UNICAMP

UNIVERSIDADE ESTADUAL DE CAMPINAS

Instituto de Matemática, Estatística e Computação Científica

JUAN FERNANDO GARCIA PULGARIN

Funções Isoperimétricas de Alguns Grupos Metabelianos

Campinas

2021

Juan Fernando Garcia Pulgarin

Funções Isoperimétricas de Alguns Grupos Metabelianos

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Mestre em Matemática.

Orientadora: Dessislava Hristova Kochloukova

Este trabalho corresponde à versão final da Dissertação defendida pelo aluno Juan Fernando Garcia Pulgarin e orientada pela Profa. Dra. Dessislava Hristova Kochloukova.

Campinas

2021

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Ana Regina Machado - CRB 8/5467

G165f

Garcia Pulgarin, Juan Fernando, 1996-
Funções isoperimétricas de alguns grupos metabelianos / Juan Fernando Garcia Pulgarin. – Campinas, SP : [s.n.], 2021.

Orientador: Dessislava Hristova Kochloukova.
Dissertação (mestrado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Teoria dos grupos. 2. Problemas de palavras (Matemática). 3. Desigualdades isoperimétricas. I. Kochloukova, Dessislava Hristova, 1970-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: Isoperimetric functions of some metabelian groups
Palavras-chave em inglês:
Group theory
Word problems (Mathematics)
Isoperimetric inequalities
Área de concentração: Matemática
Titulação: Mestre em Matemática
Banca examinadora:
Dessislava Hristova Kochloukova [Orientador]
Mikhailo Dokuchaev
Marcelo Muniz Silva Alves
Data de defesa: 19-04-2021
Programa de Pós-Graduação: Matemática

Identificação e informações acadêmicas do(a) aluno(a)
- ORCID do autor: https://orcid.org/0000-0003-1972-9742
- Currículo Lattes do autor: http://lattes.cnpq.br/3884846836622062

Dissertação de Mestrado defendida em 19 de abril de 2021 e aprovada pela banca examinadora composta pelos Profs. Drs.

Prof(a). Dr(a). DESSISLAVA HRISTOVA KOCHLOUKOVA

Prof(a). Dr(a). MIKHAILO DOKUCHAEV

Prof(a). Dr(a). MARCELO MUNIZ SILVA ALVES

A Ata da Defesa, assinada pelos membros da Comissão Examinadora, consta no SIGA/Sistema de Fluxo de Dissertação/Tese e na Secretaria de Pós-Graduação do Instituto de Matemática, Estatística e Computação Científica.

Agradecimentos

Inicialmente, quero expressar meu profundo agradecimento à minha orientadora, a professora Dessislava. Ela, além de cumprir seu papel de orientadora excelentemente, me apoiou e deu ânimo nos momentos mais difíceis, particularmente durante a pandemia de Covid-19. Agradeço pela sua confiança desde o primeiro dia.

Agradeço aos meus pais e irmãos, que sempre estão torcendo para que eu seja feliz e fazem todo o que for possível para me ajudar a consegui-lo.

Agradeço aos grandes amigos que fiz no Brasil, que me ajudaram com a adaptação ao país e me ofereceram uma maravilhosa companhia. Também, agradeço ao meu amigo e orientador da graduação, o professor Carlos Cadavid por me mostrar a beleza da matemática e me motivar a entrar no mestrado.

Agradeço ao Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq pelo auxílio econômico na forma de bolsa de mestrado (processo N° 132324/2019-9). Isto representa uma grande oportunidade para milhares de pessoas que desfrutamos da ciência e sonhamos com contribuir ao desenvolvimento da mesma.

Finalmente, agradeço à UNICAMP e ao IMECC pela oportunidade que me deram de entrar no mestrado e por disponibilizar todos os médios necessários para desenvolver meus estudos. Em particular, agradeço aos docentes do programa de Pós-Graduação em Matemática pela sua grande contribuição na minha formação.

Resumo

Neste trabalho estudamos os resultados de M. Kassabov e T. Riley em [7], onde se prova que o grupo de Baumslag tem função de Dehn exponencial, em contraste com o que ocorre com seu análogo em que uma relação de torção é acrescentada, o qual satisfaz uma desigualdade isoperimétrica polinomial. Apresentamos alguns preliminares sobre teoria de grupos e módulos, além de estudar com detalhe a construção de grupos livres e o conceito de apresentação de um grupo.

Palavras-chave: Teoria dos grupos, grupos finitamente apresentáveis, problema da palavra, desigualdades isoperimétricas.

Abstract

In this work we study the results of M. Kassabov and T. Riley in [7], where they prove that Baumslag group has an exponential Dehn function, in contrast to its analog when a torsion relation is added, which satisfies a polynomial isoperimetric inequality. We present some basic concepts of group theory and modules. Additionally we study the contruction of free groups and the concept of presentation of a group in detail.

Keywords: Group theory, finitely presented groups, word problem, isoperimetric inequalities.

Lista de símbolos

$\mathbb{Z}$	Conjunto dos números inteiros
$\mathbb{R}$	Conjunto dos números reais
$\mathbb{Z}_n$	Grupo dos inteiros módulo n
$\|X\|$	Número de elementos do conjunto X
S_X	Grupo das permutações em X
S_n	Grupo das permutações no conjunto $\{1, 2, \ldots, n\}$
$\cong$	Isomorfismo
$Hom(G, K)$	Conjunto de homomorfismo de G em K
$\langle X \rangle$	Subgrupo gerado por X
$H \vee K$	Subgrupo gerado por $H \cup K$
$[G : S]$	Índice de S em G
$\langle X \rangle^G$	Subgrupo normal de G gerado por X
G/N	Grupo quociente de G por N
$[a, b]$	Comutador de a e b
G'	Subgrupo comutador de G
$H \rtimes K$	Produto semidireto de H com K
a^G	Classe de conjugação de a em G
$Z(G)$	Centro do grupo G
$C_G(a)$	Centralizador de a em G
$N_G(H)$	Normalizador de H em G
$\mathcal{O}(x)$	Órbita de x
G_x	Estabilizador de x em G
$\oplus$	Soma direta

$R[G]$	Anel de grupo de G sobre R
$Ann_R(a)$	Aniquilador de a em R
$GL_n(R)$	Grupo de matrizes $n \times n$ com entradas em R
$M(X)$	Conjunto de sequências finitas em X
$F(X)$	Grupo livre com base X
$\langle X \mid R \rangle$	Apresentação do grupo com geradores X e relações R
$Area_a(w)$	Área algébrica da palavra w
δ_P	Função de Dehn do grupo com apresentação P
$\preceq$	Relação de dominância assintótica
$\simeq$	Equivalência assintótica
Γ	Grupo de Baumslag
Γ_m	Grupo Γ acrescentando a relação $a^m = 1$
$[\![a]\!]_r^f$	ver página 69
$\{\!\{a\}\!\}_r^f$	ver página 75

Sumário

Introdução

Nesta dissertação vamos estudar funções de Dehn e funções isoperimétricas de grupos finitamente apresentáveis. A função de Dehn de um grupo finitamente apresentado é um invariante do grupo que desde o ponto de vista combinatório, dá conta da complexidade do problema da palavra no grupo ([6]). Este é um problema algorítmico proposto por M. Dehn na década de 1910 que consiste em decidir se duas palavras nos geradores de um grupo representam ou não o mesmo elemento, ou equivalentemente, decidir se uma palavra representa o elemento identidade do grupo.

Falamos que um grupo é finitamente apresentável se ele pode ser definido por um número finito de geradores e relações. Assim, a função de Dehn depende da apresentação finita usada para o grupo. Mas como é usual nos problemas de complexidade algorítmica, o interesse está sobre o comportamento assintótico das funções, que no caso das funções de Dehn é independente da apresentação finita usada. Tal independência é descrita pela seguinte relação de dominância assintótica:

$$f \preceq g \quad \Longleftrightarrow \quad \exists C > 0 : \forall l \geqslant 0,\ f(l) \leqslant Cg(Cl + C) + Cl + C,$$

onde $f \simeq g$ quando $f \preceq g$ e $g \preceq f$.

Por exemplo, o grupo $\mathbb{Z}^2$ tem apresentação $\langle a, b \,|\, [a, b] = 1\rangle$. Aqui uma palavra representa o elemento identidade se a e b aparecem o mesmo número de vezes que a^{-1} e b^{-1} respectivamente. Assim, para saber se uma palavra representa a identidade, usamos a comutatividade de a e b ($[a, b] = 1$) para colocar na esquerda as letras a, a^{-1} e na direita as letras b, b^{-1}, de forma que reduzimos a palavra removendo os fragmentos da forma aa^{-1}, $a^{-1}a$, $bb^{-1}, b^{-1}b$. No caso de que a palavra represente a identidade, este processo produz a palavra vazia e o máximo de vezes que é usada a relação $[a, b] = 1$ é menor que n^2, onde n é o comprimento da palavra. Então a função de Dehn de $\mathbb{Z}^2$ é no máximo quadrática.

Achar a função de Dehn de um grupo em particular é normalmente muito difícil e muitas vezes é um problema geométrico pois de fato depende da geometria das palavras que descrevem as relações do grupo. Por causa disso na literatura tem bastantes resultados onde se procuram limites superiores para tais funções de Dehn. Tais limites superiores são chamados de funções isoperimétricas. Encontrar estes limites é mais simples, pois é possível usar técnicas algébricas combinatoriais para fazer os cálculos.

O objetivo desta dissertação é explicar detalhadamente o trabalho de M. Kassabov & T. Riley [7], no qual mostram desigualdades isoperimétricas para a função de Dehn do grupo

de Baumslag

$$\Gamma = \langle a, s, t \,|\, [a, a^t] = 1,\ [s, t] = 1,\ a^s = aa^t \rangle$$

e o grupo

$$\Gamma_m = \langle a, s, t \,|\, [a, a^t] = 1,\ [s, t] = 1,\ a^s = aa^t,\ a^m = 1 \rangle.$$

Em particular, o grupo Γ foi introduzido por G. Baumslag em [1] como o primeiro exemplo de um grupo finitamente apresentável que possui um subgrupo normal abeliano de posto infinito.

Os resultados principais demonstrados são o Teorema 4.1, que estabelece o comportamento exponencial da função de Dehn de Γ, e o Teorema 4.2, que mostra uma desigualdade isoperimétrica quártica para a função de Dehn de Γ_m.

O conteúdo deste trabalho está distribuído da seguinte forma:

No Capítulo 1 presentamos algumas definições e resultados básicos da teoria de grupos que serão usados mais na frente, além de falar um pouco sobre grupo abelianos finitamente gerados. Também fixamos parte da notação usada no resto do texto. O Capítulo 2 tem algumas definições e resultados sobre módulos que precisamos para entender a maioria dos argumentos utilizados no Capítulo 4 quando provamos desigualdades isoperimétricas.

No Capítulo 3 introduzimos os conceitos de grupo livre, grupo finitamente apresentável e função de Dehn, e mostramos alguns resultados importantes. Finalmente, no Capítulo 4 estudamos com detalhe os resultados presentados no artigo [7].

1 Noções de Teoria dos Grupos

O conteúdo deste capítulo trata de resultados básicos em teoria de grupos e portanto omitimos as demonstrações. Tomamos como referência principal o livro [8].

1.1 Noções básicas

Definição 1.1. *Um **grupo** é um par $(G, *)$, onde G é um conjunto não vazio e $* : G \times G \to G$ é uma operação binaria, satisfazendo as seguintes propriedades:*

(i) $a * (b * c) = (a * b) * c$ *para todo* $a, b, c \in G$,

(ii) existe $e \in G$ *tal que* $a * e = e * a = a$ *para todo* $a \in G$,

(iii) para todo $a \in G$ *existe* $b \in G$ *tal que* $a * b = b * a = e$.

Quando não houver ambiguidade, denotamos $a * b$ simplesmente por ab.

Pode se mostrar facilmente que dado um grupo $(G, *)$, o elemento $e \in G$ mencionado em (ii) é único e é chamado de elemento ***identidade***, as vezes denotado por 1. Também, o elemento b em (iii) é único para cada $a \in G$, este é chamado de ***inverso*** de a e denotado por a^{-1}.

Definição 1.2. *Sejam $(G, *)$ um grupo e $a, b \in G$. Dizemos que a e b **comutam** se $a * b = b * a$. $(G, *)$ é dito **abeliano**, se todo par de elementos $a, b \in G$ comutam. Neste caso é comum usar a notação aditiva, onde a operação do grupo é denotada por $+$, o elemento identidades por 0 e o inverso de g por $-g$.*

Exemplo 1.1. *Os seguintes são exemplos de grupos abelianos:*

1. *$(\mathbb{Z}, +)$, onde 0 é o elemento identidade, e para cada $a \in \mathbb{Z}$, $-a$ é o inverso.*
2. *$(\mathbb{R}\backslash\{0\}, \cdot)$, onde 1 é o elemento identidade, e para cada $a \in \mathbb{R}\backslash\{0\}$, $\dfrac{1}{a}$ é o inverso.*
3. *Dado $n \in \mathbb{N}$ com $n \geqslant 2$, tem se a relação de equivalência em $\mathbb{Z}$ dada por: $a \equiv b \mod n \iff n$ divide $a - b$. Seja $\mathbb{Z}_n$ o conjunto das classes de equivalência. Dado $a \in \mathbb{Z}$, denotamos por $[a]$ a classe de equivalência de a. Assim $(\mathbb{Z}_n, +_n)$ é um grupo abeliano, onde $+_n : \mathbb{Z}_n \to \mathbb{Z}_n$ está definida por*

$$[a] +_n [b] = [a + b].$$

Neste caso, o elemento identidade é $[0]$*, e para cada* $[a] \in \mathbb{Z}_n$*, o elemento inverso é* $[-a]$*.*

Exemplo 1.2. *Dado um conjunto* $X \neq \emptyset$*, uma* ***permutação*** *em* X *é uma bijeção* $\alpha : X \to X$*. Denotamos por* S_X *o conjunto de todas as permutações em* X*.* S_X *é um grupo com a operação de composição de funções. Aqui, o elemento identidade é a função identidade em* X*,* id_X *e para cada permutação* $\alpha \in S_X$ *o seu inverso é a sua função inversa* α^{-1}*.* S_X *é chamado de* ***grupo simétrico*** *em* X*. Se o numero de elementos de* X *for maior ou igual a 3, o grupo simétrico não é abeliano.*

Definição 1.3. *Um caso muito importante do exemplo anterior é quando* $X = \{1, 2, \ldots, n\}$*, onde* S_X *é denotado por* S_n *e é chamado de* ***grupo simétrico de grau*** n*.*
Dados $i_1, i_2, \ldots, i_r$ *inteiros distintos entre* 1 *e* n*. Se* $\alpha \in S_n$ *fixa os* $n - r$ *inteiros restantes (i.e.* $\alpha(i) = i$ *para todo* $i \notin \{i_1, \ldots, i_r\}$*) e*

$$\alpha(i_1) = i_2,\ \alpha(i_2) = i_3,\ \ldots,\ \alpha(i_{r-1}) = i_r,\ \alpha(i_r) = i_1,$$

α *é dito de* r***-ciclo*** *e denotado por* $\alpha = (i_1 i_2 \ldots i_r)$*. Os* 2*-ciclos são chamados de* ***transposições****.*

Duas permutações $\alpha, \beta \in S_n$ *são ditas* ***disjuntas****, se para todo* $i, j \in \{1, \ldots, n\}$*,*

$$\alpha(i) \neq i \Rightarrow \beta(i) = i \quad e \quad \beta(j) \neq j \Rightarrow \alpha(j) = j.$$

É fácil ver que se duas permutações são disjuntas, então elas comutam.

Teorema 1.1. *Seja* $\alpha \in S_n$*, então:*

(i) α *tem uma única fatoração completa (modulo a ordem) como produto de ciclos disjuntos, i.e.*

$$\alpha = \beta_1 \beta_2 \cdots \beta_t$$

onde cada $\beta_i = (\beta_{i1}, \beta_{i2}, \ldots, \beta_{ir_i}) \in S_n$ *é um* r_i*-ciclo e para cada* $a \in \{1, 2, \ldots, n\}$ *existem únicos* i, j *tais que* $\beta_{ij} = a$*.*

(ii) α *é produto de transposições.*

Definição 1.4. *Sejam* $(G, *)$*,* $(H, \circ)$ *grupos. Uma função* $f : G \to H$ *é um* ***homomorfismo****, se para todo* $a, b \in G$*,*

$$f(a * b) = f(a) \circ f(b).$$

Um homomorfismo $f : G \to H$ é dito ***epimorfismo*** *se for uma função sobrejetora, e* ***isomorfismo*** *se for uma função bijetora. Se $H = G$ e f é isomorfismo, este é dito* ***automorfismo****. Dizemos que $(G, *)$ é* ***isomorfo*** *a $(H, \circ)$, se existir um isomorfismo $f : G \to H$ e denotamos isto por $G \cong H$.*

Exemplo 1.3. *Seja $\alpha \in S_n$ e $\alpha = \beta_1\beta_2 \cdots \beta_t$ uma fatoração completa em ciclos disjuntos, então o* ***sinal*** *de α é definido por*

$$sgn(\alpha) = (-1)^{n-t}.$$

Alternativamente, se escrevemos $\alpha = \gamma_1\gamma_2 \ldots \gamma_m$ como produto de transposições, é possível verificar que

$$sgn(\alpha) = (-1)^m.$$

Uma permutação α é dita ***par*** *se $sgn(\alpha) = 1$ ou* ***impar****, caso contrário. Pode se verificar que para todo $\alpha, \beta \in S_n$,*

$$sgn(\alpha\beta) = sgn(\alpha)sgn(\beta)$$

logo, sgn é um homomorfismo entre S_n e $\{1, -1\}$ (que é grupo com a multiplicação usual), no caso $n = 2$, sgn é isomorfismo.

Exemplo 1.4. *A função $f : \mathbb{Z} \to \mathbb{Z}_n$, definida por $f(a) = [a]$ é um homomorfismo, mas não é isomorfismo para nenhum n.*

Definição 1.5. *Seja G um grupo. Um subconjunto não vazio $S \subseteq G$ é um* ***subgrupo*** *se para todo $s, t \in S$, $s^{-1} \in S$ e $st \in S$. Denotamos isto por $S \leqslant G$. Neste caso é fácil ver S é um grupo com a mesma operação binaria de G, restrita a $S \times S$.*

Exemplo 1.5. *Seja $f : G \to H$ um homomorfismo, definimos a* ***imagem*** *e o* ***núcleo*** *de f como*

$$Im(f) = \{h \in H : h = f(a) \text{ para algum } a \in G\} \quad e \quad Ker(f) = \{a \in G : f(a) = 1_H\},$$

respectivamente. Temos que $Ker(f) \leqslant G$ e $Im(f) \leqslant H$.

Proposição 1.1. *Seja G um grupo e $\{S_i\}_{i\in I}$ uma família não vazia de subgrupos de G, então $\bigcap_{i\in I} S_i$ é um subgrupo de G.*

Da proposição anterior segue a validade da seguinte definição:

Definição 1.6. *Seja G um grupo e $X \subseteq G$, então o mínimo subgrupo de G (com respeito a inclusão) que contém a X é chamado de* ***subgrupo gerado por*** *X e denotado por $\langle X \rangle$. Se $G = \langle a_1, a_2, \ldots, a_n \rangle$ para alguns $a_i \in G$, dizemos que G é finitamente gerado. Se H, K são subgrupos de G, então o subgrupo $\langle H \cup K \rangle$ é denotado por $H \vee K$.*

Proposição 1.2. *Seja G um grupo e $X \subseteq G$. Se $X = \varnothing$, então $\langle X \rangle = \{1\}$, caso contrário $\langle X \rangle$ é o conjunto de todas as* ***palavras*** *em X, isto é, os elementos $w \in G$ da forma*

$$w = x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n},$$

com $x_i \in X$, $e_i = \pm 1$, $n \geqslant 1$.

Exemplo 1.6. *Se G é um grupo e $a \in G$, temos do teorema anterior que $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$, este subgrupo é chamado de* ***subgrupo cíclico gerado por*** *a. O número de elementos deste subgrupo, $|\langle a \rangle|$, é chamado de* ***ordem*** *de a. G é dito* ***cíclico****, se existe $a \in G$ com $G = \langle a \rangle$.*
Pode se mostrar que se $a \in G$ tem ordem finita m, então m é o menor inteiro positivo tal que $a^m = 1$.

Definição 1.7. *Seja G um grupo e $S \leqslant G$. A* ***classe lateral à direita*** *de S com* ***representante*** *$t \in G$ é o conjunto $St = \{st : s \in S\}$ (a* ***classe lateral à esquerda*** *é $tS = \{ts : s \in S\}$).*

Exemplo 1.7. *Seja G o grupo aditivo $\mathbb{Z}$ e $n \in \mathbb{Z}$. Se $S = \langle n \rangle$ e $a \in \mathbb{Z}$, então a classe lateral de S com representante a é o conjunto $a + S = \{a + zn : z \in \mathbb{Z}\}$, que é precisamente a classe de equivalência $[a]$ do exemplo 1.1-3). Dada a comutatividade de $+$ em $\mathbb{Z}$, as classes à direita e esquerda resultam ser iguais.*

Proposição 1.3. *Seja G um grupo e $S \leqslant G$, então:*

(i) A família de classes laterais à direita (ou à esquerda) forma uma partição de G.

(ii) O número de classes laterais à direita é igual ao número de classes laterais à esquerda.

Definição 1.8. *Seja G um grupo, o número de elementos de G, $|G|$, é dito a* ***ordem*** *de G. Se $S \leqslant G$ então o* ***índice*** *de S em G, denotado por $[G : S]$, é o número de classes laterais à direita (ou esquerda) de S em G.*

Teorema 1.2. (Lagrange). *Seja G um grupo finito e $S \leqslant G$ então $|S|$ divide a $|G|$ e $[G : S] = |G|/|S|$.*

Como consequência deste teorema segue que se G é um grupo de ordem p e p é primo, então G é grupo cíclico.

Proposição 1.4. *Sejam G um grupo finito e $S, T \leqslant G$, então*

$$|ST||S \cap T| = |S||T|,$$

onde $ST = \{st : s \in S \ e \ t \in T\}$.

Definição 1.9. *Seja G um grupo. Um subgrupo $K \leqslant G$ é um **subgrupo normal**, se para todo $g \in G$, $gKg^{-1} = \{gkg^{-1} : k \in K\} = K$. Denotamos isto por $K \lhd G$.*

Pode se observar que se $K \lhd G$, então as classes laterais à esquerda e à direita de K em G são iguais, no sentido em que $Kg = gK$ para todo $g \in G$.

Exemplo 1.8. *Sejam G, H grupos e $f : G \to R$ um homomorfismo, então $ker(f) \lhd G$.*

Proposição 1.5. *Seja G um grupo,*

(i) se G é abeliano, então todo subgrupo de G é normal;

(ii) se $H, K \lhd G$, então $H \vee K \lhd G$;

(iii) se $\{H_i : i \in I\}$ é uma família não vazia de subgrupos normais de G, então $\bigcap_{i \in I} H_i \lhd G$.

De (iii) segue que dado um subconjunto $X \subseteq G$ não vazio, existe um mínimo subgrupo normal de G que contém a X, chamado de ***subgrupo normal gerado por*** X ou ***fecho normal*** de $\langle X \rangle$, denotado por $\langle X \rangle^G$.

Teorema 1.3. *Seja G um grupo e $N \lhd G$.*

*(i) Então a família das classes laterais de N em G forma um grupo de ordem $[G : N]$ chamado de **grupo quociente** e denotado por G/N, com a operação*

$$(Na, Nb) \longmapsto Nab;$$

*(ii) a função $v : G \to G/N$ definida por $v(a) = Na$ é um homomorfismo sobrejetivo com $ker(v) = N$, chamada de **projeção canônica**.*

Exemplo 1.9. *Seja $G = \mathbb{Z}$ e $n \in \mathbb{Z}$. Do exemplo 1.1-3), sabemos que em $\mathbb{Z}_n$ os elementos são do tipo $[a] = a + \langle n \rangle$, com $a \in \mathbb{Z}$. Como $\mathbb{Z}$ é abeliano, $\langle n \rangle$ é normal pela proposição 1.5, então existe o grupo quociente $\mathbb{Z}/\langle n \rangle$, que é precisamente o grupo $\mathbb{Z}_n$.*

Definição 1.10. *Seja G um grupo e $a, b \in G$. O* ***comutador*** *de a e b é definido como $[a, b] = a^{-1}b^{-1}ab$. O* ***subgrupo comutador*** *de G é o subgrupo de G gerado por todos os comutadores e é denotado por G'.*

Proposição 1.6. *Seja G um grupo, então G' é subgrupo normal de G e se $H \lhd G$, então G/H é abeliano se, e somente se, $G' \leqslant H$.*

1.2 Teoremas de Isomorfismo e Ações

Teorema 1.4. (Teoremas de Isomorfismo)

(Primeiro) *Seja $f : G \to H$ um homomorfismo de grupos, então $G/ker(f) \cong Im(f)$.*

(Segundo) *Sejam N, T subgrupos de G, com N normal. Então $N \cap T \lhd T$ e*

$$T/(N \cap T) \cong NT/N.$$

(Terceiro) *Sejam $K \leqslant H \leqslant G$, onde K e H são subgrupos normais de G. Então H/K é subgrupo normal de G/K e*

$$(G/K)\,/\,(H/K) \cong G/H.$$

Exemplo 1.10. *Seja $G = \langle g \rangle$ um grupo cíclico de ordem n. Seja*

$$f : \mathbb{Z} \to G$$

o homomorfismo de grupos dado por $f(k) = g^k$, $\forall k \in \mathbb{Z}$. Então f é sobrejetivo e $ker(f) = \langle n \rangle$, então, pelo Primeiro Teorema de Isomorfismo, $\mathbb{Z}/\langle n \rangle \cong G$. Assim, todo grupo cíclico de ordem n é isomorfo a $\mathbb{Z}_n$.

