grupos e R um subconjunto do produto livre $A * B$. Então $\langle H, K | R \rangle$ denotará o quociente de $H * K$ pelo fecho normal de R em $H * K$.*

Observação 1.41. *Seja $G = \langle H, K | R \rangle$, onde $H = \langle X | P \rangle$ e $K = \langle Y | S \rangle$. A definição $G = \frac{H*K}{\langle R \rangle^{H*K}}$ implica que G possui a apresentação $\langle X, Y | P, S, R \rangle$. Nesse sentido, diremos que $\langle H, K | R \rangle$ é uma apresentação de G, gerada pelos grupos H, K e tendo R como relações.*

Definição 1.42. *Uma sequência $a_1, \ldots, a_n$ chama-se reduzida em $H * K$ quando cada $a_i \neq 1$, cada a_i pertence a algum grupo fator H ou K, e os elementos a_i, a_{i+1} nunca pertencem ao mesmo grupo fator.*

Exemplo 1.11. *Sejam $A = \langle a | a^5 = 1 \rangle$ e $B = \langle b | b^3 = 1 \rangle$. Os elementos de A são $1, a^2, a^3, a^4$ e os elementos de B são $1, b, b^2$. As sequências a^4, b, a, b^2 e a^2b são reduzidas, enquanto que a^3, a, b, a, b^2 e $a^2, 1, b$ não são.*

Assim como em grupos livres, podemos definir uma forma normal para os elementos de $H * K$.

Proposição 1.43. *(Forma normal) Considere o produto livre $H * K$. Então as seguintes duas afirmações são equivalentes e verdadeiras:*

(I) Cada elemento w de $H * K$ pode ser expresso de maneira única como $w = a_1 \ldots a_n$, onde $a_1, \ldots, a_n$ é uma sequênia reduzida.

(II) Se $w = a_1 a_2 \dots a_n$, $n > 0$, *onde* $a_1, \dots, a_n$ *é uma sequência reduzida, então* $w \neq 1$ *em* $H * K$.

Prova. Equivalência: Suponha (I) verdadeira e seja w nas condições de (I); se fosse $w = 1$ não teríamos unicidade na expressão de 1 como produto dos elementos de uma sequência reduzida. Agora suponha (II) verdadeira e sejam $w = a_1, \dots, a_n$ e $w = b_1, \dots, b_m$ em suas formas reduzidas. Decorre de (II) que $a_1, \dots, a_n, b_m^{-1}, \dots, b_1^{-1}$ não pode ser reduzida, logo a_n e b_m^{-1} estão no mesmo grupo fator. Também $a_1, \dots, (a_n b_m^{-1}), b_{m-1}, \dots, b_1^{-1}$ não pode ser reduzida e necessariamente $a_n = b_m$. Prosseguindo com o mesmo argumento, obtemos $m = n$ e $a_i = b_i$ para todo $i = 1, \dots, n$.

Provemos agora que (I) é verdadeira. Seja W o conjunto de todas as sequências reduzidas de $H * K$ e S_W o grupo das permutações de W. Para cada $h \in H$ defina uma permutação $\sigma_h \in S_W$ da seguinte maneira: Se $h = 1$, então $\sigma_h = 1_W$; se $h \neq 1$ e $a_1, \dots a_n$ é uma sequência reduzida, então

$$\sigma_h(a_1, \dots, a_n) = \begin{cases} h, a_1, \dots, a_n & \text{se} \quad a_1 \in K \\ ha_1, \dots, a_n & \text{se} \quad a_1 \in H \text{ e } ha_1 \neq 1 \\ a_2, \dots, a_n & \text{se} \quad a_1 = h^{-1} \end{cases}$$

Para a sequência vazia 1, definimos ainda $\sigma_h(1) = h$. Notanto que $(\sigma_h)^{-1} = \sigma_{h^{-1}}$, vemos que σ_h é uma permutação de W. Avaliando $\sigma_{hh'}$ para os devidos casos dados em sua definição, checamos que $\sigma_{hh'} = \sigma_h \sigma_{h'}$. Deste modo a aplicação $\alpha : H \longrightarrow S_W$, $h \to \sigma_h$ é um homomorfismo. Analogamente obtemos o homomorfismo $\beta : K \longrightarrow S_W$, $k \to \sigma_k$. Seja $\alpha * \beta : H * K \longrightarrow S_W$ o homomorfismo que obtemos pelo teste da substituição. Agora seja $w \in H * K$ com $w = a_1 \dots a_n$, onde $a_1, \dots, a_n$ é reduzida. Afirmamos que a permutação $w^{\alpha * \beta}$ leva a sequência vazia 1 em $a_1, \dots, a_n$. De fato, $w^{\alpha * \beta} = a_1^{\alpha * \beta} \dots a_n^{\alpha * \beta} = \sigma_{a_1} \dots \sigma_{a_n}$ e $1^{\sigma_{a_1} \dots \sigma_{a_n}} = a_1^{\sigma_{a_2} \dots \sigma_{a_n}} = \dots = a_1, \dots, a_n$. Finalmente, se tivéssemos $w = 1$, então $w^{\alpha * \beta} : 1 \longrightarrow 1$ e isto implicaria que $a_1, \dots, a_n$ é a sequência vazia 1, o que é absurdo, pois tomamos $n > 0$. □

Quando $w = a_1 \dots a_n$ é um elemento de $H * K$ tal que a sequência $a_1, \dots, a_n$ é reduzida, dizemos que w está na *forma reduzida*.

Exemplo 1.12. *Sejam H e K grupos não triviais e tome $h \in H$ e $k \in K$. O elemento $w = hk$ de $H * K$ está na forma reduzida. Também está na forma reduzida qualquer potência w^n com $n > 0$, assim pela Proposição 1.43, (II); temos $w^n \neq 1$ para todo $n > 0$, em particular, o produto livre $H * K$ é infinito.*

CAPÍTULO 2

O Grupo de Comutatividade Fraca

Todos os resultados sem referência neste capítulo encontram-se no artigo principal Oliveira e Sidki[7].

2.1 A finitude do grupo $G(H,K,\sigma)$

Nesta seção vamos definir o grupo de comutatividade fraca por bijeção $G = G(H,K,\sigma)$ e enunciar, sem demonstração, alguns resultados obtidos por Sidki[11] para certas classes de grupos relacionadas com G.

Definição 2.1. *Seja $\sigma : H \longrightarrow K$ uma bijeção entre grupos tal que $1^\sigma = 1$. O grupo*

$$G(H,K,\sigma) = \langle H,K | [h,h^\sigma] = 1 : \forall h \in H \rangle$$

é definido como sendo o quociente do produto livre $H * K$ pelo fecho normal de $\{[h,h^\sigma], \forall h \in H\}$ em $H * K$.

Observe que $G = G(H,K,\sigma)$ é dado como na Definição 1.40, onde as relações definidoras $[h,h^\sigma] = 1$ são expressas dizendo que H e K comutam fracamente através da bijeção σ. Se $H \cong K$, quando for conveniente, denotaremos $G(H,K,\sigma)$ por $G(H,\sigma)$.

Definição 2.2. *Sejam H e K grupos finitos e $\gamma : H \longrightarrow K$ uma função. Então a tripla (H,K,γ) é dita especial se γ satisfaz*

(i) $1^\gamma = 1$ *e* $1^{\gamma^{-1}} = 1$,

(ii) $|(S^{\gamma^{-1}}h)^\gamma| \geq |S|$,

para todo subconjunto S de K tal que $1 \in S$ e para todo $h \in H$.

O critério de finitude a seguir é dado para um grupo mais geral do que $G(H,K,\sigma)$.

Teorema 2.3. *(Sidki [11]) Seja (H,K,γ) uma tripla especial, onde H e K são grupos finitos de ordens m e n, respectivamente, tal que $1 < n \leq m$. Sejam $\delta : H \longrightarrow K$ e $\varepsilon : H \longrightarrow H$ funções. Então o grupo definido por*

$$G(H,K,\gamma,\delta,\varepsilon) = \langle H,K | hh^{\gamma}(h^{\varepsilon})^{-1}(h^{\delta})^{-1} = 1, \forall h \in H \rangle$$

é finito de ordem no máximo $(m-1)e^m$, onde e é o número de Euler.

Quando $|H| = |K| = n$ e $\sigma : H \longrightarrow K$ é uma bijeção fixando a identidade, vemos que σ satisfaz as condições (i) e (ii) da Definição 2.2 e portanto a tripla (H,K,σ) é especial. Neste caso, Sidki [11] mostrou como um corolário do teorema acima que $G(H,K,\sigma,\delta,\varepsilon)$ possui ordem limitada por ne^{n-1}. Tomando $\delta = \sigma$ e ε igual a identidade $id : H \longrightarrow H$, vemos que $G(H,K,\sigma)$ é um caso particular do grupo $G(H,K,\sigma,\delta,\varepsilon)$, possuindo portanto, ordem limitada por ne^{n-1}.

Se (H,K,γ) é especial, então necessariamente $\gamma : H \longrightarrow K$ é uma sobrejeção. De fato, pondo $S = K$ e $h = 1$ na Definição 2.2, temos $|(K^{\gamma^{-1}})^{\gamma}| \geq |K|$, o que significa que $(K^{\gamma^{-1}})^{\gamma} = K$ e portanto γ é sobrejetiva. Ocorre porém que se $\sigma : H \longrightarrow K$ for apenas sobrejetiva, $G(H,K,\sigma) = \langle H,K | [h,h^{\sigma}] = 1, \forall h \in H \rangle$ pode não ser finito.

Exemplo 2.1. *Seja $A = \langle a \rangle$ um grupo cíclico de ordem n^3, $B = \langle b \rangle$ um grupo cíclico de ordem n^2 e defina $\sigma : A \longrightarrow B$ pela escolha de aplicações sobrejetivas:*

$$\begin{aligned} \sigma : 1 &\longrightarrow 1, \\ A \backslash \langle a^n \rangle &\longrightarrow \langle b^n \rangle \backslash \{1\}, \\ \langle a^n \rangle \backslash \{1\} &\longrightarrow B \backslash \langle b^n \rangle. \end{aligned}$$

Afirmamos que $\frac{G(A,B,\sigma)}{\langle a^n, b^n \rangle} \cong \mathbb{Z}_n * \mathbb{Z}_n$ e uma vez que $\mathbb{Z}_n * \mathbb{Z}_n$ é infinito (Exemplo 1.12), temos que $G = G(A,B,\sigma)$ é infinito. Começemos observando que as relações definidoras $[a,b^n] = 1$ e $[a^n,b] = 1$ em G implicam o seguinte:

(i) $[a^r,b^n] = 1 = [a^n,b^s], \quad \forall r,s \in \mathbb{Z},$

(ii) $\langle a^n,b^n \rangle$ *é central em* G.

Assim por (i), todas as relações definidoras de G são consequências de $[a,b^n] = 1$ e $[a^n,b] = 1$, logo

$$\begin{aligned} G &= \langle A,B | [a,b^n] = 1 = [a^n,b] \rangle, \\ \frac{G}{\langle a^n,b^n \rangle^G} &= \langle A,B | [a,b^n] = 1 = [a^n,b], a^n = 1 = b^n \rangle \quad (\textit{pelo teorema de von Dick}), \\ &= \langle A,B | a^n = 1 = b^n \rangle \quad (\textit{por remoção de consequências}), \\ &= \langle a,b | a^{n^3} = 1 = b^{n^2}, a^n = 1 = b^n \rangle \quad (\textit{pela Observação 1.41}). \end{aligned}$$

$$\begin{aligned}\frac{G}{\langle a^n, b^n\rangle^G} &= \langle a,b|a^n=1=b^n\rangle && (\textit{por remoção de consequências}),\\ \frac{G}{\langle a^n, b^n\rangle} &= \mathbb{Z}_n * \mathbb{Z}_n && (\textit{por (ii)}).\end{aligned}$$

Quando $\varphi : H \longrightarrow K$ é um isomorfismo, escrevemos $\chi(H)$ ao invés de $G(H,K,\varphi)$, isso porque $\chi(H)$ não depende do isomorfismo φ. De fato, seja $\phi : H \longrightarrow K$ um isomorfismo, pelo teste da substituição obtemos os homomorfismos naturais

$$\begin{array}{rccc} \alpha: & \chi(H,\varphi) & \longrightarrow & \chi(H,\phi),\\ & h & \longmapsto & h\\ & h^{\varphi} & \longmapsto & h^{\phi}\end{array} \qquad \begin{array}{rccc} \beta: & \chi(H,\phi) & \longrightarrow & \chi(H,\varphi)\\ & h & \longmapsto & h\\ & h^{\phi} & \longmapsto & h^{\varphi}\end{array}$$

que são inversos um do outro, assim $\chi(H,\varphi) \cong \chi(H,\phi)$. Além de finitude χ conserva outras propriedades.

