Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Grupos com ao menos dois geradores a mais do que relações

por

João Vitor Gonçalves de Almeida

Brasília
2010

À minha família, aos meus
amigos e à minha namorada.

AGRADECIMENTOS

A Deus, por sempre ter abençoado, protegido e iluminado a minha vida.

À minha família, que sempre me apoiou e me ajudou em todos os projetos de minha vida, em especial nesta caminhada.

À minha namorada, Jaqueline, pelo carinho, incentivo, compreensão e paciência.

Aos meus amigos João Paulo, Paulo Henrique, Pedro Henrique e Wendel, por estarem sempre presentes nos momentos difíceis.

Aos meus colegas de graduação, pelos momentos de alegria e descontração. Em especial, Diego, Bruno, Isaac, Harudgy, Humberto e Fillippi.

Aos meus colegas de mestrado, pelos momentos de companheirismo e trocas de conhecimentos. Em especial, Marcos Mesquita, Felipe Batista, Igor dos Santos, Andréia Avelar e Laura Cristina.

À minha orientadora, Aline G. S. Pinto, pelos ensinamentos, esclarecimentos, correções e sugestões.

Aos professores Sheila C. Chagas e Antônio P. B. Júnior, por participarem da comissão examinadora desta dissertação e pelas suas contribuições.

Aos professores do Departamento de Matemática da UnB, que muito me ensinaram e contribuíram para a minha formação acadêmica. Em especial, Lineu Neto, José Alfredo, Angel Baigorri, Maurício Ayala, Cátia Gonçalves e Alexei Krassilnikov.

Aos funcionários do Departamento de Matemática da UnB, pela prestatividade que sempre demonstraram. Em especial, Manuel, Isabel, Tânia e Eveline.

Ao CNPq, pelo apoio financeiro.

"O valor das coisas não está no tempo que elas duram,
mas na intensidade com que acontecem.
Por isso, existem momentos inesquecíveis,
coisas inexplicáveis e pessoas incomparáveis."
(Fernando Pessoa)

RESUMO

Neste trabalho, estudamos grupos finitamente apresentados com mais geradores do que relações. Inicialmente, consideramos um grupo tendo uma apresentação finita com ao menos um gerador a mais do que relações e, neste caso, provamos que existe um epimorfismo deste grupo para $\mathbb{Z}$. Posteriormente, consideramos um grupo tendo uma apresentação finita com ao menos dois geradores a mais do que relações e, neste caso, expomos a demonstração feita por Baumslag e Pride em [1] que garante que este grupo possui um subgrupo de índice finito que pode ser epimorficamente aplicado para o grupo livre F_2 de posto 2.

ABSTRACT

In this work, we study finitely presented groups with more generators than relators. First, we consider a group having a finite presentation with at least one more generator than relators and, in this case, we prove that there is an epimorphism from this group to $\mathbb{Z}$. Later, we consider a group having a finite presentation with at least two more generators than relators and, in this case, we give the proof done by Baumslag and Pride in [1] which ensure that this group has a subgroup of finite index that can be mapped homomorphically onto the free group F_2 of rank 2.

SUMÁRIO

INTRODUÇÃO

Esta dissertação tem como objetivo demonstrar os dois seguintes resultados principais:

Lema 2.7. *Seja G um grupo tendo uma apresentação finita $\varphi : F \longrightarrow G$ com p geradores e q relações, onde $p - q \geq 1$. Então, existe um epimorfismo de G para $\mathbb{Z}$. Além disso, podemos obter uma nova apresentação para G com p geradores e q relações, na qual um dos geradores aparece com soma dos expoentes zero em todas as relações;*

Teorema 2.8. *Seja G um grupo tendo uma apresentação finita com g geradores e r relações, onde $g - r \geq 2$. Então, G possui um subgrupo H de índice finito que pode ser epimorficamente aplicado para F_2 (o grupo livre de posto 2).*

O Teorema 2.8 é devido a Baumslag e Pride e, nesta monografia, a demonstração que expomos para este teorema é a dada por tais autores em [1].

O Lema 2.7 garante que qualquer grupo tendo uma apresentação finita com ao menos um gerador a mais do que relações pode ser epimorficamente aplicado para $\mathbb{Z}$ (o grupo livre de posto 1). Logo, faz sentido perguntarmos se qualquer grupo tendo uma apresentação finita com ao menos dois geradores a mais do que relações pode ser epimorficamente aplicado para F_2. Assim, o Lema 2.7 nos serve como uma motivação para estudarmos o Teorema 2.8.

Mas, em 1975, Stallings mostrou em [10] que existem grupos tendo apresentações finitas com ao menos dois geradores a mais do que relações que não podem ter F_2 como imagem homomórfica. Dessa maneira, Stallings provou que não é possível fortalecermos a conclusão do Teorema 2.8 dizendo que existe um epimorfismo de G para F_2.

Notemos também que não é possível enfraquecermos a hipótese $g - r \geq 2$ do Teorema 2.8 para $g - r \geq 1$, pois um grupo com apresentação $\langle a_1, \ldots, a_n \mid a_1, \ldots, a_{n-1} \rangle$ é cíclico infinito e, portanto, não possui nenhum subgrupo tendo F_2 como imagem homomórfica.

Em 1979, Baumslag e Pride conjeturaram em [2] que qualquer grupo tendo uma apresentação finita com ao menos um gerador a mais do que relações possui um subgrupo de índice finito que pode ser epimorficamente aplicado para F_2, desde que uma das relações da apresentação seja uma potência própria. Notemos que não pode ser omitida a condição de uma relação da apresentação ser uma potência própria, já que um grupo com apresentação $\langle a_1, \ldots, a_n \mid a_1, \ldots, a_{n-1} \rangle$ é cíclico infinito e, portanto, não pode ter F_2 como imagem homomórfica.

Esta conjetura teve duas provas independentes. Uma foi feita por Gromov em [3] usando "bounded cohomology"no ano de 1982 e a outra foi feita por Stöhr em [11] usando um argumento algébrico direto no ano de 1983.

Em 2005, Lackenby obteve tanto o Teorema 2.8 quanto a conjectura supracitada como corolários de um teorema por ele demonstrado em [6].

Mas, nesta dissertação, não são estudados tais resultados nem suas demonstrações. Eles foram mencionados aqui apenas para termos uma noção histórica que envolve o Teorema 2.8.

No Capítulo 1, desenvolvemos todos os pré-requisitos necessários para o completo entendimento da prova do Teorema 2.8, introduzindo os conceitos básicos e os resultados essenciais sobre grupos abelianos livres, grupos abelianos finitamente gerados, grupos livres, produto livre, transformações de Tietze e o processo de reescrita de Reidemeister-Schreier. As referências principais para a construção deste capítulo são [9], [4], [7] e [8].

No Capítulo 2, o último deste trabalho, exibimos alguns resultados e definições auxiliares para, enfim, demonstrarmos os dois resultados principais, que são o Lema 2.7 e o Teorema 2.8.

CAPÍTULO 1

PRELIMINARES

Descreveremos, neste capítulo, alguns pré-requisitos necessários para melhor entendermos os assuntos introduzidos no Capítulo 2. Dessa maneira, apresentaremos os conceitos de **grupo abeliano livre**, de **grupo abeliano finitamente gerado**, de **grupo livre** e de **produto livre**, além de abordarmos algumas propriedades importantes referentes a estas classes de grupos. Também estudaremos as **transformações de Tietze** e o **processo de reescrita de Reidemeister-Schreier**, que são tópicos interessantes da Teoria de Grupos.

1.1 Grupos Abelianos

Nesta seção, adotaremos a notação aditiva.

1.1.1 Soma Direta

Sejam K um conjunto qualquer e $\{A_k; k \in K\}$ uma família de grupos abelianos.

Definição 1.1. *O* **produto direto** *dos A_k's, denotado por $\prod_{k\in K} A_k$, é o grupo cujo conjunto subjacente é o produto cartesiano dos A_k's (ou seja, o conjunto de todos os "vetores" (a_k) com k-componente $a_k \in A_k$) e cuja operação é definida coordenada a coordenada (ou seja, $(a_k) + (b_k) = (a_k + b_k)$, $\forall a_k, b_k \in A_k$).*

É claro que o elemento identidade de $\prod_{k\in K} A_k$ é (0) e que $-(a_k) = (-a_k)$.

A **soma direta** *dos $A_k's$, denotada por $\bigoplus_{k\in K} A_k$, é o subgrupo de $\prod_{k\in K} A_k$ formado por todos os "vetores" (a_k) para os quais $a_k \neq 0$ somente para um número finito de $k \in K$.*

Logo, se K é finito, então $\prod_{k\in K} A_k = \bigoplus_{k\in K} A_k$.

Proposição 1.2. *Seja $\{A_k; k \in K\}$ uma família de subgrupos de um grupo abeliano G, onde K é um conjunto qualquer. Então, são equivalentes:*

a) $G \cong \bigoplus_{k\in K} A_k$. Mais precisamente, $\begin{array}{rcl} \varphi : \bigoplus_{k\in K} A_k & \longrightarrow & G \\ (a_k) & \longmapsto & \sum_{k\in K} a_k \end{array}$ *é um isomorfismo;*

b) Cada $g \in G$ tem uma única expressão da forma

$$g = \sum_{k\in K} a_k,$$

onde $a_k \in A_k$, todos os k são distintos e $a_k \neq 0$ somente para um número finito de k;

c) $G = \langle \bigcup_{k\in K} A_k \rangle$ e, para cada $j \in K$, $A_j \cap \langle \bigcup_{k\neq j} A_k \rangle = \{0\}$.

Demonstração: Mostremos que $a)$ implica $b)$. Como φ é sobrejetiva, segue que cada $g \in G$ pode ser escrito como $g = \sum_{k\in K} a_k$. Falta mostrarmos que esta expressão é única. Assim, suponhamos que $g = \sum_{k\in K} b_k$. Logo, $\varphi((a_k)) = \varphi((b_k))$. Como φ é injetiva, segue que $(a_k) = (b_k)$ e, portanto, $a_k = b_k$, $\forall k \in K$.

Agora, $b)$ implica $c)$. Como cada $g \in G$ tem uma expressão da forma $g = \sum_{k\in K} a_k$, segue que $G = \langle \bigcup_{k\in K} A_k \rangle$. Falta mostrarmos que $A_j \cap \langle \bigcup_{k\neq j} A_k \rangle = \{0\}$, para cada $j \in K$. Assim, seja $g = A_j \cap \langle \bigcup_{k\neq j} A_k \rangle$. Então, $g = a_j$ e $g = \sum_{k\neq j} a_k$. Como a expressão de g é única, segue que $a_j = 0$ e $a_k = 0$, $\forall k \neq j$. Logo, $g = 0$.

Finalmente, $c)$ implica $a)$. Como $G = \langle \bigcup_{k\in K} A_k \rangle$, segue que φ é sobrejetiva. É claro que φ é um homomorfismo, pois $\varphi((a_k) + (b_k)) = \varphi((a_k + b_k)) = \sum (a_k + b_k) = \sum a_k + \sum b_k = \varphi(a_k) + \varphi(b_k)$. Falta mostrarmos que φ é injetiva. Se $(a_k) \in Ker\varphi$, então $\sum_{k\in K} a_k = 0$. Portanto, $-a_j = \sum_{k\neq j} a_k \in A_j \cap \langle \bigcup_{k\neq j} A_k \rangle = \{0\}$. Assim, $a_j = 0$, $\forall j \in K$. Logo, $(a_k) = (0)$.

■

Teorema 1.3. *Sejam G um grupo abeliano, $\{A_k; k \in K\}$ uma família de grupos abelianos e $\{i_k : A_k \to G; k \in K\}$ uma família de homomorfismos. Então, $G \cong \bigoplus_{k\in K} A_k$ se, e somente se, para todo grupo abeliano H e para toda família de homomorfismos $\{f_k : A_k \to H; k \in K\}$,* *existir um único homomorfismo $\varphi : G \to H$ fazendo o seguinte diagrama comutar para todo $k \in K$ ($\varphi i_k = f_k$).*

$$\begin{tikzcd} G \arrow[dr, dashed, "\exists!\varphi"] & \\ A_k \arrow[u, "i_k"] \arrow[r, "f_k"'] & H \end{tikzcd}$$

Demonstração: Suponhamos que $G \cong \bigoplus_{k\in K} A_k$. Definamos $i_k : A_k \hookrightarrow G$ pela inclusão. Pela Proposição 1.2, cada $g \in G$ tem uma única expressão da forma $g = \sum_{k\in K} a_k$. Definamos $\varphi : G \to H$ por $\varphi(g) = \sum_{k\in K} f_k(a_k)$. Com isso, φ é um homomorfismo e faz o seguinte diagrama comutar para todo $k \in K$ ($\varphi i_k = f_k$).

$$\begin{tikzcd} G \arrow[dr, "\varphi"] & \\ A_k \arrow[u, hook, "i_k"] \arrow[r, "f_k"'] & H \end{tikzcd}$$

Supondo outra $\bar{\varphi}$ com a mesma propriedade ($\bar{\varphi} i_k = f_k$), temos que $\bar{\varphi} = \varphi$, já que $\bar{\varphi}(g) = \bar{\varphi}(\sum_{k\in K} a_k) = \sum_{k\in K} \bar{\varphi}(a_k) = \sum_{k\in K} \bar{\varphi}(i_k(a_k)) = \sum_{k\in K} f_k(a_k) = \varphi(g)$, para todo $g \in G$.

Agora, a recíproca. Consideremos o diagrama com $H = \bigoplus_{k\in K} A_k$ e $f_k = j_k$, onde $j_k : A_k \hookrightarrow \bigoplus_{k\in K} A_k$ é a inclusão. Por hipótese, existe um homomorfismo $\varphi : G \to \bigoplus_{k\in K} A_k$ fazendo este primeiro diagrama comutar. Analogamente, consideremos o diagrama substituindo G por $\bigoplus_{k\in K} A_k$, i_k por j_k, H por G e f_k por i_k. Por hipótese, existe um homomorfismo $\psi : \bigoplus_{k\in K} A_k \to G$ fazendo este segundo diagrama comutar. Vejamos o diagrama abaixo.

$$\begin{tikzcd} & \bigoplus_{k\in K} A_k \arrow[d, shift left, "\psi"] \\ A_k \arrow[ur, hook, "j_k"] \arrow[r, "i_k"'] & G \arrow[u, shift left, "\varphi"] \end{tikzcd}$$

Finalmente, mostremos que $\psi\varphi$ e $\varphi\psi$ são identidades. Como $\psi\varphi$ e 1_G fazem o seguinte digrama comutar para todo $k \in K$,

$$\begin{tikzcd} G \arrow[dr, "1_G"] & \\ A_k \arrow[u, "i_k"] \arrow[r, "i_k"'] & G, \end{tikzcd}$$

segue, pela hipótese de unicidade, que $\psi\varphi = 1_G$. Analogamente, segue que $\varphi\psi = 1_{\oplus_{k\in K} A_k}$.

■

1.1.2 Grupos Abelianos Livres

Definição 1.4. *Um grupo abeliano F é* **abeliano livre** *se é uma soma direta de grupos cíclicos infinitos. Mais precisamente, se existe um subconjunto $X \subset F$ de elementos de ordem infinita, chamada de* **base** *de F, com $F = \bigoplus_{x \in X} \langle x \rangle$.*

Admitimos a possibilidade $X = \varnothing$, o que resulta em $F = \{0\}$.

Proposição 1.5. *Se F é um grupo abeliano livre com base X, então cada elemento $u \in F$ tem uma única expressão da forma $u = \sum_{x \in X} m_x x$, onde $m_x \in \mathbb{Z}$ e $m_x \neq 0$ somente para um número finito de $x \in X$.*

Demonstração: Segue da Proposição 1.2.

■

Teorema 1.6. *Sejam F um grupo abeliano livre com base X, G um grupo abeliano arbitrário e $f : X \longrightarrow G$ uma função qualquer. Então, existe um único homomorfismo $\varphi : F \longrightarrow G$ estendendo f, ou seja, de maneira que o seguinte diagrama comute ($\varphi i = f$).*

$$\begin{tikzcd} F \arrow[dr, dashed, "\exists!\varphi"] & \\ X \arrow[u, hook, "i"] \arrow[r, "f"'] & G \end{tikzcd}$$

Demonstração: Se $u \in F$, então há uma única expressão $u = \sum_{x \in X} m_x x$. Definamos $f_x : \langle x \rangle \longrightarrow G$ por $f_x(mx) = mf(x)$. Temos que f_x é um homomorfismo, para todo $x \in X$. Como $\langle x \rangle \leq F$ e $F = \bigoplus_{x \in X} \langle x \rangle$, temos, pelo Teorema 1.3, o seguinte diagrama

$$\begin{tikzcd} F \arrow[dr, dashed, "\varphi"] & \\ \langle x \rangle \arrow[u, hook, "i_x"] \arrow[r, "f_x"'] & G, \end{tikzcd}$$

onde i_x é a aplicação inclusão. Assim, φ estende cada f_x e, portanto, estende f, já que $f(x) = f_x(x) = \varphi(i_x(x)) = \varphi(x)$, para todo $x \in X$.