Teorema 1.5. *Sejam K, H grupos, $R \subseteq K$, e $\theta : K \to H$ um homomorfismo tal que $\theta(R) = \{1\}$, então existe um homomorfismo $\psi : K/\langle R \rangle^K \to H$ tal que $\theta = \psi \circ v$, onde v é a projeção de K em $K/\langle R \rangle^K$. Aqui $\langle R \rangle^K = \langle R^K \rangle$, onde $R^K = \{k^{-1}rk \mid k \in K, r \in R\}$.*

Teorema 1.6. (Teorema de Correspondência). *Sejam $K \lhd G$ e $v : G \to G/K$ a projeção canônica. Então*

$$\{S \mid S \leqslant G, K \leqslant S\} \longmapsto \{M \mid M \leqslant G/K\}$$

é uma bijeção entre a família dos subgrupos G que contém a K, e a família dos subgrupos de G/K que envia S para $v(S) = S/K$. Também, denotando S/K por S^*, tem se que para todo $T \leqslant G$, com $K \leqslant T$:

(i) $T \leqslant S$ se, e somente se, $T^* \leqslant S^*$, com $[S : T] = [S^* : T^*]$;

(ii) $T \lhd S$ se, e somente se $T^* \lhd S^*$, com $S/T \cong S^*/T^*$.

Definição 1.11. *Dados dois grupos H, K, definimos no produto cartesiano $H \times K$ a operação binaria*

$$(h, k)(h', k') = (hh', kk').$$

$H \times K$ com esta operação binaria é um grupo, chamado de ***produto direto*** *de H e K, com elemento identidade $(1_H, 1_K)$ e inverso $(h, k)^{-1} = (h^{-1}, k^{-1})$.*

Proposição 1.7. *Seja G um grupo, $H \lhd G$ e $K \lhd G$. Se $G = HK$ e $H \cap K = 1$, então $G \cong H \times K$.*

O produto direto visto como na Definição 1.11 é dito de produto direto ***externo***. No caso da Proposição 1.7, o produto $H \times K$ é chamado de produto direto ***interno***, pois pode ser visto como uma operação entre alguns subgrupos normais de G. Também, se no enunciado da Proposição 1.7 $K \leqslant G$ não é necessariamente normal mas as outras propriedades são preservadas, então o grupo G é dito produto ***semidireto*** de H com K e denotamos por $G = H \rtimes K$.

Proposição 1.8. *Se $A \lhd H$ e $B \lhd K$, então $A \times B \lhd H \times K$ e*

$$(H \times K)/(A \times B) \cong (H/A) \times (K/B).$$

Proposição 1.9. *Sejam G um grupo, $N \lhd G$ e*

$$\phi : G \to G/N$$

a projeção canônica. Se existe um homomorfismo

$$\psi : G/N \to G \text{ tal que } \phi \circ \psi = id_{G/N},$$

então $G = N \rtimes \psi(G/N)$. Neste caso dizemos que ϕ ***cinde****.*

Definição 1.12. *Dado um grupo G e $x, y \in G$, dizemos que x e y são* ***conjugados*** *se*

$$y = gxg^{-1} \text{ para algum } g \in G.$$

Isto define uma relação de equivalência em G. A classe de equivalência de $a \in G$ é chamada de ***classe de conjugação*** *de a, denotada por a^G.*

Note se que quando $a \in G$ é o único elemento da sua classe de conjugação, então a comuta com todos os elementos de G.

Exemplo 1.11. *Seja S_n o grupo simétrico de ordem n. Duas permutações $\alpha, \beta \in S_n$ tem a* ***mesma estrutura cíclica****, se sua fatoração em ciclos disjuntos tem a mesma quantidades de r-ciclos, para cada $r \in \{1, \ldots, n\}$.*
Neste caso acontece que duas permutações são conjugadas se, e somente se, tem a mesma estrutura cíclica. Assim, um subgrupo $H \leqslant S_n$ é normal se, e somente se, para todo $\alpha \in H$ as permutações com a mesma estrutura cíclica que α estão em H.

$\alpha = (123)(456), \beta = (164)(235) \in S_6$ *tem a mesma estrutura cíclica e* $\beta = (15)\alpha(15)^{-1}$.

Definição 1.13. *O* ***centro*** *de um grupo G é o conjunto dos elementos $a \in G$ que comutam com todos os elementos de G, denotado por $Z(G)$. Dado $a \in G$, o* ***centralizador*** *de a em G é o conjunto dos $g \in G$ que comutam com a, denotado por $C_G(a)$.*

É fácil ver que $Z(G)$ é um subgrupo normal e abeliano em G e $C_G(a) \leqslant G$.

Definição 1.14. *Seja G um grupo, $H \leqslant G$ e $g \in G$, o conjunto gHg^{-1} é dito o* ***conjugado*** *de H por g. O conjunto*

$$N_G(H) := \{a \in G : aHa^{-1} = H\}$$

é chamado o ***normalizador*** *de H em G.*

Tem se que gHg^{-1} e $N_G(H)$ são subgrupos de G e $H \lhd N_G(H)$.

Proposição 1.10. *Seja G um grupo, $a \in G$ e $H \leqslant G$, então:*

(i) o número de conjugados de a é igual ao índice $[G : C_G(a)]$ do seu centralizador $C_G(a)$ em G;

(ii) o número de conjugados de H é igual ao índice $[G : N_G(H)]$ do seu normalizador $N_G(H)$ em G.

Teorema 1.7. *Seja G um grupo e $H \leqslant G$, então:*

(i) **(Cayley).** *G pode ser mergulhado como subgrupo de S_G, por médio do homomorfismo*

$$\begin{aligned} \phi_1 : G &\to S_G \\ a &\mapsto L_a : g \mapsto ag. \end{aligned}$$

(ii) Se X denota a família de classes laterais à esquerda de H em G, então a função

$$\begin{aligned} \phi_2 : G &\to S_X \\ a &\mapsto \rho_a : gH \mapsto agH \end{aligned}$$

é um homomorfismo com $ker(\phi_2) \leqslant H$.

(iii) Se Y denota a família dos conjugados de H em G, então a função

$$\begin{aligned}\phi_3 : G &\to S_Y \\ a &\mapsto \psi_a : gHg^{-1} \mapsto agHg^{-1}a^{-1}\end{aligned}$$

é um homomorfismo com $ker(\phi_3) \leqslant N_G(H)$.

Definição 1.15. *Nas condições do teorema anterior, o homomorfismo ϕ_1 é chamado de **representação regular (à esquerda)** de G, o homomorfismo ϕ_2 é chamado de **representação de** G **em classes laterais de** H, e o homomorfismo ϕ_2 é chamado de **representação de** G **em conjugados de** H.*

Definição 1.16. *Seja X um conjunto e G um grupo. X é dito **G-conjunto** à esquerda se existe uma função $\alpha : G \times X \to X$ (chamada **ação**), tal que*

(i) $\alpha(1, x) = x$, $\forall x \in X$;

(ii) $\alpha(g, \alpha(h, x)) = \alpha(gh, x)$, $\forall g, h \in G, x \in X$.

*neste caso, dizemos que G **age** sobre X.*

Exemplo 1.12. *Se R é um anel comutativo, S_n age em $Y = R[x_1, \ldots, x_n]$ com a ação*

$$\alpha : S_n \times Y,$$

definida por $\alpha(\sigma, f) = f^\sigma$, onde $f^\sigma(x_1, \ldots, x_n) = f\left(x_{\sigma(1)}, \ldots, x_{\sigma(n)}\right)$.

Teorema 1.8. *Seja X um G-conjunto à esquerda com ação α, então a função*

$$\begin{aligned}\tilde{\alpha} : G &\to S_X \\ g &\mapsto \tilde{\alpha}(g) : x \mapsto \alpha(a, x)\end{aligned}$$

é um homomorfismo. Reciprocamente, se

$$\phi : G \to S_X$$

é um homomorfismo, então a função

$$\begin{aligned}\tilde{\phi} : G \times X &\to X \\ (g, x) &\mapsto (\phi(g))(x)\end{aligned}$$

define uma ação que torna X um G-conjunto à esquerda.

Exemplo 1.13. *Pelo teorema anterior, as representações definidas pelo Teorema 1.7 podem se ver como ações do grupo G:*

1. *em (i), $X = G$ e $\tilde{\phi}_1(a, g) = (\phi_1(a))(g) = L_a(g) = ag$;*
2. *em (ii), X é o conjunto das classes laterais à esquerda de H em G e $\tilde{\phi}_2(a, gH) = (\phi_2(a))(gH) = \rho_a(gH) = agH$;*
3. *em (iii) X é a família dos conjugados de H em G e $\tilde{\phi}_3(a, gHg^{-1}) = (\phi_3(a))(gHg^{-1}) = \psi_a(gHg^{-1}) = agHg^{-1}a^{-1}$.*

Definição 1.17. *Seja X um G-conjunto à esquerda com ação α e $x \in X$, então a* ***órbita*** *de x é o conjunto $\mathcal{O}(x) = \{gx : g \in G\}$ e o* ***estabilizador*** *de x é o subgrupo $G_x = \{g \in G : gx = x\} \leqslant G$.*

Proposição 1.11. *Se X é um G-conjunto à esquerda e $x \in X$, então $|\mathcal{O}(x)| = [G : G_x]$.*

Exemplo 1.14. *Dado um grupo G, é fácil ver que G age sobre ele mesmo por conjugação, neste caso $\mathcal{O}(x) = x^G$ e $G_x = C_G(x)$ para todo $x \in G$. Também, G age sobre o conjunto de todos os subgrupos de G, onde $\mathcal{O}(H) = \{\text{conjugados de } H\}$ e $G_H = N_G(H)$. Então, a proposição anterior tem como consequência a Proposição 1.10.*

1.3 Grupos Abelianos Finitamente Gerados

Dado que agora vamos tratar com grupos abelianos usamos a notação aditiva onde também denotamos o elemento g^n como ng e o produto direto $G_1 \times \ldots \times G_n$ por soma direta $G_1 \oplus \ldots \oplus G_n$.

Definição 1.18. *Um grupo finitamente gerado G é dito* ***grupo abeliano livre*** *se é isomorfo a $\mathbb{Z}^n$ para algum $n \geqslant 0$, neste caso n é chamado de* ***posto*** *de G.*

Proposição 1.12. *Sejam G, H grupos abelianos tais que H é grupo finitamente gerado e livre abeliano e existe um epimorfismo $\phi : G \to H$, então existe*

$$\psi : H \to G \text{ tal que } \phi \circ \psi = id_H$$

(nesse caso falamos que ϕ cinde) e $G \cong ker(\phi) \oplus H$.

Como corolário temos o seguinte lema

Lema 1.1. *Se G é um grupo abeliano com k geradores tal que existe $N \lhd G$ com G/N grupo abeliano livre de posto k, então $G \cong \mathbb{Z}^k$.*

Definição 1.19. *Um grupo G é dito* ***livre de torção*** *se o único elemento $g \in G$ com $|g|$ finito é o elemento identidade.*

Proposição 1.13. *Se G é um grupo abeliano finitamente gerado, com mais de um elemento e é livre de torção, então G é grupo abeliano livre.*

Teorema 1.9. *Seja G é um grupo abeliano finitamente gerado, definimos*

$$G_{tor} = \{g \in G \mid |g| \text{ finito}\}.$$

Então G_{tor} é subgrupo finito de G e G/G_{tor} é grupo livre abeliano.

2 Módulos sobre anéis associativos

Na hora de trabalhar com grupos metabelianos finitamente apresentáveis precisamos de alguns conceitos sobre módulos, para o qual dedicamos este capítulo. Usamos como referência o texto [2].

Definição 2.1. *Seja R um anel associativo com unidade. Um $R-$**módulo (à direita)** consiste de um grupo abeliano M (usamos a notação aditiva) junto com uma ação de R (à direita) $\phi : M \times R \to M$, $(x, r) \mapsto xr$, onde*

1. $(x + y)r = xr + yr$
2. $x(r + s) = xr + xs$
3. $x(rs) = (xr)s$
4. $x1_R = x$,

para todo $x, y \in M$, $r, s \in R$. Analogamente se definem os R-módulos à esquerda. Como caso particular, temos que quando R é um corpo, um R-módulo é um espaço vetorial sobre R.

Exemplo 2.1. *Dado um grupo abeliano A, este pode se considerar como um $\mathbb{Z}-$módulo, por meio da ação à direita $(a, z) \mapsto za$, onde (usando notação aditiva para A)*

$$za = \begin{cases} \overbrace{a + \cdots + a}^{z-vezes}, & z > 0 \\ 0_A, & z = 0 \\ (-z)(-a), & z < 0 \end{cases}.$$

Exemplo 2.2. *Todo anel com unidade R é um R-módulo à direita (também à esquerda), onde a ação é o produto em R, $(r, s) \mapsto rs$, e R é visto como grupo abeliano com respeito à operação soma.*

Definição 2.2. *Seja M um R-módulo à direita, um subconjunto $\varnothing \neq N \subseteq M$ é um **submódulo** de M, se N for subgrupo de M e para todo $x \in M$, $r \in R$ tem se $xr \in N$. Dado um subconjunto $\varnothing \neq X \subseteq M$, o conjunto*

$$\langle X \rangle = \left\{ \sum_{i=1}^{n} x_i r_i \,|\, x_i \in X, r_i \in R, n \in \mathbb{N} \right\}$$

*é um submódulo de M, chamado **submódulo gerado por** X (se $X = \varnothing, \langle X \rangle = \{0\}$). X é dito **conjunto gerador** de M, se $M = \langle X \rangle$. Dizemos que M é **cíclico** se tem um conjunto gerador de cardinalidade 1.*

Exemplo 2.3. *Seja R um anel associativo com unidade. No Exemplo 2.2 consideramos R como um R-módulo à direita. Nesta situação, os submódulos de R são precisamente os ideais à direita de R.*

Definição 2.3. *Sejam M, N R-módulos à direita. Uma função $f : M \to N$ é um* ***homomorfismo de módulos*** *se*

(i) $f(x + y) = f(x) + f(y)$, *para todo* $x, y \in M$;

(ii) $f(xr) = f(x)r$, *para todo* $x \in M, r \in R$.

Se f for sobrejetor, f é dito ***epimorfismo****. Se f for uma bijeção, então f é um* ***isomorfismo*** *e dizemos que M, N são* ***isomorfos****.*

Proposição 2.1. *Sejam M, N R-módulos à direita e*

$$f : M \to N$$

um homomorfismo. Então para todo submódulo $X \subseteq M$, $f(X)$ é submódulo de N; e para todo submódulo $Y \subseteq N$, $f^{-1}(Y)$ é submódulo de M. Em particular, $f^{-1}(\{0\})$ é um submódulo de M, chamado de ***núcleo*** *de f, denotado por $ker(f)$.*

Definição 2.4. *Seja M um R-módulo à direita e $N \subseteq M$ um submódulo. Então podemos definir uma relação de equivalência em M da seguinte forma $x \sim y \iff x - y \in N$. O conjunto de classes de equivalência M/N é um R-módulo à direita com a operação $[x] + [y] = [x + y]$ e a ação*

$$([x], r) \mapsto [xr],$$

aqui $[x] = x + N$ denota a classe de equivalência de x. M/N é chamado de ***módulo quociente*** *de M por N. Notamos que projeção natural*

$$\pi : M \to M/N,$$

$x \mapsto [x]$ é um homomorfismo sobrejetor.

Como no caso de grupos, existe Teorema de Correspondência e Teorema de Isomorfismos para módulos

Teorema 2.1. *Se N é um submódulo de um R-módulo M, então*

$$\begin{array}{rcl} \theta : \{ \text{ submódulos de } M \text{ que contém } N\} & \longrightarrow & \{ \text{ submódulos de } M/N\} \\ A & \longmapsto & A/N \end{array}$$

é uma bijeção que preserva inclusão.

Teorema 2.2. *Sejam M, N R-módulos à direita e*

$$f : M \to N$$

um homomorfismo de módulos. Então existe um único isomorfismo

$$\phi : M/ker(f) \to f(M),$$

tal que $\phi \circ \pi = f$, onde π é a projeção natural de M sobre $M/ker(f)$.

Exemplo 2.4. *Seja M um R-módulo à direita cíclico, e consideramos R como um R-módulo à direita. Seja $m_0 \in M$ elemento gerador de M, consideramos o homomorfismo de R-módulos*

$$f : R \to M$$

dado por $f(r) = m_0 r$. É claro que f é epimorfismo, além disso,

$$ker(f) = \{r \in R \,|\, f(r) = 0\} = \{r \in R \,|\, m_0 r = 0\} := Ann_R(m_0),$$

logo M é isomorfo a $R/Ann_R(m_0)$ pelo teorema anterior.

Definição 2.5. *Seja M um R-módulo à direita, e $\{M_i\}_{i\in I}$ uma família de submódulos. Definimos o conjunto*

$$\sum_{i\in I} M_i := \left\{ \sum_{i\in I} x_i \,|\, x_i \in M_i, \text{ e } x_i = 0 \text{ exceto para finitos } i \in I \right\}.$$

$\sum_{i\in I} M_i$ *é o submódulo de M gerado por $\{M_i\}_{i\in I}$. Dizemos que $\sum_{i\in I} M_i$ é* ***soma direta*** *de $\{M_i\}_{i\in I}$ se $M_i \cap (\sum_{j\neq i} M_j) = \{0\}$ para todo $i \in I$, e denotamos isto como*

$$\sum_{i\in I} M_i = \bigoplus_{i\in I} M_i.$$

M é dito ***módulo livre com base*** *$X \subseteq M$, se*

$$M = \bigoplus_{x\in X} xR \text{ e } xR \cong R \text{ para todo } x \in X.$$

Exemplo 2.5. *Se G é um grupo abeliano, pelo exemplo 2.1 podemos considerar G como $\mathbb{Z}$-módulo. Se G é $\mathbb{Z}$-módulo livre com base $X \subseteq G$, chamamos G de* ***grupo abeliano livre com base*** *X, neste que caso temos que*

$$G = \bigoplus_{x\in X} x\mathbb{Z} \cong \bigoplus_{x\in X} \mathbb{Z}.$$

Definição 2.6. *Dado um grupo G e um anel associativo e comutativo com unidade R, definimos o* ***anel de grupo de*** *G* ***sobre*** *R denotado por $R[G]$ (ou RG), como o conjunto das combinações lineares formais*

$$\alpha = \sum_{g\in G} r_g g,$$

onde $r_g \in R$ para todo $g \in G$ e $r_g = 0$ exceto para finitos $g \in G$. $R[G]$ é um anel junto com as operações $+, \cdot$ dadas por

$$\left(\sum_{g\in G} r_g g\right) + \left(\sum_{g\in G} s_g g\right) = \sum_{g\in G}(r_g + s_g)g$$

$$\left(\sum_{g\in G} r_g g\right) \cdot \left(\sum_{h\in G} s_h h\right) = \left(\sum_{g,h\in G} r_g s_h gh\right),$$

com $0_{R[G]} = \sum_{g\in G} 0_R g$ e $1_{R[G]} = \sum_{g\in G} r_g g$, onde $r_g = \begin{cases} 1_R, & g = 1_G \\ 0_R, & g \neq 1_G \end{cases}$. Observamos que RG é R-módulo livre com base G.

Exemplo 2.6. *Por definição, dado um grupo metabeliano G, temos que existe um subgrupo normal $A \lhd G$, tal que A é abeliano e $Q = G/A$ é abeliano. Podemos considerar A como $\mathbb{Z}[Q]$-módulo à direita da seguinte forma.*

Definimos a seguinte ação de Q sobre A. Dados $a \in A$, $q \in Q$, temos que $q = Ag$ para algum $g \in G$, seja

$$a \circ q = a^g \in A.$$

Vejamos que $\circ$ está bem definida. De fato, se $Ag = Ah$ então $a_0 = gh^{-1} \in A$, logo $a^g = a^{a_0 h} = (a^{a_0})^h$, mas dado que A é abeliano temos $a^{a_0} = a$, portanto $a^g = a^h$.
Estendemos esta ação por linearidade a uma ação à direita de $\mathbb{Z}[Q]$ sobre A, assim (usando notação aditiva para A)

$$a \circ \left(\sum_{q\in Q} z_q q\right) = \sum_{q\in Q}(z_q a) \circ q \ \in A,$$

onde $z_q a$ é definido como no Exemplo 2.1.

3 Grupos Finitamente Apresentáveis

3.1 Grupos Livres

Começamos este capítulo falando sobre grupos livres, tomando como referência o livro [4].

Definição 3.1. *Seja X um conjunto, G um grupo e $i : X \to G$ uma função. O par (G, i) é dito* ***livre sobre*** *X, se para todo grupo H e uma aplicação $f : X \to H$ existe um único homomorfismo*

$$\phi : G \to H \text{ tal que } \phi \circ i = f.$$

Como será mostrado logo, na definição anterior podemos considerar a X como um subconjunto de G, ainda mais um conjunto gerador, e denotando

$$X^{-1} = \{x^{-1} : x \in X\},$$

o fato de (G, i) ser livre sobre X é equivalente a que um produto de elementos em $X \cup X^{-1}$ é igual a 1, somente quando este for 1 em todos os grupos. Isto se apresenta formalmente na Proposição. 3.3.

Exemplo 3.1. *O grupo aditivo dos inteiros $\mathbb{Z}$ é livre sobre qualquer conjunto unitário $\{x\}$ junto com a função $i(x) = 1$.*

Proposição 3.1. *Um grupo livre sobre um conjunto X é único a menos de isomorfismo, i.e. se (G_1, i_1) é livre em X e $\phi : G_1 \to G_2$ é isomorfismo, então (G_2, i_2) é livre sobre X, onde $i_2 = \phi \circ i_1$. Reciprocamente, se $(G_1, i_1), (G_2, i_2)$ são livres sobre X, então existe um isomorfismo $\phi : G_1 \to G_2$, tal que $\phi \circ i_1 = i_2$.*

Demonstração. ($\Rightarrow$) Suponhamos (G_1, i_1) livre em X e $\phi : G_1 \to G_2$ isomorfismo. Dado um grupo H e $f : X \to H$, existe um único homomorfismo $\psi : G_1 \to H$ tal que $\psi \circ i_1 = f$, então $\psi \circ \phi^{-1} : G_2 \to H$ é um homomorfismo com

$$\psi \circ \phi^{-1} \circ i_2 = \psi \circ \phi^{-1} \circ \phi \circ i_1 = \psi \circ i_1 = f,$$

a unicidade segue imediato da unicidade de ψ.

($\Leftarrow$) Se $(G_1, i_1), (G_2, i_2)$ são livres sobre X, existem homomorfismos

$$\phi : G_1 \to G_2 \text{ e } \psi : G_2 \to G_1,$$

tais que $i_2 = \phi \circ i_1$ e $i_1 = \psi \circ i_2$. Assim,

$$id_1 \circ i_1 = i_1 = \psi \circ \phi \circ i_1 \text{ e } id_2 \circ i_2 = i_2 = \phi \circ \psi \circ i_2,$$

onde id_1, id_2 são as funções identidades de G_1, G_2, respectivamente. Então

$$\psi \circ \phi = id_1, \phi \circ \psi = id_2,$$

assim ϕ é o isomorfismo desejado. □

Proposição 3.2. *Se (G, i) é livre sobre X, então i é injetora.*

Demonstração. Seja $\mathbb{Z}^X$ o conjunto das funções de X em $\mathbb{Z}$, com a operação $\alpha + \beta$ definida por

$$(\alpha + \beta)(x) = \alpha(x) + \beta(x).$$

Com esta operação, $\mathbb{Z}^X$ é um grupo abeliano.

Seja

$$f : X \to \mathbb{Z}^X \text{ dada por } f(x) = \alpha_x,$$

onde

$$\alpha_x(y) = \begin{cases} 1 & y = x \\ 0 & y \neq x \end{cases}.$$

Assim, existe um homomorfismo $\phi : G \to \mathbb{Z}^X$, tal que $\phi \circ i = f$. É claro que f é injetora, logo i também é. □

Vejamos agora que dado um conjunto $X = \{x_i\}_{i \in I}$ qualquer, existe um grupo $F(X)$ que é livre sobre X. Seja $M(X)$ o conjunto das sequências finitas em X

$$M(X) = \bigcup_{n=0}^{\infty} X^n,$$

onde X^0 é o conjunto formado pela sequência vazia. Definimos o produto em $M(X)$ como segue

$$(x_{i_1}, \ldots, x_{i_n})(x_{j_1}, \ldots, x_{j_m}) = (x_{i_1}, \ldots, x_{i_n}, x_{j_1}, \ldots, x_{j_m}).$$

Esta operação é claramente associativa e tem como elemento identidades a sequência vazia. Identificando

$$x \leftrightarrow (x)$$

temos que todo elemento de $M(X)$ é da forma $x_{i_1} \cdots x_{i_n}$. O conjunto $M(X)$ é chamado de ***monoide livre*** em X.

Agora, seja X^{-1} um conjunto bijectivo com X, com uma bijeção que leva x em um elemento denotado por x^{-1} em X^{-1}, de forma que

$$X \cap X^{-1} = \varnothing.$$

Os elementos de $M(X \cup X^{-1})$ são chamados ***palavras*** em X. Denotando os elementos de X por $x^1 := x$, temos que as palavras em X são da forma

$$w = x_{i_1}^{e_1} \cdots x_{i_n}^{e_n}, \text{ onde } n \geqslant 0, e_k = \pm 1.$$

$l(w) := n$ é chamado de ***comprimento*** de w.