Teorema 2.4. *(Sidki [11]) Seja $\mathscr{P}$ qualquer uma das seguintes propriedade de grupos: p-grupo, nilpotente, solúvel; então*

$$H \textit{ é um } \mathscr{P}\textit{-grupo} \Longrightarrow \chi(H) \textit{ é um } \mathscr{P}\textit{-grupo}.$$

Como $G(H,K,\sigma)$ é uma generalização de $\chi(H)$, é natural indagar se o teorema acima continua válido para $G(H,K,\sigma)$; Oliveira e Sidki [7] proporam então a seguinte

Conjectura 3. *Se H e K são grupos nilpotentes finitos e $\sigma : H \longrightarrow K$ é uma bijeção fixando a identidade, então $G(H,K,\sigma)$ é nilpotente.*

Mas devido a dificuldade do problema, Oliveira e Sidki [7] concentraram-se no caso mais particular em que os grupos H e K da conjectura acima são isomorfos a $\mathbb{Z}_p \times \ldots \times \mathbb{Z}_p$. Portanto o problema básico estudado nesta dissertação é o seguinte:

Conjectura 4. *Se $H,K \cong \mathbb{Z}_p \times \ldots \times \mathbb{Z}_p$, então $G(H,K,\sigma)$ é um p-grupo.*

Um grupo H isomorfo a $\mathbb{Z}_p \times \ldots \times \mathbb{Z}_p$, com k fatores $\mathbb{Z}_p$, onde p é um número primo, é chamado *p-grupo abeliano elementar de posto k*, que denotaremos por $H \cong A_{p,k}$. O estudo do grupo $G(A_{p,k},\sigma)$ é facilitado pelas seguintes propriedades do grupo $A_{p,k}$:

(i) $A_{p,k}$ pode ser visto como um espaço vetorial sobre $\mathbb{Z}_p$;

(ii) Todo elemento de $A_{p,k}$ possui ordem p.

Assim um isomorfismo do grupo $A_{p,k}$ pode ser visto como um isomorfismo do espaço vetorial $A_{p,k}$, que por sua vez, pode ser identificado com uma matriz $k \times k$ invertível, com entradas em $\mathbb{Z}_p$. Indicando o conjunto de tais matrizes por $GL(k,p)$, temos então que $Aut(A_{p,k}) \cong GL(k,p)$.

2.2 O grupo $G(H,K,\sigma)$ com $H,K \cong \mathbb{Z}_n$

Nessa seção vamos considerar $H,K \cong \mathbb{Z}_n$ e mostrar que $G(H,K,\sigma) \cong H \times K$, mas antes, precisaremos de um resultado da teoria elementar dos números.

Lema 2.5. *Sejam $1 < r,s < n$ inteiros com r,s dividindo n e ϕ a função de Euler. Então*

$$\begin{aligned} X &= \{1 \leq i < n,\ mdc(i,s) = 1\} \Longrightarrow |X| = \phi(s)\frac{n}{s}; \\ Y &= \{1 < j \leq n, r|j\} \Longrightarrow |Y| = \frac{n}{r}. \end{aligned}$$

Prova. Observe que $mdc(x,s) = 1 \iff mdc(x+s,s) = 1$ para todo inteiro x. Pondo $n = sq$, vemos que em cada um dos q intervalos

$$[1,s],[s,2s],...,[(q-1)s,sq]$$

existem exatamente $\phi(s)$ números que são primos com s, logo $|X| = \phi(s)\frac{n}{s}$. A segunda igualdade é imediata. □

Teorema 2.6. *Se H e K são grupos cíclicos de ordem n então $G(H,K,\sigma) \cong H \times K$.*

Prova. Sejam $H = \langle a \rangle$ e $K = \langle b \rangle$, se mostrarmos que a comuta com b, então sendo $(a^i)^\sigma = b^j$, com $1 \leq i,j < n$, segue da Proposição 1.6, (iii) que

$$[a,b] = 1 \text{ implica } [a^i,b^j] = 1$$

e assim

$$G = \langle H,K |\ [a,b] = 1 \rangle,$$

que é uma apresentação do grupo $H \times K$ (Exemplo 1.10). Suponha o contrário, que $[a,b] \neq 1$, logo $\sigma : a^i \to b$ para algum $1 < i < n$ e $\sigma : a \to b^j$ para algum $1 < j < n$. Assim existem inteiros minimais $1 < r,s < n$ tais que $[a,b^r] = 1 = [a^s,b]$. Primeiramente, r e s dividem n. De fato, pondo $n = rq + t$ com $0 \leq t < r$, temos

$$\begin{aligned} 1 = [a,b^n] = [a,b^{rq}b^t] &= [a,b^t][a,b^{rq}]^{b^t}, \\ &= [a,b^t] \qquad (\text{porque } [a,b^{rq}] = 1), \end{aligned}$$

o que implica $t = 0$ pela minimalidade de r. Analogamente se mostra que $s|n$. Agora considere os conjuntos

$$\begin{aligned} X &= \{a^i : 1 \leq i < n, mdc(i,s) = 1\}, \\ Y &= \{b^j : 1 < j \leq n, r|j\}. \end{aligned}$$

Afirmamos que $X^\sigma \subseteq Y$. De fato, sejam $(a^i)^\sigma = b^j$ com $a^i \in X$ e inteiros u,v tais que $iu+sv=1$, devemos mostrar que r divide j. Seja então $j = rq+t$ com $0 \leq t < r$, temos

$$\begin{aligned} 1 = [a^i,(a^i)^\sigma] = [a^i,b^j] = [a^i,b^{rq}b^t] &= [a^i,b^t][a^i,b^{rq}]^{b^t}, \\ &= [a^i,b^t] \qquad (\text{porque } [a^i,b^{rq}]=1), \\ &= [a^{iu},b^t], \\ &= [a^{sv}a^{iu},b^t] \qquad (\text{porque } [a^{sv},b^t]=1), \\ &= [a,b^t], \end{aligned}$$

o que implica $t=0$ por causa da minimalidade de r, logo r divide j.

Como $1 = b^n \in Y$, $\sigma : 1 \longrightarrow 1$ mas $1 \notin X$, temos $X^\sigma \neq Y$, logo $|X| < |Y|$, que combinado com o lema anterior nos dá

$$\phi(s)\frac{n}{s} < \frac{n}{r}. \tag{2-1}$$

Definindo os conjuntos

$$\begin{aligned} \hat{Y} &= \{b^i : 1 \leq i < n, mdc(i,r) = 1\}, \\ \hat{X} &= \{a^j : 1 \leq j < n, s|j\}, \end{aligned}$$

segue de modo inteiramente análogo que

$$\phi(r)\frac{n}{r} < \frac{n}{s}. \tag{2-2}$$

Combinando 2-1 e 2-2 obtemos finalmente

$$\phi(s)\phi(r)\frac{n}{r} < \phi(s)\frac{n}{s} < \frac{n}{r},$$

o que implica $\phi(s)\phi(r) < 1$, uma contradição, logo a comuta com b e $G(H,K,\sigma) \cong H \times K$. □

Observação 2.7. *Sejam $H = \langle X|R\rangle$ e $K = \langle Y|S\rangle$. Então $H \times K = \langle X,Y|R,S,[X,Y]\rangle$, ou ainda $H \times K = \langle H,K|[h,k]=1, \forall h \in H, k \in K\rangle$. Acrescentando as relações de $H \times K$ à apresentação do grupo $G = G(H,K,\sigma)$, temos $\frac{G}{[H,K]^G} = \langle H,K|[h,k]=1,[h,h^\sigma]=1,\forall h \in H,k \in K\rangle$. Removendo as consequências $[h,h^\sigma]=1$, obtemos $\frac{G}{[H,K]^G} = H \times K$. Decorre das identidades $[h_1,k]^{h_2} = [h_1h_2,k][h_2,k]^{-1}$ e $[h,k_1]^{k_2} = [h,k_2]^{-1}[h,k_1k_2]$ que $[H,K] \trianglelefteq G$, portanto $\frac{G}{[H,K]} \cong H \times K$. No caso particular de G ser abeliano temos $G(H,K,\sigma) \cong H \times K$.*

2.3 Cálculo do grupo $G(H,\sigma)$ com H p-grupo abeliano elementar de ordem no máximo 16

Nesta seção, vamos fazer uso do sistema GAP (Groups, Algorithms and Programming) para calcular os grupos $G(H,\sigma)$, onde $H = A_{2,2}, A_{2,3}, A_{2,4}, A_{3,2}$. Veremos que para estes grupos, a Conjectura 2 é verdadeira. O cálculo direto dos $(|H|-1)!$ grupos $G(H,\sigma)$ torna-se inviável muito rapidamente por causa do crescimento fatorial. A Proposição 2.9 abaixo nos permite fazer uma melhoria no cálculo do grupos $G(H,\sigma)$ via GAP, pois ela afirma que a maioria desses grupos são isomorfos.

Definição 2.8. *Sejam H,K subgrupos de um grupo G com $x \in G$. O subconjunto*

$$HxK = \{hxk : h \in H, k \in K\}$$

é chamado de classe dupla.

Observe que no caso particular de H ou K serem triviais, uma classe dupla torna-se uma classe lateral. Assim como as classes laterais, as classes duplas formam uma partição de G, isto é:

(i) $G = \bigcup_{x \in G} HxK$;

(ii) Para todos $x, y \in G$, temos $HxK = HyK$ ou $HxK \cap HyK = \emptyset$.

Para ver isso basta verificar que a relação em G definida por "$x \sim y \iff y = hxk$" para algum $h \in H$ e $k \in K$ é uma relação de equivalência e a classe de equivalência contendo x é HxK.

Proposição 2.9. *Sejam H,K grupos e $\sigma : H \longrightarrow K$ uma bijeção fixando a identidade. Se $\alpha \in Aut(H)$ e $\beta \in Aut(K)$, então $G(H,K,\sigma) \cong G(H,K,\alpha\sigma\beta)$.*

Prova. Pelo teste da substituição, a aplicação $\theta : H \cup K \longrightarrow G(H,K,\alpha\sigma\beta)$ definida por $h \to h^{\alpha^{-1}}$, $k \to k^{\beta}$ estende-se ao epimorfismo $\tilde{\theta} : G(H,K,\sigma) \longrightarrow G(H,K,\alpha\sigma\beta)$, pois

$$[h, h^{\sigma}]^{\tilde{\theta}} = [h^{\alpha^{-1}}, h^{\sigma\beta}] = [h^{\alpha^{-1}}, h^{\alpha^{-1}(\alpha\sigma\beta)}].$$

Analogamente, a aplicação $\phi : H \cup K \longrightarrow G(H,K,\sigma)$ definida por $h \to h^{\alpha}$, $k \to k^{\beta^{-1}}$ estende-se ao epimorfismo $\tilde{\phi} : G(H,K,\alpha\sigma\beta) \longrightarrow G(H,K,\sigma)$ porque

$$[h, h^{\alpha\sigma\beta}]^{\tilde{\phi}} = [h^{\alpha}, h^{(\alpha\sigma\beta)\beta^{-1}}] = [h^{\alpha}, h^{\alpha\sigma}].$$

Claramente $\tilde{\phi}$ é o inverso de $\tilde{\theta}$, assim $G(H,K,\sigma) \cong G(H,K,\alpha\sigma\beta)$. □

Um grupo no GAP é ordenado por comprimento e lexicografia, isto é, pela ordem que definimos no início da Seção 1.2.1, onde a ordem nos geradores é dada como no Exemplo 1.4. Seja $H = \{1, h_2, \ldots, h_n\}$, podemos identificar $Aut(H)$ com um subgrupo de $S_{|H|-1}$ simplesmente observando que um automorfismo α de H induz uma permutação σ nos índices dos elementos de H, isto é $i^\sigma = j \iff h_i^\alpha = h_j$. Fazendo as mesmas considerações para $K \cong H$, podemos escrever

$$A = Aut(H) = Aut(K) \leq S_{n-1}.$$

Agora podemos calcular as classes duplas $A\backslash S_{n-1}/A = \{AsA : s \in S_{n-1}\}$ no GAP, utilizando a função

```
DoubleCosetRepsAndSizes(G,U,V)
```

que retorna uma lista com os representantes das classes duplas $U\backslash G/U$ junto com a respectiva ordem de cada classe. Nas tabelas abaixo, c é a classe de nilpotência e d é o comprimento derivado; o algoritmo para o cálculo dos grupos encontra-se no Apêndice.

(i) $H = A_{2,2}$.
Neste caso $GL(2,2) = S_3$ e temos uma única classe dupla em $GL(2,2)S_3GL(2,2)$ e portanto um único representante de classe dupla. Assim $G(H,\sigma) \cong G(H,\varphi)$ para todo $\sigma \in S_3$.

σ	$\lvert G(H,\sigma)\rvert$	c	d
$()$	2^5	2	2

(ii) $H = A_{2,3}$.
Neste caso, os representantes de classes duplas em $GL(3,2)S_7GL(3,2)$ com as respectivas quantidades de elementos de cada classe são:

$$\{(), 168\}, \{(6,7), 1176\}, \{(5,6,7), 2352\}, \{(4,5,6,7), 1344\}$$

σ	$\lvert G(H,\sigma)\rvert$	c	d
$()$	2^{10}	3	2
$(6,7)$	2^{10}	3	2
$(5,6,7)$	2^8	2	2
$(4,5,6,7)$	2^8	2	2

(iii) $H = A_{2,4}$.
Para este caso existem 3374 representantes de classes duplas em $GL(4,2)S_{15}GL(4,2)$. Vamos listar apenas as ordens dos grupos com as suas

respectivas quantidades:

$$\{2^9,1888\},\{2^{10},1278\},\{2^{11},171\},\{2^{12},14\},\{2^{13},13\},\{2^{15},5\},\{2^{19},5\}$$

σ	$\lvert G(H,\sigma)\rvert$	c
$()$	2^{19}	4
$(14,15)$	2^{19}	5
$(10,13)(14,15)$	2^{19}	5
$(8,11)(9,12)(10,13)$	2^{19}	4
$(8,11)(9,12)(10,14,13,15)$	2^{19}	5

(iv) $H = A_{3,2}$.