■

Corolário 1.7. *Todo grupo abeliano G é isomorfo a um quociente de um grupo abeliano livre.*

Demonstração: Seja F a soma direta de $|G|$ cópias de $\mathbb{Z}$ e denotemos por x_g um gerador da g-ésima cópia de $\mathbb{Z}$, onde $g \in G$. Logo, $F = \bigoplus_{g \in G} \langle x_g \rangle$ e, portanto, F é um grupo abeliano livre com base $X = \{x_g; g \in G\}$. Consideremos a bijeção $f : X \longrightarrow G$ definida por $f(x_g) = g$. Assim, pelo Teorema 1.6, existe um homomorfismo $\varphi : F \longrightarrow G$ estendendo f. Como f é sobrejetiva, temos que φ também o é. Portanto, $G \cong F/Ker(\varphi)$.

■

Teorema 1.8. *Sejam $F = \bigoplus_{x \in X} \langle x \rangle$ e $G = \bigoplus_{y \in Y} \langle y \rangle$ grupos abelianos livres com bases X e Y, respectivamente. Então, $F \cong G$ se, e somente se, $|X| = |Y|$.*

Demonstração: Suponhamos que $F \cong G$. Se p é um primo, então não é difícil vermos que

$$V = F/pF = \{u + pF; u \in F\}$$

é um espaço vetorial sobre $\mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \ldots, \overline{p-1}\}$. Mostremos que $\overline{X} = \{x + pF; x \in X\}$ é uma base de V. Seja $v \in V$ qualquer. Logo, $v = u + pF$, para algum $u \in F$. Pela Proposição 1.5, existem inteiros m_x com $v = (\sum_{x \in X} m_x x) + pF$. Como pF é um subgrupo normal de F, segue que

$$v = \sum_{x \in X} (m_x x + pF) = \sum_{x \in X} m_x (x + pF).$$

Logo, $\overline{X}$ gera V. Falta mostrarmos que $\overline{X}$ é um conjunto linearmente independente. Assim, suponhamos que $\sum_{x \in X} \overline{m_x}(x + pF) = pF$, onde $\overline{m_x} \in \mathbb{Z}/p\mathbb{Z}$, para cada $x \in X$. Como m_x é um representante da classe $\overline{m_x}$, então $\sum_{x \in X} m_x(x + pF) = pF$ e, portanto, $\sum_{x \in X} m_x x \in pF$. Logo, existem inteiros n_x com $\sum_{x \in X} m_x x = \sum_{x \in X} p n_x x$. Pela unicidade da Proposição 1.5, segue que $m_x = p n_x$, para todo $x \in X$. Assim, temos que $\overline{m_x} = \overline{p n_x} = \overline{0}$, para todo $x \in X$. Logo, $\overline{X}$ é linearmente independente e, portanto, $\overline{X}$ é uma base de V. Daí, segue que $dim\ F/pF = |\overline{X}| = |X|$. Analogamente, temos que $dim\ G/pG = |Y|$. Como, por hipótese, $F \cong G$, então $|X| = dim\ F/pF = dim\ G/pG = |Y|$.

Agora, a recíproca. Como $|X| = |Y|$, existe uma bijeção $f : X \longrightarrow Y \subset G$, que podemos considerar $f : X \longrightarrow G$. Como F é abeliano livre com base X, existe um único homomorfismo $\varphi : F \longrightarrow G$ estendendo f. Analogamente, existe um único homomorfismo $\psi : G \longrightarrow F$ estendendo $f^{-1} : Y \longrightarrow X$. A composta $\psi\varphi : F \longrightarrow F$ é um homomorfismo que estende a função inclusão $i : X \hookrightarrow F$, pois $(\psi\varphi)(x) = \psi(\varphi(x)) = \psi(f(x)) = f^{-1}(f(x)) = x$, para todo $x \in X$. Mas, o homomorfismo identidade 1_F também estende i. Logo, pela unicidade da extensão, temos que $\psi\varphi = 1_F$. Da mesma forma, concluímos que $\varphi\psi = 1_G$ e, portanto, $\varphi : F \longrightarrow G$ é um isomorfismo.

■

Definição 1.9. *O* **posto** *de um grupo abeliano livre F é o número de elementos de uma base de F.*

O Teorema 1.8 diz que dois grupos abelianos livres são isomorfos se, e somente se, eles têm o mesmo posto.

Logo, o posto de um grupo abeliano livre F está bem definido, isto é, não depende da escolha da base de F.

Teorema 1.10 (Propriedade Projetiva). *Seja $\beta : B \to C$ um homomorfismo sobrejetor de grupos abelianos. Se F é um grupo abeliano livre e $\alpha : F \to C$ é um homomorfismo, então existe um homomorfismo $\gamma : F \to B$ fazendo o diagrama abaixo comutar ($\beta\gamma = \alpha$).*

$$\begin{tikzcd} & F \arrow[dl, dashed, "\gamma"'] \arrow[d, "\alpha"] & \\ B \arrow[r, "\beta"'] & C \arrow[r] & 0 \end{tikzcd}$$

Demonstração: Seja X uma base de F. Para cada $x \in X$, existe um elemento $b_x \in B$ com $\beta(b_x) = \alpha(x)$, pois $\alpha(x) \in C$ e β é sobrejetiva.

Portanto, temos a função $f : X \to B$ definida por $f(x) = b_x$. Pelo Teorema 1.6, existe um único homomorfismo $\gamma : F \to B$ com $\gamma(x) = b_x$, para todo $x \in X$. Assim, temos que $\beta\gamma(x) = \beta(b_x) = \alpha(x)$, para todo $x \in X$.

■

Corolário 1.11. *Sejam G um grupo abeliano e $H \leq G$. Se G/H é abeliano livre, então H é um somando direto de G, isto é, $G = H \oplus K$, onde $K \leq G$ e $K \cong G/H$.*

Demonstração: Sejam $F = G/H$ e $\beta : G \to F$ a projeção canônica. Consideremos o seguinte diagrama,

$$\begin{tikzcd} & F \arrow[dl, dashed, "\gamma"'] \arrow[d, "1_F"] & \\ G \arrow[r, "\beta"'] & F \arrow[r] & 0, \end{tikzcd}$$

onde 1_F é a aplicação identidade. Como F tem a propriedade projetiva, existe um homomorfismo $\gamma : F \to G$ com $\beta\gamma = 1_F$. Isso implica que γ é injetiva. Seja $K = Im(\gamma)$. Logo, temos que $F/Ker(\gamma) \cong K$ e, portanto, $F \cong K$.

Agora, como $H = Ker(\beta)$, mostremos que $G = H \oplus K$.

(i) $Ker(\beta) \cap K = \{0\}$: Seja $g \in Ker(\beta) \cap K$. Logo, $\beta(g) = 0$ e existe $x \in F$ tal que $\gamma(x) = g$. Daí, segue que $x = 1_F(x) = \beta(\gamma(x)) = \beta(g) = 0$. Portanto, $g = \gamma(0) = 0$, já que γ é um homomorfismo.

(ii) $G = Ker(\beta) + K$: Todo elemento de G pode ser escrito da forma

$$g = \underbrace{g - \gamma\beta(g)}_{\in Ker(\beta)} + \underbrace{\gamma\beta(g)}_{\in K}.$$

De (i) e (ii), segue que $G = H \oplus K$.

■

Teorema 1.12 ([9],Teorema 10.18)**.** *Todo subgrupo H de um grupo abeliano livre F é abeliano livre.*

1.1.3 Grupos Abelianos Finitamente Gerados

Daremos, agora, teoremas que caracterizam melhor os grupos abelianos finitamente gerados.

Definição 1.13. *Seja G um grupo abeliano. O* **subgrupo de torção** *de G é*

$$t(G) = \{g \in G \ ; \ ng = 0, \ \textit{para algum inteiro } n \textit{ diferente de zero}\}.$$

Definição 1.14. *Um grupo abeliano G é dito de* **torção** *se $t(G) = G$; e* **livre de torção** *se $t(G) = \{0\}$.*

Teorema 1.15. *O grupo quociente $G/t(G)$ é livre de torção e, portanto, todo grupo abeliano G é uma extensão de um grupo de torção por um grupo livre de torção.*

Demonstração: Seja $g + t(G) \in G/t(G)$. Suponhamos que, para algum inteiro $n \neq 0$, $n(g + t(G)) = t(G)$. Então, $ng \in t(G)$ e, portanto, existe um inteiro $m \neq 0$ tal que $m(ng) = 0$. Como $mn \neq 0$, temos que $g \in t(G)$ e, assim, $g + t(G) = t(G)$. Logo, $G/t(G)$ é livre de torção, já que a identidade é seu único elemento de ordem finita.

■

Teorema 1.16. *Todo grupo abeliano finito G é uma soma direta de grupos cíclicos finitos.*

Demonstração: Seja n o menor inteiro positivo tal que G pode ser gerado por um conjunto com n elementos. Dentre todos os conjuntos $\{x_1, \ldots, x_n\}$ de tamanho n que geram G, escolhamos o que contém um elemento x_1 de menor ordem e seja k esta ordem.

Agora, façamos indução sobre os geradores de G. Se $n = 1$, então $G = \langle x_1 \rangle$ e, portanto, $\langle x_1 \rangle$ é finito. Suponhamos que o teorema seja válido para os $n-1$ geradores de G. Assim, pela hipótese de indução, um subgrupo $H = \langle x_2, \ldots, x_n \rangle$ de G é uma soma direta de grupos cíclicos finitos. Mostremos que $G = \langle x_1 \rangle \oplus H$. Para isso, é suficiente mostrarmos que $\langle x_1 \rangle \cap H = \{0\}$, já que $\langle x_1 \rangle + H = \langle x_1, \ldots, x_n \rangle = G$.

Suponhamos, por absurdo, que $\langle x_1 \rangle \cap H \neq \{0\}$. Seja $z \in \langle x_1 \rangle \cap H$ com $z \neq 0$. Então, $z = a_1 x_1 = \sum_{i=2}^{n} a_i x_i$, onde $a_1, \ldots, a_n \in \mathbb{Z}$ e $0 < a_1 < k$. Agora, seja $d = \text{M.D.C.}\{a_1, \ldots, a_n\}$ e definamos $g = -(a_1/d)x_1 + \sum_{i=2}^{n}(a_i/d)x_i$. Primeiro, notemos o Lema 6.8 de [9], que diz que: "Se $G = \langle x_1, \ldots, x_n \rangle$ e $a_1, \ldots, a_n$ são inteiros co-primos, então existe um conjunto gerador de G com n elementos ao qual $\sum_{i=1}^{n} a_i x_i$ pertence". Assim, como $a_1/d, \ldots, a_n/d$ são co-primos, existe um conjunto gerador de G com n elementos ao qual g pertence. Logo, $g \neq 0$, pois, caso contrário, teríamos um conjunto gerador de G com $n-1$ elementos, o que seria um absurdo pela minimalidade de n. Além disso, segue que a ordem de g é menor do que k, pois $dg = 0$ e $d \leq a_1 < k$. Logo, g pertence a um conjunto de tamanho n que gera G, sendo sua ordem menor do que k. Isto é um absurdo pela minimalidade de k. Assim, temos que $\langle x_1 \rangle \cap H = \{0\}$ e, portanto, G é uma soma direta de grupos cíclicos finitos.

■

Teorema 1.17. *Todo grupo abeliano finitamente gerado livre de torção G é abeliano livre.*

Demonstração: Provemos por indução sobre n, onde $G = \langle x_1, \ldots, x_n \rangle$. Se $n = 1$ e $G \neq \{0\}$, então $G \cong \mathbb{Z}$ por ser livre de torção. Assim, G é abeliano livre. Agora, suponhamos que o teorema seja válido para todo grupo abeliano livre de torção com $n-1$ geradores.

Definamos $H = \{g \in G \ ; \ mg \in \langle x_n \rangle, \textit{ para algum inteiro positivo } m\}$. Afirmamos que H é um subgrupo de G e que G/H é livre de torção. Não é difícil vermos o primeiro fato. Já o segundo, é mais detalhado. Seja $x \in G$ tal que $k(x + H) = H$, para algum inteiro $k \neq 0$. Então, $kx \in H$, o que implica $m(kx) \in \langle x_n \rangle$, para algum inteiro positivo m. Assim, $x \in H$ e, portanto, $x + H = H$. Logo, G/H é livre de torção, já que a identidade é seu único elemento de ordem finita.

Como, $\forall z, m \in \mathbb{Z}$ $(m > 0)$, $zx_n \in G$ com $m(zx_n) = (mz)x_n \in \langle x_n \rangle$, então $zx_n \in H$. Logo, $G/H = \langle x_1 + H, \ldots, x_{n-1} + H \rangle$ e, portanto, G/H é um grupo abeliano livre de torção com $n-1$ geradores. Assim, pela hipótese de indução, G/H é abeliano livre.

Pelo Corolário 1.11, temos que $G = H \oplus F$, onde $F \cong G/H$. Assim, é suficiente provarmos que H é cíclico infinito, pois, caso seja, G vai satisfazer a Definição 1.4. Notemos que H é finitamente gerado, pois é um somando direto do grupo finitamente gerado G.

Se $g \in H - \{0\}$, então $mg = kx_n$, para alguns inteiros m e k diferentes de zero. Definamos $\varphi : H \to \mathbb{Q}$ por $\varphi(g) = k/m$. É fácil checarmos que φ define um homomorfismo injetor. Assim, H é isomorfo a um subgrupo finitamente gerado de $\mathbb{Q}$. Seja $H = \langle a_1/b_1, \ldots, a_t/b_t \rangle$. Se $b = \prod_{i=1}^{t} b_i$, então a aplicação $\psi : H \to \mathbb{Z}$, dada por $\psi(h) = bh$, é um monomorfismo. Logo, H é isomorfo a um subgrupo não-trivial de $\mathbb{Z}$ e, portanto, é cíclico infinito.

■

Teorema 1.18. *Todo grupo abeliano finitamente gerado G é uma soma direta de grupos cíclicos finitos e infinitos. Além disso, o número de somandos diretos de cada tipo depende somente de G.*

Demonstração: Pelo Teorema 1.17, temos que $G/t(G)$ é abeliano livre. Assim, pelo Corolário 1.11, temos que $G = t(G) \oplus F$, onde $F \cong G/t(G)$. Como $t(G)$ é abeliano finitamente gerado e todos os seus elementos têm ordem finita, segue que $t(G)$ é finito. Logo, pelo Teorema 1.16, temos que $t(G)$ é uma soma direta de grupos cíclicos finitos.

Como o número de cíclicos finitos depende da ordem de $t(G)$ e o número de cíclicos infinitos depende do posto de $G/t(G)$, segue que o número de somandos diretos de cada tipo depende somente de G.

■

Quando G não é finitamente gerado, o teorema acima pode ainda ser verdadeiro, como podemos ver na proposição abaixo.

Definição 1.19. *Seja G um grupo abeliano. Dizemos que G tem* **expoente finito** *se existir algum inteiro positivo n tal que $nG = \{0\}$, ou seja, n é um inteiro que anula todos os elementos de G.*

Proposição 1.20 ([9], Corolário 10.37)**.** *Se um grupo abeliano G tem expoente finito, então G é uma soma direta de grupos cíclicos finitos.*

1.2 Grupos Livres

Definição 1.21. *Sejam F um grupo e X um subconjunto de F. Dizemos que F é um* **grupo livre** *com base X se, para todo grupo G e para toda aplicação $f : X \longrightarrow G$, existir um único homomorfismo $\varphi : F \longrightarrow G$ estendendo f, ou seja, de maneira que o diagrama abaixo comute ($\varphi i = f$).*

$$\begin{tikzcd} F \arrow[dr, dashed, "\exists!\varphi"] & \\ X \arrow[u, hook, "i"] \arrow[r, "f"'] & G \end{tikzcd}$$

A definição acima é formal, abstrata e não nos permite garantir a existência nem mesmo conhecer a estrutura de um grupo livre. Por isso, faremos uma construção explícita de um grupo livre com base X, caracterizando-o a partir de seus elementos e de sua apresentação.

Mas, antes, precisamos garantir a existência de grupos livres. Faremos isto, provando que, dado um conjunto X, existe um grupo livre F cuja base é X.

Sejam X um conjunto e X^{-1} um conjunto disjunto de X, para os quais existe uma bijeção $X \longrightarrow X^{-1}$, definida por $x \longmapsto x^{-1}$. Chamemos os elementos de X de **símbolos**.