Uma palavra $w = x_{i_1}^{e_1} \cdots x_{i_n}^{e_n}$ é dita ***reduzida*** se

$$\text{para todo } 1 \leqslant r \leqslant n-1,\ i_{r+1} \neq i_r \text{ ou } i_{r+1} = i_r \text{ com } e_{r+1} \neq -e_r.$$

Se w não é reduzida, existe $1 \leqslant r \leqslant n-1$, tal que $i_{r+1} = i_r$ e $e_{r+1} = -e_r$. A palavra w' obtida deletando $x_{i_r}^{e_r}$ e $x_{i_{r+1}}^{e_{r+1}}$ de w é dita obtida de w por ***redução elementar***. Se w'' é obtida de w por uma sequência de reduções elementares, dizemos que w'' vem de w por ***redução***.

Definimos em $M(X \cup X^{-1})$ a relação $w \sim w' \Leftrightarrow w = w'$ ou existe uma sequência de palavras $w_1, \ldots, w_k$, onde $w_1 = w$, $w_k = w'$ e para todo $j < k$, uma de w_j, w_{j+1} é obtida da outra por redução elementar.

Observamos que $\sim$ é uma relação de equivalência, e denotamos por $F(X)$ o conjunto das classes de equivalência. Pode se observar que se

$$u, v \text{ são palavras e } w \sim w' \quad \Longrightarrow \quad uwv \sim uw'v,$$

assim,

$$w \sim w' \text{ e } u \sim u' \quad \Longrightarrow \quad uw \sim u'w'.$$

Portanto, a operação em $F(X)$ dada por

$$[u][w] = [uw]$$

(onde $[u]$ é a classe de equivalência de u) está bem definida, é associativa e tem como elemento identidade a classe da palavra vazia, denotada por 1. Também, se

$$w = x_{i_1}^{e_1} \cdots x_{i_n}^{e_n} \text{ e definimos } w^{-1} = x_{i_1}^{-e_1} \cdots x_{i_n}^{-e_n}, \text{ temos que } [w][w^{-1}] = 1.$$

Assim, $F(X)$ com esta operação é um grupo.

Teorema 3.1. *Cada elemento de $F(X)$ tem exatamente uma palavra reduzida.*

Demonstração. Seja

$$\lambda : M(X \cup X^{-1}) \to M(X \cup X^{-1})$$

a função definida recursivamente por $\lambda(1) = 1, \lambda(x^\epsilon) = x^\epsilon$,

$$\lambda(ux^\epsilon) = \lambda(u)x^\epsilon \text{ se } \lambda(u) \neq vx^{-\epsilon} \text{ para toda palavra } v,$$

e

$$\lambda(ux^\epsilon) = v \text{ se } \lambda(u) = vx^{-\epsilon} \text{ para alguma palavra } v.$$

Vejamos primeiro que

$$\lambda(w) \text{ é reduzida para toda palavra } w,$$

além disso, $\lambda(w)$ é obtida por redução a partir de w e se w é reduzida então $\lambda(w) = w$. Isso vai ser demonstrado por indução sobre o comprimento de w. É claro que quando w tem comprimento 0 ou 1 $\lambda(w)$ é reduzida e $\lambda(w) = w$.

Se w tem comprimento $n \geqslant 1$, então

$$w = ux^\epsilon, \text{com } u \text{ uma palavra de comprimento } n-1, x \in X, \epsilon = \pm 1.$$

Pela hipótese indutiva, $\lambda(u)$ é reduzida, vem de u por redução e se u reduzida então $\lambda(u) = u$.

Se $\lambda(u) = vx^{-\epsilon}$ para alguma palavra v, então v é reduzida e $vx^{-\epsilon}$ vem de u por redução, portanto

$$\lambda(w) = \lambda(ux^\epsilon) = v$$

é reduzida e $vx^{-\epsilon}x^\epsilon$ (logo $v = \lambda(w)$) vem de $ux^\epsilon = w$ por redução.

Se $\lambda(u) \neq vx^{-\epsilon}$ para toda palavra v, então

$$\lambda(w) = \lambda(ux^\epsilon) = \lambda(u)x^\epsilon,$$

como $\lambda(u)$ é reduzida e não é da forma $vx^{-\epsilon}$ então $\lambda(w)$ é reduzida e dado que $\lambda(u)$ vem de u por redução, então $\lambda(w) = \lambda(u)x^\epsilon$ vem de $ux^\epsilon = w$ por redução. Se w é reduzida, então u é reduzida e $\lambda(u) = u$. Como $w = ux^\epsilon$ é reduzida, então $u = \lambda(u)$ não pode ser da forma $vx^{-\epsilon}$, assim, $\lambda(w) = \lambda(ux^\epsilon) = \lambda(u)x^\epsilon = ux^\epsilon = w$.

Vamos provar agora que para toda palavra u,

$$\lambda(ux^\epsilon x^{-\epsilon}) = \lambda(u)$$

Se $\lambda(u) = vx^{-\epsilon}$ para alguma palavra v, então $vx^{-\epsilon}$ é reduzida, logo v não e da forma wx^ϵ, assim $\lambda(ux^\epsilon) = v$ não é da forma wx^ϵ, então

$$\lambda(ux^\epsilon x^{-\epsilon}) = \lambda(ux^\epsilon)x^{-\epsilon} = vx^{-\epsilon} = \lambda(u).$$

Se $\lambda(u)$ não é da forma $vx^{-\epsilon}$, então $\lambda(ux^{\epsilon}) = \lambda(u)x^{\epsilon}$, logo

$$\lambda(ux^{\epsilon}x^{-\epsilon}) = \lambda(u).$$

Por último, provamos que se u, v são palavras e $x \in X$, então

$$\lambda(ux^{\epsilon}x^{-\epsilon}v) = \lambda(uv).$$

Fixamos u e x, e procedemos por indução no comprimento de v. No caso de comprimento 1 temos $v = y^r$, com $y \in X, r = \pm 1$. Se $y^r = x^{\epsilon}$, então

$$\lambda(ux^{\epsilon}x^{-\epsilon}v) = \lambda(ux^{\epsilon}x^{-\epsilon}x^{\epsilon}) = \lambda(ux^{\epsilon}) = \lambda(uv),$$

caso contrário temos duas possibilidades: se $\lambda(u)$ é da forma wy^{-r}, então

$$\lambda(ux^{\epsilon}x^{-\epsilon}) = \lambda(u) = wy^{-r},$$

logo

$$\begin{aligned}\lambda(ux^{\epsilon}x^{-\epsilon}v) = \lambda(ux^{\epsilon}x^{-\epsilon}y^r) = w \quad &\text{(pela definição de } \lambda) \\ = \lambda(uy^r) = \lambda(uv).&\end{aligned}$$

Se $\lambda(u)$ não é da forma wy^{-r}, então $\lambda(ux^{\epsilon}x^{-\epsilon})$ não é da forma wy^{-r}, logo

$$\lambda(ux^{\epsilon}x^{-\epsilon}v) = \lambda(ux^{\epsilon}x^{-\epsilon}y^r) = \lambda(ux^{\epsilon}x^{-\epsilon})y^r = \lambda(u)y^r = \lambda(uy^r) = \lambda(uv).$$

Agora, se v tem comprimento $n \geqslant 1$, $v = wy^r$ com w de comprimento $n-1$, então pela hipótese indutiva,

$$\lambda(ux^{\epsilon}x^{-\epsilon}w) = \lambda(uw).$$

Se $\lambda(uw) = hy^{-r}$, então

$$\lambda(ux^{\epsilon}x^{-\epsilon}v) = \lambda(ux^{\epsilon}x^{-\epsilon}wy^r) = h = \lambda(uwy^r) = \lambda(uv).$$

Se $\lambda(uw)$ não é da forma hy^{-r} então $\lambda(ux^{\epsilon}x^{-\epsilon}w)$ não é da forma hy^{-r}, logo

$$\lambda(ux^{\epsilon}x^{-\epsilon}v) = \lambda(ux^{\epsilon}x^{-\epsilon}wy^r) = \lambda(ux^{\epsilon}x^{-\epsilon}w)y^r = \lambda(uw)y^r = \lambda(uwy^r) = \lambda(uw).$$

Assim, se w' é obtida de w por redução então $\lambda(w) = \lambda(w')$, logo, se $w \sim w''$ então $\lambda(w) = \lambda(w'')$. Em particular, se $w \sim w''$ e w, w'' são reduzidas, temos que

$$w = \lambda(w) = \lambda(w'') = w''.$$

Portanto, os elementos de $F(X)$ tem no máximo uma palavra reduzida e como $\lambda(w)$ é reduzida e obtida de w por redução para toda palavra w então $\lambda(w) \in [w]$, logo cada elemento de $F(X)$ tem pelo menos uma palavra reduzida.

□

Teorema 3.2. *Seja X um conjunto, e $i : X \to F(X)$ dada por $i(x) = [x]$, então $(F(X), i)$ é livre sobre X.*

Demonstração. Seja H um grupo e $f : X \to H$ uma aplicação de conjuntos. Seja

$$\phi : F(X) \to H$$

dada por

$$\phi([x_{i_1}^{e_1} \cdots x_{i_n}^{e_n}]) = f(x_{i_1})^{e_1} \cdots f(x_{i_n})^{e_n},$$

ϕ está bem definida pois se $x_{i_1}^{e_1} \cdots x_{i_{r-1}}^{e_{r-1}} x_{i_{r+2}}^{e_{r+2}} \cdots x_{i_n}^{e_n}$ é obtida de $x_{i_1}^{e_1} \cdots x_{i_n}^{e_n}$ por redução elementar, onde $i_r = i_{r+1}$ e $e_r = -e_{r+1}$, então

$$f(x_{i_1})^{e_1} \cdots f(x_{i_n})^{e_n} = f(x_{i_1})^{e_1} \cdots f(x_{i_{r-1}})^{e_{r-1}} f(x_{i_{r+2}})^{e_{r+2}} \cdots f(x_{i_n})^{e_n}.$$

É claro que ϕ é um homomorfismo e $f = \phi \circ i$. Como $F(X)$ é gerado por $i(X)$, temos a unicidade de ϕ. □

Como consequência das proposições anteriores podemos assumir X como um subconjunto de $F(X)$ e i sendo a inclusão. Também, podemos identificar os elementos de $F(X)$ com a correspondente palavra reduzida.

Agora, podemos mostrar formalmente a interpretação dos grupos livres que foi dada inicialmente.

Proposição 3.3. *Seja G um grupo, X um conjunto e $j : X \to G$ uma aplicação de conjuntos, então são equivalentes:*

(i) (G, j) é livre sobre X;

(ii) G é gerado por $j(X)$ e se $j(x_{i_1})^{e_1} \cdots j(x_{i_n})^{e_n} = 1$, então para todo grupo H e $f : X \to H$, $f(x_{i_1})^{e_1} \cdots f(x_{i_n})^{e_n} = 1$.

Demonstração. $(i) \Rightarrow (ii)$. Pela Proposição 3.1 existe um isomorfismo

$$\phi : F(X) \to G,$$

tal que $j = \phi \circ i$, assim, como $F(X)$ é gerado por $i(X)$, então G é gerado por $\phi(i(X)) = j(X)$.
Se

$$j(x_{i_1})^{e_1} \cdots j(x_{i_n})^{e_n} = 1$$

então dados um grupo H e $f : X \to H$, temos que como (G, j) é livre sobre X, existe $\psi : G \to H$ tal que $f = \psi \circ j$, logo

$$f(x_{i_1})^{e_1} \cdots f(x_{i_1})^{e_1} = \psi(j(x_{i_1}))^{e_1} \cdots \psi(j(x_{i_1}))^{e_1} = \psi(j(x_{i_1})^{e_1} \cdots j(x_{i_1})^{e_1}) = \psi(1) = 1.$$

$(ii) \Rightarrow (i)$. Seja H um grupo e $f : X \to H$. Dado $g \in G$, $g = j(x_{i_1})^{e_1} \cdots j(x_{i_n})^{e_n}$, pois $j(X)$ gera G. Definimos

$$\phi : G \to H \text{ por } \phi(g) = f(x_{i_1})^{e_1} \cdots f(x_{i_n})^{e_n}.$$

Vejamos que ϕ está bem definida.

$$\begin{aligned} & j(x_{i_1})^{e_1} \cdots j(x_{i_n})^{e_n} = j(x_{r_1})^{t_1} \cdots j(x_{r_m})^{t_m} \\ \Rightarrow \quad & j(x_{i_1})^{e_1} \cdots j(x_{i_n})^{e_n} j(x_{r_m})^{-t_m} \cdots j(x_{r_1})^{-t_1} = 1 \\ \Rightarrow \quad & f(x_{i_1})^{e_1} \cdots f(x_{i_n})^{e_n} f(x_{r_m})^{-t_m} \cdots f(x_{r_1})^{-t_1} = 1 \\ \Rightarrow \quad & f(x_{i_1})^{e_1} \cdots f(x_{i_n})^{e_n} = f(x_{r_1})^{t_1} \cdots f(x_{r_m})^{t_m}. \end{aligned}$$

Claramente, ϕ é um homomorfismo. Também, $\phi(j(x)) = f(x)$ para todo $x \in X$, então $f = \phi \circ j$. Como $j(X)$ gera G temos a unicidade de ϕ. Assim, (G, j) é um grupo livre sobre X. □

Proposição 3.4. *Seja X um conjunto, então $F(X)$ é um grupo* ***residualmente finito****, ou seja, para todo $1 \neq w \in F(X)$, existe $N \lhd F(X)$ com $w \notin N$ e $F(X)/N$ finito.*

Demonstração. Seja

$$w = x_{i_1}^{e_1} \cdots x_{i_n}^{e_n} \in F(X)$$

uma palavra reduzida não vazia. Vamos encontrar um homomorfismo

$$\phi : F(X) \to S_{n+1}$$

tal que $\phi(w) \neq 1_{S_{n+1}}$, desta forma $w \notin ker(\phi) \lhd F(X)$ com $F(X)/ker(\phi) \cong Im(\phi) \subseteq S_{n+1}$ finito.
Seja

$$f : X \to S_{n+1}$$

definida por: $f(x) \equiv 1_{S_{n+1}}$, se $x \notin \{x_{i_1}, \ldots, x_{i_n}\}$. Se $x \in \{x_{i_1}, \ldots, x_{i_n}\}$, tomamos $f(x)$ como uma permutação que leva $r+1$ em r se $x = x_{i_r}$ e $e_r = 1$, e leva r em $r+1$ se $x = x_{i_r}$ e $e_r = -1$, para $r \leqslant n$; se as condições anteriores definem uma função injetora entre subconjuntos de $\{1, \ldots, n+1\}$, a permutação desejada $f(x)$ é qualquer extensão bijetora desta função. Assim, um número r não pode ter duas imagens pois estas seriam $r-1$ e $r+1$, que implica $x = x_{i_r}$, $e_r = -1$, $x = x_{i_{r-1}}$ e $e_{r-1} = 1$, que não é possível pois w é reduzida. Também, se um número s tem duas pré-imagens ($s-1$ e $s+1$) ocorreria $x = x_{i_s}$, $e_s = 1$, $x = x_{i_{r-1}}$ e $e_{s-1} = -1$, que de novo não é possível porque w é reduzida. Observamos então que mesmo se x aparecer mais de uma vez em w, $f(x)$ fica bem definida. Logo, a função f está bem definida, então existe um homomorfismo $\phi : F(X) \to S_{n+1}$, tal que

$$\phi(x) = f(x) \text{ para todo } x \in X.$$

Temos que $\phi(w) \neq 1$, pois

$$(\phi(w))(n+1) = (\phi(x_{i_1}^{e_1} \cdots x_{i_n}^{e_n}))(n+1) = (\phi(x_{i_1})^{e_1} \cdots \phi(x_{i_n})^{e_n})(n+1) = 1.$$

O último vale pois

$$\phi(x_{i_n}^{e_n})(n+1) = n, \phi(x_{i_{n-1}}^{e_{n-1}})(n) = n-1, \ldots, \phi(x_{i_1}^{e_1})(2) = 1.$$

□

Proposição 3.5. *Se G é um grupo residualmente finito e finitamente gerado, então ele é* ***hopfiano****, ou seja, todo homomorfismo sobrejetor $f : G \to G$ é automorfismo. Em particular, se X é um conjunto finito, $F(X)$ é hopfiano.*

Demonstração. Seja

$$\alpha : G \to G$$

um homomorfismo sobrejetor. Suponhamos que α não é automorfismo, então $ker(\alpha) \neq 1$. Seja

$$1 \neq g \in ker(\alpha).$$

Como G é residualmente finito, existe

$$N \lhd G, \text{ tal que } G/N \text{ finito e } g \notin N.$$

Seja

$$\varphi : G \to G/N \text{ a projeção canônica.}$$

Temos que $\varphi \circ \alpha^n$ é homomorfismo de G em G/N para todo $n \in \mathbb{N}$. Como G é finitamente gerado e G/N é finito, só podem existir número finito de homomorfismos de G em G/N, logo

$$\varphi \circ \alpha^n = \varphi \circ \alpha^m \text{ para alguns } n > m.$$

Observamos que α^m é sobrejetor pois α é, logo existe $h \in G$ tal que

$$\alpha^m(h) = g, \text{ então } (\varphi \circ \alpha^m)(h) = \varphi(g) \neq 1,$$

mas

$$(\varphi \circ \alpha^n)(h) = (\varphi \circ \alpha^{n-m})(g) = \varphi(1) = 1,$$

obtendo uma contradição. □

Proposição 3.6. *Sejam X, Y conjuntos, então $F(X) \cong F(Y) \iff |X| = |Y|$.*

Demonstração. ($\Leftarrow$) Seja

$$f : X \to Y$$

uma bijeção, então existe um único homomorfismo

$$\phi : F(X) \to F(Y)$$

que estende f e um único homomorfismo

$$\psi : F(Y) \to F(X)$$

que estende f^{-1}. Logo,

$$id_{F(X)}, \phi \circ \psi : F(X) \to F(X)$$

são homomorfismos que são extensões de $id_X : X \to X$, e

$$id_{F(Y)}, \psi \circ \phi : F(Y) \to F(Y)$$

são homomorfismos que são extensões de $id_Y : Y \to Y$. Assim, $id_{F(X)} = \phi \circ \psi$ e $id_{F(Y)} = \psi \circ \phi$, então ϕ é isomorfismo.

($\Rightarrow$) Considerando a quantidade de homomorfismos de $F(X)$ em $\mathbb{Z}_2$, temos que esta é igual ao número de funções de X em $\mathbb{Z}_2$, logo

$$|Hom(F(X), \mathbb{Z}_2)| = 2^{|X|}.$$

Como $F(X) \cong F(Y)$ temos então que

$$2^{|X|} = |Hom(F(Y), \mathbb{Z}_2)| = 2^{|Y|},$$

então se X ou Y for finito, temos que $|X| = |Y|$.
Se X, Y são infinitos, usando o Axioma da Escolha pode se provar que $|M(X \cup X^{-1})| = |X \cup X^{-1}|$, e dado que X é infinito temos $|X \cup X^{-1}| = |X|$, logo

$$|M(X \cup X^{-1})| = |X|.$$

Como $F(X)$ é o conjunto das classes de equivalência da relação $\sim$ em $M(X \cup X^{-1})$, temos $|F(X)| \leqslant |X|$ e é claro que $|X| \leqslant |F(X)|$, então

$$|X| = |F(X)| = |F(Y)| = |Y|.$$

□

Apresentamos agora uma definição equivalente do que é um grupo livre.

Definição 3.2. *Um grupo G é dito* ***grupo livre****, se G é isomorfo a $F(X)$ para algum conjunto X. Neste caso, se $i : F(X) \to G$ é um isomorfismo, $i(X)$ é chamado de* ***base*** *e o número de elementos de uma base $|i(X)| = |X|$ é chamado de* ***posto*** *de G.*

Note que o posto está bem definido pois se A, B são bases de G, existem conjuntos X, Y e isomorfismos $i : F(X) \to G$, $j : F(Y) \to G$ tais que $A = i(X)$ e $B = j(Y)$. Assim $F(X) \cong F(Y)$, e pela proposição 3.6, $|X| = |Y|$ que implica $|A| = |B|$, e toda bijeção $f : A \to B$ se estende a um automorfismo em G. Reciprocamente, se ϕ for um automorfismo tem se que $\phi(A)$ também é base de G, pois $\phi \circ i : F(X) \to G$ é isomorfismo e $(\phi \circ i)(X) = \phi(A)$.

Vamos ver agora que a definição acima é de fato equivalente à Definição 3.1 e que se G é um grupo livre com base $X \subseteq G$, ele pode se identificado como o conjunto das palavras reduzidas em X.

Proposição 3.7. *Seja G um grupo e $X \subseteq G$. Então são equivalentes:*

(i) *G é livre sobre X.*

(ii) *G é livre com base X.*

(iii) *Todo elemento $w \in G$ se escreve de forma única como $w = x_{i_1}^{e_1} \cdots x_{i_n}^{e_n}$, onde $n \geqslant 0$, $x_{i_r} \in X$, $e_r = \pm 1$ e $e_{r+1} \neq -e_r$ quando $i_{r+1} = i_r$.*

(iv) *G é gerado por X e $1 \neq x_{i_1}^{e_1} \cdots x_{i_n}^{e_n}$ para todo $n > 0, x_{i_r} \in X$ e $e_r = \pm 1$, onde $e_{r+1} \neq -e_r$ quando $i_{r+1} = i_r$.*

Demonstração. $(i) \Rightarrow (ii)$ Como G é livre sobre X, e $F(X)$ também é livre sobre X, então pela Proposição 3.1, existe um isomorfismo

$$\phi : F(X) \to G \text{ tal que } \phi(X) = X,$$

logo X é uma base de G.

$(ii) \Rightarrow (i)$ Se G é livre com base X, então existe um conjunto Y e um isomorfismo

$$\phi : F(Y) \to G$$

tal que $\phi(Y) = X$. Como $|X| = |Y|$ existe um isomorfismo

$$\psi : F(X) \to F(Y)$$

com $\psi(X) = Y$ pela Proposição 3.6, logo

$$\phi \circ \psi : F(X) \to G$$

é um isomorfismo, com $(\phi \circ \psi)(X) = X$. Assim, dado que $F(X)$ é livre sobre X, temos que G é livre sobre X pela proposição 3.1.

$(iii) \Rightarrow (iv)$ É imediato.

$(iv) \Rightarrow (iii)$ Como G é gerado por X, todo elemento de G se escreve como em (iii), e se um elemento $w \in G$ se escreve de duas formas, $w = x_{i_1}^{e_1} \cdots x_{i_n}^{e_n} = x_{j_1}^{t_1} \cdots x_{j_m}^{t_m}$, onde $n, m \geqslant 0$, $x_{i_r}, x_{j_s} \in X$, $e_r = \pm 1, t_s = \pm 1$, $e_{r+1} \neq -e_r$ quando $i_{r+1} = i_r$ e $e_{s+1} \neq -e_s$ quando $j_{s+1} = j_s$, então $1 = ww^{-1} = x_{i_1}^{e_1} \cdots x_{i_n}^{e_n} x_{j_m}^{-t_m} \cdots x_{j_1}^{-t_1}$, logo $n = m, i_r = j_r, e_r = t_r$ com $r = 1, \ldots, n$.

$(i) \Rightarrow (iii)$ Como $F(X)$ satisfaz (iii), então G também, pois é livre sobre X.

$(iv) \Rightarrow (ii)$ Seja $\phi : F(X) \to G$ o homomorfismo que estende à função $x \mapsto x$ definida em X. ϕ é sobrejetora porque G é gerado por X, e ϕ é injetora pois (iv) implica que $ker(\phi) = 1$. Então ϕ é isomorfismo e $\phi(X) = X$. □

Como consequência imediata de (iv) na proposição anterior, temos que se G é livre sobre X e $Y \subseteq X$ então $\langle Y \rangle$ é livre sobre Y.

Definição 3.3. *Seja F um grupo livre sobre X e $g = x_{i_1}^{e_1} \cdots x_{i_n}^{e_n} \in F$ uma palavra reduzida. Dizemos que g é **ciclicamente reduzida** se $i_1 \neq i_n$ ou $i_1 = i_n$ com $e_1 \neq -e_n$.*

Segue da definição anterior que se $g \in F$ é ciclicamente reduzida, então g^n é ciclicamente reduzida e $|g^n| = n|g|$ para todo $n \in \mathbb{N}$.