Para este grupo, temos 26 representantes de classes duplas em $GL(3,2)S_8GL(3,2)$, sendo 3 grupos de ordem 243 e 23 grupos de ordem 81.

σ	$\lvert G(H,\sigma)\rvert$	c	d
$()$	3^5	2	2
$(6,7)$	3^5	2	2
$(4,6,8,7)$	3^5	2	2
$(7,8)$	3^4	1	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$(3,4,7,5,6,8)$	3^4	1	1

Observação 2.10. *Em sua tese de doutorado, Oliveira [6] deu provas diretas para todos esses casos apresentados.*

2.4 Fixando uma base

Nesta seção vamos olhar para $H = A_{p,k}$ como um espaço vetorial sobre $\mathbb{Z}_p$ e denotar por B_k ao conjunto formado por todas a bases de H. Nosso objetivo será mostrar que $B_k \cap B_k^\sigma$ é não vazio, isto é, σ permuta alguma base de H. Obteremos a partir disso, um resultado útil que afirma que no grupo $G(H,\sigma)$ podemos considerar σ permutando alguma base de H.

Lema 2.11. *Sejam $H = A_{p,k}$ e B_k o conjunto formado por todas as bases de H. Então*

(i) $|B_k| = p^{\binom{k}{2}} \prod_{0\le j\le k-1} (p^{k-j}-1)$;

(ii) *Existem $\frac{p^k-1}{p-1}$ subgrupos cíclicos de H.*

Prova.

(i) Uma base para H é um subconjunto ordenado $\{a_1, a_2, ..., a_k\}$, onde $a_{j+1} \notin \langle a_1, a_2, ..., a_j \rangle$, para todo $j = 1, ..., k-1$. Temos $p^k - 1$ modos de escolher a_1, como $|\langle a_1 \rangle| = p$, temos $p^k - p$ maneiras de escolher a_2, sendo $|\langle a_1, a_2 \rangle| = p^2$, haverá $p^k - p^2$ possibilidades para a_3. Continuando assim

$$\begin{aligned} |B_k| &= (p^k-1)(p^k-p)(p^k-p^2)...(p^k-p^{k-1}), \\ &= (p^k-1)(p^{k-1}-1)p(p^{k-2}-1)p^2...(p-1)p^{k-1}, \\ &= p^{\binom{k}{2}} \prod_{0 \leq j \leq k-1} (p^{k-j}-1). \end{aligned}$$

(ii) Como todo elemento em H, diferente de 1, possui ordem p, segue que dois subgrupos cíclicos quaisquer de H são iguais ou disjuntos. Seja n a quantidade de subgrupos cíclicos de H, cada um dos quais com ordem p. Sendo H igual a união desses n subgrupos, obtemos $p^k = n(p-1)+1$, isto é, $n = \frac{p^k-1}{p-1}$.

□

Definição 2.12. *Seja σ uma permutação de H fixando a identidade. Um subconjunto linearmente independente C de H é chamado $\sigma-$independente se C^σ é um subconjunto linearmente independente de H.*

Por conveniência, vamos adotar a notação aditiva para $H = A_{p,k}$.

Proposição 2.13. *A proporção $\frac{|B_k \cap B_k^\sigma|}{|B_k|}$ de σ-bases de $H = A_{p,k}$ é no mínimo $\frac{k!}{(p-1)^{k-1} p^{\binom{k}{2}}}$, portanto σ permuta alguma base de B_k.*

Prova. Seja C um subconjunto σ-independente de H com tamanho j. Sejam $U = \langle C \rangle$ e $W = \langle C^\sigma \rangle$. Suponha $U \neq H$, isto é $j < n$. Observe que $|U| = |W| = p^j$. Fixando $v \in H \backslash U$, obtemos que o conjunto

$$L_v = \{u + iv : u \in U, 1 \leq i \leq p-1\}$$

é independente de C com $|L_v| = p^j(p-1)$. De fato, se algum $u + iv$ pertencesse a $U = \langle C \rangle$ teríamos $iv \in U$, mas como $\langle iv \rangle = \langle v \rangle$, seguiria que $v \in U$, uma contradição. Dois elementos quaisquer de L são distintos pois $u + iv = w + lv$ implica $(i-l)v \in U$. Agora temos que

$$L_v^\sigma \cap W \subseteq W^\# \backslash C^\sigma.$$

De fato, para $x \in L_v^\sigma \cap W$, temos $x = y^\sigma$ com $y \in L_v$, se supormos que $x \in C^\sigma$, obtemos $y = x^{\sigma^{-1}} \in L_v \cap C$, o que é impossível pois L_v é independente de C. Desse modo

$|L_v^\sigma \cap W| \leq |W^\# \backslash C^\sigma| \leq p^j - (j+1)$. Logo

$$\begin{aligned} |L_v^\sigma \backslash L_v^\sigma \cap W| = |L_v^\sigma| - |L_v^\sigma \cap W| &\geq p^j(p-1) - ((p^j - (j-1)) \\ &= p^{j+1} - 2p^j + (j+1) \geq j+1. \end{aligned} \tag{2-3}$$

Fixado o conjunto C, seja P o conjunto formado por todos os subgrupos cíclicos $\langle U+v\rangle$ do grupo $A\backslash U = A_{p,k-j}$, pelo lema anterior $|P| = \frac{p^{k-j}-1}{p-1}$. Seja $L = \{L_v : v \in H\backslash U\}$, a aplicação

$$\theta : P \longrightarrow L, \quad \langle U+v\rangle \rightarrow L_v$$

é uma bijeção, mais ainda, $\langle U+v\rangle \neq \langle U+w\rangle$ implica $L_v \cap L_w = \emptyset$; para ver isso observe que L_v é igual à união de todos $U+v, U+(2v), \cdots, U+(p-1)v$ e L_w é igual à união de todos $U+w, U+(2w), \cdots, U+(p-1)w$, sendo os subgrupos cíclicos de H iguais ou disjuntos, vemos que $\langle Uv\rangle \cap \langle Uw\rangle = \emptyset$ implica $L_v \cap L_w = \emptyset$.

Agora por (2-3), L_v contribui com $j+1$ elementos v' em L_v tal que $\{C^\sigma, v'^\sigma\}$ é linearmente independente. Se denotarmos por $N(j)$ ao conjuntos cujos elementos são os conjuntos σ-independentes de H de tamanho j, teremos que cada conjunto em $N(j)$ produz $\frac{p^{k-j}-1}{p-1}(j+1)$ conjuntos em $N(j+1)$,

$$\begin{array}{ccccc} \langle U+v_1\rangle & \longleftrightarrow & L_{v_1} & - & j+1 \\ \vdots & & \vdots & & \vdots \\ \langle U+v_n\rangle & \longleftrightarrow & L_{v_n} & - & j+1 \end{array}$$

por conseguinte

$$|N(j+1)| \geq |N(j)| \frac{p^{k-j}-1}{p-1}(j+1).$$

Notando que $|N(1)| = p^k - 1$, a expressão acima nos leva a

$$|N(k)| \geq (p^k-1) \prod_{1 \leq j \leq k-1} \frac{p^{k-j}-1}{p-1}(j+1).$$

Sendo, $|N(k)| = |B_k \cap B_k^\sigma|$, pelo Lema 2.11 (i), obtemos

$$\begin{aligned} \frac{|B_k \cap B_k^\sigma|}{|B_k|} &\geq \frac{(p^k-1) \prod_{1 \leq j \leq k-1} \frac{p^{k-j}-1}{p-1}(j+1)}{p^{\binom{k}{2}} \prod_{0 \leq j \leq k-1} (p^{k-j}-1)} \\ &\geq \frac{(p^k-1)k!}{p^{\binom{k}{2}}(p-1)^{k-1}} \geq \frac{k!}{p^{\binom{k}{2}}(p-1)^{k-1}}. \end{aligned}$$

Portanto $|B_k \cap B_k^\sigma| > 0$ e segue que σ permuta alguma base de B_k. □

Corolário 2.14. *Sejam $H,K \cong A_{p,k}$ com $H = \langle a_1,\ldots,a_k\rangle$ e $K = \langle b_1,\ldots,b_k\rangle$. Então para toda bijeção $\sigma : H \longrightarrow K$, fixando a identidade, podemos obter uma bijeção $\tilde{\sigma} : H \longrightarrow K$, fixando a identidade, tal que $a_i^{\tilde{\sigma}} = b_i$, $i = 1,2,\ldots,k$ e $G(H,\sigma) \cong G(H,\tilde{\sigma})$.*

Prova. Pela proposição anterior podemos encontrar uma base $C = \{c_1,\ldots,c_k\}$ de H tal que $C^\sigma = \{c_1^\sigma,\ldots,c_k^\sigma\}$ é uma base de K. As aplicações $a_i \longrightarrow c_i$ e $b_i^\sigma \longrightarrow c_i$ estendem-se a isomorfismos $\alpha : H \longrightarrow H$ e $\beta : K \longrightarrow K$, respectivamente. Tomando $\tilde{\sigma} = \alpha\sigma\beta$, temos $a_i^{\tilde{\sigma}} = b_i$ e pela Proposição 2.9, segue que $G(H,\sigma) \cong G(H,\tilde{\sigma})$. □

2.5 Permutando os subgrupos cíclicos

Sejam $C_1,C_2,\cdots,C_n$ os subgrupos cíclicos de $H = A_{p,k}$, escolhamos um único gerador a_i de cada C_i e formemos o conjunto $C = \{a_1,a_2,\cdots,a_n\}$. O Teorema 2.18, provado adiante, diz que para cada permutação σ de H, fixando a identidade, podemos obter uma permutação $\hat{\sigma}$ de H, também fixando a identidade e com a seguinte propriedade:

$$a^{\hat{\sigma}} = a^\sigma,\ \ (a^i)^{\hat{\sigma}} = (a^{\hat{\sigma}})^i,$$

para todos $a \in C$ e $i = 1,...,p-1$. Agora dado $h \in H$, temos $h = a^j$ para algum $a \in C$ e $j \in \{1,...,p-1\}$, e assim

$$\begin{aligned}[h,h^{\hat{\sigma}}] &= [a^i,(a^i)^{\hat{\sigma}}]\\ &= [a^i,(a^{\hat{\sigma}})^i],\end{aligned}$$

donde segue que $[h,h^{\hat{\sigma}}] = 1$ é consequência de $[a,a^{\hat{\sigma}}] = 1$. Podemos então escrever

$$\begin{aligned}G(H,\hat{\sigma}) &= \langle H \mid [h,h^{\hat{\sigma}}] = 1,\ \ \forall h \in H\rangle\\ &= \langle H \mid [a,a^{\hat{\sigma}}] = 1,\ \ \forall a \in C\rangle.\end{aligned}$$

Como $a^{\hat{\sigma}} = a^\sigma$ para todo $a \in C$, se acrescentarmos a $G(H,\hat{\sigma})$ as relações definidoras

$$[h,h^\sigma] = 1,\ \ h \notin C,$$

obtemos pelo Teorema de von Dick (Proposição 1.34), que $G(H,\sigma)$ é uma imagem homomorfa de $G(H,\hat{\sigma})$. Isso nos permite obter informações de $G(H,\sigma)$ a partir de $G(H,\hat{\sigma})$, cujo cálculo no GAP é mais viável.

A cada bijeção σ de H fixando a identidade, vamos associar um grafo orientado Γ (veja o Apêndice), cujos vértices são os subgrupos cíclicos de A e cujas arestas orientadas

são definidas do seguinte modo:

$$(C,C') \text{ é aresta de } \Gamma \iff a^{\sigma} = a', \textit{ onde } C = \langle a\rangle, C' = \langle a'\rangle.$$

Cada um desses subgrupos cíclicos possuem $p-1$ geradores, logo existem $p-1$ arestas "chegando" e "saindo" de cada vértice. Enumerando os subgrupos cíclicos de H, definimos uma matriz N, chamada matriz de adjacência de Γ, da seguinte maneira:

$$N_{ij} = l, \tag{2-4}$$

onde l é o número de arestas conectando o vértice C_i ao vértice C_j. Observe que a soma dos elementos de cada linha i (ou coluna j) é sempre igual a $p-1$.

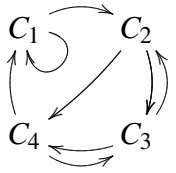
Exemplo 2.2. *Vamos dar dois exemplos que ilustram as definições acima para o grupo* $H = \mathbb{Z}_3 \times \mathbb{Z}_3 = \langle a,b\rangle$.

(i)

h	1	a	a^2	b	b^2	ab	a^2b	ab^2	a^2b^2
h^{σ}	1	b	a^2	ab	ab^2	a^2b	a	a^2b^2	b^2

Os subgrupos cíclicos de H, o grafo Γ e a matriz N são respectivamente:

$C_1 = \langle a\rangle, \quad C_2 = \langle b\rangle,$
$C_3 = \langle a^2b\rangle, \quad C_4 = \langle ab\rangle.$



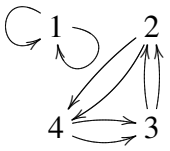
$$N = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

(ii)

h	1	a	a^2	b	b^2	ab	a^2b	ab^2	a^2b^2
h^{σ}	1	a	a^2	a^2b	ab^2	b	ab	a^2b^2	b^2

Para este caso, os subgrupos cíclicos de H, o grafo Γ e a matriz N são respectivamente:

$C_1 = \langle a\rangle, \quad C_2 = \langle b\rangle,$
$C_3 = \langle a^2b\rangle, \quad C_4 = \langle ab\rangle.$



$$N = \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \end{bmatrix}$$

Definição 2.15. *Sejam* $M = (M_{ij})$, $N = (N_{ij})$ *matrizes* $n \times n$ *sobre os números reais. Então*

(i) *M e N são ditas equivalentes quando uma delas puder ser obtida da outra através de sucessivas permutações de linhas ou colunas;*

(ii) *N é dita duplamente estocástica quando a soma dos elementos de uma linha ou coluna qualquer é sempre a mesma constante s;*

(iii) *N é dita totalmente singular quando*

$$N_{1,1^\tau}N_{2,2^\tau}...N_{n,n^\tau} = 0$$

para toda permutação τ *de* $\{1,2,...,n\}$.