Definição 1.22. *a) Uma* **palavra** *sobre X é uma expressão da forma $w = x_1^{e_1}x_2^{e_2}\dots x_n^{e_n}$, onde todos os $x_i \in X$, todos os $e_i = \pm 1$ e $n \in \mathbb{N}$. A palavra que não contém nenhum símbolo é dita a* **palavra vazia** *e é denotada por 1;*

b) Duas palavras $w = x_1^{e_1}x_2^{e_2}\dots x_n^{e_n}$ e $u = y_1^{d_1}y_2^{d_2}\dots y_n^{d_n}$ sobre X são ditas **iguais** *se $x_i = y_i$ e $e_i = d_i$, para todo $i = 1, \dots, n$;*

c) O comprimento da palavra $w = x_1^{e_1}x_2^{e_2}\dots x_n^{e_n}$ é definido como sendo n e o comprimento da palavra vazia é definido como sendo zero;

d) Se $w = x_1^{e_1}x_2^{e_2}\dots x_n^{e_n}$ é uma palavra sobre X, então sua **inversa** *é a palavra $w^{-1} = x_n^{-e_n}\dots x_2^{-e_2}x_1^{-e_1}$.*

Notemos que, se o comprimento de uma palavra w é n, então sua inversa w^{-1} também tem comprimento n.

Definição 1.23. *Uma palavra w sobre X é dita* **reduzida** *se w ou é a palavra vazia ou é uma palavra que não contém nenhum par de símbolos consecutivos da forma xx^{-1} ou $x^{-1}x$.*

Exemplo 1.24. Seja $X = \{x_1, x_2, x_3\}$. A palavra $u = x_3x_1x_2^{-1}x_1$ é reduzida sobre X, enquanto a palavra $v = x_2x_3x_3^{-1}x_1$ não é reduzida sobre X.

A inversa de uma palavra reduzida é também reduzida.

Definição 1.25. *Uma* **subpalavra** *da palavra* $w = x_1^{e_1}x_2^{e_2}\ldots x_n^{e_n}$ *ou é a palavra vazia ou é uma palavra da forma* $v = x_i^{e_i}\ldots x_j^{e_j}$*, onde* $1 \leq i \leq j \leq n$*.*

Podemos definir uma multiplicação de palavras: se $w = x_1^{e_1}x_2^{e_2}\ldots x_n^{e_n}$ e $u = y_1^{d_1}y_2^{d_2}\ldots y_m^{d_m}$, então $wu = x_1^{e_1}x_2^{e_2}\ldots x_n^{e_n}y_1^{d_1}y_2^{d_2}\ldots y_m^{d_m}$. Agora, esta multiplicação não define um produto no conjunto de todas as palavras reduzidas sobre X, pois o produto wu não é necessariamente uma palavra reduzida sobre X. Mas, podemos definir uma nova multiplicação de palavras reduzidas w e u como sendo a palavra reduzida obtida de wu após todos os possíveis cancelamentos. Mais precisamente, se existe uma subpalavra (possivelmente vazia) v de w, com $w = w'v$, tal que v^{-1} é uma subpalavra de u, com $u = v^{-1}u'$, de tal maneira que $w'u'$ é reduzida, então definimos o produto wu como sendo

$$wu = w'u'.$$

Esta multiplicação é chamada de **justaposição**.

Exemplo 1.26. Se $w = x_2x_3x_1x_2^{-1}$ e $u = x_2x_1^{-1}x_2x_3x_3x_2$, então

$$wu = (x_2x_3x_1x_2^{-1})(x_2x_1^{-1}x_2x_3x_3x_2) =$$

$$= x_2x_3(x_1(x_2^{-1}x_2)x_1^{-1})x_2x_3x_3x_2 = x_2x_3x_2x_3x_3x_2.$$

Agora, estamos prontos para provar que, dado um conjunto X, existe um grupo livre cuja base é X. Para isto, vamos utilizar o truque de **Van der Waerden**, que consiste em mostrar que o conjunto F de todas as palavras reduzidas sobre X pode ser imerso, via isomorfismo, no grupo das permutações de F. E, assim, provaremos que F é um grupo com a operação de justaposição.

Teorema 1.27. *Dado um conjunto X, existe um grupo livre F cuja base é X.*

Demonstração: Seja F o conjunto de todas as palavras reduzidas sobre X. Para cada $x \in X$, consideremos as funções $|x| : F \longrightarrow F$ e $|x^{-1}| : F \longrightarrow F$, definidas como segue: para $e = \pm 1$,

$$|x^e|(x_1^{e_1}x_2^{e_2}\ldots x_n^{e_n}) = \begin{cases} x_2^{e_2}\ldots x_n^{e_n}, & \text{se} \quad x^e = x_1^{-e_1} \quad , \\ x^e x_1^{e_1}x_2^{e_2}\ldots x_n^{e_n}, & \text{se} \quad x^e \neq x_1^{-e_1} \quad . \end{cases}$$

Como, para cada $x \in X$, as compostas $|x| \circ |x^{-1}|$ e $|x^{-1}| \circ |x|$ são ambas iguais à função identidade $1_F : F \to F$, temos que $|x|$ é uma permutação de F cuja permutação inversa é $|x^{-1}|$. Sejam S_F o grupo das permutações de F e $\overline{F}$ o subgrupo de S_F gerado pelo conjunto $\overline{X} = \{|x| : x \in X\}$. Observemos que existe uma bijeção $\xi : \overline{X} \longrightarrow X$, dada por $|x| \longmapsto x$.

Afirmamos que $\overline{F}$ é um grupo livre com base $\overline{X}$.

Se $g \in \overline{F} - \{1_F\}$, então temos que g possui uma fatoração

$$g = |x_1^{e_1}| \circ |x_2^{e_2}| \circ \ldots \circ |x_n^{e_n}|, \tag{1.1}$$

onde $e_i = \pm 1$ e $|x_i^{e_i}|, |x_i^{-e_i}|$ nunca são adjacentes, pois, do contrário, poderíamos cancelá-los. Uma tal fatoração de g é única, pois $g(1) = x_1^{e_1} x_2^{e_2} \ldots x_n^{e_n}$ e já observamos que a ortografia de uma palavra (reduzida) é única.

Usemos a definição de grupos livres dada anteriormente para provarmos que $\overline{F}$ é um grupo livre com base $\overline{X}$. Assim, sejam G um grupo e $f : \overline{X} \longrightarrow G$ é um função qualquer. Já que a fatoração (1.1) é única, a função $\varphi : \overline{F} \longrightarrow G$, dada por

$$\varphi(|x_1^{e_1}| \circ |x_2^{e_2}| \circ \ldots \circ |x_n^{e_n}|) = f(|x_1|)^{e_1} f(|x_2|)^{e_2} \ldots f(|x_n|)^{e_n},$$

está bem definida e estende f. Como $\overline{X}$ gera $\overline{F}$, basta mostrarmos que φ é um homomorfismo, pois, para provarmos que φ é único, basta observarmos que dois homomorfismos coincidindo sobre um mesmo conjunto gerador devem ser iguais.

Sejam w e u palavras reduzidas sobre $\overline{X}$. É claro que $\varphi(w \circ u) = \varphi(w)\varphi(u)$, sempre que a palavra $w \circ u$ for reduzida sobre $\overline{X}$. Se a palavra $w \circ u$ não for reduzida sobre $\overline{X}$, escrevamos $w = w' \circ v$ e $u = v^{-1} \circ u'$, como na definição de justaposição, e teremos

$$\varphi(w \circ u) = \varphi((w' \circ v) \circ (v^{-1} \circ u')) = \varphi(w' \circ u') = \varphi(w')\varphi(u') =$$

$$= \varphi(w')\varphi(v)\varphi(v)^{-1}\varphi(u') = \varphi(w' \circ v)\varphi(v^{-1} \circ u') = \varphi(w)\varphi(u).$$

Então, de fato, φ é um homomorfismo. Até agora, mostramos que $\overline{F}$ é um grupo livre com base $\overline{X}$. Finalizando, consideremos a aplicação $\overline{\xi} : \overline{F} \longrightarrow F$, definida por

$$|x_1^{e_1}| \circ |x_2^{e_2}| \circ \ldots \circ |x_n^{e_n}| \longmapsto x_1^{e_1} x_2^{e_2} \ldots x_n^{e_n}.$$

Como $\overline{\xi}$ é uma bijeção com $\overline{\xi}(\overline{X}) = \xi(\overline{X}) = X$, podemos considerar F como um grupo isomorfo a $\overline{F}$ e, portanto, F é um grupo livre com base X.

■

Corolário 1.28. *Todo grupo G é isomorfo a um quociente de um grupo livre.*

Demonstração: Seja G um grupo qualquer e consideremos o conjunto $X = \{x_g; g \in G\}$. Assim, a aplicação $f : X \to G$, dada por $f(x_g) = g$, é uma bijeção. Pelo Teorema 1.27, existe um grupo livre F cuja base é X. Logo, existe um homomorfismo $\varphi : F \to G$ estendendo f. Como f é sobrejetiva, temos que φ também o é. Portanto, $G \cong F/Ker(\varphi)$.

■

Proposição 1.29. *Se F é um grupo livre com base X, então F é gerado por X.*

Demonstração: Seja $H = \langle X \rangle = \cap\{K \leq F; K \supseteq X\}$ e denotemos por $\theta : X \hookrightarrow H$ a inclusão, sendo $\theta^{'} : F \to H$ sua correspondente extensão. Denotando por $i : H \hookrightarrow F$ a inclusão, vemos no diagrama abaixo

$$\begin{tikzcd}
F \arrow[dr, dashed, "\theta'"] & & \\
X \arrow[u, hook, "inc"] \arrow[r, hook, "\theta"'] & H \arrow[r, hook, "i"'] & F
\end{tikzcd}$$

que $i\theta^{'}$ estende $i\theta = inc$. Mas, a aplicação identidade 1_F também estende $i\theta = inc$. Assim, pela unicidade da extensão, temos que $i\theta^{'} = 1_F$. Logo, $F = Im\ 1_F = Im\ i\theta^{'} = Im\ \theta^{'} \subseteq H$. Como, por definição, $H \subseteq F$, segue que $H = F$ e, portanto, F é gerado por X.

■

Agora, podemos definir o que é uma **apresentação** de um grupo.

Definição 1.30. *Sejam X um conjunto e Δ uma família de palavras sobre X. Um grupo G tem* **geradores** *X e* **relações** *Δ se $G \cong F/R$, onde F é o grupo livre com base X e R é o subgrupo normal de F gerado por Δ (também conhecido como fecho normal de Δ em F). O par ordenado $\langle X|\Delta\rangle$ é chamado uma* **apresentação** *de G.*

Exemplo 1.31. O grupo cíclico de ordem 4, $C_4 = \{1, x, x^2, x^3\}$, pode ser visto como o quociente entre o grupo livre sobre um gerador $\langle x \rangle$ e o subgrupo normal gerado por x^4. Logo, $C_4 \cong \langle x \rangle / \langle x^4 \rangle$ e, portanto, uma apresentação de C_4 é $\langle x | x^4 \rangle$.

Assim, as relações de um grupo G são as palavras obtidas a partir dos geradores de G que determinam, não trivialmente, a identidade de G. As relações da forma xx^{-1} ou $x^{-1}x$ são ditas **relações triviais**.

Exemplo 1.32. Um grupo livre é um grupo que tem uma apresentação da forma $\langle X|\varnothing\rangle$, ou seja, ele não possui relações (não triviais).

Duas consequências imediatas são:

(i) Um grupo livre é livre de torção, ou seja, ele não possui elementos de ordem finita;

(ii) Os geradores de um grupo livre não comutam. Logo, se F é um grupo livre com base X, então o centro $\mathbf{Z}(F)$ de F é não trivial se, e somente se, $|X| = 1$.

Já provamos que grupos livres existem. No próximo teorema, vamos provar que eles são únicos, ou seja, vamos fornecer uma condição necessária e suficiente para decidirmos quando é que dois grupos livres são isomorfos. Mas, antes, notemos a seguinte observação:

Observação 1.33. *Sejam F e G grupos quaisquer, $X \subseteq F$, $Hom(F,G)$ o conjunto dos homomorfismos de F em G, $Map(X,G)$ o conjunto das aplicações de X em G e*

$$\begin{array}{rcl} \rho : Hom(F,G) & \longrightarrow & Map(X,G) \\ (F \xrightarrow{\phi} G) & \longmapsto & (X \overset{i}{\hookrightarrow} F \xrightarrow{\phi} G) \end{array}$$

a função restrição. Então, temos que:

$$\begin{array}{rcl} \rho \text{ é sobrejetiva} & \Longleftrightarrow & \forall \theta \in Map(X,G),\ \exists \bar{\theta} \in Hom(F,G)\ ;\ \bar{\theta}|_X = \bar{\theta} \circ i = \theta; \\ \rho \text{ é injetiva} & \Longleftrightarrow & \bar{\theta} \in Hom(F,G),\ \text{se existir},\ \text{é único}. \end{array}$$

Assim, F é um grupo livre com base X se, e somente se, ρ é uma bijeção para qualquer grupo G.

Teorema 1.34. *Sejam F_1 e F_2 grupos livres com bases X_1 e X_2, respectivamente. Então, $F_1 \cong F_2$ se, e somente se, $|X_1| = |X_2|$.*

Demonstração: Primeiro, suponhamos que $F_1 \cong F_2$. Consideremos as funções

$$\begin{array}{rcl} \rho_1 : Hom(F_1, C_2) & \longrightarrow & Map(X_1, C_2) \\ (F_1 \xrightarrow{\phi} C_2) & \longmapsto & (X_1 \overset{i_1}{\hookrightarrow} F_1 \xrightarrow{\phi} C_2) \end{array} \qquad \text{e}$$

$$\begin{array}{rcl} \rho_2 : Hom(F_2, C_2) & \longrightarrow & Map(X_2, C_2) \\ (F_2 \xrightarrow{\theta} C_2) & \longmapsto & (X_2 \overset{i_2}{\hookrightarrow} F_2 \xrightarrow{\theta} C_2) \end{array} \qquad ,$$

onde C_2 é o grupo cíclico de ordem 2. Como F_1 é livre em X_1 e F_2 é livre em X_2, então, pela Observação 1.33, ρ_1 e ρ_2 são bijeções. Como $F_1 \cong F_2$, temos que $|Hom(F_1, C_2)| = |Hom(F_2, C_2)|$ e, portanto, $|Map(X_1, C_2)| = |Map(X_2, C_2)|$. Mas, $|Map(B, C)| = c^b$, para quaisquer conjuntos B e C de cardinalidades b e c, respectivamente. Assim, $2^{|X_1|} = 2^{|X_2|}$ e, portanto, $|X_1| = |X_2|$.

Agora, suponhamos que $|X_1| = |X_2|$, sendo $k : X_1 \to X_2$ uma bijeção entre X_1 e X_2. Sejam α e β as extensões dadas pelos seguintes diagramas:

$$\begin{tikzcd} & F_1 \arrow[dr, dashed, "\alpha"] & \\ X_1 \arrow[ur, hook, "i_1"] \arrow[r, "k"'] & X_2 \arrow[r, hook, "i_2"'] & F_2 \end{tikzcd}$$

$$\begin{tikzcd} & F_2 \arrow[dr, dashed, "\beta"] & \\ X_2 \arrow[ur, hook, "i_2"] \arrow[r, "k^{-1}"'] & X_1 \arrow[r, hook, "i_1"'] & F_1. \end{tikzcd}$$

Agora, para todo $x_1 \in X_1$, temos que

$$(\beta \circ \alpha)(x_1) = \beta(\alpha(x_1)) = \beta(k(x_1)) = k^{-1}(k(x_1)) = x_1 = i_1(x_1).$$

Portanto, $\beta \circ \alpha : F_1 \to F_1$ estende $i_1 : X_1 \hookrightarrow F_1$. Mas, a aplicação identidade 1_{F_1} também estende $i_1 : X_1 \hookrightarrow F_1$. Assim, pela unicidade da extensão, segue que $\beta \circ \alpha = 1_{F_1}$. Analogamente, segue que $\alpha \circ \beta = 1_{F_2}$. Logo, α é um isomorfismo e, portanto, $F_1 \cong F_2$.

■

O Teorema 1.34, que acabamos de demonstrar, nos permite dar a seguinte definição:

Definição 1.35. *O* **posto** *de um grupo livre F é o número de elementos de uma base de F.*

Logo, o Teorema 1.34 estabelece que o posto de um grupo livre F está bem definido, isto é, não depende da escolha da base de F.

Mais adiante, através do teorema de **Nielsen-Schreier**, provaremos que todo subgrupo de um grupo livre é também livre.