Proposição 3.8. *Todo elemento de um grupo livre F é conjugado de uma palavra ciclicamente reduzida, ou seja, para todo $g \in F$, $g = uvu^{-1}$, onde $u, v \in F$ e v é ciclicamente reduzida.*

Demonstração. O resultado é claro quando $|g| \leqslant 1$. Seja $g = x_{i_1}^{e_1} \cdots x_{i_n}^{e_n}$ reduzida com $n \geqslant 2$. Se g é ciclicamente reduzida então definimos $u = 1, v = g$. Se g não é ciclicamente reduzida, então $x_{i_1} = x_{i_n}$ e $e_1 = -e_n$, tomando $u_0 = x_{i_1}^{e_1}$ temos que $g = u_0 v_0 u_0^{-1}$, onde $|v_0| < |g|$, pois $g = x_{i_1}^{e_1} \cdots x_{i_n}^{e_n}$ é reduzida, o resultado segue por indução sobre $|g|$. □

Proposição 3.9. *Os grupos livres são **livres de torção**.*

Demonstração. Seja F um grupo livre e $g \in F$ com $g \neq 1$. Pela proposição anterior, existem $u, h \in F$ tais que $g = uhu^{-1}$, com h ciclicamente reduzida. Como $g \neq 1$, então $h \neq 1$, logo $|h| > 0$. Assim, $|h^n| = n|h| > 0$ para todo $n > 0$. Então $h^n \neq 1$, obtendo $g^n = uh^n u^{-1} \neq 1$ para todo $n > 0$. □

Proposição 3.10. *Todo grupo é quociente de um grupo livre.*

Demonstração. Seja G um grupo, então existe um homomorfismo

$$\phi : F(G) \to G$$

que estende o mapa identidade de G, $g \mapsto g$. Claramente ϕ é sobrejetor, logo $G = Im(\phi) \cong F(G)/ker(\phi)$. □

3.2 Grupos finitamente apresentáveis

Definição 3.4. *Uma* ***apresentação*** *de um grupo G consiste de um conjunto X, um epimorfismo de grupos*

$$\phi : F(X) \to G$$

e um conjunto $R \subseteq F(X)$ tais que

$$ker(\phi) = \langle R \rangle^{F(X)}$$

Nesta situação,

$$G \cong F(X)/\langle R \rangle^{F(X)} \text{ e escrevemos } G = \langle X \,|\, R \rangle^{\phi}.$$

Os elementos de X são chamados de ***símbolos geradores*** *de G, e as expressões de tipo $u = v$, onde $u, v \in F(X)$ e $uv^{-1} \in ker(\phi)$ são chamadas de* ***relações*** *em G. Assim, cada elemento $u \in ker(\phi)$ tem uma relação correspondente $u = 1$.*

Quando X e R são finitos, dizemos que $\langle X \,|\, R \rangle$ é uma ***apresentação finita*** *de G e que G é* ***finitamente apresentável****.*

É comum omitir a função ϕ quando ela é o mapa natural de $F(X)$ a $F(X)/\langle R \rangle^{F(X)}$ ou quando é injetora em X (e consideramos X como subconjunto de G), e escrevemos

$$G = \langle X \,|\, R \rangle.$$

Às vezes é conveniente escrever os elementos de $r \in R$ como a sua relação correspondente $r = 1$ ou alguma equivalente de tipo $u = v$, com $uv^{-1} = r$.

Exemplo 3.2. *O grupo trivial tem apresentação $\langle \varnothing \,|\, \varnothing \rangle$. Também é fácil ver que a apresentação*

$$\langle x, y \,|\, x^3 = 1, y^2 = 1, xy = 1 \rangle$$

corresponde igualmente ao grupo trivial. De fato, como $y = x^{-1}$ temos que

$$|x| = |y| \text{ deve ser divisor de } 2 \text{ e de } 3 \implies |x| = 1 \implies x = 1.$$

Exemplo 3.3. *O grupo dos números inteiros $(\mathbb{Z}, +)$ tem apresentação $\langle x \,|\, \varnothing \rangle$.*

Exemplo 3.4. *$\langle x \,|\, x^n \rangle$ é uma apresentação do grupo $\mathbb{Z}_n$.*

Exemplo 3.5. *$\langle x_1, \ldots, x_n \,|\, x_i x_j = x_j x_i, 1 \leqslant i < j \leqslant n \rangle$ é uma apresentação do grupo $\mathbb{Z}^n = \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{n-vezes}$.*

Teorema 3.3. (von Dyck). *Sejam G, H grupos com*

$$G = \langle X \mid R \rangle^{\phi},$$

$f : X \to H$ aplicação de conjuntos, e

$$\theta : F(X) \to H$$

o homomorfismo que estende f.
Então se $\theta(r) = 1$ para todo $r \in R$, existe um homomorfismo

$$\psi : G \to H \text{ tal que } \psi(\phi(x)) = f(x) \text{ para todo } x \in X.$$

Além disso, se $H = \langle f(X) \rangle$ então ψ é epimorfismo.

Demonstração. Suponhamos $\theta(r) = 1$ para todo $r \in R$, então $R \subseteq ker(\theta)$, logo

$$ker(\phi) = \langle R \rangle^{\phi} \subseteq ker(\theta).$$

Então para cada $g \in G$ definimos

$$\psi(g) = \theta(w),$$

onde w é qualquer elemento de $F(X)$ tal que $\phi(w) = g$ (que existe pois ϕ é sobrejetora). Vejamos que ψ está bem definida. Se $\phi(w_1) = \phi(w_2) = g$, então $1 = \phi(w_1)\phi(w_2)^{-1} = \phi(w_1 w_2^{-1})$, logo $w_1 w_2^{-1} \in ker(\phi) \subseteq ker(\theta)$, assim $\theta(w_1 w_2^{-1}) = 1$ e portanto $\theta(w_1) = \theta(w_2)$.

Observamos que ψ é homomorfismo pois se $g_1, g_2 \in G$ com $\phi(w_1) = g_1, \phi(w_1) = g_2$ então $\phi(w_1 w_2) = g_1 g_2$, logo $\psi(g_1 g_2) = \theta(w_1 w_2) = \theta(w_1)\theta(w_2) = \psi(w_1)\psi(w_2)$.

É claro que $\psi(G) = \theta(F(X)) = \langle f(X) \rangle$, então se $H = \langle f(X) \rangle$, ψ é epimorfismo. □

O teorema anterior pode ser visto como um caso particular do Teorema 1.5 considerando $K = F(X)$, $v = \phi$ (portanto $\langle R \rangle^K = ker(\phi)$ e $K/\langle R \rangle^K \cong G$).

Exemplo 3.6. *Dados dois conjuntos X, Y, e $R \subseteq F(X)$, $S \subseteq F(X \cup Y)$. A inclusão $X \overset{i}{\hookrightarrow} X \cup Y$ induz um homomorfismo*

$$\langle X \mid R \rangle \to \langle X \cup Y \mid R \cup S \rangle$$

segundo o teorema anterior.
Em termos do enunciado do teorema anterior,

$$H = \langle X \cup Y \mid R \cup S \rangle,$$

ϕ é a projeção natural de $F(X)$ em $\langle X \mid R\rangle$ e $f = \pi \circ i$ onde π é a projeção natural de $F(X \cup Y)$ em $\langle X \cup Y \mid R \cup S\rangle$. Vemos que se θ é o homomorfismo que estende f e $r = x_{i_1}^{e_1} \cdots x_{i_n}^{e_n} \in R$, então

$$\theta(r) = \theta(x_{i_1})^{e_1} \cdots \theta(x_{i_n})^{e_n} = f(x_{i_1})^{e_1} \cdots f(x_{i_n})^{e_n} = \pi(x_{i_1})^{e_1} \cdots \pi(x_{i_n})^{e_n} = \pi(r) = 1$$

pois $r \in R \subseteq R \cup S$.

Agora vamos ver como comparar apresentações do mesmo grupo.

Definição 3.5. *Seja G um grupo e $\langle X \mid R\rangle^{\phi}$ uma apresentação de G. Se $S \subseteq \langle R\rangle^{F(X)}$ então $\langle X \mid R \cup S\rangle^{\phi}$ também é apresentação de G. Neste caso dizemos que*

$$\langle X \mid R \cup S\rangle^{\phi} \text{ é uma } \textbf{\textit{transformação geral de Tietze Tipo I}} \text{ de } \langle X \mid R\rangle^{\phi},$$

e

$$\langle X \mid R\rangle^{\phi} \text{ é uma } \textbf{\textit{transformação de Tietze geral Tipo I'}} \text{ de } \langle X \mid R \cup S\rangle^{\phi}.$$

*Quando $|S| = 1$ falamos de **transformações de Tietze simples**.*

Proposição 3.11. *Seja $G = \langle X \mid R\rangle^{\phi}$ e Y um conjunto tal que $X \cap Y = \varnothing$. Para cada $y \in Y$ seja $u_y \in F(X)$, então*

$$\langle X \cup Y \mid R \cup \{yu_y^{-1} : y \in Y\}\rangle^{\psi}$$

é uma apresentação de G, onde

$$\psi : F(X \cup Y) \to G$$

é o homomorfismo de grupos que estende a função $z \mapsto \begin{cases} \phi(z) & \text{se } z \in X \\ \phi(u_y) & \text{se } z \in Y \end{cases}$.

Demonstração. Seja

$$N = \langle R \cup \{yu_y^{-1} : y \in Y\}\rangle^{F(X \cup Y)}.$$

Dado $r \in R$, como $R \subseteq F(X)$ sabemos que $\psi(r) = \phi(r) = 1$. Se $y \in Y$, temos que

$$\psi(yu_y^{-1}) = \psi(y)\psi(u_y)^{-1} = \phi(u_y)\phi(u_y)^{-1} = 1.$$

Então pelo Teorema 1.5 existe um homomorfismo

$$\tilde{\psi} : F(X \cup Y)/N \to G$$

tal que $\psi(w) = \tilde{\psi}(Nw)$ para todo $w \in F(X \cup Y)$. Claramente ψ é epimorfismo, então $\tilde{\psi}$ também é.

De outro lado, seja

$$\pi : X \to F(X \cup Y)/N$$

a restrição a X da projeção canônica de $F(X \cup Y)$ em N e $\tilde{\pi}$ o homomorfismo que estende π a $F(X)$, então

$$\tilde{\pi}(r) = Nr = N.$$

Então pelo Teorema de von Dyck, existe um homomorfismo

$$\theta : G \to F(X \cup Y)/N$$

tal que $\theta(\phi(x)) = \pi(x) = Nx$ para todo $x \in X$. Como $F(X \cup Y)/N$ é gerado por $\{Nx : x \in X\}$ (pois $F(X \cup Y)$ é gerado por $X \cup Y$ e se $y \in Y$, $Ny = Nu_y$ onde $u_y \in F(X)$) então θ é um epimorfismo.

Agora, $\tilde{\psi} \circ \theta$ é a identidade em G, pois $G = \langle \phi(X) \rangle$ e

$$\tilde{\psi}(\theta(\phi(x))) = \tilde{\psi}(Nx) = \psi(x) = \phi(x).$$

Também, $\theta \circ \tilde{\psi}$ é a identidade em $F(X \cup Y)/N$ pois $F(X \cup Y)/N$ é gerado por $\{Nx : x \in X\}$ e

$$\theta(\tilde{\psi}(Nx)) = \theta(\psi(x)) = \theta(\phi(x)) = Nx.$$

Portanto $\tilde{\psi}$ é isomorfismo, assim,

$$\psi(w) = 1 \iff \tilde{\psi}(Nw) = 1 \iff Nw = 1 \iff w \in N,$$

logo $ker(\psi) = N$. □

Definição 3.6. *Na situação da proposição anterior, dizemos que*

$$\langle X \cup Y \mid R \cup \{yu_y^{-1} : y \in Y\} \rangle^{\psi}$$

é uma ***transformação geral de Tietze Tipo II*** *de* $\langle X \mid R \rangle^{\phi}$*, e*

$$\langle X \mid R \rangle^{\phi}$$

é uma ***transformação de Tietze geral Tipo II'*** *de* $\langle X \cup Y \mid R \cup \{yu_y^{-1} : y \in Y\} \rangle^{\psi}$*. Quando* $|Y| = 1$ *falamos de* ***transformações de Tietze simples****.*

Note-se que uma transformação de Tietze geral pode se obter, no caso que $|S|$ ou $|Y|$ sejam finitos, por meio de um número finito de transformações de Tietze simples do tipo correspondente.

Teorema 3.4. *Sejam $\langle X \mid R\rangle^{\phi}, \langle Y \mid S\rangle^{\psi}$ duas apresentações de um grupo G. Então $\langle Y \mid S\rangle^{\psi}$ pode se obtida a partir de $\langle X \mid R\rangle^{\phi}$ por meio de um número finito de transformações de Tietze gerais (ou simples no caso que ambas apresentações forem finitas).*

Demonstração. Suponhamos que $X \cap Y = \varnothing$. Para cada $y \in Y$ seja

$$u_y \in F(X) \text{ tal que } \psi(y) = \phi(u_y)$$

e para cada $x \in X$,

$$v_x \in F(Y) \text{ tal que } \phi(x) = \psi(v_x).$$

Seja

$$\theta : F(X \cup Y) \to G$$

o homomorfismo de grupos que estende a função

$$z \mapsto \begin{cases} \phi(z) & \text{se } z \in X \\ \phi(u_y) & \text{se } z \in Y \end{cases}.$$

Então pela Proposição 3.11

$$\langle X \cup Y \mid R \cup \{yu_y^{-1} : y \in Y\}\rangle^{\theta}$$

é uma apresentação de G, obtida de $\langle X \mid R\rangle$ por uma transformação de Tietze geral tipo II.

Agora, para todo $y \in Y$

$$\theta(y) = \phi(u_y) = \psi(y),$$

logo $\theta(w) = \psi(w)$ para todo $w \in F(Y)$. Então para $s \in S$,

$$\theta(s) = \psi(s) = 1.$$

Além disso, para todo $x \in X$,

$$\theta(v_x) = \psi(v_x) = \phi(x).$$

Portanto

$$\langle X \cup Y \mid R, S, \{yu_y^{-1} : y \in Y\}, \{xv_x^{-1} : x \in X\}\rangle^{\theta}$$

é uma apresentação de G, obtida da anterior por meio de uma Transformação geral de Tietze tipo I.

Por simetria, esta última também vem de $\langle Y \mid S\rangle^{\psi}$ por transformações de Tietze gerais de tipo II e I. Logo $\langle Y \mid S\rangle^{\psi}$ vem de $\langle X \mid R\rangle^{\phi}$ por transformações de Tietze gerais

de tipo II, I, I' e II'.

No caso geral que $X \cap Y \neq \varnothing$, tomamos um conjunto X' bijetivo com X, tal que

$$X' \cap Y = \varnothing = X' \cap X.$$

Claramente, $\langle X' \,|\, R' \rangle^{\phi'}$ é uma apresentação de G, onde cada elemento de R' é obtido substituindo cada $x \in X$ pelo respectivo $x' \in X'$, e $\phi'(x') = \phi(x)$. Usando o caso anterior temos que $\langle X' \,|\, R' \rangle^{\phi'}$ vem de ambos, $\langle Y \,|\, S \rangle^{\psi}$ e $\langle X \,|\, R \rangle^{\phi}$ por uma sequência finita de Transformações de Tietze gerais. □

Proposição 3.12. *Seja $\langle X \,|\, R \rangle^{\phi}$ uma apresentação de um grupo G que é finitamente gerado. Então existe um subconjunto finito $X_1 \subseteq X$ tal que G é gerado por $\phi(X_1)$.*

Demonstração. Seja $H \subseteq G$ um subconjunto finito que gera o grupo G. Então cada $h \in H$ é produto de número finito de elementos de $\phi(X)$ e seus inversos. Então existe $X_1 \subseteq X$ finito tal que $H \subseteq \langle \phi(X_1) \rangle$, logo G é gerado por $\phi(X_1)$. □

Proposição 3.13. *Sejam $\langle X \,|\, R \rangle^{\phi}$, $\langle Y \,|\, S \rangle^{\psi}$ apresentações de um grupo G. Se X, R e Y são finitos, então existe $S_1 \subseteq S$ finito tal que $\langle Y \,|\, S_1 \rangle^{\psi}$ é apresentação de G.*

Demonstração. Sejam θ, u_y, v_x como na demonstração do Teorema 3.4, de onde sabemos que

$$\langle X \cup Y \,|\, T \rangle^{\theta} \text{ é uma apresentação de } G \text{ com } T = R \cup \{y u_y^{-1} : y \in Y\}.$$

Agora,

$$\theta(x v_x^{-1}) = \theta(x)\theta(v_x)^{-1} = \phi(x)\psi(v_x)^{-1} = \phi(x)\phi(x)^{-1} = 1,$$

então

$$\langle X \cup Y \,|\, T \cup \{x v_x^{-1} : x \in X\} \rangle^{\theta}$$

é uma apresentação de G.

Para cada $t \in T$ seja t' a palavra obtida de t ao substituir cada elemento $x \in X$ que aparecer nela pelo respectivo v_x, e seja

$$T' = \{t' : t \in T\}.$$

Claramente $T' \subseteq F(Y)$. Sejam

$$N = \langle \{x v_x : x \in X\} \rangle^{F(X \cup Y)}$$

e

$$\pi : F(X \cup Y) \to F(X \cup Y)/N \text{ a projeção canônica.}$$

Então como $\pi(x) = \pi(v_x)$ para todo $x \in X$, temos que

$$Nt = \pi(t) = \pi(t') = Nt' \text{ para todo } t \in T.$$

Logo

$$T \subseteq NT' \subseteq \langle N \cup T' \rangle^{F(X \cup Y)} \text{ e } T' \subseteq NT \subseteq \langle N \cup T \rangle^{F(X \cup Y)}.$$

Como $T' \subseteq \langle N \cup T \rangle^{F(X \cup Y)}$, então

$$G = \langle X \cup Y \,|\, T, T', \{xv_x : x \in X\} \rangle^{\theta}$$

é uma transformação de Tietze geral tipo I da apresentação anterior de G. Como $T \subseteq \langle N \cup T' \rangle^{F(X \cup Y)}$, então

$$G = \langle X \cup Y \,|\, T', \{xv_x : x \in X\} \rangle^{\theta}$$

é uma transformação de Tietze geral tipo I' da anterior. Agora, para $y \in Y$, $\theta(y) = \phi(u_y) = \psi(y)$ e para $x \in X$, $\theta(x) = \phi(x) = \psi(v_x)$, além disso $T' \subseteq F(Y)$, portanto

$$G = \langle Y \,|\, T' \rangle^{\psi}$$

é uma transformação de Tietze geral tipo II' da anterior.

Como R, Y são finitos, então

$$T = R \cup \{yu_y^{-1} : y \in Y\} \text{ é finito,}$$

portanto T' é finito. Como $T' \subseteq \langle S \rangle^{F(Y)}$ (pois $G = \langle Y \,|\, S \rangle^{\psi}$) então os elementos de T são produtos de finitos elementos de S com seu inversos, então como T' é finito, existe um subconjunto finito $S_1 \subseteq S$ tal que $\langle T' \rangle^{F(Y)} \subseteq \langle S_1 \rangle^{F(Y)}$, mas

$$ker(\psi) = \langle T' \rangle^{F(Y)} = \langle S \rangle^{F(Y)} \supseteq \langle S_1 \rangle^{F(Y)},$$

logo $\langle S_1 \rangle^{F(Y)} = \langle T' \rangle^{F(Y)} = ker(\psi)$. Portanto $G = \langle Y \,|\, S_1 \rangle^{\psi}$. □

Proposição 3.14. *Seja G um grupo e $K \lhd G$ tal que K e G/K são finitamente apresentáveis, então G é finitamente apresentável.*

Demonstração. Sejam

$$K = \langle X \,|\, R \rangle, G/K = \langle Y \,|\, S \rangle$$

apresentações finitas. Seja

$$\pi : G \to G/K \text{ a projeção canônica.}$$

Seja

$$\theta : F(X \cup Y) \to G$$

o homomorfismo que satisfaz $\theta(x) = x$, para todo $x \in F(X)$ e $\theta(y)$ é algum elemento de $\pi^{-1}(y)$ para cada $y \in Y$ (logo $\pi(\theta(y)) = y$ em G/K).

Para cada $s \in S$ temos que $\pi(\theta(s)) = s = 1$ em G/K, logo $\theta(s) \in ker(\pi) = K$, assim

$$\theta(s) = u_s \text{ em } K \text{ para algum } u_s \in F(X).$$

Também, como $K \lhd G$, temos que $\forall x \in X, y \in Y$, $\theta(y^{-1}xy) = \theta(y)^{-1}x\theta(y) \in K$, pois $x \in K$. Então

$$\theta(y^{-1}xy) = w_{xy} \text{ para algum } w_{xy} \in F(X)$$

e

$$\theta(yxy^{-1}) = v_{xy} \text{ para algum } v_{xy} \in F(X).$$

Vejamos que

$$\langle X \cup Y \mid R \cup \{su_s^{-1} : s \in S\} \cup \{y^{-1}xyw_{xy}^{-1}, yxy^{-1}v_{xy}^{-1} : x \in X, y \in Y\}\rangle^{\theta}$$

é uma apresentação de G. Isto é, que θ é epimorfismo e $ker(\theta) = N$, onde

$$N = \langle R \cup \{su_s^{-1} : s \in S\} \cup \{y^{-1}xyw_{xy}^{-1}, yxy^{-1}v_{xy}^{-1} : x \in X, y \in Y\}\rangle^{F(X\cup Y)}.$$

A inclusão $N \subseteq ker(\theta)$ é clara pela definição de θ, u_s e w_{xy}.

Seja $w \in ker(\theta)$. Notamos que se $x \in X, y \in Y$,

$$Ny^{-1}xyw_{xy}^{-1} = N \text{ e } Nyxy^{-1}v_{xy}^{-1} = N$$

portanto $Ny^{-1}x = Nw_{xy}y^{-1}$ e $Nyx = Nv_{xy}y$. Assim,

$$Nw = Nw_1w_2,$$

onde $w_1 \in F(X), w_2 \in F(Y)$. Agora, como $N \subseteq ker(\theta)$ e $\theta(w) = 1$, temos que

$$1 = \theta(Nw) = \theta(Nw_1w_2) = \theta(w_1w_2).$$

Portanto, em G/K

$$1 = \pi(\theta(w_1w_2)) = \pi(\theta(w_1))\pi(\theta(w_2)) = \pi(w_1)w_2 = w_2,$$

então $w_2 \in \langle S\rangle^{F(Y)}$. Mas dados $y \in Y, s \in S$, temos que

$$Ny^{\pm 1}u_sy^{\mp 1} = Nv$$

para algum $v \in F(X)$, pois $Ny^{-1}xy = Nw_{xy}$ e $Nyxy^{-1} = Nv_{xy}$ para todo $x \in X$. Portanto, $Nw_2 = Nw_3$ para algum $w_3 \in F(X)$. Novamente, temos

$$Nw = Nw_1Nw_2 = Nw_1Nw_3 = Nw_1w_3,$$

e como $\theta(N) = 1 = \theta(w)$ temos que

$$1 = \theta(w) = \theta(w_1w_3),$$

então $w_1w_3 \in \langle R \rangle^{F(X)} \subseteq N$, portanto

$$N = Nw_1w_3 = Nw$$

ou seja, $w \in N$. Concluímos que $ker(\phi) = N$.

Por último, vejamos que θ é epimorfismo. Seja $H = \langle \theta(X), \theta(Y) \rangle$. Por construção temos $K = \langle \theta(X) \rangle \subseteq H$, $\pi(\theta(X)) \subseteq \pi(K) = 1$ e

$$\pi(H) = \langle \pi(\theta(X)), \pi(\theta(Y)) \rangle = \langle \pi(\theta(Y)) \rangle = \langle Y \rangle = G/K.$$

Portanto $H = G$. □

3.3 A função de Dehn de um grupo

Nesta seção definimos funções de Dehn e desigualdades isoperimétricas para um grupo, baseados em [3] e [5].

Dada uma apresentação finita

$$\langle X \mid R \rangle$$

de um grupo G (onde tratamos X como subconjunto de G), sabemos que os elementos de G podem ser representados como palavras em $X \cup X^{-1}$. Portanto é importante poder identificar quando uma palavra $w \in F(X)$ corresponde ao elemento identidade em G, ou seja, quando

$$w \in \langle R \rangle^{F(X)}.$$

Esta questão é conhecida como o *Problema da palavra* para G.

Nesta situação, precisamos usar as relações $r \in R$ para transformar a palavra w no elemento identidade em G, no seguinte sentido: se

$$r \equiv u_1 u_2 u_3 \in R$$

(u_i possivelmente vazia) e $w \equiv w_1 u_2^{\pm 1} w_2$, temos que $(u_3 u_1)^{-1} = u_2$ em G, logo

$$w = w_1 (u_3 u_1)^{\mp 1} w_2 \equiv w' \text{ em } G$$

e dizemos que w' foi ***obtida a partir de*** w ***usando a relação*** r.

Chamamos ***custo*** de obter w' a partir de w o número mínimo de vezes que deve se usar alguma relação para obter w' começando de w. Se obtemos a palavra vazia a partir de w por meio das relações $r \in R$, concluímos que

$$w = 1 \text{ em } G.$$

Assim, obter informação sobre o custo de converter uma palavra w de determinado comprimento na palavra vazia, está intimamente relacionado com obter uma solução ao problema da palavra em G.

Agora, suponhamos que $w' = w_1 (u_3 u_1)^{-1} w_2$ foi obtida de $w = w_1 u_2 w_2$ usando a relação $r = u_1 u_2 u_3$. Temos então que em $F(X)$, $u_1^{-1} r u_3^{-1} = u_2$, logo

$$\begin{aligned} w &= w_1 (u_1^{-1} r u_3^{-1}) w_2 = w_1 u_1^{-1} r u_3^{-1} u_3 u_1 w_1^{-1} w_1 (u_3 u_1)^{-1} w_2 \\ &= (u_1 w_1^{-1})^{-1} r (u_1 w_1^{-1}) w' \\ &= v_1^{-1} r v_1 w', \end{aligned}$$

com $v_1 = u_1 w_1^{-1}$. Igualmente, se w'' é obtida de w' usando a relação $r' \in R$, vamos obter que $w' = v_2^{-1}(r')^{\pm 1} v_2 w''$. Assim, se conseguirmos obter a palavra vazia a partir de w usando N relações em R, obtemos que

$$w = \prod_{i=1}^{N} v_i^{-1} r_i^{e_i} v_i, \quad \text{com} \quad e_i = \pm 1, v_i \in F(X), r_i \in R,$$

ou seja, $w \in \langle R \rangle^{F(X)}$.