A matriz definida em (2-4) é duplamente estocástica, mas as matrizes do Exemplo 2.2 não são totalmente singulares: tomando a permutação $\tau = (243)$, temos para a primeira matriz $N_{1,1}N_{2,4}N_{3,2}N_{4,3} = 1$ e para a segunda $N_{1,1}N_{2,4}N_{3,2}N_{4,3} = 16$.

Lema 2.16. *Toda matriz totalmente singular N é equivalente a uma matriz que contém uma submatriz* $0_{(n-l)\times(l+1)}$ *para algum* $l \geq 0$.

Prova. O caso $n = 2$ não oferece dificuldade, N é equivalente a alguma das matrizes

$$\begin{bmatrix} * & * \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} * & 0 \\ * & 0 \end{bmatrix}$$

e forma a base da indução sobre n. Seja N uma matriz totalmente singular de ordem $n+1$. O caso $N = 0$ é trivial, logo podemos assumir que $N \neq 0$ com $N_{11} \neq 0$. Vemos assim que a submatriz

$$N'_{n\times n} = \begin{bmatrix} N_{22} & \cdots & N_{2n+1} \\ \vdots & & \vdots \\ N_{n+12} & \cdots & N_{n+1n+1} \end{bmatrix}$$

é totalmente singular. Utilizando a hipótese de indução em N', podemos assumir que

$$N = \begin{bmatrix} N_{11} & * & E_{1\times(l+1)} \\ A_{l\times 1} & C_{l\times(n-l-1)} & F_{l\times(l+1)} \\ B_{(n-l)\times 1} & D_{(n-l)\times(n-l-1)} & 0_{(n-l)\times(l+1)} \end{bmatrix}$$

Pondo

$$Y_{(n-l)\times(n-1)} = \begin{bmatrix} B_{(n-l)\times 1} & D_{(n-l)\times(n-l-1)} \end{bmatrix}, \quad Z_{(l+1)\times(l+1)} = \begin{bmatrix} E_{1\times(l+1)} \\ F_{l\times(l+1)} \end{bmatrix}$$

Obtemos

$$N = \begin{bmatrix} * & Z_{(l+1)\times(l+1)} \\ Y_{(n-l)\times(n-l)} & 0_{(n-l)\times(l+1)} \end{bmatrix}$$

O que mostra que $Y = Y_{(n-l)\times(n-l)}$ ou $Z = Z_{(l+1)\times(l+1)}$ são totalmente singulares (caso contrário N não seria totalmente singular). Se Y for totalmente singular, novamente pela

hipótese de indução, podemos escrever

$$Y = \begin{bmatrix} \cdots & Y'_{m\times(m+1)} \\ \cdots & 0_{(n-l-m)\times(m+l)} \end{bmatrix}$$

e obtemos em N, a submatriz $0_{((k+1)-(l+m+1))\times((l+m+1)+1)}$. No caso de Z ser totalmente singular, de maneira análoga obtemos uma submatriz $0_{((k+1)-s)\times(s+1)}$ de N com $s \geq 0$.

□

Lema 2.17. *Seja N uma matriz $n \times n$ sobre os números reais não negativos. Se N for totalmente singular e duplamente estocástica, então $N = 0$.*

Prova. Pelo lema anterior, existe $l \geq 0$ tal que

$$N = \begin{bmatrix} X_{l\times(n-l)} & Z_{l\times(l+1)} \\ Y_{(n-l)\times(n-l)} & 0_{(n-l)\times(l+1)} \end{bmatrix}$$

Se s for a soma dos elementos de sua coluna (ou linha), temos que $(l+1)s$ é a soma de todos os elementos da sub-matriz $Z_{l\times(l+1)}$. Como a soma dos elementos da submatriz

$$\begin{bmatrix} X_{l\times(n-l)} & Z_{l\times(l+1)} \end{bmatrix}$$

é ls, temos $(l+1)s \leq ls$, donde $s = 0$ e portanto $N = 0$.

□

Teorema 2.18. *Seja σ uma permutação de $H = A_{p,k}$, fixando a identidade, e considere a relação $R \subseteq H \times H$ definida por*

$$R = \{(a^i, b^j)(1 \leq i, j \leq p-1) : a^\sigma = b\}.$$

Então existe pelo menos $p-1$ permutações $\hat{\sigma}$ de H fixando a identidade tal que $(a^i)^{\hat{\sigma}} = (a^{\hat{\sigma}})^i$ para todo $1 \leq i \leq p-1$, cujo gráfico $\{(a, a^{\hat{\sigma}}) : h \in H\}$ está contido em R.

Prova. Seja Γ o grafo e N a matriz duplamente estocástica, associados a permutação σ. Como $N \neq 0$, pelo lema anterior, N não é totalmente singular, logo existe uma permutação τ satisfazendo

$$N_{1,1^\tau} N_{2,2^\tau} \ldots N_{n,n^\tau} \neq 0,$$

Assim $N_{i,i^\tau} \neq 0$ para todo $i = 1, \ldots, n$. Afirmamos que τ induz uma permutação $\hat{\sigma}$ contida em R. De fato, $N_{i,i^\tau} \neq 0$ implica que (C_i, C_{i^τ}) é uma aresta ordenada do grafo Γ, logo para

cada i, existem $a,b \in H$ tais que $a^{\sigma} = b$ e $C_i = \langle a \rangle$, $C_{i^{\tau}} = \langle b \rangle$. Definindo

$$a^{\hat{\sigma}} = a^{\sigma}, \;\; (a^j)^{\hat{\sigma}} = (a^{\hat{\sigma}})^j, \;\; j = 1, ..., p-1,$$

obtemos uma permutação $\hat{\sigma}$ de H, contida em R. Removendo as arestas correspondentes a $\hat{\sigma}$ do grafo Γ, obtemos um grafo que é $p-2$ regular. Repetindo o mesmo raciocínio $p-1$ vezes, obtemos as $p-1$ permutações $\hat{\sigma}$ anunciadas.

□

Seja $H = K = A_{p,k} = \langle a_1, \ldots, a_n \rangle$ e fixemos $C = \{a_1, \ldots, a_n\}$. Pelo teorema anterior, para toda permutação σ de H, fixando a identidade, existe uma permutação $\hat{\sigma}$ de H, também fixando a identidade, tal que

$$a^{\hat{\sigma}} = a^{\sigma}, \quad (a^i)^{\hat{\sigma}} = (a^{\hat{\sigma}})^i, \quad \forall a \in C, \quad i = 1, 2, \ldots, p.$$

Como vimos no início desta seção, $G(H,\sigma)$ é um quociente do grupo $G(H,\hat{\sigma})$, onde

$$G(H,\hat{\sigma}) = \langle H, H | [a, a^{\hat{\sigma}}] = 1, \forall a \in C \rangle.$$

Observe que pelo Lema 2.11, (ii), $|C| = \frac{p^k-1}{p-1}$ e assim podemos imaginar $\hat{\sigma}$ permutando os $\frac{p^k-1}{p-1}$ subgrupos cíclicos de H. Como veremos logo adiante (Corolário 2.21), essa propriedade de $\hat{\sigma}$ torna o cálculo computacional do grupo $G(H,\hat{\sigma})$ mais viável do que o cálculo de $G(H,\sigma)$.

Procuramos agora, dar uma descrição das classes duplas em $G(H, \alpha\hat{\sigma}\beta)$.

Definição 2.19. *O quociente de $GL(k,p)$ pelo seu centro $Z(GL(k,p))$ é chamado Grupo Linear Projetivo e é denotado por $PGL(k,p)$.*

Lema 2.20. *O centro de $GL(k,p)$ é o grupo formado pelas matrizes escalares aI_k, onde $a \in \mathbb{Z}_p \backslash \{0\}$ e I_k é a matriz identidade de ordem k.*

Prova. Claramente toda matriz escalar aI_k comuta com toda matriz de $GL(k,p)$. Reciprocamente, seja $A = (a_{ij})$ pertencendo ao centro de $GL(k,p)$. Escrevendo E_{ij} para a matriz elementar $k \times k$ cuja entrada (i,j) é 1 e todas as demais entradas são 0, temos que $I_k + E_{ij}$ com $i < j$, é uma matriz triangular superior cujos elementos da diagonal principal são todos iguais a 1, logo $det(I_k + E_{ij}) = 1$ e portanto

$$(I_k + E_{ij})A = A(I_k + E_{ij}) \;\text{ implica }\; E_{ij}A = AE_{ij}.$$

Agora $(AE_{ij})_{sj} = a_{si}$, enquanto que $(E_{ij}A)_{sj} = \delta_{si}a_{jj}$, assim $a_{si} = 0$ se $s \neq i$ e $a_{ii} = a_{jj}$, o que mostra que A é uma matriz escalar. □

Pelo lema acima, os isomorfismos lineares z associados às matrizes de $Z = Z(GL(k,p))$ são do tipo $h^z = (cI_k)h = ch$, para algum $c \in \mathbb{Z}_p{}^{\#} = \{1,2,\ldots,p-1\}$. Identificando $GL(k,p)$ com $Aut(H)$ e utilizando a notação multiplicativa, vemos que dado $a \in C$, existe $c \in \{1,2,\ldots,p-1\}$ tal que

$$a^z = a^c.$$

Isso significa que os subgrupos cíclicos de H são invariantes por todos os automorfismos de Z. Identificando $PGL(k,p)$ com um transversal de Z em $GL(k,p)$, contendo a identidade, vemos que todo $\bar{\alpha} \in GL(k,p)$ se escreve como $z\alpha$, onde $z \in Z$ e $\alpha \in PGL(k,p)$. Como z não permuta os elementos de C, segue que α deve permutar os elementos de C. Assim $PGL(k,p)$ pode ser visto como um subgrupo de $S_{|C|}$ ou ainda, como um subgrupo de $S_{|H|-1}$.

Corolário 2.21. *Se $\alpha,\beta \in PGL(k,p)$, então $G(H,\hat{\sigma}) \cong G(H,\alpha\hat{\sigma}\beta)$.*

Prova. Dados $\bar{\alpha},\bar{\beta} \in GL(n,k)$, temos pela Proposição 2.9 que $G(H,\hat{\sigma}) \cong G(H,\bar{\alpha}\hat{\sigma}\bar{\beta})$. Sejam

$$\bar{\alpha} = z_1\alpha, \quad \bar{\beta} = z_2\beta,$$

onde $z_1,z_2 \in Z(G(k,p))$ e $\alpha,\beta \in PGL(k,p)$. Como $h^{z_1} = h^c$ e $h^{z_2} = h^d$ com $c,d \in \{1,2,\ldots,p-1\}$, dado $h = a^i$ em H, obtemos

$$\left[h,h^{\bar{\alpha}\hat{\sigma}\bar{\beta}}\right] = \left[a^i,(a^i)^{z_1\alpha\hat{\sigma}z_2\beta}\right] = \left[a^i,\left(a^{\alpha\hat{\sigma}\beta}\right)^{icd}\right].$$

Assim, toda relação definidora $[h,h^{\bar{\alpha}\hat{\sigma}\bar{\beta}}] = 1$ é consequência de alguma relação definidora $[a,a^{\alpha\sigma\beta}] = 1$, com $a \in C$. Portanto

$$G(H,\hat{\sigma}) \cong G(H,\bar{\alpha}\hat{\sigma}\bar{\beta}) = \langle H | [a,a^{\alpha\hat{\sigma}\beta}] = 1,\ \forall a \in C\rangle = G(H,\alpha\hat{\sigma}\beta).$$

□

Exemplo 2.3. *Vamos retornar ao grupo $H = A_{3,2} = \langle a_1,a_2\rangle$ da Seção 2.3. O conjunto dos geradores dos subgrupos cíclicos de H é*

$$C = \{a_1,a_2,a_1a_2,a_1^2a_2\}.$$

Como $PGL(2,3) = S_4$, temos que $\varphi = id$ é o único representante de classe dupla em $PGL(2,3)S_4PGL(2,3)$. Assim $\chi(G,\varphi) \cong G(H,\hat{\sigma})$ e portanto $G(H,\sigma)$ é uma imagem homomorfa de $\chi(H,\varphi)$ para todo $\sigma \in S_{|H|-1}$.

Exemplo 2.4. *Para o grupo $A_{3,3}$ temos 13 geradores de subgrupos cíclicos e 252 classes duplas em $PGL(3,3)S_{13}PGL(3,3)$. As ordens dos grupos com as respectivas quantidades são:*

$$\{3^6,235\},\{3^7,11\},\{3^8,5\},\{3^9,1\}.$$

Obtemos ainda as seguintes informações:

(i) Todos os grupos de ordem 3^6 possuem classes de nilpotência iguais a 1, isto é, são abelianos e portanto isomorfos a $A_{3,3} \times A_{3,3}$ (veja a Observação 2.7). Os demais grupos são todos nilpotentes de classe 2.

(ii) Para o único grupo de ordem 3^9, o representante de classe dupla é $\sigma = id$, logo este grupo de ordem máxima é isomorfo a $\chi(A_{3,3})$.