1.3 Produto Livre

Definiremos, nesta seção, o conceito de produto livre de grupos como sendo uma solução para que um certo diagrama comute, assim como definimos no caso de grupos livres. Veremos que um grupo livre é o produto livre de grupos cíclicos infinitos e, por isso, consideraremos o conceito de produto livre como uma generalização do conceito de grupo livre. Uma vez estabelecidas a existência e a unicidade de produtos livres, daremos uma descrição concreta destes grupos em termos de seus elementos e de suas apresentações.

Definição 1.36. *Seja* $\{A_i; i \in I\}$ *uma família de grupos, onde* I *é um conjunto qualquer de índices. Um* **produto livre** *dos* A_i *é um grupo* P *e uma família de homomorfismos* $j_i : A_i \longrightarrow P$ *tais que, para todo grupo* G *e para toda família de homomorfismos* $f_i : A_i \longrightarrow G$*, existe um único homomorfismo* $\varphi : P \longrightarrow G$ *de maneira que o diagrama abaixo comute para todo* $i \in I$ $(\varphi j_i = f_i)$*.*

$$\begin{tikzcd} P \arrow[dr, dashed, "\exists!\varphi"] & \\ A_i \arrow[u, "j_i"] \arrow[r, "f_i"'] & G \end{tikzcd}$$

Lema 1.37. *Se* P *é um produto livre de* $\{A_i; i \in I\}$*, então os homomorfismos* j_i *são injetivos.*

Demonstração: Para um índice $i \in I$ fixado, consideremos o diagrama em que $G = A_i$, f_i é o homomorfismo identidade e, para $k \neq i$, as aplicações $f_k : A_k \longrightarrow A_i$ são triviais.

$$\begin{tikzcd} P \arrow[dr, dashed, "\exists!\varphi"] & \\ A_i \arrow[u, "j_i"] \arrow[r, "1_{A_i}"'] & A_i \end{tikzcd}$$

Assim, temos que $\varphi j_i = 1_{A_i}$ e, portanto, o homomorfismo j_i é injetor.

■

Por causa deste lema, as aplicações $j_i : A_i \longrightarrow P$ são chamadas de **imersões**.

Proposição 1.38. *Assumamos que os conjuntos* $\{X_i; i \in I\}$ *sejam dois a dois disjuntos. Se* F_i *é o grupo livre com base* X_i*, então* $F = *_{i \in I} F_i$ *é o grupo livre com base* $\bigcup_{i \in I} X_i$*.*

Demonstração: Provemos que, dados um grupo G e uma função $f : \bigcup_{i\in I} X_i \longrightarrow G$, existe um único homomorfismo $\varphi : F \longrightarrow G$ estendendo f, ou seja, $\varphi|_{\cup_{i\in I} X_i} = f$. Para isso, consideremos funções $f_i : X_i \longrightarrow G$, definidas por $f_i = f|_{X_i}$. Como F_i é o grupo livre com base X_i, existe um único homomorfismo $\varphi_i : F_i \longrightarrow G$ satisfazendo $\varphi_i|_{X_i} = f_i$. Então, o homomorfismo $\varphi : F \longrightarrow G$, definido por $\varphi|_{F_i} = \varphi_i$, está unicamente determinado pelos já únicos homomorfismos φ_i. Logo, $\varphi|_{\cup_{i\in I} X_i} = f$ e, assim, F é o grupo livre com base $\bigcup_{i\in I} X_i$.

■

Exemplo 1.39. Um grupo livre F é um produto livre de grupos cíclicos infinitos. De fato, se X é uma base para o grupo livre F, então $\langle x\rangle$ é um grupo cíclico infinito, para cada $x \in X$. Definamos $j_x : \langle x\rangle \hookrightarrow F$ como sendo o homomorfismo inclusão. Se G é um grupo qualquer, então uma função $f : X \to G$ determina uma família de homomorfismos $f_x : \langle x\rangle \to G$, a saber, $x^n \mapsto f(x)^n$. Agora, pela definição de grupo livre, existe um único homomorfismo $\varphi : F \to G$ estendendo a função f. Então, é claro que φ estende cada homomorfismo f_x, já que $\varphi j_x = f_x$, para todo $x \in X$. Logo, F é um produto livre de $\{\langle x\rangle; x \in X\}$.

Agora, demonstremos que um produto livre de uma família qualquer de grupos é, a menos de isomorfismo, único.

Teorema 1.40. *Seja $\{A_i; i \in I\}$ uma família de grupos. Se P e Q são, cada um deles, um produto livre dos A_i, então $P \cong Q$.*

Demonstração: Sejam $j_i : A_i \longrightarrow P$ e $k_i : A_i \longrightarrow Q$ as imersões. Como P é um produto livre dos A_i, existe um homomorfismo $\varphi : P \longrightarrow Q$ satisfazendo $\varphi j_i = k_i$, para todo $i \in I$. Analogamente, existe um homomorfismo $\psi : Q \longrightarrow P$ com $\psi k_i = j_i$, para todo $i \in I$.

$$\begin{tikzcd} & P \arrow[d, shift left, "\varphi"] \\ A_i \arrow[ur, "j_i"] \arrow[r, "k_i"'] & Q \arrow[u, shift left, "\psi"] \end{tikzcd}$$

Assim, vemos que

$$j_i = \psi k_i = \psi(\varphi j_i) = (\psi\varphi) j_i$$

e também que

$$k_i = \varphi j_i = \varphi(\psi k_i) = (\varphi\psi) k_i.$$

Logo, por unicidade, $\psi\varphi = 1_P$ e $\varphi\psi = 1_Q$ e, portanto, $\varphi : P \longrightarrow Q$ é um isomorfismo. ■

Pelo Teorema 1.40, podemos nos referir *ao* produto livre P de $\{A_i; i \in I\}$. Vamos denotá-lo por

$$P = *_{i\in I} A_i.$$

Se existir um número finito de grupos A_i, então denotaremos o produto livre por

$$P = A_1 * \ldots * A_n.$$

Agora, tratemos da existência de produtos livres.

Teorema 1.41. *Dada uma família $\{A_i; i \in I\}$ de grupos, o produto livre $P = *_{i\in I} A_i$ existe.*

Demonstração: A prova é similar à prova da existência de grupos livres.

Seja $\{A_i; i \in I\}$ uma família de grupos. Suponhamos que os conjuntos $A_i^{\#} = A_i - \{1\}$ sejam dois a dois disjuntos. Chamemos $\bigcup_{i\in I} A_i^{\#} \cup \{1\}$ o *alfabeto*, chamemos seus elementos de *letras*, que formam *palavras* $w = a_1 a_2 \ldots a_n$, onde cada a_i está em algum A_i. Uma palavra w é *reduzida* se ou $w = 1$ ou $w = a_1 a_2 \ldots a_n$, onde cada letra $a_j \in A_{i_j}^{\#}$ e letras adjacentes estão em distintos $A_i^{\#}$.

Seja P o conjunto de todas as palavras reduzidas sobre $\bigcup_{i\in I} A_i^{\#} \cup \{1\}$ e consideremos a operação de *justaposição* sobre os elementos de P da seguinte maneira: assumamos que as palavras $w = a_1 \ldots a_n$ e $v = b_1 \ldots b_m$ sejam reduzidas. Se a_n e b_1 pertencem a distintos $A_i^{\#}$, definimos

$$wv = a_1 \ldots a_n b_1 \ldots b_m,$$

pois o lado direito da equação acima é uma palavra reduzida. Se a_n e b_1 pertencem ao mesmo $A_i^{\#}$ com $a_n b_1 \neq 1$, definimos

$$wv = a_1 \ldots a_n b_1 \ldots b_m,$$

pois, de novo, esta é uma palavra reduzida. Se a_n e b_1 pertencem ao mesmo $A_i^{\#}$ com $a_n b_1 = 1$, então cancelamos o fator $a_n b_1$ e repetimos o processo para as palavras $w' = a_1 \ldots a_{n-1}$ e $v' = b_2 \ldots b_m$. Como o comprimento de uma palavra reduzida é finito, temos que o processo termina com uma palavra reduzida, que será justamente o resultado da multiplicação wv. Claramente, 1 é a identidade de P e a inversa de uma palavra reduzida é também reduzida. Para verificação da associatividade, basta usarmos o truque de *Van der Waerden* como foi feito antes para grupos livres e, desta forma, está provado o teorema.

■

Teorema 1.42 (Forma normal). *Se $g \in *_{i\in I}A_i$ e $g \neq 1$, então g tem uma fatoração única*

$$g = a_1 a_2 \dots a_n,$$

onde os fatores adjacentes estão em diferentes $A_i^{\#}$.

Demonstração: Na construção do produto livre feita acima, definimos seus elementos como palavras reduzidas que, naturalmente, já têm a forma supracitada.

■

Assim, já temos uma descrição completa dos elementos do produto livre $*_{i\in I}A_i$ dos grupos A_i. Fornecemos, agora, uma descrição do produto livre a partir de uma apresentação.

Teorema 1.43. *Seja $\{A_i; i \in I\}$ uma família qualquer de grupos cujas apresentações são, respectivamente, $\langle X_i \mid \Delta_i \rangle$, onde os conjuntos X_i são dois a dois disjuntos. Então, uma apresentação de $*_{i\in I}A_i$ é $\langle \bigcup_{i\in I} X_i \mid \bigcup_{i\in I} \Delta_i \rangle$.*

Demonstração: Pela Proposição 1.38, se F_i é o grupo livre com base X_i, então $F = *_{i\in I}F_i$ é o grupo livre com base $\bigcup_{i\in I} X_i$. Logo, basta mostrarmos que $*_{i\in I}A_i \cong F/R$, onde R é o subgrupo normal de F gerado por $\bigcup_{i\in I} \Delta_i$. Pelo Corolário 1.28, temos que $A_i \cong F_i/R_i$, onde R_i é o subgrupo normal de F_i gerado pelas relações Δ_i. Logo, existem epimorfismos $\phi_i : F_i \longrightarrow A_i$ com $Ker(\phi_i) = R_i$. Portanto, pela definição de produto livre aplicada a F, deve existir um homomorfismo (sobrejetivo) $\varphi : F \longrightarrow *_{i\in I}A_i$ estendendo todos $F_i \xrightarrow[\phi_i]{} A_i \xhookrightarrow[\nu_i]{} *_{i\in I}A_i$ cujo núcleo é o subgrupo normal de F gerado por $\bigcup_{i\in I} \Delta_i$.

■

Já sabemos que todo grupo livre é um produto livre de grupos cíclicos infinitos. Agora, vejamos um exemplo interessante que mostra que nem todo produto livre é um grupo livre.

Exemplo 1.44. Sejam D_∞ o grupo diedral infinito e C_2 o grupo cíclico de ordem 2. Pelo Teorema 1.43, o produto livre $C_2 * C_2 \cong \langle x \mid x^2 \rangle * \langle y \mid y^2 \rangle = \langle x, y \mid x^2, y^2 \rangle = D_\infty$ não é livre.

1.4 Transformações de Tietze

Nesta seção, apresentaremos um método formal para passarmos de uma apresentação de um grupo para outra apresentação deste mesmo grupo: as **transformações de Tietze**. Mas, antes, notemos algumas definições.

Definição 1.45. *Sejam G um grupo qualquer e $\alpha : \{a, b, c, \cdots\} \longrightarrow G$ uma aplicação, com $\alpha(a) = g$, $\alpha(b) = h$, $\alpha(c) = k$, $\cdots$. Então, dizemos que (sob α) a define g, b define h, c define k, $\cdots$, a^{-1} define g^{-1}, b^{-1} define h^{-1}, c^{-1} define k^{-1}, $\cdots$.*

Além disso, se $w = x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ é uma palavra sobre o conjunto $\{a, b, c, \cdots\}$, então w define (sob α) o elemento de G dado por $g_1^{e_1} g_2^{e_2} \cdots g_n^{e_n}$, onde cada símbolo x_i define o elemento g_i de G.

A palavra vazia 1 define o elemento neutro 1 de G. Se as palavras u e v definem, respectivamente, os elementos p e q de G, então u^{-1} define p^{-1} e uv define pq.

Definição 1.46. *Se todo elemento de G pode ser definido (sob α) por alguma palavra sobre o conjunto $\{a, b, c, \cdots\}$, então dizemos que (sob α) a, b, c, $\cdots$ são* **símbolos geradores** *para G enquanto que g, h, k, $\cdots$ são os* **elementos geradores** *de G.*

Sabemos que uma **relação** de G é uma palavra que define o elemento neutro de G. Em qualquer grupo, a palavra vazia e as palavras xx^{-1}, $x^{-1}x$ sempre são relações, chamadas **relações triviais**.

Definição 1.47. *Sejam r e s palavras sobre um conjunto X qualquer. Então, dizemos que a equação $r = s$ é uma relação de G se a palavra rs^{-1} é uma relação de G ou, equivalentemente, se r e s definem o mesmo elemento de G.*

Definição 1.48. *Sejam $p, q, r, \cdots$ relações quaisquer do grupo G. Dizemos que uma palavra w é* **gerada** *a partir de $p, q, r, \cdots$ quando as seguintes operações, aplicadas um número finito de vezes, transformam w na palavra vazia:*

(i) Inserção de uma das relações $p, p^{-1}, q, q^{-1}, r, r^{-1}, \cdots$ ou de uma relação trivial entre quaisquer dois símbolos consecutivos de w, ou antes de w, ou depois de w;

(ii) Exclusão de uma das relações $p, p^{-1}, q, q^{-1}, r, r^{-1}, \cdots$ ou de uma relação trivial quando esta formar um bloco de símbolos consecutivos em w.

Dizemos que a equação $w = v$ é gerada a partir das relações $p_1 = p_2, q_1 = q_2, r_1 = r_2, \cdots$ se, e somente se, a palavra wv^{-1} é gerada a partir das relações $p_1p_2^{-1}, q_1q_2^{-1}, r_1r_2^{-1}, \cdots$.

É óbvio que se a palavra w é gerada a partir das relações $p, q, r, \cdots$, então w é também uma relação. De fato, como as operações (i) e (ii) aplicadas à palavra w não mudam o elemento do grupo definido pela mesma e a palavra vazia é alcançada, temos que w define o elemento neutro de G e, portanto, é uma relação de G.

Definição 1.49. *Se toda relação de* G *é gerada a partir das relações* $p, q, r, \cdots$*, então dizemos que* $\{p, q, r, \cdots\}$ *é um* **conjunto de relações definidoras** *ou* **um conjunto completo de relações** *para o grupo* G*.*

Um grupo G pode ter várias apresentações. De fato, dados um conjunto de elementos geradores de G e seus correspondentes símbolos geradores para G, existem muitas possíveis relações definidoras para G.

Por exemplo, seja S_3 o grupo das permutações de $\{1, 2, 3\}$. O 3-ciclo (123) e o 2-ciclo (12) formam um conjunto de elementos geradores de S_3. Sob a aplicação $a \longmapsto (123)$, $b \longmapsto (12)$, S_3 tem a apresentação

$$\langle a, b \mid a^3, b^2, ab = ba^2 \rangle. \tag{1.2}$$

S_3 também pode ser apresentado sob a mesma aplicação por

$$\langle a, b \mid a^3, b^2, ab = ba^{-1} \rangle. \tag{1.3}$$

De fato, como as relações em (1.2) são geradas a partir das relações de (1.3) e vice-versa, (1.2) e (1.3) definem a mesma *"equivalence class group"*. É menos óbvio que S_3 pode ser apresentado sob a mesma aplicação por

$$\langle a, b \mid ab^2a^2, a^2(b^2a^3)^4a, b^3a^4ba \rangle. \tag{1.4}$$

O leitor pode verificar que as relações em (1.4) são geradas a partir das de (1.2) e vice-versa.

Denotemos por $w(a, b, c, \cdots)$ uma palavra w sobre o conjunto $\{a, b, c, \cdots\}$.

Em geral, se G tem duas apresentações sob a mesma aplicação,

$$\langle a_1, a_2, \cdots \mid r_1(a_1, a_2, \cdots), r_2(a_1, a_2, \cdots), \cdots \rangle \tag{1.5}$$

e

$$\langle a_1, a_2, \cdots \mid s_1(a_1, a_2, \cdots), s_2(a_1, a_2, \cdots), \cdots \rangle, \tag{1.6}$$

então cada uma das relações de (1.6) é gerada a partir das relações de (1.5) e vice-versa.

Além disso, outras apresentações para G podem ser obtidas usando outros conjutos de relações definidoras para G.