Definição 3.7. *Seja $P \equiv \langle X \mid R \rangle$ uma apresentação finita do grupo G. $w \in F(X)$ é dita* ***homotopicamente nula*** *em G, se $w = 1$ em G. Definimos sua* ***área algébrica*** *como*

$$Area_a^P(w) = min\{N \in \mathbb{N} \mid w = \prod_{i=1}^{N} v_i^{-1} r_i^{e_i} v_i,\ e_i = \pm 1, v_i \in F(X), r_i \in R\}.$$

Assim, definimos a ***função de Dehn*** *da apresentação P como a função $\delta_P : \mathbb{N} \to \mathbb{N}$ dada por*

$$\delta_P(n) := max\{Area_a^P(w) \mid w \in F(X) \text{ homotopicamente nula e } |w| \leqslant n\}.$$

Notamos então que $Area_a^P(w)$ representa o número mínimo de passos necessários para solucionar o problema da palavra no caso particular da palavra w. Assim, $\delta_P(n)$ dá conta da complexidade do problema da palavra no grupo correspondente à apresentação P.

Exemplo 3.7. *Consideremos as seguintes apresentações do grupo $\mathbb{Z}$. $P_1 = \langle x \mid \varnothing \rangle$, $P_2 = \langle x, y \mid y \rangle$, temos que $\delta_{P_1}(n) = 0$ e $\delta_{P_2}(n) = n$, para todo $n \in \mathbb{N}$.*

Do exemplo anterior, observamos que duas apresentações de um mesmo grupo podem ter diferentes funções de Dehn, mas elas são equivalentes no seguinte sentido.

Definição 3.8. *Dadas duas funções*

$$f, g : [0, \infty) \to [0, \infty),$$

dizemos que f é ***dominada assintoticamente*** *por g, se*

$$\text{existe } C > 0 \text{ tal que } f(l) \leqslant Cg(Cl + C) + Cl + C \text{ para todo } l \geqslant 0$$

e denotamos isto por $f \preceq g$. Dizemos que

$$f, g \text{ são } \textbf{\textit{equivalentes assintoticamente}} \text{ se } f \preceq g \text{ e } g \preceq f$$

e denotamos isto por $f \simeq g$.

Proposição 3.15. *As funções de Dehn de duas apresentações finitas do mesmo grupo são equivalentes assintoticamente.*

Demonstração. Seja G um grupo e $P \equiv \langle X \mid R \rangle$ uma apresentação finita de G. Por causa do Teorema 3.4, basta ver o que acontece com as funções de Dehn das apresentações dadas por transformações de Tietze simples de P.

Assim, consideramos primeiro a apresentação de G,

$$P' \equiv \langle X \mid R \cup \{r'\} \rangle, \text{ onde } r' \in \langle R \rangle^{F(X)}.$$

Temos então que

$$r' = \prod_{i=1}^{m} v_i^{-1} r_i v_i, \ v_i \in F(X), r_i \in R^{\pm 1}.$$

Agora, se $w \in \langle R \cup \{r'\} \rangle^{F(X)}$ temos que

$$w = \prod_{i=1}^{N} w_i^{-1} r_i' w_i, \ w_i \in F(X), r_i' \in (R \cup \{r'\})^{\pm 1}.$$

Substituindo r' pelo respectivo produto, temos que w se escreve como produto de máximo mN conjugados de elementos de R. Assim,

$$\text{para todo } n \in \mathbb{N} \text{ temos } \delta_P(n) \leqslant m\delta_{P'}(n).$$

Além disso,

$$\delta_{P'}(n) \leqslant \delta_P(n)$$

é claro, pois $R \subseteq R \cup \{r'\}$, logo $\delta_{P'} \simeq \delta_P$.

Consideramos agora a apresentação de G,

$$P'' \equiv \langle X \cup \{y\} \mid R \cup \{y u_y^{-1}\} \rangle$$

onde $u_y \in F(X)$. Sejam $M = |u_y|$ e $w \in F(X \cup Y)$ homotopicamente nula. Substituindo em w, y por u_y, obtemos uma palavra $w' \in F(X)$ com $|w'| \leqslant M|w|$, isto é, obtemos w' usando no máximo $|w|$ relações de $R \cup \{y u_y^{-1}\}$. E para obter a palavra vazia a partir de w' precisamos de usar no máximo $\delta_P(M|w|)$ relações de R, portanto

$$Area_a^{P''}(w) \leqslant \delta_P(M|w|) + |w|,$$

logo

$$\delta_{P''}(n) \leqslant \delta_P(Mn) + n$$

para todo $n \in \mathbb{N}$, obtendo $\delta_{P''} \preceq \delta_P$.

Agora, vejamos que $\delta_P \preceq \delta_{P''}$. Seja

$$\phi : F(X \cup \{y\}) \to F(X)$$

o homomorfismo de grupos que satisfaz $\phi(y) = u_y$ e $\phi(x) = x$ para todo $x \in X$. Se $w \in F(X)$ é homotopicamente nula, temos que

$$w = \prod_{i=1}^{N} v_i^{-1} r_i v_i, \text{ com } v_i \in F(X \cup \{y\}), r_i \in (R \cup \{y u_y^{-1}\})^{\pm 1}.$$

Então como $w \in F(X)$, temos que

$$w = \phi(w) = \prod_{i=1}^{m} w_i^{-1} r_i' w_i \quad \text{com } w_i \in F(X), r_i' \in R^{\pm 1} \text{ e } m \leqslant N$$

onde $\phi(v_i) = w_i, \phi(r_i) = r_i'$. Assim, $\delta_P(n) \leqslant \delta_{P''}(n)$ para todo $n \in \mathbb{N}$.

□

Definição 3.9. *Dado um grupo G finitamente apresentável, podemos falar agora da* ***função de Dehn*** *de G, δ_G sendo a função de Dehn de alguma das suas apresentações a menos de $\simeq$ equivalência. Dizemos que G satisfaz uma* ***desigualdade isoperimétrica*** *quadrática (ou linear, ou exponencial, etc...) se $\delta_G(n) \preceq n^2$ (ou $\preceq n$, ou $\preceq 2^n$, etc...; respectivamente).*

Exemplo 3.8. *Uma classe importante de grupos são os chamados* ***grupos hiperbólicos****, que podem se definir de forma alternativa, como os grupos finitamente apresentáveis que tem função de Dehn linear ($\simeq n$). Como caso particular, temos que grupo livre $F(X)$ com X finito é hiperbólico pois $\delta_{F(X)}(n) \simeq n$.*

Exemplo 3.9. *Para o grupo abeliano $\mathbb{Z}^k$ com $k \geqslant 2$, temos que sua função de Dehn é $\delta_{\mathbb{Z}^k}(n) \simeq n^2$.*

4 A função de Dehn do grupo metabeliano de Baumslag

Nesta seção vamos estudar com detalhe o artigo [7], sobre a função de Dehn e algumas propriedades do grupo metabeliano de Baumslag.

4.1 O grupo de Baumslag

Definição 4.1. *O* ***grupo de Baumslag*** Γ *está dado pela seguinte apresentação*

$$\langle a, s, t \,|\, [a, a^t] = 1, [s, t], a^s = aa^t \rangle,$$

lembrando que

$$[x, y] = x^{-1}y^{-1}xy \text{ e } x^y = y^{-1}xy,$$

onde x, y são elementos de um grupo. Também, acrescentando em Γ a relação $a^m = 1$ para $m \geqslant 2$, definimos a família de grupos

$$\Gamma_m = \langle a, s, t \,|\, [a, a^t] = 1, [s, t], a^s = aa^t, a^m = 1 \rangle.$$

Lema 4.1. *O subgrupo normal de Γ gerado por a, $A = \langle a \rangle^\Gamma$ é abeliano.*

Demonstração. Primeiro, vamos mostrar que $[a, a^{t^i}] = 1$ para cada $i > 0$ por indução sobre i.
Para $i = 1$ temos $[a, a^t] = 1$ pela definição de Γ. Suponhamos que dado $i \geqslant 2$ vale $[a, a^{t^j}] = 1$, para todo $1 \leqslant j < i$. Então

$$1 = 1^s = [a, a^{t^{i-1}}]^s = [a^s, a^{t^{i-1}s}] = [aa^t, a^{s(t^{i-1})}]. \tag{4.1}$$

A ultima igualdade vem do fato de que $[s, t] = 1$. Agora,

$$a^{s(t^{i-1})} = (a^s)^{t^{i-1}} = (aa^t)^{t^{i-1}} = a^{t^{i-1}}a^{t^i}$$

substituindo isto no ultimo termo de (4.1), temos que $1 = [aa^t, a^{t^{i-1}}a^{t^i}]$. Agora,

$$1 = [aa^t, a^{t^{i-1}}a^{t^i}] = [aa^t, a^{t^i}][aa^t, a^{t^{i-1}}]^{a^{t^i}}. \tag{4.2}$$

Olhamos para o termo $[aa^t, a^{t^i}]$:

$$[aa^t, a^{t^i}] = [a, a^{t^i}]^{a^t}[a^t, a^{t^i}] = [a, a^{t^i}]^{a^t}[a, a^{t^{i-1}}]^t = [a, a^{t^i}]^{a^t}1^t = [a, a^{t^i}]^{a^t}. \tag{4.3}$$

Para o termo $[aa^t, a^{t^{i-1}}]$ temos que

$$[aa^t, a^{t^{i-1}}] = [a, a^{t^{i-1}}]^{a^t}[a^t, a^{t^{i-1}}] = 1^{a^t}[a, a^{t^{i-2}}]^t = 1^t = 1. \tag{4.4}$$

Substituindo (4.3) e (4.4) em (4.2), temos então que

$$1 = [a, a^{t^i}]^{a^t} 1^{a^{t^i}} = [a, a^{t^i}]^{a^t},$$

portanto, $1 = [a, a^{t^i}]$.

Para $i < 0$ temos que $[a, a^{t^i}] = [a^{t^{-i}}, a]^{t^i}$, mas pelo provado anteriormente, temos que $[a, a^{t^{-i}}] = 1$, que implica $[a^{t^{-i}}, a] = 1$, assim $[a, a^{t^i}] = 1^{t^i} = 1$. Assim, $[a, a^{t^i}] = 1$ para todo $i \in \mathbb{Z}$.

Podemos ver que A é gerado como grupo por elementos da forma $a^{s^i t^j}$, $i, j \in \mathbb{Z}$. De fato, sabemos que A é gerado por elementos da forma a^u, com $u \in \Gamma$, mas u é produto de elementos da forma $va^k w$ com $k \in \mathbb{Z}$ e $v, w \in F(\{s, t\})$, e temos

$$a^{va^k w} = ((a^k)^{-1} a^v a^k)^w = ((a^w)^k)^{-1} a^{vw} (a^w)^k.$$

Este ultimo, dado que $st = ts$, é produto de elementos da forma $a^{s^i t^j}$ e seus inversos. Assim,

$$A = \langle \{a^{s^i t^j} \mid i, j \in \mathbb{Z}\} \rangle.$$

Sabemos que $a^s = aa^t$, então para $i \geqslant 1$

$$a^{s^i} = (a^s)^{s^{i-1}} = (aa^t)^{s^{i-1}} = a^{s^{i-1}} a^{ts^{i-1}} = a^{s^{(i-1)}} (a^{s^{i-1}})^t,$$

portanto, por indução sobre i, vemos que $a^{s^i} \in H = \langle \{a^{t^j} \mid j \in \mathbb{Z}\} \rangle \leqslant A$ para todo $i \geqslant 0$.

Para ver que A é abeliano, basta provar que

$$[a^{s^i t^j}, a^{s^{i_0} t^{j_0}}] = 1 \text{ para todo } i, j, i_0, j_0 \in \mathbb{Z}.$$

Podemos supor que $i \geqslant i_0$ (pois temos que $[a^{s^i t^j}, a^{s^{i_0} t^{j_0}}] = [a^{s^{i_0} t^{j_0}}, a^{s^i t^j}]^{-1}$). Assim,

$$\begin{aligned} [a^{s^i t^j}, a^{s^{i_0} t^{j_0}}] = 1 &\iff [a^{t^j s^i}, a^{t^{j_0} s^{i_0}}] = 1 \\ &\iff [a^{t^j s^{i-i_0}}, a^{t^{j_0}}] = 1 \\ &\iff [a^{s^{i-i_0} t^j}, a^{t^{j_0}}] = 1 \end{aligned}$$

mas $a^{s^{i-i_0}} \in H$ pois $i - i_0 \geqslant 0$, então $a^{s^{i-i_0} t^j} \in H$. Também, $a^{t^{j_0}} \in H$. H é abeliano porque $[a, a^{t^k}] = 1$ para todo $k \in \mathbb{Z}$. Logo $[a^{s^{i-i_0} t^j}, a^{t^{j_0}}] = 1$. Portanto, temos que $A \lhd \Gamma$ é abeliano. □

Proposição 4.1. *O grupo de Baumslag Γ é metabeliano.*

Demonstração. Pelo lema anterior temos que $\langle a \rangle^{\Gamma} = A \lhd \Gamma$ é abeliano. Precisamos ver que Γ/A é abeliano. Basta provar que $[g, h] \in A$ para todo $g, h \in \Gamma$. Usando o fato de que A é normal, isso é equivalente a provar que $[a, t], [a, s], [s, t] \in A$. De fato,

$$[a, t] = a^{-1}t^{-1}at = a^{-1}a^t \in A, [a, s] = a^{-1}s^{-1}as = a^{-1}a^s \in A,$$

por último $[s, t] = 1 \in A$. Assim, Γ é metabeliano. □

Ressaltamos da prova do Lema 4.1 que as relações $[a, a^{t^k}] = 1$, $k \in \mathbb{Z}$ se satisfazem em Γ. Entender o papel de tais relações vai ser fundamental no resto do trabalho, portanto aparecerão várias das suas propriedades daqui na frente.

Proposição 4.2. *O subgrupo $\langle a, t \rangle$ de Γ tem apresentação $\langle a, t \,|\, [a, a^{t^k}] = 1, k \in \mathbb{Z} \rangle$, e o subgrupo $\langle a, t \rangle$ de Γ_m tem apresentação $\langle a, t \,|\, a^m = 1, [a, a^{t^k}] = 1, k \in \mathbb{Z} \rangle$.*

Demonstração. Seja $A = \langle a \rangle^{\Gamma}$, na proposição anterior vimos que

$$Q = \Gamma/A \text{ é abeliano.}$$

Então podemos considerar o grupo A como um $\mathbb{Z}[Q]$-módulo à direita, tal como foi feito no Exemplo 2.6. Como $A = \langle a \rangle^{\Gamma}$, temos que A é cíclico como $\mathbb{Z}[Q]$-módulo, e é gerado por a.

Como $Q = \Gamma/A$, Q é isomorfo como grupo ao grupo Γ adicionando a relação $a = 1$, isto é, o subgrupo $\langle s, t \rangle \leqslant \Gamma$. Identificando Q com $\langle s, t \rangle$, temos que $\mathbb{Z}[Q]$ é precisamente o anel comutativo $\mathbb{Z}[s, s^{-1}, t, t^{-1}]$, pois $[s, t] = 1$.

Como vimos no Exemplo 2.4, o fato de A ser módulo cíclico gerado por a implica que

$$A \cong \mathbb{Z}[s, s^{-1}, t, t^{-1}]/Ann_{\mathbb{Z}[Q]}(a).$$

Mas observamos que $u \in Ann_{\mathbb{Z}[Q]}(a)$ quando $a \circ u = 0$, e isto acontece se $u \in (s - t - 1)$ (o ideal de $\mathbb{Z}[s, s^{-1}, t, t^{-1}]$ gerado por $s - t - 1$), pois a relação $a^s = aa^t$, em notação aditiva, se traduz em $a^s - a^t - a = 0$, ou seja $a \circ (s - t - 1) = 0$. Notamos que a relação $[a, a^t] = 1$ em notação aditiva, equivale a $-a - a^t + a + a^t = 0$, que é trivial em A visto como $\mathbb{Z}[Q]$-módulo. Assim,

$$Ann_{\mathbb{Z}[Q]}(a) = (s - t - 1) \text{ e } A \cong \mathbb{Z}[s, s^{-1}, t, t^{-1}]/(s - t - 1).$$

Temos então que

$$\Gamma = A \rtimes Q = \mathbb{Z}[s, s^{-1}, t, t^{-1}]/(s - t - 1) \rtimes Q, \text{ com } A \cap Q \text{ trivial.}$$

Seja agora

$$H = \langle a, t \rangle \leqslant \Gamma,$$

temos que H é metabeliano, onde $B = A \cap H \lhd H$ é subgrupo abeliano normal de H e $Q_0 = H/B$ é isomorfo ao grupo cíclico gerado por t, e portanto abeliano. Novamente, podemos considerar B como um $\mathbb{Z}[Q_0]$-módulo, assim B é um $\mathbb{Z}[Q_0]$-módulo cíclico com gerador a e $H = B \rtimes Q_0$. Identificando Q_0 com o subgrupo de H gerado por t, temos que $\mathbb{Z}[Q_0]$ corresponde ao subanel comutativo $\mathbb{Z}[t, t^{-1}]$ e

$$B \cong \mathbb{Z}[t, t^{-1}]/Ann_{\mathbb{Z}[Q_0]}(a).$$

Temos que

$$Ann_{\mathbb{Z}[Q_0]}(a) = Ann_{Z[Q]}(a) \cap \mathbb{Z}[t, t^{-1}] = (s - t - 1) \cap \mathbb{Z}[t, t^{-1}].$$

Assim, se $f \in (s - t - 1) \cap \mathbb{Z}[t, t^{-1}]$, $f = (s - t - 1)h$ com $h \in \mathbb{Z}[s, s^{-1}, t, t^{-1}]$ e f não depende de s, s^{-1}, assim $f = f(t, s = s_0)$, com s_0 arbitrário então $f = f(t, s = t + 1) = (t + 1 - t - 1)h(t, t + 1) = 0$. Logo

$$Ann_{\mathbb{Z}[Q_0]}(a) = \{0\} \text{ e portanto } B \cong \mathbb{Z}[t, t^{-1}],$$

então B é o grupo abeliano livre com base $\{a^{t^z}, z \in \mathbb{Z}\}$.

Como $H = B \rtimes Q_0$ e Q_0 é o grupo livre gerado por t, temos que $\langle a, t \,|\, R\rangle$ é apresentação de H, onde R são as relações que fazem a B ser abeliano, ou seja, $R = \{[a^{t^{z_1}}, a^{t^{z_2}}], z_1, z_2 \in \mathbb{Z}\}$. Mas observamos que as relações em R são consequências das relações $\{[a, a^{t^z}], z \in \mathbb{Z}\}$, pois $[a^{t^{z_1}}, a^{t^{z_2}}] = [a, a^{(z_2 - z_1)}]^{t^{z_1}}$. Portanto,

$$\langle a, t \,|\, [a, a^{t^k}] = 1, k \in \mathbb{Z}\rangle \text{ é uma apresentação de } H.$$

Se adicionarmos a relação $a^m = 1$, notamos que em notação aditiva equivale a $am = 0$, portanto B como módulo, vira $(\mathbb{Z}/m\mathbb{Z})$-módulo livre com base $\{a^{t^z}, z \in \mathbb{Z}\}$. Então as relações em R neste caso seriam as que fazem B abeliano junto com $a^m = 1$, portanto $\langle a, t \,|\, a^m = 1, [a, a^{t^k}] = 1, k \in \mathbb{Z}\rangle$ seria apresentação de H considerado como subgrupo de Γ_m. □

4.2 Um limite inferior para função de Dehn de Γ

Agora, consideramos o seguinte grupo

$$\overline{\Gamma} = \left\langle a,p,q,s,t \;\middle|\; \begin{array}{cccc} [a,a^t]=p, & aa^t=a^sq, & s^{-1}ps=p^{-1}, & t^{-1}pt=p^{-1}, \quad [a,p]=1, \\ [s,t]=1, & [p,q]=1, & s^{-1}qs=q^{-1}, & t^{-1}qt=q^{-1}, \quad [a,q]=1 \end{array} \right\rangle.$$

Seja $H := \langle p,q\rangle \leqslant \overline{\Gamma}$.

Lema 4.2. *$H \leqslant \overline{\Gamma}$ é normal e $\Gamma = \overline{\Gamma}/H$.*

Demonstração. Basta verificar que $x^{-1}Hx = H$ e $xHx^{-1} = H$ para $x \in \{a,p,q,s,t\}$. Agora, $s^{-1}ps = p^{-1} \in H$ então conjugando com s^{-1} temos que $p = sp^{-1}s^{-1} = (sps^{-1})^{-1} \in H$, logo $sps^{-1} \in H$. Analogamente, temos que $s^{-1}qs, sqs^{-1} \in H$. Portanto, como $H = \langle p,q\rangle$ temos que

$$sHs^{-1} = H \text{ e } s^{-1}Hs = H.$$

Da mesma forma,

$$tHt^{-1} = H \text{ e } t^{-1}Ht = H.$$

Como $pq = qp$, temos que H é abeliano, portanto

$$x^{-1}Hx = H \text{ para } x \in \{p,q,p^{-1},q^{-1}\}.$$

Além disso, como $ap = pa$ e $aq = qa$ temos $apa^{-1} = a^{-1}pa = p \in H$ e $aqa^{-1} = a^{-1}qa = q \in H$, assim

$$aHa^{-1} = H \text{ e } a^{-1}Ha = H$$

Logo $H \lhd \overline{\Gamma}$.
Como $H = \langle p,q\rangle$ é normal então uma apresentação (por meio de geradores e relações) de $\overline{\Gamma}/H$ se obtém tomando $p = 1$,$q = 1$ na apresentação de $\overline{\Gamma}$

$$\begin{aligned} \overline{\Gamma}/H &= \left\langle a,s,t \;\middle|\; \begin{array}{cccc} [a,a^t]=1, & aa^t=a^s1, & s^{-1}1s=1^{-1}, & t^{-1}1t=1^{-1}, \quad [a,1]=1, \\ [s,t]=1, & [1,1]=1, & s^{-1}1s=1^{-1}, & t^{-1}1t=1^{-1}, \quad [a,1]=1 \end{array} \right\rangle \\ &= \langle a,s,t \,|\, [a,a^t]=1, aa^t=a^s, [s,t]=1\rangle = \Gamma. \end{aligned}$$

□

Sabemos que p e q comutam em $\overline{\Gamma}$, portanto é razoável pensar que $H \cong \mathbb{Z}^2$. Isto de fato acontece, mas não é obvio por causa de que p,q não são geradores livres em $\overline{\Gamma}$.

Lema 4.3. *H é isomorfo a $\mathbb{Z}^2$.*

Demonstração. Seja R o anel $\mathbb{Z}[x, x^{-1}, (x+1)^{-1}]$ e

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad P = \begin{pmatrix} 1 & 0 & -2x-1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad Q = \begin{pmatrix} 1 & 0 & -x-1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & x+1 & 0 \\ 0 & 0 & -x^2-x \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & -x^2-x \end{pmatrix}.$$

Temos que

$$det(A) = det(P) = det(Q) = 1 \in R^*,$$

$$det(T) = x(-x^2-2) = -x^2(x+1) \in R^*$$

e

$$det(S) = (x+1)(-x^2-x) = -x(x+1)^2 \in R^*,$$

logo $A, P, Q, S, T \in GL_3(R)$.

Considerando em $GL_3(R)$ as relações análogas às que definem $\overline{\Gamma}$ usando A, P, Q, S, T. Temos que são satisfeitas as relações

i) $[A, A^T] = P, AA^T = A^S Q$, $[S, T] = 1$, $[P, Q] = 1$, $[A, P] = 1$ e $[A, Q] = 1$:

$$A^T = T^{-1}AT = \begin{pmatrix} 1 & 0 & 0 \\ 0 & x^{-1} & 0 \\ 0 & 0 & -x^{-1}(x+1)^{-1} \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & -x^2-x \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 1 & 0 \\ 0 & x^{-1} & x^{-1} \\ 0 & 0 & -x^{-1}(x+1)^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & -x^2-x \end{pmatrix} = \begin{pmatrix} 1 & x & 0 \\ 0 & 1 & -x-1 \\ 0 & 0 & 1 \end{pmatrix},$$

então

$$[A, A^T] = A^{-1}(A^T)^{-1}AA^T$$

$$= \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -x & -x(x+1) \\ 0 & 1 & x+1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x & 0 \\ 0 & 1 & -x-1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & -x-1 & 1-(x+1)^2 \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x+1 & -x-1 \\ 0 & 1 & -x \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & -2x-1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$= P;$$

$$A^S = S^{-1}AS = \begin{pmatrix} 1 & 0 & 0 \\ 0 & (x+1)^{-1} & 0 \\ 0 & 0 & -x^{-1}(x+1)^{-1} \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & x+1 & 0 \\ 0 & 0 & -x^2-x \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 1 & 0 \\ 0 & (x+1)^{-1} & (x+1)^{-1} \\ 0 & 0 & -x^{-1}(x+1)^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & x+1 & 0 \\ 0 & 0 & -x^2-x \end{pmatrix} = \begin{pmatrix} 1 & x+1 & 0 \\ 0 & 1 & -x \\ 0 & 0 & 1 \end{pmatrix},$$

então

$$A^S Q = \begin{pmatrix} 1 & x+1 & 0 \\ 0 & 1 & -x \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -x-1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+1 & -x-1 \\ 0 & 1 & -x \\ 0 & 0 & 1 \end{pmatrix} = AA^T;$$

$$[P,Q] = P^{-1}Q^{-1}PQ$$
$$= \begin{pmatrix} 1 & 0 & 2x+1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & x+1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -2x-1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -x-1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 0 & 3x+2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -3x-2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix};$$

$$[A,P] = A^{-1}P^{-1}AP$$
$$= \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 2x+1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -2x-1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & -1 & 2x+2 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & -2x-1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix};$$

$$[A,Q] = A^{-1}Q^{-1}AQ$$
$$= \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & x+1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -x-1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & -1 & x+2 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & -x-1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Claramente, $ST = TS$ pois são matrizes diagonais e o produto em R é comutativo, logo $[S,T] = 1$.