2.6 O grupo $G(H,K,\sigma)$ com $H,K \cong \mathbb{Z}_p \times \mathbb{Z}_p$, onde p é um primo

Seja $H = \langle a_1, a_2 \rangle$ um grupo abeliano 2-gerado de *expoente n*, isto é, n é o menor inteiro positivo tal que $h^n = 1$ para todo $h \in H$. Vemos assim que H é formado pelos n^2 elementos $a_1^i a_2^j$ com $0 \leq i, j < n$. Observando que $a_k^i = a_k^j \iff i \equiv j (mod\ n)$, $k = 1,2$, podemos mostrar, de modo análogo ao caso de grupos cíclicos, que vale

$$H = \langle a_1^r, a_2^s \rangle \text{ se, e somente se } mdc(r,n) = 1 = mdc(s,n).$$

Assim, quando $H = A_{p,2}$ e $a_1, a_2 \in H$ são fixados, temos $H = \langle a_1^r, a_2^s \rangle \iff mdc(r,p) = mdc(s,p) = 1$, logo existem exatamente $(p-1)^2$ elementos $a_1^r a_2^s$ onde $\{a_1^r, a_2^s\}$ gera H. Denotando o conjunto de tais elementos por B, obtemos

$$H \backslash B = p^2 - (p-1)^2 = 2p - 1$$

Agora a diferença entre o número de elementos de B e $H \backslash B$ é dada por

$$(p-1)^2 - (2p-1) = p^2 - 4p + 2$$

que é um número sempre positivo para $p \geq 5$. Como consequência obtemos o seguinte

Lema 2.22. *Para toda permutação σ de $H = A_{p,2} = \langle a_1, a_2 \rangle$, com $p \geq 5$ existem conjuntos geradores $\{a_1^r, a_2^s\}$ e $\{a_1^u, a_2^v\}$ de H de tal modo que $\sigma : a_1^r a_2^s \longrightarrow a_1^u a_2^v$.*

Na Seção 2.3 vimos que $H = A_{2,2}, A_{3,2}$ eram 2-grupo e 3-grupo, respectivamente, com classe de nilpotência no máximo 2. Portanto no teorema abaixo, podemos ir direto ao caso $p \geq 5$.

Teorema 2.23. *Seja $H,K \cong A_{p,2}$ com $H = \langle a_1, a_2\rangle$ e $K = \langle b_1, b_2\rangle$. Então $G = G(H,\sigma)$ é um p-grupo com classe de nilpotência no máximo 2.*

Prova. Pelo Corolário 2.14 podemos supor que $\sigma : a_1 \longrightarrow b_1$, $\sigma : a_2 \longrightarrow b_2$ e uma vez que σ é uma bijeção, decorre do lema anterior que existem conjuntos geradores $\{a_1^r, a_2^s\}$ de H e $\{b_1^u, b_2^v\}$ de K, de maneira que $\sigma : a_1^r a_2^s \longrightarrow b_1^u b_2^v$. Por conseguinte

$$\begin{aligned} 1 = [a_1^r a_2^s, b_1^u b_2^v] &= [a_1^r a_2^s, b_2^u][a_1^r a_2^s, b_1^u]^{b_2^v} \\ &= [a_1^r, b_2^v]^{a_2^s}[a_2^s, b_2^v][a_1^r, b_1^u]^{a_2^s, b_2^v}[a_2^s, b_1^u]^{b_2^v} \\ &= [a_1^r, b_2^v]^{a_2^s}[a_2^s, b_1^u]^{b_2^v} \\ &= [a_1^r, b_2^v][a_2^s, b_1^u] \qquad (2\text{-}5) \\ [b_1^u, a_2^s] &= [a_1^r, b_2^v]. \end{aligned}$$

Como $[b_1^u, a_2^s]^{a_1} = [b_1^u, a_2^s] = [b_1^u, a_2^s]^{b_2}$ e $[a_1^r, b_2^v]^{a_2} = [a_1^r, b_2^v] = [a_1^r, b_2^v]^{b_1}$ concluímos que $\left[b_1^u, a_2^s\right] = [a_1^r, b_2^v]$ é central em G. Escrevendo $a_1^r = \alpha_1$, $a_2^s = \alpha_2$, $b_1^u = \beta_1$ e $b_2^v = \beta_2$, obtemos

$$[\beta_1, \alpha_2] = [\alpha_1, \beta_2]. \qquad (2\text{-}6)$$

Como $H = \langle \alpha_1, \alpha_2\rangle$ e $K = \langle \beta_1, \beta_2\rangle$ são abelianos e G é gerado por H e K, temos $[G,G] = [\langle H,K\rangle, \langle H,K\rangle] = [H,K]^G$. Segue portanto que $G' = \langle [\alpha_1^i \alpha_2^j, \beta_1^k \beta_2^l] : 1 \le i,j,k,l \le p-1\rangle^G$. Agora

$$\begin{aligned} [\alpha_1^i \alpha_2^j, \beta_1^k \beta_2^l] &= [\alpha_1^i, \beta_2^l][\alpha_2^j, \beta_1^k] \qquad (\text{porque } [\alpha_1,\beta_1] = 1 = [\alpha_2,\beta_2]), \\ &= [\alpha_1^i, \beta_2^l][\beta_1^k, \alpha_2^j]^{-1}, \\ &= [\alpha_1, \beta_2]^{il}[\beta_1, \alpha_2]^{-jk} \quad (\text{porque } [\alpha_1,\beta_2] \text{ e } [\beta_1,\alpha_2] \text{ são centrais em } G), \\ &= [\alpha_1, \beta_2]^{il}[\alpha_1, \beta_2]^{-jk} \quad (\text{por (2-6)}). \end{aligned}$$

Assim, G' é cíclico gerado por $[\alpha_1, \beta_2]$. Como G' é central em G, temos $\gamma_3(G) = [G', G] = 1$, donde G é nilpotente de classe no máximo 2. Vale então a seguinte identidade em G: $(xy)^m = x^m y^m [y,x]^{\binom{m}{2}}$, para todo $m \ge 1$ inteiro, (Veja Robinson [8], pág. 141). Como G/G' é abeliano, segue dessa identidade e do fato de H ser p-grupo abeliano elementar, que G/G' é um p-grupo abeliano elementar. Agora observe que sendo $[\alpha_1, \beta_2]$ central em G, obtemos $[\alpha_1, \beta_2]^p = [\alpha_1^p, \beta_2] = 1$, donde vemos que $|G'| = 1$ ou $|G'| = p$. Qualquer dos dois casos implica que G é p-grupo.

□

2.7 O grupo $G(\tilde{H},\tilde{K},\tilde{\sigma})$, $\tilde{H}$ e $\tilde{K}$ extensões de H e K

Sejam $\tilde{H}$ e $\tilde{K}$ grupos possuindo subgrupos normais M e N, respectivamente. Seja H um transversal de M em $\tilde{H}$ com $1 \in H$ e K um transversal de N em $\tilde{K}$ com $1 \in K$. Deste modo podemos fazer a seguinte identificação

$$H = \frac{\tilde{H}}{M}, \qquad K = \frac{\tilde{K}}{N}.$$

Considerando $|\tilde{H}| = |\tilde{K}|$ e $|M| = |N|$, tomemos bijeções $\sigma : H \longrightarrow K$ e $\alpha : M \longrightarrow N$, ambas fixando a identidade. Seja ainda γ uma bijeção entre M e N (não necessariamente fixando a identidade). Observe que $\tilde{H} = \{mh : m \in M, h \in H\}$ e $\tilde{K} = \{nk : n \in N, k \in K\}$. Obtemos assim uma bijeção $\tilde{\sigma} : \tilde{H} \longrightarrow \tilde{K}$ definida por

$$\begin{aligned} \tilde{\sigma} &: m \to m^{\alpha} \\ \tilde{\sigma} &: mh \to m^{\gamma}h^{\sigma} \quad \text{se } h \neq 1, \end{aligned} \tag{2-7}$$

que fixa a identidade. Se $h \in \tilde{H}$, definimos $\bar{h}$ como sendo $\bar{h} = Mh \cap H$. Decorre daí que se $m \in M$ e $h \in H$, então

$$\overline{m} = 1, \quad \bar{h} = h \Longleftrightarrow h \in H, \quad \overline{mh} = h. \tag{2-8}$$

Analogamente definimos $\bar{k}$, com $k \in \tilde{K}$ e obtemos as três propriedades em (2-8). Fixada a notação acima, pomos $\tilde{G} = G(\tilde{H},\tilde{K},\tilde{\sigma})$ e $G = G(H,K,\sigma)$ e obtemos o seguinte

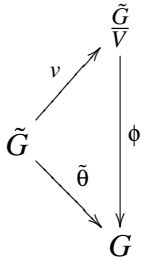
Lema 2.24. *O grupo G é isomorfo ao quociente de $\tilde{G}$ pelo fecho normal de $\langle M,N\rangle$ em $\tilde{G}$.*

Prova. Segue do teste da substituição que a aplicação $\theta : \tilde{H} \cup \tilde{K} \longrightarrow G$ definida por $x \to \bar{x}$, $y \to \bar{y}$, com $x \in \tilde{H}, y \in \tilde{K}$ estende-se a um epimorfismo $\tilde{\theta} : \tilde{G} \longrightarrow G$. De fato, utilizando as propriedades dadas em (2-8), temos

$$\begin{aligned} \left[m, m^{\tilde{\sigma}}\right]^{\tilde{\theta}} &= [m, m^{\alpha}]^{\tilde{\theta}} = [\overline{m}, \overline{m^{\alpha}}] = 1 \\ \left[mh, (mh)^{\tilde{\sigma}}\right]^{\tilde{\theta}} &= [mh, m^{\gamma}h^{\sigma}]^{\tilde{\theta}} = [\overline{mh}, \overline{m^{\gamma}h^{\sigma}}] \\ &= [h, h^{\sigma}]. \end{aligned}$$

Como $M,N \subseteq Ker(\tilde{\theta})$, temos $\langle M,N\rangle^{\tilde{G}} \subseteq Ker(\tilde{\theta})$. Pondo $V = \langle M,N\rangle^{\tilde{G}}$, segue do Lema

1.33 que



$\phi : \frac{\tilde{G}}{V} \longrightarrow G$ definida por $(Vg)^{\phi} = g^{\tilde{\theta}}$, $g \in \tilde{G}$, é um homomorfismo. Por outro lado, a aplicação $\pi : H \cup K \longrightarrow \frac{\tilde{G}}{V}$, $h \to Vh$, $k \to Vk$ estende-se ao homomorfismo $\tilde{\pi} : G \longrightarrow \frac{\tilde{G}}{V}$. De fato

$$\begin{aligned}[h,h^{\sigma}]^{\tilde{\pi}} = [Vh,Vh^{\sigma}] &= [VmVh,Vm^{\gamma}Vh^{\sigma}] \qquad (\text{porque } M,N \leq V),\\ &= V[mh,h^{\gamma}m^{\sigma}] = V \qquad (\text{porque } [mh,m^{\gamma}h^{\sigma}] = 1).\end{aligned}$$

Agora $h^{\tilde{\pi}\phi} = (Vh)^{\phi} = h^{\tilde{\theta}} = h$ e $(Vh)^{\phi\tilde{\pi}} = h^{\tilde{\theta}\tilde{\pi}} = h^{\tilde{\pi}} = Vh$, para todo $h \in H$. Analogamente $k^{\tilde{\pi}\phi} = k$ e $(Vk)^{\phi\tilde{\pi}} = Vk$, para todo $k \in K$. Isso mostra que o homomorfismo π é o inverso do homomorfismo ϕ, consequentemente G é isomorfo a $\frac{\tilde{G}}{V}$. □

Teorema 2.25. *Mantendo a notação prévia, suponha M,N centrais em $\tilde{H},\tilde{K}$, respectivamente e que $G(M,N,\alpha)$ seja abeliano. Então $V = \langle M,N\rangle^{\tilde{G}}$ é abeliano.*

Prova. Defina $\delta : M \longrightarrow N$, $\varepsilon : M \longrightarrow M$ por

$$m^{\delta} = m^{\alpha}((mm^{\alpha\gamma^{-1}})^{\gamma})^{-1}, \quad m^{\varepsilon} = m((m^{\alpha}m^{\gamma})^{\gamma^{-1}})^{-1}. \tag{2-9}$$

Sejam $m \in M$ e $h \in H$ com $m \neq 1 \neq h$. Temos

$$\begin{aligned}
[m,h^{\sigma}] &= [m,m^{\alpha}h^{\sigma}] && (\text{porque } [m,m^{\alpha}] = 1),\\
&= [(m^{\alpha\gamma^{-1}}h)m,m^{\alpha}h^{\sigma}] && (\text{porque } (m^{\alpha\gamma^{-1}}h)^{\tilde{\sigma}} = m^{\alpha}h^{\sigma}),\\
&= [(mm^{\alpha\gamma^{-1}})h,m^{\alpha}h^{\sigma}] && (\text{porque } M \text{ é central em } \tilde{H}),\\
&= [(mm^{\alpha\gamma^{-1}})h,((mm^{\alpha\gamma^{-1}})^{\gamma}h^{\sigma})^{-1}m^{\alpha}h^{\sigma}] && (\text{porque } ((mm^{\alpha\gamma^{-1}})h)^{\tilde{\sigma}} = (mm^{\alpha\gamma^{-1}})^{\gamma}h^{\sigma}),\\
&= [(mm^{\alpha\gamma^{-1}})h,m^{\alpha}((mm^{\alpha\gamma^{-1}})^{\gamma})^{-1}(h^{\sigma})^{-1}h^{\sigma}] && (\text{porque } N \text{ é central em } \tilde{K}),\\
&= [(mm^{\alpha\gamma^{-1}})h,m^{\delta}] && (\text{por 2-9}),\\
[m,h^{\sigma}] &= [m^{\alpha\gamma^{-1}}h,m^{\delta}] = [h,m^{\delta}]. && (2\text{-}10)
\end{aligned}$$