Por exemplo, o grupo S_3 das permutações de $\{1, 2, 3\}$ é gerado pelos 2-ciclos (13) e (23). Sob a aplicação $c \longmapsto (13)$, $d \longmapsto (23)$, S_3 tem a apresentação

$$\langle c, d \mid c^2, d^2, (cd)^3 \rangle. \tag{1.7}$$

Existe algum método para mudar da apresentação (1.2) para (1.7)? Em 1908, *H. Tietze* mostrou em [12] que dada uma apresentação

$$\langle a, b, c, \cdots \mid p, q, r, \cdots \rangle \tag{1.8}$$

de um grupo G, qualquer outra apresentação de G pode ser obtida a partir de (1.8) por uma aplicação repetida das seguintes transformações:

($T1$) Se as palavras $s, t, \cdots$ são geradas a partir de $p, q, r, \cdots$, então adicione $s, t, \cdots$ às relações em (1.8);

($T2$) Se algumas das relações, digamos $s, t, \cdots$, listadas entre as relações $p, q, r, \cdots$ são geradas a partir das demais, então apague $s, t, \cdots$ das relações em (1.8);

($T3$) Se $u, v, \cdots$ são palavras quaisquer nos símbolos $a, b, c, \cdots$, então adicione os símbolos $x, y, \cdots$ aos símbolos geradores em (1.8) e adicione as relações $x = u, y = v, \cdots$ às relações em (1.8);

($T4$) Se algumas relações em (1.8) são da forma $x = u, y = v, \cdots$, onde $x, y, \cdots$ são geradores em (1.8) e $u, v, \cdots$ são palavras em outros geradores diferentes de $x, y, \cdots$, então apague $x, y, \cdots$ dos geradores, apague $x = u, y = v, \cdots$ das relações e substitua $x, y, \cdots$ por $u, v, \cdots$ (respectivamente) nas relações restantes em (1.8).

Definição 1.50. *As transformações* ($T1$), ($T2$), ($T3$) *e* ($T4$) *são chamadas* **transformações de Tietze**.

Definição 1.51. *Uma transformação de Tietze é dita* **elementar** *quando ela envolve a inserção ou exclusão de uma relação definidora ou quando ela envolve a inserção ou exclusão de um gerador e a correspondente relação definidora.*

As transformações de Tietze não mudam o grupo definido por uma apresentação. Suponhamos que (1.8) apresenta G sob a função

$$a \longmapsto g, \;\; b \longmapsto h, \;\; c \longmapsto k, \;\; \cdots . \tag{1.9}$$

Então, aplicando ($T1$) ou ($T2$) em (1.8), geramos uma apresentação para G sob a mesma função (1.9).

Aplicando $(T3)$ em (1.8), geramos uma apresentação para G sob a função (1.9) suplementada por

$$x \longmapsto u(g, h, k, \cdots), y \longmapsto v(g, h, k, \cdots), \cdots . \tag{1.10}$$

De fato, se $n(a, b, c, \cdots, x, y, \cdots)$ é uma relação em G sob a função determinada por (1.9) e (1.10), então usando as relações $x = u, y = v, \cdots$, a palavra n pode ser transformada em uma palavra que esteja somente nos símbolos $a, b, c, \cdots$, a qual é uma relação sob a função (1.9) e, portanto, pode ser gerada a partir de $p, q, r, \cdots$. Assim, $\{p, q, r, x = u, y = v, \cdots\}$ é um conjunto completo de relações para G sob (1.9) e (1.10).

Aplicando $(T4)$ em (1.8), geramos uma apresentação para G sob a restrição de (1.9) aos geradores de (1.8) restantes na nova apresentação. De fato, usando $(T3)$ para inserirmos os geradores excluídos e suas correspondentes relações definidoras, nós voltamos para (1.8) (depois de substituir $u, v, \cdots$ por $x, y, \cdots$ onde quer que seja necessário usando $(T1)$ e $(T2)$). Como $(T3)$ não muda o grupo definido por uma apresentação, então $(T4)$ também não muda.

Como um exemplo do uso das transformações de Tietze, mostremos que o grupo

$$\langle a, b, c \mid (ab)^2 ab^2 \rangle$$

é um grupo livre de posto 2. Para fazermos isto, introduzamos as novas relações ab e ab^2 por $(T3)$ e obtenhamos

$$\langle a, b, c, x, y \mid (ab)^2 ab^2, x = ab, y = ab^2 \rangle.$$

Depois, apliquemos $(T1)$ para obtermos

$$\langle a, b, c, x, y \mid (ab)^2 ab^2, x^2 y, x = ab, y = ab^2 \rangle$$

e, então, $(T2)$ para obtermos

$$\langle a, b, c, x, y \mid x^2 y, x = ab, y = ab^2 \rangle.$$

Agora, resolvamos para a e b e usemos $(T1)$ para obtermos

$$\langle a, b, c, x, y \mid x^2 y, x = ab, y = ab^2, b = x^{-1} y, a = x y^{-1} x \rangle.$$

Aplicando $(T4)$ para eliminarmos a e b, obtemos

$$\langle c, x, y \mid x^2 y, x = (x y^{-1} x)(x^{-1} y), y = (x y^{-1} x)(x^{-1} y)^2 \rangle,$$

que por $(T2)$ é

$$\langle c, x, y \mid x^2y \rangle.$$

Esta apresentação pode ser transformada por $(T1)$ e por $(T2)$ em

$$\langle c, x, y \mid y = x^{-2} \rangle$$

e, portanto, aplicando $(T4)$ novamente, obtemos a apresentação

$$\langle c, x \mid \varnothing \rangle,$$

ou seja, um grupo livre de posto 2.

Teorema 1.52. *Dadas duas apresentações para um grupo G,*

$$G = \langle a_1, a_2, \cdots \mid r_1(a_\nu), r_2(a_\nu), \cdots \rangle \tag{1.11}$$

e

$$G = \langle b_1, b_2, \cdots \mid s_1(b_\mu), s_2(b_\mu), \cdots \rangle, \tag{1.12}$$

então (1.12) *pode ser obtida a partir de* (1.11) *por uma aplicação repetida das transformações de Tietze* $(T1)$, $(T2)$, $(T3)$ *e* $(T4)$.

Demonstração: Seja (1.11) uma apresentação de G sob a aplicação

$$a_1 \longmapsto g_1, a_2 \longmapsto g_2, \cdots \tag{1.13}$$

e seja (1.12) uma apresentação de G sob a aplicação

$$b_1 \longmapsto h_1, b_2 \longmapsto h_2, \cdots . \tag{1.14}$$

Primeiro, devemos, através das transformações de Tietze, transformar (1.11) de modo que os símbolos $b_1, b_2, \cdots$ de (1.12) apareçam como símbolos geradores. Para este propósito, desejamos expressar $h_1, h_2, \cdots$ em termos dos $g_1, g_2, \cdots$. Como $g_1, g_2, \cdots$ formam um conjunto de elementos geradores de G, então

$$h_1 = \beta_1(g_1, g_2, \cdots), h_2 = \beta_2(g_1, g_2, \cdots), \cdots . \tag{1.15}$$

Assim, por $(T3)$, adicionemos os novos símbolos $b_1, b_2, \cdots$ aos símbolos geradores em (1.11) e adicionemos as correspondentes relações

$$b_1 = \beta_1(a_1, a_2, \cdots), b_2 = \beta_2(a_1, a_2, \cdots), \cdots \tag{1.16}$$

obtendo a apresentação

$$\langle a_1, a_2, \cdots, b_1, b_2, \cdots \mid r_1(a_\nu), r_2(a_\nu), \cdots, b_1 = \beta_1(a_\nu), b_2 = \beta_2(a_\nu), \cdots \rangle. \tag{1.17}$$

Além disso, G é apresentado por (1.17) sob a aplicação

$$a_1 \longmapsto g_1, a_2 \longmapsto g_2, \cdots, b_1 \longmapsto h_1, b_2 \longmapsto h_2, \cdots, \tag{1.18}$$

determinada por (1.13) e (1.14).

Agora, desejamos trazer as relações de (1.12) para (1.17). Para este propósito, notemos que

$$s_1(b_1, b_2, \cdots), s_2(b_1, b_2, \cdots), \cdots \tag{1.19}$$

são relações sob (1.18), já que são relações sob (1.14). Então, (1.19) pode ser unida às relações definidoras em (1.17) por $(T1)$, obtendo a apresentação

$$\langle a_1, a_2, \cdots, b_1, b_2, \cdots \mid r_1(a_\nu), r_2(a_\nu), \cdots, b_1 = \beta_1(a_\nu), b_2 = \beta_2(a_\nu), \cdots, s_1(b_\mu), s_2(b_\mu), \cdots \rangle, \tag{1.20}$$

a qual apresenta G sob (1.18).

Agora, desejamos expressar $a_1, a_2, \cdots$ em termos dos $b_1, b_2, \cdots$ de modo que nós possamos deletar $a_1, a_2, \cdots$ de (1.20). Para este propósito, expressemos $g_1, g_2, \cdots$ como palavras em $h_1, h_2, \cdots$. Como $h_1, h_2, \cdots$ formam um conjunto de elementos geradores de G, então

$$g_1 = \alpha_1(h_1, h_2, \cdots), g_2 = \alpha_2(h_1, h_2, \cdots), \cdots .$$

Logo, sob a aplicação (1.18),

$$a_1 = \alpha_1(b_1, b_2, \cdots), a_2 = \alpha_2(b_1, b_2, \cdots), \cdots \tag{1.21}$$

são relações em G e, portanto, são geradas a partir das relações em (1.20). Então, por $(T1)$, podemos unir as relações (1.21) às relações em (1.20), obtendo a apresentação

$$\begin{aligned} \langle a_1, a_2, \cdots, b_1, b_2, \cdots \quad \mid \quad & r_1(a_\nu), r_2(a_\nu), \cdots, b_1 = \beta_1(a_\nu), b_2 = \beta_2(a_\nu), \cdots, \\ & s_1(b_\mu), s_2(b_\mu), \cdots, a_1 = \alpha_1(b_\mu), a_2 = \alpha_2(b_\mu), \cdots \rangle. \end{aligned} \tag{1.22}$$

Em vez de deletarmos $a_1, a_2, \cdots$ como planejado, observemos que (1.22) é simétrica. Logo, podemos obter (1.22) a partir de (1.12) através das transformações de Tietze. Como a inversa de uma transformação de Tietze é uma sequência de transformações de Tietze, segue que (1.12) pode ser obtida a partir de (1.22) através de uma sequência de transformações de Tietze. Então, (1.12) pode ser obtida a partir de (1.11) por uma aplicação repetida das transformações de Tietze.

■

1.5 Processo de Reescrita de Reidemeister-Schreier

Nesta seção, iremos apresentar o **teorema de Nielsen-Schreier**, que afirma que todo subgrupo de um grupo livre é também livre, e o **processo de reescrita de Reidemeister-Schreier**, que é um método que fornece uma apresentação de um subgrupo quando uma apresentação do grupo é conhecida. Mas, antes, fixemos a notação que será usada e provemos alguns resultados necessários.

Sejam F um grupo livre com base X e W um subgrupo arbitrário de F. As classes laterais à direita de W em F serão rotuladas por meio de um conjunto de índices I contendo o símbolo 1,

$$\{W_i; i \in I\},$$

com a convenção de que $W_1 = W$.

Escolhamos um transversal à direita para W em F, no qual o representante da classe W_i seja escrito por

$$\overline{W_i},$$

com a convenção de que $\overline{W} = 1$.

Se $u \in F$, então os elementos $\overline{W_i}u$ e $\overline{W_iu}$ pertencem à mesma classe lateral à direita W_iu, ou seja,

$$\overline{W_i}u\overline{W_iu}^{-1} \in W.$$

A idéia por trás da demonstração do teorema de Nielsen-Schreier é encontrar um transversal à direita T para W em F tal que os elementos não-triviais $\overline{W_i}x\overline{W_ix}^{-1}$ constituam um conjunto de geradores livres de W, onde $x \in X$ e $i \in I$.

Com este objetivo em mente, para cada $i \in I$ e $x \in X$, associemos um símbolo y_{ix}, denotando por

$$\widehat{F}$$

o grupo livre sobre o conjunto de todos os y_{ix}. Pela definição de grupo livre, a aplicação $y_{ix} \longmapsto \overline{W_i}x\overline{W_ix}^{-1}$ determina um homomorfismo $\tau : \widehat{F} \longrightarrow W$. O primeiro passo é mostrar que τ é sobrejetiva.

Definição 1.53. *Para cada $u \in F$ e $i \in I$, associemos um elemento $u^{W_i} \in \widehat{F}$, referindo-se à aplicação $u \longmapsto u^{W_i}$ como uma **"coset map"**.*

Definição 1.54. *Definamos*

$$1^{W_i} = 1, \quad x^{W_i} = y_{ix} \quad e \quad (x^{-1})^{W_i} = (x^{W_i x^{-1}})^{-1},$$

se $x \in X$. Geralmente, se $u = vy$ na forma reduzida com $y \in X \cup X^{-1}$, então definamos u^{W_i} por indução sobre o comprimento de u por meio da equação

$$u^{W_i} = v^{W_i} y^{W_i v}.$$

É importante sabermos como uma **"coset map"** afeta produtos e inversos. Por isso, notemos a seguinte proposição:

Proposição 1.55. *Se $u, v \in F$, então $(uv)^{W_i} = u^{W_i} v^{W_i u}$ e $(u^{-1})^{W_i} = (u^{W_i u^{-1}})^{-1}$.*

Demonstração: Primeiro, consideremos a fórmula do produto. Ela certamente é válida se $v = 1$. Suponhamos , então, que $v \in X \cup X^{-1}$. Se o último símbolo de u não é v^{-1}, então a fórmula é verdadeira por definição. Caso contrário, segue que $u = u_1 v^{-1}$ na forma reduzida, com $uv = u_1$. Logo, $(uv)^{W_i} = {u_1}^{W_i}$. Mas, por definição, temos que $u^{W_i} = (u_1 v^{-1})^{W_i} = {u_1}^{W_i} (v^{-1})^{W_i u_1} = {u_1}^{W_i} (v^{W_i u_1 v^{-1}})^{-1} = {u_1}^{W_i} (v^{W_i u})^{-1}$. Assim, ${u_1}^{W_i} = u^{W_i} v^{W_i u}$, como queríamos.

Agora, assumamos que o comprimento de v (como uma palavra reduzida sobre X) exceda 1. Escrevamos $v = v_1 y$ na forma reduzida com $y \in X \cup X^{-1}$. Assim, por indução sobre o comprimento de v, temos que

$$(uv)^{W_i} = ((uv_1)y)^{W_i} = (uv_1)^{W_i} y^{W_i uv_1} = u^{W_i} (v_1^{W_i u}) y^{W_i uv_1} = u^{W_i} v^{W_i u}.$$

Para provarmos a fórmula $(u^{-1})^{W_i} = (u^{W_i u^{-1}})^{-1}$, basta aplicarmos a regra do produto a $u^{-1}u$, pois

$$1 = 1^{W_i} = (u^{-1}u)^{W_i} = (u^{-1})^{W_i} u^{W_i u^{-1}}.$$

■

Agora, computemos a composta de uma **"coset map"** com $\tau : \widehat{F} \longrightarrow W$.

Proposição 1.56. *Se $u \in F$ e $i \in I$, então $\tau(u^{W_i}) = \overline{W_i} u \overline{W_i u}^{-1}$*

Demonstração: Façamos indução sobre o comprimento de u. A equação é verdadeira se $u = 1$ ou $u \in X \cup X^{-1}$. Assim, escrevamos $u = u_1 u_2$, onde u_1 e u_2 tenham comprimento menor do que u. Então, pela regra do produto, segue que

$$\begin{aligned}
\tau(u^{W_i}) &= \tau((u_1u_2)^{W_i}) = \tau({u_1}^{W_i}{u_2}^{W_iu_1}) = \tau({u_1}^{W_i})\tau({u_2}^{W_iu_1}) \\
&= \overline{W_i}u_1\overline{W_iu_1}^{-1}\overline{W_iu_1}u_2\overline{W_iu_1u_2}^{-1} \\
&= \overline{W_i}u\overline{W_iu}^{-1},
\end{aligned}$$

como queríamos provar.

■

Agora, consideremos a restrição da **"coset map"** $u \longmapsto u^W$ ao subgrupo W. Vamos chamá-la de $\psi : W \longrightarrow \widehat{F}$.

Pela Proposição 1.55, segue que ψ é um homomorfismo, já que

$$\psi(uv) = (uv)^W = u^W v^{Wu} = u^W v^W = \psi(u)\psi(v)$$

sempre que $u, v \in W$. Já pela Proposição 1.56, temos que

$$(\tau \circ \psi)(u) = \tau(\psi(u)) = \tau(u^W) = \overline{W}u\overline{Wu}^{-1} = u,$$

visto que $\overline{W} = 1 = \overline{Wu}$ sempre que $u \in W$. Consequentemente,

$$\tau \circ \psi = 1_W.$$

Daí, segue que ψ é injetiva e τ é sobrejetiva. Portanto, τ é uma apresentação de W nos y_{ix}.