Mas não são satisfeitas as relações

ii) $S^{-1}PS = P^{-1},\ S^{-1}QS = Q^{-1},\ T^{-1}PT = P^{-1},\ T^{-1}QT = Q^{-1}$, pois para todo $f \in R$

$$\begin{aligned} S^{-1}\begin{pmatrix}1&0&f\\0&1&0\\0&0&1\end{pmatrix}S &= \begin{pmatrix}1&0&0\\0&(x+1)^{-1}&0\\0&0&-x^{-1}(x+1)^{-1}\end{pmatrix}\begin{pmatrix}1&0&f\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&x+1&0\\0&0&-x(x+1)\end{pmatrix} \\ &= \begin{pmatrix}1&0&f\\0&(x+1)^{-1}&0\\0&0&-x^{-1}(x+1)^{-1}\end{pmatrix}\begin{pmatrix}1&0&0\\0&x+1&0\\0&0&-x(x+1)\end{pmatrix} \\ &= \begin{pmatrix}1&0&-x(x+1)f\\0&1&0\\0&0&1\end{pmatrix}, \end{aligned}$$

$$\begin{aligned} T^{-1}\begin{pmatrix}1&0&f\\0&1&0\\0&0&1\end{pmatrix}T &= \begin{pmatrix}1&0&0\\0&x^{-1}&0\\0&0&-x^{-1}(x+1)^{-1}\end{pmatrix}\begin{pmatrix}1&0&f\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&x&0\\0&0&-x(x+1)\end{pmatrix} \\ &= \begin{pmatrix}1&0&f\\0&x^{-1}&0\\0&0&-x^{-1}(x+1)^{-1}\end{pmatrix}\begin{pmatrix}1&0&0\\0&x&0\\0&0&-x(x+1)\end{pmatrix} \\ &= \begin{pmatrix}1&0&-x(x+1)f\\0&1&0\\0&0&1\end{pmatrix}. \end{aligned} \tag{4.5}$$

Seja

$$G := \left\{ \begin{pmatrix}1&h_1&h_2\\0&g_1&h_3\\0&0&g_2\end{pmatrix} \middle|\ h_i \in R,\ g_j \in R^* \right\} \subseteq GL_3(R).$$

Temos que $A, P, Q, S, T \in G$. Vejamos que G é subgrupo de $GL_3(R)$. De fato, se $N = \begin{pmatrix}1&h_1&h_2\\0&g_1&h_3\\0&0&g_2\end{pmatrix}$, $N' = \begin{pmatrix}1&h_1'&h_2'\\0&g_1'&h_3'\\0&0&g_2'\end{pmatrix}$ temos que $NN' = \begin{pmatrix}1&f_1&f_2\\0&g_1g_1'&f_3\\0&0&g_2g_2'\end{pmatrix} \in G$ onde $f_i \in R$ e $g_jg_j' \in R^*$ pois $g_j, g_j' \in R^*$. Além disso, $N^{-1} = \begin{pmatrix}1&f_1'&f_2'\\0&g_1^{-1}&f_3'\\0&0&g_2^{-1}\end{pmatrix} \in G$, pois $g_i^{-1} \in R^*$.

Seja agora

$$M := \left\{ \begin{pmatrix} 1 & 0 & f \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \middle| \; f \in R \right\} \subseteq G.$$

Observamos que M é um subgrupo normal de G pois para todo $f_1, f_2 \in R$

$$\begin{pmatrix} 1 & 0 & f_1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & f_2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & f_1 + f_2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in M, \qquad \begin{pmatrix} 1 & 0 & f_1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 & -f_1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in M, \tag{4.6}$$

então M é subgrupo de G, e dado $N = \begin{pmatrix} 1 & h_1 & h_2 \\ 0 & g_1 & h_3 \\ 0 & 0 & g_2 \end{pmatrix} \in G$,

$$\begin{aligned} N^{-1} \begin{pmatrix} 1 & 0 & f_1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} N &= \begin{pmatrix} 1 & -h_1 g_1^{-1} & (h_1 h_3 - h_2 g_1) g_1^{-1} g_2^{-1} \\ 0 & g_1^{-1} & -h_3 g_1^{-1} g_2^{-1} \\ 0 & 0 & g_2^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 & f_1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & h_1 & h_2 \\ 0 & g_1 & h_3 \\ 0 & 0 & g_2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & -h_1 g_1^{-1} & (h_1 h_3 - h_2 g_1) g_1^{-1} g_2^{-1} \\ 0 & g_1^{-1} & -h_3 g_1^{-1} g_2^{-1} \\ 0 & 0 & g_2^{-1} \end{pmatrix} \begin{pmatrix} 1 & h_1 & h_2 + f_1 g_2 \\ 0 & g_1 & h_3 \\ 0 & 0 & g_2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & f_1 g_2 \\ 0 & g_1 & 0 \\ 0 & 0 & g_2 \end{pmatrix} \in M, \end{aligned} \tag{4.7}$$

portanto $M \lhd G$.

Como vemos nas equações (4.6) temos um isomorfismo entre o grupo M com a multiplicação de matrizes e o grupo abeliano $(R, +)$, por meio da aplicação

$$\phi : M \longrightarrow R$$

que leva $\begin{pmatrix} 1 & 0 & f \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ em f.

Consideramos

$$\tau = (-1 + \sqrt{5})/2$$

e

$$\psi : R \to \mathbb{Z}[\tau]$$

o epimorfismo dado por $\psi(f) = f(\tau)$. Sejam

$$R_0 = ker(\psi) \text{ e } M_0 = \phi^{-1}(R_0).$$

M_0 é subgrupo normal de G porque dados $W = \begin{pmatrix} 1 & 0 & f \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in M_0$ e $N = \begin{pmatrix} 1 & h_1 & h_2 \\ 0 & g_1 & h_3 \\ 0 & 0 & g_2 \end{pmatrix} \in G$,

temos por (4.7) que $N^{-1}WN = \begin{pmatrix} 1 & 0 & fg_2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, portanto

$$\psi(\phi(N^{-1}WN)) = \psi(fg_2) = f(\tau)g_2(\tau) = 0,$$

pois $f(\tau) = \psi(\phi(W))$ e $\phi(W) \in ker(\psi)$. Assim $\phi(N^{-1}WN) \in ker(\psi) = R_0$, logo

$$N^{-1}WN \in \phi^{-1}(R_0) = M_0.$$

Seja

$$\hat{G} := G/M_0.$$

Temos que em $\hat{G}$ são satisfeitas as relações $i)$, pois valem em G. As relações $ii)$ também são satisfeitas. Para ver isto, notamos que para todo $f \in R$

$$\begin{pmatrix} 1 & 0 & -x(x+1)f \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -f \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 & -(x^2+x-1)f \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} =: C,$$

assim $\phi(C) = -(x^2+x-1)f$ e $\psi(-(x^2+x-1)f) = -(\tau^2+\tau-1)f(\tau) = 0$, logo $-(x^2+x-1)f \in R_0$ e portanto $C \in \phi^{-1}(R_0) = M_0$. Então em $\hat{G} = G/M_0$ temos que

$$\begin{pmatrix} 1 & 0 & -x(x+1)f \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & -f \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

substituindo em (4.5) obtemos as relações $ii)$. Portanto, a aplicação $a \mapsto A, p \mapsto P, q \mapsto Q, s \mapsto S, t \mapsto T$ induz um homomorfismo

$$\theta : \overline{\Gamma} \to \hat{G}.$$

Como $H = \langle p, q \rangle$, temos que

$$\theta(H) = \langle M_0P, M_0Q \rangle \leqslant M/M_0 \leqslant \hat{G},$$

pois $P, Q \in M$. Notamos que

$$Im(\psi \circ \phi) = \mathbb{Z}[\tau] \text{ e } M_0 = ker(\psi \circ \phi),$$

logo $M/M_0 \cong \mathbb{Z}[\tau]$. Além disso, $(\psi \circ \phi)(P) = -\sqrt{5}$ e $(\psi \circ \phi)(Q) = (-1 - \sqrt{5})/2$, logo as imagens de P e Q geram o grupo aditivo $\mathbb{Z}[\tau]$ por completo. Portanto

$$\langle M_0P, M_0Q \rangle = M/M_0 \cong \mathbb{Z}[\tau]$$

e este último como grupo aditivo é isomorfo a $\mathbb{Z}^2$. Assim temos que

$$H/ker(\theta) \cong \theta(H) = \langle M_0P, M_0Q \rangle \cong \mathbb{Z}^2,$$

mas H é um grupo abeliano gerado por dois elementos então temos finalmente pelo Lema 1.1 que $H \cong \mathbb{Z}^2$. □

Lema 4.4. $[a, a^{t^n}] = p^{(-1)^{n+1}F_n}$ *em* $\overline{\Gamma}$ *para todo* $n \geqslant 0$, *onde* F_n *é o n-ésimo número de Fibonacci, dado por* $F_0 = 0, F_1 = 1$ *e* $F_{n+2} = F_n + F_{n+1}$, $n \geqslant 0$.

Demonstração. Dado $n \geqslant 0$ temos na prova do Lema 4.1 que $[a, a^{t^n}] = 1$ em Γ. Além disso, no Lema 4.2 temos que $\Gamma = \overline{\Gamma}/H$, então como elemento de $\overline{\Gamma}$ temos que $[a, a^{t^n}] \in H = \langle p, q \rangle$. Portanto $[a, a^{t^n}] = p^\lambda q^\mu$ para alguns $\lambda, \mu \in \mathbb{Z}$, pois p, q comutam. Para encontrar λ, μ, consideramos de novo os grupos de matrizes e homomorfismos da prova do Lema 4.3. Em particular, vejamos que

$$[A, A^{T^n}] = \begin{pmatrix} 1 & 0 & (-x-1)^n - x^n \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{4.8}$$

De fato,

$$T^n = \begin{pmatrix} 1 & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & -x^2 - x \end{pmatrix}^n = \begin{pmatrix} 1 & 0 & 0 \\ 0 & x^n & 0 \\ 0 & 0 & (-x^2 - x)^n \end{pmatrix}.$$

Então

$$\begin{aligned} A^{T^n} = (T^n)^{-1} A T^n &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & x^{-n} & 0 \\ 0 & 0 & (-x^2 - x)^{-n} \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & x^n & 0 \\ 0 & 0 & (-x^2 - x)^n \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 & 0 \\ 0 & x^{-n} & x^{-n} \\ 0 & 0 & (-x^2 - x)^{-n} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & x^n & 0 \\ 0 & 0 & (-x^2 - x)^n \end{pmatrix} = \begin{pmatrix} 1 & x^n & 0 \\ 0 & 1 & (-x-1)^n \\ 0 & 0 & 1 \end{pmatrix}, \end{aligned}$$

portanto

$$\begin{aligned}
[A, A^{T^n}] &= A^{-1}(A^{T^n})^{-1}AA^{T^n} \\
&= \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -x^n & (-x^2-x)^n \\ 0 & 1 & -(-x-1)^n \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & x^n & 0 \\ 0 & 1 & (-x-1)^n \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & -x^n-1 & (-x^2-x)^n+(-x-1)^n+1 \\ 0 & 1 & -(-x-1)^n-1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & x^n+1 & (-x-1)^n \\ 0 & 1 & (-x-1)^n+1 \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 & (-x-1)^n-x^n \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.
\end{aligned}$$

De outro lado,

$$P^\lambda Q^\mu = \begin{pmatrix} 1 & 0 & -2x-1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^\lambda \begin{pmatrix} 1 & 0 & -x-1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^\mu = \begin{pmatrix} 1 & 0 & \lambda(-2x-1)+\mu(-x-1) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Olhando para $[a, a^{t^n}] = p^\lambda q^\mu$ em $\hat{G}$ temos que $[A, A^{T^n}] = P^\lambda Q^\mu$, ou seja

$$\begin{pmatrix} 1 & 0 & (-x-1)^n-x^n \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & \lambda(-2x-1)+\mu(-x-1) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

e este último corresponde em $\mathbb{Z}[\tau]$ a $(-\tau-1)^n - \tau^n = \lambda(-2\tau-1)+\mu(-\tau-1)$. Agora, $\lambda(-2\tau-1)+\mu(-\tau-1) = \lambda(-\sqrt{5})+\mu(-\sqrt{5}-1)/2$. Vejamos por indução que $(-\tau-1)^n-\tau^n = (-1)^n\sqrt{5}F_n$; para $n = 0, 1$ é claro; se $n \geqslant 2$ suponhamos que vale para todo $i \leqslant n$, então

$$\begin{aligned}
(-1)^{n+1}\sqrt{5}F_{n+1} &= (-1)^{n+1}\sqrt{5}(F_n + F_{n-1}) \\
&= -(-1)^n\sqrt{5}F_n + (-1)^{n-1}\sqrt{5}F_{n-1} \\
&= -((-\tau-1)^n - \tau^n) + (-\tau-1)^{n-1} - \tau^{n-1} \\
&= -(-\tau-1)^n + (-\tau-1)^{n-1} + \tau^n - \tau^{n-1} \\
&= (-(-\tau-1)+1)(-\tau-1)^{n-1} + (\tau-1)\tau^{n-1} \\
&= (\tau+1+(\tau^2+\tau))(-\tau-1)^{n-1} + (\tau-(\tau^2+\tau))\tau^{n-1} \quad (\text{pois } \tau^2+\tau = 1) \\
&= (\tau^2+2\tau+1)(-\tau-1)^{n-1} - \tau^2\tau^{n-1} \\
&= (-\tau-1)^2(-\tau-1)^{n-1} - \tau^{n+1} \\
&= (-\tau-1)^{n+1} - \tau^{n+1}.
\end{aligned}$$

Então $\lambda(-\sqrt{5}) + \mu(-\sqrt{5}-1)/2 = (-1)^n\sqrt{5}F_n$, e portanto $\mu = 0$ e $\lambda = (-1)^{n+1}F_n$. □

Agora é possível estabelecer um limite inferior para a função de Dehn δ_Γ de Γ.

Proposição 4.3. $\delta_\Gamma \geq 2^n$.

Demonstração. Temos que $\overline{\Gamma}$ tem apresentação

$$\overline{\Gamma} = \langle X | R \rangle,$$

onde $X = a, p, q, s, t$ e R são as correspondentes relações que definem a $\overline{\Gamma}$. Como $\Gamma = \overline{\Gamma}/H$ onde $H = \langle p, q \rangle$, então Γ tem apresentação

$$\Gamma = \langle X | R \cup \{p, q\} \rangle,$$

chamemos de U esta apresentação.

Agora fixamos $n \geqslant 0$. Sabemos que $w = [a, a^{t^n}] = 1$ em Γ, então w é homotopicamente nula. Seja

$$k = Area_a^U(w), \text{ então } w = \prod_{i=1}^{k} (r_i^{f_i})^{e_i},$$

onde $f_i \in F(X)$, $r_i \in R \cup \{p, q\}$, $e_i = \pm 1$. Então projetando w em $F(X)/R^{F(X)} = \overline{\Gamma}$, temos que $r_i = 1$ para $r_i \in R$, então substituindo em w temos

$$w = \prod_{i=1}^{k'} (u_i^{g_i})^{e_i}$$

com $u_i \in \{p, q\}$, $g_i \in F(X)$, $e_i = \pm 1$, mas $k' \leqslant k$.

Agora $p^v = p^{\pm 1}$ e $q^v = q^{\pm 1}$ em $\overline{\Gamma}$ para todo $v \in F(X)$, portanto $w = \prod_{i=1}^{k'} (u_i)^{\epsilon_i}$, com $u_i \in \{p, q\}$, $\epsilon_i = \pm 1$. Como p, q comutam então

$$w = p^\lambda q^\mu \text{ com } \lambda, \mu \in \mathbb{Z} \text{ e } |\lambda| + |\mu| \leqslant k' \leqslant k.$$

Pelo lema anterior

$$w = p^{(-1)^{n+1} F_n} \text{ então } F_n \leqslant k.$$

Como o comprimento de w é $4n + 4$ temos que

$$\delta_\Gamma(4n + 4) \geqslant F_n.$$

Assim

$$\delta_\Gamma(n) \simeq \delta_\Gamma(4n + 4) \geq F_n.$$

E temos da fórmula de Binet que

$$F_n = \frac{1}{\sqrt{5}} \left(\frac{1 + \sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1 - \sqrt{5}}{2} \right)^n \simeq \left(\frac{1 + \sqrt{5}}{2} \right)^n \simeq 2^n.$$

□

4.3 Um limite superior para função de Dehn de Γ

Agora vamos procurar um limite superior para a função de Dehn de Γ. Esquecemos $\overline{\Gamma}$ e voltamos para a apresentação de Γ

$$\Gamma = \langle a, s, t \,|\, [a, a^t] = 1, [s, t] = 1, a^s = aa^t \rangle.$$

Começamos definindo, para $n \in \mathbb{Z}$

$$C(n) := Area\left([a, a^{t^n}]\right),$$

que é o mínimo numero de vezes que precisa se usar alguma relação para converter a palavra $[a, a^{t^n}]$ na palavra vazia, ou equivalentemente, converter a palavra aa^{t^n} em $a^{t^n}a$, em Γ.

Lema 4.5. *$C(n) \leqslant 4^n$ para todo $n \geqslant 1$.*

Demonstração. Vamos provar este fato por indução. Para $n = 1$, temos a própria relação $[a, a^t] = 1$, ou seja $C(1) = 1$. Para $n = 2$, temos

$$\begin{aligned}
& aa^t = a^t a \quad \text{(custo 1)} \\
\Longrightarrow \quad & (aa^t)^s = (a^t a)^s \quad \text{(custo 0)} \\
\Longrightarrow \quad & a^s a^{ts} = a^{ts} a^s \quad \text{(custo 0)} \\
\Longrightarrow \quad & aa^t a^{ts} = a^{ts} aa^t \quad \text{(custo 2, usamos } a^s = aa^t\text{)} \\
\Longrightarrow \quad & aa^t a^{st} = a^{st} aa^t \quad \text{(custo 4, usamos } [s,t] = 1\text{)} \\
\Longrightarrow \quad & aa^t (aa^t)^t = (aa^t)^t aa^t \quad \text{(custo 2, usamos } a^s = aa^t\text{)} \\
\Longrightarrow \quad & aa^t (a^t a)^t = (a^t a)^t aa^t \quad \text{(custo 2, usamos } [a, a^t] = 1\text{)} \\
\Longrightarrow \quad & aa^t a^{t^2} a^t = a^{t^2} a^t aa^t \quad \text{(custo 0)} \\
\Longrightarrow \quad & a(aa^t)^t a^t = a^{t^2} a^t aa^t \quad \text{(custo 0)} \\
\Longrightarrow \quad & a(a^t a)^t a^t = a^{t^2} aa^t a^t \quad \text{(custo 2, usamos } [a, a^t] = 1\text{)} \\
\Longrightarrow \quad & aa^{t^2} a^t a^t = a^{t^2} aa^t a^t \quad \text{(custo 0)} \\
\Longrightarrow \quad & aa^{t^2} = a^{t^2} a \quad \text{(custo 0),}
\end{aligned}$$

no total temos custo $C(2) \leqslant 13 < 16 = 4^2$. Para $n = 3$, temos

$$\begin{aligned}
& aa^{t^2} = a^{t^2}a \quad \text{(custo } C(2)\text{)} \\
\Longrightarrow\ & (aa^{t^2})^s = (a^{t^2}a)^s \quad \text{(custo 0)} \\
\Longrightarrow\ & a^s a^{t^2 s} = a^{t^2 s}a^s \quad \text{(custo 0)} \\
\Longrightarrow\ & aa^t a^{t^2 s} = a^{t^2 s}aa^t \quad \text{(custo 2, usamos } a^s = aa^t\text{)} \\
\Longrightarrow\ & aa^t a^{st^2} = a^{st^2}aa^t \quad \text{(custo 8, usamos } [s,t] = 1\text{)} \\
\Longrightarrow\ & aa^t(aa^t)^{t^2} = (aa^t)^{t^2}aa^t \quad \text{(custo 2, usamos } a^s = aa^t\text{)} \\
\Longrightarrow\ & aa^t(a^t a)^{t^2} = (a^t a)^{t^2}aa^t \quad \text{(custo 2, usamos } [a, a^t] = 1\text{)} \\
\Longrightarrow\ & aa^t a^{t^3} a^{t^2} = a^{t^3}a^{t^2}aa^t \quad \text{(custo 0)} \\
\Longrightarrow\ & a(aa^{t^2})^t a^{t^2} = a^{t^3}(a^{t^2}a)a^t \quad \text{(custo 0)} \\
\Longrightarrow\ & a(a^{t^2}a)^t a^{t^2} = a^{t^3}aa^{t^2}a^t \quad \text{(custo } 2C(2)\text{, usamos } [a, a^{t^2}] = 1\text{)} \\
\Longrightarrow\ & aa^{t^3}a^t a^{t^2} = a^{t^3}aa^{t^2}a^t \quad \text{(custo 0)} \\
\Longrightarrow\ & aa^{t^3}(aa^t)^t = a^{t^3}aa^{t^2}a^t \quad \text{(custo 0)} \\
\Longrightarrow\ & aa^{t^3}(a^t a)^t = a^{t^3}aa^{t^2}a^t \quad \text{(custo 1, usamos } [a, a^t] = 1\text{)} \\
\Longrightarrow\ & aa^{t^3}a^{t^2}a^t = a^{t^3}aa^{t^2}a^t \quad \text{(custo 0)} \\
\Longrightarrow\ & aa^{t^3} = a^{t^3}a \quad \text{(custo 0)},
\end{aligned}$$

no total, temos custo $C(3) \leqslant 3C(2) + 15 < 3 \cdot 4^2 + 16 = 4^3$. Agora, em geral suponhamos que $n \geqslant 3$ e $C(i) \leqslant 4^i$ para $1 \leqslant i \leqslant n$, então

$$\begin{aligned}
& aa^{t^n} = a^{t^n}a \quad \text{(custo } C(n)\text{)} \\
\Longrightarrow\ & (aa^{t^n})^s = (a^{t^n}a)^s \quad \text{(custo 0)} \\
\Longrightarrow\ & a^s a^{t^n s} = a^{t^n s}a^s \quad \text{(custo 0)} \\
\Longrightarrow\ & aa^t a^{t^n s} = a^{t^n s}aa^t \quad \text{(custo 2, usamos } a^s = aa^t\text{)} \\
\Longrightarrow\ & aa^t a^{st^n} = a^{st^n}aa^t \quad \text{(custo } 4n\text{, usamos } [s,t] = 1\text{)} \\
\Longrightarrow\ & aa^t(aa^t)^{t^n} = (aa^t)^{t^n}aa^t \quad \text{(custo 2, usamos } a^s = aa^t\text{)} \\
\Longrightarrow\ & aa^t(a^t a)^{t^n} = (a^t a)^{t^n}aa^t \quad \text{(custo 2, usamos } [a, a^t] = 1\text{)} \\
\Longrightarrow\ & aa^t a^{t^{n+1}} a^{t^n} = a^{t^{n+1}}a^{t^n}aa^t \quad \text{(custo 0)} \\
\Longrightarrow\ & a(aa^{t^n})^t a^{t^n} = a^{t^{n+1}}(a^{t^n}a)a^t \quad \text{(custo 0)} \\
\Longrightarrow\ & a(a^{t^n}a)^t a^{t^n} = a^{t^{n+1}}aa^{t^n}a^t \quad \text{(custo } 2C(n)\text{, usamos } [a, a^{t^n}] = 1\text{)} \\
\Longrightarrow\ & aa^{t^{n+1}}a^t a^{t^n} = a^{t^{n+1}}aa^{t^n}a^t \quad \text{(custo 0)} \\
\Longrightarrow\ & aa^{t^{n+1}}(aa^{t^{n-1}})^t = a^{t^{n+1}}aa^{t^n}a^t \quad \text{(custo 0)} \\
\Longrightarrow\ & aa^{t^{n+1}}(a^{t^{n-1}}a)^t = a^{t^{n+1}}aa^{t^n}a^t \quad \text{(custo } C(n-1)\text{, usamos } [a, a^{t^{n-1}}] = 1\text{)} \\
\Longrightarrow\ & aa^{t^{n+1}}a^{t^n}a^t = a^{t^{n+1}}aa^{t^n}a^t \quad \text{(custo 0)} \\
\Longrightarrow\ & aa^{t^{n+1}} = a^{t^{n+1}}a \quad \text{(custo 0)},
\end{aligned}$$

no total temos

$$C(n+1) \leqslant 3C(n) + C(n-1) + 4n + 6 \leqslant 3 \cdot 4^n + 4^{n-1} + 4n + 6 \leqslant 4^{n+1}$$

pois $n \geqslant 3$. □

Introduzimos a seguinte notação que permite usar melhor a relação $a^s = aa^t$ em Γ. Dado um polinômio $f(x) = \sum_{i=0}^{n} c_i x^i \in \mathbb{Z}[x]$ e símbolos a, r, definimos a palavra

$$[\![a]\!]_r^f := a^{c_0} r^{-1} a^{c_1} r^{-1} \cdots a^{c_{n-1}} r^{-1} a^{c_n} r^n.$$

Notamos que no grupo livre $F(a, r)$

$$\begin{aligned} a^{c_0} a^{c_1 r} \cdots a^{c_{n-1} r^{n-1}} a^{c_n r^n} &= a^{c_0} r^{-1} a^{c_1} r r^{-2} a^{c_2} r^2 \cdots r^{-(n-1)} a^{c_{n-1}} r^{n-1} r^{-n} a^{c_n} r^n \\ &= a^{c_0} r^{-1} a^{c_1} r^{-1} \cdots a^{c_{n-1}} r^{-1} a^{c_n} r^n = [\![a]\!]_r^f. \end{aligned}$$

Lema 4.6. *Para todo* $f(x) = \sum_{i=0}^{n} c_i x^i \in \mathbb{Z}[x]$ *tal que* $\max_i |c_i| \leqslant c$,

$$[\![a]\!]_s^{f(x)} = [\![a]\!]_t^{f(x+1)}$$

em Γ*, e o custo desta igualdade é no máximo* $D_c(n) := c^2 4^{n+1}$.