As duas últimas igualdades seguem das identidades $[m,m^{\delta}] = 1 = [m^{\alpha\gamma^{-1}},m^{\delta}]$, que por

sua vez, seguem do fato de $G(M,N,\alpha)$ ser abeliano. De maneira semelhante

$$\begin{aligned}
[h,m^{\alpha}] &= [mh,m^{\alpha}] && (\text{porque } [m,m^{\alpha}]=1),\\
&= [mh,(m^{\gamma}h^{\sigma})m^{\alpha}] && (\text{porque } (mh)^{\tilde{\sigma}}=m^{\gamma}h^{\sigma}),\\
&= [mh,m^{\alpha}m^{\gamma}h^{\sigma}] && (\text{porque } N \text{ é central em } \tilde{K}),\\
&= [((m^{\alpha}m^{\gamma})^{\gamma^{-1}}h)^{-1}mh,m^{\alpha}m^{\gamma}h^{\sigma}] && (\text{porque } ((m^{\alpha}m^{\gamma})^{\gamma^{-1}}h)^{\tilde{\sigma}}=m^{\alpha}m^{\gamma}h^{\sigma}),\\
&= [m((m^{\alpha}m^{\gamma})^{\gamma^{-1}})^{-1}h^{-1}h,m^{\alpha}m^{\gamma}h^{\sigma}] && (\text{porque } M \text{ é central em } \tilde{H}),\\
&= [m^{\varepsilon},m^{\alpha}m^{\gamma}h^{\sigma}] && (\text{por 2-9}),\\
&= [m^{\varepsilon},h^{\sigma}].
\end{aligned}$$

onde a última igualdade segue do fato de m^{ε} comutar com $m^{\alpha}m^{\gamma}$, isto porque $G(M,N,\alpha)$ é abeliano.

Observe também que m comuta com $[m^{\alpha\gamma^{-1}}h,m^{\delta}]=[m,h^{\sigma}]$ pois m comuta com m^{δ} e com $m^{\alpha\gamma^{-1}}h\in\tilde{H}$ (porque M é central em $\tilde{H}$). Assim

$$1=[[m,h^{\sigma}],m]=[m^{-1}m^{h^{\sigma}},m]=[m^{h^{\sigma}},m],$$

e portanto, m comuta com h^{σ}, para todo $h\in H$. Seja $m^{\tilde{K}}=\{m^{x}:x\in\tilde{K}\}$. Como M comuta com N, temos $m^{\tilde{K}}=m^{K}$. Agora dados $k_1,k_2\in K$, vem

$$\begin{aligned}
1=[m^{k_1},m^{k_2}] &= [m,m^{k_2k_1^{-1}}]^{k_1}\\
&= 1 \qquad (\text{porque } h^{\sigma}=k_2k_1^{-1} \text{ para algum } h\in H \text{ e } [m,m^{h^{\sigma}}]=1).
\end{aligned}$$

Assim $\langle M^{\tilde{K}}\rangle$ é um subgrupo abeliano de $\tilde{G}$. Agora

$$[m,h^{\sigma}]=[h,m^{\delta}] \implies [M,K]\leq[H,M^{\delta}]\leq[H,N]; \tag{2-11}$$

$$[h,m^{\alpha}]=[m^{\varepsilon},h^{\sigma}] \implies [H,N]\leq[M^{\varepsilon},K]\leq[M,K]. \tag{2-12}$$

De (2-11) e (2-12) obtemos $[H,N]=[M,K]$. Como $\tilde{G}=\langle\tilde{H},\tilde{K}\rangle$ e $M\leq Z(\tilde{H}),N\leq Z(\tilde{K})$, temos

$$V=\langle M,N\rangle^{\tilde{G}}=\langle M^{\langle\tilde{H}\tilde{K}\rangle},N^{\langle\tilde{H}\tilde{K}\rangle}\rangle=\langle M^{K},N^{H}\rangle.$$

Sendo $m^{k}=m[m,k]$ e $n^{h}=n[n,h]$, podemos escrever

$$\begin{aligned}
V &= \langle M,N,[M,K],[N,H]\rangle\\
&= \langle M,N,[M,K]\rangle \quad \text{porque } [H,N]=[M,K].
\end{aligned}$$

Agora observe que M e N são abelianos, M centraliza $[M,K](=[H,N])$ e N centraliza $[M,K]$. Assim, para provar que V é abeliano, é suficiente mostrar que $[M,K]$ é abeliano,

mas isto é verdadeiro pois $[M,K] \leq \langle M^K \rangle$ (que segue de $[m,k] = m^{-1}m^k$) e já mostramos que $\langle M^K \rangle$ é abeliano.

□

Corolário 2.26. *Suponha nas hipóteses do teorema acima que $M = \langle m \rangle$ e $N = \langle n \rangle$ são cíclicos, cada um deles com ordem igual a um primo p. Então $V = \langle M,N \rangle^{\tilde{G}}$ é um p-grupo abeliano elementar de posto no máximo $|H|+1$.*

Prova. Neste caso temos

$$V = \langle M,N \rangle^{\tilde{G}} = \langle M^K, N^H \rangle = \langle m^K, n^H \rangle,$$

de onde vemos que V é um p-grupo abeliano elementar. Considere $m^k = m[m,k]$, com $m \in M$ e $k \in K$. Da igualdade $[M,K] = [H,N]$, obtemos $[m,k] \in [N,H]$, donde $[m,k]$ é o produto de comutadores do tipo $[n,h] = n^{-1}n^h$, segue assim que $[m^K, n^H] \subseteq [m,n^H]$. A inclusão contrária é imediata, portanto $V = \langle m, n^H \rangle$ que possui no máximo $|H|+1$ geradores. □

Para o exemplo a seguir vamos fazer uso do seguinte exercício: Se H é um grupo não abeliano com ordem p^3, p um número primo, então $Z(H) \cong \mathbb{Z}_p$ e $H/Z(H) \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Exemplo 2.5. *Já sabemos que $G(\mathbb{Z}_p, \alpha) \cong \mathbb{Z}_p \times \mathbb{Z}_p$, para toda permutação α de $\mathbb{Z}_p$ (Teorema 2.6) e que $G(\mathbb{Z}_p \times \mathbb{Z}_p, \sigma)$ é um p-grupo para toda permutação σ de $\mathbb{Z}_p \times \mathbb{Z}_p$ (Teorema 2.23). Seja agora $\tilde{H} = \tilde{K}$ um grupo não abeliano de ordem p^3, p primo. Fazendo $M = N = Z(\tilde{H}) = \mathbb{Z}_p$ e $H = K = \tilde{H}/M = \mathbb{Z}_p \times \mathbb{Z}_p$ no Lema 2.24, obtemos $\frac{\tilde{G}(\tilde{H},\tilde{\sigma})}{\langle \mathbb{Z}_p, \mathbb{Z}_p \rangle^{\tilde{G}}} \cong G(\mathbb{Z}_p \times \mathbb{Z}_p, \sigma)$, onde $\tilde{\sigma}$ é definida como em (2-7):*

$$\begin{aligned} \tilde{\sigma} &: m \to m^{\alpha} \\ \tilde{\sigma} &: mh \to m^{\gamma}h^{\sigma} \quad \text{se } h \neq 1. \end{aligned} \tag{2-13}$$

Pelo corolário anterior $\langle \mathbb{Z}_p, \mathbb{Z}_p \rangle^{\tilde{G}}$ é um p-grupo, logo $G(\tilde{H},\tilde{\sigma})$ é um p-grupo para toda permutação $\tilde{\sigma}$ do tipo acima. Por exemplo, consultando no GAP [12], vemos que só existem dois grupos não abelianos de ordem 3^3 :

$$(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_3, \qquad \mathbb{Z}_9 \rtimes \mathbb{Z}_3.$$

Sejam $H = (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_3$ e $K = \mathbb{Z}_9 \rtimes \mathbb{Z}_3$. Calculando no GAP obtemos $|Aut(H)| = 432$ e $|Aut(K)| = 54$; isso mostra que existem pelo menos $2!3!8! - 432 = 483408$ bijeções $\tilde{\sigma}$ (que não são isomorfismos) tal que $G((\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_3, \tilde{\sigma})$ é um p-grupo e pelo menos $2!3!8! - 54 = 483786$ bijeções $\tilde{\sigma}$ (que não são isomorfismos) tal que $G(Z_9 \rtimes \mathbb{Z}_3, \tilde{\sigma})$ é um

p-grupo. Essas quantidades são irrisórias se comparadas ao número de 26! *bijeções que deveriam ser testadas, mas podem ser razoáveis se considerarmos que a quantidade* 26! *de grupos a serem testados diminui drasticamente pelo método das classes duplas.*

2.8 O quociente meta-abeliano de $G(H,K,\sigma)$

Como vimos na Seção 1.1, um grupo G é meta-abeliano quando existe $N \trianglelefteq G$ abeliano tal que G/N é abeliano, disto segue que $G' \leq N$ e portanto

Se G é meta-abeliano, então G' é abeliano.

Nesta seção vamos considerar $G = G(H,K,\sigma)$, com H,K abelianos finitos de mesma ordem. Nosso objetivo será mostrar que o quociente meta-abeliano G/G'' (veja o Exemplo 2.29) é nilpotente de classe no máximo n. Observe que para um grupo qualquer G, o quociente G/G'' pode não ser nilpotente, por exemplo, $S_3/S_3'' \cong S_3$, que não é nilpotente.

Lema 2.27. *Seja G um grupo meta-abeliano com $u \in G'$ e $x_i \in G$ com $i = 1,2,...,s$, temos*

$$[u,x_1,x_2,...,x_s] = [u,x_{j_1},x_{j_2},...,x_{j_s}] \tag{2-14}$$

onde os $j_{r's}$ são quaisquer reordenação dos números $1,2,...,s$.

Prova. Vejamos primeiramente o caso $s = 2$:

$$\begin{aligned}
[[u,x_1],x_2] &= [u,x_1]^{-1}[u,x_1]^{x_2} \\
&= [u,x_1]^{-1}[u^{x_2},x_1^{x_2}] \\
&= [u,x_1]^{-1}[u[u,x_2],x_1[x_1,x_2]] \\
&= [u,x_1]^{-1}[u,x_1[x_1,x_2]]^{[u,x_2]}[[u,x_2],x_1[x_1,x_2]] \\
&= [u,x_1]^{-1}[u,[x_1,x_2]]^{[u,x_2]}[u,x_1]^{[x_1,x_2][u,x_2]}[[u,x_2],[x_1,x_2]][[u,x_2],x_1]^{[x_1,x_2]} \\
&= [u,x_1]^{-1}[u,x_1][[u,x_2],x_1] \quad (\text{porque } G' \text{ é abeliano}), \\
&= [[u,x_2],x_1].
\end{aligned}$$

Agora considere a identidade 2-14 verdadeira para algum $s > 2$. Como

$$[u,x_1,...,x_{s-2},x_{s-1},x_s] = [[u,x_1,...,x_{s-2}],x_{s-1},x_s],$$

o resultado segue de sucessivas aplicações do caso $s = 2$ e da hipótese de indução.