Agora, procuremos um conjunto de relações definidoras para τ, isto é, um subconjunto cujo fecho normal em $\widehat{F}$ seja igual a $Ker\ \tau$. Denotemos por

$$\chi = \psi \circ \tau$$

um endomorfismo de $\widehat{F}$.

Proposição 1.57. *O grupo W tem uma apresentação $\tau : \widehat{F} \longrightarrow W$ com geradores y_{ix} e relações definidoras $y_{ix}^{-1}\chi(y_{ix})$, onde $i \in I$ e $x \in X$.*

Demonstração: Sejam $K = Ker\ \tau$ e N o fecho normal em $\widehat{F}$ do conjunto de todos os $y_{ix}^{-1}\chi(y_{ix})$. Como ψ é injetiva, observemos que K é igual a $Ker\ \chi$, pois

$$\begin{aligned}
Ker\ \chi &= \{a \in \widehat{F}; \chi(a) = 1\} = \{a \in \widehat{F}; \psi(\tau(a)) = 1\} \\
&= \{a \in \widehat{F}; \tau(a) = 1\} = K.
\end{aligned}$$

Como $\tau \circ \psi = 1_W$, temos que $\chi^2 = (\psi \circ \tau) \circ (\psi \circ \tau) = \psi \circ (\tau \circ \psi) \circ \tau = \chi$. Isso mostra que $\chi(y_{ix}^{-1}\chi(y_{ix})) = 1$, já que χ é um homomorfismo. Logo, $y_{ix}^{-1}\chi(y_{ix}) \in K$ e, portanto, $N \subseteq K$. Reciprocamente, seja $k \in K$. Então, k pode ser escrito em termos dos y_{ix}. Como χ é um homomorfismo e $\chi(y_{ix}) \equiv y_{ix}$ *mod* N, segue que $\chi(k) \equiv k$ *mod* N. Logo, $k \in N$, já que $\chi(k) = 1$. Assim, $K \subseteq N$ e, portanto, $K = N$.

■

Agora, passemos para um conjunto mais econômico de relações associadas com os elementos do transversal.

Proposição 1.58. *Se u denota um elemento não-trivial do transversal, então os elementos u^W formam um conjunto de relações definidoras para a apresentação $\tau : \widehat{F} \longrightarrow W$.*

Demonstração: Sejam $K = Ker\ \tau = Ker\ \chi$ e N o fecho normal em $\widehat{F}$ do conjunto de todos os u^W. Se u é um elemento do transversal, segue, pela Proposição 1.56, que $\tau(u^W) = \overline{W}u\overline{Wu}^{-1} = uu^{-1} = 1$. Logo, $u^W \in K$ e, portanto, $N \subseteq K$. Pela demonstração da Proposição 1.57, para provarmos a outra inclusão, basta mostrarmos que $\chi(y_{ix}) \equiv y_{ix}$ *mod* N. Usando as Proposições 1.55 e 1.56, temos que

$$\chi(y_{ix}) = \psi(\tau(y_{ix})) = (\tau(y_{ix}))^W = (\overline{W_i}x\overline{W_i x}^{-1})^W = \overline{W_i}^W x^{W\overline{W_i}}(\overline{W_i x}^{-1})^{W\overline{W_i}x}.$$

Como $W\overline{W_i} = W_i$ e, pela Proposição 1.55, $(\overline{W_i x}^{-1})^{W\overline{W_i}x} = (\overline{W_i x}^W)^{-1}$, segue que

$$\chi(y_{ix}) = \overline{W_i}^W x^{W_i}(\overline{W_i x}^W)^{-1} \equiv y_{ix}\ mod\ N,$$

já que $x^{W_i} = y_{ix}$ e todos os u^W estão em N. Assim, $K \subseteq N$ e, portanto, $K = N$.

■

Até agora, nós temos construído uma apresentação de W para cada transversal à direita. Chegou a hora de fazermos uma escolha especial de transversal, o qual irá fornecer uma apresentação de W, tornando clara a estrutura deste subgrupo. Mas, antes, notemos algumas definições.

Definição 1.59. *Dizemos que um subconjunto S de F tem a* **propriedade de Schreier** *quando $v \in S$ sempre que $vy \in S$. Aqui, $y \in X \cup X^{-1}$ e vy está na forma reduzida. Assim, S contém todas as partes iniciais de seus elementos.*

Definição 1.60. *Um* **transversal de Schreier** *para W em F é um transversal para W em F com a propriedade de Schreier.*

O que nós precisamos é de um transversal de Schreier para W em F. Porém, não é óbvio que um tal transversal existe. Portanto, isto deve ser estabelecido primeiramente.

Teorema 1.61. *Existe um transversal de Schreier para W em F.*

Demonstração: Definamos o comprimento de uma classe lateral à direita de W em F como sendo o menor comprimento de uma palavra nessa classe. A única classe de comprimento zero é W. À ela, o representante 1 é associado. Seja W_i uma classe de comprimento $l > 0$ e assumamos que representantes têm sido associados à todas as classes de comprimento menor do que l, nas quais a propriedade de Schreier é válida. Logo, existe um elemento u de comprimento l em W_i. Escrevamos $u = vy$, onde $y \in X \cup X^{-1}$ e v tem comprimento $l - 1$. Então, $\overline{Wv}$ já tem sido associado. Definimos $\overline{W_i}$ como sendo $\overline{Wv}y$, observando que as partes iniciais deste $\overline{W_i}$ estão no transversal. Assim, um transversal de Schreier pode ser construído.

■

Agora, o teorema de Nielsen-Schreier pode ser provado. Mas, antes, notemos a seguinte observação:

Observação 1.62. *Se F é o grupo livre com base X e $\varnothing \neq Y \subset X$, então $F/\langle Y^F\rangle$ é livre com base $X\backslash Y = \{x \in X; x \notin Y\}$, onde $\langle Y^F\rangle$ denota o fecho normal de Y em F.*

Demonstração: Seja L o grupo livre com base $X\backslash Y$. Mostremos que $L \cong F/\langle Y^F\rangle$. Pela Definição 1.21, dada a função $f : X\backslash Y \longrightarrow F/\langle Y^F\rangle$, definida por $f(x) = x\langle Y^F\rangle$, existe um único homomorfismo $\varphi : L \longrightarrow F/\langle Y^F\rangle$ tal que $\varphi(x) = f(x)$, para todo $x \in X\backslash Y$, ou seja, de maneira que o diagrama abaixo comute ($\varphi i = f$).

$$\begin{tikzcd}
L \arrow[dr, dashed, "\varphi"] & \\
X\backslash Y \arrow[u, hook, "i"] \arrow[r, "f"'] & F/\langle Y^F\rangle
\end{tikzcd}$$

Como $Ker\ \varphi = \{u \in L; u\langle Y^F\rangle = \langle Y^F\rangle\} = \{u \in L; u \in \langle Y^F\rangle\} = L \cap \langle Y^F\rangle = \{1_L\}$, segue que φ é injetiva. Seja $v \in F/\langle Y^F\rangle$. Assim, $v = x_1^{e_1} \dots x_n^{e_n}\langle Y^F\rangle$, para alguma palavra reduzida $x_1^{e_1} \dots x_n^{e_n} \in F$. Como $y\langle Y^F\rangle = \langle Y^F\rangle$, $\forall y \in Y$, segue que $v = \varphi(x_i^{e_i} \dots x_j^{e_j})$, onde $x_i^{e_i} \dots x_j^{e_j} \in L$ com $1 \leq i \leq j \leq n$. Logo, φ é sobrejetiva e, portanto, φ é um isomorfismo. ■

Teorema 1.63 (O teorema de Nielsen-Schreier). *Se W é um subgrupo de um grupo livre F, então W é um grupo livre. Além disso, se W tem índice finito m em F, o posto de W é precisamente $nm + 1 - m$, onde n é o posto de F (o qual pode ser infinito).*

Demonstração: Escolhamos um transversal de Schreier para W em F. Como de costume, escrevamos $K = Ker\ \tau = Ker\ \chi$. Sabemos, a partir da Proposição 1.58, que K é o fecho normal em $\widehat{F}$ dos u^W, onde u é um elemento não-trivial do transversal. Escrevamos $u = vx^e$, onde $x \in X$, $e = \pm 1$ e v tem comprimento menor que u. Então, $u^W = v^W (x^e)^{Wv}$. Agora, $x^{Wv} = y_{ix}$, onde $W_i = Wv$. Além disso, $(x^{-1})^{Wv} = y_{jx}^{-1}$, onde $W_j = Wvx^{-1}$. Portanto,

$$u^W = v^W y_{kx}^e, \tag{1.23}$$

para algum $k \in I$. Agora, pela propriedade de Schreier, v pertence ao transversal. Então, assim como u^W está em K, v^W também está. Portanto, $y_{kx} \in K$. Daí, segue de (1.23) que cada u^W pode ser escrito em termos de certos y_{kx}, os quais pertencem a K.

Nós concluimos a partir do último parágrafo que K é o fecho normal em $\widehat{F}$ de certos geradores livres y_{kx}. Assim, pela Observação 1.62, segue que W é um grupo livre.

Agora, suponhamos que W tenha índice finito m em F. O posto de $\widehat{F}$ é nm. Se nós pudermos mostrar que exatamente $m - 1$ dos y_{ix}'s pertencem a K, então irá seguir que W tem posto igual a $nm - (m - 1) = nm + 1 - m$.

Em primeiro lugar, $y_{ix} \in K$ se, e somente se, $\overline{W_i}x = \overline{W_i x}$. Tomemos qualquer classe W_i diferente de W. Deletemos o símbolo final de $\overline{W_i}$ (na forma reduzida) para obtermos um outro elemento do transversal, digamos $\overline{W_j}$. Então, $\overline{W_i} = \overline{W_j}x^e$ e $W_i = W_j x^e$, para algum $x \in X$ e $e = \pm 1$. Se $e = 1$, então $\overline{W_j}x\overline{W_j x}^{-1} = 1$ e $y_{jx} \in K$. Se $e = -1$, então $\overline{W_i}x\overline{W_i x}^{-1} = 1$ e $y_{ix} \in K$. Assim, cada uma das $m - 1$ classes $W_i \neq W$ fornece um y_{ix} em K. Claramente, todos esses y_{ix} são distintos. Reciprocamente, seja $y_{ix} \in K$, ou seja, $\overline{W_i}x = \overline{W_i x}$. Seja $W_j = W_i x$. Então, ou $W_i \neq W$ ou $W_j \neq W$. Portanto, y_{ix} aparece a partir ou de W_i ou de W_j. Assim, todos os y_{ix} em K são obtidos dessa maneira: eles são exatamente $m - 1$ em quantidade.

■

Agora, apresentemos o processo de reescrita de Reidemeister-Schreier, que é um método que fornece uma apresentação de um subgrupo quando uma apresentação do grupo é conhecida.

Teorema 1.64 (Reidemeister-Schreier). *Sejam G um grupo e H um subgrupo de G. Suponhamos que $\varphi : F \longrightarrow G$ seja uma apresentação de G com geradores X e relações S. Seja W a pré-imagem de H por φ. Então, com a notação acima, temos que:*

(i) $\varphi \circ \tau : \widehat{F} \longrightarrow H$ é uma apresentação de H com geradores y_{ix} e relações definidoras s^{W_i}, u^W, onde $i \in I$, $s \in S$ e u é um elemento não-trivial de um transversal para W em F;

(ii) Se $[G : H] = m < \infty$ e G é um grupo n-gerado, então H pode ser gerado por $nm+1-m$ elementos.

Demonstração: (i) Claramente, $Ker\ (\varphi \circ \tau)$ é igual a pré-imagem de $Ker\ \varphi$ por τ. Seja N o fecho normal em $\widehat{F}$ de todos os s^{W_i} e u^W. Seja $s \in S$. Como $S \subseteq Ker\ \varphi \leq W$, temos que $W_i s = W_i$, $\forall i \in I$. Portanto, $\tau(s^{W_i}) = \overline{W_i} s \overline{W_i}^{-1}$. Além disso, pela Proposição 1.58, $\tau(u^W) = 1$. Assim, $\tau(N)$ é o fecho normal em W de todos $\overline{W_i} s \overline{W_i}^{-1}$, o que implica que $\tau(N) = \langle S \rangle^F = Ker\ \varphi$. Portanto, $Ker\ (\varphi \circ \tau) = \tau^{-1}(Ker\ \varphi) = \tau^{-1}(\tau(N)) = N(Ker\ \tau) = N$.
(ii) Segue a partir do teorema de Nielsen-Schreier, já que $[F : W] = [G : H] = m$.

■

Agora, vejamos um exemplo deste processo, no qual fornecemos uma apresentação para o grupo alternado A_4 a partir de uma dada apresentação do grupo simétrico S_4.

Exemplo 1.65. Se denotarmos por x_i a transposição $(i\ i+1)$, para todo $1 \leq i \leq 3$, então o grupo simétrico S_4 tem a apresentação $\langle X | R \rangle$, onde

$$X = \{x_1, x_2, x_3\}$$

$$R = \{x_1^2, x_2^2, x_3^2, (x_1x_2)^3, (x_2x_3)^3, x_1^{-1}x_3^{-1}x_1x_3\}.$$

Como A_4 é o subgrupo de S_4 de índice 2, podemos tomar $T = \{1, x_1\}$ como sendo um transversal (à direita) para A_4 em S_4, onde 1 é o representante das permutações pares e x_1 é o representante das permutações ímpares.

$\forall \sigma \in S_4$, denotemos por $\overline{\sigma}$ o representante em T da classe $A_4\sigma$. Logo, $A_4\sigma \cap T = \{\overline{\sigma}\}$. Pelas regras de paridade da multiplicação de permutações, é claro que $\overline{1x_i} = x_1$ e $\overline{x_1x_i} = 1$, para todo $1 \leq i \leq 3$. Isto produz a metade à esquerda da tabela abaixo.

	x_1	x_2	x_3	x_1^2	x_2^2	x_3^2	$(x_1x_2)^3$	$(x_2x_3)^3$	$x_1^{-1}x_3^{-1}x_1x_3$
1	$-$	$x_2x_1^{-1}$	$x_3x_1^{-1}$	x_1^2	x_2^2	x_3^2	$(x_1x_2)^3$	$(x_2x_3)^3$	$x_1^{-1}x_3^{-1}x_1x_3$
x_1	x_1^2	x_1x_2	x_1x_3	x_1^2	$x_1x_2^2x_1^{-1}$	$x_1x_3^2x_1^{-1}$	$x_1(x_1x_2)^3x_1^{-1}$	$x_1(x_2x_3)^3x_1^{-1}$	$x_3^{-1}x_1x_3x_1^{-1}$

Nesta tabela, as duas fileiras são indexadas por T e as colunas são indexadas por X e R, respectivamente. A entrada (t, x) é igual a $tx\overline{tx}^{-1}$ e a entrada (t, r) é igual a trt^{-1}, onde $t \in T$, $x \in X$ e $r \in R$.

Agora, obtemos uma nova tabela a partir desta através de uma nova rotulação dos geradores $\widehat{X} = \{tx\overline{tx}^{-1}; t \in T, x \in X, tx \notin T\}$ por novos símbolos e de uma reescrita das relações $\widehat{R} = \{trt^{-1}; t \in T, r \in R\}$ em termos destes símbolos. Por exemplo, rotulemos os geradores $\widehat{X}$ pelos símbolos

$$b_1 = x_1^2, \quad b_2 = x_2x_1^{-1}, \quad b_3 = x_1x_2, \quad b_4 = x_3x_1^{-1}, \quad b_5 = x_1x_3.$$

Agora, para expressarmos $h = x_3^{-1}x_1x_3x_1^{-1}$ em termos dos novos geradores, basta fazermos o processo indutivo da prova do Lema 3 do Capítulo 2 de [4] sobre h como abaixo

$$\begin{aligned}
t_1 &= 1, & t_2 &= \overline{1x_3^{-1}} = x_1, & a_1 &= 1x_3^{-1}x_1^{-1},\\
t_2 &= x_1, & t_3 &= \overline{x_1x_1} = 1, & a_2 &= x_1x_1,\\
t_3 &= 1, & t_4 &= \overline{1x_3} = x_1, & a_3 &= 1x_3x_1^{-1},\\
t_4 &= x_1, & t_5 &= \overline{x_1x_1^{-1}} = 1, & a_4 &= x_1x_1^{-1} = 1,
\end{aligned}$$

e, portanto, $h = a_1a_2a_3$, onde $a_j \in \widehat{X} \cup \widehat{X}^{-1}$, para todo $1 \leq j \leq 3$. Isto fornece a última entrada da seguinte tabela, sendo as outras entradas da metade à direita encontradas por inspeção.

x_1	x_2	x_3	x_1^2	x_2^2	x_3^2	$(x_1x_2)^3$	$(x_2x_3)^3$	$x_1^{-1}x_3^{-1}x_1x_3$
$-$	b_2	b_4	b_1	b_2b_3	b_4b_5	b_3^3	$(b_2b_5)^3$	$b_1^{-1}b_4^{-1}b_5$
b_1	b_3	b_5	$-$	b_3b_2	b_5b_4	$(b_1b_2)^3$	$(b_3b_4)^3$	$b_5^{-1}b_1b_4$

Aqui, a relação repetida $x_1x_1^2x_1^{-1} = x_1^2 = b_1$ é omitida. Para reduzirmos esta tabela a uma forma mais manejável, fazemos o uso informal das transformações de Tietze como segue. Primeiro, deletemos o gerador trivial b_1. Depois, usemos as relaçoes b_2b_3, b_4b_5 para substituirmos b_2, b_5 por b_3^{-1}, b_4^{-1}, respectivamente. As únicas relações não-triviais restantes são aquelas nas três últimas colunas da segunda tabela, a saber,

$$b_3^3, \quad (b_3^{-1}b_4^{-1})^3, \quad b_4^{-2}, \quad b_3^{-3}, \quad (b_3b_4)^3, \quad b_4^2.$$

Como as três primeiras relações são consequência das três últimas, segue que

$$A_4 = \langle b_3, b_4 \mid b_3^{-3}, b_4^2, (b_3b_4)^3 \rangle.$$

CAPÍTULO 2

GRUPOS COM AO MENOS DOIS GERADORES A MAIS DO QUE RELAÇÕES

Provaremos, neste capítulo, que todo grupo tendo uma apresentação finita com ao menos dois geradores a mais do que relações possui um subgrupo de índice finito que pode ser epimorficamente aplicado para o grupo livre F_2 de posto 2. Mas, antes, vejamos alguns resultados e definições auxiliares.