Demonstração. Tomamos $c \geqslant 1$ pois o lema é trivial no caso $c = 0$. Fazemos indução por n, no caso $n = 0$, ambas palavras são a^{c_0} e temos custo 0. Assumimos $n \geqslant 1$ e supomos que o lema vale para $k < n$. Seja $\hat{f}(x) = \sum_{i=1}^{n} c_i x^{i-1}$, então $f(x) = c_0 + x\hat{f}(x)$. Temos que

$$\begin{aligned} [\![a]\!]_s^{f(x)} &= a^{c_0} s^{-1} a^{c_1} s^{-1} \cdots a^{c_{n-1}} s^{-1} a^{c_n} s^n \\ &= a^{c_0} s^{-1} \left(a^{c_1} s^{-1} \cdots a^{c_{n-1}} s^{-1} a^{c_n} s^{n-1} \right) s \\ &= a^{c_0} \left([\![a]\!]_s^{\hat{f}(x)} \right)^s. \end{aligned} \tag{4.9}$$

O anterior claramente tem custo 0. Por hipótese de indução temos que

$$a^{c_0} \left([\![a]\!]_s^{\hat{f}(x)} \right)^s = a^{c_0} \left([\![a]\!]_t^{\hat{f}(x+1)} \right)^s \tag{4.10}$$

com custo $D_c(n-1)$. Sabemos $\hat{f}$ tem grau $n-1$, então escrevemos $\hat{f}(x+1) = \sum_{j=0}^{n-1} d_j x^j$, logo

$$\begin{aligned} \left([\![a]\!]_t^{\hat{f}(x+1)} \right)^s &= \left(a^{d_0} t^{-1} a^{d_1} t^{-1} \cdots a^{d_{n-2}} t^{-1} a^{d_{n-1}} t^{n-1} \right)^s \\ &= s^{-1} a^{d_0} t^{-1} a^{d_1} t^{-1} \cdots a^{d_{n-2}} t^{-1} a^{d_{n-1}} s t^{n-1} && \text{(usa } [s,t] = 1,\ n-1 \text{ vezes)} \\ &= s^{-1} a^{d_0} s s^{-1} t^{-1} a^{d_1} s s^{-1} t^{-1} \cdots s s^{-1} t^{-1} a^{d_{n-1}} s t^{n-1} && \text{(custo 0)} \\ &= s^{-1} a^{d_0} s t^{-1} s^{-1} a^{d_1} s t^{-1} s^{-1} \cdots s t^{-1} s^{-1} a^{d_{n-1}} s t^{n-1} && \text{(usa } [s,t] = 1,\ n-1 \text{ vezes)} \\ &= a^{d_0 s} t^{-1} a^{d_1 s} t^{-1} \cdots a^{d_{n-1} s} t^{n-1} \\ &= (a^s)^{d_0} t^{-1} (a^s)^{d_1} t^{-1} \cdots (a^s)^{d_{n-1}} t^{n-1} && \text{(custo 0)} \\ &= [\![a^s]\!]_t^{\hat{f}(x+1)}. \end{aligned}$$

Então

$$a^{c_0}\left(\llbracket a\rrbracket_t^{\hat{f}(x+1)}\right)^s = a^{c_0}\llbracket a^s\rrbracket_t^{\hat{f}(x+1)} \tag{4.11}$$

com custo $2(n-1)$. Agora,

$$\begin{aligned}\llbracket a^s\rrbracket_t^{\hat{f}(x+1)} &= (a^s)^{d_0}t^{-1}(a^s)^{d_1}t^{-1}\cdots(a^s)^{d_{n-1}}t^{n-1}\\ &= (aa^t)^{d_0}t^{-1}(aa^t)^{d_1}t^{-1}\cdots(aa^t)^{d_{n-1}}t^{n-1} \quad \left(\text{usa } a^s = aa^t, \sum_{j=0}^{n-1}|d_j| \text{ vezes}\right)\\ &= \llbracket aa^t\rrbracket_t^{\hat{f}(x+1)}.\end{aligned}$$

Para calcular o custo da igualdade anterior, observamos que

$$\begin{aligned}\sum_{j=0}^{n-1} d_j x^j = \hat{f}(x+1) = \sum_{i=1}^{n} c_i(x+1)^{i-1} &= \sum_{i=0}^{n-1} c_{i-1}(x+1)^i\\ = \sum_{i=0}^{n-1} c_{i-1}\sum_{j=0}^{i}\binom{i}{j}x^j, &\quad \text{logo}\\ \sum_{j=0}^{n-1}|d_j| \leqslant \sum_{i=0}^{n-1}|c_{i-1}|\sum_{j=0}^{i}\binom{i}{j} \leqslant c\sum_{i=0}^{n-1}\sum_{j=0}^{i}\binom{i}{j} &= c\sum_{i=0}^{n-1}2^i = c(2^n-1) < c2^n.\end{aligned}$$

Então temos

$$a^{c_0}\llbracket a^s\rrbracket_t^{\hat{f}(x+1)} = a^{c_0}\llbracket aa^t\rrbracket_t^{\hat{f}(x+1)} \tag{4.12}$$

com custo $\leqslant c2^n$.

Para continuar, precisamos mostrar primeiro que

$$\text{para } m \geqslant 0, (aa^t)^m = a^m a^{mt} \text{ e } (aa^t)^{-m} = a^{-m}a^{-mt} \text{ tem custo } \leqslant m^2.$$

Por indução, o caso $m = 0$ é trivial e para $m = 1$, temos $aa^t = aa^t$ tem custo 0 e $(aa^t)^{-1} = (a^t a)^{-1} = a^{-1}a^{-1t}$ tem custo 1 (usamos 1 vez $[a, a^t] = 1$). Suponhamos que $m \geqslant 2$ e que o resultado vale para todo $k < m$. Então

$$\begin{aligned}(aa^t)^m &= (aa^t)^{m-1}(aa^t)\\ &= a^{m-1}a^{(m-1)t}aa^t \quad (\text{custo} \leqslant (m-1)^2)\\ &= a^{m-1}aa^{(m-1)t}a^t \quad (\text{usa } [a,a^t]=1,\ m-1 \text{ vezes})\\ &= a^m a^{mt}.\end{aligned}$$

$$\begin{aligned}\text{Também,}\qquad (aa^t)^{-m} &= (aa^t)^{-(m-1)}(aa^t)^{-1}\\ &= a^{-(m-1)}a^{-(m-1)t}(aa^t)^{-1} \quad (\text{custo} \leqslant (m-1)^2)\\ &= a^{-(m-1)}a^{-mt}a^{-1}\\ &= a^{-(m-1)}a^{-1}a^{-mt} \quad (\text{usa } [a,a^t]=1,\ m \text{ vezes})\\ &= a^{-m}a^{-mt}.\end{aligned}$$

Nos dois casos temos custo $\leqslant (m-1)^2 + m = m^2 - 2m + 1 + m \leqslant m^2$.
Daí, temos que

$$\begin{aligned} a^{c_0}[\![aa^t]\!]_t^{\hat{f}(x+1)} &= a^{c_0}(aa^t)^{d_0}(aa^t)^{d_1 t}\cdots(aa^t)^{d_{n-1}t^{n-1}} \\ &= a^{c_0}a^{d_0}a^{d_0 t}(a^{d_1}a^{d_1 t})^t\cdots(a^{d_{n-1}}a^{d_{n-1}t})^{t^{n-1}} \quad \left(\text{custo} \leqslant \sum_{j=0}^{n-1} d_j^2\right) \\ &= a^{c_0}a^{d_0}a^{d_0 t}a^{d_1 t}a^{d_1 t^2}\cdots a^{d_{n-1}t^{n-1}}a^{d_{n-1}t^n} \\ &= a^{c_0}a^{d_0}a^{(d_0+d_1)t}a^{(d_1+d_2)t^2}\cdots a^{(d_{n-2}+d_{n-1})t^{n-1}}a^{d_{n-1}t^n} \\ &= a^{c_0}[\![a]\!]_t^{(x+1)\hat{f}(x+1)} = a^{c_0}[\![a]\!]_t^{f(x+1)-c_0} = [\![a]\!]_t^{f(x+1)}. \end{aligned}$$

Mas

$$\sum_{j=0}^{n-1} d_j^2 \leqslant \left(\sum_{j=0}^{n-1} |d_j|\right)^2 \leqslant (c2^n)^2 = c^2 4^n.$$

Então temos que

$$a^{c_0}[\![aa^t]\!]_t^{\hat{f}(x+1)} = [\![a]\!]_t^{f(x+1)} \tag{4.13}$$

com custo $\leqslant c^2 4^n$. Portanto, das equações (4.9)-(4.13) temos que

$$[\![a]\!]_s^{f(x)} = [\![a]\!]_t^{f(x+1)}$$

com custo menor ou igual que

$$\begin{aligned} D_c(n-1) + 2(n-1) + c2^n + c^2 4^n &< c^2 4^n + 2n + c2^n + c^2 4^n \\ &\leqslant c^2 4^n + c^2 4^n + c^2 4^n + c^2 4^n \quad (\text{pois } n \geqslant 2, c \geqslant 1) \\ &= c^2 4^{n+1} \\ &= D_c(n). \end{aligned}$$

□

A seguinte proposição estabelece finalmente o limite superior da função de Dehn de Γ.

Proposição 4.4. *Existe constante $K > 0$ tal que para todo $n \geqslant 1$,*

$$\delta_\Gamma(n) \leqslant K^n \max\{C(i) \mid 1 \leqslant i \leqslant 6n\}.$$

Demonstração. Sabemos que

$$\Gamma/\langle a\rangle^\Gamma = \langle s, t \mid [s,t] = 1\rangle \cong \mathbb{Z}^2.$$

Seja

$$\rho : \Gamma \longrightarrow \Gamma/\langle a\rangle^\Gamma \text{ o homomorfismo canônico.}$$

Seja

$$w \in F(a,s,t) \text{ uma palavra homotopicamente nula em } \Gamma \text{ de comprimento } n.$$

Se w não contém $a^{\pm 1}$ então $w = 1$ em $\Gamma/\langle a \rangle^{\Gamma}$ e $Area_a(w) \leqslant n^2$. Então podemos assumir que w contém algum $a^{\pm 1}$, seja k o número de vezes que $a^{\pm 1}$ aparece em w. Então w tem a forma

$$w = u_1 a^{e_1} v_1,$$

onde $e_1 = \pm 1$, $u_1 \in F(s,t)$, $v_1 \in F(s,a,t)$ e o numero de vezes que $a^{\pm 1}$ aparece em v_1 é $k-1$. Agora,

$$\rho(u_1) = t^{-\beta_1} s^{-\alpha_1}$$

para alguns $\alpha_1, \beta_1 \in \mathbb{Z}$. Sabemos que

$$|\alpha_1| + |\beta_1| \leqslant l(u_1) < n,$$

então como u_1 é uma palavra em s,t, esta pode se converter em $t^{-\beta_1} s^{-\alpha_1}$ em Γ, usando no máximo $l(u_1)^2 < n^2$ vezes a relação $[s,t] = 1$. Assim w é equivalente em Γ a

$$\begin{aligned} t^{-\beta_1} s^{-\alpha_1} a^{e_1} v_1 &= t^{-\beta_1} s^{-\alpha_1} a^{e_1} s^{\alpha_1} t^{\beta_1} t^{-\beta_1} s^{-\alpha_1} v_1 \\ &= a^{e_1 s^{\alpha_1} t^{\beta_1}} t^{-\beta_1} s^{-\alpha_1} v_1 \end{aligned}$$

com custo $< n^2$. Agora,

$$l(t^{-\beta_1} s^{-\alpha_1} v_1) \leqslant |\alpha_1| + |\beta_1| + l(v_1) \leqslant l(u_1) + l(v_1) < l(w) = n,$$

então fazemos o mesmo com a palavra $t^{-\beta_1} s^{-\alpha_1} v_1$ e convertemos ela em $a^{e_2 s^{\alpha_2} t^{\beta_2}} t^{-\beta_2} s^{-\alpha_2} v_2$, com $\beta_2, \alpha_2 \in \mathbb{Z}$, $e_2 = \pm 1$ e $v_2 \in F(a,s,t)$ onde $a^{\pm 1}$ aparece $k-2$ vezes em v_2, com um custo $< n^2$. Logo w se converte em

$$a^{e_1 s^{\alpha_1} t^{\beta_1}} a^{e_2 s^{\alpha_2} t^{\beta_2}} t^{-\beta_2} s^{-\alpha_2} v_2$$

com custo $< 2n^2$. Assim por diante, obtemos que w é equivalente em Γ a

$$\left(\prod_i^k a^{e_i s^{\alpha_i} t^{\beta_i}} \right) v, \quad \text{com } v \in F(s,t), e_i = \pm 1, \alpha_i, \beta_i \in \mathbb{Z}$$

com custo $< kn^2 \leqslant n^3$. Como w é 1 em Γ então

$$1 = \rho(w) = \left(\prod_i^k t^{-\beta_i} s^{-\alpha_i} s^{\alpha_i} t^{\beta_i} \right) \rho(v) = \rho(v),$$

assim $v \in F(s,t)$ representa a identidade em $\langle s,t \,|\, [s,t] = 1 \rangle$, logo pode se converter na palavra vazia usando no máximo $l(v)^2 < n^2$ vezes a relação $[s,t] = 1$. Portanto w é equivalente com

$$w_2 := \prod_i^k a^{e_i s^{\alpha_i} t^{\beta_i}}$$

com custo $< n^3 + n^2 \leqslant 2n^3$.

A ideia agora é usar o Lema 4.6 para $f(x) = x^{\alpha_i}$, mas precisaríamos que α_i não fosse negativo. Então consideramos

$$\alpha := \min_i \alpha_i.$$

Assim, $0 \leqslant \alpha_i - \alpha \leqslant 2n$. Sabemos que o custo de converter w_2 na palavra vazia é o mesmo custo de converter $w_2^{s^{-\alpha}}$ na palavra vazia, então temos

$$w_2' := w_2^{s^{-\alpha}} = \prod_{i=1}^{k} a^{e_i s^{\alpha_i} t^{\beta_i} s^{-\alpha}}.$$

Como $|\beta_i|, |\alpha| \leqslant n$, podemos converter $t^{\beta_i} s^{-\alpha}$ em $s^{-\alpha} t^{\beta_i}$ usando no máximo n^2 vezes a relação $[s,t] = 1$, logo converter $a^{e_i s^{\alpha_i} t^{\beta_i} s^{-\alpha}}$ em $a^{e_i s^{\alpha_i - \alpha} t^{\beta_i}}$ tem custo $\leqslant 2n^2$, então como $k \leqslant n$ podemos converter w_2' em

$$w_3 := \prod_{i=1}^{k} a^{e_i s^{\alpha_i - \alpha} t^{\beta_i}}$$

com custo $\leqslant 2n^3$. Agora,

$$w_3 = \prod_{i=1}^{k} \left([\![a]\!]_s^{x^{\alpha_i - \alpha}} \right)^{e_i t^{\beta_i}}$$

e usamos o Lema 4.6 k vezes, convertendo w_3 em

$$w_4 = \prod_{i=1}^{k} \left([\![a]\!]_t^{(x+1)^{\alpha_i - \alpha}} \right)^{e_i t^{\beta_i}}$$

com custo de no máximo $kD_1(\alpha_i - \alpha) \leqslant nD_1(2n)$. Notamos que

$$w_4 = \prod_{i=1}^{k} \left(\prod_{j=0}^{\alpha_i - \alpha} a^{b_{ij} t^j} \right)^{e_i t^{\beta_i}} \text{ com } b_{ij} = \binom{\alpha_i - \alpha}{j},\ 0 \leqslant j \leqslant \alpha_i - \alpha$$

que com custo 0 convertemos em

$$\begin{aligned} w_5 : &= \prod_{i=1}^{k} \left(\prod_{j=0}^{\alpha_i - \alpha} a^{e_i b_{ij} t^{j + \beta_i}} \right) \\ &= \prod_{m=1}^{l} a^{\mu_m t^{\gamma_m}}, \end{aligned}$$

onde $l, \mu_m, \gamma_m \in \mathbb{Z}$ satisfazem

$$\begin{aligned} l &\leqslant k \max_i(\alpha_i - \alpha + 1) \leqslant n(2n+1), \\ |\mu_m| &\leqslant \max\{\, |b_{ij}| \mid 1 \leqslant i \leqslant k,\ 0 \leqslant j \leqslant \alpha_i - \alpha\} \\ &\leqslant \max\left\{ \binom{i}{j} \;\middle|\; 1 \leqslant i \leqslant 2n, 0 \leqslant j \leqslant i \right\} \leqslant 2^{2n}, \\ |\gamma_m| &\leqslant \max\{\, j + |\beta_i| \mid 1 \leqslant i \leqslant k,\ 0 \leqslant j \leqslant \alpha_i - \alpha\} \\ &\leqslant \max\{\, \alpha_i - \alpha + |\beta_i| \mid 1 \leqslant i \leqslant k\} \leqslant 3n. \end{aligned}$$

Temos então que w_5 é produto de no máximo

$$l \cdot \max_m \mu_m \leqslant n(2n+1)2^{2n}$$

termos da forma $a^{\pm t^{\gamma_i}}$ onde $|\gamma_i| \leqslant 3n$. Agora, a relação $\left[a^{t^i}, a^{t^j}\right] = 1$ é equivalente com $\left[a, a^{t^m}\right] = 1$, onde $m = |i-j|$, então para poder comutar os termos de w_5 basta fazer uso das relações $\left[a, a^{t^i}\right] = 1$, para $0 \leqslant i \leqslant \max\{\,|\gamma_m - \gamma_r| \,|\, 0 \leqslant m, r \leqslant l\} \leqslant 6n$, assim qualquer reordenação dos termos de w_5 pode ser alcançada usando no máximo $(n(2n+1)2^{2n})^2$ vezes estas relações, logo o custo é no máximo

$$(n(2n+1)2^{2n})^2 \max\{C(i)\,|0 \leqslant i \leqslant 6n\,\}.$$

Agora,

$$w_5 \in \langle a, t\rangle = \left\langle a, t \;\middle|\; \left[a, a^{t^k}\right] = 1, k \in \mathbb{Z} \right\rangle$$

representa o elemento identidade deste grupo (pois é homotopicamente nula dado que é igual a um conjugado de w em Γ e w é homotopicamente nula), então existe uma reordenação dos termos $a^{\pm t^{\gamma_i}}$ de w_5 de forma que a palavra resultante, reduzida como elemento do grupo livre $F(a,t)$ é a palavra vazia (esta redução tem custo 0); esta reordenação tem então custo $\leqslant (n(2n+1)2^{2n})^2 \max\{C(i)\,|0 \leqslant i \leqslant 6n\,\}$ a partir de w_5.
Portanto, somando os custos desde w até w_5, temos que

$$\begin{aligned}\delta_\Gamma(n) &\leqslant 2n^3 + 2n^3 + nD_1(2n) + (n(2n+1)2^{2n})^2 \max\{C(i)\,|0 \leqslant i \leqslant 6n\,\} \\ &= 2n^3 + 2n^3 + n4^{2n+1} + (n(2n+1)2^{2n})^2 \max\{C(i)\,|0 \leqslant i \leqslant 6n\,\} \\ &\leqslant K^n \max\{C(i)\,|0 \leqslant i \leqslant 6n\,\} \quad \text{para } K \text{ suficientemente grande.}\end{aligned} \tag{4.14}$$

□

Finalmente, temos

$$\begin{aligned}\delta_\Gamma(n) &\preceq K^n \max\{C(i)\,|0 \leqslant i \leqslant 6n\,\} \\ &\preceq K^n 4^{6n} \quad \text{(pelo Lema 4.5)} \\ &\simeq 2^n,\end{aligned} \tag{4.15}$$

e junto com a Proposição 4.3 temos provado o seguinte teorema.

Teorema 4.1. *A função de Dehn de* Γ *satisfaz* $\delta_\Gamma(n) \simeq 2^n$.

Do resultado anterior pode-se concluir que o problema da palavra em Γ é de tipo não polinomial. Na seguinte seção vamos ver que acrescentando uma relação de torção no gerador a de Γ, o problema da palavra no grupo resultante vira polinomial.

4.4 Uma função isoperimétrica polinomial para o grupo Γ_m

Agora vamos calcular um limite superior para a função de Dehn do grupo

$$\Gamma_m = \langle a, s, t \,|\, [a, a^t] = 1, [s, t] = 1, a^s = aa^t, a^m = 1\rangle.$$

Introduzimos a seguinte notação análoga à do Lema 4.6. Dado $f(x) = \sum_{i=0}^{n} \hat{c}_i x^i \in \mathbb{Z}[x]$ e símbolos a, r, definimos

$$\{\!\{a\}\!\}_r^f := a^{c_0} r^{-1} a^{c_1} r^{-1} \cdots a^{c_{n-1}} r^{-1} a^{c_n} r^n,$$

onde $c_i \in \{0, 1, \ldots, m-1\}$ e $c_i \equiv \hat{c}_i \,(mod\, m)$. Temos de novo

$$\{\!\{a\}\!\}_r^f = a^{c_0} a^{c_1 r} \cdots a^{c_{n-1} r^{n-1}} a^{c_n r^n}$$

e o seguinte análogo do Lema 4.6.

Lema 4.7. $\{\!\{a\}\!\}_s^{f(x)} = \{\!\{a\}\!\}_t^{f(x+1)}$ *em* Γ_m *e esta igualdade tem custo no máximo* $K_m(n) := 10m^2n^2 + 10$.

Demonstração. A prova é análoga com a do Lema 4.6, adaptando os custos ao usar a relação $a^m = 1$. Fazemos indução por n. No caso $n = 0$, as duas palavras são a^{c_0} e temos custo 0. Tomamos $n \geqslant 1$ e supomos que o lema vale para todo $k < n$. Seja $\hat{f}(x) = \sum_{i=1}^{n} \hat{c}_i x^{i-1}$, então $f(x) = \hat{c}_0 + x\hat{f}(x)$. Fazendo a mesma conta, vale o análogo de (4.9) em Γ_m,

$$\{\!\{a\}\!\}_s^{f(x)} = a^{c_0} \left(\{\!\{a\}\!\}_s^{\hat{f}(x)}\right)^s,$$

com custo 0. Por hipótese de indução temos

$$a^{c_0} \left(\{\!\{a\}\!\}_s^{\hat{f}(x)}\right)^s = a^{c_0} \left(\{\!\{a\}\!\}_t^{\hat{f}(x+1)}\right)^s,$$

com custo no máximo $K_m(n-1)$; também vale a mesma conta feita para (4.11) e obtemos

$$a^{c_0} \left(\{\!\{a\}\!\}_t^{\hat{f}(x+1)}\right)^s = a^{c_0} \{\!\{a^s\}\!\}_t^{\hat{f}(x+1)}$$

com custo no máximo $2(n-1)$. Escrevemos $\hat{f}(x+1) = \sum_{j=0}^{n-1} \hat{d}_j x^j$, e tomamos $d_j \in \{0, 1, \ldots, m-1\}$ tais que $d_j \equiv \hat{d}_j \,(mod\, m)$, então vale o análogo de (4.12)

$$a^{c_0} \{\!\{a^s\}\!\}_t^{\hat{f}(x+1)} = a^{c_0} \{\!\{aa^t\}\!\}_t^{\hat{f}(x+1)}$$

mas neste caso tem custo no máximo

$$\sum_{j=0}^{n-1} d_j \leqslant \sum_{j=0}^{n-1} m = nm.$$

Por último, das conta feitas para (4.13) temos que

$$a^{c_0}\{\!\{aa^t\}\!\}_t^{\hat{f}(x+1)} = a^{c_0}a^{d_0}a^{(d_0+d_1)t}a^{(d_1+d_2)t^2}\cdots a^{(d_{n-2}+d_{n-1})t^{n-1}}a^{d_{n-1}t^n} \quad \left(\text{custo} \leqslant \sum_{j=0}^{n-1} d_j^2\right)$$
$$= a^{c_0}a^{d_0}a^{k_1t}a^{k_2t^2}\cdots a^{k_{n-1}t^{n-1}}a^{d_{n-1}t^n} \quad (\text{custo} \leqslant n-1, \text{ usa } a^m = 1),$$

onde $k_i \in \{0,\dots,m-1\}$ e $k_i \equiv d_{i-1} + d_i \pmod m$. Notamos que $0 \leqslant d_{i-1} + d_i < 2m$ justifica o custo anterior. Além disso, escrevendo $(x+1)\hat{f}(x+1) = \sum_{i=0}^{n} \hat{k}_i x^i$ temos que

$$\begin{aligned}
&\hat{k}_0 = \hat{d}_0 \equiv d_0 \pmod m,\\
&\hat{k}_n = \hat{d}_{n-1} \equiv d_{n-1} \pmod m, \text{ e}\\
&\hat{k}_i = \hat{d}_{i-1} + \hat{d}_i \equiv d_{i-1} + d_i \equiv k_i \pmod m, \quad i \in \{1,\dots,n-1\}.
\end{aligned}$$

Portanto

$$\begin{aligned}
a^{c_0}a^{d_0}a^{k_1t}a^{k_2t^2}\cdots a^{k_{n-1}t^{n-1}}a^{d_{n-1}t^n} &= a^{c_0}\{\!\{a\}\!\}_t^{(x+1)\hat{f}(x+1)}\\
&= a^{c_0}\{\!\{a\}\!\}_t^{f(x+1)-\hat{c_0}}\\
&= \{\!\{a\}\!\}_t^{f(x+1)} \quad (\text{custo } 1,\ a^m = 1).
\end{aligned}$$

Logo

$$a^{c_0}\{\!\{aa^t\}\!\}_t^{\hat{f}(x+1)} = \{\!\{a\}\!\}_t^{f(x+1)}$$

com custo no máximo

$$\sum_{j=0}^{n-1} d_j^2 + n - 1 + 1 \leqslant \sum_{j=0}^{n-1} m^2 + n = nm^2 + n.$$

Finalmente, concluímos que

$$\{\!\{a\}\!\}_s^{f(x)} = \{\!\{a\}\!\}_t^{f(x+1)}$$

com custo no máximo

$$\begin{aligned}
&K_m(n-1) + 2(n-1) + mn + nm^2 + n\\
&= 10m^2(n-1)^2 + 8 + (3 + m + m^2)n\\
&= 10m^2n^2 \underbrace{-20m^2n + 10m^2 + (3+m+m^2)n}_{<0} + 8\\
&< 10m^2n^2 + 10.
\end{aligned}$$

□

Agora, dados $f, g \in \mathbb{Z}[x]$ definimos

$$\begin{aligned}
\sigma_{f,g} &:= \{\!\{a\}\!\}_s^f \{\!\{a\}\!\}_s^g (\{\!\{a\}\!\}_s^{f+g})^{-1}\\
\tau_{f,g} &:= \{\!\{a\}\!\}_t^f \{\!\{a\}\!\}_t^g (\{\!\{a\}\!\}_t^{f+g})^{-1}.
\end{aligned}$$

Como $[a, a^{t^n}] = 1$ para todo $n \in \mathbb{Z}$, é claro que $\tau_{f,g}$ representa o elemento identidade em Γ (e portanto em Γ_m). Vamos precisar dos seguintes lemas para calcular $Area_a(\tau_{f,g})$ em Γ_m.