□

Lema 2.28. *Sejam H,K subgrupos abelianos de um grupo meta-abeliano G. Se $h \in H$ e $k_i \in K$, com $i = 1,...,s$, então*

$$[h,k_1,k_2,...,k_s] = [h,k_{j_1},k_{j_2},...,k_{j_s}]$$

onde os $j_{r's}$ são quaisquer reordenação dos números $1,2,...s$

Prova. Vejamos o caso $s = 2$. Pela identidade de Witt (Lema 1.6, (iv)), temos

$$\begin{aligned}
[h,k_1^{-1},k_2]^{-k_1} &= [k_1,k_2^{-1},h]^{k_2}[k_2,h^{-1},k_1]^h \\
[h^{k_1},k_1^{-1},k_2]^{-1} &= [k_2^h,h^{-1},k_1^h] \qquad (\text{porque } K \text{ é abeliano}), \\
[k_1,h,k_2]^{-1} &= [h,k_2,k_1^h] \qquad (\text{pelo Lema 1.6, (ii)}), \\
([k_1,h,k_2]^{[k_1,h]^{-1}})^{-1} &= [h,k_2,k_1[k_1,h]] \quad (\text{porque } G' \text{ é abeliano}), \\
[h,k_1,k_2] &= [[h,k_2],[k_1,h]][[h,k_2],k_1]^{[k_1,h]} \quad (\text{pelo Lema 1.6, (iii), (v)}), \\
[h,k_1,k_2] &= [h,k_2,k_1] \qquad (\text{porque } G' \text{ é abeliano}).
\end{aligned}$$

O caso geral decorre de sucessivas aplicações do caso $s = 2$ e do lema anterior, por exemplo, para $s = 3$:

$$\begin{aligned}
[h,k_1,k_2,k_3] &= [[h,k_1,k_2],k_3], \\
&= [[h,k_2],k_1,k_3] \qquad (\text{caso } s = 2), \\
&= [h,k_2,k_3,k_1] \qquad (\text{lema anterior}),
\end{aligned}$$

e assim por diante. □

Teorema 2.29. *Sejam H,K grupos abelianos finitos de ordem n e $G = G(H,K,\sigma)$. Então o grupo G/G'' é nilpotente de classe no máximo n.*

Prova. Identificando os geradores de G/G'' com os geradores de G, podemos escrever $G/G'' = \langle h_1,...,h_n,k_1,...,k_n\rangle$, se mostrarmos que

$$[x_{j_1},x_{j_2},...,x_{j_{n+1}}] = 1$$

onde os x_{j_r} são quaisquer geradores de G/G'', então pelo Corolário 1.8, o teorema seguirá. Primeiramente observe que fixado $x_{j_1} = h \in H$, se algum dos elementos $x_{j_2},...,x_{j_{n+1}}$ pertencer a H, digamos x_{j_r}, então

$$\begin{aligned}
[h,x_{j_2},...x_{j_r},...,x_{j_{n+1}}] &= [h,x_{j_r},...,x_{j_{n+1}}] \quad (\text{pelo Lema 2.28}) \\
&= 1 \qquad\qquad\qquad\qquad (\text{porque } [h,x_{j_r}] = 1).
\end{aligned}$$

É claro que a mesma observação se verifica para $k \in K$ fixado e algum $x_{j_r} \in K$. Desse modo, é suficiente mostrar que

$$[h,k_1,k_2,...,k_n] = 1,$$

com $h \in H$ fixado e todos os k_j pertencendo a K. Como $h^\sigma = k_s$ para algum $s \in \{1,...,n\}$, temos

$$\begin{aligned} [h,k_1,\ldots,k_s,\ldots,k_n] &= [h,k_s,\ldots,k_n] \quad \text{(pelo Lema 2.28)}, \\ &= [h,h^\sigma,\ldots,k_n], \\ &= 1 \quad \text{(porque } [h,h^\sigma]=1\text{)}. \end{aligned}$$

□

Corolário 2.30. *Seja $G = G(H,K,\sigma)$, se G' for nilpotente, então G é nilpotente.*

Prova. Pelo teorema de P. Hall, (veja Robinson [8] pág 134), se G é um grupo qualquer em que $N \trianglelefteq G$ com N e G/N' nilpotentes, então G é nilpotente. Fazendo $N = G'$, com $G = G(H,K,\sigma)$, no teorema de Hall, segue o corolário. □

2.9 O grupo $G(H,\sigma)$, H um p-grupo abeliano elementar, p ímpar e σ uma transposição

Nesta seção vamos provar a Conjectura 2 para um caso particular do grupo $G(H,K,\sigma)$, a saber quando $H,K \cong A_{p,k}$, p é ímpar e σ é uma transposição. Mais precisamente, se $1,h_1,h_2,\ldots,h_n$ são os elementos de H e $1,h_1^\varphi,\ldots,h_n^\varphi$ são os elementos de $K = H^\varphi$ ($\varphi : H \longrightarrow K$ um isomorfismo), então $\sigma : H \longrightarrow H^\varphi$ é uma bijeção satisfazendo

$$1^\sigma = 1,\ \ h_i^\sigma = h_j^\varphi,\ \ h_j^\sigma = h_i^\varphi \ \text{ com } \ i \neq j \ \text{ e } \ h_s^\sigma = h_s^\varphi \ \ \forall s \neq i,j \qquad \text{(2-15)}$$

Vamos começar fazendo uma pequena adaptação de um lema, encontrado em Sidki [11]; aqui H é um grupo qualquer.

Lema 2.31. *Em $G(H,\sigma)$, se $h,k \in H$ são tais que $(hk)^\sigma = h^\sigma k^\sigma$ e $(k^{-1})^\sigma = (k^\sigma)^{-1}$, então*

$$[h,(k^{-1})^\sigma] = [h^\sigma,k^{-1}].$$

Prova.

$$
\begin{aligned}
1 &= [hk,(hk)^\sigma] = [h,(hk)^\sigma]^k[k,(hk)^\sigma], && (2\text{-}16)\\
[h,(hk)^\sigma] &= [h,h^\sigma k^\sigma] = [h,k^\sigma][h,h^\sigma]^{k^\sigma} = [h,k^\sigma], && (2\text{-}17)\\
[k,(hk)^\sigma] &= [k,h^\sigma k^\sigma] = [k,k^\sigma][k,h^\sigma]^{k^\sigma} = [k,h^\sigma]^{k^\sigma}, && (2\text{-}18)\\
1 &= [h,k^\sigma]^k[k,h^\sigma]^{k^\sigma} && \text{(por substituição de (2-17) e (2-18) em (2-16))},\\
1 &= [h,k^\sigma]^{(k^\sigma)^{-1}}[k,h^\sigma]^{k^{-1}} && \text{(pela conjugação por } k^{-1}(k^\sigma)^{-1}), && (2\text{-}19)\\
[h,k^\sigma]^{(h^\sigma)^{-1}} &= [h,(k^\sigma)^{-1}]^{-1} && \text{(pelo Lema 1.6, (v))}, && (2\text{-}20)\\
[k,h^\sigma]^{k^{-1}} &= [k^{-1},h^\sigma]^{-1} && \text{(idem)}, && (2\text{-}21)\\
1 &= [h,(k^\sigma)^{-1}]^{-1}[k^{-1},h^\sigma]^{-1} && \text{(por substituição de (2-20) e (2-21) em (2-19))},\\
\left[h,(k^\sigma)^{-1}\right] &= [h^\sigma,k^{-1}],\\
\left[h,(k^{-1})^\sigma\right] &= [h^\sigma,k^{-1}] && \text{(porque } (k^{-1})^\sigma = (k^\sigma)^{-1}).
\end{aligned}
$$

□

Quando H é um grupo abeliano finito de ordem ímpar e $\sigma : h_i \longleftrightarrow h_j$ é uma transposição (conforme 2-15), decorre do lema acima que a igualdade

$$\left[h_i,(h_j^{-1})^\sigma\right] = [h_i^\sigma,h_j^{-1}] \tag{2-22}$$

é verdadeira em $G(H,\sigma)$. De fato, $h_ih_j \neq h_i$, caso contrário, teríamos $h_j^2 = 1$, o que não é possível pois H tem ordem ímpar. Analogamente $h_ih_j \neq h_j$. Segue então que

$$(h_ih_j)^\sigma = (h_ih_j)^\varphi = h_i^\varphi h_j^\varphi = h_j^\sigma h_i^\sigma = h_i^\sigma h_j^\sigma.$$

A última igualdade vale porque H é abeliano. Também $(h_j^{-1})^\sigma = (h_j^\sigma)^{-1}$, porque $h_j^{-1} \neq h_j$. Obtemos assim as condições do Lema 2.31 sobre h_i e h_j, valendo pois, a relação dada em 2-22.

Proposição 2.32. *Se H é um grupo abeliano finito de ordem ímpar e $\sigma : h_i \longleftrightarrow h_j$ é uma transposição tal que $h_j = h_i^r$, para algum r natural, então $G(H,\sigma) \cong \chi(H)$.*

Prova. As únicas relações de $G(H,\sigma) = \langle H,H^\varphi | [h_s,h_s^\sigma] = 1, s = 1,2,\ldots,n\rangle$ que não estão em $G(H,\varphi) = \langle H,H^\varphi | [h_s,h_s^\varphi] = 1, s = 1,2,\ldots,n\rangle$ são

$$[h_i,h_i^\sigma] = 1 = [h_j,h_j^\sigma].$$

Mostremos que elas são consequências das relações de $G(H,\varphi)$. De fato

$$[h_i,h_i^\sigma] = [h_i,h_j^\varphi] = [h_i,(h_i^r)^\varphi] = [h_i,(h_i^\varphi)^r].$$

Assim, $[h_i,h_i^{\varphi}]=1$ implica $[h_i,h_i^{\sigma}]=1$. Como $[h_j,h_j^{\sigma}]=[h_j,h_i^{\varphi}]=[h_i^r,h_i^{\varphi}]$, temos que $[h_i,h_i^{\varphi}]=1$ implica $[h_j,h_j^{\sigma}]=1$. Podemos então escrever

$$\begin{aligned}\chi(H) &= \langle H,H^{\varphi}|[h_s,h_s^{\varphi}]=1,s=1,2,\cdots,n,[h_i,h_i^{\sigma}]=1=[h_j,h_j^{\sigma}]\rangle \qquad (2\text{-}23)\\ &= \langle H,H^{\varphi}|[h_s,h_s^{\sigma}]=1,s=1,2,\cdots,n,[h_i,h_i^{\varphi}]=1=[h_j,h_j^{\varphi}]\rangle \qquad (2\text{-}24)\end{aligned}$$

Vamos mostrar agora que as relações definidoras $[h_i,h_i^{\varphi}]=1=[h_j,h_j^{\varphi}]$ são consequências das relações de $G(H,\sigma)$. Como $[h_j,h_j^{\varphi}]=[h_i^r,h_i^{\sigma}]$, obtemos que $[h_i,h_i^{\sigma}]=1$ implica $[h_j,h_j^{\varphi}]=1$. Agora observe que

$$\begin{aligned}[h_i,(h_j^{\sigma})^{-1}] &= [h_i,(h_j^{-1})^{\sigma}],\\ &= [h_i^{\sigma},h_j^{-1}] \qquad \text{(por (2-22))},\\ &= [h_i^{\sigma},h_i^{-r}].\end{aligned}$$

Consequentemente, $[h_i,h_i^{\sigma}]=1$ implica $[h_i,(h_j^{\sigma})^{-1}]=1$, que por sua vez, implica $[h_i,h_j^{\sigma}]=[h_i,h_i^{\varphi}]=1$. Retirando as relações definidoras $[h_i,h_i^{\varphi}]=1=[h_j,h_j^{\varphi}]$ em 2-24 obtemos

$$G(H,\varphi)=\langle H,H^{\varphi}|[h_s,h_s^{\sigma}]=1,s=1,2,\cdots,n\rangle=G(H,\sigma).$$

□

Lema 2.33. *Todos os grupos $G(H,K,\sigma)$ com $H=K=A_{p,k}$ fixado e σ permutando elementos linearmente independentes são isomorfos.*

Prova. Sejam $\sigma: h \longleftrightarrow k$ e $\tau: \tilde{h} \longleftrightarrow \tilde{k}$ transposições permutando elementos linearmente independentes. Considerando H como um espaço vetorial sobre $\mathbb{Z}_p$ e identificando $Aut(H)$ com $GL(k,p)$, podemos completar os conjuntos $\{h,k\}$ e $\{\tilde{h},\tilde{k}\}$ para obter bases B e $\tilde{B}$ de H. Assim, a aplicação $B \longrightarrow \tilde{B}$ estende-se a um automorfismo α de H onde

$$\begin{aligned}\tilde{h}^{\alpha^{-1}\sigma\alpha} &= h^{\sigma\alpha}=k^{\alpha}=\tilde{k}\\ \tilde{k}^{\alpha^{-1}\sigma\alpha} &= k^{\sigma\alpha}=h^{\alpha}=\tilde{h}\end{aligned} \qquad \begin{array}{ccc} h & \overset{\sigma}{\longleftrightarrow} & k \\ \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\alpha} \\ \tilde{h} & \underset{\sigma^{\alpha}}{\longleftrightarrow} & \tilde{k} \end{array}$$

Se $x\neq\tilde{h},\tilde{k}$, então $x^{\alpha^{-1}}\neq h,k$ e obtemos $x^{\alpha^{-1}\sigma\alpha}=x^{\alpha^{-1}\alpha}=x$, logo $\tau=\sigma^{\alpha}$ e segue pela Proposição 2.9 que $G(H,\tau)=G(H,\sigma^{\alpha})\cong G(H,\sigma)$. □

Para simplificar a notação, até ao final desta seção, vamos denotar h^{φ} por $\dot{h}$ e escrever $\dot{H}$ no lugar de H^{φ}.

Lema 2.34. *Seja $H = \langle a_1, \ldots, a_k \rangle$ um grupo abeliano e $\sigma : H \longrightarrow \dot{H}$ uma bijeção tal que $a_i^\sigma = \dot{a}_i$, $(a_i {a_j}^{-1})^\sigma = \dot{a}_i {\dot{a}_j}^{-1}$ com $i, j \in \{1, 2, \ldots, k\}$. Então a identidade*

$$[a_i, \dot{a}_j] = [\dot{a}_i, a_j], \quad i, j \in \{1, 2, \ldots, k\}$$

vale em $G(H,\sigma)$.