2.1 Resultados e Definições Auxiliares

Proposição 2.1. *Se $\psi : G \longrightarrow H$ é um homomorfismo de grupos e N é um subgrupo normal de G contido em $Ker\ \psi$, então $\overline{\psi} : G/N \longrightarrow H$, definido por $\overline{\psi}(gN) = \psi(g)$, é um homomorfismo induzido por ψ.*

Demonstração: É claro que $\overline{\psi}$ está bem definida, pois se tivermos $g_1N = g_2N$, então $g_2^{-1}g_1 \in N \leq Ker\ \psi$. Logo, $\psi(g_1) = \psi(g_2)$ e, portanto, $\overline{\psi}(g_1N) = \overline{\psi}(g_2N)$.

Como $\overline{\psi}(g_1Ng_2N) = \overline{\psi}(g_1g_2N) = \psi(g_1g_2) = \psi(g_1)\psi(g_2) = \overline{\psi}(g_1N)\overline{\psi}(g_2N)$, $\forall g_1, g_2 \in G$, segue que $\overline{\psi}$ é um homomorfismo.

■

Proposição 2.2. *Se F é um grupo livre com base X, então F/F' é um grupo abeliano livre com base $X_{\#} = \{xF'; x \in X\}$. Em particular, se F tem posto n, então F/F' tem posto n.*

Demonstração: Sejam A um grupo abeliano e $f : X_{\#} \longrightarrow A$ uma função. Definamos $f_{\#} : X \longrightarrow A$ por $f_{\#}(x) = f(xF')$. Como F é livre com base X, existe um homomorfismo $\varphi : F \longrightarrow A$ estendendo $f_{\#}$. Como A é abeliano, segue que $F' \leq Ker\ \varphi$. Portanto, pela Proposição 2.1, $\tilde{\varphi} : F/F' \longrightarrow A$, definido por $\tilde{\varphi}(wF') = \varphi(w)$, é um homomorfismo estendendo f.

Falta mostrarmos que a extensão $\tilde{\varphi}$ é única. Suponhamos que $\theta : F/F' \longrightarrow A$ seja um outro homomorfismo estendendo f, isto é, $\theta(xF') = f(xF')$, para todo $x \in X$. Se $\nu : F \longrightarrow F/F'$ é a projeção canônica, então $\theta\nu : F \longrightarrow A$ é um homomorfismo com $\theta\nu(x) = \theta(xF') = f(xF') = f_{\#}(x) = \varphi(x)$, para todo $x \in X$. Como X é uma base de F, temos que $\theta\nu = \varphi = \tilde{\varphi}\nu$. Logo, segue que $\theta = \tilde{\varphi}$, já que ν é invertível à direita por ser sobrejetiva. Assim, F/F' é abeliano livre com base $X_{\#}$.

■

Teorema 2.3. *Seja H um subgrupo de índice finito em um grupo abeliano livre F de posto finito n. Então, existem bases $\{y_1, \ldots, y_n\}$ de F e $\{h_1, \ldots, h_n\}$ de H tais que $h_i \in \langle y_i \rangle$, para todo $1 \leq i \leq n$.*

Demonstração: Se $\{b_1, b_2, \ldots, b_n\}$ é uma base ordenada de F e $h' \in H \leq F$, então, pela Proposição 1.5, h' tem uma única expressão da forma $h' = z_1b_1 + z_2b_2 + \ldots + z_nb_n$, onde os inteiros $z_1, z_2, \ldots, z_n$ são as coordenadas do elemento h' na base $\{b_1, b_2, \ldots, b_n\}$. Escolhamos uma base ordenada B de F e um elemento $h_1 \in H$ tais que, dentre todas estas possíveis escolhas, a primeira coordenada de h_1 em B seja a menor positiva. Sejam $B = \{x_1, x_2, \ldots, x_n\}$ a base ordenada escolhida de F e $h_1 = k_1x_1 + k_2x_2 + \ldots + k_nx_n$ o elemento escolhido de H. Afirmamos que k_1 divide k_i, para todo $i \geq 2$. O algoritmo da divisão fornece $k_i = q_ik_1 + r_i$, onde $0 \leq r_i < k_1$, para todo $i \geq 2$. Portanto,

$$h_1 = k_1(x_1 + q_2x_2 + \ldots + q_nx_n) + r_2x_2 + \ldots + r_nx_n.$$

Definamos $y_1 = x_1 + q_2x_2 + \ldots + q_nx_n$ e notemos que $\{y_1, x_2, \ldots, x_n\}$ é uma base ordenada de F. Agora, $h_1 = k_1y_1 + r_2x_2 + \ldots + r_nx_n$. Se $r_i \neq 0$, para algum $i \geq 2$, então a primeira coordenada de h_1 relativo à base ordenada $\{x_i, y_1, \ldots, x_n\}$, a saber r_i, viola a minimalidade de nossa escolha inicial. Assim, para todo $i \geq 2$, temos que $r_i = 0$ e, portanto, k_1 divide k_i. Logo, $h_1 = k_1y_1$ e, portanto, $h_1 \in \langle y_1 \rangle$.

Se $h = m_1y_1 + m_2x_2 + \ldots + m_nx_n$ é um elemento arbitrário de H, afirmamos que k_1 divide m_1. De fato, se $m_1 = qk_1 + r$, onde $0 < r < k_1$, então $h - qh_1 \in H$ tem primeira coordenada positiva r menor do que k_1, o que é uma contradição. Daí, segue que a aplicação $\pi : H \longrightarrow H$, dada por $h \longmapsto m_1y_1$, é uma retração com imagem $\langle h_1 \rangle$. Pelo Lema 10.3 de [9], $H = \langle h_1 \rangle \oplus ker\ \pi = \langle h_1 \rangle \oplus (H \cap \langle x_2, \ldots, x_n \rangle)$. Como $\langle x_2, \ldots, x_n \rangle$ é abeliano livre de posto $n - 1$ e $H \cap \langle x_2, \ldots, x_n \rangle$ é um subgrupo de índice finito em $\langle x_2, \ldots, x_n \rangle$, a prova pode ser completada por indução sobre n.

■

Teorema 2.4 (von Dyck). *Sejam H e $\overline{H}$ grupos com apresentações $\theta : F \longrightarrow H$ e $\phi : F \longrightarrow \overline{H}$ tais que toda relação de θ é uma relação de ϕ. Então, a função $\varphi : H \longrightarrow \overline{H}$, dada por $\varphi(\theta(f)) = \phi(f)$, é um epimorfismo.*

Demonstração: Primeiro, provemos que φ está bem definida. Assim, sejam $f, f' \in F$ com $\theta(f) = \theta(f')$. Daí, segue que $f'f^{-1} \in Ker\ \theta$. Como toda relação de θ é uma relação de ϕ, temos que $Ker\ \theta \subseteq Ker\ \phi$. Logo, $f'f^{-1} \in Ker\ \phi$. Então, $\phi(f) = \phi(f')$ e, portanto, $\varphi(\theta(f)) = \varphi(\theta(f'))$. Assim, φ está bem definida. Agora, sejam $f_1, f_2 \in F$. Como θ e ϕ são homomorfismos, temos que

$$\varphi(\theta(f_1)\theta(f_2)) = \varphi(\theta(f_1f_2)) = \phi(f_1f_2) = \phi(f_1)\phi(f_2) = \varphi(\theta(f_1))\varphi(\theta(f_2))$$

e, portanto, φ é um homomorfismo. Como ϕ é sobrejetiva, segue que φ também o é. Logo, φ é um epimorfismo.

■

Definição 2.5. *Se w é uma palavra sobre $\{a_1, a_2, \ldots, a_n\}$ dada por $w = a_{\nu_1}^{\alpha_1} a_{\nu_2}^{\alpha_2} \ldots a_{\nu_r}^{\alpha_r}$, onde $\alpha_i \in \mathbb{Z}$ e $\nu_i \in \{1, 2, \ldots, n\}$, então a* **soma dos expoentes de** a_j **em** *w é o inteiro*

$$\sigma_{a_j}(w) = \sum_{\nu_i = j} \alpha_i.$$

Vejamos o seguinte exemplo.

Exemplo 2.6. Se $w = a_1^2 a_2 a_1^{-3} a_2^{-1} a_1^{-1}$, então $\sigma_{a_1}(w) = -2$ e $\sigma_{a_2}(w) = 0$.

2.2 Resultados Principais

Lema 2.7. *Seja G um grupo tendo uma apresentação finita $\varphi : F \longrightarrow G$ com p geradores e q relações, onde $p - q \geq 1$. Então, existe um epimorfismo de G para $\mathbb{Z}$. Além disso, podemos obter uma nova apresentação para G com p geradores e q relações, na qual um dos geradores aparece com soma dos expoentes zero em todas as relações.*

Demonstração: Sejam G' o subgrupo derivado de G, F' o subgrupo derivado de F, $G_{ab} = G/G'$, $F_{ab} = F/F'$ e $\pi : G \longrightarrow G_{ab}$, dado por $\pi(g) = gG'$, o epimorfismo canônico. Consideremos o epimorfismo composto $\pi\varphi : F \longrightarrow G_{ab}$, definido por $\pi(\varphi(f)) = \varphi(f)G'$.

Como G_{ab} é abeliano e $F/Ker\ \pi\varphi \cong G_{ab}$, então $F/Ker\ \pi\varphi$ é abeliano e, portanto, $F' \subseteq Ker\ \pi\varphi$.

Assim, pela Proposição 2.1, temos que $\overline{\varphi} : F_{ab} \longrightarrow G_{ab}$, dado por $\overline{\varphi}(fF') = \varphi(f)G'$, é um epimorfismo induzido por $\pi\varphi$.

Seja $\overline{\pi} : F \longrightarrow F_{ab}$, definido por $\overline{\pi}(f) = fF'$, o epimorfismo canônico. Como

$$\pi(\varphi(f)) = \varphi(f)G' = \overline{\varphi}(fF') = \overline{\varphi}(\overline{\pi}(f)),$$

para todo $f \in F$, então o diagrama abaixo comuta.

$$\begin{array}{ccc} F & \xrightarrow{\varphi} & G \\ {\scriptstyle\overline{\pi}}\downarrow & & \downarrow{\scriptstyle\pi} \\ F_{ab} & \xrightarrow[\overline{\varphi}]{} & G_{ab} \end{array}$$

Agora, suponhamos que $\langle x_1, \ldots, x_p \mid r_1, \ldots, r_q \rangle$ seja a apresentação de G associada ao epimorfismo $\varphi : F \longrightarrow G$.

Daí, segue que F é o grupo livre com base $\{x_1, \ldots, x_p\}$. Logo, pela Proposição 2.2, F_{ab} é abeliano livre com base $\{\overline{x_1}, \ldots, \overline{x_p}\}$, onde $\overline{x_1} = x_1F', \ldots, \overline{x_p} = x_pF'$.

Assim, como $\overline{\varphi}$ é um epimorfismo, temos que $G_{ab} \cong F_{ab}/Ker\ \overline{\varphi}$ e, portanto,

$$G_{ab} = \langle \overline{x_1}, \ldots, \overline{x_p} \mid \overline{r_1}, \ldots, \overline{r_q} \rangle, \tag{2.1}$$

onde $\overline{r_1} = r_1F', \ldots, \overline{r_q} = r_qF'$.

Agora, mostremos que G_{ab} tem um elemento de ordem infinita.

Então, suponhamos, por absurdo, que G_{ab} seja de torção. Logo, G_{ab} é finito, pois é um grupo abeliano finitamente gerado de torção.

Daí, segue que o índice de $Ker\ \overline{\varphi}$ em F_{ab} é finito, pois $[F_{ab} : Ker\ \overline{\varphi}] = |G_{ab}|$. Logo, pelo Teorema 2.3, existem bases $\{y_1, \ldots, y_p\}$ de F_{ab} e $\{k_1, \ldots, k_p\}$ de $Ker\ \overline{\varphi}$ tais que $k_i \in \langle y_i \rangle$, para todo $1 \leq i \leq p$.

Pela Definição 1.4, temos que $F_{ab} = \langle y_1 \rangle \oplus \ldots \oplus \langle y_p \rangle$ e $Ker\ \overline{\varphi} = \langle k_1 \rangle \oplus \ldots \oplus \langle k_p \rangle$. Assim,

$$G_{ab} \cong \frac{F_{ab}}{Ker\ \overline{\varphi}} = \frac{\langle y_1 \rangle \oplus \ldots \oplus \langle y_p \rangle}{\langle k_1 \rangle \oplus \ldots \oplus \langle k_p \rangle} = \frac{\langle y_1 \rangle}{\langle k_1 \rangle} \oplus \ldots \oplus \frac{\langle y_p \rangle}{\langle k_p \rangle}, \tag{2.2}$$

já que $\langle k_i \rangle \lhd \langle y_i \rangle$, para todo $1 \leq i \leq p$.

Como $k_i \in \langle y_i \rangle$, então existe um inteiro z_i tal que $k_i = y_i^{z_i}$, para cada $1 \leq i \leq p$.

De (2.2), vemos que qualquer apresentação de G_{ab} obtida como quociente do grupo abeliano livre F_{ab} tem p geradores (a saber, $\frac{\langle y_1 \rangle}{\langle k_1 \rangle}, \ldots, \frac{\langle y_p \rangle}{\langle k_p \rangle}$) e, pelo menos, p relações (a saber, $k_1 = y_1^{z_1}, \ldots, k_p = y_p^{z_p}$), o que é um absurdo, já que (2.1) é uma apresentação de G_{ab} obtida como quociente de F_{ab} com p geradores e q relações, sendo $q < p$.

Portanto, de fato, G_{ab} tem um elemento de ordem infinita. Então, pelo Teorema 1.18, segue que $G_{ab} \cong \mathbb{Z}^n \oplus t(G_{ab})$, com $n > 0$. Denotemos por $\psi : G_{ab} \longrightarrow \mathbb{Z}^n \oplus t(G_{ab})$ este tal isomorfismo. Como $n > 0$, existe um epimorfismo de $\phi : \mathbb{Z}^n \oplus t(G_{ab}) \longrightarrow \mathbb{Z}$. Logo, $\phi \circ \psi \circ \pi : G \longrightarrow \mathbb{Z}$ é um epimorfismo de G para $\mathbb{Z}$.

$$\begin{tikzcd}
F \arrow[r, "\varphi"] \arrow[d, "\pi"'] & G \arrow[d, "\pi"] \\
F_{ab} \arrow[r, "\overline{\varphi}"'] & G_{ab} \arrow[d, "\psi"] \\
& \mathbb{Z}^n \oplus t(G_{ab}) \arrow[d, "\phi"] \\
& \mathbb{Z}
\end{tikzcd}$$

Agora, mostremos que podemos obter uma nova apresentação para G com p geradores e q relações, na qual um dos geradores aparece com soma dos expoentes zero em todas as relações.

Assim, consideremos a apresentação $\langle u_1, \ldots, u_n, v_1, \ldots, v_m \mid v_1^{a_1}, \ldots, v_m^{a_m} \rangle$ de $\mathbb{Z}^n \oplus t(G_{ab})$, onde $n + m = p$ e $u_1, \ldots, u_n$ sejam os geradores de ordem infinita de $\mathbb{Z}^n \oplus t(G_{ab})$.

Sejam $\{b_1, \ldots, b_p\}$ a base de F tal que $\psi(\overline{\varphi}(\overline{\pi}(b_1))) = u_1$ e

$$\langle b_1, \ldots, b_p \mid s_1, \ldots, s_q \rangle \tag{2.3}$$

a apresentação de G obtida como quociente de F em termos da base $\{b_1, \ldots, b_p\}$ (isto é, $s_1, \ldots, s_q$ são as relações $r_1, \ldots, r_q$ de G escritas em termos dos geradores $\{b_1, \ldots, b_p\}$).

Logo, (2.3) é uma apresentação de G com p geradores e q relações, na qual b_1 deve aparecer com soma dos expoentes zero em todas as relações $s_1, \ldots, s_q$, pois, caso contrário, u_1 seria um elemento de ordem finita de $\mathbb{Z}^n \oplus t(G_{ab})$, o que é um absurdo.

$\blacksquare$

Teorema 2.8. *Seja G um grupo tendo uma apresentação finita com g geradores e r relações, onde $g-r \geq 2$. Então, G possui um subgrupo H de índice finito que pode ser epimorficamente aplicado para F_2 (o grupo livre de posto 2).*

Demonstração: Pelo Lema 2.7, podemos assumir que G tem uma apresentação com geradores $X = \{t, a_1, \ldots, a_{g-1}\}$ e relações $R = \{u_1, \ldots, u_r\}$, onde $\sigma_t(u_1) = \ldots = \sigma_t(u_r) = 0$.

$$G = \langle X \mid R \rangle = \langle t, a_1, \ldots, a_{g-1} \mid u_1, \ldots, u_r \rangle \quad (g - r \geq 2 \text{ e } \sigma_t(u_1) = \ldots = \sigma_t(u_r) = 0)$$

Para cada inteiro positivo n, seja H o fecho normal em G do conjunto $\{t^n, a_1, \ldots, a_{g-1}\}$. Assim, H é o subgrupo normal de G dado por

$$\begin{aligned} H &= \langle \{t^n, a_1, \ldots, a_{g-1}\}^G \rangle \\ &= \langle b\delta b^{-1} \; ; \; b \in G \text{ e } \delta \in \{t^n, a_1, \ldots, a_{g-1}\} \rangle. \end{aligned}$$

Como a soma dos expoentes de t em qualquer elemento de H é um mútiplo de n, então $t, \ldots, t^{n-1} \notin H$ e, portanto, H depende de n.

Denotemos por γ, ρ e η os índices tomando valores inteiros nos intervalos

$$1 \leq \gamma \leq g-1, \quad 1 \leq \rho \leq r \text{ e } 0 \leq \eta \leq n-1.$$

Para cada inteiro j, sejam $a_{\gamma,j} = t^j a_\gamma t^{-j}$, $u_{\rho,j} = t^j u_\rho t^{-j}$, etc.

Como cada u_ρ é uma palavra reduzida sobre X na qual a soma dos expoentes de t é zero, então inserindo de maneira adequada relações triviais do tipo $t^{-\kappa}t^{\kappa}$ ($\kappa \in \mathbb{Z}$) entre quaisquer dois símbolos consecutivos de u_ρ, vemos que cada u_ρ pode ser escrito como uma palavra nos $a_{\gamma,\xi}$, com $\xi \in \mathbb{Z}$. Depois, conjugando cada u_ρ pela potência adequada de t se necessário, podemos assumir que existe um inteiro positivo m tal que todos os u_ρ's podem ser escritos como palavras nos $a_{\gamma,\mu}$, com $0 \leq \mu \leq m$. Por exemplo, suponhamos que $r = 3$ com

$$\begin{aligned} u_1 &= a_1^{-1}a_2t^2a_{g-1}a_1a_2^{-1}t^{-1}a_1t^{-1} \quad , \\ u_2 &= t^{-1}a_{g-1}t^2a_1^{-1}ta_2a_1t^{-2}a_2^{-1} \quad \text{e} \\ u_3 &= a_2^{-1}t^{-1}a_{g-1}a_2ta_1. \end{aligned}$$

Então, inserindo de maneira adequada relações triviais do tipo $t^{-\kappa}t^{\kappa}$ ($\kappa \in \mathbb{Z}$) entre quaisquer dois símbolos consecutivos de u_1, u_2 e u_3, temos que

$$\begin{aligned}
u_1 &= a_1^{-1}a_2t^2a_{g-1}(t^{-2}t^2)a_1(t^{-2}t^2)a_2^{-1}t^{-1}(t^{-1}t)a_1t^{-1} \\
&= (a_{1,0})^{-1}(a_{2,0})(a_{g-1,2})(a_{1,2})(a_{2,2})^{-1}(a_{1,1}) \qquad , \\
u_2 &= t^{-1}a_{g-1}t^2a_1^{-1}(t^{-1}t)ta_2(t^{-2}t^2)a_1t^{-2}a_2^{-1} \\
&= (a_{g-1,-1})(a_{1,1})^{-1}(a_{2,2})(a_{1,2})(a_{2,0})^{-1} \qquad \text{e} \\
u_3 &= a_2^{-1}t^{-1}a_{g-1}(tt^{-1})a_2(tt^{-1})ta_1 \\
&= (a_{2,0})^{-1}(a_{g-1,-1})(a_{2,-1})(a_{1,0}).
\end{aligned}$$

Agora, observemos que, em u_1, todos os $a_{\gamma,\xi}$ aparecem com $\xi \geq 0$ e, por isso, não precisamos conjugar u_1 por potência nenhuma de t. Porém, como isto não acontece em u_2 e u_3, estes precisam ser conjugados por alguma potência adequada de t para que tenhamos u_2 e u_3 escritos como palavras nos $a_{\gamma,\xi}$, com $\xi \geq 0$. Logo, temos que

$$\begin{aligned}
u_1 &= (a_{1,0})^{-1}(a_{2,0})(a_{g-1,2})(a_{1,2})(a_{2,2})^{-1}(a_{1,1}) \qquad , \\
tu_2t^{-1} &= t(a_{g-1,-1})(a_{1,1})^{-1}(a_{2,2})(a_{1,2})(a_{2,0})^{-1}t^{-1} \\
&= t(a_{g-1,-1})(t^{-1}t)(a_{1,1})^{-1}(t^{-1}t)(a_{2,2})(t^{-1}t)(a_{1,2})(t^{-1}t)(a_{2,0})^{-1}t^{-1} \\
&= (a_{g-1,0})(a_{1,2})^{-1}(a_{2,3})(a_{1,3})(a_{2,1})^{-1} \qquad \text{e} \\
tu_3t^{-1} &= t(a_{2,0})^{-1}(a_{g-1,-1})(a_{2,-1})(a_{1,0})t^{-1} \\
&= t(a_{2,0})^{-1}(t^{-1}t)(a_{g-1,-1})(t^{-1}t)(a_{2,-1})(t^{-1}t)(a_{1,0})t^{-1} \\
&= (a_{2,1})^{-1}(a_{g-1,0})(a_{2,0})(a_{1,1}).
\end{aligned}$$

Portanto, neste exemplo, temos $m = 3$.

Notemos que m é independente de n. Assim, escolhendo n suficientemente grande, podemos assumir que $n > m$. Então, denotemos por μ o índice tomando valores inteiros no intervalo

$$0 \leq \mu \leq m.$$

Agora, mostremos que $T = \{1, t, \ldots, t^{n-1}\}$ é um transversal de Schreier para H em G. É claro que $\bigcup_{j=0}^{n-1} Ht^j \subseteq G$, já que $Ht^j \subseteq G$, para todo $j \in \{0, \ldots, n-1\}$. Reciprocamente, seja $b \in G$ qualquer. Como b é uma palavra sobre X e H é um subgrupo normal de G contendo $\{t^n, a_1, \ldots, a_{g-1}\}$, segue que $Hb = Ht^{\sigma_t(b)} = Ht^j$, onde $\sigma_t(b) \equiv j \pmod{n}$. Logo, $b \in Ht^j$, para algum $j \in \{0, \ldots, n-1\}$. Assim, $b \in \bigcup_{j=0}^{n-1} Ht^j$ e, portanto, $G \subseteq \bigcup_{j=0}^{n-1} Ht^j$. Como $G = \bigcup_{j=0}^{n-1} Ht^j$, falta mostrarmos que $Ht^i \cap Ht^j = \varnothing$ sempre que $t^i, t^j \in T$ com $i \neq j$. Então, sem perda de generalidade, assumamos que $t^i, t^j \in T$ com $i > j$ e suponhamos, por absurdo, que $b \in Ht^i \cap Ht^j$. Logo, $b = h_1 t^i = h_2 t^j$, onde $h_1, h_2 \in H$. Assim, $t^{i-j} = h_1^{-1} h_2 \in H$, com $t^{i-j} \in \{t, \ldots, t^{n-1}\}$. Mas, isto é um absurdo, já que $H \cap \{t, \ldots, t^{n-1}\} = \varnothing$. Logo, $Ht^i \cap Ht^j = \varnothing$ sempre que $t^i, t^j \in T$ com $i \neq j$. Como T possui a propriedade de Schreier, então, de fato, T é um transversal de Schreier para H em G.

Seja $s = t^n$. Portanto, como T é um transversal de Schreier para H em G, segue que

$$\begin{aligned} \hat{X} &= \{\alpha x \overline{\alpha x}^{-1} \; ; \; \alpha \in T, \; x \in X \; \text{ e } \; \alpha x \notin T\} \\ &= \{s, a_{\gamma,\eta} \; ; \; 1 \leq \gamma \leq g-1 \; \text{ e } \; 0 \leq \eta \leq n-1\} \end{aligned}$$

é um conjunto de geradores de H e

$$\begin{aligned} \hat{R} &= \{\alpha \beta \alpha^{-1} \; ; \; \alpha \in T \; \text{ e } \; \beta \in R\} \\ &= \{u_{\rho,\eta} \; ; \; 1 \leq \rho \leq r \; \text{ e } \; 0 \leq \eta \leq n-1\} \end{aligned}$$

é um conjunto de relações definidoras para H em termos dos geradores X.

Logo, para obtermos uma apresentação de H, precisamos reescrever as relações $\hat{R}$ em termos dos geradores $\hat{X}$.

Como u_ρ é uma palavra nos $a_{\gamma,\mu}$, segue que $u_{\rho,\eta}$ é uma palavra nos $a_{\gamma,(\mu+\eta)}$, pois basta inserirmos a relação trivial $t^{-\eta}t^{\eta}$ entre todos os $a_{\gamma,\mu}$ que aparecerem em $u_{\rho,\eta}$.

Então, seja $v_{\rho,\eta}$ obtido a partir de $u_{\rho,\eta}$ usando o processo de reescrita de Reidemeister-Schreier. Assim, denotando por κ o índice tomando valores inteiros no intervalo

$$0 \leq \kappa \leq m-1,$$

vemos que $v_{\rho,\eta}$ é obtido a partir de $u_{\rho,\eta}$ trocando todos os símbolos $a_{\gamma,(\kappa+n)}$ por $sa_{\gamma,\kappa}s^{-1}$, pois

$$a_{\gamma,(\kappa+n)} = t^{(\kappa+n)}a_\gamma t^{-(\kappa+n)} = t^n(t^\kappa a_\gamma t^{-\kappa})t^{-n} = sa_{\gamma,\kappa}s^{-1}.$$

Dessa maneira,

$$\hat{S} = \{v_{\rho,\eta}\ ;\ 1 \leq \rho \leq r \ \text{ e } \ 0 \leq \eta \leq n-1\}$$

é um conjunto de relações definidoras para H em termos dos geradores $\hat{X}$ e, portanto,

$$H = \langle \hat{X} \mid \hat{S} \rangle = \langle s, a_{\gamma,\eta} \mid v_{\rho,\eta} \rangle. \tag{2.4}$$

Agora, consideremos o grupo

$$\overline{H} = \langle s, a_{\gamma,\eta} \mid v_{\rho,\eta}, a_{\gamma,\kappa} = 1 \rangle. \tag{2.5}$$

Como toda relação de (2.4) é uma relação de (2.5), então, pelo Teorema 2.4, existe um epimorfismo $\varphi : H \to \overline{H}$.

Denotemos por ϵ o índice tomando valores inteiros no intervalo

$$m \leq \epsilon \leq n-1.$$

Logo, aplicando a transformação de Tietze ($T4$) em (2.5) para removermos os geradores supérfluos $a_{\gamma,\kappa}$ de $\overline{H}$, temos que

$$\overline{H} = \langle s, a_{\gamma,\epsilon} \mid w_{\rho,\eta} \rangle,$$

onde $w_{\rho,\eta}$ é obtido a partir de $v_{\rho,\eta}$ substituindo todos os símbolos $a_{\gamma,\kappa}$ por 1.

Notemos que todos os $w_{\rho,\eta}$ não envolvem s, já que s só aparece na forma $sa_{\gamma,\kappa}s^{-1}$ em todos os $v_{\rho,\eta}$.

Portanto, pelo Teorema 1.43, temos que $\overline{H} = \langle s \mid \varnothing \rangle * \langle a_{\gamma,\epsilon} \mid w_{\rho,\eta} \rangle = \langle s \rangle * K$, onde

$$K = \langle a_{\gamma,\epsilon} \mid w_{\rho,\eta} \rangle. \tag{2.6}$$

Como $g - r \geq 2$, segue que $(g - r - 1) \geq 1$. Assim, em (2.6), temos que

$$\begin{aligned}
\text{n}^{\text{o}} \text{ de geradores} - \text{n}^{\text{o}} \text{ de relações} &= [(g-1)(n-m)] - rn \\
&= gn - n - gm + m - rn \\
&= (g-r-1)n + (1-g)m \\
&= (g-r-1)n + cte \\
&\geq n + cte
\end{aligned}$$

e, portanto, esta diferença é maior do que zero escolhendo n suficientemente grande.

Então, pelo Lema 2.7, existe um epimorfismo de K em $\mathbb{Z}$. Daí, segue que existe um epimorfismo de $\overline{H}$ em $\mathbb{Z} * \mathbb{Z}$, pois $\overline{H} \cong \mathbb{Z} * K$ por ser $\overline{H} = \langle s \rangle * K$.

Mas, pelo Teorema 1.43, temos que $\mathbb{Z} * \mathbb{Z} \cong F_2$, onde F_2 é o grupo livre de posto 2.

Logo, existe um epimorfismo $\psi : \overline{H} \to F_2$. Como $\varphi : H \to \overline{H}$ é um epimorfismo, temos que $\psi \circ \varphi : H \to F_2$ é um epimorfismo de H em F_2.

Como $[G : H] = |T| = n < \infty$, a demonstração do teorema está completa.

$\blacksquare$

REFERÊNCIAS BIBLIOGRÁFICAS

[1] B. Baumslag and S.J. Pride, *Groups with two more generators than relators*, J. London Math. Soc. (2) **17**, 425-426 (1978).

[2] B. Baumslag and S.J. Pride, *Groups with one more generators than relators*, Math. Z. **167**, 279-281 (1979).

[3] M. Gromov, *Volume and bounded cohomology*, IHES Publ. Math. **56**, 5-99 (1982).

[4] D.L. Johnson, *Presentation of groups*, 2nd ed., London Mathematical Society Student Texts **15**, Cambridge University Press (1997).

[5] M.I. Kargapolov and Ju.I. Merzljakov, *Fundamentals of the theory of groups*, translated from the second Russian edition by Robert G. Burns, Springer-Verlag New York Inc. (1979).

[6] M. Lackenby, *A characterisation of large finitely presented groups*, J. Algebra **287**, 458-473 (2005).

[7] W. Magnus, A. Karrass and D. Solitar, *Combinatorial group theory: presentations of groups in terms of generators and relations*, 2nd ed., Dover Publications Inc. (1976).

[8] D.J.S. Robinson, *A course in the theory of groups*, 2nd ed., Springer-Verlag New York Inc. (1996).

[9] J.J. Rotman, *An introduction to the theory of groups*, 4th ed., Springer-Verlag New York Inc. (1995).

[10] J.R. Stallings, *"Quotients of the powers of the augmentation ideal in a group ring"* in *Knots, groups and 3-manifolds: papers dedicated to the memory of R. H. Fox*, Annals of Mathematics Studies, Number 84, Princetown University Press (1975).

[11] R. Stöhr, *Groups with one more generators than relators*, Math. Z. **182**, 45-47 (1983).

[12] H. Tietze, *Über die topologischen Invarianten mehrdimensionaler Mannigfaltigkeiten*, Monatsh. Math. Phys. **19**, 1-118 (1908).