Lema 4.8. *Para* $n \geqslant \max\{grau(f), grau(g)\}$

$$Area_a(\tau_{f,g}) \leqslant Area_a(\tau_{f\pm 1,g}) + 2$$
$$Area_a(\tau_{f,g}) \leqslant Area_a(\tau_{f,g\pm x^n}) + 2.$$

Demonstração. Sejam

$$f(x) = \sum_{i=0}^{n_1} \hat{b}_i x^i,\ g(x) = \sum_{i=0}^{n_2} \hat{c}_i x^i,\ (f+g)(x) = \sum_{i=0}^{n_3} \hat{d}_i x^i,$$

onde $b_i, c_i, d_i \in \{0, \ldots, m-1\}$ com $b_i \equiv \hat{b}_i$, $c_i \equiv \hat{c}_i$, $d_i \equiv \hat{d}_i \pmod m$. Temos que

$$Area_a(\tau_{f,g}) = Area_a((\tau_{f,g})^{a^{\pm 1}}),$$

mas

$$\begin{aligned}
(\tau_{f,g})^{a^{\mp 1}} &= a^{\pm 1} \{\!\{a\}\!\}_t^f \{\!\{a\}\!\}_t^g (\{\!\{a\}\!\}_t^{f+g})^{-1} a^{\mp 1} \\
&= a^{\pm 1} a^{b_0} t^{-1} \cdots a^{b_{n_1-1}} t^{-1} a^{b_{n_1}} t^{n_1} \{\!\{a\}\!\}_t^g t^{-n_3} a^{-d_{n_3}} t a^{-d_{n_3-1}} \cdots t a^{-d_0} a^{\mp 1} \\
&= a^{b'_0} t^{-1} \cdots a^{b_{n_1-1}} t^{-1} a^{b_{n_1}} t^{n_1} \{\!\{a\}\!\}_t^g t^{-n_3} a^{-d_{n_3}} t a^{-d_{n_3-1}} \cdots t a^{-d'_0} \quad (\text{custo } \leqslant 2,\ a^m = 1) \\
&= \tau_{f\pm 1,g},
\end{aligned}$$

onde $b_0, d_0 \in \{0, 1 \ldots, m-1\}$ e $b'_0 \equiv b_0 \pm 1$, $d'_0 \equiv d_0 \pm 1 \pmod m$. Assim

$$Area_a(\tau_{f,g}) \leqslant Area_a(\tau_{f\pm 1,g}) + 2.$$

Agora,

$$\begin{aligned}
\tau_{f,g} &= \{\!\{a\}\!\}_t^f \{\!\{a\}\!\}_t^g (\{\!\{a\}\!\}_t^{f+g})^{-1} \\
&= \{\!\{a\}\!\}_t^f a^{c_0} t^{-1} \cdots a^{c_{n_2-1}} t^{-1} a^{c_{n_2}} t^{n_2} t^{-n_3} a^{-d_{n_3}} t a^{-d_{n_3-1}} \cdots t a^{-d_0}
\end{aligned} \tag{4.16}$$

temos as seguintes possibilidades em (4.16). Se $n = n_2 = n_3$,

$$\begin{aligned}
\tau_{f,g} &= \{\!\{a\}\!\}_t^f a^{c_0} t^{-1} \cdots a^{c_{n-1}} t^{-1} a^{c_n} a^{-d_n} t a^{-d_{n-1}} \cdots t a^{-d_0} \\
&= \{\!\{a\}\!\}_t^f a^{c_0} t^{-1} \cdots a^{c_{n-1}} t^{-1} a^{c_n} a^{\pm 1} t^n t^{-n} a^{\mp 1} a^{-d_n} t a^{-d_{n-1}} \cdots t a^{-d_0} \\
&= \{\!\{a\}\!\}_t^f a^{c_0} t^{-1} \cdots a^{c_{n-1}} t^{-1} a^{c'_n} t^n t^{-n} a^{-d'_n} t a^{-d_{n-1}} \cdots t a^{-d_0} \quad (\text{custo } \leqslant 2,\ a^m = 1) \\
&= \tau_{f,g\pm x^n}
\end{aligned}$$

onde $c_n, d_n \in \{0, 1 \ldots, m-1\}$ e $c'_n \equiv c_n \pm 1$, $d'_n \equiv d_n \pm 1 \pmod m$.
Se $n = n_3 > n_2$,

$$\begin{aligned}
\tau_{f,g} &= \{\!\{a\}\!\}_t^f a^{c_0} t^{-1} \cdots a^{c_{n_2-1}} t^{-1} a^{c_{n_2}} t^{n_2} t^{-n} a^{-d_n} t a^{-d_{n-1}} \cdots t a^{-d_0} \\
&= \{\!\{a\}\!\}_t^f a^{c_0} t^{-1} \cdots a^{c_{n_2-1}} t^{-1} a^{c_{n_2}} \underbrace{t^{-1} \cdots t^{-1}}_{n-n_2 \text{ vezes}} a^{-d_n} t a^{-d_{n-1}} \cdots t a^{-d_0} \\
&= \{\!\{a\}\!\}_t^f a^{c_0} t^{-1} \cdots a^{c_{n_2-1}} t^{-1} a^{c_{n_2}} \underbrace{t^{-1} \cdots t^{-1}}_{n-n_2 \text{ vezes}} a^{\pm 1} t^n t^{-n} a^{\mp 1} a^{-d_n} t a^{-d_{n-1}} \cdots t a^{-d_0} \\
&= \{\!\{a\}\!\}_t^f \{\!\{a\}\!\}_t^{g\pm x^n} t^{-n} a^{-d'_n} t a^{-d_{n-1}} \cdots t a^{-d_0} (\text{custo } \leqslant 1,\ a^m = 1) \\
&= \tau_{f,g\pm x^n},
\end{aligned}$$

onde d'_n é como no caso anterior.
Por último, se $n > n_3 \geqslant n_2$,

$$\begin{aligned}
\tau_{f,g} &= \{\!\{a\}\!\}_t^f a^{c_0}t^{-1}\cdots a^{c_{n_2-1}}t^{-1}a^{c_{n_2}}t^{n_2}t^{-n}t^{n}t^{-n_3}a^{-d_{n_3}}ta^{-d_{n_3-1}}\cdots ta^{-d_0}\\
&= \{\!\{a\}\!\}_t^f a^{c_0}t^{-1}\cdots a^{c_{n_2-1}}t^{-1}a^{c_{n_2}}t^{-(n-n_2)}t^{n-n_3}a^{-d_{n_3}}ta^{-d_{n_3-1}}\cdots ta^{-d_0}\\
&= \{\!\{a\}\!\}_t^f a^{c_0}t^{-1}\cdots a^{c_{n_2-1}}t^{-1}a^{c_{n_2}}t^{-(n-n_2)}a^{\pm 1}t^{n}t^{-n}a^{\mp 1}t^{n-n_3}a^{-d_{n_3}}ta^{-d_{n_3-1}}\cdots ta^{-d_0}\\
&= \tau_{f,g\pm x^n}
\end{aligned}$$

logo em todo caso temos que

$$Area_a \leqslant Area_a(\tau_{f,g\pm x^n}) + 2.$$

□

Lema 4.9. *Para* $n = 1 + \max\{grau(f), grau(g)\}$

$$Area_a(\tau_{(x+1)f,(x+1)g}) \leqslant Area_a(\tau_{f,g}) + 6K_m(n).$$

Demonstração.

$$\begin{aligned}
\tau_{(x+1)f,(x+1)g} &= \{\!\{a\}\!\}_t^{(x+1)f}\{\!\{a\}\!\}_t^{(x+1)g}\left(\{\!\{a\}\!\}_t^{(x+1)f+(x+1)g}\right)^{-1}\\
&= \{\!\{a\}\!\}_s^{xf(x-1)}\{\!\{a\}\!\}_s^{xg(x-1)}\left(\{\!\{a\}\!\}_s^{xf(x-1)+xg(x-1)}\right)^{-1} \quad \text{(custo } 3K_m(n),\ \text{Lema 4.7)}\\
&= \sigma_{xf(x-1),xg(x-1)}.
\end{aligned}$$

Agora, dados $f_1, g_1 \in \mathbb{Z}[x]$, com $f_1(x) = \sum_{i=0}^{l}\hat{b}_i x^i$, $b_i \in \{1,\ldots,m-1\}$ e $b_i \equiv \hat{b}_i \pmod m$,

$$\begin{aligned}
\{\!\{a\}\!\}_s^{xf_1} &= s^{-1}a^{b_0}s^{-1}\cdots a^{b_{l-1}}s^{-1}a^{b_l}s^{l+1}\\
&= \left(a^{b_0}s^{-1}\cdots a^{b_{l-1}}s^{-1}a^{b_l}s^{l}\right)^s\\
&= \left(\{\!\{a\}\!\}_s^{f_1}\right)^s,
\end{aligned}$$

logo

$$\begin{aligned}
\sigma_{xf_1,xg_1} &= \{\!\{a\}\!\}_s^{xf_1}\{\!\{a\}\!\}_s^{xg_1}\left(\{\!\{a\}\!\}_s^{xf_1+xg_1}\right)^{-1}\\
&= \left(\{\!\{a\}\!\}_s^{f_1}\right)^s\left(\{\!\{a\}\!\}_s^{g_1}\right)^s\left(\left(\{\!\{a\}\!\}_s^{f_1+g_1}\right)^{-1}\right)^s\\
&= \left(\sigma_{f_1,g_1}\right)^s
\end{aligned}$$

com custo 0. Assim,

$$\begin{aligned}
\sigma_{xf(x-1),xg(x-1)} &= \left(\sigma_{f(x-1),g(x-1)}\right)^s\\
&= \left(\{\!\{a\}\!\}_s^{f(x-1)}\{\!\{a\}\!\}_s^{g(x-1)}\left(\{\!\{a\}\!\}_s^{f(x-1)+g(x-1)}\right)^{-1}\right)^s\\
&= \left(\{\!\{a\}\!\}_t^{f}\{\!\{a\}\!\}_t^{g}\left(\{\!\{a\}\!\}_t^{f+g}\right)^{-1}\right)^s \quad \text{(custo } 3K_m(n-1),\ \text{Lema 4.7)}\\
&= \left(\tau_{f,g}\right)^s
\end{aligned}$$

e como os custos de converter $(\tau_{f,g})^s$ ou $\tau_{f,g}$ em 1 são iguais, temos que

$$\begin{aligned} Area_a(\tau_{(x+1)f,(x+1)g}) &\leqslant Area_a((\tau_{f,g})^s) + 3K_m(n) + 3K_m(n-1) \\ &\leqslant Area_a(\tau_{f,g}) + 6K_m(n). \end{aligned}$$

□

Proposição 4.5. *Sejam $f, g \in \mathbb{Z}[X]$ de grau no máximo n, então*

$$Area_a(\tau_{f,g}) \leqslant 6nK_m(n) + 4mn + 1.$$

Demonstração. Por indução em n. No caso $n = 0$ temos $f = \hat{b}_0$, $g = \hat{c}_0$, $f + g = \hat{b}_0 + \hat{c}_0$ com $b_0 \equiv \hat{b}_0$, $c_0 \equiv \hat{c}_0$, $d_0 \equiv \hat{b}_0 + \hat{c}_0 \pmod m$ e $b_0, c_0, d_0 \in \{1, \ldots, m-1\}$, assim

$$\begin{aligned} \tau_{f,g} &= a^{b_0} a^{c_0} a^{-d_0} = a^{b_0+c_0} a^{-d_0} \\ &= a^{d_0} a^{-d_0} \quad (\text{custo } \leqslant 1,\ a^m = 1) \\ &= 1 \\ (\Longrightarrow) \quad & Area_a(\tau_{f,g}) \leqslant 1. \end{aligned}$$

Consideramos $n \geqslant 1$ e supomos que o resultado vale para $k < n$. Podemos assumir que $grau(f) \geqslant 1$, caso contrário, temos $f = \hat{b}_0$, $g = \sum_{i=0}^{n_0} \hat{c}_i x^i$, $f + g = \sum_{i=1}^{n_0} \hat{c}_i x^i + (\hat{b}_0 + \hat{c}_0)$ com $b_0 \equiv \hat{b}_0$, $c_i \equiv \hat{c}_i$, $d_0 \equiv \hat{b}_0 + \hat{c}_0 \pmod m$ e $b_0, c_i, d_0 \in \{0, 1, \ldots, m-1\}$, onde

$$\begin{aligned} \tau_{f,g} &= a^{b_0} \{\!\{a\}\!\}_t^g t^{-n_0} a^{-c_{n_0}} t a^{-c_{n_0-1}} \cdots t a^{-c_1} t a^{-d_0} \\ &= a^{b_0} \{\!\{a\}\!\}_t^g t^{-n_0} a^{-c_{n_0}} t a^{-c_{n_0-1}} \cdots t a^{-c_1} t a^{-(c_0+b_0)} \quad (\text{custo } \leqslant 1,\ a^m = 1) \\ &= a^{b_0} \{\!\{a\}\!\}_t^g (\{\!\{a\}\!\}_t^g)^{-1} a^{-b_0} \\ &= 1. \\ (\Longrightarrow) \quad & Area_a(\tau_{f,g}) \leqslant 1. \end{aligned}$$

Pelo algoritmo de Euclides podemos adicionar um inteiro $\hat{r}$ a f de forma que

$$f_0(x) := f(x) + \hat{r} = (x+1) f_1(x).$$

E igualmente existe um inteiro $\hat{q}$ tal que ao adicionar $\hat{q}x^n$ a g obtemos

$$g_0(x) := g(x) + \hat{q}x^n = (x+1) g_1(x)$$

(notamos que $grau(f_1), grau(g_1) \leqslant n-1$). Sejam $r, q \in \{0, 1, \ldots, m-1\}$ tais que $r \equiv \hat{r}$, $q \equiv \hat{q} \pmod m$, temos que

$$\tau_{(x+1)f_1,(x+1)g_1} = \tau_{f_0,g_0} = \tau_{f+\hat{r},g+\hat{q}x^n} = \tau_{f+r,g+qx^n}, \quad \text{então}$$

$$\begin{aligned}
Area_a(\tau_{f,g}) &\leqslant Area_a(\tau_{f+r,g}) + 2m && \text{(Lema 4.8)}\\
&\leqslant Area_a(\tau_{f+r,g+qx^n}) + 4m && \text{(Lema 4.8)}\\
&= Area_a(\tau_{(x+1)f_1,(x+1)g_1}) + 4m\\
&\leqslant Area_a(\tau_{f_1,g_1}) + 6K_m(n) + 4m && \text{(Lema 4.9)}\\
&\leqslant 6(n-1)K_m(n-1) + 4m(n-1) + 1 + 6K_m(n) + 4m && \text{(Hipótese de indução)}\\
&\leqslant 6nK_m(n) + 4mn + 1.
\end{aligned}$$

□

Agora temos todas as ferramentas necessárias para achar um limite superior para a função de Dehn de Γ_m.

Teorema 4.2. *A função de Dehn de Γ_m satisfaz $\delta_{\Gamma_m}(n) \preceq n^4$ para todo m.*

Demonstração. Seja $w \in F(a,s,t)$ uma palavra homotopicamente nula em Γ_m, de comprimento n. Tal como foi feito na prova da Proposição 4.4 convertemos w em

$$w_2 := \prod_i^k a^{e_i s^{\alpha_i} t^{\beta_i}}$$

com custo no máximo $2n^3$, onde $e_i = \pm 1$, $\alpha_i, \beta_i \in \mathbb{Z}$, $|\alpha_i| + |\beta_i| \leqslant n$ e $k \leqslant n$.
Sejam $\alpha = \min_i \alpha_i$ e $\beta = \min_i \beta_i$, então o custo de converter w_2 na palavra vazia é igual ao custo de converter $w_2' := w_2^{s^{-\alpha}t^{-\beta}}$ na palavra vazia. Temos que

$$w_2' = \prod_{i=1}^k a^{e_i s^{\alpha_i} t^{\beta_i} s^{-\alpha} t^{-\beta}}.$$

Como $|\beta_i|, |\alpha| \leqslant n$ podemos converter $t^{\beta_i} s^{-\alpha}$ em $s^{-\alpha} t^{\beta_i}$ usando no máximo n^2 vezes a relação $[s,t] = 1$, então converter $a^{e_i s^{\alpha_i} t^{\beta_i} s^{-\alpha} t^{-\beta}}$ em $a^{e_i s^{\alpha_i - \alpha} t^{\beta_i - \beta}}$ tem custo $\leqslant 2n^2$ e portanto podemos converter w_2' em

$$w_3 := \prod_{i=1}^k a^{e_i s^{\alpha_i - \alpha} t^{\beta_i - \beta}}$$

com custo $\leqslant 2n^3$, pois $k \leqslant n$. Agora, $a^{e_i s^{\alpha_i - \alpha} t^{\beta_i - \beta}} = (a^{s^{\alpha_i - \alpha}})^{e_i t^{\beta_i - \beta}}$ com custo 0, então tomando $f_i(x) = x^{\alpha_i - \alpha}$ temos que w_3 pode se converter com custo 0 em

$$\prod_{i=1}^k (a^{s^{\alpha_i - \alpha}})^{e_i t^{\beta_i - \beta}} = \prod_{i=1}^k \left(\{\!\{a\}\!\}_s^{f_i} \right)^{e_i t^{\beta_i - \beta}},$$

que pelo Lema 4.7 se converte em

$$w_4 := \prod_{i=1}^k \left(\{\!\{a\}\!\}_t^{f_i(x+1)} \right)^{e_i t^{\beta_i - \beta}}$$

com custo de no máximo $nK_m(n)$, pois $grau(f_i) = \alpha_i - \alpha \leqslant n$ e $k \leqslant n$.
Convertemos cada $\left(\{\!\{a\}\!\}_t^{f_i(x+1)}\right)^{e_i}$ onde $e_i = -1$ em $\{\!\{a\}\!\}_t^{-f_i(x+1)}$ da seguinte forma: consideramos $\tau_{f,g}$ com $f = f_i(x+1)$, $g = -f_i(x+1)$, então

$$\begin{aligned}\tau_{f_i(x+1),-f_i(x+1)} &= \{\!\{a\}\!\}_t^{f_i(x+1)}\{\!\{a\}\!\}_t^{-f_i(x+1)}\left(\{\!\{a\}\!\}_t^{f_i(x+1)-f_i(x+1)}\right)^{-1}\\ &= \{\!\{a\}\!\}_t^{f_i(x+1)}\{\!\{a\}\!\}_t^{-f_i(x+1)},\end{aligned}$$

logo pela Proposição 4.5, $\left(\{\!\{a\}\!\}_t^{f_i(x+1)}\right)^{-1} = \{\!\{a\}\!\}_t^{-f_i(x+1)}$ em Γ_m com custo $\leqslant 6nK_m(n) + 4mn + 1$. Assim convertemos w_4 em

$$w_5 := \prod_{i=1}^{k}\left(\{\!\{a\}\!\}_t^{e_i f_i(x+1)}\right)^{t^{\beta_i-\beta}} = \prod_{i=1}^{k}\{\!\{a\}\!\}_t^{g_i},$$

onde $g_i = e_i x^{\beta_i-\beta} f_i(x+1)$, com custo $\leqslant 6n^2K_m(n) + 4mn^2 + n$.
Agora, para cada $1 \leqslant i < k$ temos a igualdade

$$\{\!\{a\}\!\}_t^{\sum_{j=1}^{i} g_j}\{\!\{a\}\!\}_t^{g_{i+1}} = \{\!\{a\}\!\}_t^{\sum_{j=1}^{i+1} g_j}$$

com custo $\leqslant 6nK_m(n)+4mn+1$ por causa da proposição 4.5, ao considerar $f = \sum_{j=1}^{i} g_j$, $g = g_{i+1}$ e

$$\tau_{f,g} = \{\!\{a\}\!\}_t^{\sum_{j=1}^{i} g_j}\{\!\{a\}\!\}_t^{g_{i+1}}\left(\{\!\{a\}\!\}_t^{\sum_{j=1}^{i+1} g_j}\right)^{-1}.$$

Então convertemos w_5 em

$$w_6 := \{\!\{a\}\!\}_t^{\sum_{j=1}^{k} g_j}$$

com custo $\leqslant 6n^2K_m(n) + 4mn^2 + n$. Temos que

$$\sum_{j=1}^{k} g_j = \sum_{i=0}^{N} \hat{b}_i x^i$$

para alguns $\hat{b_i} \in \mathbb{Z}$, $N \in \mathbb{N}$. Sejam $b_i \in \{1, \ldots, m-1\}$, tais que $b_i \equiv \hat{b_i} \pmod m$, então tomando $h(x) := \sum_{i=0}^{N} b_i x^i$ é claro que $w_6 = \{\!\{a\}\!\}_t^h$. De outro lado

$$w_6 = \{\!\{a\}\!\}_t^h = a^{b_0}a^{b_1 t}\cdots a^{b_N t^N},$$

portanto w_6 não depende de s e é produto de conjugados de a, então w_6 representa o elemento identidade do subgrupo $B := \langle a\rangle^{\Gamma_m} \cap \langle a, t\rangle$, mas como foi visto no final da prova da Proposição 4.2,

$$B \cong \mathbb{Z}_m[t, t^{-1}].$$

Neste isomorfismo $w_6 \mapsto 0$, $a \mapsto 1$, e $\{\!\{a\}\!\}_t^h \mapsto h$, logo $h = 0$. Assim, w_6 é a palavra vazia.

Finalmente, ao somar os custos obtemos que

$$\begin{aligned}\delta_{\Gamma_m}(n) &\leqslant 4n^3 + nK_m(n) + 12n^2K_m(n) + 8mn^2 + 2n \\ &= 4n^3 + 10m^2n^3 + 10n + 120m^2n^4 + 120n^2 + 8mn^2 + 2n \\ &\leq n^4.\end{aligned}$$

□

Referências

[1] G. Baumslag. A finitely presented metabelian group with a free abelian derived group of infinite rank. In *Proc. Am. Math. Soc*, volume 35, pages 61–62, 1972.

[2] T. S. Blyth. *Module Theory: An approach to linear algebra*. University of St Andrews, 2018.

[3] M. R. Bridson. The geometry of the word problem. *Invitations to geometry and topology*, 7:29–91, 2002.

[4] D. E. Cohen. *Combinatorial group theory: a topological approach*, volume 14. Cambridge University Press, 1989.

[5] W. Dison. Isoperimetric functions for subdirect products and Bestvina-Brady groups, 2008.

[6] S. M. Gersten. Isoperimetric and isodiametric functions of finite presentations. geometric group theory, vol. 1 (sussex, 1991), 79–96. *London Math. Soc. Lecture Note Ser*, 181:389–421.

[7] M. Kassabov and T. R. Riley. The dehn function of baumslag's metabelian group. *Geometriae Dedicata*, 158(1):109–119, 2012.

[8] J. Rotman. *An Introduction to the Theory of Groups*, volume 148. Springer Science & Business Media, 1999.