Prova. Inicialmente, observe que

$$\begin{aligned} [a_i, \dot{a}_j] = [a_i a_j^{-1}, \dot{a}_j] &= [a_i a_j^{-1}, \dot{a}_i \dot{a}_j^{-1} \dot{a}_j] \\ &= [a_i a_j^{-1}, \dot{a}_i] \\ &= [a_j^{-1}, \dot{a}_i]. \end{aligned} \tag{2-25}$$

Assim

$$\begin{aligned} 1 = [a_j a_j^{-1}, \dot{a}_i] &= [a_j, \dot{a}_i]^{a_j^{-1}} [a_j^{-1}, \dot{a}_i], \\ &= [a_i^{-1}, \dot{a}_j]^{a_j^{-1}} [a_i, \dot{a}_j] \qquad \text{(por (2-25))}, \\ &= [a_i^{-1}, \dot{a}_j][a_i, \dot{a}_j], \\ &= [a_j, \dot{a}_i][a_i, \dot{a}_j] \qquad \text{(por (2-25))}, \\ [a_i, \dot{a}_j] &= [\dot{a}_i, a_j]. \end{aligned}$$

□

Proposição 2.35. *Seja $H = A_{p,k}$, p ímpar, $k \geq 3$ e $\sigma : H \longrightarrow \dot{H}$ uma transposição. Então o grupo $G(H,\sigma)$ é um quociente do grupo $\chi(H)$.*

Prova. Pela Proposição 2.32, $G(H,\sigma) \cong \chi(H)$ quando σ permuta elementos linearmente dependentes de H. Assim podemos supor que σ permuta elementos linearmente independentes de H. Uma vez que $a_1 a_k$ e $a_2 a_k$ são linearmente independentes, pelo Lema 2.33, podemos supor

$$\sigma : a_1 a_k \longleftrightarrow a_2 a_k.$$

Como $a_i \neq a_1 a_k, a_2 a_k$ para $i = 1, \ldots, k$ (porque $\{a_1, \ldots, a_k\}$ é linearmente independente) e $a_i a_k^{-1} \neq a_i a_k$ para $i = 1, 2$ (porque $|H|$ é ímpar), σ satisfaz as condições do lema anterior. Observe que as únicas relações definidoras de $\chi(H)$ que não estão na definição de $G(H,\sigma)$ são

$$[a_1 a_k, \dot{a}_1 \dot{a}_k] = 1 = [a_2 a_k, \dot{a}_2 \dot{a}_k].$$

Considerando $i = 1,2$ e trabalhando em $G(H,\sigma)$, temos

$$\begin{aligned}
[a_i a_k, \dot{a}_i \dot{a}_k] &= [a_i, \dot{a}_i \dot{a}_k]^{a_k} [a_k, \dot{a}_i \dot{a}_k] \\
&= [a_i, \dot{a}_k]^{a_k} [a_i, \dot{a}_1]^{\dot{a}_k a_k} [a_k, \dot{a}_i][a_k, \dot{a}_k]^{\dot{a}_i} \\
&= [a_i, \dot{a}_k][a_k, \dot{a}_i] \\
&= [a_i, \dot{a}_k][\dot{a}_k, a_i] = 1 \qquad \text{(pelo Lema 2.34)}.
\end{aligned}$$

Assim, todas as relações de $\chi(H)$ são consequências das relações de $G(H,\sigma)$; segue do teorema de von Dick que $G(H,\sigma)$ é um quociente de $\chi(H)$. □

Teorema 2.36. *Seja $H = A_{p,k}$, p ímpar e $\sigma : H \longrightarrow \dot{H}$ uma transposição. Então $G(H,\sigma)$ é um p-grupo com classe de nilpotência no máximo 3.*

Prova. Os casos $k = 1$ e $k = 2$ já foram mostrados nos Teoremas 2.6 e 2.23. Sabemos que $\chi(H)$ possui classe de nilpotência no máximo 3 (pelo resultado de Gupta, Rocco e Sidki [1] citado na Introdução), como $G(H,\sigma)$ é um quociente de $\chi(H)$, segue da Proposição 1.5 que $G(H,\sigma)$ é um p-grupo com classe de nilpotência no máximo 3. □

Observação 2.37. *Para $p = 2$ o teorema acima pode não ser verdadeiro. De fato, o grupo $G(A_{2,4},(14,15))$ calculado na Seção 2.3 possue classe de nilpotência igual a 5. Observe também que a Proposição 2.35 não é verdadeira para $p = 2$. De fato, como os grupos $G(A_{2,4},(14,15))$ e $\chi(A_{2,4})$ possuem a mesma ordem, se o primeiro fosse um quociente do segundo, então eles deveriam ser isomorfos, mas isso não é verdade pois eles diferem quanto a classe de nilpotência.*

Observação 2.38. *Pelo que vimos na Observação 2.7, $H \times H$ é uma imagem homomorfa de $\chi(H)$, assim todos os grupos $G(A_{3,3},\sigma)$ de ordens 3^6 do Exemplo 2.4 são imagens homomorfas de $\chi(A_{3,3})$. Utilizando o GAP [12] vemos que nenhum dos 235 representantes de classes duplas são transposições.*

Referências Bibliográficas

[1] GUPTA, N.; ROCCO, N. S. S. **Diagonal embeddings of nilpotent groups**. Illiois J. of Math, 30, 1986.

[2] ISAR, S. A; TADINI, W. M. **Teoria axiomática dos conjuntos: uma introdução**. UNESP, 1998.

[3] JOHNSON, D. L. **Presentation of groups**. Cambridge University Press, 1997.

[4] LYNDON, R. C; SCHUPP, P. E. **Combinatorial group theory**. Springer-Verlag, 1977.

[5] MAGNUS, W; KARRAS, A; SOLITAR, D. **Combinatorial group theory: presentation of groups in terms of generators and relations**. Interscience, 1966.

[6] OLIVEIRA, R. N. **Comutatividade Fraca entre Grupos Isomorfos**. PhD thesis.

[7] OLIVEIRA, R. N; SIDKI, S. N. **On commutativity and finiteness in groups**. Bull. of the Braz. Math. Soc., 40(2):149–180, 2009.

[8] ROBINSON, D. J. S. **A course in the theory of groups**. Springer-Verlag, 1995.

[9] ROCCO, N. R. **On weak commutativity between finite p-groups, p odd**. Journal of Algebra, 76, 1982.

[10] ROTMAN, J. J. **The introduction to the theory of groups**. Springer-Verlag, 1994.

[11] SIDKI, S. N. **On weak permutability between groups**. Journal of Algebra, 63:186–225, 1980.

[12] **The GAP Group, GAP - Groups, Algorithms and Programming, Version 4.4.12**. (http://www.gap-system.org), 2008.

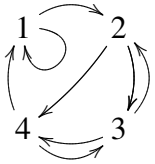
Apêndice

Grafos

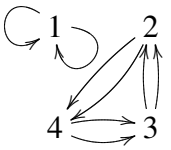
Definição .39. *Um grafo orientado $\Gamma = (V,A)$ consiste de um conjunto V de vértices e um conjunto generalizado A (não ordenado e podendo conter repetições) de elementos $a = (u,v)$ de $V \times V$, chamados arestas orientadas de u para v.*

Exemplo .6. *Um grafo orientado fica inteiramente determinado através do seu diagrama.*

(i) Para $V = \{1,2,3,4\}$ e $A = \{(1,1),(1,2),(2,3),(2,4),(3,4),(3,2),(4,1),(4,3)\}$, temos



(ii) Para $V = \{1,2,3,4\}$ e $A = \{(1,1),(1,1),(2,4),(2,4),(3,2),(3,2),(4,3),(4,3)\}$, temos

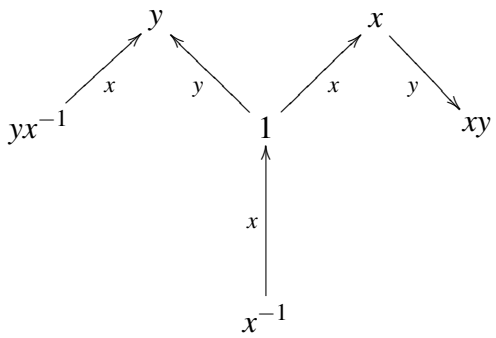


Dados dois vértices u,v em um grafo, um *caminho* de u a v é uma sequência $u = v_0, a_1, v_1, \ldots, v_{n-1}, a_n, v_n = v$ de vértices não repetidos v_i (exceto possivelmente u e v) e arestas não repetidas $a_i = (v_{i-1}, v_i)$. Um caminho de u a u é chamado de *circuito*. Um grafo orientado diz-se *conexo* se para quaisquer dois vértices u e v do grafo, existir um caminho de u a v. Assim, no exemplo anterior, o primeiro grafo orientado é conexo, mas o segundo não. Um tipo muito especial de grafo orientado é o seguinte:

Definição .40. *Uma árvore é um grafo orientado $\Gamma = (V,A)$ que é conexo, sem circuitos e A não contém arestas repetidas.*

No Exemplo .6, o primeiro grafo orientado não é uma árvore pois contém circuitos: $1(1,1)1$ e $1(1,2)2(2,4)4(4,1)1$ são dois deles; o segundo grafo orientado não é uma árvore pois falha em duas condições: não é conexo e contém arestas repetidas.

Exemplo .7. *Seja $F = F(x,y)$ um grupo livre e H o subgrupo de F do Exemplo 1.5,(iii). Seja $U = \{1, x, x^{-1}, y, x, yx^{-1}\}$ um transversal de H em F. Considere o grafo orientado Γ com vétices $V = U$ e arestas $a = (u,v) \Longleftrightarrow ux = v$ para algum $x \in X = \{x,y\}$. Afirmamos que Γ é uma árvore. De fato, não há vértices repetidos pois se $ux = v$ e $uy = v$ então $x = y$; Γ é conexo pois sendo U um transversal de Schreier, todo vértice se conecta por algum caminho a 1. Por último, não existem circuitos, porque sendo F um grupo livre, não possui relações.*



Lema .41. *Em uma árvore $\Gamma = (V,A)$, temos $|V| - |A| = 1$.*

Prova. O caso $|V| = 2$ é trivial. Supondo que valha $|V| - |A| = 1$ para algum valor $|V|$, acrescentando um vértice ao grafo obtemos mais uma aresta, logo $(|V|+1) - (|A|+1) = |V| - |A| = 1$. □

Algoritmo para o cálculo do grupo $G(H, \sigma)$

```
Reread("csetgrp.gi");
# Melhoria da rotina "DoubleCosetRepsAndSizes(G,U,V)$ fornecida por
# Alexander Hulpke
g:=  ElementaryAbelianGroup(2^4); # 2-grupo abeliano elementar de posto 4
el:= Elements(Difference(g,[One(g)])); # cria uma lista com os elementos de g\{e}
pl:= FreeProduct(g,g); # produto livre g*g
i1:= Embedding(pl,1); # imersão g --> g*h
i2:= Embedding(pl,2); # imersão h --> g*h

sym:=SymmetricGroup(Size(el)); # calcula o grupo simétrico S_{|g|-1}
aut:=AutomorphismGroup(g); # calcula o grupo Aut(g)
gen:=GeneratorsOfGroup(aut); # cria uma lista com os geradores de Aut(g)

gen1:=List(gen , x-> List(el, y->y^x)); # cria uma lista com as imagens de
# cada gerador em gen
```

```
pgen1:= List(gen1,x-> List(x,y->Position(el,y))); # cria uma lista com as posições
#  das imagens de cada gerador em gen

gaut:=List(pgen1,x-> PermListList([1..Size(el)],x)); # cria uma lista com as
# permutações em S_{|g|-1} correspondentes a cada gerador em gen

paut:=Group(gaut); # gera uma cópia de Aut(g) em S_{|g|-1}


dc:=DoubleCosetRepsAndSizes(sym,paut,paut); # cria uma lista com os representantes
# das classes duplas Aut(g)\S_{|g|-1}/Aut(g) com a respectiva ordem de cada classe

perm:=[];;

for y in dc do
Add(perm, dc[Position(dc,y)][1]);
                    od; # cria uma lista com os representantes de classes duplas

rel:=[];

for sigma in perm do
        rel[Position(perm,sigma)]:=[];
       for x in el do
 Add(rel[Position(perm,sigma)],Comm(Image(i1,x),Image(i2,el[Position(el,x)^sigma])));
     od;
   od;
# cria a lista rel:= [rel[1], rel[2], rel[3], ..., rel[|sym|] com as relações
# definidoras de cada grupo

list:=[];
for x in rel do
Add(list,FactorGroupFpGroupByRels(pl,x));
     od;
# cria a lista de grupos [G(g*g|rel[1]), G(g*g|rel[2], ..., G(g*g|rel[|sym|]

for x in list do
Print(Size(x)," ",NilpotencyClassOfGroup(x)," ",DerivedLength(x),"\n");
od;

# imprime na tela a ordem, classe de nilpotência e comprimentos derivado dos
# grupos, o "\n" realiza um quebra de linha
```

```
Reread("csetgrp.gi");
g:=ElementaryAbelianGroup(3^3); # p-grupo abeliano elementar de posto 3
sgc:=Difference(Zuppos(g),[One(g)]);
# cria uma lista com os geradores dos subgrupos cíclicos de g
pl:= FreeProduct(g,g);
i1:= Embedding(pl,1);
i2:= Embedding(pl,2);

sym:=SymmetricGroup(Size(sgc));
aut:=AutomorphismGroup(g);
gen:=GeneratorsOfGroup(aut);

gen1:=List(gen , x-> List(sgc, y-> Intersection(Group(y^x),sgc)));
gen1:=List(gen1,x->List(x,y->y[1]));

pgen1:= List(gen1,x-> List(x,y->Position(sgc,y)));

gaut:=List(pgen1,x-> PermListList([1..Size(sgc)],x));

paut:=Group(gaut);
# cria uma cópia de PGL(3,3) em S_{13}

dc:=DoubleCosetRepsAndSizes(sym,paut,paut);


perm:=[];;

for y in dc do
Add(perm, dc[Position(dc,y)][1]);
             od;


rel:=[];

for sigma in perm do
        rel[Position(perm,sigma)]:=[];
for x in sgc do
Add(rel[Position(perm,sigma)],Comm(Image(i1,x),Image(i2,sgc[Position(sgc,x)^sigma])));
od;
od;
```

```
list:=[];
for x in rel do
Add(list,FactorGroupFpGroupByRels(pl,x));
     od;

for x in list do
   Print(Size(x),"\n");
      od;
```

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo